

# Cover Letter



May 19, 2022

Object Management Group  
9C Medway Road, PMB 274  
Milford, MA 01757 (USA)

US Federal Reserve Systems Board of Governors  
20th Street & Constitution Ave, NW  
Washington DC 20551

RE: The Money and Payments: The U.S. Dollar in the Age of Digital Transformation

Greetings,

The Object Management Group® (OMG®) welcomes the opportunity to submit the attached responses to the Federal Reserve (FR) regarding the paper titled “Money and Payments: The U.S. Dollar in the Age of Digital Transformation” and has some general comments below. Specific responses to the questions posed in the discussion paper are attached.

**OMG:** The Object Management Group ([www.omg.org](http://www.omg.org)) is an international, open membership, not-for-profit technology standards consortium, positioned as a Voluntary Standards Consensus Body (VSCB) aka Standards Development Organization (SDO). Founded in 1989, its mission is to develop technical standards for a wide range of industries including artificial intelligence, automotive, business, cybersecurity, defense, finance, government, healthcare, Industrial Internet of Things (“IIoT”), insurance, manufacturing, middleware, and related services, and space. OMG also oversees the Consortium for Information and Software Quality™ (CISQ™), the Data Distribution Service™ (DDS®) foundation, the Digital Twin Consortium® (DTC™), the Industry IoT Consortium® (IIC), Augmented Reality for Enterprise Alliance™ (AREATM) and Responsible Computing™ (RCTM).

OMG is representative of an important subset of US and international stakeholders, which is those building products and services, as in the FR’s objective “to give entrepreneurs a platform to create new financial products and services; support faster and cheaper payments (including cross-border payments);”. OMG’s relevance has been proven over the years with standards like UML, SysML, UAF, Financial Industry Business Ontology® (FIBO®), Financial Instrument Global Identifier® (FIGI®), Structured Metrics Metamodel (SMMTM), Semantics of Business Vocabulary and Rules™ (SBVRTM).

OMG is dedicated to bringing together its international membership of end-users, vendors, government agencies, universities, and research institutions to develop and revise standards as technologies change

throughout the years. OMG strongly believes to enable resilience and interoperability - consistent identifiers, models, architectures, frameworks, and associated data should utilize voluntary consensus-based open standards. Core to the success and widespread adoption of those items are making them free of consumer licensing terms that restrict public use, access, transparency, or otherwise prevent interoperability, data mapping, and communication.

**General Comments:** Overall, OMG supports the FR in starting the public discussion with its stakeholders about CBDCs in general, particularly the potential benefits and risks of a U.S. CBDC. Given the U.S. Dollar is the world’s reserve currency, the importance of reputation and integrity cannot be overstated in any discussion about the technical implementation of a Digital Dollar.

As most are aware, the technology quickly evolves, frequently outpacing International Standards Organization (ISO) standard consensus and finalization. OMG has more than 33 years of technology standards experience and stands ready to assist the FR with this critically important and prominent endeavor that must be resilient for at least decades, if not centuries. Should the FR desire to move to an ISO standard, OMG has a “Fast Track” Agreement with ISO which considerably expedites their average timelines of 9 plus years.

Based on OMG’s work with the U.S. Department of Defense (DoD), NASA, and the U.S. National Institute of Standards and Technology (NIST) (all OMG members), OMG would like to highlight the critical importance of governance in this project and with distributed systems. For instance, current cryptology technology is forecast to become much less secure once quantum computing becomes available in the future.

Further important questions yet to be addressed are:

1. How should this endeavor anticipate such a technological change?
2. How is this technology change processed into a governance model?
3. Similarly, should allowance(s) be made for a future consensus reversing the decision whether to pay interest on CBDC or the need that CBDC with certain identifiers should be restricted or even canceled?
4. Finally, the design decisions over the governance process are perhaps even more important than any technology standards one might adopt, inviting the question of how those decisions would be made and by whom?

Should you have any questions regarding the OMG response, you may call me at (703)231-6335 or email [MacLaird@omg.org](mailto:MacLaird@omg.org), [cbdc-feedback@omg.org](mailto:cbdc-feedback@omg.org) or [government-chair@omg.org](mailto:government-chair@omg.org).

Sincerely,

Steven A. MacLaird, Col (Ret), USAF
Senior Vice President, Gov't & Industry Strategy
Object Management Group

Atch - Responses to FR 22 Questions

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:00\\_cover:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:00_cover:start)



Last update: **2022/05/18 21:38**



# Object Management Group® (OMG®) Response to The US Federal Reserve's

*Money and Payments: The U.S. Dollar in the Age of Digital Transformation*

Version 1.0  
20th May 2022



R. W. "Nick" Stavros  
Ian T. Stavros  
Char Wales  
**Jackrabbit Consulting**  
Steven MacLaird  
Terrance Milligan



**Object Management Group (OMG)**

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:00\\_front:00\\_coverpage](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:00_front:00_coverpage)

Last update: **2022/05/19 12:24**

# Legal Responsibility

[return to Front Matter](#)

## 1 Disclaimer

[Return to Top](#)

All content, including, without limitation, any software, provided on the OMG website is provided “as is”. OMG makes no representations or warranties, express or implied including, but not limited to warranties of merchantability, fitness for a particular purpose, and non-infringement with respect to the content of this website, except to the extent that such disclaimers are held to be legally invalid. OMG makes no representations, warranties, guaranties, or conditions as to the quality, suitability, truth, accuracy, or completeness of any of the materials contained on the website.

## 2 Limitation of Liability

[Return to Top](#)

OMG shall not be liable to any party for any damages, including liability for special, indirect, consequential or incidental damages, or damages for lost profits, loss of revenue (including but not limited to loss of business, revenue, profits, use, data or another economic advantage) however it arises, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of content available from this website, even if OMG has been previously advised of the possibility of such damage.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:00\\_front:0.1\\_omgdisclaimer](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:00_front:0.1_omgdisclaimer)

Last update: **2022/05/19 12:24**



# Abstract

[return to Front Matter](#)

The members of the [Object Management Group \(OMG\)](#) have produced a single response to the Federal Reserves White Paper “[Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#)”. The White Paper was divided into two main sections: Discussion of a Central Bank Digital Currency (CBDC), and specific questions about the potential of a U.S. CBDC. The questions were further categorized into two main areas: CBDC Benefits, Risks, and Policy Considerations; and CBDC Design Considerations. The OMG response was written as a series of small sections using a WIKI and then printed as a PDF for submission back to the Federal Reserve. After the submission to the Federal Reserve, the contents of the WIKI are publicly available on the Internet. In order to relate the two sections, the OMG first [analyzed the Discussion portion of the White Paper for "Desirements"](#) (the white paper was not written as a requirements document, therefore the use of the term “Desirements”<sup>1)</sup>). Each of the “Desirements” was classified as being a [Benefit](#) , [Policy](#) , [Risk](#) , [Design Considerations](#), numbered, referenced to the original page number in the White Paper, and listed in appropriate tables as a quick reference. Finally, each of the 22 questions was answered using the “Desirements” as context back to the discussion portion of the White Paper. As the answers to the questions were formulated, some [Common Elements](#) were identified and made into independent subsections for reuse in the formulation of the answers to multiple questions.

1)

**Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired, but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:00\\_front:2\\_abstract](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:00_front:2_abstract)



Last update: **2022/05/19 12:24**

[return to Front Matter](#)

# Intellectual Property

## 1. Copyright

[Return to Top](#)

This site and its contents are Copyright Object Management Group, Inc., 9C Medway Road, PMB 274, Milford, MA 01757 USA. All rights reserved. Unless otherwise indicated, users may make a single copy of the contents, in whole or in part, of this website strictly for personal, non-commercial use. In the event that all or part of this site is downloaded for personal use, users shall maintain all proprietary notices, including copyright notices that appear on or in connection with that content. Other than creating a single copy of contents for personal use as described herein, users may not copy, reproduce, distribute, republish, download, display, post or transmit in any form or by any means, including but not limited to electronic, mechanical, photocopying, recording, or other means, any content found or linked to the OMG website without the prior express written permission of OMG. Any unauthorized use of any content contained on the OMG website may violate the copyright laws, trademark laws, laws relating to publicity and privacy, and other regulations and statutes in the U.S. and other countries.

OMG respects the intellectual property rights of others. If you believe that your copyrighted work appears on our website in a way that constitutes copyright infringement, please send a written notice containing the following information:

- The location or URL of where on our website the material you believe is infringing can be found;
- Description of what is being infringed;
- Your contact information;
- A statement, by you, of your good faith belief that the material is infringing, and its use is not authorized;
- A statement, by you, made under the penalty of perjury, that the information you provided is accurate and that you are the copyright owner or are authorized to act on the copyright owner's behalf.

Please send your notice to [copyright-manager@omg.org](mailto:copyright-manager@omg.org).

## 2. Copyright Permission

[Return to Top](#)

Copyright Permission

Occasionally, a member or partner wishes to include informational segments from OMG documents into presentations or product-specific technical literature. Requests to do so must be submitted to [trademarks@omg.org](mailto:trademarks@omg.org) in writing with an explanation of usage intent and must be approved in writing by

the OMG. You will be required to credit the appropriate OMG document in your materials and provide notice of copyright ownership.

OMG normally requires the use of entire chapters or segments from OMG specification and documentation. This is to ensure ease of identification and location of appropriate document numbers and between specification versions.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:00\\_front:3\\_copyright](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:00_front:3_copyright)



Last update: **2022/05/19 12:25**

# About Content Providers

[return to Front Matter](#) [Provide Feedback](#)

## About the Authors

[Return to Top](#)

Table 1: The authors of the Response to the Federal Reserve **White Paper**



Photo	Name	Company	Bio
	<b>R. W. "Nick" Stavros, BS, MS, Ph.D.</b>	<b>Jackrabbit Consulting</b>	Nick is the primary author of the OMG response to the Federal Reserve <b>White Paper</b> on a U.S.-based CBDC. Nick has over 50 years of experience in Software and Systems Engineering and has worked on a wide range of projects and products, from embedded processors and microcontrollers to large mainframe applications running DBMSs. Nick has been a volunteer with the OMG for 20 years and has served as a chairperson on the Ontology PSIG, and Blockchain PSIG. He has also been an active member of the Middleware and Related Services (MARS) Platform Task Force (PTF), Artificial Intelligence (AI) PTF, and the Data Distribution Service (DDS) PSIG. Nick is also VP of Technology at the DDS Foundation. Nick still enjoys coding in C/C++, Java, JavaScript, Solidity, PL/SQL, and PostgreSQL. He also likes to use modeling tools for ERD and SysML. He has also been the principal author of the Distributed Immutable Data Objects (DIDO) Reference Architecture (DIDO-RA).
	<b>Ian Stavros, BS, BS, MS</b>	<b>Jackrabbit Consulting</b>	Ian led a Phase 1 & 2 DARPA SBIR investigating blockchain technologies, leading to the publication of the Distributed Immutable Data Objects (DIDO) Reference Architecture (DIDO-RA) by the OMG and the development of the DIDO Test Environment (DIDO TE). Ian has been a member of the OMG since 2014 and is currently a co-chair of the Blockchain PSIG.


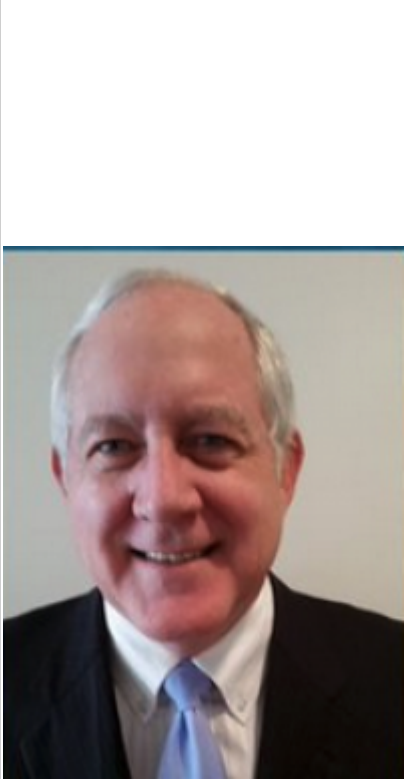

Photo	Name	Company	Bio
	<p><b>Char Wales, BS</b></p>	<p><b>Jackrabbit Consulting</b></p>	<p>Nominally retired as a systems engineer. Co-Chair of the Middleware and Related Services (MARS) Platform Task Force (PTF) in the Object Management Group (OMG), the standards body behind CORBA, UML, and other related technologies such as the Data Distribution Services (DDS) for Real-Time and Distributed Independent Data Objects (DIDO) including blockchain, distributed ledgers, etc. Have served in this role since 2003 although my participation in the OMG dates back to Dec 2000.</p>
	<p><b>Steven MacLaird</b></p>	<p><b>Object Management Group (OMG)</b></p>	<p>As Senior Vice President, Steve’s primary focus is to support the OMG government activities. The secondary focus is business development for the other OMG communities including the Augmented Reality for Enterprise Alliance (AREA), Industrial Internet Consortium® (IIC™) and the Consortium for Information &amp; Software Quality™ (CISQ™), Digital Twin Consortium® (DTC®), the Data Distribution Service (DDS®) Foundation®, and Responsible Computing™ (RC™) along with other duties. Steve retired from the United States Air Force after 27.5 years. Upon retirement, he consulted with several Fortune 200 companies as well as large, medium, and small companies; DoD and the Services; several 3 letter agencies and the Department of Energy. He was Vice-Chairman of the Board for PrismTech Solutions Americas; and a military advisor to the United Arab Emirates. His entire career spanned contracting, financial and program management working the Planning, Programming, Budgeting Submission (PPBS) financial process for air, land, sea, and space-based platforms along many areas of the Battle Management Command, Control, Communications Intelligence, Surveillance and Reconnaissance (BM-C4ISR) kill chain.</p>



Photo	Name	Company	Bio
	<p><b>Terrance Milligan, BA, BA, BS, JD, MBA</b></p>	<p><b>Object Management Group (OMG)</b></p>	<p>Marketing &amp; Analytics Manager (OMG): Served in the U.S. Army, experience in the legal field and as a Project Manager. Background in computer science (C++, CSS, HTML, Java, PHP, SQL) with an interest in blockchain and distributed ledger technology, digital currency and cryptocurrency legislation.</p>

## About the Contributors

[Return to Top](#)

Table 2: The Contributors helping formulate a Response to the Federal Reserve **White Paper**  
 The OMG Members that have contributed to the Response are:



Photo	Name	Company	Bio
	<p><b>Mike Bennett</b></p>	<p><b>hypercube</b></p>	<p>Mike Bennett is the director of Hypercube Limited, a company that helps people manage their information assets using formal semantics. Mike is the originator of the EDM Council’s Financial Industry Business Ontology (FIBO), a standards-based repository for financial industry concepts and definitions and works with the EDM Council as Director for Semantics and Standards. He has over 20 years of financial industry experience with investment management software, data management systems design, messaging standards, product testing and project management. Mike has worked on a number of financial industry standards, including the Market Data Definition Language (MDDL), the FIX message standard and others, has sat on ISO committees for the ISO 20022 messaging standard and the corresponding ISO model for securities terms and currently sits on an ISO committee for ISO 20022 and industry messaging semantics.</p>



Photo	Name	Company	Bio
	<b>Lars Toommre</b>	<b>BRC FinTech Corporation ("BRCF")</b>	Lars Toomre is BRC FinTech's lead geek and leads the BRC FinTech Corporation ("BRCF") and its subsidiary, Brass Rat Capital LLC ("BRC") team from Palm Beach County, Florida. Lars has had many pratfalls (and a "wee bit" of experience) as he has focused his professional career on uniquely adding value to financial firms and their business units. Lars organizes and helps teams to optimize Economic Value Added ("EVA") and serves as a thought leader and trusted advisor for issues that involve ontologies (think "semantic" meaning of data objects), valuations, analytics, risk, technology, and financial data.

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:00\\_front:6\\_authors](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:00_front:6_authors)



Last update: **2022/05/19 12:25**

# Preface

[return to Front Matter](#)

This document is a response by the Object Management Group (OMG) to a

White Paper

published by the U.S. Federal Reserve (The Fed) on [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation<sup>2\)</sup>](#).

## Goals

[Return to Top of Preface](#)

The OMG's goals in responding to the **White Paper** are:

- Provide the Federal Reserve direct response to the 22 questions posed in the **White Paper**
- Demonstrate how a systematic approach can be used to move the U.S. CBDC initiative to the next level of development
- Provide some general information applicable to some subset (or all) of the questions
- Provide traceability from the Desirements <sup>3)</sup> presented in the **White Paper** to answers given by OMG members to the 22 questions
- Demonstrate how the OMG [Distributed Immutable Data Object \(DIDO\) Reference Architecture \(DIDO-RA\)](#) can be used as a reference for the Federal Reserve distributed solutions such as [Stablecoin](#)
- Demonstrate to the Federal Reserve how the various Domain and Platform [Task Forces](#), [Special Interest Groups \(SIGs\)](#), and Working Groups, operating within the OMG can play a role creating standards applicable to the U.S. CBDC
- Provide a list of recommendations to the Federal Reserve on *"the next steps"*

## Audience

[Return to Top of Preface](#)

The primary audience for the OMG response to the [White Paper](#) is first and foremost the authors of the **White Paper**. This not only includes the authors responsible for providing background information about the Federal Reserve position on a U.S. CBDC, but it also includes the individuals who put forward the 22 questions. However, the hope is that anyone at the Federal Reserve interested in a CBDC would find the OMG Response to be good reference material.

The OMG members hope this content is freely shared by the Federal Reserve in the hopes that other respondents to the **White Paper** can use it as a reference and a place to start collaborating with other respondents and with the members of the Federal Reserve. Some of the content is specific to the Federal Reserve and to a U.S. CBDC; however, some of the content should be applicable to any other national

CBDC being developed.

## About this Document

[Return to Top of Preface](#)

This document is provided in two forms:

- A PDF that contains all the content and can be viewed and reviewed by anyone with access to a PDF reader or web browser
- A wiki that contains all the information in the PDF, but it is in a wiki format with multiple structured pages navigable via a web browser. In actuality, the wiki is used to generate the PDF.

The document structure in the PDF or the wiki is subdivided into three major subdivisions:

- [I. Front Matter](#)
- [II. Main Document](#)
- [III. The Appendices](#)

The Main Document is further subdivided into 6 major areas:

- [1.0 Introduction](#)
- [2.0 Methodology](#)
- [3.0 White Paper Analysis](#)
- [4.0 Common Elements](#)
- [5.0 Questions and Responses](#)
- [6.0 Recommendations](#)

The Appendices consist of:

- [Appendix A: Acronyms](#)
- [Appendix B: Glossary](#)
- [Appendix C: Other Transaction Authority \(OTA\)](#)
- [Appendix D: Model-Based Systems Engineering \(MBSE\)](#)

## How To Use the WIKI Document

[Return to Top of Preface](#)

The PDF document made from this WIKI is around 350 pages, therefore, it is not recommended to print it out. The PDF is a “long, linear, document”, which is possible to read, but by its nature, it was not intended to be read from the beginning to the end. It is comprised of a series of WIKI pages that are put together into a document, but each page can be read as a stand-alone document that is linked via

hyperlinks to the other sections of the document. The WIKI has only one purpose, to respond to the U.S. Federal Reserve (The Fed) published a

### White Paper

on [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#)<sup>4)</sup>, which provided a discussion and analysis of [Central Bank Digital Currency \(CBDC\)](#) and posted 22 questions for the community response. Since the response to each question should be stand-alone, the WIKI is recommended since each question has its own WIKI page or pages. These pages are linked back to the rest of the OMG responses for convenience and to restrict the about of duplicate material included in each response.

## WIKI Content Struction

Table 3: A summary of the Sections in the OMG Response

<b>1.0 Introduction</b>	A brief introduction to the problem space, The Federal Reserve and the <b>White Paper</b> and the Object Management Group.
<b>2.0 Methodology</b>	A brief overview of the methodology the OMG used to formulate a response to the <b>White Paper</b> .
<b>3.0 White Paper Analysis</b>	A breakdown of the <b>White Paper</b> discussion of a U.S. CBDC and the Desirements <sup>5)</sup> for that effort. Each Desirement is identified as to the page it was found on, its classification as a Benefit, Policy, Risks, Design, and a brief actionable statement.
<b>4.0 Common Elements</b>	During the review of the 22 questions posed in the <b>White Paper</b> it was decided that there were some common elements that needed to be separately addressed in order to not repeat the same information in the response to multiple questions.
<b>5.0 Questions and Responses</b>	The actual OMG response to the 22 direct questions posed in the <b>White Paper</b> . These are linked to other sections of the OMG response such as the <b>Common Elements</b> and also other questions. The OMG responded to all the questions, however, a few were felt to be beyond the scope of what the OMG members could respond to.
<b>6.0 Recommendations</b>	The OMG members wanted to make recommendations to the Federal Reserve for future activities in the area of a U.S. CBDC. They proposed 12 different direct actions or activities. One of these activities involves the use of RDT&E funding to explore eight specific topics.

## WIKI Navigation

A primary advantage of the WIKI is its rich set of navigation tools. Figure

# II. Main Document

[OMG Responses to Federal Reserve Discussion Paper](#) [Provide Feedback](#)

Table 1: A summary of the Sections in the OMG Response

<b>1.0 Introduction</b>	A brief introduction into the problem space, The Federal Reserve and the <b>White Paper</b> and the Object Management Group.
-------------------------	--

<b>2.0 Methodology</b>	A brief overview of the methodology the OMG used to formulate a response to the <b>White Paper</b> .
<b>3.0 White Paper Analysis</b>	A breakdown of the <b>White Paper</b> discussion of a U.S. CBDC and the Desirements <sup>1)</sup> for that effort. Each Desirement is identified as to the page it was found on, its classification as a Benefit, Policy, Risks, Design, and a brief actionable statement.
<b>4.0 Common Elements</b>	During the review of the 22 questions posed in the <b>White Paper</b> it was decided that there were some common elements that needed to be separately addressed in order to not repeat the same information in the response to multiple questions.
<b>5.0 Questions and Responses</b>	The actual OMG response to the 22 direct questions posed in the <b>White Paper</b> . These are linked to other sections of the OMG response such as the <b>Common Elements</b> and also other questions. The OMG responded to all the questions, however, a few were felt to be beyond the scope of what the OMG members could respond to.
<b>6.0 Recommendations</b>	The OMG members wanted to make recommendations to the Federal Reserve for future activities in the area of a U.S. CBDC. They propose 12 different direct actions or activities. One of these activities involves the use of RDT&E funding to explore eight specific Research Development Test & Evaluation (RDT&E) topics.

1)

**Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired, but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:start)

Last update: **2022/05/18 13:50**

# 1.0 Introduction

## [OMG Responses to Federal Reserve Discussion Paper](#)

A brief introduction to the problem space, The Federal Reserve and the **White Paper** and the Object Management Group.

## About the Federal Reserve White Paper

[Return to the Main Document](#) [Provide Feedback](#)

### Overview

[Return to the Top](#)

The U.S. Federal Reserve (The Fed) published a

White Paper

on [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#)<sup>6)</sup>, which provided a discussion and analysis of [Central Bank Digital Currency \(CBDC\)](#).

### Executive Summary

[Return to About the Federal Reserve White Paper](#)

*For a nation's economy to function effectively, its citizens must have confidence in its money and payment services. The Federal Reserve, as the nation's central bank, works to maintain the public's confidence by fostering monetary stability, financial stability, and a safe and efficient payment system.<sup>7)</sup>*

*This paper is the first step in a public discussion between the Federal Reserve and stakeholders about central bank digital currencies (CBDCs). For the purpose of this paper, a CBDC is defined as a digital liability of a central bank that is widely available to the general public. In this respect, it is analogous to a digital form of paper money. The paper has been designed to foster a broad and transparent public dialogue about CBDCs in general, and about the potential benefits and risks of a U.S. CBDC. The paper is not intended to advance any specific policy outcome, nor is it intended to signal that the Federal Reserve will make any imminent decisions about the appropriateness of issuing a U.S. CBDC.<sup>8)</sup>*

### Background

[Return to About the Federal Reserve White Paper](#)

*Payment technologies offered by the Federal Reserve have evolved over time. In the Federal Reserve's early years, it established a national check-clearing system and used dedicated telegraph wires to transfer funds between banks. In the 1970s, the Federal Reserve developed an automated clearinghouse (ACH) system that offered an electronic alternative to paper checks. And in 2019, the Federal Reserve committed to building the FedNow<sup>SM</sup> Service, which will provide real-time, around-the-clock interbank payments, every day of the year.<sup>9)</sup>*

*Recent technological advances have ushered in a wave of new private-sector financial products and services, including digital wallets, mobile payment apps, and new digital assets such as cryptocurrencies and Stablecoins. These technological advances have also led central banks around the globe to explore the potential benefits and risks of issuing a CBDC. Federal Reserve policymakers and staff have studied CBDC closely for several years, guided by an understanding that any U.S. CBDC should, among other things<sup>10)</sup>*

- *provide benefits to households, businesses, and the overall economy that exceed any costs and risks;*
- *yield such benefits more effectively than alternative methods;*
- *complement, rather than replace, current forms of money and methods for providing financial services;*
- *protect consumer privacy;*
- *protect against criminal activity; and*
- *have broad support from key stakeholders.*

*The Federal Reserve is committed to soliciting and reviewing a wide range of views as it continues to study whether a U.S. CBDC would be appropriate. Irrespective of any ultimate conclusion, Federal Reserve staff will continue to play an active role in developing international standards for CBDCs.<sup>11)</sup>*

## **Key Topics**

### [Return to About the Federal Reserve White Paper](#)

*This paper begins with a discussion of existing forms of money; the current state of the U.S. payment system and its relative strengths and challenges; and the various digital assets that have emerged in recent years, including Stablecoins and other cryptocurrencies. The paper then turns to CBDC, focusing on its uses and functions; potential benefits and risks; and related policy considerations.<sup>12)</sup>*

*The Federal Reserve's initial analysis suggests that a potential U.S. CBDC, if one were created, would best serve the needs of the United States by being privacy-protected, intermediated, widely transferable, and identity-verified. As noted above, however, the paper is not intended to advance a specific policy outcome and takes no position on the ultimate desirability of a U.S. CBDC.<sup>13)</sup>*

## Public Outreach

[Return to About the Federal Reserve White Paper](#)

*The Federal Reserve will seek input from a wide range of stakeholders that might use a CBDC or be affected by its introduction. **This paper concludes with a request for public comment, the first step in a broad consultation that will also include targeted outreach and public forums.***<sup>14)</sup>

## About the Object Management Group (OMG)

[Return to the Top](#)

### Overview

[Return to About the Object Management Group \(OMG\)](#)

The **Object Management Group® (OMG®)**, founded in 1989, is an international not-for-profit software consortium (aka [Standards Developing Organization \(SDO\)](#) or a [Voluntary Standards Consensus Body \(VSCB\)](#)) that sets standards in the many areas including distributed object computing. The OMG manages an open, vendor-neutral process that proposes technologies, and invites proposals, and feedback from any member company before coming to a consensus on a final adopted specification standard. Some standards the OMG has developed for specific domains such as [CORBA®](#), [SysML®](#), [UML®](#), and [IIOP®](#). OMG has a fast-track approval agreement with the [International Standards Organization \(ISO\)](#) and all OMG standards are written in ISO format.

In addition to the work OMG has done on industry-wide standards, OMG is very active in 26 vertical markets, including Business, Finance, Government, Healthcare, Manufacturing, Military, Robotics, Space, and Telecoms.

The following OMG standards have been identified as relevant to Distributed Systems by the DARPA funded [Distributed Immutable Data Object - Reference Architecture \(DIDO-RA\)](#):

- [OMG: Automated Source Code CISQ Maintainability Measure \(ASCMM\)](#)
- [OMG: Automated Source Code CISQ Measures \(ASCQM\)](#)
- [OMG: Automated Source Code CISQ Performance Efficiency Measure \(ASCPem\)](#)
- [OMG: Automated Source Code CISQ Reliability Measure \(ASCRM\)](#)
- [OMG: Automated Source Code CISQ Security Measure \(ASCSM\)](#)
- [OMG: Business Motivation Model \(BMM\)](#)
- [OMG: Business Process Model And Notation \(BPMN\)](#)
- [OMG: Case Management Model and Notation \(CMMN\)](#)
- [OMG: CISQ Automated Enhancement Points \(AEP\)](#)
- [OMG: CISQ Automated Function Points \(AFP\)](#)
- [OMG: CISQ Automated Technical Debt Measure \(ATDM\)](#)



- [OMG: Common Warehouse Metamodel \(CWM\)](#)
- [OMG: Data Distribution Service \(DDS\)](#)
- [OMG: DDS Consolidated XML Syntax \(DDS-XML\)](#)
- [OMG: DDS For Extremely Resource-Constrained Environments \(DDS-XRCE\)](#)
- [OMG: DDS Interoperability Wire Protocol \(DDSI-RTPS\)](#)
- [OMG: DDS Security \(DDS-SECURITY\)](#)
- [OMG: Distributed Ontology, Model, and Specification Language \(DOL\)](#)
- [OMG: Extensible and Dynamic Topic Types for DDS \(DDS-XTypes\)](#)
- [OMG: Financial Industry Business Ontology \(FIBO\)](#)
- [OMG: Financial Instrument Global Identifier \(FIGI\)](#)
- [OMG: Information Exchange Framework \(IEF\)](#)
- [OMG: Interface Definition Language \(IDL\)](#)
- [OMG: ISO/IEC C++ 2003 Language DDS PSM \(DDS-PSM-Cxx\)](#)
- [OMG: Java 5 Language PSM for DDS \(DDS-Java\)](#)
- [OMG: Meta Object Facility \(MOF\)](#)
- [OMG: Ontology Definition Metamodel \(ODM\)](#)
- [OMG: OPC-UA/DDS Gateway \(DDS-OPCUA\)](#)
- [OMG: RPC Over DDS \(DDS-RPC\)](#)
- [OMG: Semantics Of Business Vocabulary and Rules \(SBVR\)](#)
- [OMG: Structured Assurance Case Metamodel \(SACM\)](#)
- [OMG: Structured Metrics Metamodel \(SMM\)](#)
- [OMG: Systems Modeling Language \(SysML\)](#)
- [OMG: Test Information Interchange Format \(TestIF\)](#)
- [OMG: Unified Architecture Framework \(UAF\)](#)
- [OMG: Unified Modeling LanguageTitle \(UML\)](#)
- [OMG: Web-Enabled DDS \(DDS-WEB\)](#)
- [OMG: XML Metadata Interchange \(XMI\)](#)

## Public Response to Outreach Request

[Return to About the Object Management Group \(OMG\)](#)

The OMG has reached out to its members to solicit an overall OMG response to the White Paper. Two groups within the OMG are providing extensive information in response to The Fed's request for [Public Outreach](#).

Table 5 provides a list of OMG groups that would have interest in the U.S. Based CBDC.

Table 5: OMG Groups having interests in U.S. CBDC.

<p><b>Blockchain Platform Special Interest Group (PSIG)</b></p>	<p>The Blockchain PSIG is to work with OMG domain and platform task forces, other relevant OMG SIGs, external entities, and related industry groups to facilitate the submission and adoption of Distributed Ledger Technology (Blockchain) and related standards.</p> <p><b>Mission:</b> In order to accomplish this mission, the Blockchain PSIG will:</p> <ol style="list-style-type: none"> <li>1. Search out and assist specifications for submission to the OMG in the Distributed Ledger Technology space.</li> <li>2. Foster cooperation between implementers and users of Distributed Ledger technologies</li> <li>3. Clarify user requirements and coordinate the evolution of Distributed Ledger Technology specifications, influence related specifications, and catalyze new specifications.</li> <li>4. Identify opportunities to leverage and integrate Distributed Ledger Technology with other computing standards (including other distributed computing standards) and help develop necessary collaboration/interoperation specifications.</li> <li>5. Educate, guide, and assist the community in the use of Distributed Ledger technologies.</li> <li>6. Promote and evangelize the use of Distributed Ledger technology OMG standards in the marketplace and seek additional opportunities for the technology.</li> <li>7. Contribute to other OMG Task Forces with Blockchain and Distributed Ledger Technology insights and perspectives on their work.</li> <li>8. Establish and maintain active liaison relationships with appropriate external organizations in support of the goals of this PSIG.</li> </ol>
<p><b>Government Domain Task Force (DTF)</b></p>	<p>The Government Domain Task Force was chartered in the OMG's Domain Technology Committee Plenary, on 17 February 2006 during the Technical Committee meetings in Tampa FL.</p> <p><b>Mission:</b></p> <ol style="list-style-type: none"> <li>1. To serve as a Community of Interest in the application of Model Driven Architecture and other OMG specifications to governmental organizations in civilian, defense, and intelligence sectors.</li> <li>2. Recommend technology specifications based on OMG's Model Driven Architecture (MDA) that enable interoperability, reusability, and modularity in government systems.</li> <li>3. To provide advice, consultation, and support to the OMG in the development of specifications applicable to government systems in particular.</li> <li>4. To form and coordinate government-specific working groups within the Task Force tailored to address the particular needs of specific governmental sectors at the international, national, regional, or local levels.</li> <li>5. Liaise with external Standards and Governmental Organizations</li> </ol>

<b>Retail Domain Task Force (DTF)</b>	<p>The Retail Domain Task Force (RDTF) is a community dedicated to helping retailers and solution providers identify, adopt and integrate current and emerging information technology. The RDTF was originally founded in 1991 as a share group for retail CIOs and then incorporated in 1993 as the Association for Retail Technology Standards (ARTS). ARTS was subsequently acquired by the National Retail Federation (NRF) in 1998; the Object Management Group® (OMG®) and NRF entered into a long-term agreement to manage and develop the retail standards in 2017.</p> <p><b>Mission</b></p> <p>To increase the benefits and reduce the costs, risks, and timescales of using Information Technology within the retail sector by:</p> <ol style="list-style-type: none"><li>1. Developing and promoting standardized retail business models and practices that foster a shared understanding of retail business principles, terminology, and data between retailers and their suppliers.</li><li>2. Establishing technical standards, specifications, and best practices that enable communication of business data within retail enterprises, and between retail enterprises and their suppliers.</li><li>3. Creating standards for the integration of IT applications and devices into retail business systems.</li><li>4. Communicating the requirements of the retail industry to IT suppliers &amp; users, both inside and outside OMG.</li></ol>
---------------------------------------	---

## Summary

### [Return to the Top](#)

The members of the [Object Management Group \(OMG\)](#) have produced a single response to the Federal Reserves White Paper “ [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#)”<sup>15)</sup>. The White Paper was divided into two main sections: Discussion of a Central Bank Digital Currency (CBDC), and specific questions about the potential of a U.S. CBDC. The questions were further categorized into two main areas: CBDC Benefits, Risks, and Policy Considerations; and CBDC Design Considerations. The OMG response was written as a series of small sections using a WIKI and then printed as a PDF for submission back to the Federal Reserve. After the submission to the Federal Reserve, the contents of the WIKI are publicly available on the Internet. In order to relate the two sections, the OMG first [analyzed the Discussion portion of the White Paper for "Desirements"](#) (the white paper was not written as a requirements document, therefore the use of the term “Desirements”<sup>16)</sup>). Each of the “Desirements” was classified as being a:

- [Benefit Considerations](#),
- [Policy Considerations](#),
- [Risk Considerations](#),
- [Design Considerations](#)

Each Desirement was numbered, referenced to the original page number in the White Paper, and listed in appropriate tables as a quick reference. Finally, each of the 22 questions was answered using the “Desirements” as context back to the discussion portion of the White Paper. As the answers to the questions were formulated, some [Common Elements](#) were identified and made into independent subsections for reuse in the formulation of the answers to multiple questions.

6) 7) 8) 9) 10) 11) 12) 13) 14) 15)

Board of Governors, The Federal Reserve System, January 2022, Accessed: 5 May 2022,  
<https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>  
16)

**Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired, but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:04\\_intro:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:04_intro:start)



Last update: **2022/05/18 21:56**

# 2.0 Methodology

## OMG Responses to Federal Reserve Discussion Paper

[Return to the Main Document](#) [Provide Feedback](#)

A brief overview of the methodology the OMG used to formulate a response to the **White Paper**.

The U.S. [Federal Reserve \(Fed\)](#) published a white paper on [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation<sup>6\)</sup>](#), which provided a discussion and analysis of [Central Bank Digital Currency \(CBDC\)](#), some possible designs to address CBDC, and some direct questions they posed to stakeholders about the possibility of adoption of CBDC by the U.S. Federal Reserve.

The [Object Management Group](#) is responding to the questions posed by the White Paper. The OMG response is based on a Systems Engineering approach, see [Figure 2](#). The following briefly describes each step in the process:

The [White Paper](#) was reviewed and its content was divided into two main sections:

1. A general discussion of what the Federal Reserve believes the CBDC needs to do is restated in terms of a matrix of Federal Reserve “Desirements” (i.e., [White Paper Analysis](#)). These “Desirements”<sup>7)</sup> are classified according to the four main objectives stated in the White Paper:

- [Benefit Considerations](#)
- [Policy Considerations](#)
- [Risk Considerations](#)
- [Design Considerations](#)

2. A set of questions for potential stakeholders to answer. Upon review of the answers to the questions,

a. Some content was extracted and made into a set of [Common Elements](#) that have applicability to multiple answers to multiple questions. For example:

- [Stakeholders](#)
- [Currency Models](#)
- [Stablecoins](#)
- [National Privacy Considerations](#)
- [National Security Considerations](#)
- [International Considerations](#)
- [Dual Payment Networks](#)

b. Each question's answer tried to have the same outline when formulating answers:

- Overview
- Examples
- Discussion of Examples

The results were then collated into a single OMG response that includes a set of overall recommendations

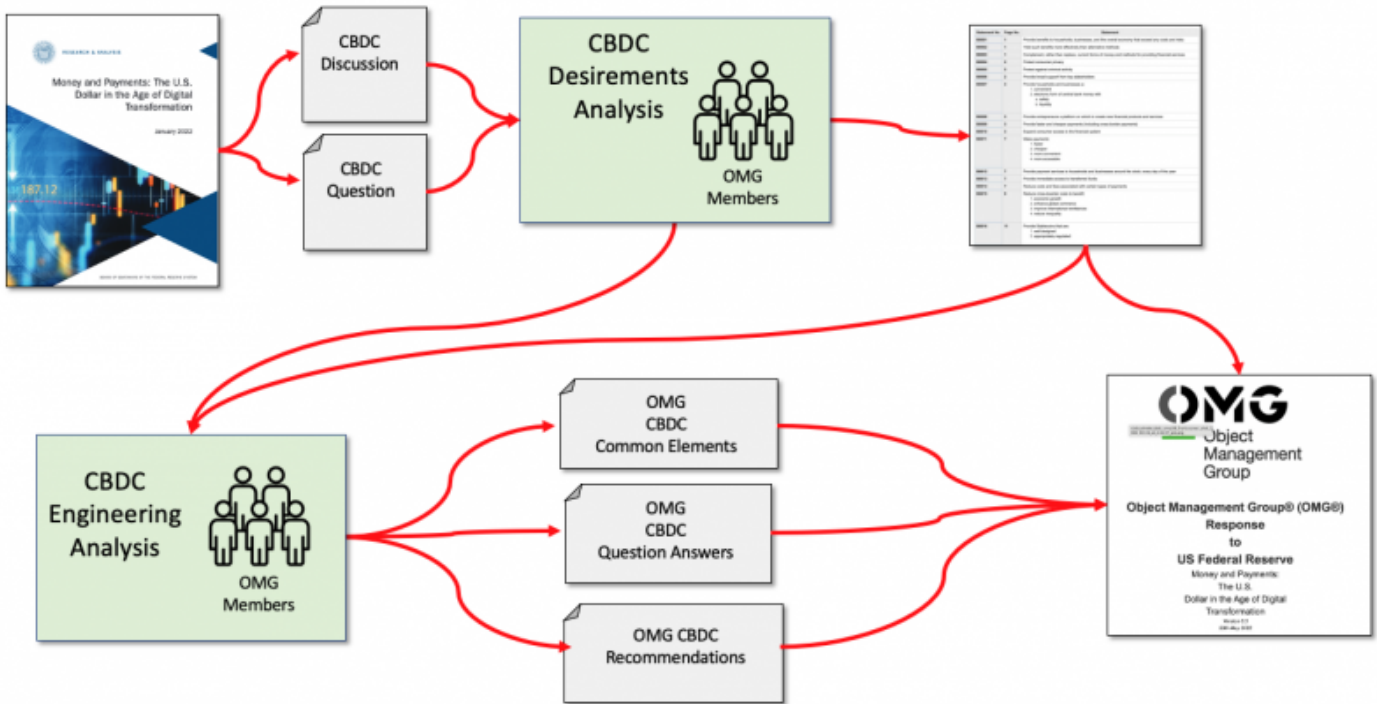


Figure 2: Overview of the OMG Methodology used to answer the Federal Reserve Questions.

6)

Board of Governors, The Federal Reserve System, January 2022, Accessed: 5 May 2022, <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

7)

**Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired, but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:08\\_method:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:08_method:start)

Last update: **2022/05/17 19:12**



# 3.0 White Paper Analysis

[OMG Responses to Federal Reserve Discussion Paper](#)

[Return to the Main Document](#) [Provide Feedback](#)

A breakdown of the **White Paper** discussion of a U.S. CBDC and the Desirements<sup>17)</sup> for that effort. Each Desirement is identified with the page number it is found on, its classification as a Benefit, Policy, Risks, Design, and a brief actionable statement.

## Executive Summary

[Return to Top](#)

The following is the **Executive Summary** provided in the [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#)<sup>18)</sup> **White Paper**:

*For a nation's economy to function effectively, its citizens must have confidence in its money and payment services. The Federal Reserve, as the nation's central bank, works to maintain the public's confidence by fostering monetary stability, financial stability, and a safe and efficient payment system.*

*This paper is the first step in a public discussion between the Federal Reserve and stakeholders about [Central Bank Digital Currencies \(CBDCs\)](#). For this paper, a CBDC is defined as a digital liability of a central bank that is widely available to the general public. In this respect, it is analogous to a digital form of paper money. The paper has been designed to foster a broad and transparent public dialogue about CBDCs in general and about the potential benefits and risks of a U.S. CBDC. The paper is not intended to advance any specific policy outcome, nor is it intended to signal that the Federal Reserve will make any imminent decisions about the appropriateness of issuing a U.S. CBDC.*

## Preparation for Responses to the Request for Comments

[Return to Top](#)

In order to provide answers to the 22 questions requested by the Federal Reserve in the [White Paper](#), it is important to summarize the rest of the content of the **White Paper** to help provide context for the questions in the White Paper and OMG's answers to these questions. The questions fall into two major categories:

- CBDC Benefits, Risks, and Policy Considerations
- CBDC Design

In order for the [Object Management Group \(OMG\)](#) to prepare responses to the questions in the **White Paper**, the OMG has taken a traditional Systems Engineering approach to understanding the problem by dissecting it into smaller, more manageable pieces based on the stated objectives outlined in the **White Paper**. We noted four major objectives:

- [Benefit Considerations](#)
- [Policy Considerations](#)
- [Risk Considerations](#)
- [Design Considerations](#)

## Methodology

[Return to Top](#)

The **White Paper** was read linearly (i.e., from top to bottom) with each statement classified as describing or providing: Background, Benefits, Policy Considerations, Risks, or Design. The sentences were copied into the appropriate table (e.g., Table 6, Benefits) in this White Paper Overview. Statements in the **White Paper** that provided Background were not transcribed into any table. This does not mean these Background statements were unimportant; they were used to provide definitions and context for the Benefits, Policy Considerations, Risks, or Design statements captured in the tables below.

**Note:** Some of the statements have been edited to allow them to be standalone and written in the form of an “action”. For future iterations, these statements need to be written as requirements. See: [Specifying Requirements](#) in the [Distributed Immutable Data Object - References Architecture \(DIDO-RA\)](#).

## Benefit Considerations

[Return to Top](#)

The following are the [U.S. CBDC Benefits](#) identified in the [White Paper](#):

Table 6: The Benefits identified in the **White Paper**

Desirement No.	Page No.	Desirement <sup>19)</sup>
<b>B0001</b>	<b>1</b>	Provide benefits to households, businesses, and the overall economy that exceed any costs and risks
<b>B0002</b>	<b>1</b>	Yield such benefits more effectively than alternative methods
<b>B0003</b>	<b>1</b>	Complement, rather than replace, current forms of money and methods for providing financial services
<b>B0004</b>	<b>2</b>	Protect consumer privacy
<b>B0005</b>	<b>2</b>	Protect against criminal activity
<b>B0006</b>	<b>2</b>	Provide broad support from key stakeholders



<b>Desirement No.</b>	<b>Page No.</b>	<b>Desirement<sup>19)</sup></b>
<b>B0007</b>	<b>3</b>	Provide households and businesses a convenient and electronic form of central bank money with: 1. safety 2. liquidity
<b>B0008</b>	<b>3</b>	Provide entrepreneurs a platform on which to create new financial products and services
<b>B0009</b>	<b>3</b>	Provide faster and cheaper payments (including cross-border payments)
<b>B0010</b>	<b>3</b>	Expand consumer access to the financial system
<b>B0011</b>	<b>7</b>	Make payments: 1. faster 2. cheaper 3. more convenient 4. more accessible
<b>B0012</b>	<b>7</b>	Provide payment services to households and businesses around the clock, every day of the year
<b>B0013</b>	<b>7</b>	Provide immediate access to transferred funds
<b>B0014</b>	<b>7</b>	Reduce costs and fees associated with certain types of payments
<b>B0015</b>	<b>9</b>	Reduce cross-border costs to benefit: 1. economic growth 2. enhance global commerce 3. improve international remittances 4. reduce inequality
<b>B0016</b>	<b>11</b>	Provide Stablecoins that are: 1. well-designed 2. appropriately regulated
<b>B0017</b>	<b>9</b>	Provide Stablecoins that are: 1. faster 2. more efficient 3. more inclusive payment
<b>B0018</b>	<b>13</b>	Allow the general public to make digital payments
<b>B0019</b>	<b>13</b>	Provide the safest digital asset available to the general public, with no: 1. associated credit 2. liquidity risk
<b>B0020</b>	<b>13</b>	Maintain public confidence by not requiring mechanisms, such as deposit insurance
<b>B0021</b>	<b>13</b>	Maintain value by not using backing by an underlying asset
<b>B0022</b>	<b>13</b>	Provide a CBDC that is: 1. <a href="#">Privacy-Protected</a> 2. <a href="#">Intermediated</a> 3. <a href="#">Widely Transferable</a> 4. <a href="#">Identity-Verified</a>
<b>B0023</b>	<b>14</b>	Create a liability to the Federal Reserve
<b>B0024</b>	<b>14</b>	Provide transactions finalized and completed in real time
<b>B0025</b>	<b>14</b>	Serve as a new foundation for the payment system
<b>B0026</b>	<b>14</b>	Provide a bridge between legacy and new payment services
<b>B0027</b>	<b>14</b>	Maintain the centrality of safe and trusted central bank money

<b>Desirement No.</b>	<b>Page No.</b>	<b>Desirement<sup>19)</sup></b>
<b>B0028</b>	<b>14</b>	Offer the general public broad access to digital money: <ol style="list-style-type: none"> <li>1. free from credit risk</li> <li>2. liquidity risk</li> </ol>
<b>B0029</b>	<b>14</b>	Support basic purchases of: <ol style="list-style-type: none"> <li>1. goods</li> <li>2. services</li> <li>3. pay bills</li> <li>4. pay taxes</li> </ol>
<b>B0030</b>	<b>14</b>	Support benefit payments directly to citizens
<b>B0031</b>	<b>14</b>	Provide the general public broad access to digital money that is free from: <ol style="list-style-type: none"> <li>1. credit risk</li> <li>2. liquidity risk</li> </ol>
<b>B0032</b>	<b>14</b>	Provide a programmable CBDC
<b>B0033</b>	<b>15</b>	Support a level playing field in payment innovation for private-sector firms of all sizes
<b>B0034</b>	<b>15</b>	Generate new capabilities to meet the speed and efficiency requirements of the digital economy
<b>B0035</b>	<b>15</b>	Streamline cross-border payments by using: <ol style="list-style-type: none"> <li>1. new technologies</li> <li>2. introducing simplified distribution channels</li> <li>3. creating additional opportunities for cross-jurisdictional collaboration and interoperability</li> </ol>
<b>B0036</b>	<b>15</b>	Preserve the dominant international role of the U.S. dollar
<b>B0037</b>	<b>15</b>	Support private-sector innovation
<b>B0038</b>	<b>15</b>	Allow private-sector innovators to focus on: <ol style="list-style-type: none"> <li>1. new access services</li> <li>2. distribution methods</li> <li>3. related service offerings</li> </ol>
<b>B0039</b>	<b>15</b>	Provide a programmable CBDC to deliver payments at certain times
<b>B0040</b>	<b>15</b>	Provide micropayment support
<b>B0041</b>	<b>15</b>	Support streamlining cross-border payments
<b>B0042</b>	<b>15</b>	Preserve the dominant international role of the U.S. dollar
<b>B0043</b>	<b>16</b>	Promoting financial inclusion—particularly for economically vulnerable households and communities
<b>B0044</b>	<b>16</b>	Facilitate access to digital payments
<b>B0045</b>	<b>16</b>	Enable rapid and cost-effective payment of taxes
<b>B0046</b>	<b>16</b>	Enable rapid and cost-effective delivery of: <ol style="list-style-type: none"> <li>1. wages</li> <li>2. tax refunds</li> <li>3. other federal payments</li> </ol>
<b>B0047</b>	<b>16</b>	Lower transaction costs
<b>B0048</b>	<b>16</b>	Provide a secure way for people to save
<b>B0049</b>	<b>16</b>	Promote access to credit
<b>B0050</b>	<b>16</b>	Extend Public Access to Safe Central Bank Money

<b>Desirement No.</b>	<b>Page No.</b>	<b>Desirement<sup>19)</sup></b>
<b>B0051</b>	<b>19</b>	Generate data about users' financial transactions similar to the current Commercial Bank <sup>20)</sup> and <a href="#">Nonbank Money</a>
<b>B0052</b>	<b>19</b>	Prevent Financial money laundering crimes
<b>B0053</b>	<b>20</b>	Provide resiliency to threats to existing payment services—including: 1. operational disruptions 2. cybersecurity risks
<b>B0054</b>	<b>19</b>	Attract risk-averse users to CBDC

## Policy Considerations

[Return to Top](#)

The following are the [U.S. CBDC Policy Considerations](#) identified in the [White Paper](#):

Table 7: The Policy Considerations identified in the **White Paper**

<b>Desirement No.</b>	<b>Page No.</b>	<b>Desirement</b>
<b>P0001</b>	<b>1</b>	Provide benefits to households, businesses, and the overall economy that exceed any 1. costs 2. risks
<b>P0002</b>	<b>1</b>	Provide Yield benefits more effectively than alternative methods
<b>P0003</b>	<b>1</b>	Complement current forms of money and methods for providing financial services
<b>P0004</b>	<b>2</b>	Protect consumer privacy
<b>P0005</b>	<b>2</b>	Protect against criminal activity
<b>P0006</b>	<b>2</b>	Garner broad support from key stakeholders
<b>P0007</b>	<b>2</b>	Be policy outcome neutral (i.e., not advancing a specific policy outcome)
<b>P0008</b>	<b>2</b>	Have a neutral position on the ultimate desirability of a U.S. CBDC
<b>P0009</b>	<b>3</b>	CBDC would be a liability of the Federal Reserve, not of a commercial bank
<b>P0010</b>	<b>3</b>	CBDC would be a liability not of a commercial bank <sup>21)</sup>
<b>P0011</b>	<b>3</b>	The Federal Reserve does not intend to proceed with the issuance of a CBDC without clear support from: 1. The Executive Branch 2. The Legislative Branch 3. ideally in the form of a specific authorizing law
<b>P0012</b>	<b>7</b>	The firms that operate interbank payment services are subject to federal supervision
<b>P0013</b>	<b>7</b>	Systemically important payment firms are subject to 1. heightened supervision 2. regulation
<b>P0014</b>	<b>12</b>	The PWG report highlights gaps in the authority of regulators to reduce these risks
<b>P0015</b>	<b>12</b>	The PWG report recommends that Congress act promptly to enact legislation that would ensure payment Stablecoins

<b>Desirement No.</b>	<b>Page No.</b>	<b>Desirement</b>
<b>P0016</b>	<b>12</b>	The PWG report recommends payment Stablecoin arrangements are subject to a consistent and comprehensive federal regulatory framework
<b>P0017</b>	<b>12</b>	The PWG report recommends CBDC complement existing authorities Regarding: 1. market integrity 2. investor protection 3. illicit finance
<b>P0018</b>	<b>13</b>	The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals
<b>P0019</b>	<b>13</b>	Federal Reserve accounts for individuals represent a significant expansion of the Federal Reserve's role in the financial system and the economy
<b>P0020</b>	<b>13</b>	The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments
<b>P0021</b>	<b>13</b>	The intermediaries would operate in an open market for CBDC services
<b>P0022</b>	<b>14</b>	CBDC itself would be a liability of the Federal Reserve
<b>P0023</b>	<b>14</b>	CBDC would need to be readily transferable between customers of different intermediaries
<b>P0024</b>	<b>14</b>	CBDC would need to comply with the U.S. robust rules
<b>P0025</b>	<b>14</b>	CBDC intermediary would need to verify the identity of a person accessing CBDC
<b>P0026</b>	<b>14</b>	CBDC transactions would need to be final and completed in real-time
<b>P0027</b>	<b>14</b>	CBDC a risk-free asset
<b>P0028</b>	<b>15</b>	Require significant international coordination to address issues such as: 1. common standards 2. infrastructure, 3. the types of intermediaries able to access any new infrastructure, 4. legal frameworks 5. preventing illicit transactions 6. the cost and timing of implementation
<b>P0029</b>	<b>16</b>	The Federal Reserve is committed to ensuring the continued safety and availability of cash
<b>P0030</b>	<b>21</b>	The Federal Reserve will only take further steps toward developing a CBDC if: 1. Research points to benefits for households, businesses, and the economy overall that exceed the downside risks 2. Indicates that CBDC is superior to alternative methods
<b>P0031</b>	<b>21</b>	The Federal Reserve would only pursue a CBDC in the context of broad public and cross-governmental support

## Risk Considerations

[Return to Top](#)

The following are the [U.S. CBDC Risks](#) identified in the [White Paper](#):

Table 8: The Risks identified in the **White Paper**

<b>Desirement No.</b>	<b>Page No.</b>	<b>Desirement</b>
<b>R0001</b>	<b>3</b>	<b>Risk</b> of affecting financial-sector market structure
<b>R0002</b>	<b>3</b>	<b>Risk</b> to the cost and availability of credit
<b>R0003</b>	<b>3</b>	<b>Risk</b> to the safety and stability of the financial system
<b>R0004</b>	<b>3</b>	<b>Risk</b> to the efficacy of monetary policy
<b>R0005</b>	<b>7</b>	New payment services could pose <b>Risks</b> to: 1. financial stability 2. payment system integrity 3. other <b>Risks</b>
<b>R0006</b>	<b>8</b>	<b>Risk</b> of extreme price volatility
<b>R0007</b>	<b>8</b>	<b>Risk</b> CBDC is difficult to use without service providers
<b>R0008</b>	<b>8</b>	<b>Risk</b> of severe limitations on transaction throughput
<b>R0009</b>	<b>8</b>	Increased <b>Risk</b> of “runs” or other instabilities to the financial system
<b>R0010</b>	<b>11</b>	CBDC has <b>Risk</b> of significant energy footprint similar to Cryptocurrencies
<b>R0011</b>	<b>11</b>	Increased <b>Risk</b> to consumer's vulnerability to: 1. loss 2. theft 3. fraud
<b>R0012</b>	<b>12</b>	<b>Risk</b> of increased concern related to the potential for: 1. destabilizing “runs” 2. disruptions in the payment system 3. concentration of economic power
<b>R0013</b>	<b>13</b>	CBDC offers no associated credit or liquidity <b>Risk</b>
<b>R0014</b>	<b>13</b>	<b>Risk</b> of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity
<b>R0015</b>	<b>14</b>	Require mechanisms to reduce liquidity <b>Risk</b>
<b>R0016</b>	<b>14</b>	Require mechanisms to reduce credit <b>Risk</b>
<b>R0017</b>	<b>15</b>	Using private digital money could present <b>Risks</b> to both individual users and the financial system as a whole
<b>R0018</b>	<b>17</b>	<b>Risk</b> a CBDC could fundamentally change the structure of the U.S. financial system, altering the private sector and central bank: 1. roles 2. responsibilities
<b>R0019</b>	<b>17</b>	<b>Risk</b> of reducing the aggregate amount of deposits in the banking system, which could in turn increase bank funding expenses, and reduce credit availability or raise credit costs for households and businesses.
<b>R0020</b>	<b>17</b>	<b>Risk</b> that interest-bearing CBDC could result in a shift away from other low-risk assets, such as shares in money market mutual funds, Treasury bills, and other short-term instruments.
<b>R0021</b>	<b>17</b>	<b>Risk</b> of reducing credit availability or raising credit costs for businesses and governments
<b>R0022</b>	<b>17</b>	<b>Risk</b> of Stablecoins and other types of nonbank money shifting deposits away from banks even without a CBDC

Desirement No.	Page No.	Desirement
<b>R0023</b>	<b>17</b>	<b>Risk</b> of financial panic causing outflows from Commercial Banks to CBDC without prudential supervision, government deposit insurance, and access to central bank liquidity

## Design Considerations

[Return to Top](#)

Table 9: The Designs identified in the **White Paper**

Desirement No.	Page No.	Desirement
<b>D0001</b>	<b>17</b>	<b>Design</b> should be for a non-interest-bearing CBDC, for example, would be less attractive as a substitute for commercial bank money
<b>D0002</b>	<b>17</b>	<b>Design</b> should allow the central bank to limit the amount of CBDC an end-user could hold
<b>D0003</b>	<b>18</b>	<b>Design</b> should allow a limit on the amount of CBDC an end-user could accumulate over short periods
<b>D0004</b>	<b>18</b>	<b>Design</b> should influence how the Federal Reserve might affect monetary policy
<b>D0005</b>	<b>18</b>	<b>Design</b> could affect monetary policy implementation and interest rate control by altering the supply of reserves in the banking system
<b>D0006</b>	<b>18</b>	<b>Design</b> should allow an increase in CBDC supply to provide an adequate buffer, so there is little effect on the federal funds rate
<b>D0007</b>	<b>18</b>	<b>Design</b> should allow the Federal Reserve to increase the level of reserves on average, in order to provide an adequate buffer against unanticipated increases in CBDC
<b>D0008</b>	<b>18</b>	<b>Design</b> should allow for interest-bearing at levels of the CBDC to be controlled independently of other safe assets
<b>D0009</b>	<b>18</b>	<b>Design</b> should allow for significant foreign demand for CBDC, further complicating monetary policy implementation
<b>D0010</b>	<b>18</b>	<b>Design</b> should consider the potential for interest-bearing CBDC as a new policy tool on the channels of influence in monetary policy
<b>D0011</b>	<b>19</b>	<b>Design</b> should generate data about users' financial transactions in the same ways that commercial bank and nonbank money generates data today
<b>D0012</b>	<b>19</b>	<b>Design</b> should address privacy concerns by leveraging existing tools already in use by intermediaries
<b>D0013</b>	<b>19</b>	<b>Design</b> should facilitate compliance with a robust set of rules already intended to combat <ol style="list-style-type: none"> <li>1. money laundering</li> <li>2. the financing of terrorism</li> <li>3. customer due diligence</li> <li>4. record-keeping</li> <li>5. reporting requirements</li> </ol>
<b>D0014</b>	<b>20</b>	<b>Design</b> should involve private-sector partners with established programs to help ensure compliance with existing rules

Desirement No.	Page No.	Desirement
D0015	20	<b>Design</b> should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks
D0016	20	<b>Design</b> should include offline capabilities to help with the operational resilience of the payment system
D0017	20	<b>Design</b> should include digital payments in areas suffering from large disruption, such as natural disasters

17)

**Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something desired but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

18)

Board of Governors, The Federal Reserve System, January 2022, Accessed: 5 May 2022, <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

19)

**Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

20)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**.

21)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:12\\_summary:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:12_summary:start)



Last update: **2022/05/18 21:48**

# 4.0 Common Elements

## [OMG Responses to Federal Reserve Discussion Paper](#)

[Return to the Main Document](#) [Provide Feedback](#)

During the review of the 22 questions posed in the **White Paper** it was decided that there were some common elements that needed to be separately addressed in order to not repeat the same information in the response to multiple questions.

## Overview

[Return to Top](#)

Based on a preliminary evaluation of the Questions given in the [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#)<sup>22)</sup> **White Paper**, it was observed that these questions shared common elements, i.e., recurring topics, that could and should be addressed independently of the individual questions so that their content can simply be referenced by OMG's answers, as appropriate.

## Outline of Common Topics

[Return to Top](#)

- [4.1 Stakeholders](#)
- [4.2 Currency Models](#)
  - [4.2.1 Digital Cash Model](#)
  - [4.2.2 Digital Account Model](#)
- [4.3 Stablecoins](#)
- [4.4 National Privacy Considerations](#)
- [4.5 National Security Considerations](#)
  - [4.5.1 Human Trafficking](#)
  - [4.5.2 Drug Trafficking](#)
  - [4.5.3 Corruption](#)
  - [4.5.4 Money Laundering](#)
- [4.6 International Considerations](#)
  - [4.6.1 Data Residency](#)
  - [4.6.2 Data Localization](#)
  - [4.6.3 Data Sovereignty](#)
- [4.7 Dual Payment Networks](#)

<sup>22)</sup>



Board of Governors, The Federal Reserve System, January 2022, Accessed: 5 May 2022,  
<https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:start)



Last update: **2022/05/18 21:21**

# 4.1 Stakeholders

[Return to Common Elements](#) [Provide Feedback](#)

## Overview

[Return to Top](#)

A **Stakeholder** is a party with an interest in a **Central Bank Digital Currency (CBDC)** effort and can either affect or be affected by the CBDC effort. The primary stakeholders in the CBDC effort are **U.S. Federal Government Oversight Authorities**, **non-U.S. Federal Government Oversight Authorities**, customers, and suppliers of goods and services.

However, with the increasing attention on social responsibility, the Stakeholder concept now includes: communities, governments, trade associations, and **Communities of Interest (Cols)**.

- A CBDC stakeholder has a vested interest in a CBDC effort and can either affect or be affected by a CBDC effort's operations and performance
- Typical CBDC stakeholders are the customers, suppliers of goods, services, **U.S. Federal Authorities**, and **non-U.S. Federal Authorities**
- CBDC stakeholders can be both internal and external to the CBDC effort.

There are two “Desirements”<sup>23)</sup> specified in the White Paper that specifies the need to establish a comprehensive list of Stakeholders:

Table 10: Desirements for identification of key Stakeholders

Statement No.	Page No.	Desirement Statement
<b>B0006</b>	<b>2</b>	<b>Provide broad support from key stakeholders</b>
<b>P0006</b>	<b>2</b>	<b>Garner broad support from key stakeholders</b>
B = <a href="#">Benefit Considerations</a>		
P = <a href="#">Policy Considerations</a>		
R = <a href="#">Risk Considerations</a>		
D = <a href="#">Design Considerations</a>		

Table 11: Summary of the estimated number of Government Stakeholders for the CBDC.

Potential Oversight Authorities	No. of Stakeholders
<b>U.S. Federal Government Oversight Authorities</b>	14
<b>non-U.S. Federal Government Oversight Authorities</b>	19
<b>Total</b>	<b>33</b>

## U.S. Federal Government Oversight Authorities

[Return to Top](#)

Table 12 provides a list of authorities within the U.S. having oversight over financial services. Some authorities listed are Agencies of the U.S. such as the [Securities and Exchange Commission \(SEC\)](#) or the [Consumer Financial Protection Bureau \(CFPB\)](#). Others are independent non-governmental organizations, such as the [Financial Industry Regulatory Authority \(FINRA\)](#).

There are roughly 14 U.S. Federal Government Authorities with financial oversight.

Table 12: U.S. Federal Government Authorities with financial oversight

Authority	Description
<b>U.S. Treasury</b>	The <b>U.S. Treasury</b> is the government department responsible for issuing all Treasury bonds, notes, and bills. Among the government departments operating under the U.S. Treasury umbrella are the: <ol style="list-style-type: none"> <li>1. Internal Revenue Service (IRS)</li> <li>2. U.S. Mint, the Bureau of the Fiscal Service</li> <li>3. Alcohol and Tobacco Tax and Trade Bureau</li> </ol>
<b>U.S. Securities and Exchange Commission (SEC)</b>	The <b>SEC</b> is the U.S. government agency in charge of the nation's <a href="#">securities</a> industry. It monitors transactions, as well as the activities of financial professionals. Its mission is to promote fairness, integrity, and transparency; prevent fraud and other deceptive acts, and ensure orderly and efficient markets.
<b>Financial Industry Regulatory Authority (FINRA)</b>	<b>FINRA</b> is an independent, nongovernmental organization that writes and enforces the rules governing registered brokers and broker-dealer firms in the United States. Its stated mission is "to safeguard the investing public against fraud and bad practices." It is considered a self-regulatory organization.
<b>Consumer Financial Protection Bureau (CFPB)</b>	The <b>CFPB</b> is a regulatory agency charged with overseeing financial products and services that are offered to consumers.
<b>Commodity Futures Trading Commission (CFTC)</b>	The <b>CFTC</b> regulates the derivatives markets, including futures contracts, options, and swaps. Its goals include the promotion of competitive and efficient markets and the protection of investors against manipulation, abusive trade practices, and fraud.
<b>Federal Reserve System (The Fed)</b>	<b>The Fed</b> is the central banking system of the United States and oversees the 12 regional Federal Reserve Banks. Its primary goals are to regulate the nation's private banks and manage the overall money supply. The Fed ensures lenders and borrowers have access to credit and loans.
<b>Federal Deposit Insurance Corporation (FDIC)</b>	The <b>FDIC</b> maintains stability and public confidence in the nation's financial system by insuring deposits; examining and supervising financial institutions for safety, soundness, and consumer protection; making large and complex financial institutions resolvable; and managing receivership.
<b>Office of the Comptroller of the Currency (OCC)</b>	The <b>OCC</b> is an organization that acts as both the issuer and guarantor for options and futures contracts and is the largest equity derivatives clearing organization in the world.
<b>National Association of Insurance Commissioners (NAIC)</b>	<b>NAIC</b> is a nonprofit, nonpartisan organization that sets standards and establishes best practices for the U.S. insurance industry, and provides support to insurance regulators. It also provides information and resources to consumers. <b>Note:</b> Insurance products sold in the U.S. are largely regulated by the states, rather than the federal government.

Authority	Description
<b>National Credit Union Administration (NCUA)</b>	The <b>NCUA</b> monitors federal credit unions across the country and provides the National Credit Union Share Insurance Fund (NCUSIF) which uses tax dollars to insure the deposits at all federal credit unions.
<b>Federal Emergency Management Agency (FEMA)</b>	<b>FEMA</b> is a United States government agency with the purpose to coordinate aid and respond to disasters around the nation when local resources are insufficient. Commanding a budget of approximately \$14 billion annually, the agency is headquartered in Washington, D.C.
<b>Department of Justice (Doj)</b>	The U.S. DOJ enforces U.S. law through its agencies and protects the public from foreign and domestic threats such as terrorism and criminal activities. The department also investigates financial fraud and manages the federal prison system. The DOJ also represents the country in legal affairs, such as in cases before the Supreme Court. The DOJ shares security responsibilities with the U.S. Department of Homeland Security (DHS) and the U.S. Department of Health and Human Services (HHS).
<b>Federal Bureau of Investigation (FBI)</b>	The <b>FBI</b> is the principal law enforcement agency and national security service of the federal government. The FBI is housed under the Department of Justice and additionally reports to the Director of National Intelligence. As a law enforcement agency, the FBI investigates an array of federal crimes, including public corruption, terrorism, cybercrime, civil rights violations, drug trafficking, sex trafficking, and white-collar crime. As a national security service, the FBI conducts counterintelligence to prevent espionage.
<b>Drug Enforcement Administration (DEA)</b>	<b>DEA</b> enforces the provisions of the controlled substances and chemical diversion and trafficking laws and regulations of the United States, and operates on a worldwide basis. It presents cases to the criminal and civil justice systems of the United States—or any other competent jurisdiction—on those significant organizations and their members involved in the cultivation, production, smuggling, distribution, laundering of proceeds, or diversion of controlled substances appearing in or destined for illegal traffic in the United States.

## non-U.S. Federal Government Oversight Authorities

[Return to Top](#)

Table 13 provides a list of authorities that are not within the U.S. and have oversight over financial services. Each of the Countries that the organization is associated with is provided in the first column. A few organizations are umbrella organizations covering several countries and are declared **international**.

There are at least 18 non-U.S. Federal Government Authorities with financial oversight.

Table 13: Non-U.S. Government Authorities with financial oversight

Country	Authority	Description
<b>United Kingdom</b>	<b>Bank of England (BoE)</b>	The <b>BoE</b> is the central bank for the United Kingdom. It acts as the government's bank and the lender of last resort. The BoE issues currency and, most importantly, oversees monetary policy.

Country	Authority	Description
	<b>Prudential Regulation Authority (PRA)</b>	The <b>PRA</b> is a part of the Bank of England and is responsible for the prudent regulation and supervision of banks, building societies, credit unions, insurers, and major investment firms. It sets standards and supervises financial institutions at the level of the individual firm.
	<b>Financial Conduct Authority (FCA)</b>	The <b>FCA</b> works alongside the <a href="#">Prudential Regulation Authority (PRA)</a> in regulating the financial services industry in the UK and is responsible for the prudential regulation of those financial services firms not supervised by the PRA such as asset managers and independent financial advisers. The FCA has “ <i>rule-making, investigative and enforcement powers</i> ” to regulate the financial services industry.
<b>Japan</b>	<b>Financial Services Agency (FSA)</b>	The <b>FSA</b> is the chief regulator of Japan’s financial services industry, responsible for maintaining its stability and integrity, and is mandated to oversee the banking, insurance and securities, and exchange industries. It’s also charged with protecting market participants from fraud and money laundering.
<b>Germany</b>	<b>Federal Financial Supervisory Authority (BaFin)</b>	<b>BaFin</b> integrates the regulatory functions of those agencies with authority over Germany’s banks, financial services companies, insurance companies, stock exchanges, and other obligated institutions. An important part of BaFin’s role as regulator is to identify and eliminate financial crime – a function that includes promoting anti-money laundering in Germany, and counter-terrorist financing.
<b>France</b>	<b>Autorité des marchés financiers (AMF)</b>	<b>AMF</b> is an independent body that supervises financial companies operating in France with three core responsibilities: <ol style="list-style-type: none"> <li>1. safeguard investments</li> <li>2. increase transparency in financial instruments</li> <li>3. ensure financial markets run smoothly</li> </ol> It is also charged with keeping the nation’s markets and financial services industry free of fraud and money laundering. Additionally, France’s AMF is a rules-setter and is responsible for implementing the EU’s 2018 <a href="#">Markets in Financial Instruments Directive II (MiFID II)</a> directive as well as its own General Regulation.
<b>Singapore</b>	<b>Monetary Authority of Singapore (MAS)</b>	The <b>MAS</b> is empowered by the Monetary Authority of Singapore Act to set regulations and supervise the city’s banking, capital markets, insurance, and payments sectors. The organization enforces its regulations and government laws through legally binding instructions called Directions. They may take the form of Directives, which are issued to specific entities or individuals, and Notices, which cover a class of asset, institution, or person, such as loans or loan issuers.
<b>Switzerland</b>	<b>Financial Market Supervisory Authority (FINMA)</b>	<b>FINMA</b> is Switzerland’s independent financial-markets regulator. Its mandate is to supervise banks, insurance companies, financial institutions, collective investment schemes, and their asset managers and fund management companies. It also regulates insurance intermediaries. It is charged with protecting creditors, investors, and policyholders. FINMA is responsible for ensuring that Switzerland’s financial markets function effectively.

Country	Authority	Description
People's Republic of China	<b>China Banking Regulatory Commission (CBRC)</b>	The <b>CBRC</b> is authorized by the State Council to regulate the banking sector of the PRC except for the territories of Hong Kong and Macau, both of which are special administrative regions.
	<b>China Insurance Regulatory Commission (CIRC)</b>	CIRC is used to regulate the Chinese insurance products and services market and maintain legal and stable operations of the insurance industry. In 2018, it was merged with the banking regulator China Banking Regulatory Commission (CBRC) to create the China Banking and Insurance Regulatory Commission (CBIRC).
	<b>China Securities Regulatory Commission (CSRC)</b>	The <b>CSRC</b> is the national regulatory body that oversees the securities and futures industry of the country. The CSRC is the functional equivalent of the <b>Securities and Exchange Commission (SEC)</b> of the U.S., charged with maintaining orderly and fair markets.
India	<b>Reserve Bank of India (RBI)</b>	The <b>RBI</b> is the central bank of India, whose primary function is to manage and govern the financial system of the country, and it regulates the issue and supply of the Indian rupee. Additionally, it looks after the central government's money and is the of the <i>bankers' bank</i> and regulates the banking sector. The RBI is important in India's development by supporting the government in its developmental projects and policies.
	<b>Securities and Exchange Board of India (SEBI)</b>	The <b>SEBI</b> is the most important regulator of securities markets in India and is the counterpart of the <b>Securities and Exchange Commission (SEC)</b> in the U.S. The stated objective of the SEBI is <i>"to protect the interests of investors in securities and to promote the development of, and to regulate the securities market and for matters connected therewith or incidental thereto."</i>
	<b>Insolvency and Bankruptcy Board of India (IBBI)</b>	<b>IBBI</b> is a key pillar of the ecosystem responsible for the implementation of the Code that consolidates and amends the laws relating to reorganization and insolvency resolution of corporate persons, partnership firms, and individuals in a time-bound manner for maximization of the value of assets of such persons, to promote entrepreneurship, availability of credit and balance the interests of all the stakeholders.
	<b>Insurance Regulatory and Development Authority of India (IRDAI)</b>	The <b>IRDAI</b> has overall responsibility for the supervision and development of the Insurance sector in India. The key objectives of the IRDAI include the promotion of competition to enhance customer satisfaction through increased consumer choice and fair premiums and ensuring the financial security of the Insurance market. Additionally, the IRDAI frames regulations laying down the regulatory framework for the supervision of the entities operating in the sector.
	<b>Pension Fund Regulatory and Development Authority (PFRDA)</b>	<b>PFRDA</b> regulates the National Pension System (NPS), subscribed by employees of the Government of India, Indian State Governments, and by employees of private institutions, organizations, and unorganized sectors. PFRDA ensures the orderly growth and development of the pension market.

Country	Authority	Description
International	<b>Financial Action Task Force (FATF)</b>	The <b>FATF</b> is an intergovernmental organization that develops standards around <a href="#">Anti Money Laundering (AML)</a> to promote policies and standards to combat the financial crime of money laundering and terrorism funding. Additionally, FATF produces two lists of uncooperative jurisdictions in efforts against money laundering (and terrorism financing).
International	<b>Markets in Financial Instruments Directive II (MiFID II)</b>	The EU's <b>MiFID II</b> is a 2018 update to the original <a href="#">Markets in Financial Instruments Directive (MiFID)</a> and is a legislative framework instituted by the European Union (EU) to regulate financial markets in the bloc and improve protections for investors. Its aim is to standardize practices across the EU and restore confidence in the industry.
International	<b>The World Bank Group</b>	The <b>World Bank Group</b> (also known as <b>World Bank</b> ) is one of the world's largest sources of funding and knowledge for developing countries. Its five institutions share a commitment to reducing poverty, increasing shared prosperity, and promoting sustainable development.

## Examples

[Return to Top](#)

Some of the “desirements” in the [Money and Payments: The U.S. Dollar in the Age of Digital Transformation White Paper](#) relating to [Central Bank Digital Currency \(CBDC\) Stakeholders](#) are summarized in the [White Paper Analysis](#) done by the [Object Management Group](#) and listed in [Table 14](#).

Table 14: List of Stakeholder Desirements identified in the White Paper

Category	Desirements
<b>Benefits</b>	B0006, B0009, B0015, B0020, B0026, B0029, B0035, B0038, B0041, B0043, B0045, B0046, B0052, B0053
<b>Policy Considerations</b>	P0006, P0011, P0017, P0020, P0021, P0023, P0025, P0028, P0031
<b>Risks</b>	R0001, R0005, R0018, R0020, R0021, R0023
<b>Design</b>	D0010, D0011, D0012, D0013, D0014, D0015, D0016, D0017

## Discussion of Examples

[Return to Top](#)

[Table 15](#) provides a comment for those “desirements” identified by the in [White Paper](#) and identified by the [OMG's White Paper Analysis](#) relating to [Central Bank Digital Currency \(CBDC\) Stakeholders](#). See: [Table 14](#).

Table 15: List of “desirements” that allude to **stakeholders**



<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>B0006</b>	<b>Provide broad support from key stakeholders</b>	This is the reason to include this section in a CBDC effort.
<b>B0009</b>	<b>Provide faster and cheaper payments (including cross-border payments)</b>	This requires the CBDC to have interaction with Authorities from <a href="#">U.S. Federal Government Oversight Authorities</a> and <a href="#">non-U.S. Federal Government Oversight Authorities</a> , making them Stakeholders.
<b>B0015</b>	<b>Reduce cross-border costs to benefit:</b> <b>1. economic growth</b> <b>2. enhance global commerce</b> <b>3. improve international remittances</b> <b>4. reduce inequality</b>	See <b>B0009</b> . This requires the CBDC to have interaction with Authorities from <a href="#">U.S. Federal Government Oversight Authorities</a> and <a href="#">non-U.S. Federal Government Oversight Authorities</a> , making them Stakeholders.
<b>B0020</b>	<b>Maintain public confidence by not requiring mechanisms, such as deposit insurance</b>	In order to instill public confidence in a CBDC, the public needs to be included as Stakeholders.
<b>B0026</b>	<b>Provide a bridge between legacy and new payment services</b>	In order to successfully bridge between the legacy and new payment services, the CBDC needs to work with existing <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>B0029</b>	<b>Support basic purchases of:</b> <b>1. goods</b> <b>2. services</b> <b>3. pay bills</b> <b>4. pay taxes</b>	1. goods - Requires the active participation of the retail sector as a Stakeholder 2. services - This should be covered under existing Intermediaries as Stakeholders 3. pay bills - This should be covered under existing Intermediaries as Stakeholders 4. pay taxes - This might require the inclusion of the U.S. Treasuries Internal Revenue Service (IRS) as a stakeholder
<b>B0035</b>	<b>Streamline cross-border payments by using:</b> <b>1. new technologies</b> <b>2. introducing simplified distribution channels</b> <b>3. creating additional opportunities for cross-jurisdictional collaboration and interoperability</b>	1. new technologies - Requires the inclusion of the new and emerging technology business areas (i.e., Stablecoins) as Stakeholders 2. introducing simplified distribution channels - Requires the participation of the existing Intermediaries as Stakeholders 3. creating additional opportunities for cross-jurisdictional collaboration and interoperability - See <b>B0009</b> . This requires the CBDC to have interaction with Authorities from <a href="#">U.S. Federal Government Oversight Authorities</a> and <a href="#">non-U.S. Federal Government Oversight Authorities</a> , making them Stakeholders.
<b>B0037</b>	<b>Support private-sector innovation</b>	Requires the inclusion of the new and emerging technology business areas (i.e., Stablecoins, Blockchains, DIDOs, etc. ) as Stakeholders



Desirement No.	Desirement Text	Comment
B0038	<b>Allow private-sector innovators to focus on:</b> <b>1. new access services</b> <b>2. distribution methods</b> <b>3. related service offerings</b>	Requires all the private-sector innovators to participate as Stakeholders
B0041	<b>Support streamlining cross-border payments</b>	See <b>B0009</b> . This requires the CBDC to have interaction with Authorities from <a href="#">U.S. Federal Government Oversight Authorities</a> and <a href="#">non-U.S. Federal Government Oversight Authorities</a> , making them Stakeholders.
B0043	<b>Promoting financial inclusion—particularly for economically vulnerable households and communities</b>	<p>This would require U.S. Government Departments and Agencies with a Charter to help the economically vulnerable be considered Stakeholders. For Example, see: <a href="#">U.S. Gov.</a></p> <ol style="list-style-type: none"> <li>1. Benefits and Financial Assistance from the Government</li> <li>2. How to Apply for Unemployment Benefits</li> <li>3. Food Stamps (SNAP Food Benefits)</li> <li>4. Welfare or Temporary Assistance for Needy Families (TANF)</li> <li>5. Medicaid and Children's Health Insurance Program (CHIP)</li> </ol> <p>It might also require the inclusion of Social Security and Medicare.</p> <ol style="list-style-type: none"> <li>1. Social Security Administration</li> </ol>
B0045	<b>Enable rapid and cost-effective payment of taxes</b>	This should require the inclusion of the U.S. Treasuries Internal Revenue Service (IRS) as a Stakeholder.
B0046	<b>Enable rapid and cost-effective delivery of:</b> <b>1. wages</b> <b>2. tax refunds</b> <b>3. other federal payments</b>	<ol style="list-style-type: none"> <li>1. wages - This should be covered under existing Intermediaries as Stakeholders.</li> <li>2. tax refunds - This should require the inclusion of the U.S. Treasuries Internal Revenue Service (IRS) as a Stakeholder.</li> <li>3. other federal payments - See <b>B0013</b>.</li> </ol>
B0051	<b>Generate data about users' financial transactions similarly to current Commercial Bank<sup>24)</sup> and Nonbank Money</b>	See: <a href="#">National Privacy Considerations</a> .
B0052	<b>Prevent Financial money laundering crimes</b>	This would require <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
B0053	<b>Provide resiliency to threats to existing payment services—including:</b> <b>1. operational disruptions</b> <b>2. cybersecurity risks</b>	<a href="#">Federal Emergency Management Agency (FEMA)</a> is the agency that provides most of the relief and coordination during Natural Disasters making them a Shareholder in a CBDC.

Desirement No.	Desirement Text	Comment
P0006	<b>Garner broad support from key stakeholders</b>	This is the reason to include this section in a CBDC effort.
P0011	<b>The Federal Reserve does not intend to proceed with the issuance of a CBDC without clear support from the Executive Branch and Legislative Branch, ideally in the form of a specific authorizing law.</b>	This makes the <b>Executive Branch</b> and the <b>Legislative Branch</b> Stakeholders in the CBDC.
P0017	<b>The PWG report recommends CBDC complement existing authorities regarding:</b> 1. market integrity 2. investor protection 3. illicit finance	This would require <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders
P0020	<b>The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments</b>	This includes both the current Intermediaries and Entrepreneurs to be included as Stakeholders.
P0021	<b>The intermediaries would operate in an open market for CBDC services</b>	To create an open market, the intermediaries would have to publish and adhere to standards. This would mean one or more <a href="#">Standards Developing Organization (SDO)</a> need to be included as Stakeholders.
P0023	<b>CBDC would need to be readily transferable between customers of different intermediaries</b>	See: <b>P0021</b> and <a href="#">Standards Developing Organizations (SDOs)</a> .
P0025	<b>CBDC intermediary would need to verify the identity of a person accessing CBDC</b>	This includes the current Intermediaries as Stakeholders
P0028	<b>Require significant international coordination to address issues such as:</b> 1. common standards 2. infrastructure, 3. the types of intermediaries able to access any new infrastructure, 4. legal frameworks 5. preventing illicit transactions 6. the cost and timing of implementation	1. common standards - See: <a href="#">Standards Developing Organization (SDO)</a> as Stakeholders. 2. the types of intermediaries able to access any new infrastructure make the intermediaries Stakeholders. 3. legal frameworks - See: <a href="#">Standards Developing Organization (SDO)</a> as Stakeholders. 4. preventing illicit transactions - See: <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
P0031	<b>The Federal Reserve would only pursue a CBDC in the context of broad public and cross-governmental support</b>	This requires a broad Stakeholder Base to participate in a transparent CBDC consortium that has policies and procedures that are well documented, fair and equitable.
R0001	<b>Risk of affecting financial-sector market structure</b>	This includes the current Intermediaries as Stakeholders.

<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>R0005</b>	<b>New payment services could pose Risks to:</b> 1. financial stability 2. payment system integrity 3. other Risks	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>R0018</b>	<b>Risk a CBDC could fundamentally change the structure of the U.S. financial system, altering private sector and central bank:</b> 1. roles 2. responsibilities	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>R0020</b>	<b>Risk that interest-bearing CBDC could result in a shift away from other low-risk assets, such as shares in money market mutual funds, Treasury bills, and other short-term instruments.</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>R0021</b>	<b>Risk of reducing credit availability or raise credit costs for businesses and governments</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>R0023</b>	<b>Risk of financial panic causing outflows from Commercial Banks to CBDC without prudential supervision, government deposit insurance, and access to central bank liquidity</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>D0001</b>	<b>Design should be for a non-interest-bearing CBDC, for example, would be less attractive as a substitute for commercial bank money</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>D0004</b>	<b>Design should influence how the Federal Reserve might affect monetary policy</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>D0005</b>	<b>Design could affect monetary policy implementation and interest rate control by altering the supply of reserves in the banking system</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
<b>D0009</b>	<b>Design should allow for significant foreign demand for CBDC, furthering complicate monetary policy implementation</b>	See: <b>B0009</b> . This requires the CBDC to have interaction with Authorities from <a href="#">U.S. Federal Government Oversight Authorities</a> and <a href="#">non-U.S. Federal Government Oversight Authorities</a> , making them Stakeholders.
<b>D0010</b>	<b>Design should consider the potential for interest-bearing CBDC as a new policy tool on the channels of influence in monetary policy</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.

Desirement No.	Desirement Text	Comment
D0011	<b>Design should generate data about users' financial transactions in the same ways that commercial bank and nonbank money generates data today</b>	See: <a href="#">National Privacy Considerations</a>
D0012	<b>Design should address privacy concerns by leveraging existing tools already in use by intermediaries</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
D0013	<b>Design should facilitate compliance with a robust set of rules already intended to combat</b> <b>1. money laundering</b> <b>2. the financing of terrorism</b> <b>3. customer due diligence</b> <b>4. record keeping</b> <b>5. reporting requirements</b>	This requires the continued coordinated efforts of the <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
D0014	<b>Design should involve private-sector partners with established programs to help ensure compliance with existing rules</b>	This includes the current Intermediaries as Stakeholders.
D0015	<b>Design should include any dedicated infrastructure required to provide a resilience to threats such as operational disruptions and cybersecurity risks</b>	This includes the current Intermediaries and <a href="#">U.S. Federal Government Oversight Authorities</a> as Stakeholders.
D0016	<b>Design should include offline capabilities to help with operational resilience of the payment system</b>	<a href="#">Federal Emergency Management Agency (FEMA)</a> is the agency that provides most of the relief and coordination during Natural Disasters making them a Shareholder in a CBDC.
D0017	<b>Design should include digital payments in areas suffering from large disruption, such as natural disasters</b>	<a href="#">Federal Emergency Management Agency (FEMA)</a> is the agency that provides most of the relief and coordination during Natural Disasters making them a Shareholder in a CBDC.

23)

**Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired, but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

24)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**&.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:15\\_common:05\\_stakeholder:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:15_common:05_stakeholder:start)

Last update: **2022/05/18 22:00**



## 4.2 Currency Models

[Return to Common Elements](#) | [Provide Feedback](#)

### Overview

[Return to Top](#)

The Bank For International Settlements provides a good explanation of the problems confronting the U.S. Federal Reserve's CBDC effort.<sup>25)</sup>

*CBDC is not a well-defined term. It is used to refer to a number of concepts. However, it is envisioned by most to be a new form of central bank money. That is, a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value. This would be an innovation for general-purpose users, but not for wholesale entities. Central banks already provide digital money in the form of reserves or settlement account balances held by commercial banks and certain other financial institutions at the central bank. This mix of new and already existing forms of central bank money makes it challenging to precisely define what a CBDC is. In fact, for purposes of analyzing what may change, it is easier to define a CBDC by highlighting what it is **NOT**:*

***a CBDC is a digital form of central bank money that is different from balances in traditional reserve or settlement accounts.***<sup>26)</sup>

*A key distinction between token [**Digital Cash**] and account-based [**Digital Account**] money is the form of verification needed when it is exchanged (Kahn and Roberds (2009)). Token-based money (or payment systems) relies critically on the ability of the payee to verify the validity of the payment object. With cash the worry is counterfeiting, while in the digital world the worry is whether the token or "coin" is genuine or not (electronic counterfeiting) and whether it has already been spent. By contrast, systems based on account money depend fundamentally on the ability to verify the identity of the account holder. A key concern is identity theft, which allows perpetrators to transfer or withdraw money from accounts without permission. Identification is needed to correctly link payers and payees and to ascertain their respective account histories.*

### Taxonomy

[Return to Top](#)

*CBDC is not a well-defined term. It is used to refer to a number of concepts. However, it is envisioned by most to be a new form of central bank money. That is, a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value. This would be an innovation for general-purpose users but not for wholesale entities. Central banks already provide digital money in the form of reserves or settlement account balances held by commercial banks and certain other financial institutions at the central bank. This mix of*

*new and already existing forms of central bank money makes it challenging to precisely define what a CBDC is. In fact, for purposes of analyzing what may change, it is easier to define a CBDC by highlighting what it is not: a CBDC is a digital form of central bank money that is different from balances in traditional reserve or settlement accounts.*<sup>27)</sup>

Figure 2 presents a Venn diagram of two different taxonomies that can be used to classify Cryptocurrencies.

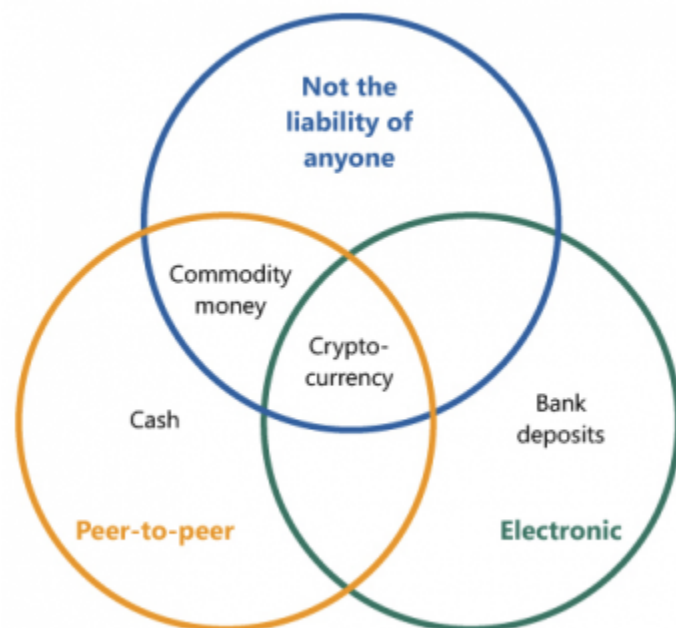
The diagram on the left side of the figure represents the forms of money. Cash, for example, is **Peer-to-Peer (P2P)** but is not electronic. Cash is a Central Bank liability.

While bank deposits (i.e., Digital Accounts) are electronic but are not P2P. Bank Deposits are the liability of the bank that holds the accounts. The money is exchanged using a centralized system such as the **Automated Clearing House (ACH) Network**.

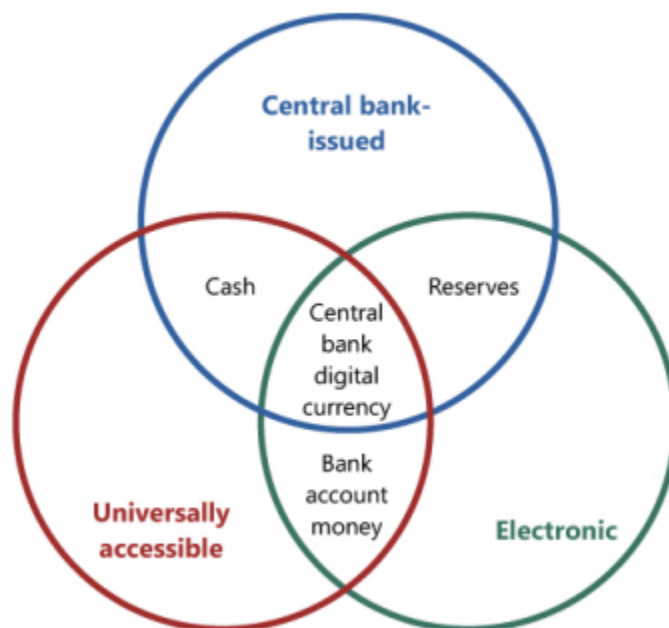
Cryptocurrencies attempt to bridge both the P2P and the electronic categories. There really isn't much liability for Cryptocurrencies other than the promises made in the governing White Papers and the value of the cryptocurrency itself.

The diagram on the right side uses a Venn Diagram to illustrate CBDC as the intersection of Central Bank Issued, Universally Accessible, and Electronic. At the intersection of the three Venn circles are: CBDC and Bank Account Money.

Cryptocurrency, CPMI (2015)



Central bank digital currency, Bjerg (2017)



© Bank for International Settlements

Figure 2: Venn Diagrams of Two Taxonomies of New Forms of Money<sup>28)</sup>

Figure 3 is often referred to as the **Money Flower**. The Venn diagram has 4 circles:

- **Universally Accessible** (red)
- **Electronic** (green)
- **Central Bank Issued** (blue)



- Peer-to-Pee (P2P) (gold)

It then labels the intersection of the circles with various “concepts”. For example, one kind of CBDC is accessible to the general public(i.e., retail CBCC) and the other is available only to financial institutions (i.e., wholesale CBCC).

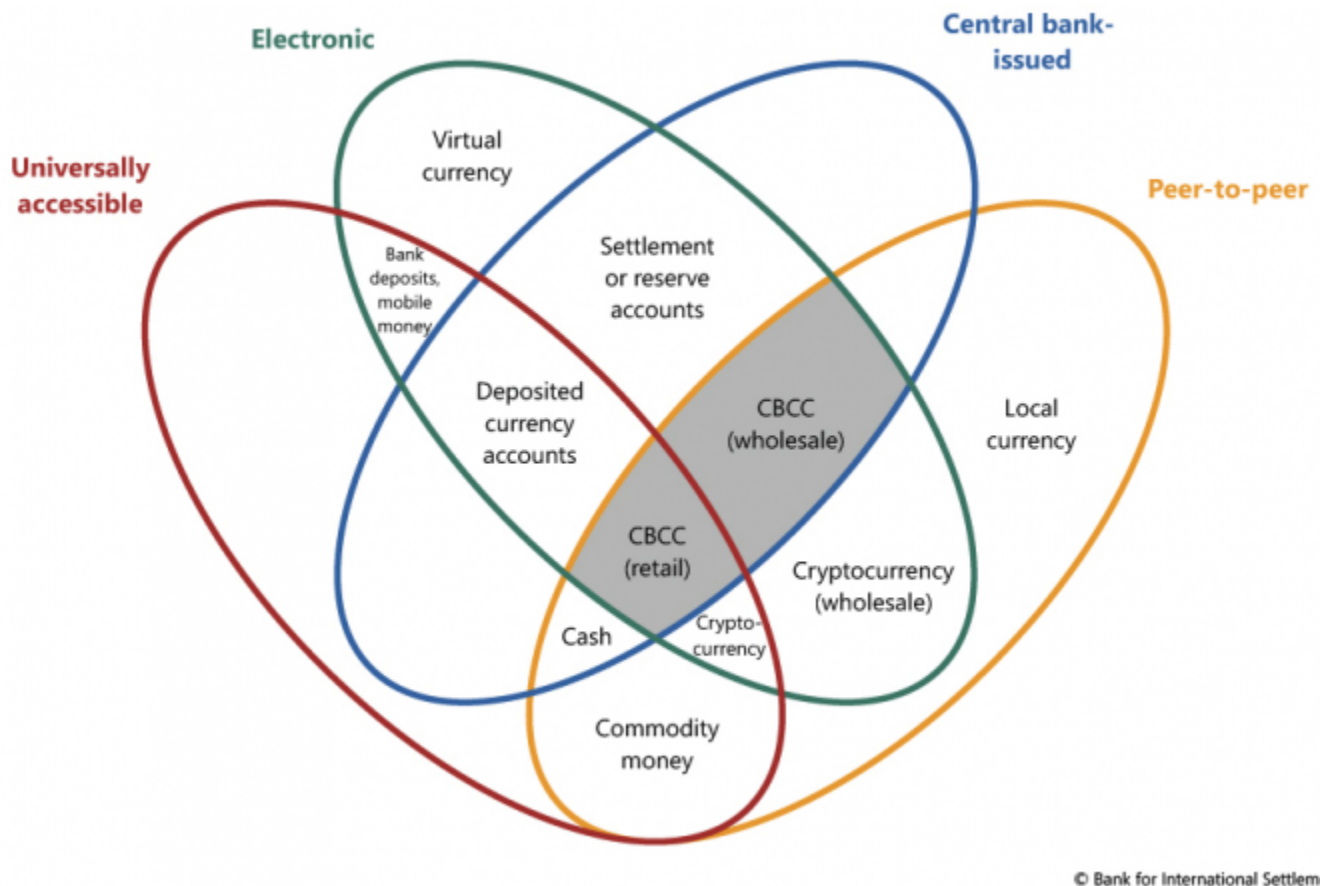


Figure 3: The Money Flower: A Venn Diagram of the Taxonomy of Money.<sup>29)</sup>

For this discussion on CBDC, two different models are used:

- [4.2.1 Digital Cash Model](#) - Tokens
- [4.2.2 Digital Account Model](#) - Accounts

<sup>25)</sup> Bank For International Settlements, Committee on Payments and Market Infrastructures, Markets Committee, March 2028, Accessed: 3 April 2022, <https://www.bis.org/cpmi/publ/d174.pdf>

<sup>26)</sup> Reserves and settlement accounts are available in most jurisdictions to “monetary policy counterparties”, i.e. financial institutions that are directly relevant for monetary policy implementation, such as deposit-taking entities, which are generally already granted access to the central bank deposit and lending facilities. In some jurisdictions, account holders may comprise a broader group and include non-monetary counterparties such as treasury, foreign central banks, or certain Financial Markets Infrastructures (FMIs). Some central banks are considering widening access. CBDC would further expand access to digital central bank money, but not to central bank lending facilities.

<sup>27)</sup> Benoît Cœuré, Jacqueline Loh, Klaus Löber, Aerd Houben, [Central Bank Digital Currencies](#), Bank of



International Settlements, Committee on Payments and Market Infrastructures - Markets Committee, March 2018, Accessed: 16 May 2022, <https://www.bis.org/cpmi/publ/d174.pdf>

28)

Morten Linnemann Bech, Rodney Garratt, Central Bank Cryptocurrencies, BIS Quarterly Review, 17 September 2017, Accessed: 16 May 2022, [https://www.bis.org/publ/qtrpdf/r\\_qt1709f.htm](https://www.bis.org/publ/qtrpdf/r_qt1709f.htm)

29)

Morten Linnemann Bech, Rodney Garratt, Central Bank Cryptocurrencies, BIS Quarterly Review, 17 September 2017, Accessed: 16 May 2022, [https://www.bis.org/publ/qtrpdf/r\\_qt1709f.htm](https://www.bis.org/publ/qtrpdf/r_qt1709f.htm)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:15\\_common:08\\_currency\\_models:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:15_common:08_currency_models:start)

Last update: **2022/05/18 21:38**



## 4.2.1 Digital Cash Model

[Return to Currency Models](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

Almost all Cryptocurrencies implemented so far use the concept of tokens, accounts, wallets, transactions, and distributed ledgers. In essence, these approaches model the way money is handled in bank accounts<sup>30</sup>. However, the CBDC could also be modeled on actual cash (i.e., \\$.01, \\$.05, \\$.10, \\$.25, \\$.50 coins and \\$1, \\$2, \\$5, \\$10, \\$20, \\$50 and \\$100 bills), in essence creating a true **Digital Dollar**. The Digital Dollar would create a [digital coin](#) for each of the denominations, with no further fractions. For example, a \\$100 digital coin would only represent a value of \$100.00 US Dollars. Representing more money would be done by collecting more \\$100 digital coins, just like a real physical wallet. Representing values less than \\$100 US dollars would be done using the other U.S.-denominated Digital Coins (i.e., \\$1, \\$5, etc). However, the Federal Reserve could issue other denominations that are higher than the \\$100 bill if it chooses<sup>31</sup>. In addition, The Federal Reserve could create smaller denominations than the penny (i.e., \$.01). These denominations are impractical and too costly for real currencies but could be useful for micropayments (see **B0040** ). The smallest denomination would most likely be limited in granularity to the cost of running the Consensus Algorithms (See the [OMG DIDO-RA discussion on Consensus](#)).

The End User could use a Digital Cash Wallet to hold their Digital Cash. These wallets could hold not only US Digital Currencies, but also other currencies, such as Digital UK Pounds, EU Euros, Japanese Yen, etc. The characteristics of Digital Cash are much like real cash, although there are no reasons an End User can not have and use only cash. At some point, in order to manage risk from loss, theft, damage, etc., it is best to put the cash into an account at some financial institution such as a bank, savings, loan, credit union, etc.

One could also allow Digital Cash to be bundled and processed into a Digital Cash Wallet. The Digital Cash Wallet would be very similar to an actual wallet. It would contain a collection of Digital Cash coins or Certificates in an array of Digital Currency Denominations.

### Digital Cash Theoretical User Scenario

[Return to Top](#)

**Note:** The following Digital Cash Theoretical User Scenario is only provided for discussion purposes. Actual User Scenarios would be developed during systems analysis and modeled using a Model-Based Systems Engineering (MBSE) approach and address the problem in far more detail with a team of experts.

**Note:** Also look at the [Digital Account Model Theoretical User Scenario](#).

In the following example, the CBDC is modeled as a collection of Stablecoins, each one representing a form of physical cash (i.e., \\$.01, \\$.05, \\$.10, \\$.25, \\$.50 coins and \\$1, \\$2, \\$5, \\$10, \\$20, \\$50 and \\$100 bills). The End User would actually “own” these Stablecoins and consequently, they would have all the same shortcomings as their physical equivalent. For example, if the Stablecoins are lost, damaged, or stolen, there is no “back-up”. Contrast this with a Digital Account Model, where there are all kinds of safeguards protecting the asset.

This lack of protection from loss, damage, or theft becomes a natural deterrent to collecting and saving these as assets, just as with real physical currency. In essence, people are free to keep large amounts of cash in their mattresses, but the risk of loss, damage, or theft is high, thus prompting most end Users to deposit the money in accounts managed by traditional financial intermediaries.

Figure 4 represents a stylized use of a Digital Cash flow of a consumer (End User) buying a product from a retail store.

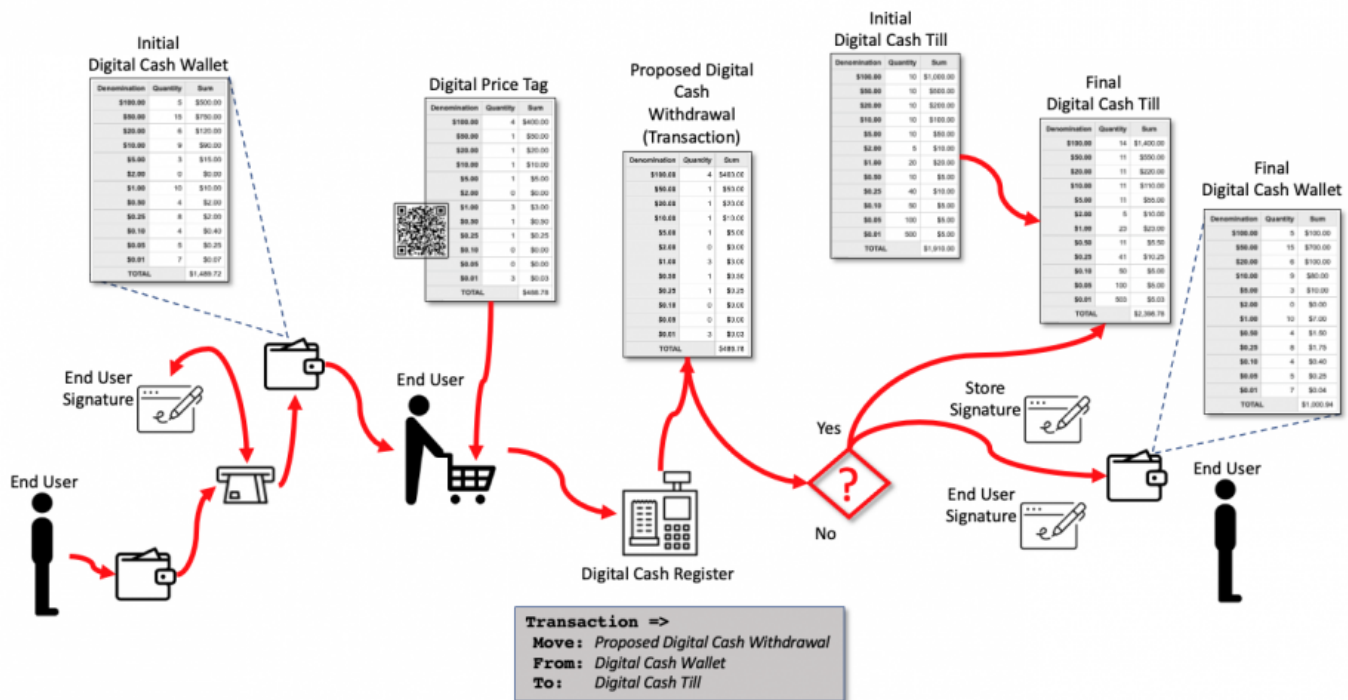


Figure 4: Simplified Digital Cash Flow

- Table 16 represents the initial contents of a Digital Cash Wallet of an End User. Each Digital Cash coin (Certificate) in the wallet, such as the five /\$100 coins, is signed by the owner of the Digital Cash Wallet. If there are Digital Cash Certificates that are not signed by the owner, they can not be used for the transaction.
- Table 17 represents the initial contents of Digital Cash Till at a store. Each Digital Cash Certificate, such as the ten /\$100 coins, is signed by the store that owns the Digital Cash Till. If there are Digital Cash Certificates that are not signed by the store, they can not be used for the transaction.

Table 16: Example of the initial contents of an End User Digital Cash Wallet.

Denomination	Quantity	Sum
\\$100.00	5	\$500.00
\\$50.00	15	\$750.00
\\$20.00	6	\$120.00
\\$10.00	9	\$90.00
\\$5.00	3	\$15.00
\\$2.00	0	\$0.00
\\$1.00	10	\$10.00
\\$0.50	4	\$2.00
\\$0.25	8	\$2.00
\\$0.10	4	\$0.40
\\$0.05	5	\$0.25
\\$0.01	7	\$0.07
<b>TOTAL</b>		\$1,489.72

Table 17: Example of the initial contents of a store's Digital Cash Till.

Denomination	Quantity	Sum
\\$100.00	10	\$1,000.00
\\$50.00	10	\$500.00
\\$20.00	10	\$200.00
\\$10.00	10	\$100.00
\\$5.00	10	\$50.00
\\$2.00	5	\$10.00
\\$1.00	20	\$20.00
\\$0.50	10	\$5.00
\\$0.25	40	\$10.00
\\$0.10	50	\$5.00
\\$0.05	100	\$5.00
\\$0.01	500	\$5.00
<b>TOTAL</b>		\$1,910.00

In this example, the End User's Digital Cash Wallet is used to purchase an item in a store that lists for \\$488.78.

Table 18 provides a possible withdrawal from the End User's Digital Cash Wallet. If the withdrawal is accepted by the Digital Cash Wallet's owner, the Digital Cash certificates ownership is changed to the stores.

Table 18: The Digital Cash from the wallet required to make the \\$488.78 purchase.

Denomination	Quantity	Sum
\\$100.00	4	\$400.00
\\$50.00	1	\$50.00
\\$20.00	1	\$20.00
\\$10.00	1	\$10.00
\\$5.00	1	\$5.00
\\$2.00	0	\$0.00
\\$1.00	3	\$3.00
\\$0.50	1	\$0.50
\\$0.25	1	\$0.25
\\$0.10	0	\$0.00
\\$0.05	0	\$0.00
\\$0.01	3	\$0.03
<b>TOTAL</b>		\$488.78

**Note:** there are many ways the \\$488.78 could have been achieved using the Digital Cash Wallet provided in Table 16. This is one way. In an actual implementation, the contents of the composition of cash could be modified by the End User as long as it summed to the \\$488.78, just as would occur in a real wallet.

- Table 19 represents the contents of the Digital Cash Wallet of the End User after the transaction.

- Table 20 represents the contents of the Digital Cash Till of the store after the transaction.

Table 19: Example of a Digital Cash Wallet and its contents for an End User after transaction.

Denomination	Quantity	Sum
\\$100.00	5	\$100.00
\\$50.00	15	\$700.00
\\$20.00	6	\$100.00
\\$10.00	9	\$80.00
\\$5.00	3	\$10.00
\\$2.00	0	\$0.00
\\$1.00	10	\$7.00
\\$0.50	4	\$1.50
\\$0.25	8	\$1.75
\\$0.10	4	\$0.40
\\$0.05	5	\$0.25
\\$0.01	7	\$0.04
<b>TOTAL</b>		\$1,000.94

Table 20: Example of a Digital Cash Wallet and its contents for a store after transaction.

Denomination	Quantity	Sum
\\$100.00	14	\$1,400.00
\\$50.00	11	\$550.00
\\$20.00	11	\$220.00
\\$10.00	11	\$110.00
\\$5.00	11	\$55.00
\\$2.00	5	\$10.00
\\$1.00	23	\$23.00
\\$0.50	11	\$5.50
\\$0.25	41	\$10.25
\\$0.10	50	\$5.00
\\$0.05	100	\$5.00
\\$0.01	503	\$5.03
<b>TOTAL</b>		\$2,398.78

## Example

[Return to Top](#)

There are three categories of requirements alluded to in the [White Paper](#) and identified within the [Object Management Group White Paper Analysis](#):

- **Digital Cash Model** - these are requirements with CBDC characteristics most closely aligned with the simple coin cash model
- **Digital Account Model** - these are requirements with CBDC characteristics most closely aligned with the [Digital Account Model](#) (i.e, savings, checking, investment, direct pay, credit, debit cards, etc. )
- **Research Areas** - these are requirements with CBDC characteristics most closely aligned as “research” models such as [Stablecoins](#)

In this discussion, only the desirements were identified during the [White Paper Analysis](#) are considered. Table 21 represents the allocated of requirements germane to the Digital Cash Model.

Table 21: Mapping a subset of Digital Cash Model requirements identified within the White Paper Analysis conducted by the OMG

Category	Desirements
<b>Benefits</b>	B0003, B0004, B0007, B0009, B0013, B0018, B0020, B0022-1, B0022-2, B0022-3, B0024, B0028, B0029, B0034, B0036, B0040, B0042
<b>Policies and Considerations</b>	P0004, P0027, P0029
<b>Risks</b>	R0013
<b>Design</b>	D0001, D0006, D0007, D0009

Category	Desirements
<b>B</b> = <a href="#">Benefit Considerations</a>	
<b>P</b> = <a href="#">Policy Considerations</a>	
<b>R</b> = <a href="#">Risk Considerations</a>	
<b>D</b> = <a href="#">Design Considerations</a>	

## Example Discussion

[Return to Top](#)

Table 22 provides a summary of using a [Digital Dollar Model](#) instead of a Digital Account, Cryptocurrency or Stablecoin Models.

Table 22: Example of mapping a subset of requirements identified in the White Paper Analysis conducted by the OMG.

Desirement No.	Desirement Text	Comment
<b>B0003, P0003</b>	<b>Complement, rather than replace, current forms of money and methods for providing financial services</b>	The Digital Coins are intended to work in parallel with existing systems and to follow much the same lifecycle as current paper money. The same institutions would fulfill the same roles they currently do but have added roles and responsibilities for Digital Currency.
<b>B0004, P0004, D0012</b>	<b>Protect consumer privacy</b>	Since the journal is kept with each individual Digital Currency rather than on a globally accessible ledger (i.e., journal) then the consumers' privacy is more obfuscated. It becomes more like paper money.
<b>B0005, P0005</b>	<b>Protect against criminal activity</b>	Once criminal activity is detected, the Digital Dollars collected as part of the investigation can provide invaluable information for the prosecutors as to the origins of the money.
<b>B0009</b>	<b>Provide faster and cheaper payments (including cross-border payments)</b>	Digital Coins can be sent using normal encrypted electronic transfer for files.
<b>B0013</b>	<b>Provide immediate access to transferred funds</b>	Once the Digital Coins are transferred to a payee, the money can be spent exactly like cash
<b>B0030</b>	<b>Support benefit payments directly to citizens</b>	Not only can the payments be made directly to the citizens, but the payments may be colored by category: rent, medicine, food, communication, etc.

<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>B0040</b>	<b>Provide micropayment support</b>	Micropayments are financial transactions involving very small amounts of money and usually occur online. A number of micropayment systems were proposed and developed in the mid-to-late 1990s, all of which were ultimately unsuccessful. <sup>32)</sup> The smallest amount of money that can be paid as a micropayment must be more than the cost of obtaining Consensus (See the <a href="#">OMG DIDO-RA discussion on Consensus</a> )
<b>B0046</b>	<b>Enable rapid and cost-effective delivery of:</b> <b>1. wages,</b> <b>2. tax refunds</b> <b>3. other federal payments</b>	Digital Coins would be immediately available.
<b>R0001</b>	<b>Risk of affecting financial-sector market structure</b>	Since the Digital Coins would follow the existing Currency Lifecycle and the major financial institutions will have the same roles as they currently have, there should be minimal disruption to the existing financial structure
<b>R0010</b>	<b>CBDC has a Risk of significant energy footprint similar to Cryptocurrencies</b>	The use of Digital Coins does not require the costly <a href="#">Consensus Algorithms</a> , the energy cost should be insignificant.
<b>D0001</b>	<b>Design should be for a non-interest-bearing CBDC, for example, would be less attractive as a substitute for commercial bank money</b>	<a href="#">Digital Dollars</a> would be for all intents and purposes be the same as current paper money. It does not accumulate interest until it is deposited in a financial institution.

<sup>30)</sup>

99% (if not all) issued Initial Coin Offering (ICO) tokens on top of the Ethereum implements the ERC-20 standard.

[https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b\\_stds:defact:ethereum:eip:erc\\_0020](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:defact:ethereum:eip:erc_0020)

<sup>31)</sup>

The Federal Reserve Board currently issues \\$1, \\$2, \\$5, \\$10, \\$20, \\$50, and \\$100 notes. The largest denomination Federal Reserve note ever issued for public circulation was the \\$10,000 note. On July 14, 1969, the Federal Reserve and the Department of the Treasury announced that banknotes in denominations of \\$500, \\$1,000, \\$5,000, and \\$10,000 would be discontinued due to lack of use. Although they were issued in 1969, they were last printed in 1945.

[https://www.federalreserve.gov/faqs/currency\\_12600.htm](https://www.federalreserve.gov/faqs/currency_12600.htm)

<sup>32)</sup>

[Micropayment](https://en.wikipedia.org/wiki/Micropayment), Wikipedia, Accessed: 16 March 2022, <https://en.wikipedia.org/wiki/Micropayment>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc\\_omg:04\\_doc:15\\_common:08\\_currency\\_models:10\\_cash:start](https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:04_doc:15_common:08_currency_models:10_cash:start)

Last update: **2022/05/18 22:02**





## 4.2.2 Digital Account Model

[Return to Currency Models](#) [Provide Feedback](#)

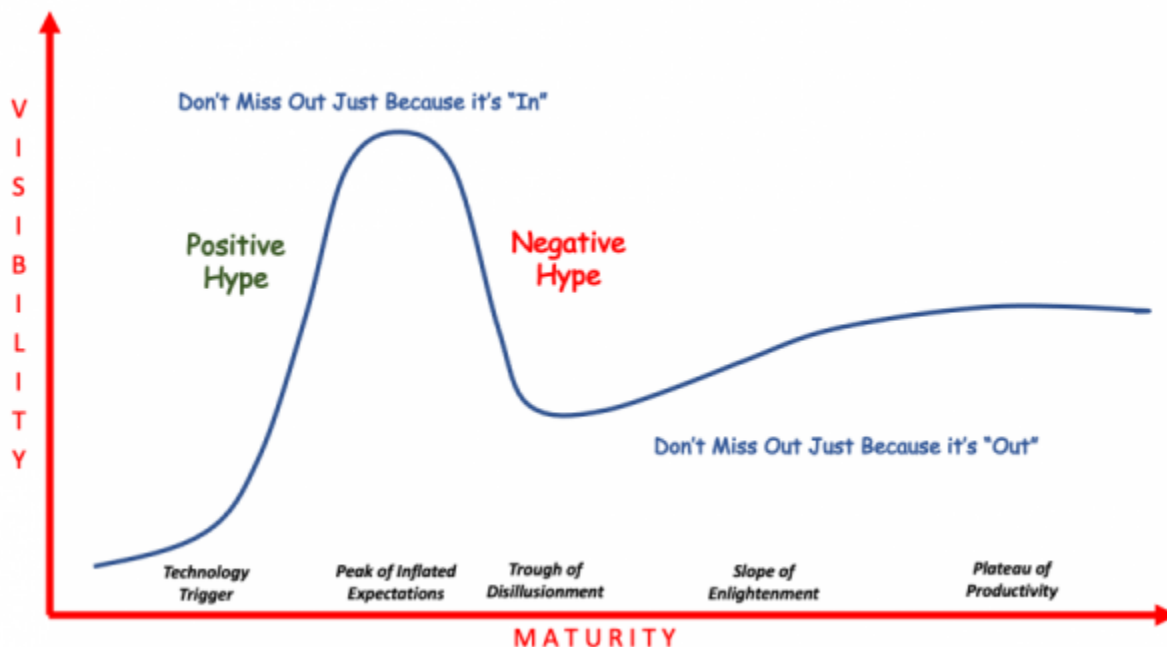
### Overview

[Return to Top](#)

Almost all Cryptocurrencies implemented so far use the concept of tokens, accounts, wallets, transactions, and distributed ledgers. In essence, these approaches use a model of the way money is handled in bank accounts<sup>33)</sup>. Underlying these Cryptocurrencies is the concept of [Coins](#). As a general rule, the Coin's value fluctuates and can be quite volatile:

- As with most commodities, assets, investments, or other products, cryptocurrency's price depends heavily on supply and demand
- As an asset, it can be adopted quickly by investors, traders, and speculators and is often based on emotion rather than underlying value. This contributes to price movements and plays a critical part in a cryptocurrency's value at any given moment. In other words, the cryptocurrency value is fickle
- Contributing to the cryptocurrency value are opinions put forth by media outlets, influencers, opinionated industry moguls, and well-known cryptocurrency fans fueling investor demands and concerns, further contributing to price fluctuations

Typically, these coins' values can be defined by the Gartner Group's Hype curve (See [OMG's DIDO-RA problem statement](#)).



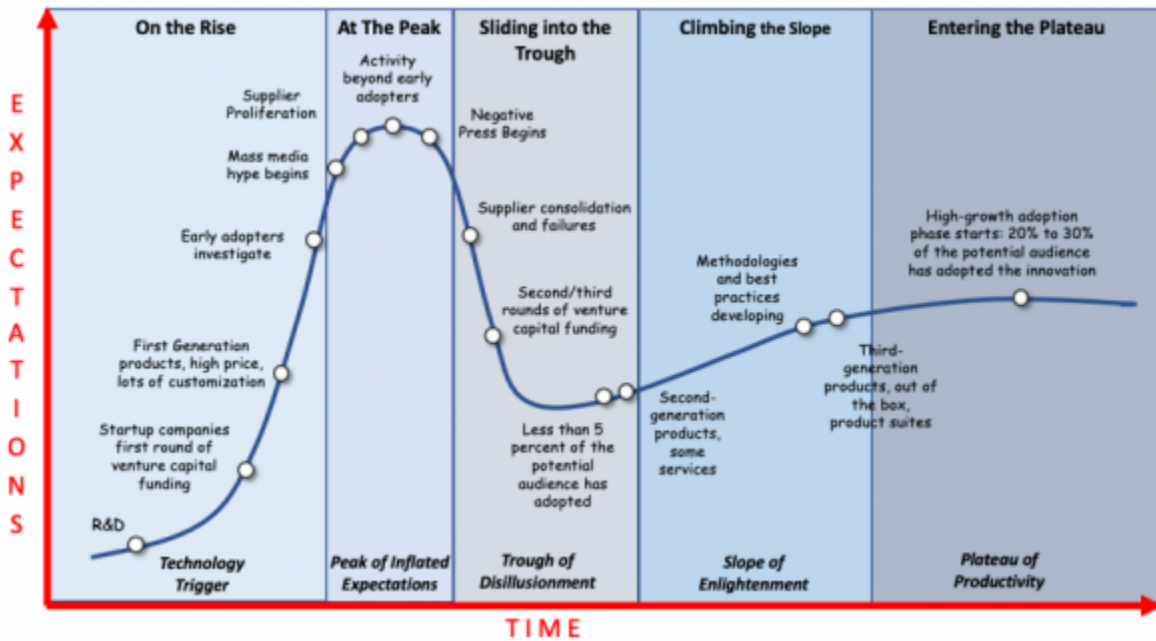


Figure 5: Gartner Group Hype Cycle

For many cryptocurrencies, the hype curve is not considered much of an issue since the life expectancy for cryptocurrencies is in the order of decades at best, while the life expectancy of CBDC needs to be much, much longer.

Obviously, the Federal Reserve does not want CBDC to follow the hype cycle. That is why it is important for the Federal Reserve to move slowly and with a well-thought-out plan for CBDC.

One method proposed to avoid this volatility is the use of [Stablecoins](#) instead of traditional cryptocurrencies like Bitcoin, Ethereum, Ripple, etc. (See the [OMG DIDO-RA discussion on Consensus Platforms](#) for a more detailed list).

## Digital Account Theoretical User Scenario

[Return to Top](#)

**Note:** The following Digital Account Theoretical User Scenario is only provided for discussion purposes. Actual User Scenarios would be developed during systems analysis and modeled using a Model-Based Systems Engineering (MBSE) approach and address the problem in far more detail with a team of experts.

In the following example, the CBDC is modeled as a Digital account, each account representing an End User. The End Users would actually “own” a wallet that contains account information where money is recorded as a balance that can be added to or subtracted from. For example, a retail purchase would deduct the amount of the purchase from the customer End User's account and add it to the Store's account.

Figure 6 represents a stylized use of a Digital Account flow.

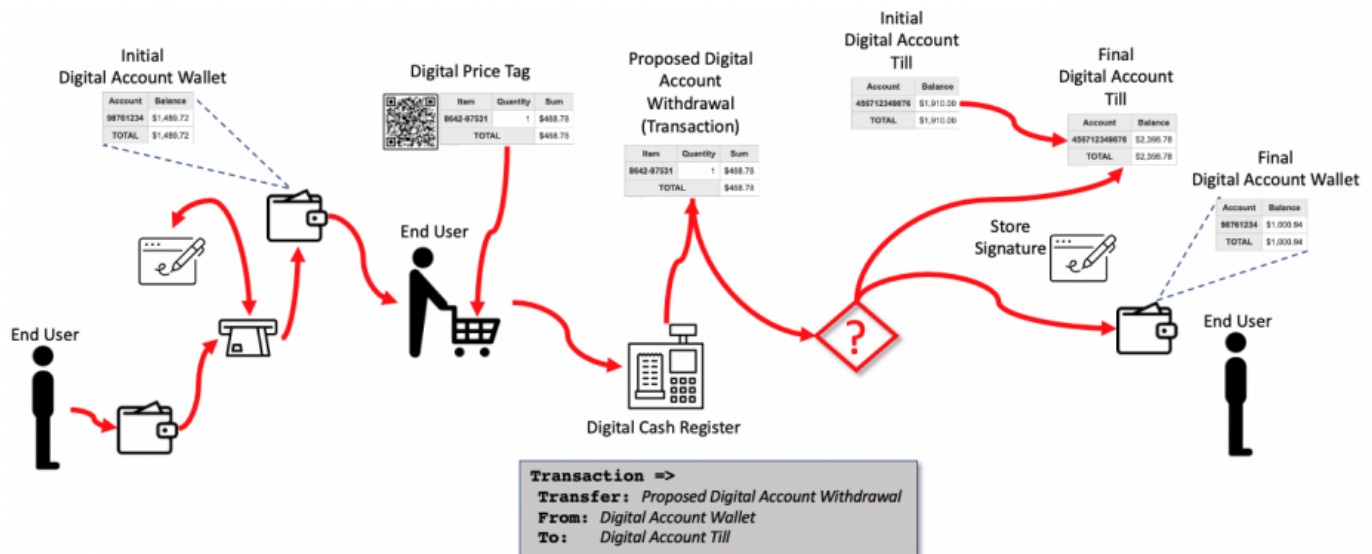


Figure 6: Simplified Digital Account Flow

- Table 23 represents the initial contents of a Digital Account Wallet of an End User. Each Digital Account Certificate in the wallet, such as the \$1,489.72 balance, is signed by the owner of the Digital Account Wallet.
- Table 24 represents the initial contents of at Digital Account Till at a store. Each Digital Account Certificate, such as the \$1,910.00 balance, is signed by the store that owns the Digital Account Till.

Table 23: Example of the initial contents of an End User Digital Account Wallet.

Account	Balance
98761234	\$1,489.72
<b>TOTAL</b>	\$1,489.72

Table 24: Example of the initial contents of a store's Digital Account Till.

Account	Balance
456712349876	\$1,910.00
<b>TOTAL</b>	\$1,910.00

In this example, the End User's Digital Account Wallet is used to purchase an item in a store that lists for \$488.78.

Table 25 provides a possible withdrawal from the End User's Digital Account Wallet. If the withdrawal is accepted by the Digital Account Wallet's owner, the Digital Account certificates ownership is changed to the stores.

Table 25: The Digital Account from the wallet required to make the \$488.78 purchase.

Item	Quantity	Sum
8642-97531	1	\$488.78
<b>TOTAL</b>		\$488.78

**Note:** there are many ways the \$488.78 could have been achieved using the Digital Account Wallet provided in Table 23. This is one way. In an actual implementation, the contents of the composition of cash could be modified by the End User as long as it summed to \$488.78, just as would occur in a real wallet.

- Table 26 represents the contents of the Digital Account Wallet of the End User after the

transaction.

- Table 27 represents the contents of the Digital Account Till of the store after the transaction.

Table 26: Example of a Digital Account Wallet and its contents for an End User after transaction.

Account	Balance
98761234	\$1,000.94
<b>TOTAL</b>	\$1,000.94

Table 27: Example of a Digital Account Wallet and its contents for a store after transaction.

Account	Balance
456712349876	\$2,398.78
<b>TOTAL</b>	\$2,398.78

## Examples

[Return to Top](#)

There are three categories of “desirements” alluded to in the [White Paper](#) and identified within the [Object Management Group White Paper Analysis](#):

- **Digital Cash Model** - these are “desirements” with CBDC characteristics most closely aligned with the simple coin cash model
- **Digital Account Model** - these are “desirements” with CBDC characteristics most closely aligned with the [Digital Account Model](#) (i.e, savings, checking, investment, direct pay, credit, debit cards, etc. )
- **Research Areas** - these are “desirements” with CBDC characteristics most closely aligned with “research” models such as [Stablecoins](#)

In this discussion, only the “desirements” identified during the [White Paper Analysis](#) are considered. Table 28 represents the allocation of “desirements” germane to the Digital Account Model.

Table 28: Example of mapping a subset of “desirements” identified during the White Paper Analysis conducted by the OMG

Topic	Desirements
<b>Digital Account Model</b>	B: B0005, B0010, B0022-4, B0038, B0047, B0048, B0049, B0051, B0054 P: P0002, P0012, P0013, P0017, P0018, P0019, P0020, P0021, P0023, P0024, P0025, P0017, P0028, P0030 R: R0002, R0009, R0012, R0015, R0020, R0023 D: D0001, D0002, D0003, D0005, D0008, D0010, D0012, D0013,
<b>B</b>	<a href="#">Benefit Considerations</a>
<b>P</b>	<a href="#">Policy Considerations</a>
<b>R</b>	<a href="#">Risk Considerations</a>
<b>D</b>	<a href="#">Design Considerations</a>

## Discussion of Examples

[Return to Top](#)

Table 29 provides a summary of using a [Digital Account Model](#) instead of a Digital Cash or Stablecoin Models. Many of the OMG identified “desirements” found in the [Money, and Payments: The U.S. Dollar in](#)

the [Age of Digital Transformation White Paper](#) during the [White Paper Analysis](#) appear to be appropriate for a CBDC “**Account Model**”. The “**Account Model**” uses Digital Money in an analogous model as Accounts for CBDC. For example, the “desirements” **B0005**, which is a requirement to “*Protect against criminal activity* | *In this context, criminal activity is either Money Laundering or Fraud. Fraud is an intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim. Types of fraud include tax fraud, credit card fraud, wire fraud, securities fraud, and bankruptcy fraud. Fraudulent activity can be carried out by one individual, multiple individuals, or a business firm as a whole*”, is easily associated with **Accounts**.

Table 29: List of “desirements” (i.e., desirements) identified in the **White Paper** indicating a **Account Model**.

Requirement	Statement	Comment
<b>B0005</b>	<b>Protect against criminal activity</b>	In this context, criminal activity is either Money Laundering or Fraud. Fraud is an intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim. Types of fraud include tax fraud, credit card fraud, wire fraud, securities fraud, and bankruptcy fraud. Fraudulent activity can be carried out by one individual, multiple individuals, or a business firm as a whole.
<b>B0010</b>	<b>Expand consumer access to the financial system</b>	A financial system is the entire set of non-cash-based institutions (i.e., banks, thrifts, insurance companies, stock exchanges, etc.) permitting and facilitating the exchange of funds. The expansion would entail adding people to these institutions
<b>B0022</b>	<b>Provide a CBDC that is:</b> 1. NOT <b>Privacy-Protected</b> 2. <b>Intermediated</b> 3. NOT <b>Widely Transferable</b> 4. <b>Identity-Verified</b>	<i>Intermediated</i> generally implies accounts or digital wallets. <i>Identity-Verified</i> generally implies validating and verifying a person's identity to gain access to their accounts
<b>B0038</b>	<b>Allow private-sector innovators to focus on:</b> 1. <b>new access services</b> 2. <b>distribution methods</b> 3. <b>related service offerings</b>	These innovations would predominately be account-based.
<b>B0047</b>	<b>Lower transaction costs</b>	Normally, there are no transaction costs for using cash
<b>B0048</b>	<b>Provide a secure way for people to save</b>	People save money in accounts unless we are offering piggy banks
<b>B0049</b>	<b>Promote access to credit</b>	Credit is, by definition, using cash you do not have access to.

<b>Requirement</b>	<b>Statement</b>	<b>Comment</b>
<b>B0051</b>	<b>Generate data about users' financial transactions similar to the current Commercial Bank<sup>34)</sup> and Nonbank Money</b>	This kind of data is collected on the activity in accounts.
<b>B0054</b>	<b>Attract risk-averse users to CBDC</b>	Risk Adverse investments usually pay little to no incentive to investors, but their value remains constant. Cash represents that kind of investment
<b>P0002</b>	<b>Provide Yield benefits more effectively than alternative methods</b>	Cash generally offers no yield, therefore, this would require accounts
<b>P0005</b>	<b>Protect against criminal activity</b>	See: <b>B0005</b>
<b>P0012</b>	<b>The firms that operate interbank payment services are subject to federal supervision</b>	These services typically use accounts to move payments unless it is referring to armored guards and vehicles
<b>P0013</b>	<b>Systemically important payment firms are subject to</b> <b>1. heightened supervision</b> <b>2. regulation</b>	Refers to the accounting practices used by the payment firms
<b>P0017</b>	<b>The PWG report recommends CBDC complement existing authorities regarding:</b> <b>1. market integrity</b> <b>2. investor protection</b> <b>3. illicit finance</b>	Refers to the accounting practices for CBDC accounts
<b>P0018</b>	<b>The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals</b>	Refers to accounts
<b>P0019</b>	<b>Federal Reserve accounts for individuals represent a significant expansion of the Federal Reserve's role in the financial system and the economy</b>	Refers to accounts
<b>P0020</b>	<b>The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments</b>	Refers to accounts
<b>P0021</b>	<b>The intermediaries would operate in an open market for CBDC services</b>	Refers to accounts
<b>P0023</b>	<b>CBDC would need to be readily transferable between customers of different intermediaries</b>	Intermediaries imply accounts
<b>P0024</b>	<b>CBDC would need to comply with the U.S. robust rules</b>	Implies accounting and oversight rules
<b>P0025</b>	<b>CBDC intermediary would need to verify the identity of a person accessing CBDC</b>	Intermediaries imply accounts
<b>P0027</b>	<b>CBDC a risk-free asset</b>	See: <b>B0054</b>

Requirement	Statement	Comment
P0028	<p><b>Require significant international coordination to address issues such as:</b></p> <ol style="list-style-type: none"> <li><b>1. common standards</b></li> <li><b>2. infrastructure,</b></li> <li><b>3. the types of intermediaries able to access any new infrastructure,</b></li> <li><b>4. legal frameworks</b></li> <li><b>5. preventing illicit transactions</b></li> <li><b>6. the cost and timing of implementation</b></li> </ol>	
P0030	<p><b>The Federal Reserve will only take further steps toward developing a CBDC if:</b></p> <ol style="list-style-type: none"> <li><b>1. Research points to benefits for households, businesses, and the economy overall that exceed the downside risks</b></li> <li><b>2. Indicates that CBDC is superior to alternative methods</b></li> </ol>	See: B0054
R0002	<b>Risk to the cost and availability of credit</b>	See: B0054
R0009	<b>Increased Risk of “runs” or other instabilities to the financial system</b>	
R0012	<p><b>Risk of increased concern related to the potential for:</b></p> <ol style="list-style-type: none"> <li><b>1. destabilizing “runs”</b></li> <li><b>2. disruptions in the payment system</b></li> <li><b>3. concentration of economic power</b></li> </ol>	See: B0054
R0013	<b>CBDC offers no associated credit or liquidity Risk</b>	See: B0054
R0015	<b>Require mechanisms to reduce liquidity Risk</b>	See: B0054
R0016	<b>Require mechanisms to reduce credit Risk</b>	See: B0054
R0020	<b>Risk that interest-bearing CBDC could result in a shift away from other low-risk assets, such as shares in money market mutual funds, Treasury bills, and other short-term instruments.</b>	See: B0054
R0023	<b>Risk of financial panic causing outflows from Commercial Banks to CBDC without prudential supervision, government deposit insurance, and access to central bank liquidity</b>	See: B0054
D0001	<b>Design should be for a non-interest-bearing CBDC, for example, would be less attractive as a substitute for commercial bank money</b>	Commercial bank money implies accounts
D0002	<b>Design should allow the central bank to limit the amount of CBDC an End-User could hold</b>	These restrictions imply accounts
D0003	<b>Design should allow a limit on the amount of CBDC an End-User could accumulate over short periods</b>	These restrictions imply accounts
D0005	<b>Design could affect monetary policy implementation and interest rate control by altering the supply of reserves in the banking system</b>	These restrictions imply accounts

Requirement	Statement	Comment
D0008	<b>Design should allow for interest-bearing at levels of the CBDC to be controlled independently of other safe assets</b>	These restrictions imply accounts
D0010	<b>Design should consider the potential for interest-bearing CBDC as a new policy tool on the channels of influence in monetary policy</b>	These restrictions imply accounts
D0011	<b>Design should generate data about users' financial transactions in the same ways that commercial bank and nonbank money generates data today</b>	These restrictions imply accounts
D0012	<b>Design should address privacy concerns by leveraging existing tools already in use by intermediaries</b>	These restrictions imply accounts
D0013	<b>Design should facilitate compliance with a robust set of rules already intended to combat</b> <b>1. money laundering</b> <b>2. the financing of terrorism</b> <b>3. customer due diligence</b> <b>4. record-keeping</b> <b>5. reporting requirements</b>	These restrictions imply accounts

33)

99% (if not all) issued Initial Coin Offering (ICO) tokens on top of the Ethereum implements the ERC-20 standard.

[https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b\\_stds:defact:ethereum:eip:erc\\_0020](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:defact:ethereum:eip:erc_0020)

34)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**.

From:

<https://www.omgwiki.org/CBDC/> - OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:15\\_common:08\\_currency\\_models:15\\_accounts:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:15_common:08_currency_models:15_accounts:start)

Last update: 2022/05/18 22:04





## 4.3 Stablecoins

[Return to Common Elements](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

**Stablecoins** is a category of cryptocurrencies attempting to control price volatility and achieve price stability by linking the value of the **Coins** offered by the cryptocurrency to an external asset.

- **Stablecoins** are cryptocurrencies that attempt to peg their market value to some external reference.
- **Stablecoins** may be pegged to a currency like the U.S. dollar or to a commodity's price, such as gold.
- **Stablecoins** achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

CB Insights defines four types of Stablecoins as depicted in Figure 7<sup>35)</sup>.



Figure 7: CB Insights defines four classes of Stablecoins<sup>36)</sup>

CB Insights defines the four classes of Stablecoins as follows<sup>37)</sup>:

- **Fiat-Collateralized Stablecoins** are the most common type of Stablecoins that are collateralized, or backed, by a fiat currency and are generally backed at a 1:1 ratio, meaning 1 Stablecoin is equal to 1 unit of currency. So for each Stablecoin that exists, there is (theoretically) one real fiat currency being held in a bank account to back it up.
- **Commodity-Collateralized Stablecoins** are backed by other kinds of interchangeable assets. The most common commodity to be collateralized is gold. However, there are also Stablecoins backed by oil, real estate, and various precious metals. Holders of commodity-backed Stablecoins are essentially exposed to the value of a real-world asset.
- **Crypto-Collateralized Stablecoins** are Stablecoins backed by a “basket” of other

cryptocurrencies. In theory, allowing crypto-backed Stablecoins to be more decentralized than their fiat-backed counterparts since everything is conducted using blockchain technology. To reduce price volatility risks, these Stablecoins are often over-collateralized to help absorb price fluctuations in the collateral.

- **Non-Collateralized Stablecoins** are not backed by anything tangible. An example is the US Dollar, which decades ago was backed by gold. However, the US Dollars are still perfectly stable because people believe in their value. Generally, these types of coins use an algorithmically governed approach to control the Stablecoin supply.

## Global StableCoins (GSC)

[Return to Top](#)

The U.S. CBDC could be implemented using a [Stablecoin](#).

As with many financial services available over the internet, the technological infrastructure underlying Stablecoins are not restricted to a geographic region. When a Stablecoins becomes popular to man End Users in multiple jurisdictions, it may become a [Global StableCoin \(GSC\)](#). A major confronting GSC are the numerous National laws and regulations in the various jurisdictions. For more details, see the following sections:

- [U.S. National Privacy Considerations](#)
- [U.S. National Security Considerations](#)
- [International Considerations](#)

GSCs are not without their vulnerabilities. These have been elaborated by The Financial Stability Board<sup>38)</sup> in Table 30.

Table 30: Examples of vulnerabilities and related functions and activities in a [Global StableCoin \(GSC\)](#) arrangement (stylised presentation)<sup>39)</sup>

Type of Vulnerability	Main Determinants	Functions and Activities Primarily Concerned
<b>Financial exposures in the <a href="#">Global StableCoin (GSC)</a> arrangement, giving rise to market, liquidity and credit risks.</b>	<ol style="list-style-type: none"> <li>1. Choice, composition, and management of the GSC reserve assets</li> <li>2. Robustness of liquidity provision by GSC resellers/market makers</li> <li>3. The ability of actors in the GSC arrangement to employ leverage</li> </ol>	<ol style="list-style-type: none"> <li>1. Governing the GSC arrangement</li> <li>2. Issuing, creating, and destroying GSCs</li> <li>3. Managing reserve assets</li> <li>4. Exchanging, trading, reselling, and market making of stablecoins</li> </ol>

Type of Vulnerability	Main Determinants	Functions and Activities Primarily Concerned
<b>Weaknesses in the GSC infrastructure, giving rise to operational risk (including cyber risks) and risk of loss of data.</b>	<ol style="list-style-type: none"> <li>1. Reliability and resilience of the GSC's ledger and validation mechanism, including validator nodes</li> <li>2. The capacity of the network to validate and process large volumes of transactions</li> </ol>	<ol style="list-style-type: none"> <li>1. Reliability of custodians/trustees</li> <li>2. Governing the GSC arrangement</li> <li>3. Operating the infrastructure</li> <li>4. Validating transactions</li> <li>5. Providing custody/trust services for reserve assets</li> </ol>
<b>Weaknesses in those parts of the GSC arrangement on which users rely to store, exchange and trade GSCs, including operational or fraud risk</b>	<ol style="list-style-type: none"> <li>1. Effectiveness of governance in preventing fraud</li> <li>2. Operational resilience</li> <li>3. Clarity and robustness of claims that users have<sup>40)</sup></li> <li>4. Robustness of liquidity provision by GSC resellers/market-makers</li> </ol>	<ol style="list-style-type: none"> <li>1. Governing the GSC arrangement</li> <li>2. Storing of private keys providing access to GSCs</li> <li>3. Exchanging, trading, reselling, and market-making of GSCs</li> </ol>

The type of regulatory coverage of Stablecoin activities varies by jurisdiction.

*For example, in many jurisdictions AML/CFT regulations, seem to apply to Stablecoin activities generally. In a few jurisdictions, other types of financial regulation, such as market integrity, and investor and consumer protection regulations, also apply to Stablecoin activities like issuance, exchanging, and trading of Stablecoin. See the Table 31 on potential vulnerabilities arising from Stablecoin activities.<sup>41)</sup>*

Table 31: Examples of vulnerabilities, regulatory tools, and international standards by activity of a [Global StableCoin \(GSC\) arrangement](#)<sup>42)</sup>

Regulatory authorities and potential tools to address the vulnerabilities			
Activities	Vulnerabilities	Authority/Tool	Relevant international standard
<p><b>Establishing rules governing the Stablecoin arrangement</b></p>	<p>Fraud or conflict of interest of those governing the GSC arrangement                      Lack of contractual arrangements among the entities of the <a href="#">Global StableCoin (GSC)</a> arrangement                      Difficulties to tackle the uncertainty for users due to an unclear definition of roles and responsibilities within the GSC arrangement                      Inadequate governance framework                      Lack of clear central body to hold accountable</p>	<p>Ability to regulate and supervise the GSC arrangement in a holistic manner, e.g. through cooperation among authorities (akin to comprehensive consolidated supervision)                      Ability to require a GSC arrangement to be governed in a manner that facilitates effective regulation and supervision, including by prohibiting fully decentralized systems                      Governance, internal control, and risk management requirements applicable at the level of the entire GSC arrangement                      Power to wind down or resolve a GSC arrangement                      Governance requirements requiring a solid legal basis                      Cyber security and other operational resiliency safeguards                      AML/CFT and sanctions controls</p>	<p>The revised FATF Standards apply. Based on known models, developers and government bodies of centralized GSCs will, in general, have AML/CFT obligations as a financial institution (e.g., as a business involved in the ‘issuing and managing means of payment’) or a VASP (e.g. as a business involved in the ‘participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset’). They can then be held accountable for the implementation of AML/CFT controls across the arrangement and for taking steps to mitigate ML/TF risks (e.g. in the design of the so-called Stablecoin). This could include, for example, limiting the scope of customers’ ability to transact anonymously using the so-called Stablecoin and/or ensuring that AML/CFT obligations of AML/CFT-obliged intermediaries within the arrangement are fulfilled.                      For GSC arrangements set up entirely by banks, the Basel Framework and associated principles for supervision and colleges would provide a basis for overseeing the setup. <sup>43)</sup>                      For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on a legal basis, governance, and comprehensive management of risks. Responsibility E would provide a strong basis for cooperation among relevant authorities. See Annex 4 on CPMI-IOSCO preliminary analysis.                      For GSC arrangements where the token or the reserve qualifies as a security, relevant IOSCO Principles and Standards that cover governance arrangements would apply, depending on the structure. These would include relevant cooperation agreements (IOSCO Principles<sup>44)</sup> covering Cooperation in regulation (Principles 13 to 15), IOSCO’s Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information,<sup>45)</sup> the Enhanced Multilateral MoU Concerning Consultation and Cooperation and the Exchange of Information,<sup>46)</sup> IOSCO’s Principles on Cross-Border Supervisory Cooperation<sup>47)</sup> of May 2010, the cross-border regulatory cooperation aspect of the IOSCO 2015 Cross-Border Regulation Task Force Report<sup>48)</sup> and the work of the Follow-Up Group to address potential regulatory arbitrage).</p>

<b>Regulatory authorities and potential tools to address the vulnerabilities</b>			
<b>Activities</b>	<b>Vulnerabilities</b>	<b>Authority/Tool</b>	<b>Relevant international standard</b>
<b>Issuing, creating, and destroying stablecoins</b>	Inability to meet redemptions in stressed conditions For algorithmic arrangements, errors in the issuance or redemption algorithm that impact value	Adequate liquidity (risk) management Liquidity risk management tools (e.g. redemption gates) Certain own funds/liquidity requirements Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF standards apply to firms “issuing and managing means of payment” or to those who provide “participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset”. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and Principles for the sound management of operational risk. For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those related to frameworks for comprehensive risk management and settlement. See Annex 4 on CPMI-IOSCO preliminary analysis. Depending on the creation/redemption processes, the IOSCO Principles for the Regulation of Exchange Traded Funds (2013) <sup>49)</sup> could be relevant.
<b>Managing reserve assets</b>	A sharp fall in price and/or liquidity of reserve asset(s) Change in reserve allocation across reserve assets Lack of transparency in the composition of reserve Fraud or mismanagement of the reserve Investment in illiquid assets Significant increase in the price volatility of the reserve assets that cannot be or is not readily managed	Portfolio diversification rules and issuer limits rules Liquidity and other financial risk safeguards Liquidity risk management tools (e.g. redemption gates) Requirements on disclosure of the composition of the assets Disclosure of investment policies Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF standards apply to those who provide “safekeeping and administration of cash and liquid securities on behalf of other persons”, or “safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets”. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and Principles for the sound management of operational risk. Depending on its structure, the reserve may engage IOSCO Liquidity Risk Management Recommendations (2018), <sup>50)</sup> IOSCO Principles for the Regulation of Exchange Traded Funds or IOSCO Policy Recommendations for MMFs (2012). <sup>51)</sup> For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on custody and investment risks and transparency. See Annex 4 on CPMI-IOSCO preliminary analysis.

<b>Regulatory authorities and potential tools to address the vulnerabilities</b>			
<b>Activities</b>	<b>Vulnerabilities</b>	<b>Authority/Tool</b>	<b>Relevant international standard</b>
<b>Providing custody/trust for reserve assets</b>	Custodian failure, cross-border resolution, fraud Liquidity Lack of legal clarity regarding rights to reserve assets, particularly where legal regimes of different jurisdictions are implicated	Segregation requirements/rights for reserve assets Liquidity and other financial risk safeguards Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF standards apply to those who provide “safekeeping and administration of cash and liquid securities on behalf of other persons” or “safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets”. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and Principles for the sound management of operational risk. IOSCO Recommendations Regarding the Protection of Client Assets (2013). <sup>52)</sup> For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on custody and investment risks and transparency. See Annex 4 on CPMI-IOSCO preliminary analysis.
<b>Operating the infrastructure</b>	Disruption to the mechanism that links the value of the stablecoin and the value of its reserves, for example, a cyber incident Uncertainty on the revocability of the payments GSC ledger compromised due to design flaw, operational (e.g. cyber) incident	Liquidity and other financial risk safeguards Requirements on payments finality Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF Standards apply to GSC infrastructure if it satisfies the definition of a financial institution or a virtual asset service provider provided in the FATF glossary. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and Principles for the sound management of operational risk. For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, some of the most relevant principles regarding these vulnerabilities would be those on a framework for the comprehensive management of risks and settlement. See Annex 4 on CPMI-IOSCO preliminary analysis.



<b>Regulatory authorities and potential tools to address the vulnerabilities</b>			
<b>Activities</b>	<b>Vulnerabilities</b>	<b>Authority/Tool</b>	<b>Relevant international standard</b>
<b>Validating transactions</b>	GSC ledger compromised due to failure of multiple validator nodes	Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	Depending on the functions they perform, the validator nodes that validate the underlying distributed ledger technology may be VASPs or financial institutions. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and Principles for the sound management of operational risk. For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, some of the most relevant principles regarding this vulnerability would be on operational risk and settlement. See Annex 4 on CPMI-IOSCO preliminary analysis.
<b>Storing the private keys providing access to Stablecoins (wallets)</b>	Disruption of a wallet, for example, theft of coins from a digital wallet or operational (e.g. cyber) incident. Direct loss, including by consumers	Liquidity and other financial risk safeguards Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF Standards apply to all businesses providing custodial wallet services. The FATF Standards do not place explicit obligations on unhosted wallets. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and Principles for the sound management of operational risk. For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. On the basis of a preliminary analysis, a relevant principle regarding these vulnerabilities would be an operational risk. See Annex 4 on CPMI-IOSCO preliminary analysis.
<b>Exchanging, trading, reselling and market making of stablecoins</b>	Withdrawal of liquidity provision by authorized resellers/market makers Disruption of a trading platform. Fraud, market manipulation, unauthorized transactions Cyber incident	Liquidity and other financial risk safeguards Settlement finality requirements Allocation of legal responsibility for unauthorized transactions Cyber security and other operational resiliency safeguards AML/CFT and sanctions controls	FATF Standards apply to all businesses carrying out trading/exchanging activity. The FATF Standards do not explicitly apply to peer-to-peer transactions without the use of a VASP or financial institution. For GSC arrangements involving banks, the prudential risks and operational resilience vulnerabilities would be subject to the Basel Framework and Principles for the sound management of operational risk. For GSC arrangements deemed to perform systemically important payment system functions or other FMI functions that are systemically important, the PFMI applies. See Annex 4 on CPMI-IOSCO preliminary analysis. Issues Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms (2020) <sup>53)</sup> , discussing IOSCO Principles <sup>54)</sup> , <sup>55)</sup> <sup>56)</sup> and associated IOSCO reports.

# Stablecoin Theoretical User Scenario

[Return to Top](#)

**Note:** The following Stablecoin Theoretical User Scenario is only provided for discussion purposes. Actual User Scenarios would be developed during systems analysis and modeled using a Model-Based Systems Engineering (MBSE) approach and address the problem in far more detail with a team of experts.

In the following example, the CBDC is modeled as Stablecoins, each account representing an End User. The End Users would actually “own” a wallet that contains account information, where Stablecoins are recorded as a balance that can be added to or subtracted from. For example, a retail purchase would deduct the amount of the purchase from the customer End User's account and add it to the Store's account.

Figure 8 represents a stylized use of a Stablecoin flow of a consumer (End User) buying a product from a retail store.

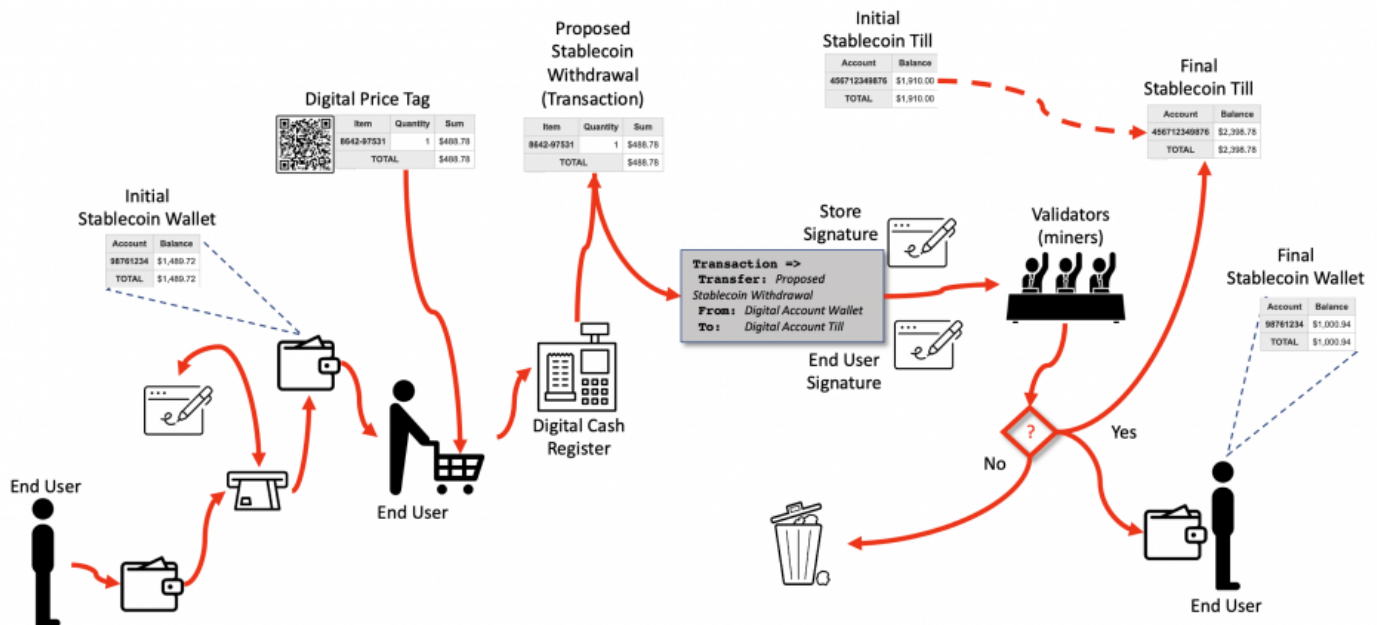


Figure 8:

- Table 23 represents the initial contents of a Stablecoins of an End User. Each Stablecoin balance in the wallet, such as the \ \$1,489.72 balance, is signed by the owner of the Stablecoin Wallet.
- Table 24 represents the initial contents of at Stablecoins Till at a store. Each Stablecoin, such as the \$1,910.00 balance, is signed by the store that owns the Stablecoin Till.

Table 32: Example of the initial contents of an End User Stablecoin Wallet.

Account	Balance
98761234	\$1,489.72
<b>TOTAL</b>	<b>\$1,489.72</b>

Table 33: Example of the initial contents of a store's Stablecoin Till.

Account	Balance
456712349876	\$1,910.00
<b>TOTAL</b>	<b>\$1,910.00</b>



In this example, the End User's Stablecoin Wallet is used to purchase an item in a store that lists for \ \$488.78.

Table 25 provides a possible withdrawal from the End User's Stablecoin Wallet. If the withdrawal is accepted by the Stablecoin Wallet's owner, the Stablecoin ownership is changed to the stores.

Table 34: The Stablecoin from the wallet required to make the \ \$488.78 purchase.

Item	Quantity	Sum
8642-97531	1	\$488.78
<b>TOTAL</b>		\$488.78

**Note:** there are many ways the \ \$488.78 could have been achieved using the Stablecoin Wallet provided in Table 32. This is one way. In an actual implementation, the contents of the composition of cash could be modified by the End User as long as it summed to \ \$488.78, just as would occur in a real wallet.

- Table 26 represents the contents of the Stablecoin Wallet of the End User after the transaction.
- Table 27 represents the contents of the Stablecoin Till of the store after the transaction.

Table 35: Example of a Stablecoin Wallet and its contents for an End User after transaction.

Account	Balance
98761234	\$1,000.94
<b>TOTAL</b>	\$1,000.94

Table 36: Example of a Stablecoin Wallet and its contents for a store after transaction.

Account	Balance
456712349876	\$2,398.78
<b>TOTAL</b>	\$2,398.78

## Examples

[Return to Top](#)

In this discussion, only the requirements were identified during the [White Paper Analysis](#) are considered. Table 37 represents the allocated of requirements germane to the Stablecoins.

Table 37: Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG

Area	Desirements
<b>Benefits</b>	B0016, B0017, B0021
<b>Policy and Considerations</b>	P0008, P0015, P0016
<b>Risks</b>	R0010, R0022

**Note:** **B** = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.

## Discussion of Examples

[Return to Top](#)Table 38: List of requirements (i.e., desirements) identified in the **White Paper** that require further research

<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>B0016</b>	<b>Provide Stablecoins that are:</b> <b>1. well-designed</b> <b>2. appropriately regulated</b>	Stablecoin is a specific solution
<b>B0017</b>	<b>Provide Stablecoins that are:</b> <b>1. faster</b> <b>2. more efficient</b> <b>3. more inclusive payment</b>	Stablecoin is a specific solution
<b>B0021</b>	<b>Maintain value by not using backing by an underlying asset</b>	<b>Conflict with B0017</b>
<b>P0015</b>	<b>The PWG report recommends that Congress act promptly to enact legislation that would ensure payment of stablecoins</b>	Stablecoin is a specific solution
<b>P0016</b>	<b>The PWG report recommends payment stablecoin arrangements are subject to a consistent and comprehensive federal regulatory framework</b>	Stablecoin is a specific solution
<b>R0010</b>	<b>CBDC has Risk of significant energy footprint similar to Cryptocurrencies</b>	This depends on the <a href="#">Consensus Algorithm</a> used for the Stablecoin.
<b>R0022</b>	<b>Risk of stablecoins and other types of nonbank money shifting deposits away from banks even without a CBDC</b>	Stablecoin is a specific solution
<b>B = <a href="#">Benefit Considerations</a></b>		
<b>P = <a href="#">Policy Considerations</a></b>		
<b>R = <a href="#">Risk Considerations</a></b>		
<b>D = <a href="#">Design Considerations</a></b>		

<sup>35)</sup> <sup>36)</sup> <sup>37)</sup>

CB Insights, [What Are Stablecoins?](#), 25 January 2022, Accessed: 20 March 2022,

<https://www.cbinsights.com/research/report/what-are-stablecoins/>

<sup>38)</sup> <sup>39)</sup> <sup>41)</sup>

The Financial Stability Board, [Regulation, Supervision, and Oversight of “Global Stablecoin” Arrangements Final Report and High-Level Recommendations](#), 13 October 2020, Accessed: 26 April 2022,

<https://www.fsb.org/wp-content/uploads/P131020-3.pdf>

<sup>40)</sup>

Including whether or not users have a right to redeem at par in fiat.

<sup>42)</sup>

The Financial Stability Board, [Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements Final Report and High-Level Recommendations](#), 13 October 2020, Accessed: 26 April 2022,

<https://www.fsb.org/wp-content/uploads/P131020-3.pdf>

<sup>43)</sup>

[Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information \(EMMoU\)](#), 2016, 2017, Accessed: 26 April 2022,

<https://www.iosco.org/about/?subsection=emmou>

<sup>44)</sup> <sup>55)</sup>

International Organization of Securities Commissions, Objectives and Principles of Securities Regulation, May 2017, Accessed: 26 April 2022, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD561.pdf>

45) 56)

International Organization of Securities Commissions, Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (MMoU), 2022, Accessed: 26 April 2022, <https://www.iosco.org/about/?subsection=mmou>

46)

International Organization of Securities Commissions, Enhanced Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (EMMoU), 2016, 2017, Accessed: 26 April 2022, <https://www.iosco.org/about/?subsection=emmou>

47)

Technical Committee of the International Organization of Securities Commissions, Principles Regarding Cross-Border Supervisory Cooperation, Final Report, May 2010, Accessed 26 April 2022, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD322.pdf>

48)

The Board of the International Organization of Securities Commissions, IOSCO Task Force on Cross-Border Regulation, Final Report, September 2015, Accessed: 26 April 2022, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD507.pdf>

49)

Board of the International Organization of Securities Commissions, Principles for the Regulation of Exchange Traded Funds Final Report, June 2013, Accessed: 26 April 2022, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD414.pdf>

50)

International Organization of Securities Commissions, IOSCO issues recommendations and good practices to improve liquidity risk management for investment funds, IOSCO/MR/02/2018, 1 February 2018, Accessed: 26 April 2022, <https://www.iosco.org/news/pdf/IOSCONEWS486.pdf>

51)

International Organization of Securities Commissions, IOSCO Consults on Money Market Fund Systemic Risk Analysis and Reform Options, OSCO/MR/07/2012, 27 April 2012, Accessed: 26 April 2022, <https://www.iosco.org/news/pdf/IOSCONEWS232.pdf>

52)

International Organization of Securities Commissions, IOSCO Publishes Recommendations Regarding the Protection of Client Assets, IOSCO/MR/03/2013, 8 February 2013, Accessed: 26 April 2022, <https://www.iosco.org/news/pdf/IOSCONEWS265.pdf>

53)

International Organization of Securities Commissions, IOSCO publishes key considerations for regulating crypto-asset trading platforms, IOSCO/MR/03/2020, 12 February 2020, Accessed: 26 April 2022, <https://www.iosco.org/news/pdf/IOSCONEWS556.pdf>

54)

Financcail Stability Board, Objectives and Principles of Securities Regulation, 31 May 2017, Accessed: 26 April 2022, [https://www.fsb.org/2017/05/cos\\_100601/](https://www.fsb.org/2017/05/cos_100601/)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:15\\_common:30\\_stablecoins:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:15_common:30_stablecoins:start)

Last update: **2022/05/18 22:05**



## 4.4 National Privacy Considerations

[Return to Common Elements](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

Although there is no general federal legislation for data and metadata protection and privacy, there are a number of federal data protection laws that are sector-specific or focus on particular types of data. In addition to the Federal regulations, there are some state laws that are also applicable.

Table 39 summarizes the number of U.S. Laws and Regulations covering Privacy Considerations. The total number (i.e., **16**) indicates the complexity of the Privacy that confronts the CBDC just within the U.S. The more Laws and Regulations, the more effort there is to coordinate the CBDC efforts and to work with the Legislative and Executive Branches to keep the Laws and Regulations current with CBDC efforts.

Table 39: Summary of the number of laws and regulations covering National Security Considerations.

U.S. Privacy Consideration	No. of Laws and Regulations
<a href="#">U.S. Federal Laws and Regulations</a>	10
<a href="#">U.S. State Laws and Regulations</a>	6
<b>Total</b>	<b>16</b>

### U.S. Federal Laws and Regulations

[Return to Top](#)

There is no single U.S. law or regulation covering **Privacy**, but a whole set of laws. Table 40 outlines most of the laws as determined by the [OMG DIDO-RA](#).

There are roughly 10 Laws and Regulations in the U.S. covering Privacy.

Table 40: List of Applicable U.S. Federal Laws.

U.S. Federal Laws		
Kind	Law / Regulation	Description
Privacy	<a href="#">Driver's Privacy Protection Act of 1994 (DPPA)</a>	DPPA governs the privacy and disclosure of personal information gathered by state Departments of Motor Vehicles, including photographs, Social Security Number (SSN), Driver Identification Number (DID), name, address (but not the five-digit ZIP code), telephone number, medical information and disability information.
Privacy	<a href="#">Video Privacy Protection Act (VPPA)</a>	VPPA restricts the disclosure of rental or sale records of videos or similar audio-visual materials, including online streaming.
Privacy	<a href="#">Cable Subscriber Protection</a>	Cable Subscriber Protection provides access to all <a href="#">Personal Identifiable Information (PII)</a> regarding the subscriber which is collected and maintained by a cable operator.

<b>U.S. Federal Laws</b>		
<b>Kind</b>	<b>Law / Regulation</b>	<b>Description</b>
<b>Privacy</b>	<b>Right to Financial Privacy Act of 1978 (RFPA)</b>	The RFPA was put in place to limit the government's ability to freely access nonpublic financial records. The RFPA defines financial institutions as any institution that engages in activities regarding banking, credit cards, and consumer finance. It also defines financial records as any documentation of a consumer's relationship with a financial institution.
<b>Privacy</b>	<b>Gramm-Leach-Bliley Act (GLBA)</b>	The GLBA promotes consumer privacy, the Gramm-Leach-Bliley Act included regulations to limit the ways in which companies handled and shared financial data.
<b>Privacy</b>	<b>Fair Credit Reporting Act (FCRA)</b>	The FCRA regulates credit agencies and promotes fair and secure handling of consumer information. The FCRA attempts to limit the dissemination of information through five main rules: 1. Credit reports and investigative reports must be differentiated so that any irrelevant data are not mixed 2. Reports can only be made available to those with "legitimate business needs" 3. The subject of a report must be notified of any request for their information 4. Agencies must give consumers access to their own files if they should ever request them 5. A time limit is set for the retention of information on reports. Information that is seven years or older must be deleted, while information regarding bankruptcies can be removed only after fourteen years
<b>Privacy</b>	<b>Fair and Accurate Credit Transactions Act (FACTA)</b>	FCRA amended the FCRA with stricter regulations that need to be enforced first. State laws regarding credit scores, credit reports, and insurance were to remain in effect as a result of the amendments. FCRA gave consumers more rights to explanations of their credit scores and the right to a free credit report each year. It also includes two rules: 1. Disposal Rule - how to dispose of consumer records 2. Red Flag Rule - how financial institutions identify and prevent identity thefts
<b>Privacy</b>	<b>Credit and Debit Card Receipt Clarification Act</b>	Credit and Debit Card Receipt Clarification Act requires account numbers printed on receipts have to be shortened to five digits in order to protect consumer privacy
<b>Privacy</b>	<b>Fair Debt Collection Practices Act (FDCPA)</b>	Under the FDCPA, collectors are not allowed to publish a consumer's name and address on a bad debt list or reveal any information regarding the debt to unaffiliated third parties except the consumer's partner or attorney.
<b>Privacy</b>	<b>Electronic Funds Transfer Act</b>	The act implemented requirements so that banks have to notify their customers of any policies regarding the electronic transfer of funds. Banks are also held liable in the event that information is disclosed through telephone without consent. Also, banks would be held responsible for any damages that came as a result of unauthorized access to a consumer's information.

## U.S. State Laws and Regulations

[Return to Top](#)

The U.S. States each can have their own laws or regulations covering **Privacy**, as well as, a whole set of laws. Table 41 outlines most of the U.S. State laws as determined by [OMG DIDO-RA](#) .

There are roughly 6 major U.S. State Laws and Regulations covering Privacy.

**Note:** FACTA ensured that any state laws with stricter regulations than those outlined in the FCRA would be enforced first. State laws regarding credit scores, credit reports, and insurance that were to remain in effect as a result of the amendments were outlined within the act.

Table 41: List of Applicable U.S. State Laws and Regulations.

State Laws		
Kind	Law / Regulation	Description
Privacy	<a href="#">California Privacy Act</a>	California Privacy Act is a state-level privacy act that provides protection of consumer information. The act is described as a stricter version of the Gramm-Leach-Bliley Act.
Privacy	<a href="#">California Consumer Privacy Act (CCPA)</a>	CCPA gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law.
Privacy	<a href="#">California Consumer Credit Reporting Agencies Act (CCCRA)</a>	The CCCRA regulates consumer credit reporting agencies as well as any users of credit reports. The act also provides a narrower definition of “consumer credit report” as any information that falls within credit reports is protected by the act.
Privacy	<a href="#">California Right to Financial Privacy Act</a>	California's Right to Financial Privacy Act regulates the state's government agencies' abilities to access nonpublic consumer information. As a result of the act, California's government agencies are not authorized to access financial records unless the consumer gives consent or if a subpoena or a search warrant is issued for the information.
Privacy	<a href="#">California Song-Beverly Credit Card Act</a>	Under the California Song-Beverly Credit Card Act, companies may not collect personally identifiable information from consumers who purchase goods or services using credit cards. Companies cannot set conditions in which consumers must consent to share their information in order to use their credit cards for a transaction. However, consumer information can be requested in order to complete a credit card transaction as long as the information is never recorded. The act also set a redundant state-level requirement that companies must shorten a consumer's credit and debit card information on receipts.
Privacy	<a href="#">Vermont Privacy of Consumer Financial and Health Information</a>	The law defines the purpose, scope, application, compliance, and exceptions to the law. The purpose of the Vermont Privacy of Consumer Financial and Health Information is to govern the treatment of nonpublic personal information about consumers by financial institutions.

## Exemplar for Metadata

[Return to Top](#)

The following user scenario is meant as an exemplar of the importance of Data Strategy and Data Governance for a U.S.-based CBDC.

### Theoretical Problem

[Return to Top](#)

The following is a theoretical problem used to highlight some major issues with privacy.

Two U.S. citizens go into a U.S. clinic: John Doe and Jane White.

- John Doe works in an assembly line
- Jane White is a Chief Executive Officer (CEO) and President of one of the largest, most valued innovative companies in the world

Both show up at a medical facility that treats mental health and substance abuse. The diagnosis and treatment for John and Jane are identical, with the same prognosis, and the outcomes are expected to be the same. On a personal level, this is a tragedy for both John and Jane, their families, and their friends.

Both John and Jane would like to keep their visit to the medical facility quiet. John has a better chance of keeping his visit secret, especially since there is no real economic incentive to divulge the secret. However, if it is known that Jane has visited this clinic, the collateral impact on her company, its employees, the investors, and even those investing in competing companies can be wide-reaching and significant.

Regardless, if the data and metadata are about John or Jane, there is a reasonable expectation by both of them that data and metadata about their transaction with the medical facility are secure and remain private.

### Theoretical Solution

[Return to Top](#)

A theoretical solution is for the CBDC to develop a rigorous and comprehensive Data Strategy that guarantees the security and privacy of the transactional data associated with the CBDC. The CBDC and the Federal Reserve do not need to develop their own Security and Privacy framework but can rely on the existing framework laid out by the U.S. Federal Government.

The [OMG DIDO Reference Architecture \(DIDO-RA\)](#) provides a discussion on what a **U.S. Federal Data Strategy** is.



## U.S. Federal Government on Data Strategy

[Return to Top](#)

The following is from the U.S. Federal Government on Data Strategy:

*The U.S. **Federal Data Strategy (FDS)** provides a common set of data principles and best practices. The 2020 Action Plan identifies milestones that are essential for establishing processes, building capacity, and aligning existing efforts. This initial plan builds a solid foundation that will support the implementation of the strategy over the next decade.*

<https://strategy.data.gov/progress/>

- Privacy refers to the control over a person's [Personal Identifiable Information\(PII\)](#) and how the information is used. PII is any information that can be used to determine a person's identity.
- Security refers to how protected a person's PII is from unauthorized or unintended use.

The DIDO-RA summarizes the areas required for a U.S. Federal Data Strategy covering the following areas:

### 1. Principles

- Ethical Governance
- Conscious Design
- Learning Culture

### 2. Practices

- Building a Culture that Values Data and Promotes Public Use
- Governing, Managing, and Protecting Data
- Promoting Efficient and Appropriate Data

### 3. Actions

- Agency Actions
- Community of Practice Actions
- Shared Solution Actions

## Examples

[Return to Top](#)

The “desirements” specified in [White Paper](#) and identified by the [OMG's White Paper Analysis](#) as **Privacy Issues** are listed in Table 42.

Table 42: Examples of **Privacy Desirements** identified during the White Paper Analysis conducted by

the OMG

Category	Desirements
Benefits	B0004, B0022
Policies and Considerations	P0004
Risks	R0014
Design	D0012

**Note:** **B** = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.

## Discussion of Examples

[Return to Top](#)

Table 43 provides discussion points for each of the “desirements” identified by the [OMG's White Paper Analysis](#).

Table 43: Privacy references of desirements in the **White Paper**

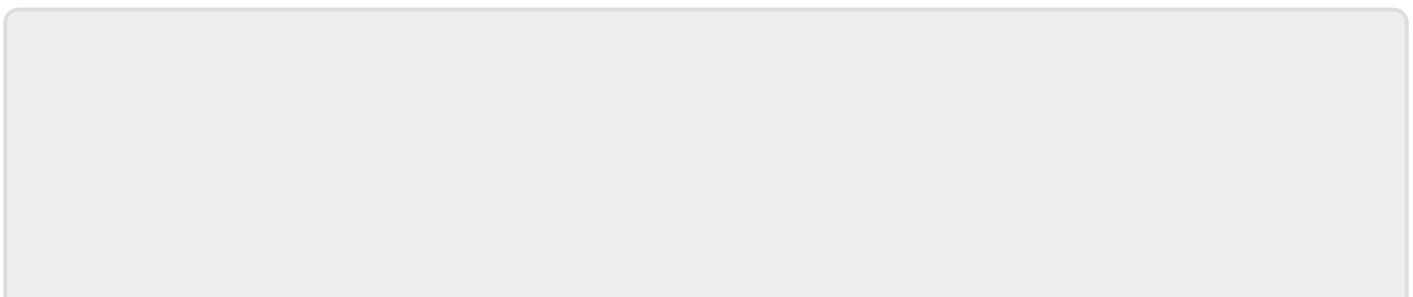
Desirement No.	Desirement Text	Comment
<b>B0004</b>	<b>Protect consumer privacy</b>	Consumer privacy is information privacy as it relates to the consumers of products and services. A variety of social, legal and political issues arise from the interaction of the public's potential expectation of privacy and the collection and dissemination of data by businesses or merchants
<b>B0022</b>	<b>Provide a CBDC that is:</b> <b>1. YES Privacy-Protected</b> <b>2. NO Intermediated</b> <b>3. NO Widely Transferable</b> <b>4. NO Identity-Verified</b>	Privacy-Protected means that the Central Bank Digital Currency (CBDC) protecting consumer privacy is critical. Any CBDC would need to strike an appropriate balance, however, between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity.
<b>P0004</b>	<b>Protect consumer privacy</b>	See <b>B0004</b> .
<b>R0014</b>	<b>Risk of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity</b>	1. See <b>B0004</b> for Consumer privacy. 2. Transparency is the ability to easily access and work with data no matter where they are located or what application created them, or the assurance that data being reported are accurate and are coming from the official source.
<b>D0012</b>	<b>Design should address privacy concerns by leveraging existing tools already in use by intermediaries</b>	Intermediaries means commercial banks and regulated <b>nonbank</b> financial service providers that would operate in an open market for CBDC services
<b>B</b> = <a href="#">Benefit Considerations</a>		
<b>P</b> = <a href="#">Policy Considerations</a>		

Desirement No.	Desirement Text	Comment
R = Risk Considerations		
D = Design Considerations		

**Note:** FACTA ensured that any state laws with stricter regulations than those outlined in the FCRA would be enforced first. State laws regarding credit scores, credit reports, and insurance that were to remain in effect as a result of the amendments were outlined within the act.

Table 44: List of Applicable U.S. State Laws and Regulations.

State Laws		
Kind	Law / Regulation	Description
Privacy	<b>California Privacy Act</b>	California Privacy Act is a state-level privacy act that provides protection of consumer information. The act is described as a stricter version of the Gramm-Leach-Bliley Act.
Privacy	<b>California Consumer Credit Reporting Agencies Act (CCCRA)</b>	The CCCRA regulates consumer credit reporting agencies as well as any users of credit reports. The act also provides a narrower definition of “consumer credit report” as any information that falls within credit reports is protected by the act.
Privacy	<b>California Right to Financial Privacy Act</b>	California's Right to Financial Privacy Act regulates the state's government agencies' abilities to access nonpublic consumer information. As a result of the act, California's government agencies are not authorized to access financial records unless the consumer gives consent or if a subpoena or a search warrant is issued for the information.
Privacy	<b>California Song-Beverly Credit Card Act</b>	Under the California Song-Beverly Credit Card Act, companies may not collect personally identifiable information from consumers who purchase goods or services using credit cards. Companies cannot set conditions in which consumers must consent to share their information in order to use their credit cards for a transaction. However, consumer information can be requested in order to complete a credit card transaction as long as the information is never recorded. The act also set a redundant state-level requirement that companies must shorten a consumer's credit and debit card information on receipts.
Privacy	<b>Vermont Privacy of Consumer Financial and Health Information</b>	The law defines the purpose, scope, application, compliance, and exceptions to the law. The purpose of the Vermont Privacy of Consumer Financial and Health Information is to govern the treatment of nonpublic personal information about consumers by financial institutions.



From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:45\\_privacy:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:45_privacy:start)

Last update: **2022/05/18 22:06**



## 4.5 National Security Considerations

[Return to Common Elements](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

**Note:** See the [OMG DIDO-RA Financial Laws, Regulations and Authorities](#) for more on Security.

The following Laws and Regulations governing Privacy, Money Laundering, Terrorism, and Financials apply in the U.S. and need to be part of any DIDO solution concerned with currency, money, financials, or cryptocurrencies. Often these Laws and Regulations are considered obstacles or barriers to innovation, but each law or regulation is developed in response to some situation that occurred in the past. To prevent a “modern” repeat of these situations, the laws and regulations should be upgraded, not ignored or overturned.

Some of these Laws, Regulations and Authorities have general applicability to DIDOs when the data stored within the DIDO refers to [Personal Identifiable Information \(PII\)](#) and therefore subject to the tenets of privacy. See [Right to Privacy](#)..

Some Laws, Regulations, and Authorities are relevant to DIDO when the DIDO is considered a [Financial Instrument](#) or a [Security](#). Certain [Cryptocurrencies](#) and [Initial Coin Offerings \(ICOs\)](#) may be found to meet the definition of an “investment contract” under the [Howey Test](#) from which the U.S. Supreme Court ruling determined that an Investment Contract must:

1. Have an investment of money
2. Enter into a common enterprise
3. Have the expectation of profit
4. Be derived from the efforts of others

### Details of National Security Considerations

[Return to Top](#)

Table 45 summarizes the number of Laws and Regulations covering National Security Considerations. The total number (i.e., **44**) indicates the complexity of National Security issues that confront the CBDC. The more Laws and Regulations, the more effort to coordinate the CBDC efforts and work with the Legislative and Executive Branches to keep the Laws and Regulations current with CBDC efforts.

Table 45: Summary of the number of laws and regulations covering National Security Considerations.

National Security Consideration	No. of Laws and Regulations
<a href="#">Human Trafficking</a>	14
<a href="#">Drug Trafficking</a>	9

National Security Consideration	No. of Laws and Regulations
<a href="#">Corruption</a>	10
<a href="#">Money Laundering</a>	11
<b>Total</b>	<b>44</b>

National Security Considerations are concerned with: Human Trafficking, Drug Trafficking, Corruption and Money Laundering. These are discussed in more detail in the following subsections:

- [4.5.1 Human Trafficking](#)
- [4.5.2 Drug Trafficking](#)
- [4.5.3 Corruption](#)
- [4.5.4 Money Laundering](#)

## Examples

[Return to Top](#)

Table 46: Examples of **security** Desirements identified during the White Paper Analysis conducted by the OMG

Category	Desirements
<b>Benefits</b>	B0005, B0052, B0053
<b>Policies and Considerations</b>	P0005, P0024, P0028
<b>Risks</b>	
<b>Design</b>	D0013, D0016, D0017

**Note:** **B** = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.


## Discussion of Examples

[Return to Top](#)

The “desirements” specified in [White Paper](#) and identified by the [OMG's White Paper Analysis](#) as **Security Issues** are listed in [Table 47](#).

Table 47: Security references of Desirements in the **White Paper**

Desirement No.	Desirement Text	Comment
<b>B0005</b>	<b>Protect against criminal activity</b>	Criminal Activity is a broad, extensive topic that requires an understanding of the U.S. Laws and Regulations as well as international treaties and agreements. Within the context of the CBDC, criminal activity can be one more of the following: 1. <a href="#">Human Trafficking</a> 2. <a href="#">Drug Trafficking</a> 3. <a href="#">Corruption</a> 4. <a href="#">Money Laundering</a>
<b>B0052</b>	<b>Prevent Financial money laundering crimes</b>	There are already quite a few Laws and Regulations within the U.S. to cover <a href="#">Money Laundering</a> . However, within the context of CBDC, these laws need to be reviewed, updated, or amended to reflect Digital Currency and how it might be used in Criminal Activities.

Desirement No.	Desirement Text	Comment
B0053	<p><b>Provide resiliency to threats to existing payment services—including:</b></p> <ol style="list-style-type: none"> <li><b>1. operational disruptions</b></li> <li><b>2. cybersecurity risks</b></li> </ol>	<p><b>1. Operational Disruptions</b> occur when there is a failure in the infrastructure of the CBDC. This implies a compound <b>Non-Functional Requirement</b> that needs to be levied on the CBDC. The following <b>Non-Functional</b> requirements need to be specified for the CBDC:</p> <ol style="list-style-type: none"> <li>1. <b>Reliability</b> <ol style="list-style-type: none"> <li>a. Maturity</li> <li>b. Availability</li> <li>c. Fault Tolerance</li> <li>d. Recoverability</li> </ol> </li> <li>2. <b>Maintainability</b> <ol style="list-style-type: none"> <li>a. Modularity</li> <li>b. Reusability</li> <li>c. Analyzability</li> <li>d. Modifiability</li> <li>e. Testability</li> </ol> </li> <li>3. <b>Manageability</b> <ol style="list-style-type: none"> <li>a. Types of Manageability Functions</li> <li>b. Manageability Costs</li> <li>c. System Manageability Issues</li> <li>d. Software Manageability Issues</li> </ol> </li> </ol> <p><b>Note:</b> Although the OMG DIDO-RA provides general definitions for these non-functional requirements, only the Federal Reserve, in conjunction with the <b>CBDC Stakeholders</b>, can define these requirements in terms of the CBDC. This process takes time and there are no shortcuts. It is part of the System Engineering process.</p> <p><b>2. Cybersecurity Risks</b>, as with <b>Operation Disruptions</b>, represent a compound non-functional requirement for the CBDC. The following <b>Securability Non-Functional</b> requirements need to be specified for the CBDC:</p> <ol style="list-style-type: none"> <li>a. Confidentiality</li> <li>b. Data Integrity</li> <li>c. Non-repudiation</li> <li>d. Authenticity</li> <li>e. Accountability</li> </ol> <p>Securability is also a layered stack:</p>  <p>Figure 9: The layers of Security. The layers of Security:</p> <ol style="list-style-type: none"> <li>1. Physical Security</li> <li>2. Data Security</li> <li>3. Network Security</li> <li>4. Platform Security</li> <li>5. Application Security</li> <li>6. Culture Security</li> </ol>
P0005	<p><b>Protect against criminal activity</b></p>	<p>See <b>B0005</b>.</p>



Desirement No.	Desirement Text	Comment	
P0024	CBDC would need to comply with the U.S. robust rules	<b>Criminal Activity</b>	<b>Approx. Number of Laws and Regulations</b>
		Human Trafficking	14
		Drug Trafficking	9
		Corruption	10
		Money Laundering	11
		<b>Total</b>	<b>44</b>

Desirement No.	Desirement Text	Comment
P0028	<p>Require significant international coordination to address issues such as:</p> <ol style="list-style-type: none"> <li>1. common standards</li> <li>2. infrastructure,</li> <li>3. the types of intermediaries able to access any new infrastructure,</li> <li>4. legal frameworks</li> <li>5. preventing illicit transactions</li> <li>6. the cost and timing of implementation</li> </ol>	<p><b>1. Common Standards:</b> There are lots of “common standards” that can apply to Blockchains. See within each of these sections for a list of applicable standards:</p> <ol style="list-style-type: none"> <li>a. <a href="#">DIDO RA - Technical Standard Bodies</a></li> <li>b. <a href="#">DIDO RA - de facto Standards Bodies</a></li> </ol> <p>Unfortunately, within the “<i>blockchain</i>” world, there is confusion about what constitutes a standard. Often, if something is Open Source, it is considered a standard. However, often these projects lack the rigor needed to be considered a “<i>standard</i>”. Also, see the discussion in the DIDO RA on <a href="#">Talk Openly Develop Openly (TODO)</a> and look at the DIDO RA definition of a <a href="#">Standards Developing Organization (SDO)</a>.</p> <p><b>2. Infrastructure:</b> The CBDC Infrastructure needs to be considered <a href="#">Mission Critical</a> since any loss of functionality could be considered as a threat to survival. This is why the desirements: <b>B0053, D0015, D0016, D0017</b> are in the <b>White paper</b>.</p> <p><b>3. Types of Intermediaries able to access any new infrastructure:</b> <b>B0026</b> specifies bridges between legacy and new payment services and this will require new infrastructure. <b>D0012</b> specifies leveraging existing tools already in use by intermediaries</p> <p><b>4. Legal Frameworks:</b> There are already legal frameworks in place to handle:</p> <ol style="list-style-type: none"> <li>a. <a href="#">National Privacy Considerations</a></li> <li>b. <a href="#">National Security Considerations</a></li> </ol> <p>Although these frameworks were developed without a CBDC, they already “<i>comply with the United States are subject to robust rules</i>” and are continuously being reviewed, updated, and amended based on new information obtained from the field. As part of this process, these frameworks need to add to the existing frameworks rather than created new frameworks.</p> <p><b>5. Preventing Illicit Transactions:</b> There are two areas within the existing legal frameworks covering Illicit transactions:</p> <ol style="list-style-type: none"> <li>a. <a href="#">Money Laundering</a></li> <li>b. <a href="#">Corruption</a></li> </ol> <p>Although these frameworks were developed without a CBDC, they already “<i>comply with the United States are subject to robust rules</i>” and are continuously being reviewed, updated, and amended based on new information obtained from the field. As part of this process, these frameworks need to add to the existing frameworks rather than created new frameworks.</p> <p><b>6. Cost and Timing of Implementation:</b> The CBDC is a complex issue that, once released, could have a life expectancy of many, many years. Only through extensive Systems Analysis, Engineering, Design, and Testing will CBDC have the stability it needs to instill confidence in the public (<b>B0020</b>).</p>

Desirement No.	Desirement Text	Comment
D0013	<p><b>Design should facilitate compliance with a robust set of rules already intended to combat</b></p> <ol style="list-style-type: none"> <li><b>1. money laundering</b></li> <li><b>2. the financing of terrorism</b></li> <li><b>3. customer due diligence</b></li> <li><b>4. record-keeping</b></li> <li><b>5. reporting requirements</b></li> </ol>	<p><b>1. Money Laundering:</b> There are roughly <b>11</b> Laws and Regulations in the U.S. covering <a href="#">4.5.4 Money Laundering</a> that took years to create, usually in response to known or discovered Money Laundering schemes that are continuing to evolve. In many ways, it is an “<i>Arms Race</i>”. The people with a need to launder money keep developing new ways around existing rules, requiring the government to create new rules. The CBDC must at least start from the same place as the existing systems with as many of the rules in place as possible in order to prevent the entire system from imploding. It also needs to assess the current sets of Laws and Regulations to determine if there are required updates or amendments that need to be made before the CBDC can “go live”.</p> <p><b>2. Financing of Terrorism:</b> The main way to finance terrorism is to engage in <a href="#">Financial Crimes</a>. There are four main areas of Financial Crimes used to fund terrorism:</p> <ol style="list-style-type: none"> <li>a. <a href="#">Human Trafficking</a></li> <li>b. <a href="#">Drug Trafficking</a></li> <li>c. <a href="#">Corruption</a></li> <li>d. <a href="#">Money Laundering</a></li> </ol> <p>The U.S. and much of the rest of the world have developed extensive systems of Laws and Regulations to combat these crimes and the design of the CBDC should use and leverage these existing systems rather than try to build something new.</p> <p><b>3. Customer Due Diligence:</b> There are two main tools of the <a href="#">Anti-Money Laundering (AML)</a>:</p> <ol style="list-style-type: none"> <li>a. <a href="#">Know Your Customer (KYC)</a></li> <li>b. <a href="#">Customer Due Diligence</a></li> </ol> <p>Both of these are well understood and documented in the existing system by Intermediaries. Regardless of the <a href="#">Currency Model</a> used for the CBDC (i.e., <a href="#">Digital Cash Model</a> or <a href="#">Digital Account Model</a>), it should embrace these existing sets of tools and adapt them as need be.</p> <p><b>4. Record Keeping:</b> Under the <a href="#">US Patriot Act, Title III: Anti-money-laundering to prevent terrorism of 2001</a> Title III facilitates the prevention, detection, and prosecution of international money laundering and the financing of terrorism <a href="#">Second Subtitle</a> attempts to improve communication between law enforcement agencies and financial institutions, as well as expanding <b>record-keeping</b> and <b>reporting requirements</b>. Also, under the definition of <a href="#">Financial Crimes</a> provided by the Federal Reserve, financial institutions must comply with a robust set of rules that are designed to combat Financial Crimes. These rules include <a href="#">Customer Due Diligence</a>, record keeping, and reporting requirements. Therefore, the CBDC should rely on the existing Intermediaries to help provide well-documented, tried, and true Record Keeping. Blockchain Technology may help alleviate some of the record-keeping responsibilities, but the blocks must include enough information to support <b>record-keeping</b> and <b>reporting requirements</b>.</p> <p><b>5. reporting requirements:</b> See number 6 above.</p>

Desirement No.	Desirement Text	Comment
D0016	<b>Design should include offline capabilities to help with operational resilience of the payment system</b>	See the answer to <a href="#">Question: 18. Should a CBDC have "offline" capabilities? If so, how might that be achieved?</a> .
D0017	<b>Design should include digital payments in areas suffering from large disruption, such as natural disasters</b>	See the answer to <a href="#">Question: 18. Should a CBDC have "offline" capabilities? If so, how might that be achieved?</a> .
B = <a href="#">Benefit Considerations</a>		
P = <a href="#">Policy Considerations</a>		
R = <a href="#">Risk Considerations</a>		
D = <a href="#">Design Considerations</a>		

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:48\\_natsec:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:48_natsec:start)

Last update: 2022/05/18 21:25



## 4.5.1 Human Trafficking

[Return to National Security Considerations](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

The U.S. Department of Justice defines [Human Trafficking](#) as:

***Human Trafficking**, also known as trafficking in persons or modern-day slavery, is a crime that involves compelling or coercing a person to provide labor or services, or to engage in commercial sex acts. The coercion can be subtle or overt, physical or psychological. The exploitation of a minor for commercial sex is human trafficking, regardless of whether any form of force, fraud, or coercion was used.* <https://www.justice.gov/humantrafficking/what-is-human-trafficking>

### U.S. Laws and Regulations

[Return to Top](#)

There is no single U.S. law or regulation covering **Human Trafficking**, but a whole set of laws. Table 46 outlines most of the laws as determined by [U.S. Department of Homeland Security](#) and by the [American Bar Association](#).

There are roughly 14 Laws and Regulations in the U.S. covering Human Trafficking.

Table 46: List of U.S. Laws and Regulations covering Human Trafficking.

Law or Regulation	Description
<a href="#">Trade Facilitation and Enforcement Act of 2015</a>	The <b>Trade Facilitation and Enforcement Act of 2015</b> allows for stiffer enforcement by the U.S. Customs and Border Protection Agency of supply chains of goods made by child or forced labor. The Act enables ICE to investigate the production of any good reported to be a product of child or forced labor and ban the goods from entry into the U.S.
<a href="#">National Defense Authorization Act (2013)</a>	The <b>National Defense Authorization Act (2013)</b> requires a written certification for all grants and contracts over \500,000 that no party involved will engage in or support human trafficking. It also gives governmental agencies the ability to terminate, without penalty, any contract or grant with any organization or individual that engages in human trafficking.
<a href="#">Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) (2003)</a>	<b>PROTECT</b> Act of 2003, established enhanced penalties for individuals engaging in sex tourism with children, both within the United States and in other countries.

Law or Regulation	Description
<b>RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS (RICO)</b>	<b>RICO</b> was created to be a tool for the federal government to more effectively prosecute members of organized crime for racketeering offenses. Federal human trafficking offenses are included as racketeering offenses.
<b>Customs and Facilitations and Trade Enforcement Act (2009)</b>	The <b>Customs and Facilitations and Trade Enforcement Act (2009)</b> prohibits the sale of goods made through the use of coercion or goods made by victims of human trafficking.
<b>Trafficking Victims Protection Reauthorization Act of 2013 (TVPRA 2013)</b>	<b>TVPRA 2013</b> , puts into place emergency response provisions within the State Department to respond to disaster areas and crises where people are particularly susceptible to being trafficked. It also established measures to prevent child marriage and strengthened collaboration efforts between state and local law enforcement.
<b>Trafficking Victims Protection Reauthorization Act of 2008 (TVPRA of 2008)</b>	<b>TVPRA of 2008</b> expanded anti-trafficking prevention strategies and expanded protections available with the T Visa. It also regulated that all unaccompanied alien children be screened as potential victims of human trafficking.
<b>Trafficking Victims Protection Reauthorization Act of 2005 (TVPRA of 2005)</b>	<b>TVPRA of 2005</b> established a pilot program for sheltering human trafficking victims who are minors and provided grant programs to assist state and local law enforcement combat trafficking. It also included provisions to combat sex tourism and regulated government contracts to ensure they are not made with individuals or organizations that promote or engage in human trafficking.
<b>Trafficking Victims Protection Reauthorization Act of 2003 (TVPRA of 2003)</b>	<b>TVPRA of 2003</b> established human trafficking as a chargeable crime under the Racketeering Influenced Corrupt Organizations (RICO) statute. It provided a civil right of action for trafficking victims to sue their traffickers. It further protected victims and their families from deportation and required that the Attorney General report to Congress annually on the activities of the U.S. government in the fight against trafficking.
<b>Trafficking Victims Protection Act (TVPA)</b>	<b>TVPA of 2000</b> established methods of prosecuting traffickers, preventing human trafficking, and protecting victims and survivors of trafficking. The act established human trafficking and related offenses as federal crimes. It established the Office to Monitor and Combat Trafficking in Persons, which is required to publish a Trafficking In Persons (TIP) report each year. The TIP report describes and ranks the efforts of countries to combat human trafficking. The act also established the Interagency Task Force to Monitor and Combat Trafficking, which assists in the implementation of the TVPA. It provides for restitution for victims and immigration relief through the T Visa.
<b>Executive Order on Strengthening Protections Against Trafficking in Persons in Federal Contracts</b>	The <b>Executive Order on Strengthening Protections Against Trafficking in Persons in Federal Contracts orders the Federal Acquisition Regulatory (FAR) Council</b> to amend the Federal Acquisition Regulations to prohibit Federal contractors and subcontractors in solicitations, contracts, and subcontracts for supplies or services from engaging in any trafficking activities such as employee recruitment fees or withholding of identification documents. Additionally, it orders that the Administrator for Federal Procurement Policy shall provide guidance to agencies on developing appropriate internal procedures and controls for awarding and administering Federal contracts to improve monitoring of and compliance with actions to prevent trafficking in persons.

Law or Regulation	Description
<b>Intelligence Reform and Terrorism Prevention Act of 2004</b>	The <b>Intelligence Reform and Terrorism Prevention Act, section 7202</b> established the Human Smuggling and Trafficking Center to achieve greater integration and overall effectiveness in the U.S. government's enforcement and other response efforts, and to work with foreign governments to address the separate but related issues of alien smuggling, trafficking in persons, and criminal support of clandestine terrorist travel.
<b>Civil Asset Forfeiture Reform Act of 2000 (CAFRA)</b>	The Department of Homeland Security (DHS) fights human smuggling and trafficking through the issuance of <b>CAFRA</b> , which provides notice to property owners whose properties have been identified as being used to facilitate smuggling or harboring aliens; it is an important tool because many employers turn a blind eye to the facilitation of criminal activity on their properties.
<b>Mann Act</b>	The <b>Mann Act</b> , also known as the White-Slave Traffic Act of 1910 and its subsequent amendment resolutions, makes it a felony to knowingly persuade, induce, entice, or coerce an individual to travel across state lines to engage in prostitution or attempt to do so. It is an effective tool used to prosecute human traffickers.

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc\\_omg:04\\_doc:15\\_common:48\\_natsec:10\\_human\\_traf](https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:04_doc:15_common:48_natsec:10_human_traf)

Last update: **2022/05/17 20:48**



# 4.5.2 Drug Trafficking

[Return to National Security Considerations](#) [Provide Feedback](#)

## Overview

[Return to Top](#)

[Drug Trafficking](#) is a big and difficult problem to address, especially since the laws have not been updated to reflect the use of Cryptocurrencies and especially a CBDC.

**Drug Trafficking**, also known as **Drug Distribution**, is the crime of selling, transporting, or illegally importing unlawful controlled substances, such as heroin, cocaine, marijuana, or other illegal drugs.

Drug trafficking also applies to the illegal selling or transportation of prescription drugs, which has become an increasing problem in recent years.

According to the Department of Justice, the **sale and manufacture of drugs accounts for almost one-fifth of all drug-related arrests.** <sup>57)</sup>

Drugs continue to come into the U.S. from many sources despite the efforts of numerous U.S. agencies (i.e., Drug Enforcement Administration (DEA)), law enforcement agencies, and border patrols. etc. This trafficking occurs regardless of U.S. and International laws trying to prevent it. Figure 10 shows a map of the world's drug trafficking lanes.



Figure 10: Major Drug Trafficking Routes throughout the world<sup>58)</sup>.

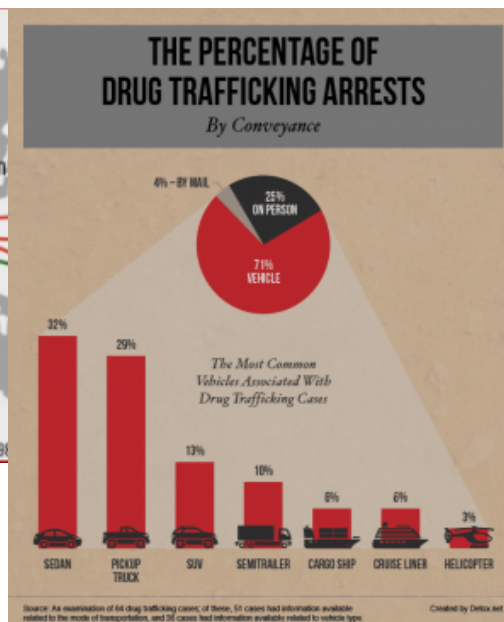


Figure 11: The Percentage of Drug Trafficking Arrests by Conveyance<sup>59)</sup>



Drug offenses of all types were the second most common federal crime in the fiscal year 2020. The 16,829 total drug cases reported to the Commission accounted for 26.1 percent of all cases, a decrease of 3,564 cases (17.5%) from the year before.<sup>60)</sup>

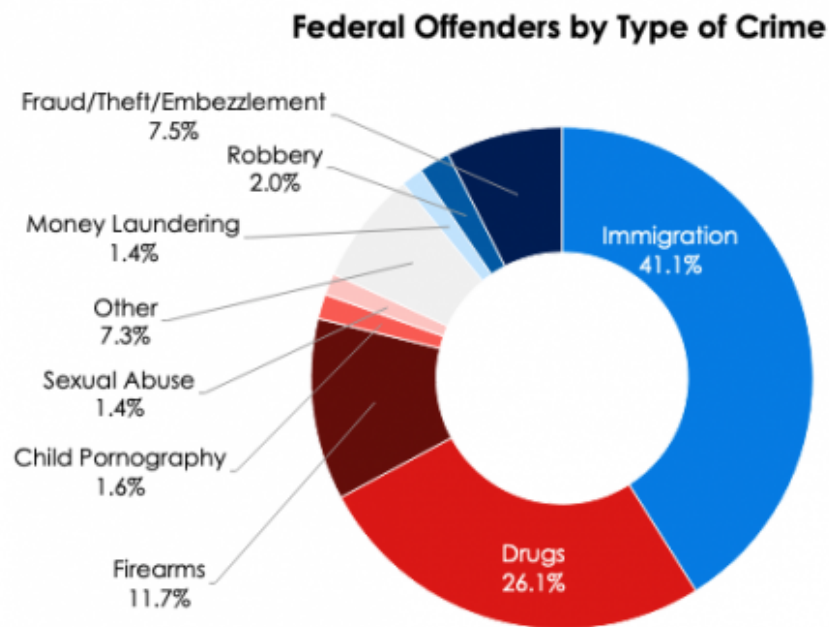


Figure 12: Federal Offenders by Type of Crime

## U.S. Laws and Regulations

[Return to Top](#)

There is no single law or regulation within the U.S. that covers **Drug Trafficking**, but a whole set of laws. Table 47 outlines most of the laws as determined by [United States Attorney's Offices](#) and by the [Seattle Pacific University \(SPU\)](#) .

There are roughly 9 Laws and Regulations in the U.S. covering Drug Trafficking.

Table 47: List of U.S. Laws and Regulations covering Drug Trafficking.

Law or Regulation	Description
<a href="#">21 U.S. Code § 844 - Penalties for simple possession</a>	Persons convicted of illegally possessing any controlled substance face penalties of up to 1 year in prison and a minimum fine of \ \$1,000, or both. Second convictions are punishable by not less than 15 days, but not more than 2 years in prison and a minimum fine of \$2,500. Subsequent convictions are punishable by not less than 90 days but not more than 3 years in prison and a minimum fine of \ \$5,000. Special sentencing provisions for possession of Flunitrazepam (Rohypnol, "roofies" or "roaches") impose a prison term of up to 3 years, a fine, or both. Civil penalties of up to \ \$10,000 may also be imposed for possession of controlled substances, whether or not criminal prosecution is pursued. Persons convicted of possession may also be fined for the reasonable costs of the investigation and prosecution of the offense. Penalties for possession with intent to distribute are potentially even more severe.
<a href="#">21 U.S. Code § 863 - Drug paraphernalia</a>	Persons convicted on federal charges of the sale, import, export, or shipping of drug paraphernalia face penalties of up to 3 years in prison and a monetary fine

Law or Regulation	Description
<b>21 U.S. Code § 853 - Criminal forfeitures</b>	Any person convicted of a federal drug offense punishable by more than one year in prison shall forfeit to the United States any personal or real property related to the violation, including houses, cars, and other personal belongings. Property may be seized upon arrest on charges that may result in forfeiture.
<b>21 U.S. Code § 862 - Denial of Federal benefits to drug traffickers and possessors</b>	A federal drug conviction may result in the loss of federal benefits, including school loans, grants, contracts, and licenses. Federal drug trafficking convictions may result in denial of federal benefits for up to 5 years for a first conviction, 10 years for a second conviction, and permanent denial of federal benefits for a third conviction. Federal drug convictions for possession may result in denial of federal benefits for up to 1 year for a first conviction and up to 5 years for subsequent convictions.
<b>21 U.S. Code § 841 - Prohibited acts A</b>	Penalties for federal drug trafficking convictions vary according to the number of controlled substances involved in the transaction. The tables below summarize penalty information for several types of controlled substances. Persons who violate federal drug trafficking laws within 1,000 feet of a university may face penalties or prison terms and fines up to twice as high as the regular penalties for the offense, with a mandatory prison sentence of at least one year (21 USC §860).
<b>21 U.S. Code § 846 - Attempt and conspiracy</b>	Prohibits conspiracies and attempts to violate any substantive offense established by Subchapter I of Title 21 ("Control and Enforcement")—in other words, Section 846 makes it a crime to conspire to violate or attempt to violate any substantive offense set forth in 21 U.S.C. §§ 801-904.
<b>21 U.S. Code § 843 - Prohibited acts C</b>	<ol style="list-style-type: none"> <li>1. It shall be unlawful for any person to place in any newspaper, magazine, handbill, or other publications, any written advertisement knowing that it has the purpose of seeking or offering illegally to receive, buy, or distribute a Schedule [1] I controlled substance.</li> <li>2. It shall be unlawful for any person to knowingly or intentionally use the Internet, or cause the Internet to be used, to advertise the sale of, or to offer to sell, distribute, or dispense, a controlled substance where such sale, distribution, or dispensing is not authorized by this subchapter or by the Controlled Substances Import and Export Act [21 U.S.C. 951 et seq.].</li> </ol>
<b>21 U.S. Code § 848 - Continuing criminal enterprise - "Drug Kingpin Statute"</b>	A mandatory minimum of 20 years and a maximum of life can be imposed on a leader of an organization of five or more individuals who engage in a continuing series of drug violations from which the person derived substantial income. Mandatory life and death penalty available under certain circumstances.
<b>18 U.S. Code § 1952 - Interstate and foreign travel or transportation in aid of racketeering enterprises</b>	Five-year maximum for traveling or using the mail or instruments of interstate commerce (telephone/ <b>internet</b> ) with intent to facilitate drug trafficking.

57)

Justia, Accessed: 5 April 2022, <https://www.justia.com/criminal/offenses/drug-crimes/drug-trafficking/>

58)

Wikipedia - Public Commons

59)

American Addiction Centers, Editorial Staff, 14 December 2021, Accessed: 7 April 2022,

<https://detox.net/uncover/drug-mules-trafficking-by-the-numbers/>

60)

United States Sentencing Commission, [the Fiscal Year 2020 - Overview of Federal Criminal Cases](https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/FY20_Overview_Federal_Criminal_Cases.pdf), April 2021, Accessed: 7 April 2022,  
[https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/FY20\\_Overview\\_Federal\\_Criminal\\_Cases.pdf](https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/FY20_Overview_Federal_Criminal_Cases.pdf)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:15\\_common:48\\_natsec:20\\_drug\\_traf](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:15_common:48_natsec:20_drug_traf)

Last update: **2022/05/18 21:38**



## 4.5.3 Corruption

[Return to National Security Considerations](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

**Corruption** is “*the abuse of entrusted power for private gain*”, a high level definition provided by [Transparency International](#)<sup>61</sup>.

According to the United Nations<sup>62</sup>:

*Corruption is a complex social, political and economic phenomenon that affects all countries. Corruption undermines democratic institutions, slows economic development, and contributes to governmental instability.*

*Corruption attacks the foundation of democratic institutions by distorting electoral processes, perverting the rule of law, and creating bureaucratic quagmires whose only reason for existing is the soliciting of bribes. Economic development is stunted because foreign direct investment is discouraged and small businesses within the country often find it impossible to overcome the “start-up costs” required because of corruption.*

*On 31 October 2003, the General Assembly adopted the United Nations Convention against Corruption and requested that the Secretary-General designate the United Nations Office on Drugs and Crime (UNODC) as secretariat for the Convention’s Conference of States Parties ( [resolution 58/4](#)).*

*The Assembly also designated 9 December as International Anti-Corruption Day, to raise awareness of corruption and of the role of the Convention in combating and preventing it. The Convention entered into force in December 2005.*

*Governments, the private sector, non-governmental organizations, the media, and citizens around the world are joining forces to fight this crime. The United Nations Development Programme(UNDP) and the United Nations Office on Drugs and Crime (UNODC) are at the forefront of these efforts.*

### Definitions

[Return to Top](#)

Although the definition of corruption by Transparency International is not perfect and not legal, it encapsulates three core elements of corruption: Abuse, Entrusted Power, and Private Gain. See [Table 48](#).

Table 48: Classification of the elements of Corruption<sup>63)</sup>

Type of Corruption	Description
<b>Abuse</b>	Corruption involves a violation of norms of conduct or professional obligations – explicit or implicit – arising from formal or other entrusted duties. The notion implies decision-making without due impartiality; counter to public policies; or more broadly against the public interest.
<b>Entrusted Power</b>	Corruption arises when a person misuses the authority derived from all kinds of formal or professional roles, but also informal or traditional ones. This phrasing covers not only public officials but also individuals working in the private sector, media, civil society actors, and religious leaders. It also covers people such as community elders who hold customary authority. A company employee selling commercial secrets to a competitor is an example of private sector corruption.
<b>Private Gain</b>	The gain realized through corruption is private because it does not benefit the entity or the collective that the official is entrusted to represent or serve. Private gain expresses the opposite of public good. But the gain need not go directly to the official in question: it may also benefit a designated family member, friend, associate, or political party. Also note that anything of value can constitute a benefit: it's not only money and material goods, but also power and influence, and other advantages – even sexual favors.

Another way to define corruption at a high level is that it is a form of dishonesty that is undertaken by an individual or organization in a position of authority in order to gain benefits, including personal gain.

***Public Corruption** involves a breach of public trust and/or abuse of position by federal, state, or local officials and their private sector accomplices. By broad definition, a government official, whether elected, appointed or hired, may violate federal law when he/she asks, demands, solicits, accepts, or agrees to receive anything of value in return for being influenced in the performance of their official duties.*<sup>64)</sup>

## Taxonomy of Corruption

[Return to Top](#)

Under the umbrella of **Corruption**, there is a taxonomy of the elements that are useful for differentiating the kinds of Corruption (i.e., Taxonomy). These elements can be used to categorize corruption; these terms are often additive in nature. For example, the **Conflict of Interest** leads to **Bribery** of an **Administrative Corruption** nature.

Table 49: Classification of the elements of Corruption<sup>65)</sup>

<b>Corruption Term</b>	<b>Definition</b>
<b>Active Bribery</b>	Active bribery refers to the act of promising or giving a bribe, as opposed to the act of receiving a bribe (passive bribery). The term does not mean the active briber has taken the initiative, since the bribe may have been demanded by the receiving party (who commits “passive bribery”). When a citizen reluctantly makes an informal payment in order to receive medical care, which would be refused otherwise, she is nevertheless committing active bribery. The distinction between active and passive bribery is primarily made in legal definitions, which need to be precise and allow for the possibility to sanction either side of the transaction, as appropriate. The classification is similar to the distinction between supply-side and demand-side corruption, which is used in analyzing the patterns of incentives or drivers of corrupt practices.
<b>Administrative Corruption</b>	Corruption occurs at the interface between the state, represented by public officials/bureaucrats in decision-making positions, and the public/citizens when they need a service. For example, when a citizen coming to take out an ID card is only provided this service if he/she pays the bureaucrat an unofficial payment in addition to the official fee.
<b>Bribery</b>	The offer or exchange of money, services, or other valuables to influence the judgment or conduct of a person in a position of entrusted power. The benefit does not need to go to the official in question directly – it can go to a spouse, a child, another relative, a friend, or even to the official's political party as a donation. A bribe is sometimes paid after the fact – for instance, in monthly installments to the official issuing permits to street vendors as long as they are allowed to operate. This form of bribery is called a kickback. Bribery is widely criminalized, and both the party paying the bribe and the party receiving may be liable (see active bribery/ passive bribery). However, in practice, certain forms of bribery are often exempt from prosecution (see facilitation payments).
<b>Clientelism</b>	An informal exploitative system of exchanges (of resources, services, favors) between a wealthier and/or more powerful “patron” or “boss” and less wealthy/weaker “clients” or “followers.” Such systems are typically found in settings where formal governance structures fail to provide adequate resources (including protection), leaving poor and/or marginalized members of society to seek assistance from powerful figures that can deliver them. The corruption dimension is clear when the “patron” is an elected official who distributes resources under his/her control inequitably (abusing his/her entrusted power), as a reward for electoral support (private benefit). Similar informal systems may not involve elected officials directly, but may nevertheless undermine formal rules and institutions, including efforts to combat corruption.
<b>Conflict of Interest</b>	A conflict of interest is a conflict between an entrusted duty on the one hand and the private interest of the duty-bearer on the other hand. For example, a parliamentarian sitting on the committee for healthcare reform might own stock in a major pharmaceutical company. The existence of this private interest could improperly influence the performance of entrusted responsibilities. Because conflicts of interest create opportunities for corruption to take place, they should be avoided or managed.
<b>Demand-Side Corruption</b>	The demand side of the bribe (also known as “passive” bribery) focuses on the person or entity soliciting or receiving the bribe.
<b>Embezzlement</b>	The misappropriation of property or funds legally entrusted to someone in their formal position as an agent or guardian. Accountants and financial managers typically have access to an agency's funds and so are in a position to embezzle them. Other forms of embezzlement include the taking of supplies, equipment, etc.

<b>Corruption Term</b>	<b>Definition</b>
<b>Extortion</b>	The practice of obtaining something (money, favors, property) through the use of threats or force. For example, extortion takes place when armed guards exact money for passage through a roadblock. Withholding life-saving medical attention unless a bribe is paid could also be considered an act of extortion. See also sextortion, which involves threats or force to obtain sexual benefits.
<b>Facilitation Payments</b>	Refer to relatively small, individual amounts paid beyond the official fees to speed up services such as customs clearance, work permits, border crossings, etc. Technically, these are a bribe. In many countries, however, facilitation payments by companies doing business abroad are exempt from prosecution for bribery in their home countries as long as they are used to speed up legal processes, rather than to avoid regulations. This exception recognizes the fact that in certain settings, it is impossible to operate a business without conceding to such payments.
<b>Fraud</b>	An economic crime involving deceit, trickery, or false pretenses by which someone gains unlawfully. Fraud often accompanies corrupt acts, in particular embezzlement, where it is typically used to falsify records to hide stolen resources.
<b>Grand Corruption</b>	In contrast to “petty corruption”, high-level or “grand” corruption is perpetrated at the highest levels of government and usually involves both substantial benefits for the officials involved and significant losses for the state and its citizens. It can refer to specific acts such as ministers taking multi-million dollar bribes to award lucrative government concessions or embezzling millions from state coffers into a secret bank account. But it also refers to illicit exchanges in the realm of policy formation (see also state capture). Though large sums of money may be involved, other benefits like high-level appointments, inside information, and policy influence can be the currency of grand corruption. Corruption at this level is also sometimes referred to as political corruption.
<b>Kickback</b>	A bribe is paid after the fact for an undue favor or service. For instance, a company that receives a government contract might send the responsible official regular payoffs for the duration of the contract. Street vendors may pay the permission-granting authority a small sum each month as long as they are allowed to operate.
<b>Kleptocracy</b>	A Greek word meaning “rule by thieves”, kleptocracy refers to a system of government in which leaders use their position for private gain at the expense of the governed. It is typically correlated with autocratic regimes with no meaningful accountability mechanism, effectively allowing the leader to plunder the state and its citizens for personal enrichment and to entrench his hold on power. Some well-known former kleptocrats include Francois Duvalier (“Papa Doc”) of Haiti, Mobutu of Zaire, and Suharto of Indonesia.
<b>Nepotism</b>	A form of favoritism involving family relationships, in which someone exploits his or her authority to procure jobs or other favors for relatives. When this treatment is extended to friends and associates, the appropriate term is cronyism.
<b>Passive Bribery</b>	Refers to the act of receiving the bribe. This does not mean the passive briber has taken no initiative – in many cases, he or she may have demanded the bribe in the first place.
<b>Patronage</b>	The support or sponsorship of a patron (wealthy or influential guardian). Patronage is used to make appointments to government jobs, promotions, contracts for work, etc. The desire to gain power, wealth, and status through their behavior motivates most patrons. Patronage violates the boundaries of legitimate political influence and the principles of merit.

<b>Corruption Term</b>	<b>Definition</b>
<b>Petty Corruption</b>	Alternatively called “administrative” or “bureaucratic” corruption, the term refers to the everyday corruption that takes place when bureaucrats meet the public. While the sums of money involved tend to be small, they are far from “petty” for the people concerned. Examples include paying bribes to get an ID; enrolling in school; or having a phone line installed.
<b>Political Corruption</b>	The term is both narrowly used to designate the manipulation of policies, institutions, and rules in the financing of political parties and in electoral campaigns, and also more broadly as a synonym for “grand corruption”, or corruption taking place at the highest levels of government where policies and rules are formulated and executive decisions are made.
<b>Sextortion</b>	The abuse of power to obtain a sexual benefit or advantage. Related to the concept of extortion.
<b>Sporadic Corruption</b>	Sporadic corruption is the opposite of systemic corruption. Because it occurs irregularly, it does not threaten the mechanisms of control or the economy as such. It is not crippling, but can seriously undermine morale and sap the economy of resources.
<b>State Capture</b>	Coined by the World Bank in the early 2000s, state capture refers to a type of systemic political corruption in which private interests significantly influence a state's decision-making processes to their own advantage. For example, businesses can improperly influence legislators to pass favorable laws.
<b>Supply-Side Corruption</b>	Supply-side refers to the person or entities who offer or provide the illicit benefit in corrupt transactions. The officials with entrusted authority who received illicit benefits constitute the demand side. The distinction is similar to that between active and passive bribery, which is used primarily for legislative purposes. Also similar is the fact that the term “demand-side” does not imply that it is the official on the receiving end who proactively solicited the bribe. The distinction between supply and demand can be useful in analyzing the different sets of incentives that contribute to corruption.
<b>Systemic Corruption</b>	(Also known as endemic corruption). A situation when corruption is an integral part of a state's economic, social and political system, and where most people have no alternatives to dealing with corrupt officials. Sporadic corruption, in contrast, occurs irregularly and does not compromise the mechanisms of governance in the same crippling way.
<b>Trading in influence</b>	(Also known as influence peddling). Trading in influence occurs when a person who has a real or apparent influence on the decision-making of a public official exchanges this influence for undue advantage. The offense is similar to bribery with one important difference: trading in influence concerns the “middleman”, or the person that serves as the go-between the decision-maker and the party that seeks an improper advantage. The final decision-maker may not even be aware of the illicit exchange. One example is when an MP receives a payment from a company to attempt to convince fellow legislators to support amendments that would benefit that company. Trading in influence is difficult to prove because the legal definitions involve disputable criteria of “intentionality” and “undue”/improper influence. Trading in influence is also often difficult to distinguish from permissible forms of lobbying.

## Corruption is Ubiquitous

[Return to Top](#)



Often it is assumed that corruption is a “third world problem”. While it is often prevalent or detected more in the third world, it does not mean that the CBDC can ignore the problem here or around the world. Figure 13 provides a map of known corruption around the world.

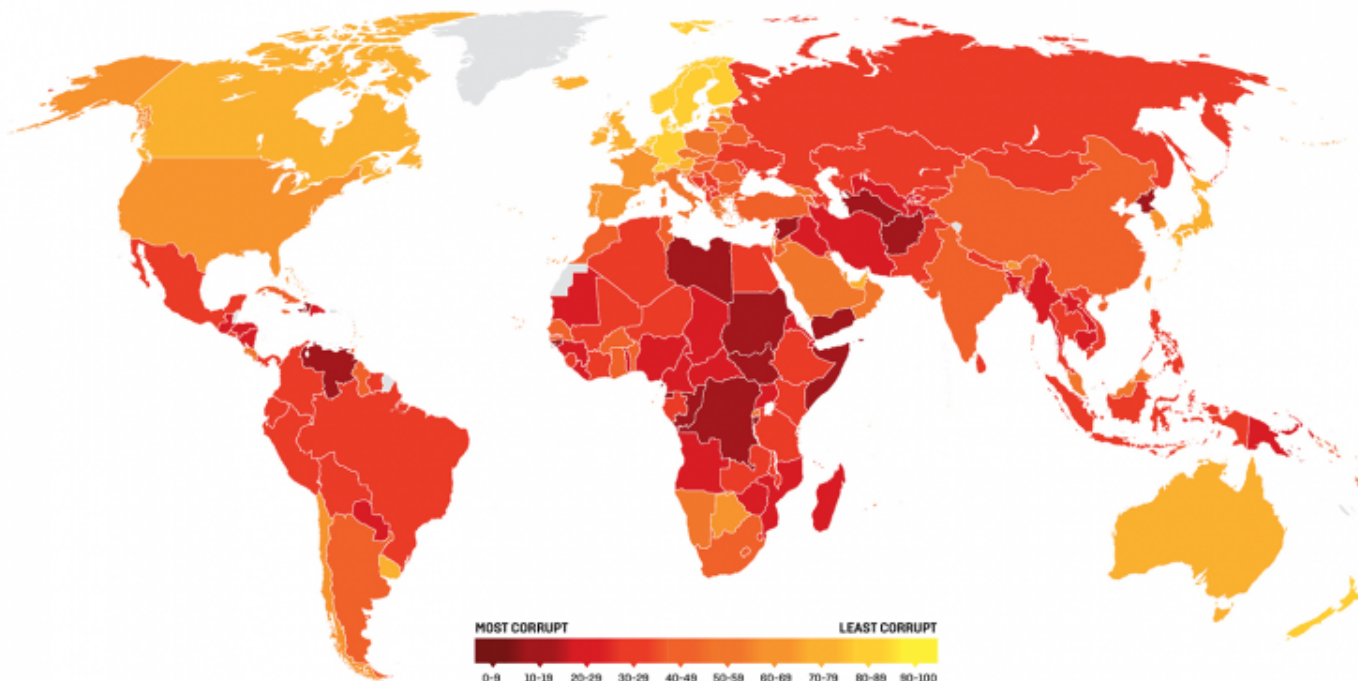


Figure 13: The ubiquitous nature of Corruption in the world.

The Foreign Graphics website produced a report and reported the following about the U.S. <sup>66)</sup>:

*In the annual Corruption Perceptions Index (CPI), the United States fell to a low of 67 out of a maximum possible score of 100, down from a high of 76 in 2015. By its nature, corruption is difficult to document, so the index relies on a variety of different sources to measure the level of perceived public sector corruption. The lower the score, the worse the corruption. Two-thirds of the 180 countries and territories included in the 2020 index scored below 50, with an average of 43.*

## U.S. Laws and Regulations

[Return to Top](#)

There is no single law or regulation within the U.S. that covers **Corruption**, but a whole set of laws or frameworks. Table 50 outlines most of the laws as determined by [U.S. Department of Justice](#).

There are roughly 10 Laws and Regulations in the U.S. covering Corruption.

Table 50: List of U.S. Laws and Regulations covering Corruption.

Law or Regulation	Description
<p><b>U.S. Foreign Corrupt Practices Act</b></p>	<p>1. Under the Foreign Corrupt Practices Act (FCPA), it is unlawful for a U.S. person or company to offer, pay, or promise to pay money or anything of value to any foreign official for the purpose of obtaining or retaining business.</p> <p>2. A U.S. person or company may also be an officer, director, employee, or agent of a company or any stockholder acting on behalf of the company. And a foreign official may be a foreign political party or candidate for foreign political office.</p> <p>3. Also covered by the FCPA is the authorization of any money, offer a gift, or promise authorizing the giving of anything of value to any person while knowing that all or a portion of it will be offered, given, or promised—directly or indirectly—to any foreign official for the purposes of assisting the U.S. person or company in obtaining or retaining business.</p> <p>4. “Knowing” includes the concepts of conscious disregard and willful blindness.</p> <p>5. The FCPA also covers foreign persons or companies that commit acts in furtherance of such bribery in the territory of the United States, as well as U.S. or foreign public companies listed on stock exchanges in the United States or which are required to file periodic reports with the U.S. Securities and Exchange Commission.</p> <p>6. The FCPA accounting provisions require such publicly listed companies to make and keep accurate books and records and to devise and maintain an adequate system of internal accounting controls. The accounting provisions also prohibit individuals and businesses from knowingly falsifying books and records or knowingly circumventing or failing to implement a system of internal controls. U.S. persons or companies, or covered foreign persons or companies, should consult an attorney or use the Department of Justice Opinion Procedure when confronted with FCPA issues.</p>
<p><b>18 U.S. Code § 201 - Bribery of public officials and witnesses</b></p>	<p>Section 201 of Title 18 is entitled “Bribery of public officials and witnesses.” The statute comprises two distinct offenses, however, and in common parlance, only the first of these is true “bribery.”<sup>67)</sup></p> <p>The first offense, codified in section 201(b), prohibits the giving or accepting of anything of value to or by a public official, if the thing is given “with intent to influence” an official act, or if it is received by the official “in return for being influenced.”</p> <p>The second offense, codified in section 201©, concerns what is commonly known as “gratuities,” although that word does not appear anywhere in the statute. Section 201© prohibits that same public official from accepting the same thing of value if he does so “for or because of” any official act and prohibits anyone from giving any such thing to him for such a reason.</p> <p>The specific subsections of the statute are:</p> <ol style="list-style-type: none"> <li>1. <b>Bribery</b> <ol style="list-style-type: none"> <li>a. § 201(b)(1): offering a bribe to a public official</li> <li>b. § 201(b)(2): acceptance of a bribe by a public official</li> </ol> </li> <li>2. <b>Gratuities</b> <ol style="list-style-type: none"> <li>a. § 201©(1)(A): offering a gratuity to a public official</li> <li>b. § 201©(1)(B): acceptance of a gratuity by a public official.</li> </ol> </li> </ol> <p>The two offenses differ in several respects. The most important of these differences concerns how close a connection there is between the giving (or receiving) of the thing of value, on the one hand, and the doing of the official act, on the other.</p> <p>Also see: <a href="#">Anti-Corruption in the United States</a></p>

Law or Regulation	Description
<p><b>18 U.S. Code § 1952 - Interstate and foreign travel or transportation in aid of racketeering enterprises</b></p>	<p>(a) Whoever travels in interstate or foreign commerce or uses the mail or any facility in interstate or foreign commerce, with intent to—</p> <p>(1) distribute the proceeds of any unlawful activity; or</p> <p>(2) commit any crime of violence to further any unlawful activity; or</p> <p>(3) otherwise promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on, of any unlawful activity, and thereafter performs or attempts to perform—</p> <p>(A) an act described in paragraph (1) or (3) shall be fined under this title, imprisoned not more than 5 years, or both; or</p> <p>(B) an act described in paragraph (2) shall be fined under this title, imprisoned for not more than 20 years, or both, and if death results shall be imprisoned for any term of years or for life.</p>
<p><b>18 U.S. Code § 1341 - Frauds and swindles</b></p>	<p>“There are two elements in mail fraud: (1) having devised or intending to devise a scheme to defraud (or to perform specified fraudulent acts), and (2) use of the mail for the purpose of executing, or attempting to execute, the scheme (or specified fraudulent acts).” <i>Schmuck v. United States</i>, 489 U.S. 705, 721 n. 10 (1989); see also <i>Pereira v. United States</i>, 347 U.S. 1, 8 (1954) (“The elements of the offense of mail fraud under . . . § 1341 are (1) a scheme to defraud, and (2) the mailing of a letter, etc., for the purpose of executing the scheme.”); <i>Laura A. Eilers &amp; Harvey B. Silikovitz, Mail and Wire Fraud</i>, 31 <i>Am. Crim. L. Rev.</i> 703, 704 (1994) (cases cited).<sup>68)</sup></p>
<p><b>18 U.S. Code § 1343 - Fraud by wire, radio, or television</b></p>	<p>The elements of wire fraud under Section 1343 directly parallel those of the mail fraud statute but require the use of an interstate telephone call or electronic communication made in furtherance of the scheme. <i>United States v. Briscoe</i>, 65 F.3d 576, 583 (7th Cir. 1995) (citing <i>United States v. Ames Sintering Co.</i>, 927 F.2d 232, 234 (6th Cir. 1990) (per curiam)); <i>United States v. Frey</i>, 42 F.3d 795, 797 (3d Cir. 1994) (wire fraud is identical to mail fraud statute except that it speaks of communications transmitted by wire); see also, e.g., <i>United States v. Profit</i>, 49 F.3d 404, 406 n. 1 (8th Cir.) (the four essential elements of the crime of wire fraud are: (1) that the defendant voluntarily and intentionally devised or participated in a scheme to defraud another out of money; (2) that the defendant did so with the intent to defraud; (3) that it was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were in fact used) (citing <i>Manual of Model Criminal Jury Instructions for the District Courts of the Eighth Circuit</i> 6.18.1341 (West 1994)), cert. denied, 115 S.Ct. 2289 (1995); <i>United States v. Hanson</i>, 41 F.3d 580, 583 (10th Cir. 1994) (two elements comprise the crime of wire fraud: (1) a scheme or artifice to defraud; and (2) use of interstate wire communication to facilitate that scheme); <i>United States v. Faulkner</i>, 17 F.3d 745, 771 (5th Cir. 1994) (essential elements of wire fraud are: (1) a scheme to defraud and (2) the use of, or causing the use of, interstate wire communications to execute the scheme), cert. denied, 115 S.Ct. 193 (1995); <i>United States v. Cassiere</i>, 4 F.3d 1006 (1st Cir. 1993) (to prove wire fraud government must show (1) scheme to defraud by means of false pretenses, (2) defendant's knowing and willful participation in a scheme with intent to defraud, and (3) use of interstate wire communications in furtherance of the scheme); <i>United States v. Maxwell</i>, 920 F.2d 1028, 1035 (D.C. Cir. 1990) (“Wire fraud requires proof of (1) a scheme to defraud; and (2) the use of an interstate wire communication to further the scheme.”).<sup>69)</sup></p>

Law or Regulation	Description
<p><b>18 U.S. Code § 1346 - Definition of “scheme or artifice to defraud”</b></p>	<p>Honest services fraud is defined in federal statute 18 U.S.C. §1346 as a scheme to defraud another of the intangible right to honest services through a scheme to violate a fiduciary duty by bribery or kickbacks. A fiduciary duty is a duty to act only for the benefit of the public, an employer, shareholders, or a union. The statute was created by Congress as a response to the government's limitation in its use of the wire fraud statute. <a href="https://www.federalcriminallawyer.us/honest-services-fraud/">https://www.federalcriminallawyer.us/honest-services-fraud/</a></p>
<p><b>Sections 13(b)(2)(A) and (B) of the Securities Exchange Act of 1934</b></p>	<p>Sections 13(b)(2)(A) and (B) of the Securities Exchange Act of 1934, as amended. Section 13(b)(2)(A) of the Exchange Act requires issuers to make and keep books, records, and accounts, that accurately and fairly reflect the transactions and dispositions of the assets of the issuer. Section 13(b)(2)(B) of the Exchange Act requires issuers to devise and maintain a system of internal accounting controls that, among other things, is sufficient to provide reasonable assurances that assets are used, transactions are executed, only in accordance with management’s general or specific authorization. <a href="https://tinyurl.com/5n87cf3u">https://tinyurl.com/5n87cf3u</a></p>
<p><b>15 U.S. Code § 78dd-1 - Prohibited foreign trade practices by issuers</b></p>	<p>The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. (“FCPA”), was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. Specifically, the anti-bribery provisions of the FCPA prohibit the willful use of the mails or any means of the instrumentality of interstate commerce corruptly in furtherance of any offer, payment, promise to pay, or authorization of the payment of money or anything of value to any person, while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to a foreign official to influence the foreign official in his or her official capacity, induce the foreign official to do or omit to do an act in violation of his or her lawful duty or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person.</p> <p>Since 1977, the anti-bribery provisions of the FCPA have applied to all U.S. persons and certain foreign issuers of securities. With the enactment of certain amendments in 1998, the anti-bribery provisions of the FCPA now also apply to foreign firms and persons who cause, directly or through agents, an act in furtherance of such a corrupt payment to take place within the territory of the United States.</p> <p>The FCPA also requires companies whose securities are listed in the United States to meet its accounting provisions. See 15 U.S.C. § 78m. These accounting provisions, which were designed to operate in tandem with the anti-bribery provisions of the FCPA, require corporations covered by the provisions to (a) make and keep books and records that accurately and fairly reflect the transactions of the corporation and (b) devise and maintain an adequate system of internal accounting controls.<sup>70)</sup></p>
<p><b>17 CFR § 240.15d-1 - Requirement of annual reports from Securities Exchange Act of 1934</b></p>	<p>This practice note discusses reporting obligations under Section 15(d) (15 USCS § 78o) of the Securities Exchange Act of 1934, as amended (the Exchange Act). Section 15(d) provides that any issuer who registers a class of securities under the Securities Act of 1933, as amended (the Securities Act) shall become subject to periodic reporting requirements under Section 13(a) (15 USCS § 78m) of the Exchange Act, including annual reports on Form 10-K, quarterly reports on Form 10-Q and current reports on Form 8-K. However, Section 15(d) does not trigger all Exchange Act obligations. For example, reports under Section 16 (15 USCS § 78p) or Section 13(d) or obligations with respect to proxies are not triggered by the application of Section 15(d) alone. <a href="https://tinyurl.com/583z6nxv">https://tinyurl.com/583z6nxv</a></p>

Law or Regulation	Description
<p><b>2018 Chapter 8 Chapter Eight - Sentencing of Organizations</b></p>	<p>The guidelines and policy statements in this chapter apply when the convicted defendant is an organization. Organizations can act only through agents and, under federal criminal law, generally are vicariously liable for offenses committed by their agents. At the same time, individual agents are responsible for their own criminal conduct. Federal prosecutions of organizations therefore frequently involve individual and organizational co-defendants. Convicted individual agents of organizations are sentenced in accordance with the guidelines and policy statements in the preceding chapters. This chapter is designed so that the sanctions imposed upon organizations and their agents, taken together, will provide just punishment, adequate deterrence, and incentives for organizations to maintain internal mechanisms for preventing, detecting, and reporting criminal conduct.</p> <p>This chapter reflects the following general principles:</p> <ol style="list-style-type: none"> <li>1. First, the court must, whenever practicable, order the organization to remedy any harm caused by the offense. The resources expended to remedy the harm should not be viewed as punishment, but rather as a means of making victims whole for the harm caused.</li> <li>2. Second, if the organization operated primarily for a criminal purpose or primarily by criminal means, the fine should be set sufficiently high to divest the organization of all its assets.</li> <li>3. Third, the fine range for any other organization should be based on the seriousness of the offense and the culpability of the organization. The seriousness of the offense generally will be reflected by the greatest of the pecuniary gain, the pecuniary loss, or the amount in a guideline offense level fine table. Culpability generally will be determined by six factors that the sentencing court must consider. The four factors that increase the ultimate punishment of an organization are: (i) the involvement in or tolerance of criminal activity; (ii) the prior history of the organization; (iii) the violation of an order; and (iv) the obstruction of justice. The two factors that mitigate the ultimate punishment of an organization are: (i) the existence of an effective compliance and ethics program; and (ii) self-reporting, cooperation, or acceptance of responsibility.</li> <li>4. Fourth, probation is an appropriate sentence for an organizational defendant when needed to ensure that another sanction will be fully implemented or to ensure that steps will be taken within the organization to reduce the likelihood of future criminal conduct.</li> </ol> <p>These guidelines offer incentives to organizations to reduce and ultimately eliminate criminal conduct by providing a structural foundation from which an organization may self-police its own conduct through an effective compliance and ethics program. The prevention and detection of criminal conduct, as facilitated by an effective compliance and ethics program, will assist an organization in encouraging ethical conduct and in complying fully with all applicable laws.</p>

61)

Transparency International is a global movement working in over 100 countries to end the injustice of corruption

62)

United Nations, International Anti-Corruption Day - December 9, [Background](https://www.un.org/en/observances/anti-corruption-day/background), Accessed: 7 April 2022, <https://www.un.org/en/observances/anti-corruption-day/background>

63)

U4, [Basic Guide to Anti-Corruption](https://www.u4.no/topics/anti-corruption-basics/basics), Accessed 6 April 2022, <https://www.u4.no/topics/anti-corruption-basics/basics>

64)

Legal Information Institute, Cornell Law School, Public Corruption, Accessed: 6 April 2022,  
[https://www.law.cornell.edu/wex/public\\_corruption](https://www.law.cornell.edu/wex/public_corruption)

65)

U4, Glossary of Terms, Accessed 6 April 2022, <https://www.u4.no/terms>

66)

Foreign Policy, Report: Corruption in the U.S. at Worst Levels in Almost a Decade, 28 January 2021,  
Accessed: 8 April 2022,  
<https://foreignpolicy.com/2021/01/28/report-transparency-international-corruption-worst-decade-united-states/>

67)

U.S. Department of Justice, 2041. Bribery Of Public Officials, Accessed: 6 April 2022,  
<https://www.justice.gov/archives/jm/criminal-resource-manual-2041-bribery-public-officials>

68)

U.S. Department of Justice, 940. 18 U.S.C. Section 1341—Elements of Mail Fraud, Accessed: 6 April 2022,  
<https://www.justice.gov/archives/jm/criminal-resource-manual-940-18-usc-section-1341-elements-mail-fraud>

69)

U.S. Department of Justice, 941. 18 U.S.C. 1343—Elements of Wire Fraud, Accessed: 6 April 2022,  
<https://www.justice.gov/archives/jm/criminal-resource-manual-941-18-usc-1343-elements-wire-fraud>

70)

U.S. Department of Justice, Foreign Corrupt Practices Act, Accessed: 6 April 2022,  
<https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:15\\_common:48\\_natsec:30\\_corrupt](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:15_common:48_natsec:30_corrupt)Last update: **2022/05/18 21:38**



## 4.5.4 Money Laundering

[Return to National Security Considerations](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

The U.S. Treasury, Financial Crimes Enforcement Network provides the following overview of the problem with [Money Laundering](#):

*Money Laundering is the process of making illegally-gained proceeds (i.e. “dirty money”) appear legal (i.e. “clean”). Typically, it involves three steps: placement, layering and integration. First, illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the “dirty money” appears “clean.” Money laundering can facilitate crimes such as drug trafficking and terrorism, and can adversely impact the global economy.*

*In its mission to “safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity,” the Financial Crimes Enforcement Network acts as the designated administrator of the Bank Secrecy Act (BSA). The BSA was established in 1970 and has become one of the most important tools in the fight against money laundering. Since then, numerous other laws have enhanced and amended the BSA to provide law enforcement and regulatory agencies with the most effective tools to combat money laundering. An index of anti-money laundering laws since 1970 with their respective requirements and goals is listed below in chronological order.*

Money Laundering is an illegal process of converting large amounts of money generated through a criminal activity that appear to be from a legitimate source. The money from the criminal activity is considered “dirty”, and the process “launders” it to make it look “clean”, thus the use of the term **Money Laundering**.

Money Laundering is a serious financial crime employed by both white-collar and street-level criminals and can be in small amounts or large. Most financial companies (i.e., **Financial Intermediaries**) have [Anti-Money Laundering \(AML\)](#) policies to help detect and prevent this activity.

There are two main tools of the AML:

- [Know Your Customer \(KYC\)](#)
- [Customer Due Diligence](#)

Money Laundering can be divided into three main steps (see [Figure 14](#)):

1. Deposit of illicit funds into the financial system

2. Transactions designed to conceal the illicit origin of the funds, known as “layering”
3. Use of laundered funds to acquire real estate, financial instruments, or commercial investments

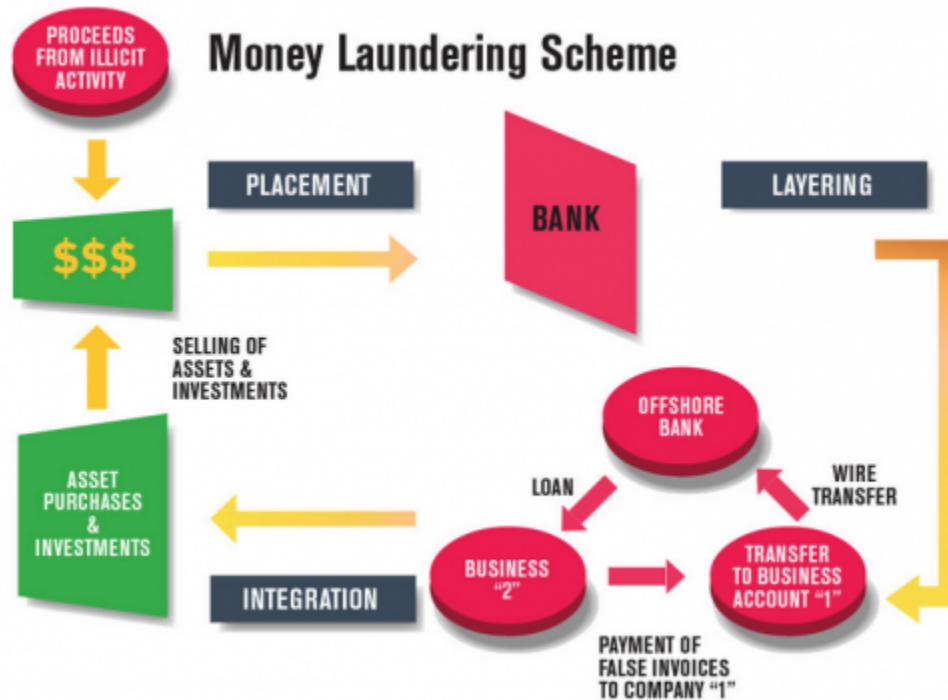


Figure 14: Basic Money Laundering Scheme<sup>71)</sup>

There are two categories of Money Laundering:

- Domestic Money Laundering
- International Money Laundering

## U.S. Laws and Regulations

[Return to Top](#)

There is no single U.S. law or regulation covering **Human Trafficking**, but a whole set of laws. Table 51 outlines most of the laws as determined by [U.S. Treasury - Financial Crimes Enforcement Network](#).

There are roughly 11 Laws and Regulations in the U.S. covering Money Laundering.

Table 51: List of Applicable U.S. Federal and State Laws governing National Security and Money Laundering.

U.S. Federal Laws	
Law / Regulation	Description
<a href="#">Bank Secrecy Act of 1970 (BSA)</a>	The BSA is U.S. law requiring financial institutions in the United States to assist U.S. government agencies in detecting and preventing money laundering.



<b>U.S. Federal Laws</b>	
<b>U.S. Foreign Corrupt Practices Act (FCPA) of 1977</b>	<p>1. Under the Foreign Corrupt Practices Act (FCPA), it is unlawful for a U.S. person or company to offer, pay, or promise to pay money or anything of value to any foreign official for the purpose of obtaining or retaining business.</p> <p>2. A U.S. person or company may also be an officer, director, employee, or agent of a company or any stockholder acting on behalf of the company. And a foreign official may be a foreign political party or candidate for foreign political office.</p> <p>3. Also covered by the FCPA is the authorization of any money, offer a gift, or promise authorizing the giving of anything of value to any person while knowing that all or a portion of it will be offered, given, or promised—directly or indirectly—to any foreign official for the purposes of assisting the U.S. person or company in obtaining or retaining business.</p> <p>4. “Knowing” includes the concepts of conscious disregard and willful blindness.</p> <p>5. The FCPA also covers foreign persons or companies that commit acts in furtherance of such bribery in the territory of the United States, as well as U.S. or foreign public companies listed on stock exchanges in the United States or which are required to file periodic reports with the U.S. Securities and Exchange Commission.</p> <p>6. The FCPA accounting provisions require such publicly listed companies to make and keep accurate books and records and to devise and maintain an adequate system of internal accounting controls. The accounting provisions also prohibit individuals and businesses from knowingly falsifying books and records or knowingly circumventing or failing to implement a system of internal controls. U.S. persons or companies, or covered foreign persons or companies, should consult an attorney or use the Department of Justice Opinion Procedure when confronted with FCPA issues.</p>
<b>Money Laundering Control Act of 1986 (MCLA)</b>	<p>The MCLA makes money laundering, a federal crime, by criminalizing money laundering. It also prohibits individuals from engaging in a financial transaction with proceeds that were generated from certain specific crimes, known as <a href="#">Specified Unlawful Activities (SUAs)</a>. Additionally, the law requires that an individual specifically intends in making the transaction to conceal the source, ownership, or control of the funds.</p>
<b>Anti-Drug Abuse Act of 1988</b>	<p>The Anti-Drug Abuse Act of 1988 expanded the definition of “financial institution” to include car dealerships and real estate closers. These financial services businesses often handle large amounts of money, so they were attractive options for funneling large sums of money. These entities are now required to file reports on large currency transactions. They are also required to verify the identity of purchasers in amounts of over \ \$3,000.</p>
<b>Annunzio-Wylie Anti-Money Laundering Act of 1992</b>	<p>The legislation strengthened the sanctions for BSA violations, required verification and recordkeeping for wire transfers, and notably, established the Bank Secrecy Act Advisory Group (BSAAG). Additionally, the legislation required Suspicious Activity Reports (SARs) and eliminated previously used Criminal Referral Forms.</p> <p><a href="https://www.sigmaratings.com/knowledge-center/history-of-aml-laws">https://www.sigmaratings.com/knowledge-center/history-of-aml-laws</a></p>

<b>U.S. Federal Laws</b>	
<b>Money Laundering Suppression Act of 1994</b>	<p>The Money Laundering Suppression Act of 1994 required banking agencies to enhance training and to review how they refer cases to law enforcement. It also folded “money service businesses” into anti-money laundering laws. These are businesses that cash checks, issue traveler's checks, money orders, or stored value cards, or exchange currency.</p> <p><a href="https://www.findlaw.com/criminal/criminal-charges/money-laundering.html">https://www.findlaw.com/criminal/criminal-charges/money-laundering.html</a></p>
<b>Money Laundering and Financial Crimes Strategy Act of 1998</b>	<p>Money Laundering and Financial Crimes Strategy Act of 1998 - Amends Federal law governing monetary transactions to redefine money laundering and related financial crimes as either: (1) the movement of illicit cash or cash equivalent proceeds into, out of, or through the United States or through certain U.S. financial institutions; or (2) the meaning given under State and local criminal statutes pertaining to the movement of illicit cash or cash equivalent proceeds.</p> <p><a href="https://www.congress.gov/bill/105th-congress/house-bill/1756">https://www.congress.gov/bill/105th-congress/house-bill/1756</a></p>
<b>US Patriot Act, Title III: Anti-money-laundering to prevent terrorism of 2001</b>	<p>US Patriot Act, Title III facilitates the prevention, detection, and prosecution of international money laundering and the financing of terrorism. It primarily amends portions of the Money Laundering Control Act of 1986 (MLCA) and the Bank Secrecy Act of 1970 (BSA). It was divided into three subtitles:</p> <ol style="list-style-type: none"> <li>1. The <a href="#">First Subtitle</a> deals primarily with strengthening banking rules against money laundering, especially on the international stage</li> <li>2. The <a href="#">Second Subtitle</a> attempts to improve communication between law enforcement agencies and financial institutions, as well as expanding record-keeping and reporting requirements</li> <li>3. The <a href="#">Third Subtitle</a> deals with currency smuggling and counterfeiting, including quadrupling the maximum penalty for counterfeiting foreign currency.</li> </ol>

<b>U.S. Federal Laws</b>	
<b>18 U.S. Code § 1956 - Laundering of monetary instruments</b>	<p>Section 1956(a) defines three types of criminal conduct: domestic money laundering transactions (§ 1956(a)(1)); international money laundering transactions (§ 1956(a)(2)); and undercover “sting” money laundering transactions (§ 1956(a)(3)). See this Manual at 2182.</p> <p>To be criminally culpable under 18 U.S.C. § 1956(a)(1), a defendant must conduct or attempt to conduct a financial transaction, knowing that the property involved in the financial transaction represents the proceeds of some unlawful activity, with one of the four specific intents discussed below, and the property must in fact be derived from a specified unlawful activity. The actual source of the funds must be one of the specified forms of criminal activity identified by the statute, in 18 U.S.C. § 1956©(7), or those incorporated by reference from the RICO statute (18 U.S.C. § 1961(1)).</p> <p>Section 1956©(7)(B) includes in the list of specified unlawful activity certain offenses against a foreign nation. Thus, proceeds of certain crimes committed in another country may constitute proceeds of specified unlawful activity for purposes of the money laundering statutes.</p> <p>To prove a violation of § 1956(a)(1), the prosecutor must prove, either by direct or circumstantial evidence, that the defendant knew that the property involved was the proceeds of any felony under State, Federal or foreign law. The prosecutor need not show that the defendant knew the specific crime from which the proceeds were derived; the prosecutor must prove only that the defendant knew that the property was illegally derived in some way. See § 1956©(1).</p> <p>The prosecutor must also prove that the defendant initiated or concluded, or participated in initiating or concluding, a financial transaction. A “transaction” is defined in § 1956©(3) as a purchase, sale, loan, pledge, gift, transfer, delivery, other disposition, and with respect to a financial institution, a deposit, withdrawal, transfer between accounts, loan, exchange of currency, an extension of credit, purchase or sale safe-deposit box, or any other payment, transfer or delivery by, through or to a financial institution.</p> <p>A “financial transaction” is defined in § 1956©(4) as a transaction that affects interstate or foreign commerce and: (1) involves the movement of funds by wire or by other means; (2) involves the use of a monetary instrument; or (3) involves the transfer of title to real property, a vehicle, a vessel or an aircraft; or (4) involves the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce.</p>
<b>Intelligence Reform &amp; Terrorism Prevention Act of 2004</b>	<p>Intelligence Reform &amp; Terrorism Prevention Act of 2004: The legislation amended the BSA to require the Secretary of the Treasury to prescribe regulations requiring certain financial institutions to report cross-border electronic transmittals of funds if the Secretary determines that such reporting is “reasonably necessary” to aid in the fight against money laundering and terrorist financing</p>
<b>Financial Action Task Force (FATF)</b>	<p>The <b>FATF</b> is an intergovernmental organization that develops standards around <a href="#">Anti Money Laundering (AML)</a> to promotes policies and standards to combat the financial crime of money laundering and terrorism funding. Additionally, FATF produces two lists of uncooperative jurisdictions in efforts against money laundering (and terrorism financing).</p>

71)

Virtual Currencies in the Money Laundering Scheme, [Money Laundering Scheme](#), 24 August 2015, Accessed: 7 April 2022,

<https://www.acamstoday.org/virtual-currencies-money-laundering-cycle/money-laundering-table/>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:48\\_natsec:40\\_launder](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:48_natsec:40_launder)

Last update: **2022/05/18 21:38**



## 4.6 International Considerations

[Return to Common Elements](#) | [Provide Feedback](#)

### Overview

[Return to Top](#)

The [Bank for International Settlements \(BIS\)](#) has produced a paper on Central Bank Digital Currencies discussing the foundational principles and core features of a CBDC. The following is an excerpt from the Executive Summary:<sup>72)</sup>

*CBDC issuance and design are sovereign decisions to be made by each jurisdiction. This report is not about if or when to issue a CBDC. Central banks will make that decision for their jurisdictions (in consultation with governments and stakeholders). None of the central banks contributing to this report have reached a decision on whether to issue a CBDC. Instead, this report advances the foundational international work by outlining common principles and the key features a CBDC and supporting infrastructure would need in order to contribute to central bank public policy objectives.*

*The principles emphasize that:*

- (i) a central bank should not compromise monetary or financial stability by issuing a CBDC;*
- (ii) a CBDC would need to coexist with and complement existing forms of money; and*
- (iii) a CBDC should promote innovation and efficiency. The possible adverse impact of a CBDC on bank funding and financial intermediation, including the potential for destabilizing runs into central bank money, has been a concern of central banks.*

*Any decision to launch a CBDC would depend on an informed judgment that these risks can be managed, likely through some combination of safeguards incorporated in the design of a CBDC and financial system policies more generally. Understanding the potential market structure effects of CBDC, their implications for financial stability, and any potential mitigants is a further area of work for this group.*

The Federal Reserve has suggested “Desirements”<sup>73)</sup> in a **White Paper** named [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#). These “Desirements” were captured and summarized in a [White Paper Analysis](#) conducted by the [Object Management Group](#). Ultimately, these “Desirements” need to be incorporated into a **CBDC Data Strategy** following the guidelines set by the U.S. government for government entities to develop a Federal Data Strategy.

The Federal Reserve has suggested a “Desirement” have the CBDC used internationally and as a mechanism to transfer funds across borders. These “Desirements” need to be added to a Federal Reserve CBDC Data Strategy. For more information, the OMG DIDO-RA provides a discussion on [Federal Data Strategy](#). The Federal Reserve and the implementation of the CBDC should formulate their own

**Federal Data Strategy.** The Data Strategy should also address matters covered in Section [4.4 National Privacy Considerations](#).

Since the Federal Reserve is striving for a CBDC with international appeal, it also needs to develop a Data Strategy, covering [Data Governance, Compliance and Regulation](#). Table 52 provides some insight into data governance the CBDC needs as part of a **Data Strategy**.

Table 52: Governance issues associated with “data storage”

<b>Data Residency</b> ‡	<b>Data Residency</b> is the set of issues and practices related to the location of data and metadata, the movement of (meta)data across geographies and jurisdictions, and the protection of that (meta)data against unintended access and other location-related risks <sup>74)</sup>
<b>Data Sovereignty</b>	<b>Data Sovereignty</b> is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located.
<b>Data Localization</b> ‡	<b>Data Localization</b> is the act of storing data on any device that is physically present within the borders of a specific country where the data was generated.

‡ **Note:** **Data Localization** and **Data Residency** are sometimes mistakenly used interchangeably. On its own, *Data Residency* refers to the place where data is stored. *Data Residency* requirements often compel organizations to change where the data resides. *Data Localization* is the action of complying with *Data Residency* requirements.<sup>75)</sup>

## Governance Issues Associated with Data Storage

- [4.6.1 Data Residency](#)
- [4.6.2 Data Localization](#)
- [4.6.3 Data Sovereignty](#)

## Examples

[Return to Top](#)

The following “Desirements” are from the [White Paper](#) as identified by the [Object Management Group's](#) report called [White Paper Analysis](#):

Table 53: Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG

Category	Desirements
<b>Benefits</b>	B0009, B0015, B0035, B0036, B0041, B0052
<b>Policies</b>	P0004, P0005, P0006, P0012, P0023, P0024, P0028
<b>Risks</b>	R0014


<b>Category</b>	<b>Desirements</b>
<b>Design</b>	D0013, D0015, D0016, D0017

**Note:** B = Benefit, P = Policy, R = Requirement, D = Design.

## Example Discussion

[Return to Top](#)

Table 54: "Desirements" identified in the **White Paper** that have potential international impacts.

Statement No.	Statement	Comment
<b>B0009</b>	<b>Provide faster and cheaper payments (including cross-border payments)</b>	<p>There is a lot of promise coming from the Blockchain world vis-a-vis decentralization and transactions per second, To a large extent this is driving the Stablecoin Desirements such as: <b>B0016, B0017, P0015, P0016, R0022</b>. These promises of a a global and international game changer has performance and cost issues.</p> <p> <a href="#">Figure 15: Cryptocurrencies Transactions Speeds compared to Visa and Paypal<sup>76)</sup></a>  <i>For now, any time a new blockchain starts making promises about "beating Visa's 24,000 tps", be skeptical and examine the fine print. IOTA's meant to be fast and scalable, but like a kid who's terrified of removing the stabilizers from their bike, it still doesn't function without its coordinator. Hashgraph is also meant to be fast, but it comes with threats to sue anyone who tries to fork it and any blockchain that can be sued isn't a decentralized network. Come to think of it, it's more like Visa.<sup>77)</sup></i>                      In addition to the speed issues, there are huge costs associated with consensus. See the OMG DIDO-RA discussion on Consensus Platforms.  <b>Note:</b> However, this does not mean the Federal Reserve should not continue to have Research Development Test &amp; Evaluation (RDT&amp;E) Funding into Blockchains or Stablecoin.  <b>Note:</b> See: <b>B0041</b>.</p>

Statement No.	Statement	Comment
B0015	<p><b>Reduce cross-border costs to benefit:</b></p> <ol style="list-style-type: none"> <li><b>1. NO economic growth</b></li> <li><b>2. enhance global commerce</b></li> <li><b>3. improve international remittances</b></li> <li><b>4. NO reduce inequality</b></li> </ol>	<p>The U.S. Dollar is already an international global currency. <i>According to the International Monetary Fund, the U.S. dollar is the most popular [currency]. As of the fourth quarter of 2019, it makes up over 60% of all known central bank foreign exchange reserves. That makes it the de facto global currency, even though it doesn't hold an official title.</i> <sup>78)</sup></p> <p>However, even though the U.S. Dollar is the <i>de facto</i> world currency, it is partially because it is perceived as a neutral, unbiased, well-managed, and transparent commodity. If the CBDC were to change the rules to make it less well-managed, neutral, unbiased, and transparent there will be serious challenges to the U.S. Dollar. Part of the explanation for Bitcoins' adoption was that transactions were perceived to be beyond the purview of the U.S. government, in specific, but other governments as well. <i>Despite trillions of dollars in foreign debt and continuous large deficit spending, the United States still holds global trust and confidence in its ability to pay its obligations. For this reason, the U.S. dollar remains the strongest world currency. It may continue to be the top global currency in the years to come. The dollar's current number one status is under contention though. Countries such as China and Russia feel a new one-world currency, one not backed by any one nation, is overdue in this increasingly integrated global economy.</i> (Kimberly Amadeo, <a href="https://www.thebalance.com/world-currency-3305931">Why the US Dollar Is the Global Currency</a>, The Balance 16 March 2022, Accessed: 10 April 2022, <a href="https://www.thebalance.com/world-currency-3305931">https://www.thebalance.com/world-currency-3305931</a> ))</p> <p>Part of the reservation about the U.S. Dollar is also attributable to the Snowden revelation. See: <a href="#">Data Sovereignty</a> and MacAskill and Dance. <sup>79)</sup></p>
B0035	<p><b>Streamline cross-border payments by using:</b></p> <ol style="list-style-type: none"> <li><b>1. NO new technologies</b></li> <li><b>2. introducing simplified distribution channels</b></li> <li><b>3. creating additional opportunities for cross-jurisdictional collaboration and interoperability</b></li> </ol>	See B0015.
B0036	<p><b>Preserve the dominant international role of the U.S. dollar</b></p>	See B0015.



Statement No.	Statement	Comment
<b>B0041</b>	<b>Support streamlining cross-border payments</b>	<p>The <a href="#">Bank for International Settlements (BIS)</a> has produced a paper for the G20 on <a href="#">Central bank digital currencies for cross-border payments</a><sup>80)</sup></p> <p><i>Cross-border payments with CBDCs can be envisioned in two fundamentally different ways:</i></p> <ol style="list-style-type: none"> <li>1. <i>A retail CBDC of a given jurisdiction becomes available to anybody inside and outside of that jurisdiction, with no specific coordination between the issuing central banks</i></li> <li>2. <i>Access and settlement arrangements are established among different retail and/or wholesale CBDCs, built on strong cooperation among central banks</i></li> </ol> <p><i>In the first scenario of international use, the CBDC, being digital, could be designed so that it faces no constraints on where and by whom it is used. If the design allows for anonymous payments like cash, it would by default be accessible to foreign residents. In practice, however, relatively few central banks are considering fully anonymous systems (Auer, Cornelli, and Frost (2020)). Alternatively, and in contrast to cash, a CBDC could be designed so as to be subject to certain restrictions on cross-border use imposed by the issuing central bank.</i></p> <p><i>In the second scenario, coordination and cooperation among central banks would favor less disruptive approaches. This could happen either by allowing foreigners from partnering jurisdictions to access the domestic CBDC solution or by means of multi-CBDC (CBD) arrangements.<sup>12</sup> These are coordinated design frameworks including technological, market structure, and legal aspects, aiming to facilitate cross-border interoperability of multiple CBDCs from different jurisdictions.</i></p>
<b>B0042</b>	<b>Preserve the dominant international role of the U.S. dollar</b>	See <b>B0015</b> .

Statement No.	Statement	Comment
B0052	Prevent Financial money laundering crimes	<p>There is already a rich legal framework in place to cope with <a href="#">Money Laundering</a> within the U.S.; many of these can help prevent money laundering across U.S. borders. One example is the <a href="#">US Patriot Act, Title III: Anti-money-laundering to prevent terrorism of 2001</a>, especially the</p> <ol style="list-style-type: none"> <li>1. The <a href="#">First Subtitle</a> deals primarily with strengthening banking rules against money laundering, especially on the international stage</li> <li>2. The <a href="#">Third Subtitle</a> deals with currency smuggling and counterfeiting, including quadrupling the maximum penalty for counterfeiting foreign currency.</li> </ol> <p>Also, <a href="#">18 U.S. Code § 1956 - Laundering of monetary instruments</a> has provisions for international situations:</p> <ol style="list-style-type: none"> <li>3. Unlawful activity, certain offenses against <b>foreign</b> nations</li> <li>4. The defendant knew that the property involved was the proceeds of any felony under State, Federal or <b>foreign</b> law</li> <li>5. Defines “<i>financial transactions</i>” to include interstate or foreign commerce</li> </ol> <p><b>Note:</b> These laws and regulations need to be reviewed when a U.S. CBDC design is finally ready for testing to ensure the framework is still adequate to protect criminal activities and that CBDC does not open loopholes and backdoors.</p>
P0004	Protect consumer privacy	<p>Internationally, a major method of protecting consumer privacy is referred to as <a href="#">Data Localization</a>. This section includes examples from Russia, China, India, European Union, and Brazil.</p> <p>Data Localization policies classification <sup>81)</sup> is summarized below:</p> <p><b>Local-only Storing, Transmission, and Processing:</b> This generally means an obligation to locally manage data or a prohibition of international data transfers. This is the strictest type of localization policy and is more likely to be descriptive of nations seeking broader control over citizen activities.</p> <p><b>Local Copy Required:</b> Companies are required to keep a copy of data in local servers or data centers. This allows for easier access to this data for regulation and law enforcement purposes, i.e., it is generally easier for local law enforcement agencies to access data stored locally than it is for them to access data stored in another jurisdiction.</p> <p><b>Narrower, conditional restrictions:</b> Transfers of data outside the country are only permitted if certain conditions are met by the transferee and/or by the recipient country.</p>

Statement No.	Statement	Comment												
P0005	Protect against criminal activity	<p>There is already a rich legal framework within the U.S. to protect against criminal activity, which includes international activities (see the <a href="#">Details of National Security Considerations</a>). Many of these laws and regulations are already well established and operational on the international level.</p> <p>Some examples:</p> <p><b>Human Trafficking:</b> <a href="#">Intelligence Reform and Terrorism Prevention Act of 2004</a> The <b>Intelligence Reform and Terrorism Prevention Act, section 7202</b> established the Human Smuggling and Trafficking Center to achieve greater integration and overall effectiveness in the U.S. government's enforcement and other response efforts, and to work with foreign governments to address the separate but related issues of alien smuggling, trafficking in persons, and criminal support of clandestine terrorist travel.</p> <p><b>Drug Trafficking:</b> <a href="#">18 U.S. Code § 1952 - Interstate and foreign travel or transportation in aid of racketeering enterprises</a> Five years maximum for traveling or using the mail or instruments of interstate commerce (telephone/<b>internet</b>) with intent to facilitate drug trafficking.</p> <p>Table 54: Summary of the number of laws and regulations covering National Security Considerations.</p> <table border="1" data-bbox="618 972 1502 1266"> <thead> <tr> <th data-bbox="618 972 1097 1052">National Security Consideration</th> <th data-bbox="1097 972 1502 1052">No. of Laws and Regulations</th> </tr> </thead> <tbody> <tr> <td data-bbox="618 1052 1097 1094"><b>Human Trafficking</b></td> <td data-bbox="1097 1052 1502 1094">14</td> </tr> <tr> <td data-bbox="618 1094 1097 1136"><b>Drug Trafficking</b></td> <td data-bbox="1097 1094 1502 1136">9</td> </tr> <tr> <td data-bbox="618 1136 1097 1178"><b>Corruption</b></td> <td data-bbox="1097 1136 1502 1178">10</td> </tr> <tr> <td data-bbox="618 1178 1097 1220"><b>Money Laundering</b></td> <td data-bbox="1097 1178 1502 1220">11</td> </tr> <tr> <td data-bbox="618 1220 1097 1266"><b>Total</b></td> <td data-bbox="1097 1220 1502 1266"><b>44</b></td> </tr> </tbody> </table> <p><b>Note:</b> These laws and regulations need to be reviewed when a U.S. CBDC design is finally ready for testing to ensure the framework is still adequate to protect criminal activities and that CBDC does not open loopholes and backdoors</p>	National Security Consideration	No. of Laws and Regulations	<b>Human Trafficking</b>	14	<b>Drug Trafficking</b>	9	<b>Corruption</b>	10	<b>Money Laundering</b>	11	<b>Total</b>	<b>44</b>
National Security Consideration	No. of Laws and Regulations													
<b>Human Trafficking</b>	14													
<b>Drug Trafficking</b>	9													
<b>Corruption</b>	10													
<b>Money Laundering</b>	11													
<b>Total</b>	<b>44</b>													
P0006	Garner broad support from key stakeholders	<p>See <a href="#">4.1 Stakeholders</a>. The primary international stakeholders in the CBDC effort are identified in <a href="#">non-U.S. Federal Government Oversight Authorities</a>. This is a minimum set and could include more countries and specific agencies within these countries.</p>												

Statement No.	Statement	Comment
P0012	<b>The firms that operate interbank payment services are subject to federal supervision</b>	<p>This is highly dependent on the <a href="#">Currency Model</a> or mix of currency models chosen to implement the U.S. CBDC. Existing intermediaries must already follow:</p> <ol style="list-style-type: none"> <li>1. <a href="#">Know Your Customer (KYC)</a></li> <li>2. <a href="#">Customer Due Diligence</a></li> </ol> <p>As well as take steps to prevent Money Laundering, such as:</p> <ol style="list-style-type: none"> <li>1. Deposit of illicit funds into the financial system</li> <li>2. Transactions designed to conceal the illicit origin of the funds, known as “layering”</li> <li>3. Use of laundered funds to acquire real estate, financial instruments, or commercial investments</li> </ol> <p>U.S. Federal law requires a person to report cash transactions of more than \ \$10,000 by filing IRS Form 8300 PDF, Report of Cash Payments Over \ \$10,000 received in a Trade or Business. <sup>82)</sup></p> <p><b>Note:</b> These laws and regulations need to be reviewed when a U.S. CBDC design is finally ready for testing to ensure the framework is still adequate to protect criminal activities and that CBDC does not open loopholes and backdoors. This means that all new intermediaries are subject to the same rules.</p>
P0023	<b>CBDC would need to be readily transferable between customers of different intermediaries</b>	<p>This requires international agreement on the details of what constitutes a transfer, the rules of the transfers, limits or restrictions on the transfers, etc. Although there are already agreements using the existing systems, these are often too slow for modern expectations. Even though streamlining transfer processing using technologies such as Blockchain is promising (in order to reduce the time it takes to do a transfer) this should in no way mean that the rules can be ignored.</p>
P0024	<b>CBDC would need to comply with the U.S. robust rules</b>	<p>Most of the international agreements have to do with the detection and prevention of <a href="#">National Security</a> which is a broad, extensive topic that requires an understanding of the U.S. Laws and Regulations, as well as, international treaties and agreements. Within the context of the CBDC, criminal activity can be one or more of the following:</p> <ol style="list-style-type: none"> <li>1. <a href="#">Human Trafficking</a></li> <li>2. <a href="#">Drug Trafficking</a></li> <li>3. <a href="#">Corruption</a></li> <li>4. <a href="#">Money Laundering</a></li> </ol>

Statement No.	Statement	Comment
P0028	<p><b>Require significant international coordination to address issues such as:</b></p> <ol style="list-style-type: none"> <li><b>1. common standards</b></li> <li><b>2. infrastructure,</b></li> <li><b>3. the types of intermediaries able to access any new infrastructure,</b></li> <li><b>4. legal frameworks</b></li> <li><b>5. preventing illicit transactions</b></li> <li><b>6. the cost and timing of implementation</b></li> </ol>	

72)

Bank for International Settlements (BIS), Report no 1, Central Bank Digital Currencies - foundational principles and core features, ISBN: 978-92-9259-427-5 (online) 2020, Accessed: 8 April 2022, <https://www.bis.org/publ/othp33.pdf>

73)

**Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired, but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

74)

Cloud Standards Customer Council and the Object Management Group, Data Residency Challenges, May 2017, Accessed: 8 April 2022, <https://www.omg.org/cloud/deliverables/CSCC-Data-Residency-Challenges.pdf>

75)

Cloudflare, What is data localization?, Accessed: 8 April 2022, <https://www.cloudflare.com/learning/privacy/what-is-data-localization/>

76)

HowMuch.net, Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?, Accessed: 15 May 2022, <https://howmuch.net/articles/crypto-transaction-speeds-compared>

77)

Kai Sedwick, No, Visa Doesn't Handle 24,000 TPS and Neither Does Your Pet Blockchain, Bitcoin.com April 10, 2022, Accessed 10 April 2022, <https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/>

78)

Kimberly Amadeo, Why the US Dollar Is the Global Currency, The Balance 16 March 2022, Accessed: 10 April 2022, <https://www.thebalance.com/world-currency-3305931>

79)

Ewen MacAskill and Gabriel Dance, The Guardian, NSA Files: Decided - What the revelations mean for you, 1 November 2013, Accessed: 9 April 2022, <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

80)

Bank for International Settlements (BIS) - Committee on Payments and Market Instructions, Central bank

digital currencies for cross-border payments, July 2021, Accessed: 10 April 2022,  
<https://www.bis.org/publ/othp38.pdf>

81)

Emily Wu, Harvard Kennedy School - Belfer Center - For Science and International Affairs, Sovereignty and Data Localization, July 2021, Accessed: 9 April 2022,

<https://www.belfercenter.org/publication/sovereignty-and-data-localization>

82)

Internal Revenue Service, Cash payment report helps government combat money laundering, Accessed 2 March 2022,

<https://www.irs.gov/newsroom/cash-payment-report-helps-government-combat-money-laundering>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:50\\_international:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:50_international:start)

Last update: **2022/05/18 22:11**



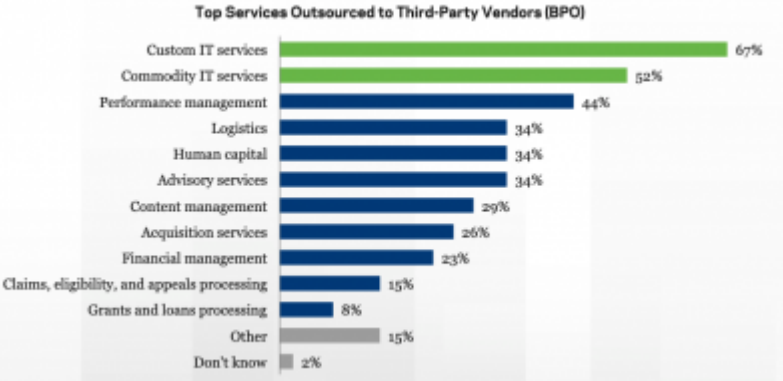
## 4.6.1 Data Residency

[International Considerations](#) [Provide Feedback](#)

According to the OMG Cloud Working Group's Discussion Paper on Data Residency<sup>83</sup>). The **Data Residency** issues from the **Cloud Working Group Data Residency White Paper** are summarized in Table 55 with each issue being given a unique number.

Table 55: A review of the Data Residency Issues the CBDC needs to address.

<b>Data Residency Issue Number</b>	<b>Description</b>	<b>CBDC Explanation</b>
<b>DR01</b>	<b>Large multinational companies wish to consolidate data centers from multiple countries into a smaller set of locations (data center consolidation).</b>	Although a U.S.-based CBDC is not a multinational company, it is, by nature, a multinational enterprise. A summary of the multinational nature of the CBDC found in OMG <a href="#">White Paper Analysis</a> follows: 1. <b>B0036</b> and <b>B0042</b> set as a “desirement” the preservation the dominance of the U.S. Dollar internationally 2. <b>B0009</b> , <b>B0024</b> , <b>B0034</b> , <b>P0026</b> express the “need for speed” 3. <b>B0027</b> expressed the need for trust and reliability 4. <b>B0053</b> is resiliency 5. <b>B0009</b> , <b>B0015</b> , <b>B0035</b> , <b>B0041</b> for the need of cross-border operations 6. <b>D0009</b> to support foreign demand
<b>DR02</b>	<b>Organizations migrate some of their services to the cloud or to a hosted solution managed by an outsourcing company located in another country. “Services” is a very broad term here, and risk arises simply if a remote backup solution stores the backup data in another country.</b>	For the same reasons given in the explanation for <b>DR01</b> above, the CBDC has an implied “desirement” for cloud-based data collection and the redundancy it offers. In addition, <b>B0051</b> , and <b>D0011</b> both refer to data collection, which can cause Data Residency issues when data is from outside U.S. sources.

Data Residency Issue Number	Description	CBDC Explanation
DR03	<p><b>A Business Process Outsourcing (BPO) solution, or a managed helpdesk solution, causes agents in a different country to have access to protected information in order to perform the contracted service.</b></p>	<p>Figure 16 provides a list of the top services to outsource to third Party BPOs. Some of these are relatively benign in terms of data visibility by BPO employees. Other areas such as “<i>Information Technology(IT)</i>” and “<i>Claims, eligibility, and appeals processing</i>” might need to be addressed for any CBDC implantation.</p>  <p>Figure 16: Federal Managers report that BPO is used for a wide range of services<sup>84)</sup></p>
DR04	<p><b>Employees travel across borders, carrying sensitive data with them on their laptops and smartphones.</b></p>	<p>For the U.S. CBDC, it is not about employees traveling across borders as much as U.S.-based citizens and residents traveling across the border. Even if the people do not travel across the borders, their money may travel through international purchases and remittances.</p>

For the CBDC, the Data Residency issues **DR01**, **DR01** will cause issues if the CBDC obtains international usage and will probably reduce adoption of the U.S. Dollar which are among the stated desirements the Federal Reserve **White Paper**. See Table 55.

Table 55: International “desirements” specified in the Federal Reserve **White Paper**.

Statement No.	Statement
<b>B0036</b>	<b>Preserve the dominant international role of the U.S. dollar</b>
<b>B0041</b>	<b>Support streamlining cross-border payments</b>
<b>B0042</b>	<b>Preserve the dominant international role of the U.S. dollar</b>

The level of risk to the CBDC mostly depends on several factors in how the design of the CBDC and the international laws and regulations that will ultimately cover the CBDC. The **Cloud Working Group Data Residency White Paper** identified four major risk areas which have relevance to the CBDC:

1. Nature of the being gathered and stored by the CBDC
2. Severity of the laws and regulations governing data in the jurisdiction where the data resides, passes through, or is being manipulated
3. Nature of the services the CBDC will offer internationally
4. Level of awareness (or ignorance) of the issues by international communities

The **Cloud Working Group Data Residency White Paper** (see Table 17) uses a series of Use-Cases to



help explain how to classify data usage and when there might be **Data Residency** issues. The table lists each Use-Case and where it is being generated, stored, processed, routed, and finally accessed by the End User. In other words, the [State of the Data](#):

- [Data-At-Rest](#)
- [Data-In-Process](#)
- [Data-In-Use](#)

Use Case Description	Data Source Location	Data Storage Location	Application Execution Location	Network Path	End User Location
Classical in-house hosted process	In-house	In-house	In-house	In-house	In-house
Hybrid Cloud execution services (data mining, seismic processing) with in-country cloud provider	In-house	In-house	In-country	In-country	In-house
In-country public cloud-based process (e.g., a CRM solution)	In-house	In-country	In-country	In-country	In-house
Outsourced (3rd party location), In-country cloud process	In-house	In-country	In-country	In-country	In-country
As above, with the data also supplied from outside of the organization's premises (e.g., data entered on an ATM)	In-country	In-country	In-country	In-country	In-country
Emerging world location with in-house hosted process, external network paths (e.g., satellite ground station, Internet routing)	In-country	In-house	In-house	External	In-house
Emerging world location with In-country cloud and external network paths (e.g., satellite ground station, Internet routing)	In-country	In-country	In-country	External	In-country
Hybrid Cloud execution services (data mining, seismic processing) with an out-of-country cloud provider	In-house	In-country	External	External	In-house
As above, with end users also located out of the country	In-country	In-country	External	External	External
Citrix/MTS access to host country. Data loading, QC (i.e., user processes/manipulates but does not typically view data)	In-country	In-country	In-country	External	External
Citrix/MTS access to host country. Metadata access (job logs, backups, DBA)	In-country	In-country	In-country	External	External
Offshore-hosted and outsourced business process	In-country	External	External	External	External
Cloud/hosting services outside of host country	In-country	External	External	External	In-house
Restricted data on mobile devices when end user is out of host country	In-House	External	External	External	External

The table is color-coded as follows:

	No data residency-related risk
	Low risk – assess and monitor risk
	Medium risk – specific measures are strongly desirable
	High risk – strong specific measures are required

Figure 17: Data Residency Use Case Matrix from the **Cloud Working Group Data Residency White Paper**.

Table 56 gives an explanation for the values in each of the cells in Figure 17.

Table 56: Where the data is stored (i.e., [Data at Rest](#).)

<b>In-country</b>	Data is physically present within the boundaries of the jurisdiction in question. When this location is on the physical premises of the data custodian, it is equivalent to in-house
-------------------	--

<b>In-house</b>	Data is present within the physical premises of the data custodian. Whether this is a single (computer) room, building or campus is not germane. What is germane is whether the storage, servers and network infrastructure are all privately controlled by the data custodian. As a specific case, if two locations are physically separate and connected by an Internet connection, this criterion would be violated. Examples of data sources that are in-country but not in-house are a well-site sensor on a private owner's oil lease and an automatic teller machine (ATM) is in an International airport, on a ferry, or on a cruise ship.
<b>External</b>	One or more infrastructure components (storage, servers, network) are outside the jurisdiction in question. An example is a seismic vessel acquiring data within the territorial waters of a country. The acquisition process is being monitored by personnel physically within that country. The data is transmitted via satellite to a ground station located in another country (e.g., Russian Arctic via a Norwegian ground station, offshore Indonesia via a Singapore ground station, etc.) and then via the Internet to the company's home country

83)

Cloud Standards Customer Council and the Object Management Group, [Data Residency Challenges](#), May 2017, Accessed: 8 April 2022,

<https://www.omg.org/cloud/deliverables/CSCC-Data-Residency-Challenges.pdf>

84)

Government Business Council, [Inside Federal Outsourcing - A Candid Survey of Federal Managers](#), May 2015, Accessed: 8 April 2022,

[http://cdn.govexec.com/media/gbc/docs/gbc\\_government\\_outsourcing\\_report.pdf](http://cdn.govexec.com/media/gbc/docs/gbc_government_outsourcing_report.pdf)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:50\\_international:10\\_residency](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:50_international:10_residency)

Last update: **2022/05/18 21:38**

## 4.6.2 Data Localization

[International Considerations](#) [Provide Feedback](#)

**Data localization** is about jurisdictions adopting policies with an aim to protect the jurisdictions' sovereignty over the data generated from within its geographic boundaries or from its residents. The policies are intended to help protect the jurisdiction and its residents from external entities (private or public).

Figure 18 shows the increase in **Data Localization** measures globally from 1960-2015. This increase indicates that this is a problem that will only get bigger as time goes by. The CBDC needs to understand and recognize it as a growing international trend.

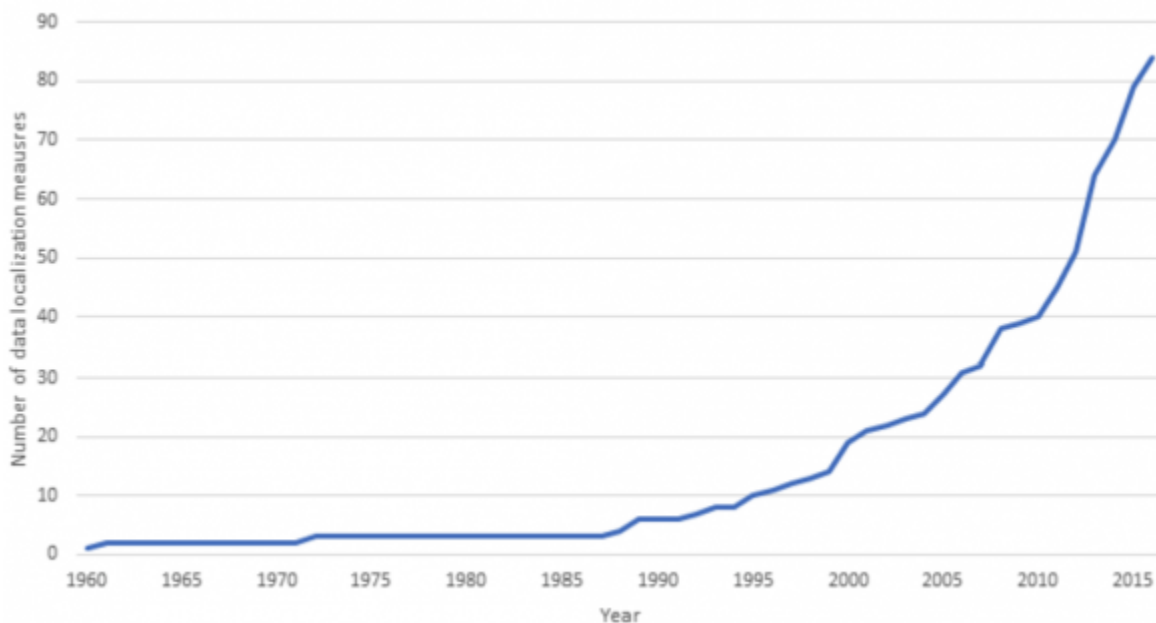


Figure 18: Increase in data localization measures globally (1960 - 2015)<sup>85)</sup>

The need for **Data Localization** is justified for different reasons, such as the protection of data from:

- [Hackers](#) engaged in nefarious activities.
- [Personal Identifiable Information \(PII\)](#)
- Regulators wanting to access the information on participants in cross-border transactions
- External jurisdictions trying to identify individuals engaged in activities it finds illegal or offensive, but that are not considered that way locally
- Unwanted or desired commercial mining
- Public opinion favoring in-country data storage solutions and strategies

This usually takes the form of a mandate and/or a set of laws or regulations that require certain data to be physically stored on servers within the country of origin.

Data Localization policies tend to fall into three categories<sup>86)</sup>:

Table 57: Data Localization Policies. See: <sup>87)</sup>

Localization Category	Description	Law or Regulation Examples
<b>Local-only Storing, Transmission, and Processing</b>	<b>This generally means an obligation to locally manage data or a prohibition of international data transfers. This is the strictest type of localization policy and is more likely to be descriptive of nations seeking broader control over citizen activities.</b>	<p><b>Russia</b> Under Russia’s Federal Law No. 242-FZ, operators must ensure the recording, systematization, accumulation, storage, adjustment (update, alteration), and retrieval of personal data of citizens of the Russian Federation will be performed through database servers located in the territory of the Russian Federation. Substantial fines are imposed on organizations and individuals that fail to comply with data localization requirements.</p> <p><b>China</b> Article 37 of the Cybersecurity Law of the People’s Republic of China (‘CSL’) requires critical information infrastructure operators (‘CIIOs’) to store personal information and important data generated from critical information infrastructure in China. These requirements are likely to be expanded by the Personal Information Protection Law, the draft of which was released in October 2020.</p>
<b>Local Copy Required</b>	<b>Companies are required to keep a copy of data in local servers or data centers. This allows for easier access to this data for regulation and law enforcement purposes, i.e., it is generally easier for local law enforcement agencies to access data stored locally than it is for them to access data stored in another jurisdiction.</b>	<p><b>India</b> Under India’s Personal Data Protection Bill, sensitive personal data (which includes financial information) must be stored in India, but a copy of the data can be transferred internationally if certain requirements are met. These include:</p> <ol style="list-style-type: none"> <li>1. The data principal provides explicit consent, the transfer is made pursuant to a contract or intra-group scheme approved by the Data Protection Authority</li> <li>2. The government has deemed a country to provide adequate protection</li> <li>3. The Data Protection Authority has specifically authorized the transfer</li> </ol>

Localization Category	Description	Law or Regulation Examples
<p><b>Narrower, conditional restrictions</b></p>	<p><b>Transfers of data outside the country are only permitted if certain conditions are met by the transferee and/or by the recipient country.</b></p>	<p><b>European Union</b>                      Under the EU’s GDPR, the transfer of personal data outside the European Economic Area is permitted only where:                      1. The recipient is in a territory considered by the European Commission to offer an adequate level of protection for personal data                      2. Safeguards are in place, such as binding corporate rules approved by Data Protection Authorities                      3. A legal exemption applies, such as where data subjects provide explicit consent, the transfer is necessary to fulfill a contract or there is a public interest founded in EU or member state law</p> <p><b>Brazil</b>                      Under the General Personal Data Protection Law (LGPD) international data transfers are only permitted in certain situations, including when recipient countries ensure an adequate level of data protection, when approved legal mechanisms (such as model contract clauses) are employed or when data subjects have provided their consent.</p>

85) 86) 87)

Emily Wu, Harvard Kennedy School - Belfer Center - For Science and International Affairs, Sovereignty and Data Localization, July 2021, Accessed: 9 April 2022, <https://www.belfercenter.org/publication/sovereignty-and-data-localization>

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:50\\_international:20\\_local](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:50_international:20_local)

Last update: **2022/05/18 21:38**



## 4.6.3 Data Sovereignty

[International Considerations](#) [Provide Feedback](#)

**Data Sovereignty** is concerned with any jurisdictions' laws and regulations covering any data collection or processing done within that jurisdiction, governing the data. **Data Sovereignty** differs from **Data Residency** in that Data Residency reflects a business decision on where to store and process data, often based on **Data Sovereignty** Laws and Regulations applicable to a particular jurisdiction.

Much of the current interest in **Data Sovereignty** by jurisdictions (i.e., Countries) around the world is traceable to the revelations made public of U.S. activities of surveillance and collecting data globally on people (i.e., internally and externally to the U.S.) <sup>79)</sup>. The simplest way to look at **Data Sovereignty** is to consider national [Privacy Considerations](#) and preventing data stored in a foreign country from subpoenas by the host country's government.

A globally accepted U.S. CBDC needs to take the Data Sovereignty issues seriously if there is any hope of *"Preserving the dominant international role of the U.S. dollar (B0036)*

A theoretical example of how complicated a globally accepted U.S. CBDC would be:

- Assume U.S. CBDC transactions that occur in the E.U. are stored and processed in the U.K.
- A U.S. CBDC transaction occurs in Italy and would be subject to the **Data Sovereignty** laws and regulations of Italy and the EU.
- However, since the data is stored and processed in the U.K., the data would be subject to the data sovereignty rights of the U.K. as Italy and the E.U.
- To further complicate matters, U.S. CBDC transactions made and stored in the U.K. are backed up on servers in Ireland, making the CBDC transaction also subject to the data **Sovereignty Rights** of Ireland too.

A real-world example of **Data Sovereignty** issues is [Microsoft's Data Privacy Case vs. the DoJ](#)<sup>80)</sup>:

*Microsoft's case against the US Department of Justice (DoJ) was also a high-profile event that further highlighted the importance of data sovereignty.*

*After the DoJ ordered the tech company to grant access to emails stored in Ireland-based servers related to a narcotics investigation in 2013, Microsoft had refused to comply with the Department of Justice's request.*

*Despite that Microsoft stating that complying with the request would break the data privacy laws of the European Union, the initial ruling ordered the company to fulfill the DoJ's request.*

*However, later on, after Microsoft won the appeal and the DoJ changed its data-related policies.*

The adoption of U.S. CBDC could break traditional geopolitical barriers more than ever before, especially depending on the [Currency Model](#) selected. Depending on the perception of privacy protection of the CBDC, many countries may amend existing laws and regulations or greatly restrict the use of a U.S.

CBDC.

The U.S. CBDC needs to be completely honest and open about where data:

- Servers are hosted (i.e., [Data-At-Rest](#))
- Flows over networks (i.e., [Data-In-Motion](#))
- Is processed (i.e., [Data-In-Use](#))

79)

Ewen MacAskill and Gabriel Dance, The Guardian, [NSA Files: Decided - What the revelations mean for you](#), 1 November 2013, Accessed: 9 April 2022, <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>

80)

Benjamin Vitaris, Permission.io, [What Is Data Sovereignty? Everything You Need to Know](#), 11 August 2020, Accessed: 9 April 2022, <https://permission.io/blog/data-sovereignty/>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:15\\_common:50\\_international:30\\_overn](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:15_common:50_international:30_overn)

Last update: **2022/05/17 20:59**





# 4.7 Dual Payment Networks

[Return to Common Elements](#) [Provide Feedback](#)

## Overview

[Return to Top](#)

**Note:** Also see:

- [4.4 National Privacy Considerations](#)
- [4.5 National Security Considerations](#)
- [4.6 International Considerations](#)
- [Answer to Question: 04. How might a U.S. CBDC affect the Federal Reserve's ability to effectively implement monetary policy in the pursuit of its maximum-employment and price-stability goals?](#)

The simplest way to add a U.S. CBDC would be to build a parallel payment transaction network to the existing [Automated Clearing House \(ACH\) Network](#). The existing payment network would continue to function "as-is", while the new real-time U.S. CBDC Network would handle payment transactions using the U.S. CBDC (probably a Stablecoin).

**Note:** The ACH has embarked on its own support for real-time transactions with [Real-Time Payments \(RTP\) Network](#). This should not be confused with the Stablecoin or other Crypto solutions.

Both networks would rely on the existing intermediary financial institutions to continue to do what they already do in terms of [Privacy](#), [National Security](#), and [International Security](#) BUT with the addition of the ability to use a real-time U.S. CBDC transfer mechanism instead of only the existing [Automated Clearing House \(ACH\) Network](#). This allows the existing mechanisms that are part of the existing intermediaries structure to remain in place for Privacy and Security. This of course assumes the existing mechanism on Privacy and Security is acceptable.

However, it would also be possible for new financial intermediaries to startup but they would only be allowed to use the U.S. CBDC payment network. These new financial intermediaries would **NOT** be released from following the existing Laws and Regulations of the traditional financial intermediaries. In other words, they would have to ensure the End User's privacy (both ends of the Payment Transactions). They would also have conform to all the [National Security Laws and Regulations](#). If either End User in the Payment Transaction is not in the U.S., they would have to abide by all the [International Laws and Regulations](#). This would mean these new Intermediaries would be subject to oversight and auditing.

The new U.S. CBDC network handles the real-time transaction requirements of the U.S. CBDC. This requires the:

Table 58: Theoretical components of a Dual ACH / CBDC System



- Development of a U.S. CBDC is probably based on Stablecoin Model.
- Use of an energy-efficient [Consensus Algorithm](#)
- Development of a **bridge** between the existing [Automated Clearing House \(ACH\) Network](#) and the new U.S. CBDC Network
- Development of a new standardized [Application Programming Interface \(API\)](#) to connect the outside world to the newly enhanced combined ACH Network and CBDC Network for the existing intermediaries to use for transfers

**Note:** The [API](#) could be in the form of [Web Services](#), [Remote Procedure Calls \(RPC\)](#), [Common Object Request Broker Architecture \(CORBA\)](#), [Data Distribution Service \(DDS\)](#) or other interprocess communication mechanisms defined using [ISO/OMG Interface Definition Language \(IDL\)](#), [standardized Web Services Interface Language \(WSDL\)](#), etc.

## The Dual ACH/CBDC Payment Networks

[Return to Top](#)

Figure 19 provides a very simplistic overview of how a Dual ACH/CBDC network might work. The intention is to build onto the existing financial system already in place but to allow an option to use a U.S. CBDC probably built as a Stablecoin. The Existing Intermediaries would still fulfill their existing roles while providing an option to use a CBDC network to transfer the money. The existing validation and verification for the number of transactions, the quantity of money transferred, and all of the checks for criminal activity and assurance for privacy would stay in place.

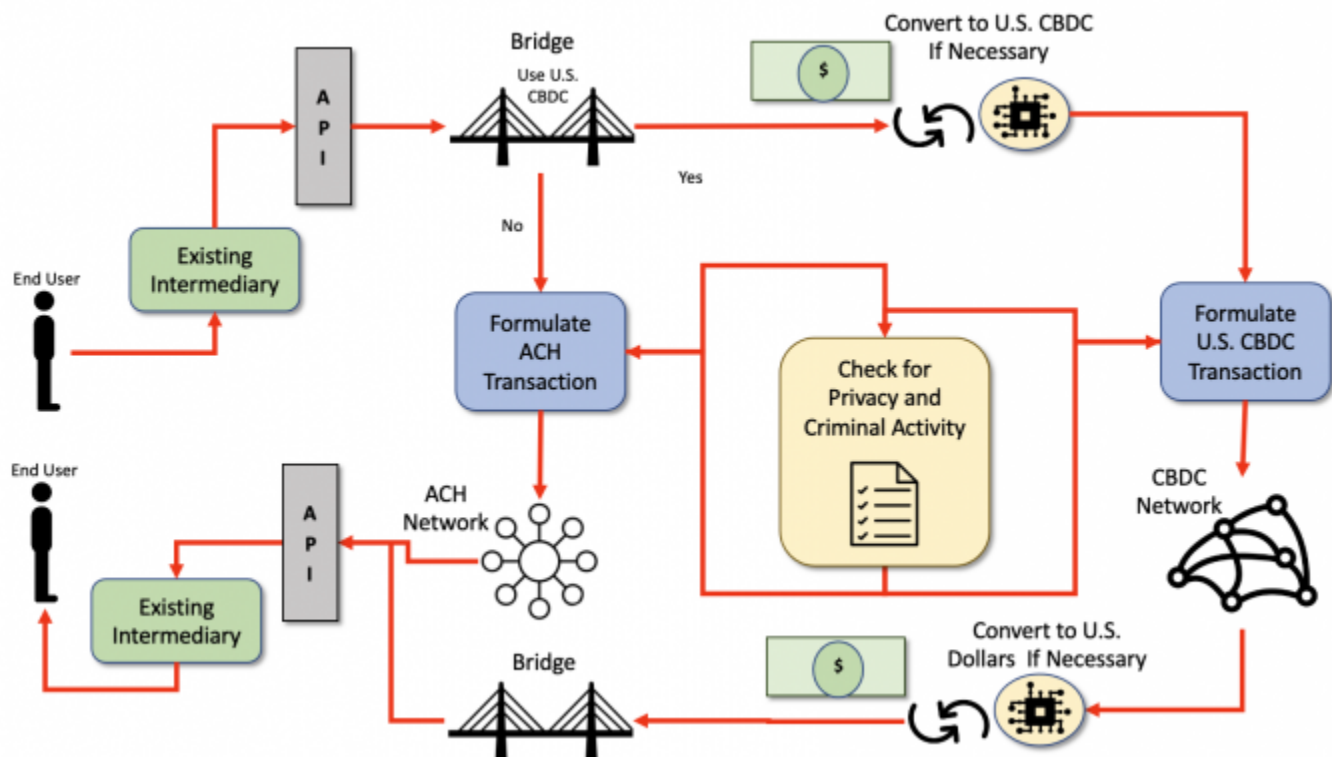


Figure 19: Theoretical Very Simplified Dual ACH-CBDC Network Concept.

Scenario	Step Number	Description
<b>Current Process</b>	1	The First End User (Person, Corporation, Institution, a Computer process, etc.) goes into an Existing Intermediary and wants to transfer money to a Second End User.
	2	The First Existing Intermediary uses the newly U.S. CBDC <a href="#">Application Programming Interface (API)</a> to start the transaction. The First Existing Intermediary asks if the money is to be transferred immediately requiring U.S. CBDC or if it will just be done using U.S. Dollars.
	3	The First End User responds that they will be using U.S. Dollars.
	4	A transaction is created that meets the requirements of the ACH is formulated.
	5	The ACH Transaction is placed onto the existing ACH Network and routed to the appropriate Second Existing Intermediary.
	6	The Second Existing Intermediary receives the transaction and waits for the transaction to settle (usually within 24 hours).
	7	The Second Existing Intermediary places the money designated in the transfer transaction to the Second End User's bank account (i.e., debit, credit, checking, savings, Credit Card account, etc.)
	8	The Second End User possesses the money.
Scenario	Step Number	Description
<b>U.S. CBDC Process</b>	1	The First End User (Person, Corporation, Institution, a Computer process, etc.) goes into an Existing Intermediary and wants to transfer money to a Second End User.
	2	The First Existing Intermediary uses the newly U.S. CBDC <a href="#">Application Programming Interface (API)</a> to start the transaction. The First Existing Intermediary asks if the money is to be transferred immediately requiring U.S. CBDC or if it will just be done using U.S. Dollars.
	3	The First End User responds that they will be using U.S. CBDC.
	4	The First Existing Intermediary verifies that the First End User has the correct amount of U.S. CBDC to complete the transaction. If Not, the First End User can convert some existing U.S. Dollars to U.S. CBDC to complete the transaction.
	5	A transaction is created that meets the requirements of the U.S. CBDC is formulated.
	6	The U.S. CBDC Transaction is placed onto the new U.S. CBDC Network and routed to the appropriate Second Existing Intermediary.
	7	The Second Existing Intermediary receives the U.S. CBDC transaction after the transaction is been validated and verified by the U.S. CBDC Consensus Algorithm.
	8	The Second End User possesses the money.

Table 59: Various steps in using a simplistic theoretical dual ACH/CBDC network.

### Only the CBDC Payment Network

[Return to Top](#)

Allowing new or existing Payment Networks to only use the new U.S. CBDC Payment Network is possible. See Figure 20. This allows for new and creative ways of having payment transactions. In this scenario, the new Intermediary would use the same new [Application Programming Interface \(API\)](#) as in the Dual situation, but in this scenario, all the transactions would need to be in U.S. CBDC. This means that any U.S. Dollars would have to be exchanged for U.S. CBDC before the transactions can take place. However, the New Intermediaries might allow accounts to contain U.S. CBDC. In this case, there would be no conversion required.

The same situation occurs on the other end of the payment transaction. The recipient could level all or some of the transactions as U.S. Dollars or U.S. CBDC.

**NOTE:** These new financial intermediaries would **NOT** be released from following the existing Laws and Regulations of the traditional financial intermediaries. In other words, they would have to ensure the End User's privacy (both ends of the Payment Transactions). They would also have to conform to all the [National Security Laws and Regulations](#). If either End User in the Payment Transaction is not in the U.S., they would have to abide by all the [International Laws and Regulations](#). This would mean these new Intermediaries would be subject to oversight and auditing.

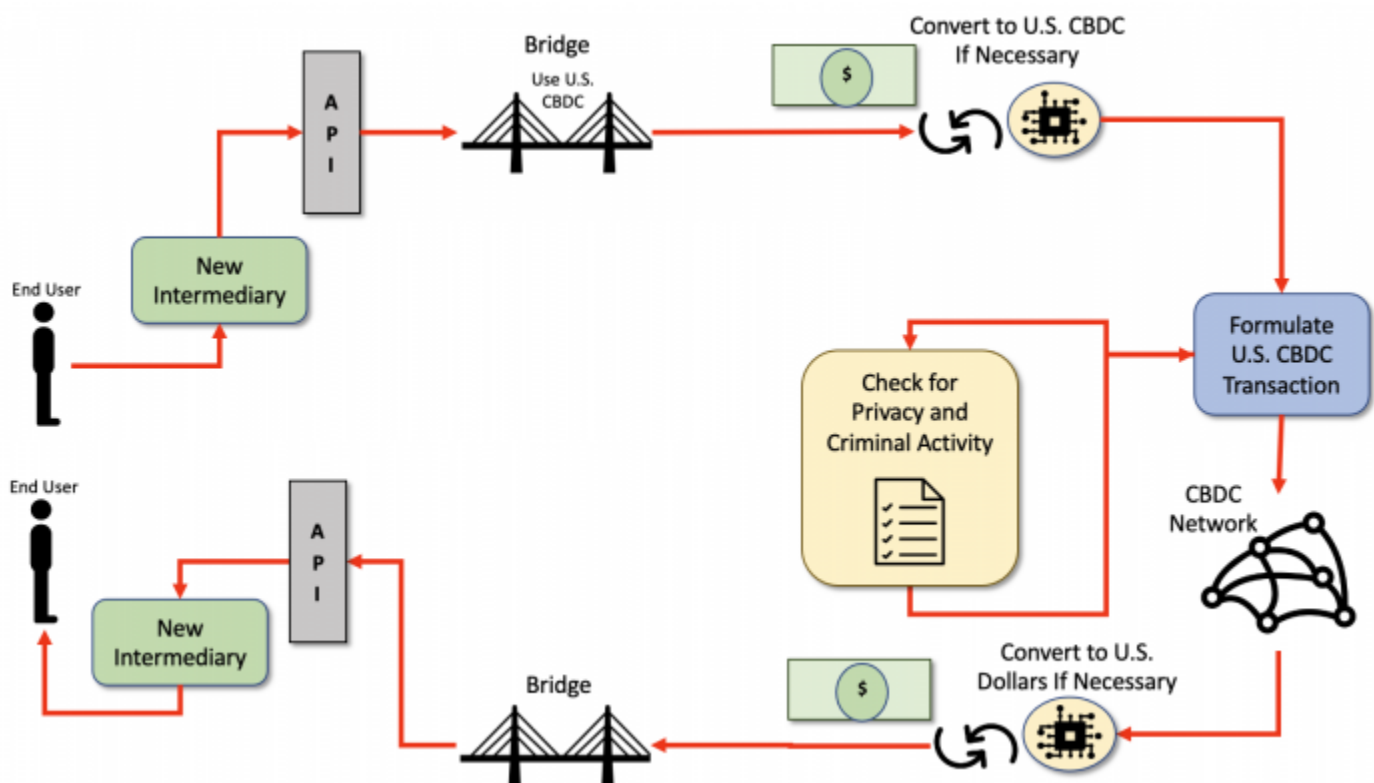


Figure 20: Theoretical Very Simplified single CBDC Network Concept.

## Examples

[Return to Top](#)

The “desirements” specified in [White Paper](#) and identified by the [OMG's White Paper Analysis](#) as **Privacy Issues** are listed in Table 42.

Table 60: Examples of **Privacy Desirements** identified during the White Paper Analysis conducted by the OMG

Category	Desirements
<b>Benefits</b>	B0003, B0004, B0005, B0007, B0008, B0009, B0011, B0012, B0013, B0022, B0024, B0026, B0027, B0037, B0038, B0045, B0046, B0047, B0051
<b>Policies and Considerations</b>	P0021, P0023, P0025, P0026, P0028
<b>Risks</b>	R0007, R0010, R0014, R0018, R0019, R0020
<b>Design</b>	D0012, D0013, D0014, D0015

**Note:** **B** = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.

## Discussion of Examples

[Return to Top](#)

Table 43 provides discussion points for each of the “desirements” identified by the [OMG's White Paper Analysis](#).

Table 61: Privacy references of desirements in the **White Paper**

Desirement No.	Desirement Text	Comment
<b>B0003</b>	<b>Complement, rather than replace, current forms of money and methods for providing financial services</b>	The proposed Dual ACH/CBDC networks would do exactly that. The existing Intermediaries would be allowed to expand their services to include U.S. CBDC by basically making it as a consumer choice.
<b>B0004</b>	<b>Protect consumer privacy</b>	The proposed Dual ACH/CBDC networks would still place the burden on protecting the privacy of the End-User on the existing and new intermediaries. The intermediaries would be subject to reviews and audits.
<b>B0005</b>	<b>Protect against criminal activity</b>	The proposed Dual ACH/CBDC networks would still place the burden on protecting the national security on the existing and new intermediaries. The intermediaries would be subject to reviews and audits.
<b>B0007</b>	<b>Provide households and businesses a convenient and electronic form of central bank money with:</b> <b>1. safety</b> <b>2. liquidity</b>	In all accounts, U.S. money could be kept as U.S. Dollars or as U.S. CBDC. Since the U.S. CBDC would probably be backed by a U.S. Dollar Stablecoin, there should be no advantage or disadvantage to either. The main difference is the End User's choice to use the real-time CBDC or the existing ACH Network. Note: There may be a cost associated with converting between the two currencies.

Desirement No.	Desirement Text	Comment
B0008	<b>Provide entrepreneurs a platform on which to create new financial products and services</b>	Entrepreneurs would be able to create new Intermediaries that only used the U.S. CBDC Payment Network. This might not require bricks and mortar establishments and might work completely in a virtual environment.
B0009	<b>Provide faster and cheaper payments (including cross-border payments)</b>	If the U.S. CBDC network is selected by the End User, the transactions will most likely be faster, but not necessarily cheaper. There is a cost associated with using the <a href="#">Consensus facilities</a> of the U.S. CBDC as well as the possibility of costs associated with converting U.S. Dollars to U.S. CBDC.
B0011	<b>Make payments:</b> <b>1. faster</b> <b>2. cheaper</b> <b>3. more convenient</b> <b>4. more accessible</b>	Using the Dual Network, the End User can decide how fast they want the payments to be made. The cost of using a U.S. CBDC is still unknown. There is a cost associated with using the <a href="#">Consensus facilities</a> of the U.S. CBDC as well as the possibility of costs associated with converting U.S. Dollars to U.S. CBDC. Also see <b>B0008</b> . It is up to the free market and the entrepreneurs to make it more convenient and more accessible.
B0012	<b>Provide payment services to households and businesses around the clock, every day of the year</b>	Currently, most existing Intermediaries offer online banking addressing this already. However, some transactions may require a “person-in-the-middle” to complete. The U.S. CBDC would still require these “person-in-the-middle” for some kinds of transactions.
B0013	<b>Provide immediate access to transferred funds</b>	If an End User chooses to use the U.S. CBDC network, the funds will be available as fast as the U.S. CBDC infrastructure permits. Usually within minutes. See <a href="#">Consensus Algorithms</a> for more information.
B0022	<b>Provide a CBDC that is:</b> <b>1. Privacy-Protected</b> <b>2. Intermediated</b> <b>3. Widely Transferable</b> <b>4. Identity-Verified</b>	Using the Dual Network Model for payment transfers should fulfill all these desirements. <b>NOTE:</b> These new financial intermediaries would <b>NOT</b> be released from following the existing Laws and Regulations of the traditional financial intermediaries. In other words, they would have to ensure the End User's privacy (both ends of the Payment Transactions). They would also have to conform to all the <a href="#">National Security Laws and Regulations</a> . If either End User in the Payment Transaction is not in the U.S., they would have to abide by all the <a href="#">International Laws and Regulations</a> . This would mean these new Intermediaries would be subject to oversight and auditing.
B0024	<b>Provide transactions finalized and completed in real-time</b>	If the U.S. CBDC Payment network is selected by the End User, the transactions will happen as fast as the U.S. CBDC Infrastructure permits. See <a href="#">Consensus Algorithms</a> for more information.

<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>B0026</b>	<b>Provide a bridge between legacy and new payment services</b>	The Dual ACH Network and U.S. CBDC Networks presented provides a bridge between the two networks. In order to be used effectively, the use of a standardized <a href="#">Application Programmer Interface (API)</a> is also recommended. <b>Note:</b> The <a href="#">API</a> could be in the form of Web Services, Remote Procedure Calls (RPC), <a href="#">Common Object Request Broker Architecture (CORBA)</a> , <a href="#">Data Distribution Service (DDS)</a> or other interprocess communication mechanisms defined using <a href="#">ISO/OMG Interface Definition Language (IDL)</a> , <a href="#">standardized Web Services Interface Language (WSDL)</a> , etc.
<b>B0027</b>	<b>Maintain the centrality of safe and trusted central bank money</b>	The Dual ACH Network and U.S. CBDC Networks maintain the U.S. Dollar as the legal tender for both payment networks. The ACH Network continues to use the U.S. Dollar as it currently does. The U.S. CBDC would use a U.S. Dollar backed Stablecoin.
<b>B0037</b>	<b>Support private-sector innovation</b>	See <b>B0009</b> above.
<b>B0038</b>	<b>Allow private-sector innovators to focus on:</b> <b>1. new access services</b> <b>2. distribution methods</b> <b>3. related service offerings</b>	See <b>B0009</b> above.
<b>B0045</b>	<b>Enable rapid and cost-effective payment of taxes</b>	The Internal Revenue Service (IRS) would be required to support the ACH/CBDC API and Bridge to make this happen. It is beyond the control of the Federal Reserve.
<b>B0046</b>	<b>Enable rapid and cost-effective delivery of:</b> <b>1. wages,</b> <b>2. tax refunds</b> <b>3. other federal payments</b>	This would require the employers, the U.S. Benefits agencies, and the Internal Revenue Service (IRS) to support the ACH/CBDC API and Bridge to make this happen.
<b>B0047</b>	<b>Lower transaction costs</b>	At this point in time, it can only be conjectured that the transaction costs would be less. Often it is assumed that the <a href="#">Privacy</a> and <a href="#">Security</a> laws and regulations can be skipped when using a U.S. CBDC. This will most likely not happen. If the U.S. CBDC uses a Stablecoin, the cost is highly dependent on the <a href="#">Platform</a> chosen. See: <a href="#">Consensus Algorithms</a>
<b>B0051</b>	<b>Generate data about users' financial transactions similar to the current Commercial Bank<sup>88)</sup> and Nonbank Money</b>	The Dual ACH/CBDC network model would require all Intermediaries to collect the same kind of data on all transactions providing one degree of freedom between the End Users and the Government.



Desirement No.	Desirement Text	Comment
P0021	<b>The intermediaries would operate in an open market for CBDC services</b>	Currently, the Intermediaries operate in an open market that is confined by the Laws and Regulations of the U.S. and Foreign governments when applicable. The proposed Dual ACH/CBDC networks would allow the existing Intermediaries to participate in the CBDC services as long as they are compliant with the standardized <a href="#">Application Programmer Interface (API)</a> and Bridge. The proposed Dual ACH/CBDC networks would also allow new Intermediaries to only offer CBDC services.
P0023	<b>CBDC would need to be readily transferable between customers of different intermediaries</b>	As long as the Intermediaries use the standardized <a href="#">Application Programmer Interface (API)</a> and Bridge, all transfers between Intermediaries is possible.
P0025	<b>CBDC intermediary would need to verify the identity of a person accessing CBDC</b>	See <b>B0022</b> above.
P0026	<b>CBDC transactions would need to be final and completed in real-time</b>	See <b>B0007</b> and <b>B0024</b> above.
P0028	<b>Require significant international coordination to address issues such as:</b> <b>1. common standards</b> <b>2. infrastructure,</b> <b>3. the types of intermediaries able to access any new infrastructure,</b> <b>4. legal frameworks</b> <b>5. preventing illicit transactions</b> <b>6. the cost and timing of implementation</b>	See <b>B0026</b> , <b>P0021</b> , and <b>B0045</b> above.
R0007	<b>Risk CBDC is difficult to use without service providers</b>	At a minimum, the existing Intermediaries would be able to use most of their existing infrastructure to use the U.S. CBDC. In the Workflow for creating a payment transaction: 1. Need to ask if it is going to use a CBDC transfer. a. If yes, they need to make sure the End Users account has the correct amount of CBDC Stablecoins i. If not, they need to convert U.S. Dollars to U.S. CBDC Stablecoins ii. formulate a standardized U.S. CBDC transaction and all the required data b. If not, do ACH Network business as usual
R0010	<b>CBDC has a Risk of significant energy footprint similar to Cryptocurrencies</b>	This is highly dependent on the DIDO Platform selected for the U.S. CBDC and the <a href="#">Consensus Algorithm</a> selected.

Desirement No.	Desirement Text	Comment
R0011	<b>Increased Risk to consumer's vulnerability to:</b> <b>1. loss</b> <b>2. theft</b> <b>3. fraud</b>	<p>In the Dual ACH/CBDC network the risk should remain the same as it is under just the ACH Network.</p>
R0014	<b>Risk of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity</b>	<p>Assuming that the current balance is acceptable, using the Dual Network Model for payment transfers would keep in place all existing Privacy and Security Laws and Regulations. The new Intermediaries would have to follow the same rules as the existing Intermediaries. <b>NOTE:</b> These new financial intermediaries would <b>NOT</b> be released from following the existing Laws and Regulations of the traditional financial intermediaries. In other words, they would have to ensure the End User's privacy (both ends of the Payment Transactions). They would also have conform to all the <a href="#">National Security Laws and Regulations</a>. If either End User in the Payment Transaction is not in the U.S., they would have to abide by all the <a href="#">International Laws and Regulations</a>. This would mean these new Intermediaries would be subject to oversight and auditing.</p>
R0018	<b>Risk a CBDC could fundamentally change the structure of the U.S. financial system, altering the private sector and central bank:</b> <b>1. roles</b> <b>2. responsibilities</b>	<p>The Dual ACH/CBDC Network models should extend the current structure of the U.S. financial system and provide more potential Intermediaries. The more Intermediaries, the more robust the system should become.</p>
R0019	<b>Risk of reducing the aggregate amount of deposits in the banking system, which could in turn increase bank funding expenses, and reduce credit availability or raise credit costs for households and businesses.</b>	<p>In the Dual ACH/CBDC Network model, U.S. Dollars in accounts or U.S. CBDC would still be treated as transfers. See the answer to <a href="#">Question: 13. How could a CBDC be designed to foster operational and cyber resiliency? What operational or cyber risks might be unavoidable?</a></p>
R0020	<b>Risk that interest-bearing CBDC could result in a shift away from other low-risk assets, such as shares in money market mutual funds, Treasury bills, and other short-term instruments.</b>	<p>Using the Dual ACH/CBDC Transaction Network, the U.S. CBDC should be treated exactly the same way as U.S. Dollars. The Intermediary accounts would have to segment the accounts into those that contain U.S. Dollars and those that contain U.S. CBDC if the End User wants to avail themselves of the new U.S. CBDC network.</p>



Desirement No.	Desirement Text	Comment
D0012	<b>Design should address privacy concerns by leveraging existing tools already in use by intermediaries</b>	See <b>B0004</b> , <b>B0024</b> , <b>B0047</b> , and <b>R0014</b> above.
D0013	<b>Design should facilitate compliance with a robust set of rules already intended to combat</b> <b>1. money laundering</b> <b>2. the financing of terrorism</b> <b>3. customer due diligence</b> <b>4. record-keeping</b> <b>5. reporting requirements</b>	See <b>B0005</b> and <b>R0011</b> above.
D0014	<b>Design should involve private-sector partners with established programs to help ensure compliance with existing rules</b>	The proposed Dual ACH/CBDC networks would do exactly that. The existing Intermediaries would be allowed to expand their services to include U.S. CBDC by basically making it a consumer choice. The proposed Dual ACH/CBDC networks would still place the burden on protecting the privacy of the End-User on the existing and new intermediaries. The intermediaries would be subject to reviews and audits. The proposed Dual ACH/CBDC networks would still place the burden on protecting the national security on the existing and new intermediaries. The intermediaries would be subject to reviews and audits.
D0015	<b>Design should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks</b>	The Dual ACH/CBDC Networks would require the new infrastructure for the <a href="#">Application Programmer Interface (API)</a> , the bridges, and the building out of a Distributed Network of Nodes to handle the CBDC transactions and <a href="#">Consensus</a> . The network of nodes might have any number of node types. Figure <a href="#">21</a> describes the taxonomy of DIDO Node Types. See <a href="#">OMG DID-RA Node Taxonomy</a> for a discussion on the different kinds of nodes.
<b>B = <a href="#">Benefit Considerations</a></b>		
<b>P = <a href="#">Policy Considerations</a></b>		
<b>R = <a href="#">Risk Considerations</a></b>		
<b>D = <a href="#">Design Considerations</a></b>		

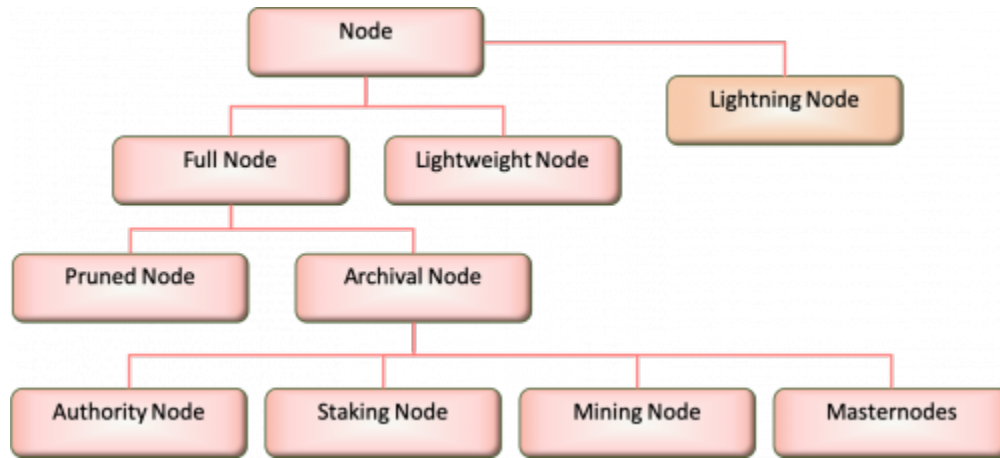


Figure 21: DIDO Node Taxonomy: Node Types

88)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**.

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:70\\_dualnets:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:15_common:70_dualnets:start)

Last update: 2022/05/18 22:22



# 5.0 Questions and Responses

## 5.0 Questions and Responses

[Return to the Main Document](#) [Provide Feedback](#)

The actual OMG response to the 22 direct questions posed in the **White Paper**. These are linked to other sections of the OMG response such as the **Common Elements** and also other questions. The OMG responded to all the questions, however, a few were felt to be beyond the scope of what the OMG members could respond to.

## Overview

[Return to Top](#)

The Federal Reserve posted a white paper in January 2022. The white paper requested comments on 22 questions posted in the [Money and Payments: The U.S. Dollar in the Age of Digital Transformation](#). The following discussion follows the original outlined provided in the **White Paper**. The questions are divided into two broad categories:

- [Benefits, Risks, and Policy Considerations](#)
- [Design](#)

## Content

[Return to Top](#)

The following sections are the responses to the questions posed in the [Object Management Group \(OMG\)](#)

- [5.1 Benefits, Risks, and Policy Considerations](#)
  - [Question: 01. What additional potential benefits, policy considerations, or risks of a CBDC may exist that have not been raised in this paper?](#)
    - [sub-Q1: Benefits](#)
    - [sub-Q2: Policies](#)
    - [sub-Q3: Risks](#)
  - [Question: 02. Could some or all of the potential benefits of a CBDC be better achieved in a different way?](#)
  - [Question: 03. Could a CBDC affect financial inclusion? Would the net effect be positive or negative for inclusion?](#)
  - [Question: 04. How might a U.S. CBDC affect the Federal Reserve's ability to effectively](#)

implement monetary policy in the pursuit of its maximum-employment and price-stability goals?

- Question: 05. How could a CBDC affect financial stability? Would the net effect be positive or negative for stability?
- Question: 06. Could a CBDC adversely affect the financial sector? How might a CBDC affect the financial sector differently from stablecoins or other nonbank money?
- Question: 07. What tools could be considered to mitigate any adverse impact of CBDC on the financial sector? Would some of these tools diminish the potential benefits of a CBDC?
- Question: 08. If cash usage declines, is it important to preserve the general public's access to a form of central bank money that can be used widely for payments?
- Question: 09. How might domestic and cross-border digital payments evolve in the absence of a U.S. CBDC?
- Question: 10. How should decisions by other large economy nations to issue CBDCs influence the decision whether the United States should do so?
- Question: 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?
  - 1. Risk of a Software Crisis
  - 2. Risk of Lack of Stakeholder Buy-In
  - 3. Risk Due to Poor Community of Interest (CoI) Governance
  - 4. Risk Due to lack of Broad, Wide Ranging Security Planning
  - 5. Risk of Data being hacked due weak Security Infrastructure
  - 6. Risk of Meta-Data being hacked due weak Security Infrastructure
  - 7. Risk of Business Processes Being Hacked
  - 8. Risk of competing Currency Models for the CBDC
- Question: 12. How could a CBDC provide privacy to consumers without providing complete anonymity and facilitating illicit financial activity?
- Question: 13. How could a CBDC be designed to foster operational and cyber resiliency? What operational or cyber risks might be unavoidable?
  - 1. How could a CBDC be designed to foster operational and cyber resiliency?
    - a) Operational Resiliency
    - b) Cyber Resiliency
  - 2. What operational or cyber risks might be unavoidable?
- Question: 14. Should a CBDC be legal tender?
- 5.2 Design
  - Question: 15. Should a CBDC pay interest? If so, why and how? If not, why not?
  - Question: 16. Should the amount of CBDC held by a single end user be subject to quantity limits?
  - Question: 17. What types of firms should serve as intermediaries for CBDC? What should be the role and regulatory structure for these intermediaries?
  - Question: 18. Should a CBDC have "offline" capabilities? If so, how might that be achieved?
  - Question: 19. Should a CBDC be designed to maximize ease of use and acceptance at the point of sale? If so, how?
  - Question: 20. How could a CBDC be designed to achieve transferability across multiple payment platforms? Would new technology or technical standards be needed?
  - Question: 21. How might future technological innovations affect design and policy choices related to CBDC?
  - Question: 22. Are there additional design principles that should be considered? Are there tradeoffs around any of the identified design principles, especially in trying to achieve the

potential benefits of a CBDC?

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:start)



Last update: **2022/05/17 21:03**

# 5.1 Benefits, Risks, and Policy Considerations

[Return to Public Questions](#) [Provide Feedback](#)

## Specific Questions

[Return to Top](#)

- Question: 01. What additional potential benefits, policy considerations, or risks of a CBDC may exist that have not been raised in this paper?
  - sub-Q1: Benefits
  - sub-Q2: Policies
  - sub-Q3: Risks
- Question: 02. Could some or all of the potential benefits of a CBDC be better achieved in a different way?
- Question: 03. Could a CBDC affect financial inclusion? Would the net effect be positive or negative for inclusion?
- Question: 04. How might a U.S. CBDC affect the Federal Reserve's ability to effectively implement monetary policy in the pursuit of its maximum-employment and price-stability goals?
- Question: 05. How could a CBDC affect financial stability? Would the net effect be positive or negative for stability?
- Question: 06. Could a CBDC adversely affect the financial sector? How might a CBDC affect the financial sector differently from stablecoins or other nonbank money?
- Question: 07. What tools could be considered to mitigate any adverse impact of CBDC on the financial sector? Would some of these tools diminish the potential benefits of a CBDC?
- Question: 08. If cash usage declines, is it important to preserve the general public's access to a form of central bank money that can be used widely for payments?
- Question: 09. How might domestic and cross-border digital payments evolve in the absence of a U.S. CBDC?
- Question: 10. How should decisions by other large economy nations to issue CBDCs influence the decision whether the United States should do so?
- Question: 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?
  - 1. Risk of a Software Crisis
  - 2. Risk of Lack of Stakeholder Buy-In
  - 3. Risk Due to Poor Community of Interest (CoI) Governance
  - 4. Risk Due to lack of Broad, Wide Ranging Security Planning
  - 5. Risk of Data being hacked due weak Security Infrastructure
  - 6. Risk of Meta-Data being hacked due weak Security Infrastructure
  - 7. Risk of Business Processes Being Hacked
  - 8. Risk of competing Currency Models for the CBDC
- Question: 12. How could a CBDC provide privacy to consumers without providing complete anonymity and facilitating illicit financial activity?
- Question: 13. How could a CBDC be designed to foster operational and cyber resiliency? What

operational or cyber risks might be unavoidable?

- 1. How could a CBDC be designed to foster operational and cyber resiliency?
  - a) Operational Resiliency
  - b) Cyber Resiliency
- 2. What operational or cyber risks might be unavoidable?
- Question: 14. Should a CBDC be legal tender?

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:start)

Last update: **2022/05/17 01:49**





# Question: 01. What additional potential benefits, policy considerations, or risks of a CBDC may exist that have not been raised in this paper?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

What additional potential benefits, policy considerations, or risks of a [Central Bank Digital Currency \(CBDC\)](#) may exist that have not been raised in this paper?

## Answer

[Return to Top](#)

This is a compound question, and each part of the question is answered separately:

- [sub-Q1: Benefits](#)
- [sub-Q2: Policies](#)
- [sub-Q3: Risks](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q01:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q01:start)

Last update: **2022/05/16 20:35**



# sub-Q1: Benefits

[Return to Question 1](#) [Provide Feedback](#)

## Question

[Return to Top](#)

What additional potential **benefits** of a [Central Bank Digital Currency \(CBDC\)](#) may exist that have not been raised in this paper?

## Answer

[Return to Top](#)

Probably the biggest benefit would be the adoption of Dual [Automated Clearing House \(ACH\) Network/CBDC Payment Networks](#) as outlined in the Common Elements section on [Dual Payment Networks](#).

1. Development of a near real-time payment network with:

- a. Efficient [Consensus Algorithms](#)
- b. Adherence to:
  - [U.S. Privacy Laws and Regulations](#)
  - [U.S. Security Laws and Regulations](#)
  - [International Cooperation and adherence to treaties](#)

2. Development of a **bridge** between the existing [Automated Clearing House \(ACH\) Network](#) and the new U.S. CBDC Network

3. Development of a new standardized [Application Programming Interface \(API\)](#) to connect the outside world to the newly enhanced combined ACH Network and CBDC Network for the existing intermediaries to use for transfers

Figure 19 provides a very simplistic overview of how a Dual ACH/CBDC network might work. The intention is to build onto the existing financial system already in place but to allow an option to use a U.S. CBDC probably built as a Stablecoin. The Existing Intermediaries would still fulfill their existing roles while providing an option to use a CBDC network to transfer the money. The existing validation and verification for the number of transactions, the quantity of money transferred, and all of the checks for criminal activity and assurance for privacy would stay in place.

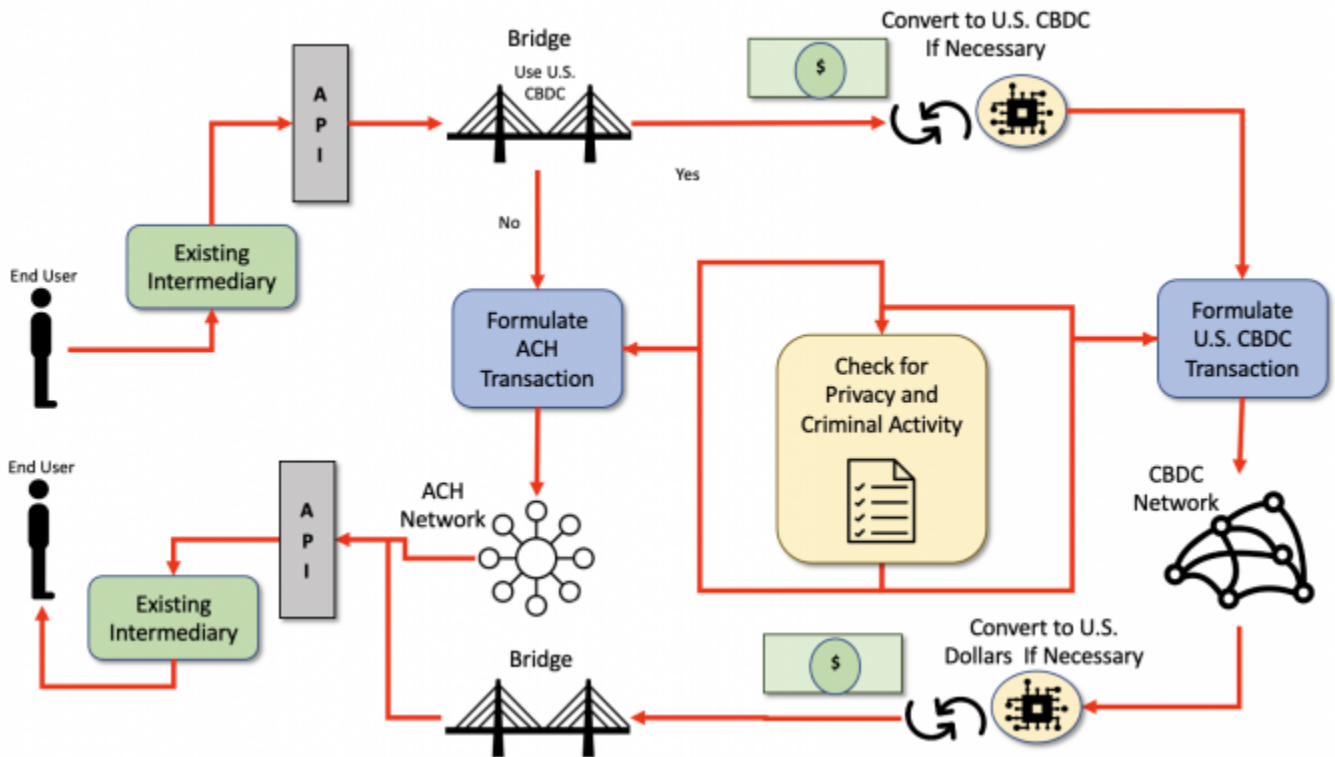


Figure 22: Theoretical Very Simplified Dual ACH-CBDC Network Concept.

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**  
Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q01:benefits](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q01:benefits)  
Last update: 2022/05/18 21:38



# sub-Q2: Policies

[Return to Question 1](#) [Provide Feedback](#)

## Question

[Return to Top](#)

What additional potential **policy considerations** of a [Central Bank Digital Currency \(CBDC\)](#) may exist that have not been raised in this paper?

## Answer

[Return to Top](#)

## Governance Overview

[Return to Top](#)

A major risk to the CBDC is the [Governance](#) of a very large, complex system. which encompasses:

- US Legislative laws and regulations
- CBDC cross US department and agency organizations
- CBDC international participants
- CBDC private sector partners
- Legal policies and procedures for the CBDC itself
- Hardware
- Networks
- Software
- Data

CBDC Governance is the system that controls the entities and direction of the CBDC effort. Its primary concern is the structure and processes for decision-making, accountability, control and behavior at the top of the CBDC. CBDC governance will set the organization's objectives, measure how well these objectives are achieved, monitor risks to the CBDC, and set actions in place to mitigate those risks. Governance is a system and a process, not a single activity; therefore successful implementation of a good governance strategy requires a systematic approach that incorporates strategic planning, risk management, and performance management. Like culture, it is a core component of the unique characteristics of a successful organization.

## Examples

[Return to Top](#)

Some “desirements” in the [Money and Payments: The U.S. Dollar in the Age of Digital Transformation White Paper](#) and summarized in the [White Paper Analysis](#) done by the [Object Management Group](#) allude to the Governance areas shown in the table below:

Table 62: Example of mapping a subset of “desirements” identified during the White Paper Analysis conducted by OMG.

<b>Governance Area</b>	<b>OMG Identified “desirements”</b>
<b>Legislation, Laws, and Regulations</b>	P: P0011, P0014, P0015, P0016, P0018, P0019, P0030
<b>External Federal Reserve, US Government Organization</b>	B: B0005, B0006, B0020, B0025, B0026, B0030, B0036, B0046, B0052, B0053 P: P0005, P0006, P0016, P0017, P0023, P0024, P0031 R: R0001, R0005, R0008, R0010, R0011, R0012, R0014, D0013, D0016, D0017
<b>External US Entities</b>	B: B0006, B0009, B0015, B0025, B0041, B0052, P0028, D0009,
<b>Private Sector Parties</b>	B: B0006, B0008, B0025, B0026, B0029, B0033, B0037, B0038, B0044, B0046, B0052, B0053 P: P0005, P0010, P0012, P0013, P0016, P0020, P0021, P0023, P0024 R: R0001, R0005, R0008, R0011, R0012, R0014, R0018, R0020, R0022, R0023 D: D0011, D0012, D0013, D0014, D0017
<b>Purpose-built Hardware</b>	P: P0025 R: R0014 D: D0002, D0003, D0011, D0015, D0016, D0017
<b>Purpose-built Software</b>	P: P0025 R: R0014 D: D0002, D0003, D0011, D0012, D0013, D0016, D0017
<b>Purpose-defined Data</b>	B: B0051 P: P0004 R: R0014 D: D0002, D0003, D0011, D0012, D0013, D0016, D0017
<b>B = Benefit Considerations</b>	
<b>P = Policy Considerations</b>	
<b>R = Risk Considerations</b>	
<b>D = Design Considerations</b>	

## Discussion of Examples

[Return to Top](#)

This discussion is divided into the sections mapped out in [Table 62](#).

- [Legislation, Laws, and Regulations](#)
- [External Federal Reserve, US Government Organization](#)
- [External US Entities](#)
- [Private Sector Parties](#)
- [Purpose-built Hardware](#)
- [Purpose-built Software](#)
- [Purpose-defined Data](#)

## Legislation, Laws, and Regulations

### [Return to Discussion of Examples](#)

Some “desirements” identified in [CBDC White Paper](#) by the [OMG White Paper Analysis effort](#) map to Legislation, Laws, and Regulations.

Table 63: **White Paper** “desirements” associated with Legislation, Laws, and Regulations.

**Note:** The following subset of “desirements” only represents a few that are relevant to Legislation, Laws, and Regulations found in the White Paper. They are provided to support further discussions.

Statement No.	Page No.	Statement
<b>P0011</b>	<b>3</b>	The Federal Reserve does not intend to proceed with the issuance of a CBDC without clear support from: <ol style="list-style-type: none"> <li>1. the Executive Branch</li> <li>2. Legislative Branch</li> <li>3. ideally in the form of a specific authorizing law</li> </ol>
<b>P0030</b>	<b>21</b>	The Federal Reserve will only take further steps toward developing a CBDC if: <ol style="list-style-type: none"> <li>1. Research points to benefits for households, businesses, and the economy overall that exceed the downside risks</li> <li>2. Indicates that CBDC is superior to alternative methods</li> </ol>

- **P0030** indicates that any actions taken regarding the CBDC require prior approval from the Executive and legislative branches of the government; however, **P0030** indicates that research can proceed to determine the alternatives and benefits of a CBDC.

## External Federal Reserve, US Government Organization

### [Return to Discussion of Examples](#)

Some “desirements” identified in [CBDC White Paper](#) by the [OMG White Paper Analysis effort](#) map to US Government organizations external to the Federal Reserve.

Table 64: **White Paper** “desirements” associated with US Government organizations external to the Federal Reserve.

**Note:** The following subset of “desirements” only represents a few that are relevant to External

Federal Reserve, US Government Organization found in the White Paper. They are provided to support further discussions.

Statement No.	Page No.	Statement
<b>B0006</b>	<b>2</b>	Provide broad support from key stakeholders
<b>B0011</b>	<b>7</b>	Make payments: 1. faster 2. cheaper 3. more convenient 4. more accessible
<b>B0052</b>	<b>19</b>	Prevent Financial money laundering crimes
<b>B0053</b>	<b>20</b>	Provide resiliency to threats to existing payment services—including: 1. operational disruptions 2. cybersecurity risks
<b>D0017</b>	<b>20</b>	Design should include digital payments in areas suffering from large disruption, such as natural disasters

- **B0006** advises that the Federal Reserve should consider other government organizations as stakeholders in the CBDC. Just based upon **B0011**, **B0052**, **B0053** and **D0017**, some of those organizations might be: US Treasury, FDIC, ACH, FEMA, DHS, DoD, SEC, FBI, Secret Service, etc.

## External US Entities

### [Return to Discussion of Examples](#)

Some “desirements” identified in [CBDC White Paper](#) by the [OMG White Paper Analysis effort](#) map to External US Government organizations.

Table 65: **White Paper** “desirements” associated with External US Government organizations.

**Note:** The following subset of “desirements” only represents a few that are relevant to External US Entities found in the White Paper. They are provided to support further discussions.

Statement No.	Page No.	Statement
<b>B0005</b>	<b>2</b>	Protect against criminal activity
<b>B0009</b>	<b>3</b>	Provide faster and cheaper payments (including cross-border payments)
<b>B0015</b>	<b>9</b>	Reduce cross-border costs to benefit: 1. economic growth 2. enhance global commerce 3. improve international remittances 4. reduce inequality
<b>B0041</b>	<b>15</b>	Support streamlining cross-border payments
<b>B0052</b>	<b>19</b>	Prevent Financial money laundering crimes
<b>P0005</b>	<b>2</b>	Protect against criminal activity

Statement No.	Page No.	Statement
<b>R0014</b>	<b>13</b>	<b>Risk</b> of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity
<b>D0009</b>	<b>18</b>	<b>Design</b> should allow for significant foreign demand for CBDC, furthering complicate monetary policy implementation

- **B0005, B0052, P0005, R0014** are all targeted at preventing criminal activities. Although there is a lot of criminal activity within the US, in this modern age of internationalism, it is important to elicit the help of foreign governments in detecting and tracking down criminal activities.
- **B0009, B0015, B0041** are all targeted at cross-border payments and remittances, which naturally would require the participation of foreign governments and institutions.
- **D0009** is concerned with foreign demand for CBDC, which again would point to some foreign governments and institutions being involved.

## Private Sector Parties

### [Return to Discussion of Examples](#)

Some “desirements” identified in [CBDC White Paper](#) by the [OMG White Paper Analysis effort](#) are intended for Private Sector organizations.

Table 66: **White Paper** “desirements” associated with Private Sector organizations.

**Note:** The following subset of “desirements” only represents a few that are relevant to Private Sector Parties found in the White Paper. They are provided to support further discussions.

Statement No.	Page No.	Statement
<b>B0006</b>	<b>2</b>	Provide broad support from key stakeholders
<b>B0029</b>	<b>14</b>	Support basic purchases of: <ol style="list-style-type: none"> <li>1. goods</li> <li>2. services</li> <li>3. pay bills</li> <li>4. pay taxes</li> </ol>
<b>B0033</b>	<b>15</b>	Support a level playing field in payment innovation for private-sector firms of all sizes
<b>B0037</b>	<b>15</b>	Support private-sector innovation
<b>B0038</b>	<b>15</b>	Allow private-sector innovators to focus on: <ol style="list-style-type: none"> <li>1. new access services</li> <li>2. distribution methods</li> <li>3. related service offerings</li> </ol>
<b>B0046</b>	<b>16</b>	Enable rapid and cost-effective delivery of: <ol style="list-style-type: none"> <li>1. wages,</li> <li>2. tax refunds</li> <li>3. other federal payments</li> </ol>



Statement No.	Page No.	Statement
<b>P0012</b>	<b>7</b>	The firms that operate inter-bank payment services are subject to federal supervision
<b>P0013</b>	<b>7</b>	Systemically important payment firms are subject to 1. heightened supervision 2. regulation
<b>P0020</b>	<b>13</b>	The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments
<b>R0005</b>	<b>7</b>	New payment services could pose <b>Risks</b> to: 1. financial stability 2. payment system integrity 3. other <b>Risks</b>
<b>D0014</b>	<b>20</b>	<b>Design</b> should involve private-sector partners with established programs to help ensure compliance with existing rules

The Private Sector Participation in the CBDC is subdivided into a few categories:

- Those participating in the building and support of the CBDC infrastructure: **B0033, B0037, B0038, P0020, D0014**
- Those participating in the use of the CBDC: **B0029, B0046**
- Those affected by the use of CBDC: **P0012, P0013, R0005**

## Purpose-built Hardware

### [Return to Discussion of Examples](#)

Some “desirements” identified in [CBDC White Paper](#) by the [OMG White Paper Analysis effort](#) call for Purpose-built Hardware.

Table 67: **White Paper** “desirements” associated with Hardware that is purpose-built for the CBDC.

**Note:** The following subset of “desirements” only represents a few that are relevant to Purpose-built Hardware found in the White Paper. They are provided to support further discussions.

Statement No.	Page No.	Statement
<b>P0025</b>	<b>14</b>	CBDC intermediary would need to verify the identity of a person accessing CBDC
<b>D0011</b>	<b>19</b>	<b>Design</b> should generate data about users’ financial transactions in the same ways that commercial bank and nonbank money generates data today
<b>D0015</b>	<b>20</b>	<b>Design</b> should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks
<b>D0016</b>	<b>20</b>	<b>Design</b> should include offline capabilities to help with the operational resilience of the payment system
<b>D0017</b>	<b>20</b>	<b>Design</b> should include digital payments in areas suffering from large disruption, such as natural disasters

- **P0025** could require hardware for identification such as [Smart Cards](#) or [https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a\\_glossary:r:rsa\\_secureid](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:r:rsa_secureid) which may or may not be Purpose-Built for the CBDC.
- **D0011** could be relevant when there is a network monitoring
- **D0015** if portions of the CBDC are over [secure, private networks](#) that are purpose-built for the operations, then they must be resilient to threats, disruptions and cybersecurity threats.
- **D0016, D0017** mean that payment systems need to be able to work autonomously in isolation from the Internet. This highlights the advantage of a [Digital Coin](#) versus a [Stablecoin](#).

## Purpose-built Software

### [Return to Discussion of Examples](#)

Some “desirements” identified in [CBDC White Paper](#) by the [OMG White Paper Analysis effort](#) call for Purpose-built Software.

Table 68: **White Paper** “desirements” associated with Software that is purpose-built for the CBDC.

**Note:** The following subset of “desirements” only represents a few that are relevant to Purpose-built Software found in the White Paper. They are provided to support further discussions.

Statement No.	Page No.	Statement
<b>P0025</b>	<b>14</b>	CBDC intermediary would need to verify the identity of a person accessing CBDC
<b>R0014</b>	<b>13</b>	<b>Risk</b> of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity
<b>D0002</b>	<b>17</b>	<b>Design</b> should allow the central bank to limit the amount of CBDC an end-user could hold
<b>D0003</b>	<b>18</b>	<b>Design</b> should allow a limit on the amount of CBDC an end-user could accumulate over short periods
<b>D0011</b>	<b>19</b>	<b>Design</b> should generate data about users’ financial transactions in the same ways that commercial bank and nonbank money generates data today
<b>D0013</b>	<b>19</b>	<b>Design</b> should facilitate compliance with a robust set of rules already intended to combat <ol style="list-style-type: none"> <li>1. money laundering</li> <li>2. the financing of terrorism</li> <li>3. customer due diligence</li> <li>4. record-keeping</li> <li>5. reporting requirements</li> </ol>
<b>D0016</b>	<b>20</b>	<b>Design</b> should include offline capabilities to help with the operational resilience of the payment system
<b>D0017</b>	<b>20</b>	<b>Design</b> should include digital payments in areas suffering from large disruption, such as natural disasters

- **P0025** could require software for identification such as [Smart Cards](#) or

[https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a\\_glossary:r:rsa\\_secureid](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:r:rsa_secureid) which may or may not be Purpose-Built for the CBDC.

- **R0014** there are [https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a\\_glossary:p:p\\_p](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:p:p_p) which can be implemented to help protect privacy but still allowing for the surveillance of activities that indicate criminal behavior. There are also Software approaches available that allow for the anonymization of data.
- **D0002, D0003** almost require a centralized system in order to enforce these rules. However, if [Digital Dollars](#) are used instead of [Stablecoins](#), the hoarding of the dollars requires a lot of planning on the part of the hoarder (i.e., money in a mattress)
- **D0011, D0013** is very important and is often overlooked by the current Cryptocurrencies and [Stablecoin](#) implementations. They are often built from the bottom up rather than from the top down or middle out. This means that many of these projects/products have to discover these rules and try to shoehorn them into their existing efforts. Just like security, many of these can not be “bolted” on *post facto*
- **D0016, D0017**, like the financial and banking rules, is something that needs to be considered very early on in the development of the requirements and architecture rather than addressed *post facto*

## Purpose-defined Data

### [Return to Discussion of Examples](#)

Some “desirements” identified in [CBDC White Paper](#) by the [OMG White Paper Analysis effort](#) for Purpose-defined Data.

Table 69: **White Paper** “desirements” associated with Data, Data Formats, and Metadata that is purpose defined for the CBDC.

**Note:** The following subset of “desirements” only represents a few that are relevant to Purpose-defined Data found in the White Paper. They are provided to support further discussions.

Statement No.	Page No.	Statement
<b>B0051</b>	<b>19</b>	Generate data about users’ financial transactions similarly to the current Commercial Bank <sup>89</sup> and <a href="#">Nonbank Money</a>
<b>P0004</b>	<b>2</b>	Protect consumer privacy
<b>R0014</b>	<b>13</b>	<b>Risk</b> of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity
<b>D0002</b>	<b>17</b>	<b>Design</b> should allow the central bank to limit the amount of CBDC an end-user could hold
<b>D0003</b>	<b>18</b>	<b>Design</b> should allow a limit on the amount of CBDC an end-user could accumulate over short periods
<b>D0011</b>	<b>19</b>	<b>Design</b> should generate data about users’ financial transactions in the same ways that commercial bank and nonbank money generates data today

Statement No.	Page No.	Statement
<b>D0013</b>	<b>19</b>	<b>Design</b> should facilitate compliance with a robust set of rules already intended to combat <ol style="list-style-type: none"> <li>1. money laundering</li> <li>2. the financing of terrorism</li> <li>3. customer due diligence</li> <li>4. record-keeping</li> <li>5. reporting requirements</li> </ol>
<b>D0016</b>	<b>20</b>	<b>Design</b> should include offline capabilities to help with the operational resilience of the payment system
<b>D0017</b>	<b>20</b>	<b>Design</b> should include digital payments in areas suffering from large disruption, such as natural disasters

- **B0051, D0011, D0011, D0013:** most existing blockchain, [Stablecoin](#) products are “organic”, evolving from the bottom up and are centered around the concepts of a ledger. Although this is part of banking, there is so much more that is required by law in the US. Many of these rules are not intended just to be administrative roadblocks (i.e., administrivia) but were instituted as a result of some previous problems and help to stabilize and instill confidence in the US financial institutions. Adding “rules” to these products will either degrade the quality and performance of the products or have spotty implementations.
- **P0004** is intended to protect consumer privacy, not just when the [Data is at Rest](#), but also when the [Data is in Motion](#) and while it is being used (processed). It is only when all the places where data is used are protected, can there be assurances of consumer privacy. While the traditional concepts of Data-At-Rest and Data-In-Motion are well known and understood, the third category, Data-In-Use, has emerged as equally important. In the past, Data-In-Use was physically protected at physically secured mainframes and Data Centers; however, with distributed computers, especially on Public Networks, there can be no such assurances. As the value of the assets on the network increase, the motivation to “hack” the data while in use increases. The CBDC, as part of the critical infrastructure, will be a prime target.
- **R0014** is about achieving a balance between a consumer's privacy and the transparency required to prevent criminal activity. In the real world, these limits are achieved through the difficulty of using physical money. Storing, transferring, and counting it is a problem. Although cash is anonymous, large amounts of cash trigger examination.
- **D0002, D0003** represent limits on CBDC holdings and the transactions associated with the current system. In many ways, these represent limits established to protect against money laundering.
- **D0016, D0017** like the financial and banking rules, is something that needs to be considered very early on in the development of the requirements and architecture rather than addressed *post facto* so the correct data can be collected.

89)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**&.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q01:policy](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q01:policy)

Last update: **2022/05/18 22:25**



# sub-Q3: Risks

[Return to Question 1](#) [Provide Feedback](#)

## Question

[Return to Top](#)

What additional **risks** of a [Central Bank Digital Currency \(CBDC\)](#) may exist that have not been raised in this paper?

## Answer

[Return to Top](#)

See the response to question [Question: 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?](#).

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q01:risks](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q01:risks)

Last update: **2022/05/16 21:25**



# Question: 02. Could some or all of the potential benefits of a CBDC be better achieved in a different way?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**Could some or all of the potential benefits of a CBDC be better achieved differently?**

## Answer

[Return to Top](#)

If differently means rather than as a Cryptocurrency or a [Stablecoin Models](#)? The answer is **Yes** and **No**.

## Overview

[Return to Top](#)

Almost all Cryptocurrencies implemented so far use the concept of tokens, accounts, wallets, transactions, and distributed ledgers. In essence, these approaches use the way money is handled in bank accounts<sup>90</sup>. However, the CBDC could also be modeled on actual currency, such as the US Dollar, in essence a true Digital Dollar (i.e., [Digital Cash](#)) that includes intelligence. The Digital Dollar could be physical or virtual.<sup>91</sup>

- **Physical Digital Dollars (PDD)** would be very similar to current printed dollars, but could have a “chip” that prevents counterfeiting and forgery, journal ownership, and can be declared obsolete or unfit and removed from circulation just like paper money is handled.
- **Virtual Digital Dollars (VDD)** would be a virtual containerized implementation of the PDD.

**Note:** PDD and VDD would support the same kinds of denominations as the current paper money (i.e., \\$1, \\$2, \\$5, \\$10, \\$20, \\$50 and \\$100)

Both PDD and VDD would be designed by the US Department of Treasury. The Federal Reserve Board (FRB) would place a yearly order with the U.S. Treasury for the production of both PDD and VDD just as they do with the current currency. FRB determines the size of the order based on estimates of public demand for PDD and VDD during the coming year and how much currency they estimate will be

destroyed because it is deemed unfit to circulate. PDD can be deemed unfit for circulation, just like paper currency (i.e., damaged, worn, or from an obsolete series) Obsolescence can be because of a change in the physical form of the PDD (i.e, Series) or can be because of the “smarts” on the PDD or VDD are obsolete, close to journaling capacity or have logged an exception during the execution of the software. The US Treasury will be responsible for its production.

Both the PDD and VDD will be signed by the Secretary of Treasury, just like paper money is.

PDD will follow a similar pattern to paper money in terms of distribution.

VDD can be distributed electronically by the Treasury to the FRB. Similarly, the FRB can distribute VDD to the Federal Reserve Banks for subsequent distribution to Commercial Banks, etc.

Each transfer is recorded in the PDD or the VDD internal journal. Every PDD or VDD will be owned by an individual and when the individual relinquishes control of the PDD or the VDD, the next owner can claim the PDD or VDD. This is not unlike current printed dollars. For example, paper money is stored in a physical wallet, the wallet is opened, and paper money is extracted and handed to someone else who places the money in their wallet.

Money that moves through a financial institution is checked for validity and fitness. And just like paper dollars, if the PDD or VDD are deemed unfit, they are removed from circulation. However, the definition of “unfit” is more extensive than with paper money.

Another important aspect of the Digital Money model is that the money can have “colors” albeit not in the physical sense but in the sense of limiting what that money can be used for. For example, money provided by a government for a housing subsidy can only be spent on housing. The money provided for food can only be used to pay for actual food and not alcohol or cigarettes. When money is transferred from one owner to another, the color of the money is checked for validity.

## Examples

### [Return to Top](#)

Some of the potential benefits outlined in the [White Paper](#) and summarized by the [Object Management Group's White Paper Analysis](#) can definitely be addressed with an alternative model to the one assumed in the White Paper.

The review in this example is not comprehensive but is meant as a demonstration of how an alternative approach might address some of the benefits, policy Considerations, risks, and design objects outlined in the White Paper.

Table 22 provides a cursory overview of using a [Digital Dollar Model](#) instead of a Cryptocurrency or Stablecoin Model.

Table 70: Example of mapping a subset of requirements identified in the White Paper Analysis conducted by the OMG.



Statement No.	Statement	Comments
<b>B0003, P0003</b>	<b>Complement, rather than replace, current forms of money and methods for providing financial services</b>	PDD and VDD are intended to work in parallel with existing systems and to follow much the same lifecycle as current paper money. The same institutions would fulfill the same roles they currently do but have added roles and responsibilities for Digital Currency.
<b>B0004, P0004, D0012</b>	<b>Protect consumer privacy</b>	Since the journal is kept with each individual Digital Currency rather than on a globally accessible ledger (i.e., journal) then the consumers' privacy is more obfuscated; it becomes more like paper money.
<b>B0005, P0005</b>	<b>Protect against criminal activity</b>	Once criminal activity is detected, the Digital Dollars collected as part of the investigation can provide invaluable information for the prosecutors as to the origins of the money.
<b>B0009</b>	<b>Provide faster and cheaper payments (including cross-border payments)</b>	PDD would have many of the same problems as paper money, but VDDs can be sent using normal encrypted electronic transfer for files.
<b>B0013</b>	<b>Provide immediate access to transferred funds</b>	Once the PDD or VDD is transferred to a payee, the money can be spent exactly like cash
<b>B0030</b>	<b>Support benefit payments directly to citizens</b>	Not only can the payments be made directly to the citizens, but the payments may be colored by category: rent, medicine, food, communication, etc.
<b>B0046</b>	<b>Enable rapid and cost-effective delivery of: 1. wages, 2. tax refunds 3. other federal payments</b>	PDD would be analogous to current paper money, but the VDD would be immediately available.
<b>R0001</b>	<b>Risk of affecting financial-sector market structure</b>	Since PDD and VDD would follow the existing Currency Lifecycle and major financial institutions will have the same roles as they currently have, there should be minimum disruption to the existing financial structure.
<b>R0010</b>	<b>CBDC has Risk of significant energy footprint similar to Cryptocurrencies</b>	The use of PDD and VDD does not require costly <a href="#">Consensus Algorithms</a> ; therefore, the energy cost should be insignificant.
<b>D0001</b>	<b>Design should be for a non-interest-bearing CBDC, for example, would be less attractive as a substitute for commercial bank money</b>	<a href="#">Digital Dollars</a> would be, for all intents and purposes, the same as current paper money. It would not accumulate interest until it is deposited in a financial institution.
<b>B = Benefit Considerations</b>		
<b>P = Policy Considerations</b>		
<b>R = Risk Considerations</b>		
<b>D = Design Considerations</b>		

## Discussion of Examples

[Return to Top](#)

Table 70 provides a comments column which covers much of the discussion associated with the set of individual requirements. However, the introduction of [Digital Dollars](#) introduces a lot of points for discussion. It is recommended that the requirements identified by the [Object Management Group's White Paper Analysis](#) need to ultimately be part of a Trade Study for the various alternatives (i.e., Cryptocurrency, Stablecoin, Digital Money). The Trade Study should be based on Conceptual Models, Logical Models and Physical Modes. Where:

- **Conceptual Models** capture the concepts that need to be addressed by any CBDC
- **Logical Models** capture the concepts as expressed in higher level technologies (i.e., Database, GUI, Journal, etc)
- **Physical Models** represent the logical constructs in a particular technology (i.e., Postgres, Oracle, HTML5, CSS, XML, JSON, etc.)

Regardless of which model (Cryptocurrency, [Stablecoin](#), [Digital Dollar](#)) is used for the CBDC, the [Object Management Group](#) recommends that the Federal Reserve use a Model Based Systems Engineering (MBSE) and Unified Architecture Framework (UAF) approach for future CBDC efforts. The CBDC is a complex issue that, once released, could have a life expectancy of many, many years. Only through extensive Systems Analysis, Engineering, Design will CBDC have the stability it needs to instill confidence in the public (**B0020**).

Some of the potential requirements in the [White Paper](#) as summarized by the [Object Management Group's White Paper Analysis](#) reflect the need to instill public confidence (See Table 71

Table 71: Some requirements in the White Paper that require the confidence of the public.

Statement No.	Page No.	Statement
<b>B0020</b>	<b>13</b>	Maintain public confidence by not requiring mechanisms, such as deposit insurance
<b>R0003</b>	<b>3</b>	<b>Risk</b> to the safety and stability of the financial system
<b>R0004</b>	<b>3</b>	<b>Risk</b> to the efficacy of monetary policy
<b>R0005</b>	<b>7</b>	New payment services could pose <b>Risks</b> to: <ol style="list-style-type: none"> <li>1. financial stability</li> <li>2. payment system integrity</li> <li>3. other <b>Risks</b></li> </ol>
<b>R0011</b>	<b>11</b>	Increased <b>Risk</b> to consumer's vulnerability to: <ol style="list-style-type: none"> <li>1. loss</li> <li>2. theft</li> <li>3. fraud</li> </ol>

<sup>90)</sup>

99% (if not all) issued Initial Coin Offering (ICO) tokens on top of the Ethereum implements the ERC-20 standard.

[https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b\\_stds:defact:ethereum:eip:erc\\_0020](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:defact:ethereum:eip:erc_0020)

<sup>91)</sup>

FinTech Futures, 31 January 2020, [Why is digitised cash better than stablecoins?](#), Accessed: 20 March

2022, <https://www.fintechfutures.com/2020/01/why-is-digitised-cash-better-than-stablecoins/>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q02:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q02:start)

Last update: **2022/05/18 22:26**



# Question: 03. Could a CBDC affect financial inclusion? Would the net effect be positive or negative for inclusion?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

This is a compound question, but the second part of the question relies on the first.

## Question

[Return to Top](#)

1. **Could a CBDC affect financial inclusion?**
2. **Would the net effect be positive or negative for inclusion?**

## Answer

[Return to Top](#)

### Could a CBDC affect financial inclusion?

[Return to Top](#)

The answer to these questions depends on the [Currency Model](#) underlying the CBDC. Based on the content of the White Paper, it appears as if the concept of “inclusion” means the participation of those who rely on [Nonbank Money](#).

The World Bank defines Financial as:

**Financial Inclusion** means that individuals' inclusion means that individuals and businesses have access to useful and affordable financial products and services that meet their needs – transactions, payments, savings, credit, and insurance – delivered in a responsible and sustainable way.

*Being able to have access to a transaction account is the first step toward broader financial inclusion since a transaction account allows people to store money, and send and receive payments. A transaction account serves as a gateway to other financial services, which is why ensuring that people worldwide can have access to a transaction account is the focus of the World Bank Group...<https://www.worldbank.org/en/topic/financialinclusion/overview#1>*

Barriers to **Financial Inclusion** have existed for a long time. Fortunately, a number of efforts are poised

to help broaden access to financial services taken for granted by affluent consumers.

Figure 23 shows the six services or capabilities that indicate **Financial Inclusion**: Bank Account, Cheaper Credit, Insurance, Savings, Financial Advice, and transfer of Funds.<sup>92)</sup> A person does not have to have all six services or capabilities in order to have Financial Inclusion but, as a general rule, more is better. For example, in the U.S., having a Bank Account probably will also provide access to the other five services and capabilities. However, in some countries, having a Bank Account might support the Transfer of Funds, and depending on where the Bank Account is, it may or may not be insured. A Bank Account may or may not support savings and the paying of interest and may or may not include financial advice or ensure that the advice provided is fair and equitable to the saver. Within the U.S. the big hurdle is to get people into the system starting with a Bank Account.

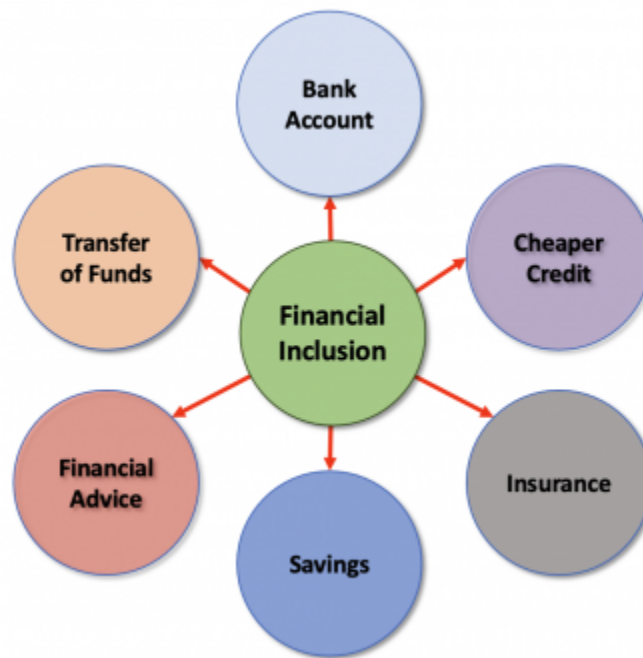


Figure 23: An Overview of Financial Inclusion Services<sup>93)</sup>

Figure 24 summarizes the problem that people who are excluded from the financial system struggle with. If they don't have a Bank Account, then they have a problem saving, getting insurance on their savings, etc.



Figure 24: An Overview of Financial Exclusion<sup>94)</sup>

The financial industry has determined that getting the non-banked or the under-banked population included in the financial system is a potential growth market for their services. Some of the financial industry have developed new methods and strategies to provide their products and services to the under-served population and can actually add to their own revenue streams.

The financial industry is making this possible through the use of low-cost [Financial Technology \(Fintech\)](#) solutions rather than trying to extend the traditional financial products and services to the financially underserved. For example, the financial industry is now using FinTech to offer cashless [Digital Transactions](#), the advent of low-fee [Robo-Advisors](#), and the rise of [Crowdfunding](#) and [Peer-to-Peer Lending \(P2P Lending\)](#) .

According to Investopedia, [Peer-to-Peer \(P2P\) Lending](#):ccc

**P2P Lending** has proved particularly beneficial to people in emerging markets, who may be ineligible for loans from traditional financial institutions because they lack a financial history or credit record to assess their creditworthiness. Microlending has also become a source of capital in places where it is otherwise hard to come by.

*While these innovative services have brought more participants into the financial marketplace, there is still a significant portion of the world's population—including in the United States—that lacks such access and remains, for example, either unbanked or underbanked.*

*The World Bank Group, which includes both the World Bank and the International Finance Corporation, is also sponsoring an initiative called Universal Financial Access 2020, the goal of which is to ensure that by the year 2020, an additional 1 billion adults will “have access to a transaction account to store money, send and receive payments as the basic building block to manage their financial lives.”*

*If successful, that effort would significantly reduce the number of adults who currently lack even rudimentary financial services, which the World Bank recently estimated at some 1.7 billion. However, the results will not be known until sometime in 2021.*

## Would the net effect be positive or negative for inclusion?

[Return to Top](#)

This would require more study; however, the Savanta: ComRes & the Financial Conduct Authority did a study which is a great first step in understanding the barriers to adoption of Digital Currency and/or Digital Accounts.<sup>95)</sup> They concluded the following:

1. ***There is a steady group of people that will continue to rely on cash, with some depending on cash:*** *There is a spectrum of self-reported reliance on cash – some consumers are more dependent, and some are closer to preference. This research found that whilst some had a reliance on cash, for others – particularly those with low financial resilience – the need to avoid overspending was such that they depended on cash. This is because, for these individuals, small budgetary errors could lead to harm such as unmanageable debt and difficulty affording essential goods.*
2. ***The key demographic factors driving dependence on cash are having a very low income and displaying characteristics of vulnerability*** *Some examples that drive dependence on cash are ill health, life events, low financial resilience, and lower financial or digital capability. These characteristics of vulnerability are present across most groups of respondents, in some more so than in others. Many of the individuals with a dependence on cash – though not all – are aged under 50.*
3. ***The more dependent/vulnerable could be at greater risk of harm:*** *If cash infrastructure declines, those with a reliance on cash may find accessing cash to be an increasing challenge. Some of those with a reliance on cash will already walk long distances and wait for extended periods of time to access cash if they do not have access to local, convenient cash infrastructure. This is harmful to those with long-term health conditions that limit mobility or their ability to spend extended periods of time in queues or outdoors. Whilst many have an aversion to pay-to-use ATM machines, some will resort to these in cases of emergency, spending money they may struggle to afford in order to access cash.*
4. ***The pandemic has affected the way people shop and the way businesses accept payments:*** *Looking ahead, we can see that some of the typologies in this research (Needs-based, Functional, and Older & disengaged) are likely to continue to rely on cash, while others have shown that they could be able to transition, though often facing psychological and behavioral barriers (Cash defenders, Impulse avoiders and Comfortable & capable). The ones that are dependent and likely to continue to use cash are more likely to have characteristics of vulnerability.*

## Examples

[Return to Top](#)

The following “desirements” are from the [White Paper](#) as identified by the [Object Management Group's](#)

report called [White Paper Analysis](#):

Table 72: Example of mapping Financial Inclusion requirements identified during the White Paper Analysis conducted by OMG.

<b>Requirements</b>	<p>B: B0007, B0008, B0009, B0010, B0011, B0012, B0013, B0014, B0015, B0018, B0019, B0028, B0029, B0030, B0031, B0033, B0034, B0035, B0038, B0041, B0043, B0045, B0046, B0047, B0048, B0049, B0054</p> <p>P: P0003, P0023, P0025, P0026, P0027</p> <p>R: R0011</p> <p>D: D0012, D0012, D0015, D0016, D0017</p>
---------------------	---

## Discussion of Examples

[Return to Top](#)

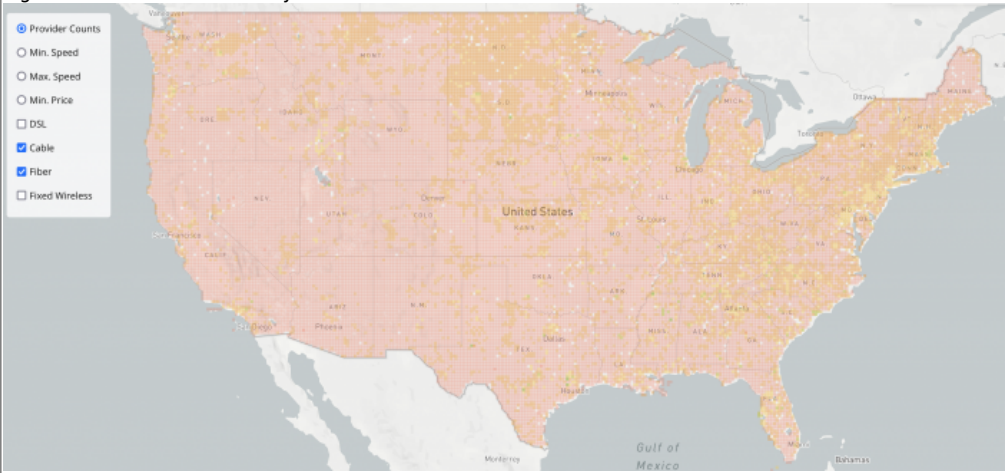
The following discussion covers both of the [Currency Models](#):

- [Digital Cash Model](#)
- [Digital Account Model](#)

Table 73: The Benefits identified in the **White Paper**

Statement No.	Statement	Comment
<b>B0007</b>	<b>Provide households and businesses a:</b> <b>1. convenient</b> <b>2. an electronic form of central bank money with</b> <b>a. safety</b> <b>b. liquidity</b>	<p>1. <b>Digital Cash:</b></p> <p>a. By definition offer, be liquid</p> <p>b. Depending on the implementation, be more convenient than physical cash</p> <p>c. Offer more safety than physical cash</p> <p>2. <b>Digital Accounts:</b></p> <p>a. Depending on the implementation, be more convenient than physical cash</p> <p>b. Offer more safety than physical cash</p> <p>c. Be less liquid than physical cash</p>
<b>B0008</b>	<b>Provide entrepreneurs a platform on which to create new financial products and services</b>	<p>1. <b>Digital Cash:</b> Since Digital Cash is new, there would be a need for more platforms that can handle Digital Cash. These platforms could be created by existing intermediaries or from new startups</p> <p>2. <b>Digital Accounts:</b> Since Digital Accounts are similar to existing intermediary accounts, the ability of entrepreneurs to create new financial products is limited.</p>
<b>B0009</b>	<b>Provide faster and cheaper payments (including cross-border payments)</b>	<p>1. <b>Digital Cash:</b> would be more efficient and safer than using Physical Cash when sending more cross-border</p> <p>2. <b>Digital Accounts:</b> would be more efficient and safer than using Physical Cash, BUT would require the receiver of the CBDC to have an account to receive the money. In essence, this means the people, not residents in the US and perhaps not US citizens have access to US accounts.</p>



Statement No.	Statement	Comment
B0010	Expand consumer access to the financial system	<p>Access to the financial systems implies <a href="#">Access to the Internet</a>. <b>Note:</b> This is beyond the scope of CBDC. Figure 25: Network Availability in the US</p>  <p>1. <b>Digital Cash:</b> would have all the same limitations as physical money as far as providing access to the financial system, however, the financial systems could provide gateways to-and-from a Digital Cash system allowing financial services to the underserved without having a physical presence.</p> <p>2. <b>Digital Accounts:</b> if people do not currently have access to existing intermediaries, the CBDC accounts would probably not improve that situation. For example, Know Your Customer.</p>
B0011	<p><b>Make payments:</b></p> <ol style="list-style-type: none"> <li>1. faster</li> <li>2. cheaper</li> <li>3. more convenient</li> <li>4. more accessible</li> </ol>	<p>1. <b>Digital Cash:</b></p> <ol style="list-style-type: none"> <li>a. Faster - Physical Cash is immediate</li> <li>b. Cheaper - Physical Cash costs nothing to use</li> <li>c. More Convenient - The use of cash is very convenient during a transaction and when the amount of cash is small. However, it is often inconvenient to obtain physical cash or to dispose of physical cash.</li> <li>d. More Accessible - Physical Cash is generally easy within the US to obtain within the US. However, see the Figure 25.</li> </ol> <p>2. <b>Digital Accounts:</b></p> <ol style="list-style-type: none"> <li>a. Faster - Digital Cash will have delays that need to be as fast as current account-based systems such as savings, checking, investment, direct pay, credit, debit cards, etc., and is dependent on electricity and network connectivity, see Figure 25.</li> <li>b. Cheaper - The main cost in Digital Accounts is most likely the cost of <a href="#">achieving consensus</a>.</li> <li>c. More Convenient - Digital Accounts must be as convenient to use as current account-based systems such as savings, checking, investment, direct pay, credit, debit cards, etc. Digital Accounts would be more convenient for large physical cash transactions. Depending on the implementation of the CBDC, Digital Cash and Digital Accounts may offer the same convenience.</li> <li>d. More Accessible - Unless more “financial infrastructure” is developed beyond the existing intermediary financial structures.</li> </ol>
B0012	Provide payment services to households and businesses around the clock, every day of the year	<p>Payment services imply Digital Accounts, which for those people already included in the financial system, it is not a problem. With the rise of FinTech solutions, many payment services already operate 24-7-365. However, if people are currently excluded from the Financial System, they must rely on physical cash or digital cash to pay bills. Often, in some areas within the U.S., there are no financial services nearby to make physical cash payments let alone 24-7-365! Although the private sector FinTech solutions are available when people have access to:</p> <ol style="list-style-type: none"> <li>1. Financial accounts</li> <li>2. Smart Phones</li> <li>3. Networks</li> </ol>
B0013	Provide immediate access to transferred funds	<ol style="list-style-type: none"> <li>1. <b>Digital Cash:</b> There are no problems with gaining access to transferred funds since they operate very similarly to the current Physical Cash system.</li> <li>2. <b>Digital Accounts:</b> As with most financial transactions, there is usually a need for a “settlement period”. Granted in the “blockchain” environments, these “settlement times” have been reduced from days to minutes. However, the same can be said with most FinTech solutions as well as <a href="#">Mobile Payment Systems</a> such as Apple Pay or Google Pay.</li> </ol>
B0014	Reduce costs and fees associated with certain types of payments	<p>FinTech is expanding and improving every day. There is also competition between FinTech vendors to compete for customers, so the costs should naturally come down. However, when intermediaries are required to complete a transaction, these intermediaries extract a price to allow the transactions. This is particularly a problem in Cross-Border transactions and the closer the transactions get to Peer-to-Peer (P2P) the less the cost.</p>

Statement No.	Statement	Comment
B0015	<b>Reduce cross-border costs to benefit:</b> 1. economic growth 2. enhance global commerce 3. improve international remittances 4. reduce inequality	See <b>B0014</b> .
B0018	<b>Allow the general public to make digital payments</b>	The FinTech industry would say that this already exists, especially with the rise of <a href="#">Mobile Payment Systems</a> such as Apple Pay or Google Pay.
B0019	<b>Provide the safest digital asset available to the general public, with no:</b> 1. associated credit 2. liquidity risk	The only way to offer the <b>safest digital asset</b> is to develop <a href="#">Digital Cash</a> .
B0028	<b>Offer the general public broad access to digital money:</b> 1. free from credit risk 2. liquidity risk	The only way to offer the <b>safest digital asset</b> is to develop <a href="#">Digital Cash</a> .
B0029	<b>Support basic purchases of:</b> 1. goods 2. services 3. pay bills 4. pay taxes	The FinTech industry would say that this already exists, especially with the rise of <a href="#">Mobile Payment Systems</a> such as Apple Pay or Google Pay.
B0030	<b>Support benefit payments directly to citizens</b>	The U.S. States like <a href="#">California</a> would claim that this already exists with <a href="#">Electronic Benefits Transfer (EBT)</a> . The FinTech industry would say that this is already possible, especially with the rise of <a href="#">Mobile Payment Systems</a> such as Apple Pay or Google Pay.
B0031	<b>Provide the general public broad access to digital money that is free from:</b> 1. credit risk 2. liquidity risk	The only way to offer the <b>safest digital asset</b> is to develop <a href="#">Digital Cash</a> .

Statement No.	Statement	Comment
B0033	<p><b>Support a level playing field in payment innovation for private-sector firms of all sizes</b></p>	<p>The U.S. Government already has programs available to help level the playing field. The Federal Reserve and the U.S. CBDC need to use the programs to help with <a href="#">Research Development Test &amp; Evaluation (RDT&amp;E) Funding</a>.</p> <p>Additional ways to help level the U.S. CBDC playing field:</p> <p><b>Small Business Innovation Research (SBIR):</b> The original charter of the SBIR program was to address four goals:<sup>96)</sup></p> <ol style="list-style-type: none"> <li>1. Stimulate technological innovation</li> <li>2. Use small businesses to meet Federal R/R&amp;D needs</li> <li>3. Foster and encourage participation by the socially and economically disadvantaged small businesses and those that are 51 percent owned and controlled by women, in technological innovation</li> <li>4. Increase private-sector commercialization of innovations derived from Federal R/R&amp;D, thereby increasing competition, productivity, and economic growth</li> </ol> <p><b>Small Business Technology Transfer (STTR):</b> The Small Business Technology Transfer program, or STTR, came later and was modeled after the SBIR program. Its goal, however, is to facilitate the transfer of technology developed by a research institution through the entrepreneurship of a small business concern (SBC). Research institutions include universities and Federally Funded Research and Development Centers, also referred to as FFRDCs. It is important to keep in mind that the applicant for an STTR award is always a small business.<sup>97)</sup></p> <p><b>Grants.gov:</b> Provide a common website for federal agencies to post discretionary funding opportunities and for grantees to find and apply to them. <a href="#">grants.gov</a></p> <p><b>SBA 8(a) Business Development Program:</b> Sections 7(j)(10) and 8(a) of the Small Business Act (15 U.S.C. §§ 636(j)(10) and 637(a)) authorizes the U.S. Small Business Administration (SBA) to establish a business development program, which is known as the 8(a) Business Development program. The 8(a) program is a robust nine-year program created to help firms owned and controlled by socially and economically disadvantaged individuals.</p> <p>Businesses that participate in the program receive training and technical assistance designed to strengthen their ability to compete effectively in the American economy. Also eligible to participate in the 8(a) program are small businesses owned by Alaska Native corporations, Community Development Corporations, Indian tribes, and Native Hawaiian organizations. Small business development is accomplished by providing various forms of management, technical, financial, and procurement assistance.</p> <p>SBA partners with federal agencies to promote maximum utilization of 8(a) program participants to ensure equitable access to contracting opportunities in the federal marketplace. Once certified, 8(a) program participants are eligible to receive federal contracting preferences and receive training and technical assistance designed to strengthen their ability to compete effectively in the American economy. <a href="https://www.sba.gov/federal-contracting/contracting-assistance-programs/8a-business-development-program">https://www.sba.gov/federal-contracting/contracting-assistance-programs/8a-business-development-program</a></p> <p><b>SBA-backed loan guarantees:</b> The U.S. Small Business Administration helps small businesses get funding by setting guidelines for loans and reducing lender risk. These SBA-backed loans make it easier for small businesses to get the funding they need. <a href="https://www.sba.gov/funding-programs/loans">https://www.sba.gov/funding-programs/loans</a></p> <p>Also see: <a href="#">Appendix C: Other Transaction Authority (OTA)</a></p>
B0034	<p><b>Generate new capabilities to meet the speed and efficiency requirements of the digital economy</b></p>	<p>See: <b>B0033</b> above.</p>
B0035	<p><b>Streamline cross-border payments by using:</b></p> <ol style="list-style-type: none"> <li>1. new technologies</li> <li>2. introducing simplified distribution channels</li> <li>3. creating additional opportunities for cross-jurisdictional collaboration and interoperability</li> </ol>	<p>See: <b>B0033</b> above.</p>
B0038	<p><b>Allow private-sector innovators to focus on:</b></p> <ol style="list-style-type: none"> <li>1. new access services</li> <li>2. distribution methods</li> <li>3. related service offerings</li> </ol>	<p>See: <b>B0033</b> above.</p>

Statement No.	Statement	Comment
B0041	<b>Support streamlining cross-border payments</b>	<a href="#">Mobile Payment Systems</a> already in many countries around the world. The barrier does not seem to be the technology or the desire on the part of the FinTech industry but the Geopolitical. Apple Pay participating banks in Africa, Europe, and the Middle East. Apple Pay works with many of the major credit and debit cards from the top banks. Just add your supported cards and continue to get all the rewards, benefits, and security of your cards. <a href="https://support.apple.com/en-us/HT206637">https://support.apple.com/en-us/HT206637</a> Google Pay users in the U.S. will be able to send money to Google Pay users in India and Singapore, thanks to a new integration with Western Union and Wise. By the end of the year, we expect that U.S. Google Pay users will be able to send money to people in more than 200 countries and territories through Western Union and to more than 80 countries through Wise. <a href="https://blog.google/products/google-pay/send-money-loved-ones-abroad/">https://blog.google/products/google-pay/send-money-loved-ones-abroad/</a>
B0043	<b>Promoting financial inclusion—particularly for economically vulnerable households and communities</b>	The financial industry is already happening through the use of low-cost <a href="#">Financial Technology (Fintech)</a> solutions rather than trying to extend the traditional financial products and services to the financially underserved. For example, the financial industry is now using FinTech to offer cashless <a href="#">Digital Transactions</a> , the advent of low-fee <a href="#">Robo-Advisors</a> , and the rise of <a href="#">Crowdfunding</a> and <a href="#">Peer-to-Peer Lending (P2P Lending)</a> .
B0045	<b>Enable rapid and cost-effective payment of taxes</b>	Sales taxes are already collected by the merchant at the point of sale. The Internal Revenue Service (IRS) uses third-party payment processors for payments by debit and credit card. It's safe and secure; your information is used solely to process your payment. <sup>98)</sup> 1. You can pay online or over the phone (see Payment Processor Contact Information below for phone payments) 2. You can pay using digital wallets such as PayPal and Click to Pay 3. There's a maximum number of card payments allowed based on your tax type and payment type 4. Employers' federal tax deposits cannot be paid by card; see how to pay employment taxes 5. For card payments of \$100,000 or more special requirements may apply Each state and local jurisdiction has different rules.
B0046	<b>Enable rapid and cost-effective delivery of: 1. wages, 2. tax refunds 3. other federal payments</b>	The U.S. States like <a href="#">California</a> would claim that this already exists with <a href="#">Electronic Benefits Transfer (EBT)</a> . This could be expanded to a national level but would require Laws and Regulations to change. According to the IRS <sup>99)</sup> : <i>The best and fastest way to get your tax refund is to have it electronically deposited for free into your financial account. The IRS program is called direct deposit. You can use it to deposit your refund into one, two, or even three accounts. Eight out of 10 taxpayers get their refunds by using Direct Deposit. It is simple, safe, and secure. This is the same electronic transfer system used to deposit nearly 98 percent of all Social Security and Veterans Affairs benefits into millions of accounts.</i>
B0047	<b>Lower transaction costs</b>	FinTech solutions as well as <a href="#">Mobile Payment Systems</a> such as Apple Pay or Google Pay have already brought the cost of a transaction down.
B0048	<b>Provide a secure way for people to save</b>	FinTech solutions as well as <a href="#">Mobile Payment Systems</a> such as Apple Pay or Google Pay already supports customers maintaining a positive balance.
B0049	<b>Promote access to credit</b>	FinTech solutions as well as <a href="#">Mobile Payment Systems</a> such as Apple Pay or Google Pay have already brought credit to customers.
B0054	<b>Attract risk-averse users to CBDC</b>	The only way to offer the <b>safest digital asset</b> is to develop <a href="#">Digital Cash</a> . See section answer for <a href="#">Question: 13. How could a CBDC be designed to foster operational and cyber resiliency? What operational or cyber risks might be unavoidable?</a>
P0003	<b>Complement current forms of money and methods for providing financial services</b>	The FinTech industry would say that this already exists, especially with the rise of <a href="#">Mobile Payment Systems</a> such as Apple Pay or Google Pay.
P0023	<b>CBDC would need to be readily transferable between customers of different intermediaries</b>	This is a place for International Standards to be created. There are lots of "common standards" that can apply to Blockchains. See within each of these sections for a list of applicable standards: 1. <a href="#">DIDO RA - Technical Standard Bodies</a> 2. <a href="#">DIDO RA - de facto Standards Bodies</a> Unfortunately, within the "blockchain" world, there is confusion about what constitutes a standard. Often, if something is Open Source, it is considered a standard. However, often these projects lack the rigor needed to be considered a "standard". Also, see the discussion in the DIDO RA on <a href="#">Talk Openly Develop Openly (TODO)</a> and look at the DIDO RA definition of a <a href="#">Standards Developing Organization (SDO)</a> .
P0025	<b>CBDC intermediary would need to verify the identity of a person accessing CBDC</b>	Many systems are now using <a href="#">Two-Factor Authentication (2FA)</a> requiring <a href="#">Biometrics</a> (i.e., facial recognition, fingerprints, etc) or <a href="#">One-Time PIN (OTP)</a> . These 2FA methods generally require the user to be physically present to successfully log in or to have access to a mobile device like a phone or tablet. Also see <a href="#">OMG DIDO-RA section on Authenticity</a> .
P0026	<b>CBDC transactions would need to be final and completed in real-time</b>	CBDC Transactions need to compete with the current Currency Model used by the financially excluded, which is primarily cash partly because it is "real-time". You see something, you want to buy it, you have the cash, and you complete the transaction then and there.

Statement No.	Statement	Comment																
P0027	CBDC a risk-free asset	<p>Obviously, cash is the ultimate risk-free asset readily available to the public at large. However, cash does have its risks too. For example: although cash is tangible and can be held in your hand, cash can be stolen or kickbacks required without a trace, which increases risks for people who use cash.</p> <p>This research identifies three key factors that drive cash reliance in general. In factors in order of the importance is <sup>100)</sup>:</p> <ol style="list-style-type: none"> <li><i>1. Avoiding overspending: For most people with a reliance on cash, avoiding overspending and living within their means was the main reason for relying on cash. Respondents felt that using cash stops them from spending more than they have, helps them to keep track of spending, and puts enough friction into the payments process to allow them to evaluate whether they want to go through with the purchase. The physical nature of cash was also helpful in making budgeting decisions easier, particularly among those with a low cognitive ability for budgeting.</i></li> <li><i>2. Ingrained habit: In all human behavior, there is a default option. For those in this research, when budgeting, using cash is often the default option. Using a different approach to budgeting would be cognitively effortful for many, and for those with low financial capabilities, very challenging.</i></li> <li><i>3. Distrust of alternatives: Many respondents have concerns about fraud, personal error, and privacy when considering using alternatives to cash such as credit or debit cards. Concern about fraud and personal error is often a function of low digital capacity.</i></li> </ol> <p><i>This is largely supported by the FCA’s Financial Lives survey, which outlines that:</i></p> <ol style="list-style-type: none"> <li><i>just over half (55%) of adults who rely on cash to a great or very great extent do so for reasons of convenience (e.g. because cash is more convenient (35%) or it is part of their daily routine (36%)).</i></li> <li><i>Under half (45%) rely on cash for budgeting reasons (e.g. to help them budget (33%))</i></li> </ol> <p>The Better than Cash Alliance held an event and as part of the program, they held a moderated an Oxford-style mock debate entitled “Is Cash the Enemy of Financial Inclusion?” which was a thought-provoking approach to discussing the pros and cons of cash in financial inclusion. Table 73 is a summary of that debate.<sup>101)</sup></p> <p>Table 73: Is Cash the Enemy of Financial Inclusion?<sup>102)</sup></p> <table border="1" data-bbox="474 835 1503 1629"> <thead> <tr> <th colspan="2" data-bbox="474 835 1503 863">Position</th> </tr> </thead> <tbody> <tr> <td data-bbox="474 863 992 919"><b>“Cash is not all bad for the financially excluded”</b></td> <td data-bbox="992 863 1503 919"><b>“Digital financial services can extend financial inclusion”</b></td> </tr> <tr> <td data-bbox="474 919 992 1052">Cash works for people who are unbanked – they have developed mechanisms that allow them to operate in the cash economy, so why “fix” a system that is not broken?</td> <td data-bbox="992 919 1503 1052">Digital payment services can bring huge cost savings and increase efficiency for payers. They are also often cheaper or the only access option for payees, especially in remote areas and rural communities</td> </tr> <tr> <td data-bbox="474 1052 992 1184">People like cash because it is tangible (unlike a digital wallet) and is accepted anywhere, which is important for functioning in local market economies.</td> <td data-bbox="992 1052 1503 1184">Digital financial services allow people to manage their money, better control how they use their funds, save for unpredictable needs such as health and emergencies, and invest in business opportunities and in their household</td> </tr> <tr> <td data-bbox="474 1184 992 1287">Cash can be cheaper because the ecosystem around it is mature versus a still-growing digital system, where players in the value chain are still looking for ways to get paid.</td> <td data-bbox="992 1184 1503 1287">Although cash is tangible and can be held in your hand, cash can be stolen or kickbacks required without a trace, which increases risks for people who use cash.</td> </tr> <tr> <td data-bbox="474 1287 992 1419">Digital systems take a long time to set up in uncertain environments and the current digital infrastructure does not solve the range of product and service needs – it’s better to reduce complexity, especially in uncertainty.</td> <td data-bbox="992 1287 1503 1419">Digital financial services provide clients, and women, in particular, greater privacy.</td> </tr> <tr> <td data-bbox="474 1419 992 1522">Cash can be easily understood it does not require memorizing passwords, help from an agent, or waiting for ages to talk to a “help desk” when there is a problem.</td> <td data-bbox="992 1419 1503 1522">Digital services create a financial history over time, and give people pathways to greater inclusion</td> </tr> <tr> <td data-bbox="474 1522 992 1629">Cash is often integrated culturally and changing cultural practices takes a lot of time... although in some cases it digitizes cultural practices so works really well.</td> <td data-bbox="992 1522 1503 1629">The informal economy often deals in cash as a way to avoid taxes, digital finance ensures that payments are handled in a more transparent way and supports inclusion in the formal economy.</td> </tr> </tbody> </table>	Position		<b>“Cash is not all bad for the financially excluded”</b>	<b>“Digital financial services can extend financial inclusion”</b>	Cash works for people who are unbanked – they have developed mechanisms that allow them to operate in the cash economy, so why “fix” a system that is not broken?	Digital payment services can bring huge cost savings and increase efficiency for payers. They are also often cheaper or the only access option for payees, especially in remote areas and rural communities	People like cash because it is tangible (unlike a digital wallet) and is accepted anywhere, which is important for functioning in local market economies.	Digital financial services allow people to manage their money, better control how they use their funds, save for unpredictable needs such as health and emergencies, and invest in business opportunities and in their household	Cash can be cheaper because the ecosystem around it is mature versus a still-growing digital system, where players in the value chain are still looking for ways to get paid.	Although cash is tangible and can be held in your hand, cash can be stolen or kickbacks required without a trace, which increases risks for people who use cash.	Digital systems take a long time to set up in uncertain environments and the current digital infrastructure does not solve the range of product and service needs – it’s better to reduce complexity, especially in uncertainty.	Digital financial services provide clients, and women, in particular, greater privacy.	Cash can be easily understood it does not require memorizing passwords, help from an agent, or waiting for ages to talk to a “help desk” when there is a problem.	Digital services create a financial history over time, and give people pathways to greater inclusion	Cash is often integrated culturally and changing cultural practices takes a lot of time... although in some cases it digitizes cultural practices so works really well.	The informal economy often deals in cash as a way to avoid taxes, digital finance ensures that payments are handled in a more transparent way and supports inclusion in the formal economy.
Position																		
<b>“Cash is not all bad for the financially excluded”</b>	<b>“Digital financial services can extend financial inclusion”</b>																	
Cash works for people who are unbanked – they have developed mechanisms that allow them to operate in the cash economy, so why “fix” a system that is not broken?	Digital payment services can bring huge cost savings and increase efficiency for payers. They are also often cheaper or the only access option for payees, especially in remote areas and rural communities																	
People like cash because it is tangible (unlike a digital wallet) and is accepted anywhere, which is important for functioning in local market economies.	Digital financial services allow people to manage their money, better control how they use their funds, save for unpredictable needs such as health and emergencies, and invest in business opportunities and in their household																	
Cash can be cheaper because the ecosystem around it is mature versus a still-growing digital system, where players in the value chain are still looking for ways to get paid.	Although cash is tangible and can be held in your hand, cash can be stolen or kickbacks required without a trace, which increases risks for people who use cash.																	
Digital systems take a long time to set up in uncertain environments and the current digital infrastructure does not solve the range of product and service needs – it’s better to reduce complexity, especially in uncertainty.	Digital financial services provide clients, and women, in particular, greater privacy.																	
Cash can be easily understood it does not require memorizing passwords, help from an agent, or waiting for ages to talk to a “help desk” when there is a problem.	Digital services create a financial history over time, and give people pathways to greater inclusion																	
Cash is often integrated culturally and changing cultural practices takes a lot of time... although in some cases it digitizes cultural practices so works really well.	The informal economy often deals in cash as a way to avoid taxes, digital finance ensures that payments are handled in a more transparent way and supports inclusion in the formal economy.																	
R0011	<b>Increased Risk to consumer's vulnerability to:</b> <b>1. loss</b> <b>2. theft</b> <b>3. fraud</b>	See P0027																
D0012	<b>Design should address privacy concerns by leveraging existing tools already in use by intermediaries</b>	See section 4.4 National Privacy Considerations/																

Statement No.	Statement	Comment
D0015	<b>Design should include any dedicated infrastructure required to provide a resilience to threats such as operational disruptions and cybersecurity risks</b>	See answer to <a href="#">Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?</a> ;
D0016	<b>Design should include offline capabilities to help with operational resilience of the payment system</b>	See answer to <a href="#">Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?</a> ;
D0017	<b>Design should include digital payments in areas suffering from large disruption, such as natural disasters</b>	See answer to <a href="#">Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?</a> ;
B = <a href="#">Benefit Considerations</a>		
P = <a href="#">Policy Considerations</a>		
R = <a href="#">Risk Considerations</a>		
D = <a href="#">Design Considerations</a>		

92) 93) 94)

Tp, Shabna Mol., [FINANCIAL INCLUSION: CONCEPTS AND OVERVIEW IN INDIAN CONTEXT](#), Abhinav-International Monthly Refereed Journal Of Research In Management & Technology, 3 (2014): 28-35, Accessed: 14 April 2022

<https://www.semanticscholar.org/paper/FINANCIAL-INCLUSION%3A-CONCEPTS-AND-OVERVIEW-IN-Tp/75a4f173e50c7d073890182fd80521e5bea45637>

95) 100)

Savanta: ComRes & the Financial Conduct Authority, [Understanding cash reliance - qualitative research](#), July 2021, Accessed 15 April 2022,

<https://www.fca.org.uk/publication/research/understanding-cash-reliance-qualitative-research.pdf>

96) 97)

SBIR, [Tutorial 1WHAT IS THE PURPOSE OF THE SBIR & STTR PROGRAMS?](#), Accessed: 14 April 2022,

<https://www.sbir.gov/tutorials/program-basics/tutorial-1#>

98)

Internal Revenue Service (IRS), [Pay Your Taxes by Debit or Credit Card or Digital Wallet](#), Accessed: 14 April 2022, <https://www.irs.gov/payments/pay-your-taxes-by-debit-or-credit-card>

99)

Internal Revenue Service (IRS), [Get Your Refund Faster: Tell IRS to Direct Deposit your Refund to One, Two, or Three Accounts](#), Accessed: 14 April 2022,

<https://www.irs.gov/refunds/get-your-refund-faster-tell-irs-to-direct-deposit-your-refund-to-one-two-or-three-accounts>

101) 102)

Better than Cash Alliance, [Is Cash the Enemy of Financial Inclusion?](#), Accessed: 15 April 2022,

<https://www.betterthancash.org/news/is-cash-the-enemy-of-financial-inclusion>



From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:brp:q03:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:brp:q03:start)

Last update: **2022/05/18 22:31**



# Question: 04. How might a U.S. CBDC affect the Federal Reserve's ability to effectively implement monetary policy in the pursuit of its maximum-employment and price-stability goals?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**How might a U.S. CBDC affect the Federal Reserve's ability to effectively implement monetary policy in the pursuit of its maximum employment and price stability goals?**

## Answer

[Return to Top](#)

## Overview

[Return to Top](#)

In order to answer this question, it is important to have some definitions that relate to Federal Reserve's ability to effectively implement monetary policy. Based on these definitions explore "*What is the Federal Reserves Monetary Policy*", and finally focus on non-Cash payments and how they relate to CBDC.

## Definitions

[Return to Top](#)

The Federal Reserve has defined the following terms:<sup>103)</sup>

Table 74: Definition of some key terms by the U.S. Federal Reserve.

<b>Discount Rate</b>	The <b>Discount Rate</b> is the interest rate charged by Federal Reserve Banks to depository institutions on short-term loans.
----------------------	--



<b>Federal Open Market Committee (FOMC)</b>	The <b>Federal Open Market Committee (FOMC)</b> formulates the nation's <b>Monetary Policy</b> . The voting members of the FOMC consist of the seven members of the Board of Governors (BOG), the president of the Federal Reserve Bank of New York, and presidents of four other Reserve Banks who serve on a one-year rotating basis. All Reserve Bank presidents participate in FOMC policy discussions whether or not they are voting members. The chairman of the Board of Governors chairs the FOMC meeting. The FOMC typically meets eight times a year in Washington, D.C. At each meeting, the committee discusses the outlook for the U.S. economy and monetary policy options.
<b>Federal Reserve Funds</b>	<b>Federal Reserve Funds</b> are the overnight lending rate at which banks borrow reserves from each other. The Federal Funds Rate is sensitive to changes in the demand for and supply of reserves in the banking system and thus provides a good indication of the availability of credit in the economy.
<b>Monetary Policy Instruments</b>	The Federal Reserve's three <b>Monetary Policy Instruments</b> are <b>Open Market Operations</b> , the <b>Discount Rate</b> , and <b>Reserve Requirements</b> .
<b>Inflation</b>	<b>Inflation</b> is a sustained increase in the general level of prices, which is equivalent to a decline in the value or purchasing power of money. If the supply of money and credit increases too rapidly over time, the result could be inflation.
<b>Monetary Policy</b>	<b>Monetary Policy</b> refers to what the Federal Reserve, the nation's central bank, does to influence the amount of money and credit in the U.S. economy. What happens to money and credit affects interest rates (the cost of credit) and the performance of the U.S. economy.
<b>Open Market</b>	<b>Open Market</b> means that the Fed doesn't decide on its own which securities dealers it will do business with on a particular day. Rather, the choice emerges from an "open market" in which the various securities dealers that the Fed does business with - the primary dealers - compete on the basis of price.
<b>Open Market Operations</b>	<b>Open Market Operations</b> involve the buying and selling of government securities. The term <b>Open Market</b> means that the Fed doesn't decide on its own which securities dealers it will do business with on a particular day. Rather, the choice emerges from an "open market" in which the various securities dealers the Fed does business with - the primary dealers - compete on the basis of price. <b>Open Market Operations</b> are flexible, and thus, the most frequently used tool of monetary policy.
<b>Reserve Balances</b>	Reserve Balances with Federal Reserve Banks is the amount of money that depository institutions maintain in their accounts at their regional Federal Reserve Banks.

## What is the Federal Reserves Monetary Policy

### [Return to Top](#)

Figure 26 illustrates the transmission of monetary policy. In the broadest terms, monetary policy works by spurring or restraining the growth of overall demand for goods and services in the economy. When overall demand slows relative to the economy's capacity to produce goods and services, unemployment tends to rise and inflation tends to decline. The FOMC helps stabilize the economy in the face of these developments through the stimulation of the overall demand using an easing of monetary policy that lowers interest rates. Conversely, when overall demand for goods and services is too strong, unemployment can fall to unsustainably low levels and inflation can rise. In these situations, the Federal Reserve guides economic activity back to more sustainable levels and keeps inflation in check by

tightening monetary policy to raise interest rates. This process of the FOMC eases and tightens monetary policy to achieve its goals.<sup>104)</sup>

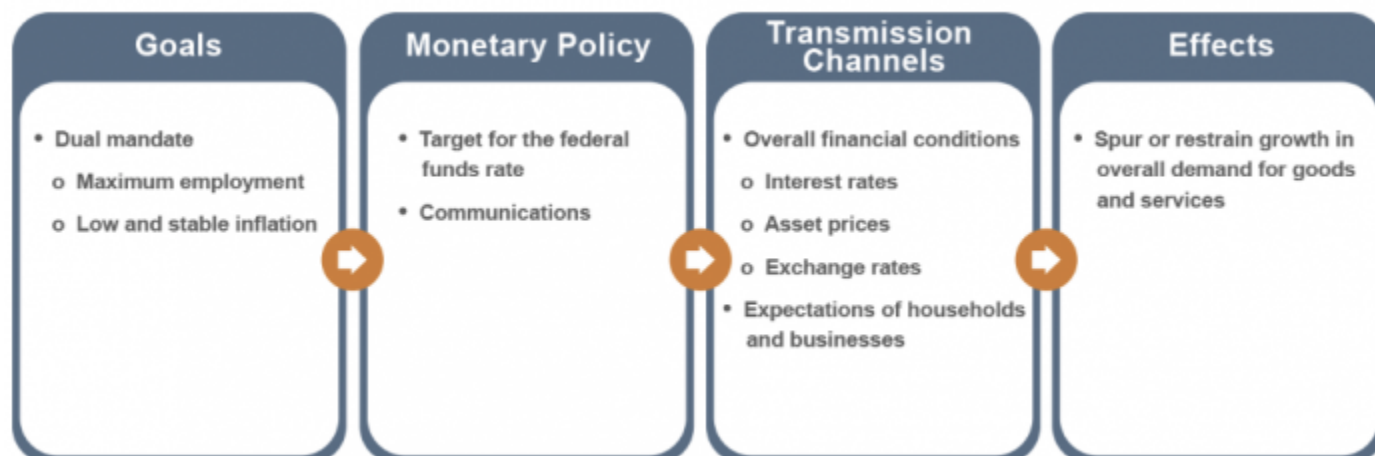


Figure 26: The transmission of Monetary Policy.<sup>105)</sup>

## CBDC as a non-Cash Payments

### [Return to Top](#)

On average, each day, U.S. consumers and businesses make noncash payments worth roughly  $\$1/2$  trillion currently using payments through:

- **debit cards**
- **credit cards**
- **electronic transfers**
- **checks**

**Note:** There is currently no tally for cryptocurrency payments.

To facilitate non-cash payments, intermediary banks hold **Reserve Balances** at the Federal Reserve. Payments are generally settled by transferring **Reserve Balances** between banks. Banks can also hold these balances to meet unexpected liquidity needs and to satisfy a number of regulatory requirements aimed at ensuring that banks are sound and that their customers' deposits are safe. Banks depend upon this borrowed money to a considerable extent in order to meet strict compliance requirements and pass stress tests used as the measurement of their financial stability.<sup>106)</sup>

Banks may borrow and lend reserves to each other depending on their needs and market conditions; as such, banks can use **Reserve Balances** both as a means of funding and as an investment. The federal funds rate is the interest rate that banks pay to borrow **Reserve Balances** overnight.

When a CBDC is created and goes public, CBDC payments will have to be added as a new way of making noncash payments. This means in order to obtain a better understanding of the banks' reserve currency requirements, all the CBDC payments in the bank need to be accounted for. In other words, these CBDC payments need to be added to the total tally of U.S. consumers' and businesses' noncash payments. This requires the CBDC to adopt a [Digital Account Model](#) leading to concerns about [End User Privacy](#).

To facilitate such payments, banks hold **Reserve Balances** at the Fed; payments can be settled by transferring **Reserve Balances** between banks. Banks also hold these balances to meet unexpected liquidity needs and to satisfy a number of regulatory requirements aimed at ensuring that banks are sound and that their customers' deposits are safe. Banks may borrow and lend reserves to each other depending on their needs and market conditions; as such, banks can use **Reserve Balances** both as a means of funding and as an investment. The federal funds rate is the interest rate that banks pay to borrow **Reserve Balances** overnight.

## Examples

[Return to Top](#)

The following “desirements” are from the [White Paper](#) as identified by the [Object Management Group's](#) report called [White Paper Analysis](#):

Table 75: Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG

<b>Benefits</b>	B0003, B0004, B0007, B0011, B0018, B0020, B0024, B0025, B0026, B0029, B0034, B0038, B0040, B0044, B0045, B0046, B0047, B0049, B0051
<b>Policies</b>	P0003, P0004, P0012, P0018, P0019, P0020, P0021, P0023, P0024, P0025, P0026
<b>Risks</b>	R0001, R0004
<b>Design</b>	D0004, D0005, D0009, P0010, P0018

## Example Discussion

[Return to Top](#)

Table 76: “Desirements” identified in the **White Paper** that have potential monetary policy impacts.

<b>Statement No.</b>	<b>Statement</b>	<b>Comment</b>
<b>B0003</b>	<b>Complement, rather than replace, current forms of money and methods for providing financial services</b>	The Cryptocurrencies and the CBDC need to be added to the tally of payments made by the intermediary banks in order for the Federal Reserve to calculate a correct <b>Reserve Balance</b> each bank needs to maintain overnight. So far, the Cryptocurrency payments have not had much of an impact on this calculation, but it is a matter of time before it does start having an impact. The adoption of a U.S. CBDC will definitely have an impact.
<b>B0004</b>	<b>Protect consumer privacy</b>	There is a fine line between collecting information about consumer transactions used to calculate the <b>Reserve Balance</b> for each bank and transgressing the required privacy requirements. See section <a href="#">4.4 National Privacy Considerations</a> .

Statement No.	Statement	Comment
B0007	<p><b>Provide households and businesses a convenient and electronic form of central bank money with:</b></p> <ol style="list-style-type: none"> <li><b>1. safety</b></li> <li><b>2. liquidity</b></li> </ol>	<p>See <b>P0018</b> - The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals. If it is amended to allow these accounts, then how will a <b>Reserve Balance</b> be calculated for the Federal Reserve commercial bank?</p>
B0011	<p><b>Make payments:</b></p> <ol style="list-style-type: none"> <li><b>1. faster</b></li> <li><b>2. cheaper</b></li> <li><b>3. more convenient</b></li> <li><b>4. more accessible</b></li> </ol>	<p>CBDC payments would be similar to the current non-cash payments done with debit cards, credit cards, electronic transfers, and checks. This has to be reported in order for the banks to calculate the <b>Reserve Balance</b> required by the Federal Reserve to banks. There is no reason that U.S. CBDC could not be treated similarly.</p>
B0018	<p><b>Allow the general public to make digital payments</b></p>	<p>The general public can already make digital payments using non-cash mechanisms such as debit cards, credit cards, electronic transfers, and checks</p>
B0020	<p><b>Maintain public confidence by not requiring mechanisms, such as deposit insurance</b></p>	<p>If the CBDC is treated like other non-cash mechanisms such as debit cards, credit cards, electronic transfers, and checks, there should be no reason to have an extra layer of protective insurance for CBDC.</p>
B0024	<p><b>Provide transactions finalized and completed in real-time</b></p>	<p>These transactions should be treated similarly to non-cash mechanisms such as debit cards, credit cards, electronic transfers, and checks. However, if a Stablecoin is used, then the transactions might be settled within minutes depending on the Consensus Algorithm used in the Stablecoin. See <a href="#">OMG DIDO-RA Consensus Algorithms</a>), answer to <b>B0025</b> below, and <b>R0010</b> - <i>CBDC has Risk of significant energy footprint similar to Cryptocurrencies.</i></p>
B0025	<p><b>Serve as a new foundation for the payment system</b></p>	<p>The CBDC could offer another mechanism to the existing non-cash mechanisms such as debit cards, credit cards, electronic transfers, and checks. However, in order to offer real-time settlements, it may need to use a different mechanism than the existing <a href="#">Automated Clearing House (ACH) Network</a> currently in use to electronically move money between banks accounts across the U.S. The current ACH network is run by an organization called Nacha, formerly the <a href="#">National Automated Clearing House Association (NACHA)</a>.</p>

Statement No.	Statement	Comment
<b>B0026</b>	<b>Provide a bridge between legacy and new payment services</b>	There definitely would need to be a bridge between the existing ACH-NACHA payment network and a U.S. CBDC, its associated Consensus Algorithms, and the network of nodes. However, in addition to the bridge between the two, there probably needs to exist a new consolidated frontend ( <a href="#">Application Programming Interface (API)</a> ?) that abstracts the type of payment from the participants in the transactions. In other words, the transaction should be agnostic to non-cash mechanisms such as debit cards, credit cards, electronic transfers, checks, and CBDC.
<b>B0029</b>	<b>Support basic purchases of:</b> <b>1. goods</b> <b>2. services</b> <b>3. pay bills</b> <b>4. pay taxes</b>	See the answer to <b>B0026</b> above. CBDC should be treated like any other payment form, even though under the hood, it might use a different payment network than the <a href="#">National Automated Clearing House Association (NACHA)</a> network.
<b>B0034</b>	<b>Generate new capabilities to meet the speed and efficiency requirements of the digital economy</b>	See answers to <b>B0025</b> , <b>B0025</b> and <b>B0029</b> above.
<b>B0038</b>	<b>Allow private-sector innovators to focus on:</b> <b>1. new access services</b> <b>2. distribution methods</b> <b>3. related service offerings</b>	By defining a new standardized <a href="#">Application Programming Interface (API)</a> as in <b>B0026</b> above, a marketplace of products can be developed by the private sector to help innovate the current payment ecosystem.

Statement No.	Statement	Comment
<b>B0040</b>	<b>Provide micropayment support</b>	<p>This is currently almost impossible with Credit and Debit cards because the cost of a transaction is so high that a vendor might lose money supporting small payments, let alone micropayments. A parallel network used by the CBDC might alleviate this problem depending on the <a href="#">Consensus Algorithm</a> used by the U.S. CBDC.</p> <p>As an example:  <i>You knew when you opened your merchant account that you'd have to pay for credit (and debit) card processing, but \$0.15 or \$0.20 per transaction (in addition to the percentage charge) didn't seem like it would be a big deal. Unfortunately, a lot of your customers come in and only buy a single item, maybe something for \$3.00 or less. They don't carry any cash and want to use their credit card. However, your margins are so thin on low-priced items that the fixed per-transaction fee you pay for processing can wipe out your profit. In fact, you might even lose money on some sales if the customer uses a credit card.</i><sup>107)</sup></p> <p>The <a href="#">Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010</a> permits businesses to impose a minimum purchase amount of up to \$10 for credit card use, but the minimum must be the same for all credit card issuers and payment card networks. Part of this legislation, the Durbin Amendment, contains the following provision:  <i>(3) NO RESTRICTIONS ON SETTING TRANSACTION MINIMUMS OR MAXIMUMS.-A payment card network shall not directly or through any agent, processor, or licensed member of the network, by contract, requirement, condition, penalty, or otherwise, inhibit the ability of any person to set a minimum or maximum dollar value for the acceptance by that person of any form of payment.</i></p>
<b>B0044</b>	<b>Facilitate access to digital payments</b>	See answers to <b>B0011, B0018, B0020, B0024, B0025, B0026</b> above.

Statement No.	Statement	Comment
<b>B0045</b>	<b>Enable rapid and cost-effective payment of taxes</b>	<p>Sales taxes are already collected by the merchant at the point of sale.</p> <p>The Internal Revenue Service (IRS) uses third-party payment processors for payments by debit and credit card. It's safe and secure; your information is used solely to process your payment. <sup>108)</sup></p> <ol style="list-style-type: none"> <li>1. You can pay online or over the phone (see Payment Processor Contact Information below for phone payments)</li> <li>2. You can pay using digital wallets such as PayPal and Click to Pay</li> <li>3. There's a maximum number of card payments allowed based on your tax type and payment type</li> <li>4. Employers' federal tax deposits cannot be paid by card; see how to pay employment taxes</li> <li>5. For card payments of \$100,000 or more special requirements may apply</li> </ol> <p>Each state and local jurisdiction has different rules.</p>
<b>B0046</b>	<b>Enable rapid and cost-effective delivery of:</b> <b>1. wages,</b> <b>2. tax refunds</b> <b>3. other federal payments</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>B0047</b>	<b>Lower transaction costs</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>B0049</b>	<b>Promote access to credit</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>B0051</b>	<b>Generate data about users' financial transactions similar to the current Commercial Bank<sup>109)</sup> and Nonbank Money</b>	
<b>P0003</b>	<b>Complement current forms of money and methods for providing financial services</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>P0004</b>	<b>Protect consumer privacy</b>	See answer <b>B0004</b> .
<b>P0012</b>	<b>The firms that operate interbank payment services are subject to federal supervision</b>	<p>Regardless of how the U.S. CBDC is implemented, for example Stablecoin, the <a href="#">Consensus Algorithms</a> need to include all the rules outlined in sections <a href="#">4.4 National Privacy Considerations</a>, <a href="#">4.5 National Security Considerations</a>, and <a href="#">4.6 International Considerations</a>. In other words, consensus includes the enforcement of the laws and regulations concerning Monetary Policy.</p>
<b>P0018</b>	<b>The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals</b>	<p>The easiest solution is to allow current intermediaries to process CBDC transactions using an upgraded payment system.</p> <p>See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.</p>



Statement No.	Statement	Comment
P0019	<b>Federal Reserve accounts for individuals represent a significant expansion of the Federal Reserve's role in the financial system and the economy</b>	The easiest solution is to allow current intermediaries to process CBDC transactions using an upgraded payment system. See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
P0020	<b>The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
P0021	<b>The intermediaries would operate in an open market for CBDC services</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
P0023	<b>CBDC would need to be readily transferable between customers of different intermediaries</b>	This would require standardization ( <a href="#">Application Programming Interface (API)</a> ?) that each intermediary would use to transfer money. The interface could be in the form of Web Services, Remote Procedure Calls (RPC), <a href="#">Common Object Request Broker Architecture (CORBA)</a> , <a href="#">Data Distribution Service (DDS)</a> or other interprocess communication mechanisms defined using <a href="#">ISO/OMG Interface Definition Language (IDL)</a> , <a href="#">Web Services Interface Language (WSDL)</a> , etc.
P0024	<b>CBDC would need to comply with the U.S. robust rules</b>	See answer to <b>P0012</b> above.
P0025	<b>CBDC intermediary would need to verify the identity of a person accessing CBDC</b>	The Federal Open Market Committee (FOMC) is interested in the <b>Reserve Balances</b> of financial institutions within the U.S. There, if the transaction has one end of the transaction as a U.S. institution, then the ID of the individuals in the transaction is required.
P0026	<b>CBDC transactions would need to be final and completed in real-time</b>	See answers to <b>B0024</b> and <b>B0025</b> above.
B0013	<b>Provide immediate access to transferred funds</b>	See answers to <b>B0024</b> and <b>B0025</b> above.
R0001	<b>Risk of affecting financial-sector market structure</b>	See answers to <b>B0025</b> , and <b>B0025</b> above.
R0004	<b>Risk to the efficacy of monetary policy</b>	See answer to <b>B0003</b> above.
D0004	<b>Design should influence how the Federal Reserve might affect monetary policy</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
D0005	<b>Design could affect monetary policy implementation and interest rate control by altering the supply of reserves in the banking system</b>	From a Monetary Policy perspective, only the <b>Reserve Balances</b> is important. As long as the <b>Reserve Balances</b> account for Cryptocurrency and U.S. CBDC balances there should be little impact on the Monetary Policy.



Statement No.	Statement	Comment
<b>D0009</b>	<b>Design should allow for significant foreign demand for CBDC, further complicating monetary policy implementation</b>	The only reason to use the U.S. CBDC Stablecoin over U.S. Dollars is the potential for faster transactions using the CBDC transactions than in traditional ACH transactions. This would mean that before a transaction is to begin, the money in U.S. Dollars (or other currency) would be transferred to U.S. Stablecoins and the transaction would be conducted in Stablecoins. Once the transaction is completed, the Stablecoins could be changed quickly for U.S. Dollars. The only reason to hold onto the Stablecoins is to conduct more transactions using the Stablecoin network.
<b>D0010</b>	<b>Design should consider the potential for interest-bearing CBDC as a new policy tool on the channels of influence in monetary policy</b>	This would vary greatly from the current way the Credit Cards, Debit Cards, and Checks currently work. These are backed by accounts that can receive interest. For example, debit cards and checking accounts can pay interest on positive balances. These checking accounts could maintain separate balances for U.S. Dollars and for Stablecoins. But since Stablecoins would be backed by U.S. Dollars anyway, it seems a bit of a moot point unless the value of the U.S. Dollar and the U.S. Stablecoins are allowed to diverge.
<b>R0018</b>	<b>Risk a CBDC could fundamentally change the structure of the U.S. financial system, altering the private sector and central bank:</b> <b>1. roles</b> <b>2. responsibilities</b>	See answers to <b>B0025</b> , and <b>B0025</b> above.
<b>B = Benefit Considerations</b>		
<b>P = Policy Considerations</b>		
<b>R = Risk Considerations</b>		
<b>D = Design Considerations</b>		

103)

The Federal Reserve Education.org, [Monetary Policy Basics](https://www.federalreserveeducation.org/about-the-fed/structure-and-functions/monetary-policy), Accessed: 17 April 2022, <https://www.federalreserveeducation.org/about-the-fed/structure-and-functions/monetary-policy>

104) 105)

Federal Reserve, [Monetary Policy: What Are Its Goals? How Does It Work?](https://www.federalreserve.gov/monetarypolicy/monetary-policy-what-are-its-goals-how-does-it-work.htm) Accessed: 18 April 2022, <https://www.federalreserve.gov/monetarypolicy/monetary-policy-what-are-its-goals-how-does-it-work.htm>

During the 2008 financial crisis, many big banks failed or faced insolvency issues due to liquidity problems. The FDIC ratio is in line with the international Basel standard, created in 2015, and reduces banks' vulnerability in the event of another financial crisis.

107)

Chris Motola, [Can You Set A Minimum Purchase Amount For Credit & Debit Card Payments?](https://www.merchantmaverick.com/can-merchants-set-minimum-amounts-on-card-transactions/), 14 January 2022, Accessed: 18 April 2022,

<https://www.merchantmaverick.com/can-merchants-set-minimum-amounts-on-card-transactions/>

108)

Internal Revenue Service (IRS), [Pay Your Taxes by Debit or Credit Card or Digital Wallet](#), Accessed: 14

April 2022, <https://www.irs.gov/payments/pay-your-taxes-by-debit-or-credit-card>  
<sup>109)</sup>

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:brp:q04:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:brp:q04:start)

Last update: **2022/05/18 22:36**



# Question: 05. How could a CBDC affect financial stability? Would the net effect be positive or negative for stability?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

1. **How could a CBDC affect financial stability?**
2. **Would the net effect be positive or negative for stability?**

## Answer

[Return to Top](#)

## Overview

[Return to Top](#)

To answer these questions, it is important to first have a good working definition of **Financial Stability**.

***Financial Stability** reflects the ability of the financial system to consistently supply the credit intermediation and payment services that are needed in the real economy if it is to continue on its growth path.*<sup>110)</sup>

When defining concepts like *stability* and the things that *affect* and *maintain*, providing to define the opposite definition (i.e., **Financial Instability**).

***Financial Instability** occurs when problems (or concerns about potential problems) within institutions, markets, payments systems, or the financial system in general significantly impair the supply of credit intermediation services - so as to substantially impact the expected path [growth path] of real economic activity.*<sup>111)</sup>

## How could a CBDC affect financial stability?

[Return to Top](#)

Eric S. Rosengren discusses the process (i.e., Model) of propagating Financial Instability, see Figure 27. There are two major factors presented in the diagram: **Increase In Uncertainty** and **Deterioration in banks' Balance Sheets** which are pertinent to a U.S. CBDC and can trigger the propagation of **Financial Instability** (i.e., the opposite of **Financial Stability**). These concerns are also echoed in the **Executive Summary** of the [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#) or **White Paper**.

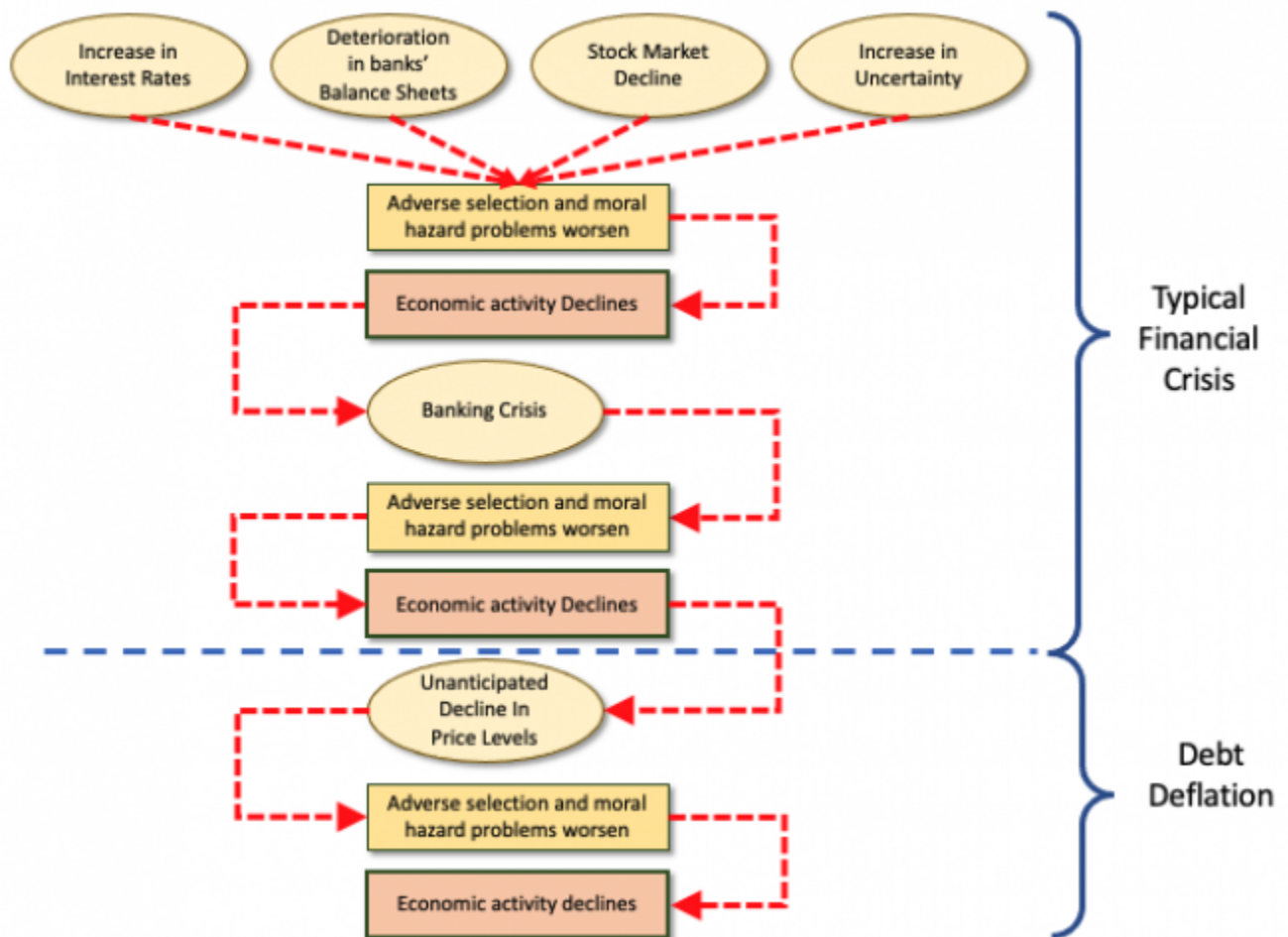


Figure 27: Propagation of Financial Instability in Industrialized Countries<sup>112)</sup>

## Increase in Uncertainty

### [Return to Top](#)

*For a nation's economy to function effectively, its **citizens must have confidence in its money and payment services**. The Federal Reserve, as the nation's central bank, works to maintain the public's confidence by fostering monetary stability, financial stability, and a safe and efficient payment system.*

The part of the statement that “*citizens must have confidence in its money and payment services*” emphasizes one of the triggers described by Rosengren's Model, “*Increase In Uncertainty*”.

Some of the “*Uncertainty*” introduced by a U.S. CBDC to the financial system have been defined by the

**White Paper** and already discussed in [Question: 10. How should decisions by other large economy nations to issue CBDCs influence the decision whether the United States should do so?](#)

Table 77: “Desirements” identified in the **White Paper** that have potential international impacts.

Statement No.	Statement	Comment
<b>R0003</b>	<b>Risk to the safety and stability of the financial system</b>	If there is a major hack to the CBDC, this could trigger a “lack of confidence” not just in the CBDC, but in the U.S. Dollar and perhaps The Federal Reserve.
<b>R0005</b>	<b>New payment services could pose Risks to:</b> <b>1. financial stability</b> <b>2. payment system integrity</b> <b>3. other Risks</b>	If there is a major hack to the CBDC, this could trigger a “lack of confidence” not just in the CBDC, but in the U.S. Dollar and perhaps The Federal Reserve.

In addition, many additional risks to the “Uncertainty” introduced by a U.S. CBDC to the financial system have already been discussed in Answer to [Question: 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?](#):

- [1. Risk of a Software Crisis](#)
- [2. Risk of Lack of Stakeholder Buy-In](#)
- [3. Risk Due to Poor Community of Interest \(CoI\) Governance](#)
- [4. Risk Due to lack of Broad, Wide Ranging Security Planning](#)
- [5. Risk of Data being hacked due weak Security Infrastructure](#)
- [6. Risk of Meta-Data being hacked due weak Security Infrastructure](#)
- [7. Risk of Business Processes Being Hacked](#)
- [8. Risk of competing Currency Models for the CBDC](#)

## Deterioration in banks’ Balance Sheets

[Return to Top](#)

Table 78 lists some highlights from some other Answers the OMG members have already answered regarding “*Deterioration in banks’ Balance Sheets*”.

Table 78: Potential deterioration in banks’ Balance Sheets are already covered by OMG answers to these Questions.

- [Question: 04. How might a U.S. CBDC affect the Federal Reserve’s ability to effectively implement monetary policy in the pursuit of its maximum-employment and price-stability goals?](#)
- [Question: 06. Could a CBDC adversely affect the financial sector? How might a CBDC affect the financial sector differently from stablecoins or other nonbank money?](#)
- [Question: 14. Should a CBDC be legal tender?](#)

## Would the net effect be positive or negative for stability?

[Return to Top](#)

### Overview

[Return to Top](#)

As the question states, there are positives and negatives on both sides. The OMG's answers to a couple of the **White Paper** have already addressed some of these issues. Obviously, the overall goal is to have overwhelmingly more positives than negatives. At this point negatives and positives are purely speculative without further understanding of exactly what the U.S. CBDC will be.

For example, in the “desirements” identified by [Object Management Group](#) from the [White Paper](#) and summarized in the [White Paper Analysis](#) are used as the basis for the ambivalent answer. From the “desirements”, it appears that there are two main sets of requirements when it comes to determining potential interest payments. Each of the sets is dependent on how the CBDC is to be modeled:

- **Cash Model** - these are requirements with CBDC characteristics most closely aligned with a simple cash model
- **Account Model** - these are requirements with CBDC characteristics most closely aligned with the account model (i.e, savings, checking, investment, direct pay, credit, debit cards, etc.)

It is only through System Engineering including a proper requirements analysis that CBDC can be defined. It may also be determined that the CBDC could actually represent two different things that need to be developed independently but in parallel. Without this analysis, all positives or negatives are merely speculative and reflect the understanding, biases, and prejudices of the individuals.

### Summary

[Return to Top](#)

In summary, determining the “positives” and “negatives” is dependent on the management of the U.S. CBDC Systems Engineering process, how well it is monitored and how well it can adapt over time. **Note:** One stakeholder's positive is another stakeholder's negative. For example, abiding by the [Privacy Laws and Regulations](#) is highly desirable from the End User perspective, but not from Law Enforcement.

<sup>110)</sup> <sup>111)</sup>

Eric S. Rosengren, Federal Reserve Bank of Boston, [Defining Financial Stability, and Some Policy Implications of Applying the Definition](#), 3 June 2011, Accessed: 27 April 2022, <https://www.bostonfed.org/news-and-events/speeches/defining-financial-stability-and-some-policy-implications-of-applying-the-definition.aspx>

<sup>112)</sup>  
Frederic S. Mishkin, [The Causes and Propagation of Financial Instability: Lessons for Policymakers](#), Kansas City Federal Reserve, pages 55-96, the graphic on page 74. Accessed: 27 April 2022,

<https://www.kansascityfed.org/documents/3591/pdf-s97Mishk.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q05:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q05:start)

Last update: **2022/05/18 21:38**



# Question: 06. Could a CBDC adversely affect the financial sector? How might a CBDC affect the financial sector differently from stablecoins or other nonbank money?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) \ [Provide Feedback](#)

## Question

[Return to Top](#)

1. **Could a CBDC adversely affect the financial sector?**
2. **How might a CBDC affect the financial sector differently from Stablecoins or other nonbank money?**

## Answer

[Return to Top](#)

## Overview

[Return to Top](#)

To answer the question it is important to first define what is meant by [Financial Sector](#), [Financial Market](#) and [Clearinghouse](#)

The **Financial Sector** refers to businesses, firms, banks, and institutions providing financial services and supporting the economy and encompasses several industries such as banking and investment, consumer finance, mortgage, money markets, real estate, insurance, retail, etc. The adoption of a U.S. CBDC will not affect all of the Financial Service industries and it will not affect each one in the same way. In general terms, the **Financial Sector** is used as an indicator of the health of the economy because it generates revenue through interest rates, mortgages, loans, debt finance, and capital funds, consequently spurring economic growth meaning the weaker the Financial Sector, the weaker the economy. This is why the question is so important.



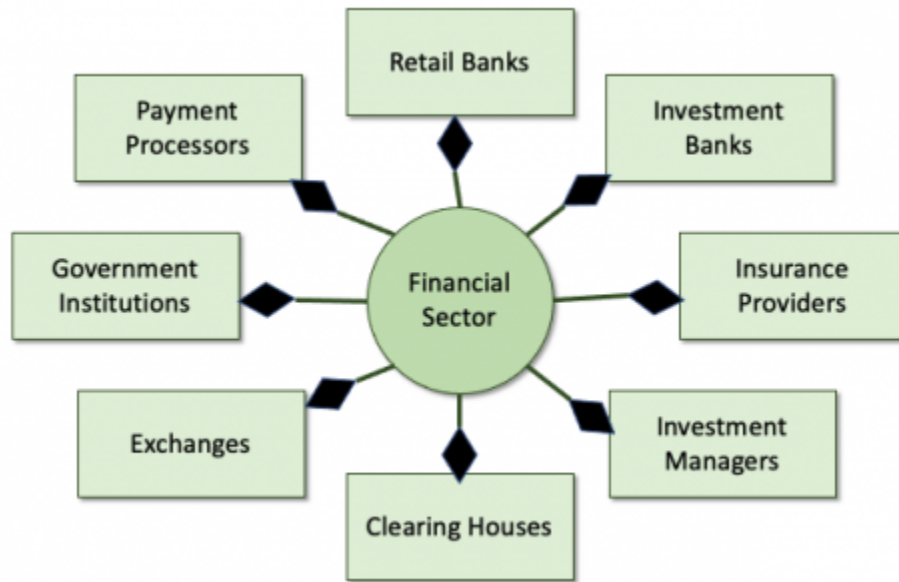


Figure 28: The Composition of the Financial Services

Sometimes, the Financial Sector is falsely equated to [Financial Markets](#) which is a broad term and includes various types of markets where companies requiring investment can borrow money at a low cost.

*These financial markets are regulated by independent regulatory bodies with strict rules and regulations. They have stringent and mandatory reporting and compliance standards. Any violation by companies, investors, brokers, banks, financial institutions, or any other authorized bodies can lead to heavy penalties and, in extreme cases, cancellation of license.* <sup>113)</sup>

Figure 29 provides a graphical representation of the composition of the Financial Markets.

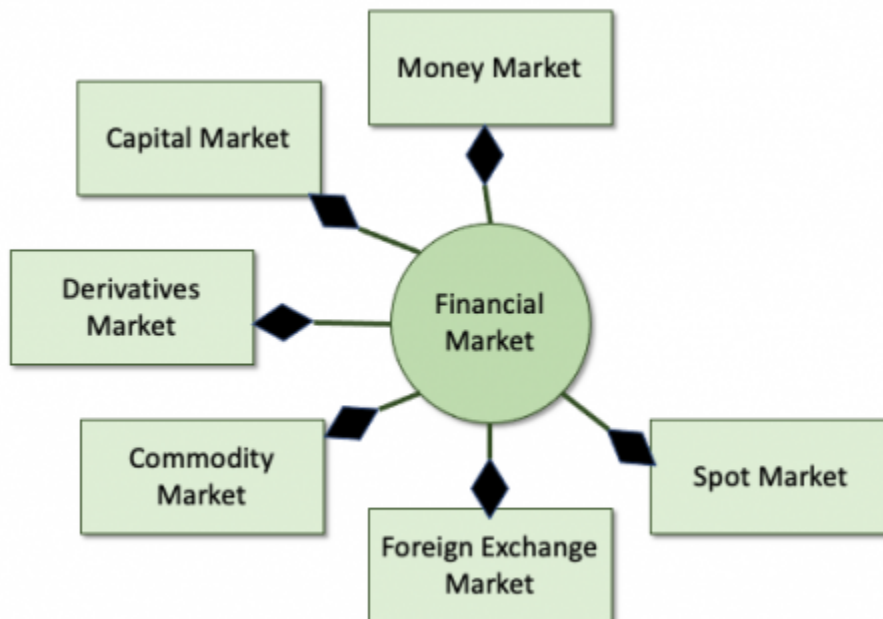


Figure 29: The Composition of the Financial Market

At the heart of the U.S. CBDC (Stablecoin) will be a [DIDO Platform](#) (i.e. [Ethereum](#), [Hyperledger](#), [Iota](#), [Hedera](#), etc.). Each DIDO Platform has its own [Consensus Mechanism](#) (i.e., [Proof-of-Work \(PoW\)](#), [Proof-of-Stake \(PoS\)](#), etc.). Within the U.S. CBDC, the [DIDO Platform Consensus](#) will act as a Clearinghouse for [Transactions](#) within the DIDO Platform (see [Figure 30](#)).



Figure 30: The relationship between a buyer, a seller and a Clearinghouse.

## 1. Could a CBDC adversely affect the financial sector?

[Return to Top](#)

### Technically

[Return to Top](#)

Each of the **Financial Sector** components will respond differently to the use of a U.S. CBDC depending on how much they want to support the use of CBDC as an alternative to the approved Clearinghouse. The Financial Sectors normally using U.S. Dollars on both sides of a transaction could use something like the [ACH/CBDC network proposal](#) ( see [Figure 22](#). This should require a minimum of change in their current processes and require them to be able to hold U.S. Dollars and U.S. CBDC in the pertinent accounts. The main benefit of using a CBDC Network should be the increase in speed (almost real-time) for settlements since the U.S. CBDC will use an automated [Consensus Mechanism](#). However, in order to check for Privacy and Criminal Activity by enforcing the [National Privacy Concerns](#) and [National Security Concerns](#) as well as respecting [International Concerns](#), the Consensus process most likely needs to be extended to help enforce the existing laws and regulations. This extension could rely heavily on the use of [Artificial Intelligence \(AI\)](#) and [Intelligent Agents](#).

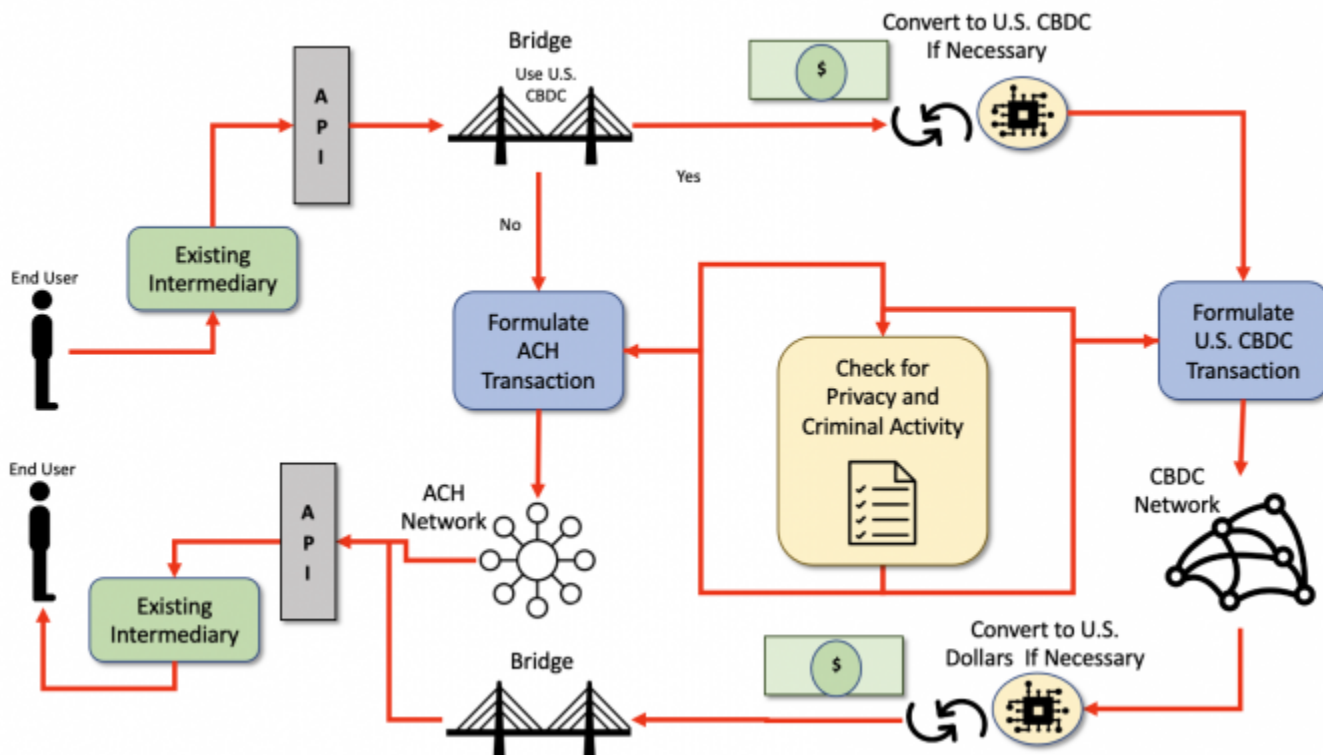


Figure 31: Theoretical Very Simplified Dual ACH-CBDC Network Concept.

For those **Financial Sector** components that use U.S. Dollar-to-Asset transactions, the appropriate Clearinghouses could also support U.S. CBDC-to-Asset the speed of the clearing may be faster since securing the U.S. CBDC would be near real-time.

For those **Financial Sector** components that do not use U.S. Dollar to Dollar transactions, the individual Clearinghouses need to address the problem individually

## Reputation

[Return to Top](#)

Obviously, if there is a breach or hack in the U.S. CBDC, all the **Financial Sector** components would be affected. See the existing [Risks](#) identified in the **White Paper** and the response to [Question: 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?](#)

## 2. How might a CBDC affect the financial sector differently from Stablecoins or other nonbank money?

[Return to Top](#)

There is an entire section on Stablecoin. See section [4.3 Stablecoins](#).

Currently, Stablecoins and nonbank money need to be converted to U.S. Dollars in order for the money to be used within the financial sector.

113)

Madhuri Thakur and Dheeraj Vaidya, What is the Financial Market?, Wall Street Mojo, Accessed: 25 April 2022, <https://www.wallstreetmojo.com/financial-market/>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q06:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q06:start)

Last update: **2022/05/18 21:38**



# Question: 07. What tools could be considered to mitigate any adverse impact of CBDC on the financial sector? Would some of these tools diminish the potential benefits of a CBDC?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

1. **What tools could be considered to mitigate any adverse impact of CBDC on the financial sector?**
2. **Would some of these tools diminish the potential benefits of a CBDC?**

## Answer

[Return to Top](#)

Before an answer can be formulated to the question, it is important to clarify the part of the question **mitigate any adverse impact of CBDC**. Since there is not currently a U.S. CBDC nor even a design for a U.S. CBDC, at this point in time, the adverse impacts are conjecture. Therefore, it is not possible to Mitigate<sup>114)</sup> the adverse impact of an unknown.

Consequently, the following question will be answered:

- **What tools could be considered to address any negative aspects of a CBDC in the financial sector?**

Probably the biggest negatives for the CBDC would be similar to those that are currently the biggest problem of Cryptocurrencies. These include:

- Lack of a solid, U.S. CBDC Platform
- Lack of adherence to reporting requirements on transactions, thus supporting criminal activity
- Lack of well defined and understood metrics and assessment of the overall value of the currency

### Lack of a Solid CBDC Platform

[Return to Top](#)

The Financial Sector could be adversely affected by U.S. CBDC failing due to inadequate planning,

designing, and implementation of a CBDC Platform. Many of these inadequacies could be addressed by using the proper tools during the creation, development, and deployment of the CBDC. Many of these tools have been eluded to throughout this response and have been identified in the [OMG DIDO-Reference Architecture \(DIDO-RA\)](#).

In summary, some of these tools are listed here.

By all descriptions, the U.S. CBDC is primarily a large [System-of-Systems \(SoS\)](#) or even an SoS of SoSs. Some of these would ideally already exist and some will need to be created. The new systems are predominately a [Software \(SW\)](#) effort. Yes, there will be some specialized [Hardware\(HW\)](#) required, but the primary focus appears to be Software (including [Commercial-Off-The-Shelf \(COTS\)](#), [Government Off-The-Shelf \(GOTS\)](#), or [Modified Off-The-Shelf \(MOTS\)](#)). This software will ultimately need to be [Managed](#) and [Modified](#).

- See Section [Question: 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?](#) for more specifics.

### **Would some of these tools diminish the potential benefits of a CBDC?**

[Return to Top](#)

The following tools are used during Requirements Analysis:

- [Assessing Requirements](#)
- [ISO/IEC 25030:2007 SQuaRE -- Quality Requirements](#)

The following tools are used during Modelling:

- [SQuaRE -- System and Software Quality Models](#)
- [SQuaRE -- Data Quality Model](#)
- [Business Motivation Model \(BMM\)](#)
- [Business Process Model And Notation \(BPMN\)](#)
- [Common Warehouse Metamodel \(CWM\)](#)
- [Distributed Ontology, Model, and Specification Language \(DOL\)](#)
- [Semantics Of Business Vocabulary and Rules \(SBVR\)](#)
- [Systems Modeling Language \(SysML\)](#)
- [Unified Architecture Framework \(UAF\)](#)
- [Unified Modeling LanguageTitle \(UML\)](#)

The following tools are used to aid in the development of software, particularly the development of [Open Source Software \(OSS\)](#).

- [Archiving and Release Management](#)
- [Bug and Issue Tracking](#)
- [Code Reviews](#)
- [Contributor License Agreements \(CLA\)](#)
- [GitHub Management at Corporate Scale](#)
- [Logging Tools](#)

- [Open Source Paradigm](#)
- [Project Quality](#)
- [Source Code Scanning and License Compliance](#)
- [Tracking Project Health](#)
- [How to create an open source program](#)
- [Measuring your open source program's success](#)
- [Tools for managing open source programs](#)
- [Using open source code](#)
- [Participating in open source communities](#)
- [Recruiting open source developers](#)
- [Starting an open source project](#)
- [Improve your open source development impact](#)
- [Shutting down an open source project](#)
- [Building leadership in an open source community](#)
- [Setting an Open Source Strategy](#)

## Lack of Reporting and Oversight

### [Return to Top](#)

According to Jason Bloomberg<sup>115)</sup>, the Cryptocurrency transactions can be classified into eight different categories, see Figure 32, and Table 79.

1. **Speculation** †
2. Darknet
3. Money Laundering
4. Ransomware
5. Evading Sanctions
6. Crypto Theft
7. Hacking Crypto Infrastructure
8. **Legitimate** †

**Note:** † Considered useful to the economy

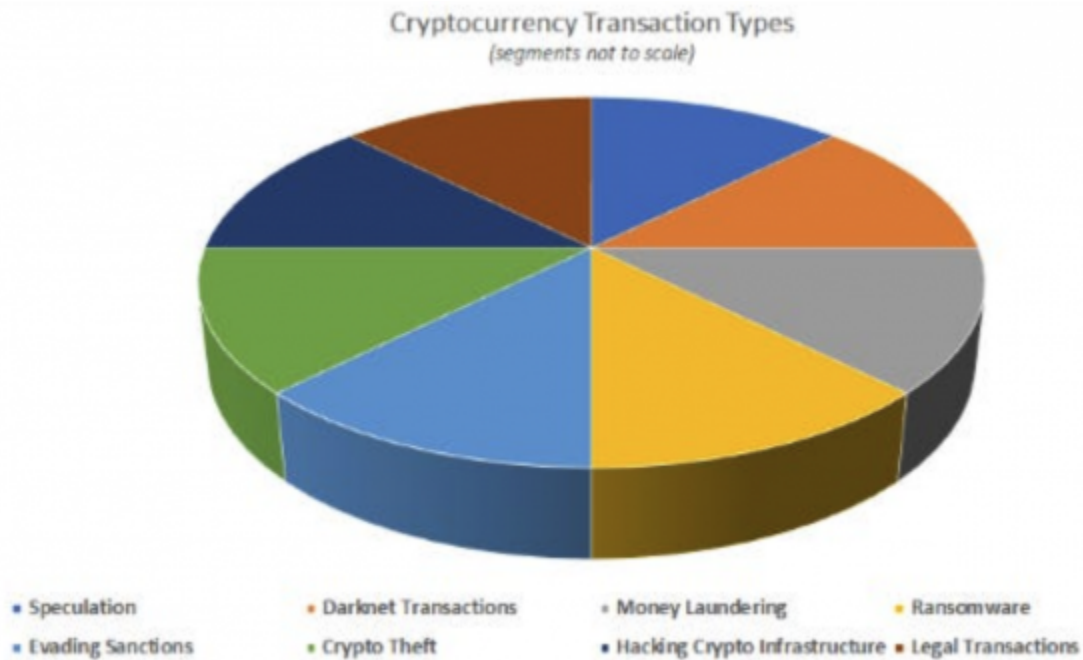


Figure 32: Eight Common Cryptocurrency Transaction Types.<sup>116)</sup>

Of the eight types of Crypto Transactions, only 2 would be considered useful to an economy: **Speculation** and **Legitimate**. The remainder of the Transaction Types are not considered desirable and should be actively discouraged by a U.S. CBDC as is currently the case with the U.S. Dollar. See Sections [4.5 National Security Considerations](#), and [4.6 International Considerations](#).

**Note:** Even though **Speculation** is not considered bad *per se*, it has come under further U.S. Federal Scrutiny. See the [Volker Rule](#) which limits the types and kinds of speculation that financial institution can participate in. A U.S. CBDC would need to follow similar rules and not provide a “back door” around these kinds of transactions.

Even the much-touted Privacy aspect of the cryptos is a double-edged sword. Granted, it does offer some anonymity to transactions, but without proper safeguards and assessment of the Crypto and its platform, there can be privacy breaches leading to harm. See Section [4.4 National Privacy Considerations](#). Sometimes these breaches have to do with fraud and theft of Cryptos, other times they can divulge proprietary aspects of transactions such as who is transacting with whom and when.

Table 79: Taxonomy of the Transactions Types used in Cryptocurrencies.<sup>117)</sup>

Rank	Cryptocurrency Transaction Type	Description
1	<b>Speculation</b>	Speculation is far from being the only reason to conduct transactions with crypto. <sup>118)</sup>



Rank	Cryptocurrency Transaction Type	Description
2	<b>Darknet Transactions</b>	<p>The Darknet consists of parts of the Internet that standard search engines cannot reach – those dark corners of the Web where purveyors of contraband from illegal drugs to child pornography do business. In fact, if it weren't for crypto, the Darknet would be a mere shadow of its current self – and Bitcoin remains the coin of the realm. “Bitcoin is the most common form of payment for drug sales on darknet marketplaces and is emerging as a desirable method to transfer illicit drug proceeds internationally,” according to the US Drug Enforcement Agency’s (DEA’s) 2017 National Drug Threat Assessment Report. “Bitcoin is the most widely used virtual currency due to its longevity and growing acceptance at legitimate businesses and institutions worldwide.”<sup>119)</sup></p>
3	<b>Money Laundering</b>	<p>Remember the piles of illicit currency from Scarface, or for that matter, Breaking Bad? Back in the day, turning criminal gains into legitimate assets required processing mountains of cash. Not so much anymore. Today, in spite of (or perhaps because of) dramatic improvement in anti-money laundering (AML) regulatory enforcement, the money laundering action has largely moved to crypto. “97% of criminal Bitcoin directly received by [crypto] exchanges flowed into those Located in countries with weak AML laws,” writes CipherTrace Cryptocurrency Intelligence in its report Cryptocurrency Anti-Money Laundering Report 2018 Q3. “Cryptocurrency exchanges in countries with weak AML regulation receive nearly 5% of their payments directly from criminal sources.”</p> <p>In particular, given China’s restrictions on the movement of capital, crypto has become quite popular for evading its laws. “CUBS [Chinese Underground Banking Systems] money brokers sell Bitcoin to drug traffickers for cash earned from drug sales in the US, Australia, and Europe. This drug cash is then sold to Chinese nationals in exchange for Bitcoin the Chinese nationals use to transfer the value of their assets outside of China,” according to the DEA report. “Many China-based firms manufacturing goods used in TBML [Trade Based Money Laundering] schemes now prefer to accept Bitcoin. Bitcoin is widely popular in China because it can be used to anonymously transfer value overseas, circumventing China’s capital controls.”<sup>120)</sup></p>

Rank	Cryptocurrency Transaction Type	Description
4	<b>Ransomware</b>	<p>Ransomware may now be less popular than cryptojacking, but it still remains a potent form of criminal extortion – and it’s simpler than ever. “Easy-to-use ‘ransomware as a service’ can be purchased cheaply on the Darknet, and at least one vendor offers customer support for users of its malware,” writes Michael Baker, Founder, and Principal at Mosaic451, a bespoke cybersecurity service provider and a consultancy, and a member of the Forbes Technology Council. “Would-be hackers who don’t want to purchase off-the-shelf ransomware can hire black-hat coders for custom development. All of these services are bought and sold using – you guessed it – cryptocurrency.”</p> <p>Even our phones aren’t safe from this pernicious application of crypto. “It is likely that ransomware will target connected devices containing personal data such as photos, emails, and even fitness progress information,” according to The cyber threat to UK business 2016/2017 Report by the National Cyber Security Centre of the National Crime Agency in the UK. “Ransomware on connected watches, fitness trackers, and TVs will present a challenge to manufacturers,” the report continues. “This data may not be inherently valuable, and might not be sold on criminal forums but the device and data will be sufficiently valuable to the victim that they will be willing to pay for it.”<sup>121)</sup></p>
5	<b>Evading Sanctions</b>	<p>It’s no surprise that countries like North Korea are desperate for hard currency – and crypto gives them one avenue to obtain it. “Crypto-currencies have the added advantage to the DPRK [North Korea] of giving them more ways to circumvent US sanctions,” according to Lourdes Miranda, cryptocurrency analyst, and financial crimes investigator at MirandaFinIntel Consulting, and Ross Delston, an attorney and certified AML specialist who frequently serves as an expert witness. “DPRK can create their own crypto-currencies or use established ones like Bitcoin. Having their own crypto-currency would also facilitate their ability to open online accounts under the guise of a non-adversarial nation using anonymous communication to conceal the user’s locations and usage on the internet.”</p> <p>Furthermore, while the United States and many of its allies have sanctions against such countries as North Korea and Iran, there are also economic sanctions against much larger economies like Russia that encourage Mr. Putin’s empire to make serious investments in crypto.</p> <p>Such investments, in fact, take place at the nation-state level. “[The] Russian government is about to take a step to start diversifying financial reserves into Bitcoin since Russia [is] forced by US sanctions to dump US Treasury bonds and [take] back US dollars,” according to Vladislav Ginko, an economist at the Russian Presidential Academy of National Economy and Public Administration, which is ironically funded by the Russian government itself. “These sanctions and the will to adopt modern financial technologies lead Russia to the way of investing its reserves into Bitcoin.”<sup>122)</sup></p>

Rank	Cryptocurrency Transaction Type	Description
6	<b>Crypto Theft</b>	<p>Money laundering, ransomware, and state-sponsored sanctions evasion all have a spine-tingling James Bond flavor to them – but what about simple theft? “CipherTrace revealed a three-fold increase in cryptocurrency thefts during the first half of 2018 compared with the entire year of 2017,” according to the Cryptocurrency Anti-Money Laundering Report 2018 Q3 by CipherTrace Cryptocurrency Intelligence. “CipherTrace estimates this trend will bring the total stolen and reported in 2018 to well over \$1 billion by the end of [2018].”</p> <p>The FBI, in fact, is warning about a type of theft that is targeting holders of small amounts of crypto. “Virtual currency is increasingly targeted by tech support criminals, with individual victim losses often in the thousands of dollars,” according to the FBI Public Service Announcement I-032818-PSA from March 2018. “Victims contact fraudulent virtual currency support numbers usually located via open-source searches. The fraudulent support asks for access to the victim’s virtual currency wallet and transfers the victim’s virtual currency to another wallet for temporary holding during maintenance. The virtual currency is never returned to the victim.”<sup>123)</sup></p>
7	<b>Hacking Crypto</b>	<p>Why bother stealing crypto if you can simply print more for yourself? That’s exactly what a particular group of criminals accomplished earlier in 2019 by targeting weaknesses in Ethereum Classic, one of the most popular cryptos behind Bitcoin. “We observed repeated deep reorganizations of the Ethereum Classic blockchain, most of which contained double spends,” reports Mark Nesbitt, Security Engineer at Coinbase. “The total value of the double spends that we have observed thus far is 219,500 ETC (~\$1.1M).”</p> <p>Double spending means taking the same unit of crypto and spending it twice – the online equivalent of running your greenbacks through a copier. A victimless crime, perhaps? You be the judge.<sup>124)</sup></p>
8	<b>Legal Use</b>	<p>Let us not forget the eighth type of crypto transaction: legal transactions that exchange crypto for goods and services – you know, like real money. Some crypto fans would have you believe that using crypto at your local coffee shop – or even sending funds to your relatives in Venezuela for buying food there – will be the prominent use of crypto at some point in the near future.</p> <p>Don’t believe it. “Cryptocurrencies will likely become a bigger part of the cybercrime realm,” concludes Yaya Jata Fanusie, director of analysis for the Center on Sanctions and Illicit Finance at the Foundation for Defense of Democracies. “Any police and intelligence departments dealing with cyber issues need to deepen their expertise on cryptocurrencies and blockchain technology.”<sup>125)</sup></p>

## Would some of these tools diminish the potential benefits of a CBDC?

[Return to Top](#)

Thinking about the U.S. CBDC as just another form of U.S. Currency and requiring the implementation to enforce the same rules will allow the leveraging of existing tools. See Section [4.7 Dual Payment Networks](#).

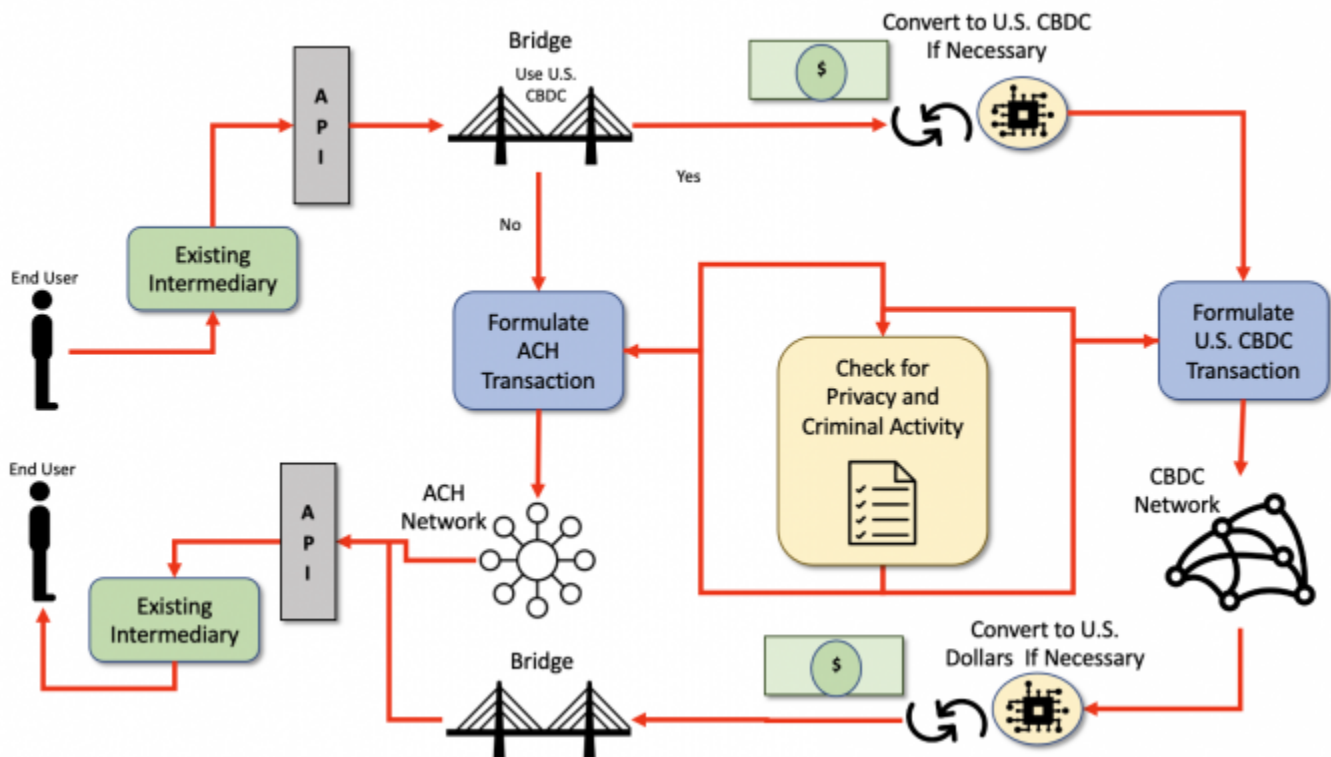


Figure 33: Theoretical Very Simplified Dual ACH-CBDC Network Concept.

There will most undoubtedly need to be more tools developed and the existing ones updated to counteract the “arms race” between criminal activity and the security of the Financial Services.

## Measuring Value

[Return to Top](#)

*The question is I do not understand where the backing of Bitcoin is coming from, you have to really stretch your imagination to infer what the intrinsic value of bitcoin is. I haven't been able to do it.*  
 Alan Greenspan, former chairman of the Federal Reserve. <sup>126)</sup>

A major problem confronting the Cryptocurrency world is the lack of tools and metrics to assess the intrinsic value of a Cryptocurrency offering. Unfortunately, at the present, most of the ways of assessing a cryptocurrency's values are to use non-empirical methods. Yes, some of the data can be empirical in nature (i.e., Market Cap), but the majority rely on feelings, emotions, and groupthink.

Table 80 provides a list developed by Richard Knight on the Seven Steps to Analyzing Crypto Projects Before Investing<sup>127)</sup>. It is interesting to note, that only the first step on **Check the Market Listing** uses empirical data, all the others rely on non-empirical data.

Table 80: Seven Steps to Analyzing Crypto Projects Before Investing<sup>128)</sup>

Step	Activity	Description
1	<b>Check the Market Listing</b>	<p>The first step is to look up the project on a cryptocurrency aggregator. The two largest cryptocurrency aggregators are CoinMarketCap and Coingecko. CMC is the most well-known while CoinGecko is known for more smaller-cap projects.</p> <p>These sites provide a high-level overview of the project: trading history, crypto ranking, a brief description of the project as well as the primary links to the project website and the project's social media links. <sup>129)</sup></p> <ol style="list-style-type: none"> <li>1. Project Ranking</li> <li>2. Market Cap</li> <li>3. Price History</li> <li>4. Trading Volume &amp; Liquidity</li> <li>5. Circulating Supply vs Total Supply</li> <li>6. The Price</li> </ol>
2	<b>Visit the Project Website</b>	<p>If the initial review of the project details on the cryptocurrency aggregator site looks positive, then the next step would be to check out the project website. Visiting a project's official website is a must!</p> <p>There is no excuse for a poorly developed website. Today it is very easy and relatively inexpensive to develop a clean and functional website. The project website should be well put together, functional and openly share details about the project, the people behind it, the roadmap, and the investors (if applicable).</p> <p>If the website is of poor quality, has spelling mistakes, is reluctant to disclose to the team members, or even worse is a copy-and-paste of a prior fork, then these are all cause for concern and should be avoided. <sup>130)</sup></p> <ol style="list-style-type: none"> <li>1. The Team (developers, executives, partners, advisors)</li> <li>2. The Road Map &amp; Vision</li> <li>3. Investors</li> </ol>
3	<b>Check Social Media Profiles</b>	<p>If everything looks good at this point, the next step is to check the social media profiles. This step will take a bit more time to assess. <sup>131)</sup></p> <ol style="list-style-type: none"> <li>1. Twitter</li> <li>2. Telegram / Discord</li> <li>3. Reddit</li> </ol>
4	<b>Assess the Community</b>	<p>It's likely been said many times and worth saying again — No community, no future. It is the community supporting the project which makes it successful! It can't be underestimated the importance of the community. If you are familiar with either Doge or Shibu, it was the community that brought these projects to great heights. The enthusiasm and size of the community play a large role in the initial and continued success of the project.</p> <p>Look for cryptocurrencies with strong, active communities. This is a good sign that there is genuine interest and belief in the project. Again, it's worth noting that Reddit is a great place to start researching the community and gaining 'street knowledge' not otherwise available anywhere else. <sup>132)</sup></p>

Step	Activity	Description
5	<b>Read the White Paper</b>	<p>A white paper is a document created by a crypto project that provides investors with technical information about the project, including the concept, the roadmap as well as how the project plans to grow and succeed. A project's white paper can provide insight into the inner workings of the project. Although many white papers may be highly technical, it is an important data point in assessing the quality of the project and the team behind it.</p> <p>If there is no White Paper, generally this is seen as a red flag. Also, White Papers with spelling mistakes, unnecessary technicality, or lacking basic grammar and punctuation are also red flags. <sup>133)</sup></p>
6	<b>Understand the Utility &amp; Use Case</b>	<p>For the long-term viability of a project, it needs to have a well-defined and clear use case. Does the project solve an important problem? If you are looking to invest in this project for the long term, then the answer needs to be a definitive YES.</p> <p>A project's success is directly related to something which its users will need (or want). While gaming and metaverse projects may not at first glance solve an important problem, they do offer something people want. No matter the niche or project, it must be able to solve an important problem (or need). When assessing the utility or use case of a project, it's important to look at both the current demand and potential future demand. Does the potential future demand include worldwide adoption or is it only local? If you are not able to determine the reasons or motivations for significant future demand, then then it's likely not a project you will want to hold for the long term. <sup>134)</sup></p>
7	<b>Conduct Scam Checks</b>	<p>Unfortunately, there are many scams within crypto and these scams are becoming increasingly more sophisticated, such as malicious contracts and rug pulls which are very difficult to detect for the average investor. To help protect against these potential scams as well as provide additional (technical) analysis of the project, there are many free online tools that can help. <sup>135)</sup></p> <p>Some of the tools:</p> <ol style="list-style-type: none"> <li>1. Scamsniper</li> <li>2. BSCheck</li> <li>3. RugDoc</li> <li>4. Token Sniffer</li> </ol>

However, investors are used to a rich set of tools and metrics to assess the quality of investments. Here are some of the metrics (i.e., tools) used to assess the worthiness of the investment. Some widely used examples of metrics used to assess stocks values are:

<caption>Some Existing tools (i.e., metrics) used by traditional investors.

Table 81:

- Debt-to-Equity ratio (D/E)
- Free Cash Flow (FCF)
- Price/Earnings-to-Growth (PEG) ratio
- Trailing Price-to-Earning (P/E)
- Forward Price-to-Earning (Forward P/E)
- Market Capitalization
- Market Value
- The Volatility Index (VIX)

- High-Low Index
- Bullish Percent Index
- Moving Averages

## Would some of these tools diminish the potential benefits of a CBDC?

### [Return to Top](#)

What tools are available, and which ones can be used with a U.S. CBDC is dependent on the system requirements, design, implementation of the CBDC, and ultimately which [Asset Class](#) it becomes. For the most part, the current tools set in use for the U.S. Dollar should be applicable to the CBDC with only minor tweaks if it is considered as a **cash or cash equivalent** asset. Obviously, the [Currency Model](#) selected for the CBDC (i.e., [Digital Cash](#) versus [Digital Account](#)) and how the CBDC is implemented (i.e., [Stablecoins](#)) all become factors in the tools used and the modifications those tools may need.

<sup>114)</sup>

Collins Dictionary, To mitigate something means to make it less unpleasant, serious, or painful. Accessed: 5 May 2022, <https://www.collinsdictionary.com/us/dictionary/english/mitigate>

<sup>115)</sup>, <sup>116)</sup>, <sup>117)</sup>, <sup>118)</sup>, <sup>119)</sup>, <sup>120)</sup>, <sup>121)</sup>, <sup>122)</sup>, <sup>123)</sup>, <sup>124)</sup>, <sup>125)</sup>

Jason Bloomberg, [The Eight Most Popular Cryptocurrency Transaction Types Are Not What You Expect](#), Forbes, 19 July 2019, Accessed 5 May 2022,

<https://www.forbes.com/sites/jasonbloomberg/2019/01/19/the-eight-most-popular-cryptocurrency-transaction-types-are-not-what-you-expect/?sh=4680b45616ea>

<sup>126)</sup>

Jason Bloomberg, [What Is Bitcoin's Elusive Intrinsic Value?](#), Forbes, 26 June 2017, Accessed: 5 May 2022, <https://www.forbes.com/sites/jasonbloomberg/2017/06/26/what-is-bitcoins-elusive-intrinsic-value/?sh=435db04f7194>

<sup>127)</sup>, <sup>128)</sup>, <sup>129)</sup>, <sup>130)</sup>, <sup>131)</sup>, <sup>132)</sup>, <sup>133)</sup>, <sup>134)</sup>, <sup>135)</sup>

Richard Knight, [How to Evaluate a Cryptocurrency - 7 Steps to Analyzing Crypto Projects Before Investing](#), 3 January 2022, Accessed: 5 May 2022,

<https://medium.datadriveninvestor.com/how-to-evaluate-a-cryptocurrency-c4c9d37ebff>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q07:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q07:start)

Last update: **2022/05/18 21:38**





# Question: 08. If cash usage declines, is it important to preserve the general public's access to a form of central bank money that can be used widely for payments?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**If cash usage declines, is it important to preserve the general public's access to a form of central bank money that can be used widely for payments?**

## Answer

[Return to Top](#)

The answer to this question is out of the scope of the [Object Management Group](#) and its members. Therefore, this question has not been addressed in the response.

From:  
<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:  
[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q08:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q08:start)

Last update: **2022/05/16 21:35**





# Question: 09. How might domestic and cross-border digital payments evolve in the absence of a U.S. CBDC?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**How might domestic and cross-border digital payments evolve in the absence of a U.S. CBDC?**

## Answer

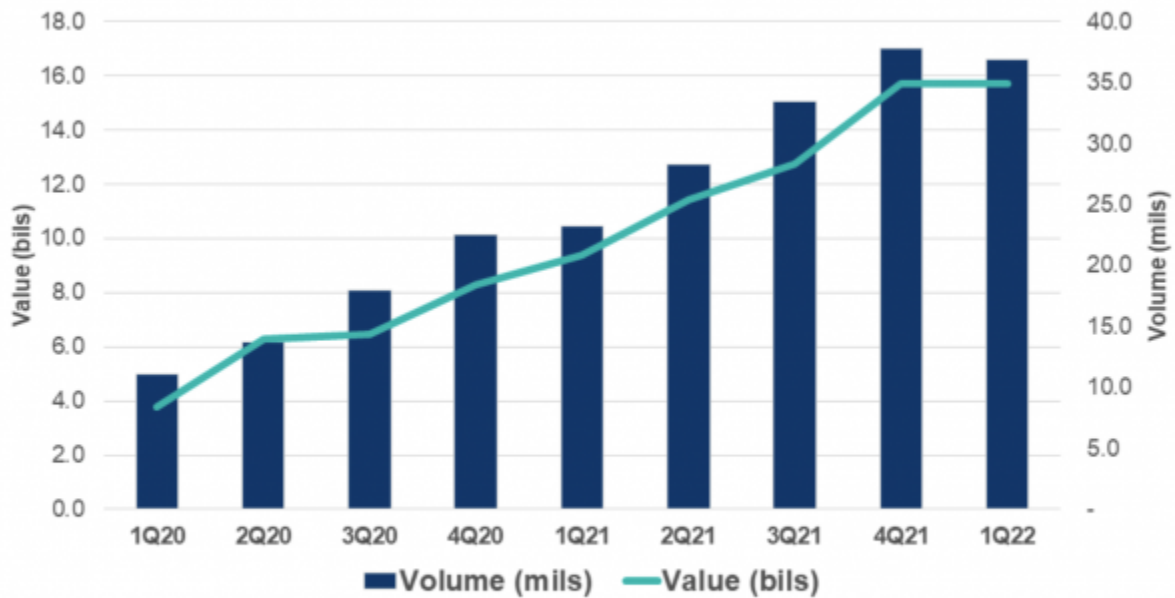
[Return to Top](#)

Without the advent of a U.S. CBDC, there are a few possible scenarios that will evolve. Some existing areas will be the use of:

- Cryptocurrencies (i.e., Bitcoin, Ethereum, etc.) to transfer money across borders
- [Europay MasterCard®, and Visa \(EMV\)](#)
- [Mobile Payment](#) systems such as PayPal, Venmo, Zelle, CashApp, Apple Pay, and Google Pay
- [Payment Cards](#) such as Credit Cards, Debit Cards, Charge Cards, Prepaid Cards or Electronic Benefits Transfer (EBT)
- [Prepaid Cards](#) issued by banks and branded by major credit card companies such as Visa, Mastercard, Discover, and American Express
- [Gift Card](#) issued by international stores and merchants such as Amazon, airlines, and hotels
- [Real-Time Payments \(RTP\) Network](#)

*The RTP® network from The Clearing House is a real-time payments platform that all federally insured U.S. depository institutions are eligible to use for payments innovation. With mobile technology and digital commerce driving the need for safer and faster payments in the U.S., financial institutions of all sizes are taking advantage of the RTP network's capabilities to create or enhance digital services for their corporate and retail customers.<sup>136)</sup>*

### RTP Quarterly Payment Activity



**1Q22** • 36.8 million transactions for \$15.7 billion

Real-time Payment Activity by Quarter.<sup>137)</sup>

Figure 34:

<sup>136)</sup> <sup>137)</sup>

The Clearing House, Real-Time Payments for All Financial Institutions, First Quarter 2022, Accessed: 5 May 2022, <https://www.theclearinghouse.org/payment-systems/rtp>

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q09:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q09:start)

Last update: **2022/05/18 21:38**



# Question: 10. How should decisions by other large economy nations to issue CBDCs influence the decision whether the United States should do so?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**How should decisions by other large economy nations to issue CBDCs influence the decision on whether the United States should do so?**

## Answer

[Return to Top](#)

No “desirements” are expressed about needing or wanting to be the first among the other large economy nations to issue a CBDC. In many ways, building a CBDC is like landing a man on the moon. It is an extremely complicated undertaking, with lots of parts and lots of requirements. See section [3.0 White Paper Analysis](#) for the “desirements” called out in the **White Paper**.

Beyond the **White Paper** there is a lot of discussion about CBDC, large systems engineering projects, and what works and does not work for large systems. Probably the most important “implied” requirement is that the CBDC is a [Mission-Critical System](#) with a long [Lifespan](#).

A major difference between a cryptocurrency and a national currency is that people's lives and the viability of the country depend and rely on its currency, whatever form its form. Built around the currency is a complex monetary system as well as an entire national economy that includes financial resources and management. The national economy encompasses the value of all goods and services manufactured within a nation. In essence, the national economy is the backing behind the U.S. Dollar. Adding to the complexity of the U.S. currency issues is that “The dollar has been the world's reserve currency since the U.S. and its allies agreed at the 1944 Bretton Woods conference to peg it to a rate of \$35 per ounce of gold. According to the International Monetary Fund, the dollar's share of global reserves stands at 59%, far above the euro at 20.5%.”<sup>138</sup>. This extends the U.S. Currency and, by proxy, the U.S. CBDC well beyond the boundaries of a national economy.

These are some of the reasons why a U.S. CBDC is much larger, complex, and trickier to create than any other national CBDC, let alone any simplistic cryptocurrency or large products offered to the public by large corporations. The following example is meant to highlight the difference between large commercial

complex products and a CBDC.

Example: If a commercial, very large, complex system (such as Facebook) has a failure or has a temporary outage, there are probably very few lives at stake (if any) or even placed in jeopardy as a result of the loss of commercial service. This is because the commercial system is **NOT** mission-critical. However, when a CBDC is deployed and there is a failure or a temporary outage – people's lives, livelihoods, or life savings could be wiped out – making the CBDC a Mission Critical system. Over and above the criticality of a CBDC to a nation and its people, the use of this currency as a Reserve Currency throughout the world makes it obvious that the breadth and scope of the U.S. CBDC are more critical than other CBDCs.

An excellent place to start understanding the U.S. CBDC is to first understand money as it currently is and how it works. Daniel Kurt<sup>139)</sup> describes how money works as follows:

*Whether we pull out paper bills or swipe a credit card, most of the transactions we engage in daily use currency. Indeed, money is the lifeblood of economies around the world. Currency refers to paper money or coins that are in circulation. But currency is actually only a small piece of the monetary economy and is just one consideration when looking at the total money supply.*

*Indeed, most money today exists as credit money or as electronic records stored in databases in banks or financial institutions. But still, the bread and butter of everyday transactions is currency, and that is what we will look more closely at here.*

- *Currency is the physical money in an economy, comprising the coins and paper notes in circulation.*
- *Currency makes up just a small amount of the overall money supply, much of which exists as credit money or electronic entries in financial ledgers.*
- *While early currency derived its value from the content of precious metal inside it, today's fiat money is backed entirely by **social agreement** and **faith in the issuer**.*
- *For traders, currencies are the units of account of various nation-states, whose exchange rates fluctuate between one another.*

An important part of the explanation of how money works comes down to **faith in the issuer** and **social agreement**. This is underpinned by the Executive Summary provided in the [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation White Paper](#):

*For a nation's economy to **function effectively**, its citizens must have **confidence in its money and payment services**. The Federal Reserve, as the nation's central bank, works to maintain the public's **confidence by fostering monetary stability, financial stability, and a safe and efficient payment system**.*

The main takeaways from the Executive Summary are the U.S. CBDC must:

- function effectively
- instill confidence in its money and payment services
- instill confidence by fostering monetary stability
- offer financial stability
- Be a safe and efficient payment system

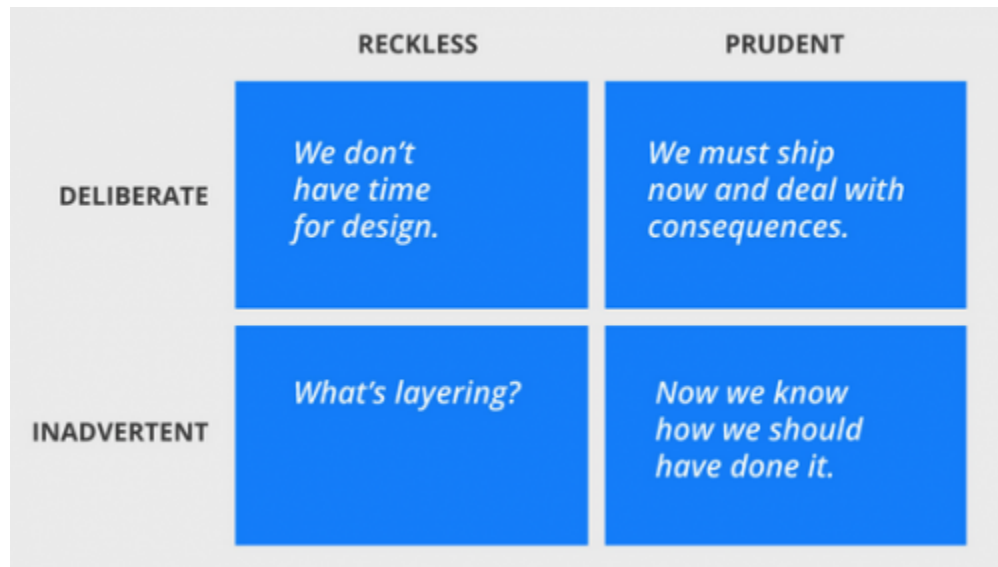
For these reasons, the U.S. CBDC must be more than a Cryptocurrency or even **Stablecoin**. It can not be organically grown and evolved using a bottom-up approach. Having a Dollar be a National Currency with a major role in the National and International economies requires a systematic, pedantic, system engineering approach. This does not mean that it has to follow the traditional **Water Fall Model** but can also use an **Agile Model** when and where appropriate. For example, if a Blockchain model is adopted for use within the CBDC, which uses a series of Smart Contracts to accomplish portions of its overall requirements, these can be developed using an **Agile Model** working within the framework of requirements set at the onset of the CBDC.

Mark Zuckerberg is quoted as saying, *“We used to have this famous mantra ... and the idea here is that as developers, moving quickly is so important that we were even willing to tolerate a few bugs in order to do it. What we realized over time is that it wasn’t helping us to move faster because we had to slow down to fix these bugs and it wasn’t improving our speed.”*<sup>140)</sup> As stated earlier, there is a big difference between working on a large, commercially available product that is not Mission Critical and a product that is Mission Critical. In Mission Critical Systems, any bug can have devastating consequences. Who wants to be in an operating room when a major piece of equipment has a bug? How about an airplane flying over your head? It is expected there will be bugs in any software, but in Mission Critical systems many can be found and corrected earlier on in the product lifecycle and especially during product testing. It is not acceptable to “let the End Users” do the testing on these kinds of systems.

**So, back to the fundamental question. Should the U.S. CBDC be worried about being first to market among the other large economies? Not if it means the Federal Reserve has to take shortcuts to race to market and ultimately accumulate Technical Debt, which like all debt, must be paid back in the future.**

*The term “technical debt” was coined by Ward Cunningham, when he described the phenomenon of meeting a release deadline by making adaptations and concessions to a product. He also outlined how the effects felt afterward were analogous to those associated with the incurring of financial debt. Cunningham acknowledged that, most often, technical debt required payback, while the inability to manage assets could lead to a complete stand-still as the interest and effects of the adaptations (or lack thereof) become unbearable.*<sup>141)</sup>

Chris Cairns and Sarah Allen proposed a quadrant as a way to classify the various types of Technical Debt (See Figure 35). Across the top of the quadrant, they divided the behavior that leads to Technical Debt as being **Reckless** or **Prudent**. Down the left side of the quadrant, they divided the mechanisms that led to the debt as being **Deliberate** or **Inadvertent**. Each cell in the quadrant is used to classify Technical Debt and is described in Table 82.



A classification of Technical Debt show in quadrants. <sup>142)</sup>

Figure 35:

Each quadrant in Figure 35 is a different type of Technical Debt. <sup>143)</sup>

Table 82:

Type of Technical Debt	Description
<b>Reckless/Deliberate Debt</b>	The team feels time-pressured and knowingly violates best practices without any forethought into how to address the consequences. Another scenario: management lacks sufficient funding to hire enough senior experts to direct and review the work of junior programmers, but decides to take the risk anyway.
<b>Prudent/Deliberate Debt</b>	The team decides that the value of shipping a “quick and dirty solution” now is worth the cost of incurring debt. They’re fully aware of the consequences, however, and have a plan in place to address them.
<b>Reckless/Inadvertent</b>	The team is ignorant of best practices and makes a big mess of the codebase.
<b>Prudent/Inadvertent</b>	Even with great programmers, the team delivers an extrinsically valuable solution, only to realize how they should have (intrinsically) designed it. (Often the process of software development is as much learning as it is coding.)

Mark Zuckerberg used the motto “Move fast and break things” in 2014.

“Move fast and break things” has come back to haunt Facebook/Meta over the years. As the company has faced wave after wave of scandals over privacy, misinformation, and harmful content, critics have held its original motto up as evidence of a tendency towards collateral damage.

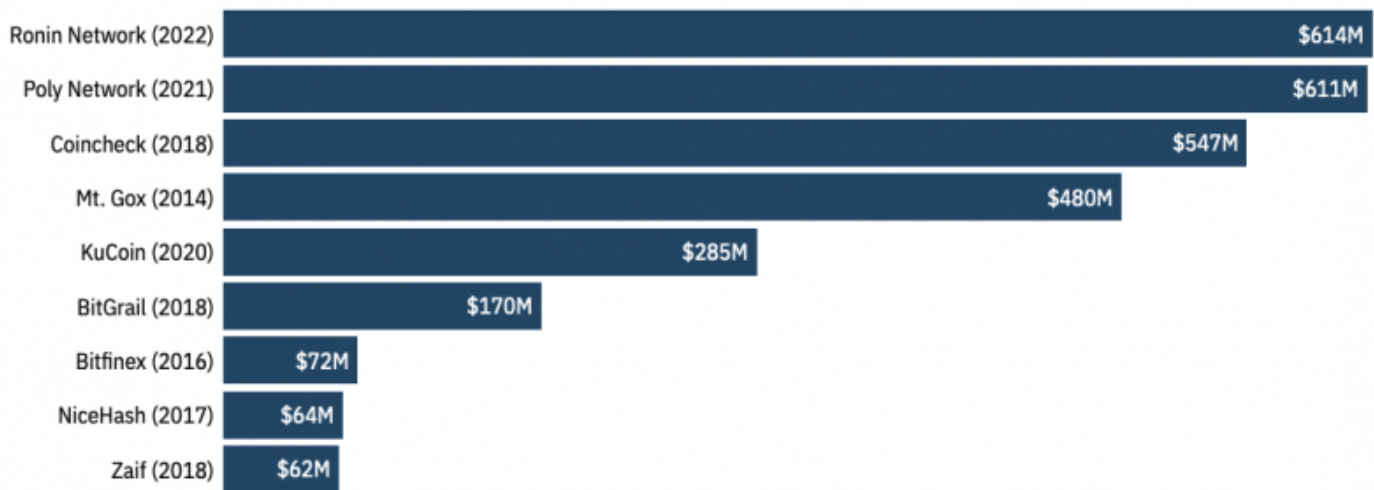
In the article on the biggest cryptocurrency hacks of all time by Tech Monitor <sup>144)</sup> they highlight that Multi-million dollar crypto heists reveal that the crypto industry is learning cybersecurity lessons the hard way, one hack at a time. The article provides the following quotes:

*Proponents argue that the crypto ecosystem is having to learn in a few years, lessons the conventional finance sector has had centuries to perfect. But the biggest crypto hack by value is also the most recent, suggesting there be many more lessons left to learn.*

*“Traditional financial companies have grown up knowing that you have to have layers of protection... in order for folks to entrust you with their money,” says Chris Caruana, VP of AML solutions at financial crime solutions platform Feedzai.*

*“Cryptocurrency exchanges, and the actual ecosystem itself, haven’t had to go through those growing pains yet,” Caruana says. “Even the most adult in the room still has some ways to go.”*

Figure 36 highlights the top biggest losses from hacks in Cryptos. The graph highlights the ever-increasing magnitude in the amount lost in each hack. This indicates that instead of getting things under control, things are only getting worse, which does not bode well for the adoption of the current technology by the CBDC.



Top nine biggest cryptocurrency thefts by estimated losses as of March 2022<sup>145)</sup>  
 Figure 36:

**Note:** Total is \ \$2,905M

**Note:** Values calculated according to cryptocurrency prices at time of theft

Source: [Statista/Bloomberg](#), [Business Insider](#), TechCrunch, CNBC

Table 83 goes through the five top biggest crypto hacks of all time and provides a detailed explanation of the current knowledge about each hack.

The top biggest biggest crypto hacks of all time<sup>146)</sup>

Table 83:

Rank Of Biggest to Smallest	Amount Lost	Year	Cryptocurrency	Explanation



1	\b614M	2021	Ronin Network	<p>The biggest cryptocurrency theft of all time, calculated using the value of the crypto assets at the time they were stolen, was March 2022's raid on Ronin Network, an exchange that allows players of the Axie Infinity videogame to exchange their in-game tokens for another cryptocurrency.</p> <p>On 30th March, the network revealed that an attacker had stolen the private keys required to authenticate transactions and had transferred 173,600 Ethereum and 25.5m USDC, a <b>Stablecoin</b> pegged to the US dollar, to their own wallets. Using the conversion rate at the time, this values the heist at \b614m. The theft was discovered when a customer tried to make a legitimate withdrawal. Sky Mavis, the company behind Axie Infinity, said it is working with "law enforcement officials, forensic cryptographers, and our investors to make sure there is no loss of user funds.</p> <p><i>"We know trust needs to be earned and are using every resource at our disposal to deploy the most sophisticated security measures and processes to prevent future attacks,"</i> the <a href="#">company statement said</a>.</p>
2	\b611M	2021	Poly Network	<p>The second biggest crypto theft of all time, calculated using the value of the crypto assets at the time they were stolen, is last year's \b611m theft from Poly Network, a smart contract platform that allows users to exchange tokens between disparate blockchains, such as Bitcoin and Ethereum.</p> <p>On August 10th, 2021, a hacker transferred \b611m-worth of Poly Network tokens to three wallets under their control. According to an analysis by security researcher Mudit Gupta, the attacker had found a way to 'unlock' (ie buy) tokens on the Poly Network protocol without 'locking' (ie selling) the corresponding tokens on other blockchains.</p> <p>Fortunately for Poly Network, the attacker began returning the tokens the next day. While some speculated that they may have struggled to sell the tokens, someone claiming to be the attacker said they had only stolen them "for fun".</p> <p>By the end of the week, all assets were returned, Poly Network said, except \b33m-worth of <b>'Stablecoin'</b> Tether, which had been frozen immediately after the attack.</p> <p>Shortly after the theft, Steven Dickens, senior analyst at technology research company Futurum, wrote that it was likely to bolster the security of decentralized finance (DeFi) systems in the long run, but discredit them in the short term. <i>"While lessons need to be learned for sure,"</i> he wrote, <i>"we need to be aware of the progress made so far by the DeFi community [which is for all] intents and purposes less than a decade old."</i></p>



3	\547M	2018	Coincheck	<p>In January 2018, Japanese crypto exchange Coincheck revealed that \547m in lesser-known cryptocurrency NEM had been stolen. The company admitted that it had stored the assets in a 'hot wallet', meaning a cryptocurrency store that is connected to the internet and therefore vulnerable to cybersecurity breaches. Shortly after the incident, 16 of Japan's crypto exchanges merged to form a self-regulatory body. The country's financial regulator, the Financial Services Association, ordered all exchanges to report on their cybersecurity defenses.</p> <p>At the time of the attack, Coincheck was one of the most high-profile exchanges in Japan, which was then among the biggest markets for crypto trading. A few months later, Coincheck was acquired by financial services provider Monex Group.</p> <p>It is still unknown who undertook the attack, but more than 30 people have been arrested in Japan in connection with selling the stolen assets.</p>
4	\480M	2014	Mt. Gox	<p>The first widely publicized - and perhaps still the best-known - crypto heist was the theft of \480m in Bitcoin from another Japanese exchange, Mt. Gox, in 2014. Founded in 2010 as a site for trading <i>'Magic the Gathering'</i> game cards, by 2014 Mt. Gox was handling over 70% of all Bitcoin transactions. In February of that year, it abruptly suspended trading, closed its exchange services, and filed for bankruptcy protection.</p> <p>Soon after, it revealed that up to 850,000 Bitcoins had gone missing, presumed stolen. Around 7% of all Bitcoin was in circulation at the time, the haul was then worth around \$480m. Today, it would be closer to /\$35bn.</p> <p>Mark Karpeles, CEO of Mt. Gox at the time of the theft, was later arrested on unrelated charges and, he claims, interrogated for eight hours a day. "I was asked about the missing Bitcoins," he told reporters. "I was even asked if I was Satoshi Nakamoto, the creator of Bitcoin." But in 2016, a US investigation concluded that Mt. Gox had been hacked by an outsider.</p>
5	\285M	2020	KuCoin	<p>In September 2020, Singapore-headquartered crypto exchange KuCoin revealed that \275m worth of cryptocurrency had been stolen, including \$127m in ERC20 tokens, which are used in Ethereum smart contracts. CEO Johnny Lyu revealed that hackers had obtained the private keys to the exchange's 'hot wallets'. The majority of the stolen tokens were recovered, and the remaining 16% in stolen funds was covered by KuCoin's insurance, the company said in February 2021, so all customers were reimbursed.</p>
<b>Total</b>	<b>\2,537M</b>			

## Examples

[Return to Top](#)

The following “desirements” are from the [White Paper](#) as identified by the [Object Management Group's](#) report called [White Paper Analysis](#):

Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG

Table 84:

<b>Benefits</b>	B0020, B0027, B0036, B0050
<b>Policies</b>	P0006, P0009, P0010, P0014, P0015, P0016, P0017, P0025, P0031
<b>Risks</b>	R0001, R0003, R0005, R0006, R0009, R0012, R0014, R0023,
<b>Design</b>	D0011, D0012, D0015

## Example Discussion

[Return to Top](#)

“Desirements” identified in the **White Paper** that have potential international impacts.

Table 85:

<b>Statement No.</b>	<b>Statement</b>	<b>Comment</b>
<b>B0020</b>	<b>Maintain public confidence by not requiring mechanisms, such as deposit insurance</b>	Even in the current Crypto world, there is a need for “deposit insurance”. <i>The 2020 KuCoin hack cost \(\$285M. The majority of the stolen tokens were recovered, and the remaining 16% in stolen funds was covered by KuCoin's <b>insurance</b>, the company said in February 2021, so all customers were reimbursed. Despite the hack, KuCoin remains the fifth most popular crypto exchange, according to the CoinMarketCap website.<sup>147)</sup></i>
<b>B0027</b>	<b>Maintain the centrality of safe and trusted central bank money</b>	
<b>B0036</b>	<b>Preserve the dominant international role of the U.S. dollar</b>	The U.S. CBDC will be a target not just from hackers who want to profit from an attack, but also as a symbol of the U.S. making it a target of espionage.

Statement No.	Statement	Comment
B0050	<b>Extend Public Access to Safe Central Bank Money</b>	By extending public access to the “safe Central Bank Money”, there is also an extension of risk to the “safe central bank money”. Currently, the separation between the “safe central bank Money” and the regular money acts as a firewall. By granting direct access to the Central Bank Money, that firewall is no longer in place and safeguards need to be added to protect the Central Bank Money.
P0006	<b>Garner broad support from key stakeholders</b>	In order to garner support from within the U.S. and from the rest of the world, the CBDC needs to uphold the laws against <a href="#">Human Trafficking</a> , <a href="#">Drug Trafficking</a> , <a href="#">Corruption</a> , and <a href="#">Money Laundering</a> just as the U.S. has done with the U.S. Dollar and numerous laws we now enforce to prevent or interrupt these illegal activities.
P0009	<b>CBDC would be a liability of the Federal Reserve, not of a commercial bank</b>	When the Federal Reserve assumes liability for the CBDC, any negative news regarding hacks, breaches, or criminal activity associated with the CBDC will be a direct reflection on The Federal Reserve.
P0010	<b>CBDC would be a liability not of a commercial bank<sup>148)</sup></b>	See <b>P0009</b>
P0014	<b>The PWG report highlights gaps in the authority of regulators to reduce these risks</b>	This is why all the <a href="#">Stakeholders</a> need to be involved in the U.S. CBDC development, not just guide the CBDC system, but also to guide the administrators and the legislators to make the appropriate updates and amendments to the laws.
P0015	<b>The PWG report recommends that Congress act promptly to enact legislation that would ensure payment Stablecoins</b>	Stablecoins are just the same as any other cryptocurrency with the exception that their value is pegged to the U.S. Dollar. If the Stablecoin software is not properly engineered and tested before deployment just to be “the first” major economy with a CBDC, it seems it will be an expensive proposition.
P0016	<b>The PWG report recommends payment Stablecoin arrangements are subject to a consistent and comprehensive federal regulatory framework</b>	See <b>P0014</b>
P0017	<b>The PWG report recommends CBDC complement existing authorities regarding:</b> <b>1. market integrity</b> <b>2. investor protection</b> <b>3. illicit finance</b>	See <b>P0014</b>

Statement No.	Statement	Comment
P0027	CBDC a risk-free asset	The CBDC will be a large project that produces many lines of code. It is not possible for it to be “risk-free”. The risk to the end-user can be alleviated with insurance, but that does not mitigate the risk. See Figure 36 and Table 83 above.
P0031	The Federal Reserve would only pursue a CBDC in the context of broad public and cross-governmental support	See P0014
R0001	Risk of affecting financial-sector market structure	If there is a major hack to the CBDC, this could trigger a “lack of confidence” not just in the CBDC, but in the U.S. Dollar and perhaps The Federal Reserve.
R0003	Risk to the safety and stability of the financial system	See R0001
R0004	Risk to the efficacy of monetary policy	See R0001
R0005	New payment services could pose Risks to: 1. financial stability 2. payment system integrity 3. other Risks	See R0001
R0006	Risk of extreme price volatility	See R0001
R0009	Increased Risk of “runs” or other instabilities to the financial system	See R0001
R0012	Risk of increased concern related to the potential for: 1. destabilizing “runs” 2. disruptions in the payment system 3. concentration of economic power	See R0001
R0014	Risk of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity	Not only does the CBDC have to worry about hacks that can steal value from the CBDC, but it also needs to worry about hacks that steal private information. Once there is a hack of private information, confidence in the CBDC will be undermined.
R0023	Risk of financial panic causing outflows from Commercial Banks to CBDC without prudential supervision, government deposit insurance, and access to central bank liquidity	This is a dangerous two-way street. Not only could there be a “flight to value” towards the CBDC, but there could also be a “flight to value” away from the CBDC.
D0011	Design should generate data about users’ financial transactions in the same ways that commercial bank and nonbank money generates data today	If the CBDC is rushed to be the first major economy in the world with a CBC, the design must assure the privacy of the end-users. See section 4.4 National Privacy Considerations. Also, see P0009 where the CBDC would be a liability of the Federal Reserve, not of a commercial bank.

Statement No.	Statement	Comment
D0012	<b>Design should address privacy concerns by leveraging existing tools already in use by intermediaries</b>	There appears to be a conflict between <b>D0012</b> and <b>P0009</b> .
D0015	<b>Design should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks</b>	A dedicated infrastructure takes time. As an indicator of how slow infrastructure can be, IPv6 has been underway since 1998 to address a shortfall of IPv4 addresses, yet the upgrade is still in progress as of 2022. <sup>149)</sup> Another example is the slow adoption in the U.S. of the “Chip and Pin” Credit Cards. According to Heather Long: <sup>150)</sup> <i>The credit card market in the US is complex (pdf). You have retailers, big banks, and then card associations like Visa and Mastercard. So you have to get three sectors of the market to work together to implement any new technology. US retailers and credit card companies have been at war for years over who pays what transaction fees. Now they're trying to sort out who will pay for the estimated \$8bn costs (pdf) for chip and pin technology.</i> The adoption of infrastructure for CBDC needs to be thought out and planned, including who is paying for it.

**B** = [Benefit Considerations](#)

**P** = [Policy Considerations](#)

**R** = [Risk Considerations](#)

**D** = [Design Considerations](#)

<sup>138)</sup>

Robert Burgess, Bloomberg, 3 March 2022, Accessed: 16 April 2022, <https://www.bloomberg.com/opinion/articles/2022-03-03/dethroning-the-dollar-as-the-world-s-reserve-currency-won-t-be-easy>

<sup>139)</sup>

Daniel Kurt, [How Currency Works](#), 24 June 2021, Accessed 15 April 2022, <https://www.investopedia.com/articles/investing/092413/how-currency-works.asp>

<sup>140)</sup>

Ramnath Kashikar, [Technical Debt - Good or Bad?](#), 7 August 2020, Accessed: 15 April 2022, <https://www.linkedin.com/pulse/technical-debt-good-bad-ramnath-kashikar/>

<sup>141)</sup>

Johannes Holvitie, Sherlock A. Licorish, Rodrigo O. Spínola, Sami Hyrynsalmi, Stephen G. MacDonell, Thiago S. Mendes, Jim Buchan, Ville Leppänen, [Technical debt and agile software development practices and processes: An industry practitioner survey](#), Information and Software Technology, Volume 96, 2018, Pages 141-160, ISSN 0950-5849, Accessed: 16 April 2022, <https://www.sciencedirect.com/science/article/pii/S0950584917305098>

<sup>142)</sup>

Chris Cairns , Sarah Allen , [What is technical debt?](#), 18f.gsa.gov, 4 September 2015, Accessed 15 April 2022, <https://18f.gsa.gov/2015/09/04/what-is-technical-debt/>

143)

Chris Cairns , Sarah Allen , [What is technical debt?](https://18f.gsa.gov/2015/09/04/what-is-technical-debt/), 18f.gsa.gov, 4 September 2015, Accessed 15 April 2022, <https://18f.gsa.gov/2015/09/04/what-is-technical-debt/>

144) 145) 146) 147)

Tech Monitor, [The biggest cryptocurrency hacks of all time](https://techmonitor.ai/technology/cybersecurity/biggest-cryptocurrency-hacks-of-all-time), 17 March 2022, Accessed: 15 April 2022, <https://techmonitor.ai/technology/cybersecurity/biggest-cryptocurrency-hacks-of-all-time>

148)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**.

149)

Josh Fruhlinger, [What is IPv6, and why is its adoption taking so long?](https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html), Network World, 21 March 2022, Accessed 17 April 2022,

<https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html>

150)

Heather Long, [Why is the US a decade behind Europe on 'chip and pin' cards?](https://www.theguardian.com/commentisfree/2014/jan/27/target-credit-card-breach-chip-pin-technology-europe), The Guardian, 27 January 2014, Accessed: 17 April 2022,

<https://www.theguardian.com/commentisfree/2014/jan/27/target-credit-card-breach-chip-pin-technology-europe>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q10:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q10:start)

Last update: **2022/05/18 22:41**

# Question: 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?**

## Answer

[Return to Top](#)

By all descriptions, the U.S. CBDC is primarily a large [System-of-Systems \(SoS\)](#) or even an SoS of SoSs. Some of these would ideally already exist and some will need to be created. The new systems are predominately a [Software \(SW\)](#) effort. Yes, there will be some specialized [Hardware\(HW\)](#) required, but the primary focus appears to be Software (including [Commercial-Off-The-Shelf \(COTS\)](#), [Government Off-The-Shelf \(GOTS\)](#), or [Modified Off-The-Shelf \(MOTS\)](#)). This software will ultimately need to be [Managed](#) and [Modified](#).

The following is a list of potential risks not identified in the **White Paper**.

- [1. Risk of a Software Crisis](#)
- [2. Risk of Lack of Stakeholder Buy-In](#)
- [3. Risk Due to Poor Community of Interest \(CoI\) Governance](#)
- [4. Risk Due to lack of Broad, Wide Ranging Security Planning](#)
- [5. Risk of Data being hacked due weak Security Infrastructure](#)
- [6. Risk of Meta-Data being hacked due weak Security Infrastructure](#)
- [7. Risk of Business Processes Being Hacked](#)
- [8. Risk of competing Currency Models for the CBDC](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:brp:q11:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:brp:q11:start)

Last update: **2022/05/16 21:38**





# 1. Risk of a Software Crisis

[Return to Question 11](#) [Provide Feedback](#)

For these reasons, the [Object Management Group \(OMG\)](#) recommends the adoption of a systematic effort for the development of an SoS identified as a [Mission-Critical SoS](#). The CBDC also has a potential [System Lifecycle](#) that spans decades at a minimum. **The need for an SoS, long-lived, Mission-Critical System sets the stage for the biggest risks for the U.S. CBDC**, the potential for a looming [Software Crisis](#).

A **Software Crisis** occurs on projects for many reasons, but the [Information Technology \(IT\)](#) industry has focused on a shortlist, which is provided in summary form in [Table 86](#). Any particular project suffering a **Software Crisis** may have any number of these issues and unfortunately, some projects might have all of these issues.

Issues causing a Project to have a **Software Crisis**.

Table 86:

1. Projects are running over budget
2. Projects are running behind schedule
3. Poor quality of the delivered software
4. Poor definition of requirements
5. Poor adherence to the requirements
6. Poor management of the entire project throughout its lifecycle
7. Poor communications between the Stakeholders, Systems Engineers, and Software Engineers
8. Poor documentation of Policies and Procedures for the project
9. Poor enforcement of Policies and Procedures for the project
10. Poor training of Stakeholders, Systems Engineers, and Software Engineers on Policies and Procedures.
11. Increase in System and Software complexity
12. Increase in Software costs compared to Hardware

However, all is not lost for the CBDC. There is a way to prevent a future CNDC **Software Crisis** by applying sound [Systems Engineering](#) practices throughout the CBDC lifecycle, starting immediately. The OMG has a rich history of working in Systems and Software Engineering. [Table 87](#) provides a list of OMG standards covering [Systems Engineering](#) and [Software Engineering](#).

The Object Management Group's list of System and Software Engineering Standards.

Table 87:

- [Business Motivation Model \(BMM\)](#)
- [Business Process Model and Notation \(BPMN\)](#)
- [Common Warehouse Metamodel \(CWM\)](#)
- [Distributed Ontology, Model, and Specification Language \(DOL\)](#)
- [Financial Industry Business Ontology \(FIBO\)](#)
- [Financial Instrument Global Identifier \(FIGI\)](#)
- [MetaObject Facility \(MOF\)](#)

- [Model Based Systems Engineering \(MBSE\)](#)
- [Model Driven Architecture \(MDA\)](#)
- [Ontology Definition Metamodel \(ODM\)](#)
- [Semantics Of Business Vocabulary And Business Rules \(SBVR\)](#)
- [Structured Assurance Case Metamodel \(SACM\)](#)
- [Systems Modeling Language \(SysML\)](#)
- [Unified Architecture Framework \(UAF\)](#)
- [Unified Modeling Language \(UML\)](#)
- [XML Metadata Interchange \(XMI\)](#)
- [Systems and software engineering -- System life cycle processes](#)
- [Measurement of System and Software Product Quality](#)

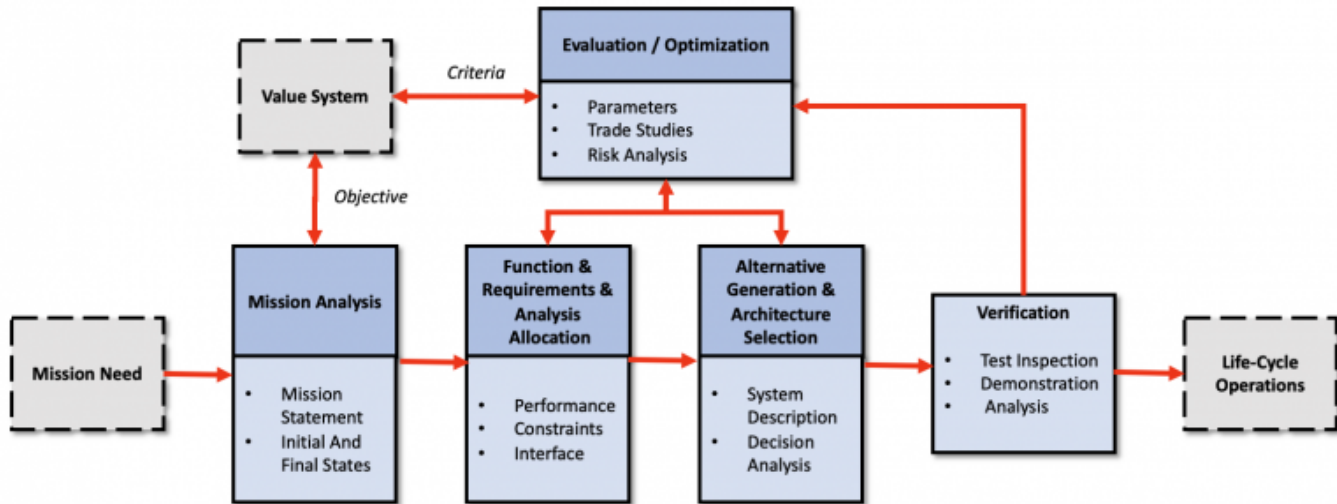
The Systems Engineering process as described by the Department of Energy (DOE) is to develop, manage, and implement large programs <sup>151</sup>. The following is a modified version of the DOE process tweaked to differentiate the Water Fall Model versus the Agile Model.

1. Orderly definition of the **System** through top-down development of **System Functions** and **System Requirements**. This is an iterative process with each iteration providing further decomposition of the System Level Requirements as needed. **Note:** These Systems-level definition iterations should not be confused with the [Agile Sprints](#) used during development. See the OMG DIDO-RA section on [The Current State of DIDO Requirements](#).
2. Clear distinction between: a. External driven **System** requirements and constraints, which are by intent not easy to modify. In other words, the identification of System Functional and Non-Functional Requirements. b. Internal driven **Design** (i.e., implementation) requirements developed by the project, which are potentially modifiable and evolutionary with new requirements added as the system is developed. In other words, Derived Requirements.
3. Top-down consideration and evaluation of alternative solutions and designs based on the System [Functional](#) and [Non-Functional Requirements](#)
4. Completeness and traceability for the design of System Components and System Interfaces, for configuration and change control, and for the system verification and validation plan(s). In other words, the SoS must come together as a cohesive, solitary group of capabilities that synergize the system to deliver the desired effects. All the Systems within the SoS must have a single, cohesive, unified understanding of the other Systems within the SoS and must be able to use standardized Application Programming Interfaces (APIs).

DOE goes on to describe the value of the Systems Engineering Process realization in a number of ways, including:

1. Increased ability to estimate system life-cycle costs
2. Reduced redesign due to consideration of the entire system throughout its development
3. Increased ability to affect design changes and retrofits due to clear traceability of requirements, design features, and configuration control
4. Increased probability of achieving the best technical design and operational concept through the iterative consideration of design alternatives, where **best** is defined through decision criteria such as cost, risk, and use. See the OMG DIDO-RA section on [Assessing Requirements](#)

Figure 37 provides a simplified high-level processes flow for Systems Engineering. This process was developed by the U.S. Department of Energy and would have to be tailored to meet the needs of a U.S. CBDC. Basically, the System's process flow is captured in Table 88



Simplified high-level Systems Engineering Process as defined by the U.S. Department of Energy. Figure 37:

The steps in the Simplified high-level Systems Engineering Process as defined by the U.S. Department of Energy:

high-level Systems Engineering Process as defined by the U.S. Department of Energy Table 88:

1. A high-level statement of system needs. In this discussion, the Mission needs are referred to as “Desirements”. The current “desirements” from the [White Paper](#) as identified by the [Object Management Group's](#) report called [White Paper Analysis](#) is a good starting point for these.
2. The “Mission Needs” are analyzed and transformed into “Mission Statements” (i.e., Systems Requirements). For example, the **White Paper** desirement of:

The Federal Reserve does not intend to proceed with the issuance of a CBDC without clear support from the Executive Branch, the Legislative Branch, and also ideally in the form of a specific authorizing law would be transformed into:

- U.S. CBDC shall be authorized by a specific U.S. Law
- U.S. CBDC Authorizing Law shall be approved by the Legislative Branch
- U.S. CBDC Authorizing Law shall be approved by the Executive Branch

3. The “Mission Statements” are transformed into [Functional](#) (i.e, performance, interfaces)and [Non-Functional](#) Requirements (i.e., constraints), see [OMG DIDO-RA Specifying Requirements](#). Also, see the [OMG DIDO-RA](#) section on Testability and especially the subsection on [Software Assurance \(SwA\)](#). If the requirements are not testable, then they serve little purpose.
4. The “Requirements” are allocated to Systems, or components (i.e., elements) and added to a formal System Description and Systems Analysis. [Table 89](#) captures the documents called out in the [Unified Architecture Framework \(UAF\)](#). These documents can be tailored for the U.S. CBDC, but many of the documents are useful for [Mission Critical Systems](#).

The kinds of documents that can be used to define the system.

Table 89:

<b>Viewpoint</b>	<b>Acronym</b>	<b>Description</b>
<b>Architecture Management</b>	<b>Am</b>	Identifies the metadata and views required to develop a suitable architecture that is fit for its purpose.
<b>Strategic</b>	<b>St</b>	Capability management process. Describes the capability taxonomy, composition, dependencies, and evolution.
<b>Operational</b>	<b>Op</b>	Illustrates the Logical Architecture of the enterprise. Describes the requirements, operational behavior, structure, and exchanges required to support (exhibit) capabilities. Defines all operational elements in an implementation/solution-independent manner.
<b>Services</b>	<b>Sv</b>	The Service-Orientated View (SOV) is a description of services needed to directly support the operational domain as described in the Operational View. A service within MODAF is understood in its broadest sense, as a unit of work through which a provider provides a useful result to a consumer. MODAF: The Service Views within the Services Viewpoint describe the design for service-based solutions to support operational development processes (JCIDS) and Defense Acquisition System or capability development within the Joint Capability Areas.
<b>Personnel</b>	<b>Ps</b>	Defines and explores organizational resource types. Shows the taxonomy of types of organizational resources as well as connections, interaction, and growth over time.
<b>Resources</b>	<b>Rs</b>	Captures a solution architecture consisting of resources, e.g., organizational, software, artifacts, capability configurations, and natural resources that implement the operational requirements. Further design of a resource is typically detailed in SysML or UML.
<b>Security</b>	<b>Sc</b>	Security assets and security enclaves. Defines the hierarchy of security assets and asset owners, security constraints (policy, laws, and guidance), and details where they are located (security enclaves).
<b>Projects</b>	<b>Pj</b>	Describes projects and project milestones, how those projects deliver capabilities, the organizations contributing to the projects, and dependencies between projects.
<b>Standards</b>	<b>Sd</b>	MODAF: Technical Standards Views are extended from the core DoDAF views to include non-technical standards such as operational doctrine, industry process standards, etc. DoDAF: The Standards Views within the Standards Viewpoint are the set of rules governing the arrangement, interaction, and interdependence of solution parts or elements.
<b>Actual Resources</b>	<b>Ar</b>	The analysis, e.g., evaluation of different alternatives, what-if, trade-offs, V&V on the actual resource configurations. Illustrates the expected or achieved actual resource configurations.
<b>Motivation</b>	<b>Mv</b>	Captures motivational elements e.g., challenges, opportunities, and concerns, that pertain to enterprise transformation efforts, and different types of requirements, e.g., operational, services, personnel, resources, or security controls.
<b>Taxonomy</b>	<b>Tx</b>	Presents all the elements as a standalone structure. Presents all the elements as a specialization hierarchy, provides a text definition for each one and references the source of the element

<b>Viewpoint</b>	<b>Acronym</b>	<b>Description</b>
<b>Structure</b>	<b>Sr</b>	Describes the breakdown of structural elements e.g., logical performers, systems, projects, etc. into their smaller parts
<b>Connectivity</b>	<b>Cn</b>	Describes the connections, relationships, and interactions between the different elements.
<b>Processes</b>	<b>Pr</b>	Captures activity-based behavior and flows. It describes activities, their Inputs/Outputs, activity actions, and flows between them.
<b>States</b>	<b>St</b>	Captures state-based behavior of an element. It is a graphical representation of the states of a structural element and how it responds to various events and actions.
<b>Sequences</b>	<b>Sq</b>	Expresses a time-ordered examination of the exchanges as a result of a particular scenario. Provides a time-ordered examination of the exchanges between participating elements as a result of a particular scenario.
<b>Information</b>	<b>If</b>	Address the information perspective on operational, service, and resource architectures. Allows analysis of an architecture's information and data definition aspect, without consideration of implementation-specific issues.
<b>Constraints</b>	<b>Ct</b>	Details the measurements that set performance requirements constraining capabilities. Also defines the rules governing behavior and structure.
<b>Roadmap</b>	<b>Rm</b>	Addresses how elements in the architecture change over time.
<b>Traceability</b>	<b>Tr</b>	Describes the mapping between elements in the architecture. This can be between different viewpoints within domains as well as between domains. It can also be between structure and behaviors.

5. Verification of the System is progressing according to plan. This is done through Test Inspection, Demonstrations, as well as Static and Dynamic Analysis of the System. Another major tool should be the use of Modeling and testing in Virtual Environments.

6. Evaluation and Optimization occur before a release to the public. Based on the results of Trade Studies, risk analysis, performance, etc, the System Design Specifications can be updated, refined, or added to. </WRAP>

151)

National Academy of Sciences, Systems Analysis and Systems Engineering in Environmental Remediation Programs at the Department of Energy Hanford Site, National Research Council 1998. Systems Analysis and Systems Engineering in Environmental Remediation Programs at the Department of Energy Hanford Site. Washington, DC: The National Academies Press.

<https://doi.org/10.17226/6224>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc\\_omg:04\\_doc:20\\_comments:brp:q11:01\\_risk](https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:04_doc:20_comments:brp:q11:01_risk)

Last update: **2022/05/19 01:20**



## 2. Risk of Lack of Stakeholder Buy-In

[Return to Question 11](#) [Provide Feedback](#)

A major risk confronting the U.S. CBDC is the lack of Stakeholders' "buy-in". The [Stakeholders](#) for a U.S. CBDC is far beyond just the Federal Reserve. The definition is applied to the U.S. CBDC is a large and spreading network of other U.S. Government Departments and Agencies, the current financial institutions that participate in the U.S. Financial system, the U.S. Executive and Legislative Branches of the U.S. Government, international governments and institutions, the citizens and residents of the U.S, and for that matter, almost everyone on the planet since the U.S. Dollar is the dominate [Reserve Currency](#). Obviously, it is not possible to invite everyone to sit down at a table and have discussions about a U.S. CBDC. Most people will rely on elected officials, government organizations, etc. to represent them.

In the Object Management Group's (OMG's) response, we tried to help enumerate the U.S. CBDC in section [4.1 Stakeholders](#). Table [11](#) is a summary of the list identified so far that could be considered potential Stakeholders.

Summary of the estimated number of Government Stakeholders for the CBDC.

Table 90:

<b>Potential Oversight Authorities</b>	<b>No. of Stakeholders</b>
<b><a href="#">U.S. Federal Government Oversight Authorities</a></b>	14
<b><a href="#">non-U.S. Federal Government Oversight Authorities</a></b>	19
<b>Total</b>	<b>33</b>

Although a U.S. CBDC is something new, it will also be part of the U.S. monetary system that is already established. The U.S. population relies on the monetary system and has expressed its aspirations for the monetary system through laws and regulations already in effect to control the monetary system. These laws and regulations have evolved since the founding of the U.S. and are generally a response to negative impacts on the U.S. people. Therefore, a major way to include the people as Stakeholders is to follow the laws and regulations of the U.S. The same can be said for the potential international stakeholders who rely on international treaties and agreements between the U.S. and their countries.

In the Object Management Group's (OMG's) response, we tried to enumerate the U.S. and U.S. State laws and regulations that are concerned with Privacy in section [4.4 National Privacy Considerations](#). Table [39](#) is a summary of the list of Laws and Regulations identified so far for the U.S. and U.S. State laws covering Privacy.

Summary of the number of laws and regulations covering National Security Considerations.

Table 91:

<b>U.S. Privacy Consideration</b>	<b>No. of Laws and Regulations</b>
<b><a href="#">U.S. Federal Laws and Regulations</a></b>	10
<b><a href="#">U.S. State Laws and Regulations</a></b>	6
<b>Total</b>	<b>16</b>

Here are some examples of "resistance" to a U.S. CBDC from potential stakeholders:

- WASHINGTON – Sen. Chuck Grassley (R-Iowa), a member and former chair of the Senate Finance Committee, and Sens. Ted Cruz (R-Texas) and Mike Braun (R-Ind.) have introduced new legislation to prohibit the Federal Reserve from issuing a central bank digital currency (CBDC) directly to individuals. Specifically, the legislation prohibits the Federal Reserve from developing a direct-to-consumer CBDC, which could potentially be used as a financial surveillance tool by the federal government – similar to what is currently happening in China.<sup>152)</sup>
- People have a wide range of views when it comes to digital assets. On one hand, some proponents speak as if the technology is so radically and beneficially transformative that the government should step back completely and let innovation take its course. On the other hand, skeptics see limited, if any, value in this technology and associated products and advocate that the government take a much more restrictive approach. Such divergence of perspectives has often been associated with new and transformative technologies.<sup>153)</sup>

<sup>152)</sup>

Chuck Grassley, News Release, 31 March 2022, Accessed: 24 April 2022,  
<https://www.grassley.senate.gov/news/news-releases/grassley-colleagues-introduce-bill-to-prohibit-unilateral-fed-control-of-a-us-digital-currency>

<sup>153)</sup>

Janet Yellen, The U.S. Department of the Treasury, Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets, 7 April 2022, Accessed: 24 April 2022,  
<https://home.treasury.gov/news/press-releases/jy0706>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q11:02\\_risks](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q11:02_risks)

Last update: **2022/05/19 01:22**





# 3. Risk Due to Poor Community of Interest (Col) Governance

[Return to Question 11](#) [Provide Feedback](#)

Governance of a Community of Interest (Col) just does not happen by chance. It must be a well-thought-out formal organization with strict Policies and Procedures in place to guarantee the whole community is represented and can help formulate the solution or in this case, solutions to solving the Community's problem (i.e., U.S. CBDC). Too often, the Governance is considered by using [Open Source Software \(OSS\)](#). Although having OSS Projects can have an important role in the Governance of a project, it is primarily focused on the development of Software. Yes, the CBDC will be predominately software, but there is much more that needs to be governed than just software.

Examples of non-Software things the U.S. CBDC Community of Interest might need to control:

## 1. [Legal Documents](#) such as

- [Charters](#)
- [By-Laws](#)
- [Policies and Procedures \(P&P\)](#)

## 2. [Guides](#)

## 3. [System](#) and [Software Engineering](#) documents such as:

- [Requirements](#) ( [Non-Functional](#) and [Functional](#) )
- [Models](#)
- [Interface Specifications](#)
- [Assurance](#) and [Assurance Models](#)
- [Testing regime](#) ( [Unit Testing](#) , [Integration Testing](#) , [End-to-End Testing \(E2E Testing\)](#), [Smoke Testing](#) , [Sanity Testing](#) , [Regression Testing](#), [Acceptance Testing](#) , [White Box Testing](#), [Black Box Testing](#) , [Interface Testing](#) , [Interoperability Testing](#) , [Test Data](#), [Test Plans](#) and [Test Results](#) )

In addition to all these requirements for Governance, the Governance Model itself must reflect the "*distributed nature*" of the participants in the Col itself. So far, we have identified 33 different Oversight Authorities that could be part of the Col (see [Table 89](#), and each one needs to be able to have a voice at the Col forum or Consortium. See the OMG DIDO-RA discussion of [Governance](#).

The U.S. CBDC will most likely be a System-of-Systems (SoS) or even an SoS of other SoSs. This means that there probably needs to be a hierarchy of Col not unlike that of the Federal Reserve itself. For example:

1. The U.S. CBDC Col might be an [Ecosphere](#)
2. The development of U.S. CBDC ATM equivalents might be an [Ecosystem](#)

- The Development of a U.S. CBDC ATM machine itself might be a [Domain](#)
- The Development of a U.S. CBDC ATM network might be a [Domain](#)

3. The Development of a Bridge between the ACH and the U.S. CBDC might be an [Ecosystem](#)

- The Development of a U.S. CBDC Bridge Hardware might be a [Domain](#)
- The Development of a U.S. CBDC Application Programming Interface (API) might be a [Domain](#)

Overview of the different kinds of Communities of Interest (Cols)

Table 91:

Col Type	Description
<b>Ecosphere Community</b>	<b>Ecosphere Community is the highest level <a href="#">Community of Interest (COI)</a> that encapsulates <a href="#">DIDO Ecosystem Communities</a> and <a href="#">DIDO Domain Communities</a>. The Ecosphere usually provides high-level requirements and some funding for the administration of the other Cols. The Ecosphere's role is to act as a coordinator of the Ecosystems and to provide a framework for all other Cols to establish working agreements such as <a href="#">Memorandum of Agreement (MoA)</a> or <a href="#">Memorandum of Understanding (MoU)</a>. The Ecosphere is often the only Col that is recognized as a Legal Entity with legally binding <a href="#">Charter</a>, <a href="#">Bylaws</a> and official <a href="#">Policies and Procedures</a>. Often the Ecosphere control <a href="#">Intellectual Property (IP) rights</a> and allowable <a href="#">Copyrights</a> that are acceptable for the Ecosphere and the Domain.</b>
<b>Ecosystem Community</b>	<b>Ecosystem Community is the midlevel level <a href="#">Community of Interest (COI)</a> that encapsulates <a href="#">Domain Communities</a>. The Ecosystem has a <a href="#">Sub-Charter</a> approved by the <a href="#">Ecosphere Col</a>. The Ecosystem usually relies on the Ecosphere for <a href="#">By-Laws</a> and <a href="#">Policy and Procedures (P&amp;P)</a> but can provide addendums that do not conflict with the Ecosphere. The primary role of the Ecosystem is to coordinate the activities of the Domains which fall under its jurisdiction. As a general rule, the Ecosystem does not actually create anything but acts as the integrator and coordinator of all the Domains it is responsible for. The Ecosystem may have more restrictive <a href="#">Intellectual Property (IP) Rights</a> than the Ecosphere. It can only subset the <a href="#">Copyrights</a> allowed by the Ecosphere. The Ecosphere's role is to act as a coordinator of the Domains, however, one Ecosystem can also have a Sub-Ecosystem that it is responsible for. The Ecosystem can have its own <a href="#">bug tracking system</a> that covers integration issues. The Ecosystem is responsible for all <a href="#">Integration Testing</a>.</b>
<b>Domain Community</b>	<b>Domain Community is the lowest level <a href="#">Community of Interest (COI)</a>. The Domain has a <a href="#">Sub-Charter</a> approved by the <a href="#">Ecosystem Community</a>. The Domain usually relies on the Ecosphere for <a href="#">By-Laws</a> and <a href="#">Policies and Procedure (P&amp;P)</a> but can provide addendums that do not conflict with the Ecosphere. The primary role of the Domain is to produce a product that meets the Functional and Non-Functional Requirements of the Ecosystem and the Ecosphere. As a general rule, the Domain actually builds or deploys things to be integrated into the Ecosystem. The Domain may have more <a href="#">Intellectual Property (IP) Rights</a> than the Ecosystem. It can have a subset of the <a href="#">Copyrights</a> allowed by the Ecosystem. The Domain's role is to build products as per the requirements and maintain products according to the <a href="#">Bug Tracking System</a>. The Domain is responsible for all testing at the Domain level (See: <a href="#">Testability</a>).</b>

**Note:** One way within the U.S. Government to create an Ecosphere, might be to use the [Other Transaction Authority provisions](#) within the U.S. Code.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q11:03\\_risks](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q11:03_risks)

Last update: **2022/05/17 21:34**



## 4. Risk Due to lack of Broad, Wide Ranging Security Planning

[Return to Question 11](#) [Provide Feedback](#)

An important way to make sure the Security Planning is adequate is to design it into the U.S. CBDC from the onset, especially if the U.S. CBDC adopts the use of Distributed Technologies currently in wide use in cryptocurrencies. First, it is important to detail what needs to be secure and why. See Table 92.

For a more detailed discussion, see the OMG DIDO-RA section on Non-Functional requirements for [Securability](#).

Main reasons why data needs to be secure.

Table 92:

- [Confidentiality](#)
- [Data Integrity](#)
- [Non-repudiation](#)
- [Authenticity](#)
- [Accountability](#)

All too often, projects try to “bolt-on” security after products are built. When building something as essential and critical to the U.S. as a new financial mechanism such, ie., as the CBDC, it is essential to think about it at every stage of development, starting at the specification of requirements and at each layer of securability. See Figure 38 and Table 93

Securability is also a layered stack. At each layer, there are different steps that need to be taken to secure the system. For example, **Culture Security** it may just mean having employees hold a security clearance and/or take Drug Tests. For **Physical Security** it may mean having a locked facility to house the computers and network devices. Data Security might be software and cultural procedures such as encrypting all data stored in a disk drive and using software to access the data.



The layers of Security.

Figure 38:

The layers of Security.

Table 93:

1. [Physical Security](#)
2. [Data Security](#)
3. [Network Security](#)
4. [Platform Security](#)
5. [Application Security](#)
6. [Culture Security](#)

The OMG members recommend a close look at the Reference Architecture (RA) defined by [Information Exchange Framework \(IEF\)](#).

The IEF RA is primarily targeting operational environments that require the ability and capacity to share information within and beyond organizational boundaries (public and private sectors) and are challenged by rapid, unpredictable changes in operational contexts (e.g., threat, risk, roles & responsibilities, scale, scope, and severity). The IEF RA is targeted towards the following areas:

- Military (coalition and Civilian-Military) operations
- National Security
- Public Safety
- Crisis Management
- Border Security
- Emergency Management
- Peace Keeping
- Humanitarian Assistance

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q11:04\\_risks](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q11:04_risks)

Last update: **2022/05/18 21:38**



## 5. Risk of Data being hacked due weak Security Infrastructure

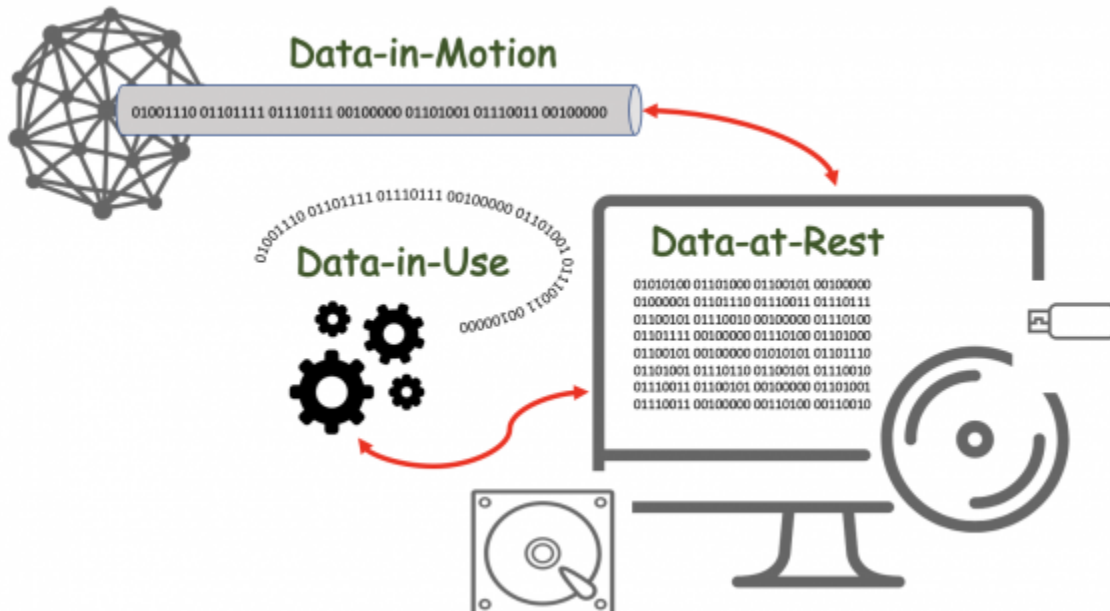
[Return to Question 11](#) [Provide Feedback](#)

*When Senator Mark Warner (D-VA) questioned witness Dr. Neha Narula, Director of the Digital Currency Initiative at MIT, on security risks associated with cryptocurrencies, she responded that, with respect to ransomware attacks, the issue is that valuable data has not been properly secured, and suggested that a CBDC could have built-in safeguards. She also believed that open-source software is critical for security.<sup>154)</sup>*

Data can exist in many states depending on how it is being used. Each of the different Data States poses its own risks of compromising data. The primary concern with data is that it compromises End User Privacy. See section [4.4 National Privacy Considerations](#).

The risks and concerns about Data in each of the different states are also important. Often, the primary focus for understanding data is to concentrate on [Data-at-Rest](#). Although this data is relatively static, it can change over time. In the past, there was little concern for [Data-in-Motion](#), which can have serious effects on [Reliability, Maintainability, and Availability \(RAM\)](#), as well as, [Securability](#) and can leave a system vulnerable to breaches. With the advent of HTTPS, these vulnerabilities are mitigated. The latest issue has become the need to secure [Data-In-Use](#). A recent WhatsApp data breach<sup>155)</sup> found that switching data between image filters could cause memory corruption followed by a crash that left data exposed.

Figure 39 graphically represents the different Data States within a system. Most systems are now able to handle the Data-in-Motion and the Data-at-Rest issues but have traditionally relied on physical security to protect Data-in-Use.



## The Various States of Data.

### Figure 39:

Any risk assessment must include the Security Infrastructure and the state of data:

- [Data-at-Rest](#)
- [Data-in-Motion](#)
- [Data-In-Use](#)

<sup>154)</sup>

Buckley Firm, [Senate holds hearing on central bank digital currency](#), 16 June 2022, Accessed: 24 April 2022,

<https://buckleyfirm.com/blog/2021-06-16/senate-holds-hearing-central-bank-digital-currency>

<sup>155)</sup>

Czarina Grace, [WhatsApp Data Breach 2021 Could Expose 2 Billion Users: Update Now on Android, iOS to Fix Security Risk](#), iTechPost, 6 September 2021, Accessed 6 October 2021,

<https://www.itechpost.com/articles/106929/20210906/whatsapp-data-breach-2021-expose-2-billion-users-update-now.htm>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q11:05\\_risks](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q11:05_risks)

Last update: **2022/05/18 21:38**



## 6. Risk of Meta-Data being hacked due weak Security Infrasture

[Return to Question 11](#) [Provide Feedback](#)

**Metadata** is data about data. Although this data can provide specific insight into personal data such as **Personal Identifiable Information (PII)** (see **Privacy Concerns**), there is also a problem with hackers gaining access to Metadata.

For example, knowing your name, address, phone number, and credit card details can be used to make illegal purchases in your name. This is a **Criminal Activity** in itself, but gaining information about your behavior and habits is a different kind of privacy violation. This information can be used to target you for advertisements or more nefariously specific scams. For instance, the metadata can now be used to determine that an individual is visiting a well-known cancer clinic and target the person for “miracle cures”.

Another example might be the discovery that a well-known founder and CEO of a publicly-traded company has visited the same well-known cancer clinic. This information is then used to in essence glean insider information about the company and make stock trades.

The use of Metadata is the primary engine for companies such as Google, Facebook, Microsoft, Apple, etc. However, this is done using their own mechanism to collect the data and users sign their rights away with the Service Level Agreements (SLAs), etc they “sign” when they choose to use these products. It is another thing to use government-provided data.

Therefore, Metadata not only contains Data about Data, but it can also contain information about the association of data elements together. Sometimes this activity is referred to as Triangulation.

**Metadata Triangulation** describes taking two pieces of metadata to infer a great deal more. Let me give you an example. You take a picture of something with your iPhone. That picture has both a date/time stamp and a GPS location tag. Two different pieces of information that, when combined, can lead to so much more. Some examples of information that can be inferred are:<sup>146)</sup>

- The weather
- Top news stories (including the content of those stories)
- Local objects, buildings, structures, etc.
- Natural disasters
- Nearby housing prices
- Stock prices, economic conditions, inflation, etc.
- Flights overhead, traffic conditions

There is an assumption that Bitcoin transactions are anonymous, the reality is that they are anonymized. The following article by John Bohannon highlights the issue:<sup>147)</sup>

*Bitcoin, the Internet currency beloved by computer scientists, libertarians, and criminals, is*



*no longer invulnerable. As recently as 3 years ago, it seemed that anyone could buy or sell anything with Bitcoin and never be tracked, let alone busted if they broke the law. "It's totally anonymous," was how one commenter put it in Bitcoin's forums in June 2013. "The FBI does not have a prayer of a chance of finding out who is who."*

*The Federal Bureau of Investigation (FBI) and other law enforcement begged to differ. Ross Ulbricht, the 31-year-old American who created Silk Road, a Bitcoin market facilitating the sale of \ \$1 billion in illegal drugs, was sentenced to life in prison in February 2015. In March, the assets of 28-year-old Czech national Tomáš Jiříkovský were seized; he's suspected of laundering \ \$40 million in stolen Bitcoins. Two more fell in September 2015: 33-year-old American Trendon Shavers pleaded guilty to running a \ \$150 million Ponzi scheme—the first Bitcoin securities fraud case—and 30-year-old Frenchman Mark Karpelès was arrested and charged with fraud and embezzlement of \ \$390 million from the now-shuttered Bitcoin currency exchange Mt. Gox.*

In this case, it was the “good guys” who used the Metadata, but this could also have been used for nefarious activities and a U.S. CBDC needs to protect this kind of data.

146)

Aaron Edell, [Coining a term: metadata triangulation](https://www.linkedin.com/pulse/coining-term-metadata-triangulation-aaron-edell/), 11 February 2016, Accessed: 24 April 2022, <https://www.linkedin.com/pulse/coining-term-metadata-triangulation-aaron-edell/>

147)

John Bohannon, [Why criminals can't hide behind Bitcoin - Even with cryptocurrency, investigators can follow the money](https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin), Science, 9 March 2016, Accessed: 24 April 2022, <https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q11:06\\_risks](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q11:06_risks)

Last update: **2022/05/17 21:36**



# 7. Risk of Business Processes Being Hacked

[Return to Question 11](#) [Provide Feedback](#)

Some government business processes need to be kept confidential, secret, or even top-secret when it comes to trying to audit or discover illegal or criminal activities. The reason is that if the processes were made readily available to the public, then the business process can be “gamed” to avoid detection. In these situations, the government is involved in an “arms race” so to speak with those who want to avoid detection. The government business processes are continuously refined and honed to detect illegal or criminal activity, while the “bad guys” continuously test the system to find its weaknesses.

As an example, the process of trying to “reverse engineer” the “rules” of a government business process for determining if an individual return gets audited run rampant when it comes to triggering an audit by the Internal Revenue Service (IRS).<sup>148)</sup>

More and more government business processes are using Artificial Intelligence (AI) to aid in the flow of the business process. Many of these AI processes are data-driven either through parameters or by using learning datasets continuously refined based on previous runs through the process. This means that either the original parameters or the learning data sets are subject to hacking attempts.

*Budget cuts and a significant drop in Special Agents that investigate criminal tax crimes have led the IRS to use Artificial Intelligence (AI) to uncover criminal tax activities. In a recent webcast hosted by the American Bar Association, the IRS revealed that research and investigative techniques that used to take weeks or months may now be accomplished in minutes with technology the IRS is rolling out to detect taxpayer noncompliance.*

*These computer tools are able to detect fraud, identity theft, money laundering, and hidden assets that Revenue Agents and Special Agents typically look for manually. The speed and sophistication of these computer data-mining programs have greatly increased the IRS' efficiency.*<sup>149)</sup>

If the government business processes are hacked, then the ability for illegal or criminal activities to go undetected is advanced.

Another problem would be if the government's business processes themselves were “hacked” to disable the government process or change the algorithms or parameters of the process to provide an unfair advantage. A simple example might be adding an exclusion for a certain individual within the process.

<sup>148)</sup>

Jacob Dayan, [IRS Audits: 10 Common Myths Debunked](https://articles.bplans.com/irs-audits-10-common-myths-debunked/), Accessed: 24 April 2022,  
<https://articles.bplans.com/irs-audits-10-common-myths-debunked/>

<sup>149)</sup>

Stahl Criminal Defense Lawyers, Accessed: 24 April 2022,  
<https://stahlesq.com/irs-artificial-intelligence-detects-tax-evaders/>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:brp:q11:07\\_risks](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:brp:q11:07_risks)

Last update: **2022/05/18 00:08**



## 8. Risk of competing Currency Models for the CBDC

[Return to Question 11](#) [Provide Feedback](#)

There are three categories of [Currency Models](#) used within the [White Paper](#) and identified in the [Object Management Group's - White Paper Analysis](#)

There is little to no explanation of why there are three different models used and no real explanation of when each is appropriate. Without clear guidance, this will continue to plague the U.S. CBDC effort.

Some of the “desirements” point to a [Digital Cash Model](#) (see Table 94) and some point to a [Digital Account Model](#) (see Table 28). There also seems to be some confusion about what and how Stablecoins fit into the CBDC. Stablecoins are a variation of the Digital Account Model that use a backing of the U.S. CBDC “coins” by the U.S. Dollar (see Table 37).

It is not impossible for the U.S. CBDC to use some combination of all three of these, BUT a clear vision needs to be developed of how the three models for a U.S. CBDC can coexist or that only one model be selected. Without this, the U.S. CBDC effort will flounder and waste time, money, and effort in the different models working against each other.

Mapping a subset of Digital Cash Model requirements identified within the White Paper Analysis conducted by the OMG

Table 94:

Category	Desirements
<b>Benefits</b>	
<b>Policies and Considerations</b>	P0004, P0027, P0029
<b>Risks</b>	R0013
<b>Design</b>	D0001, D0006, D0007, D0009

**Note:** **B** = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.

Example of mapping a subset of “desirements” identified during the White Paper Analysis conducted by the OMG

Table 95:

Topic	Desirements
<b>Digital Account Model</b>	B: B0005, B0010, B0022-4, B0038, B0047, B0048, B0049, B0051, B0054 P: P0002, P0012, P0013, P0017, P0018, P0019, P0020, P0021, P0023, P0024, P0025, P0017, P0028, P0030 R: R0002, R0009, R0012, R0015, R0020, R0023 D: D0001, D0002, D0003, D0005, D0008, D0010, D0012, D0013,

Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG

Table 96:

Area	Desirements
<b>Benefits</b>	B0016, B0017, B0021
<b>Policy and Considerations</b>	P0008, P0015, P0016
<b>Risks</b>	R0010, R0022

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q11:08\\_risks](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q11:08_risks)

Last update: **2022/05/19 01:26**



# Question: 12. How could a CBDC provide privacy to consumers without providing complete anonymity and facilitating illicit financial activity?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**How could a CBDC provide privacy to consumers without providing complete anonymity and facilitating illicit financial activity?**

## Answer

[Return to Top](#)

**Note:** See the answers to the sections:

- [4.4 National Privacy Considerations](#)
- [Question: 04. How might a U.S. CBDC affect the Federal Reserve's ability to effectively implement monetary policy in the pursuit of its maximum-employment and price-stability goals?](#)

The simplest way to achieve this would rely on the existing intermediary financial institutions to continue to do what they already do in terms of [Privacy](#), [National Security](#), and [International Security](#) BUT with the addition of the ability to use a real-time U.S. CBDC transfer mechanism instead of only the existing [Automated Clearing House \(ACH\) Network](#). This allows the existing mechanisms that are part of the existing intermediaries structure to remain in place for Privacy and Security. This of course assumes the existing mechanism on Privacy and Security is acceptable.

## Examples

[Return to Top](#)

For a list of desirements, see [Dual Payment Networks - Examples](#)

# Discussion of Examples

[Return to Top](#)

For a list of discussion of the desirements, see [Dual Payment Networks - Discussion of Examples](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q12:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q12:start) 

Last update: **2022/05/19 01:27**

# Question: 13. How could a CBDC be designed to foster operational and cyber resiliency? What operational or cyber risks might be unavoidable?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

This question is actually a compound question. Each question is answered independently:

1. [How could a CBDC be designed to foster operational and cyber resiliency?](#)
2. [What operational or cyber risks might be unavoidable?](#)

## Answer

[Return to Top](#)

In order to answer this compound question, each part of the question is answered separately:

- [1. How could a CBDC be designed to foster operational and cyber resiliency?](#)
  - [a\) Operational Resiliency](#)
  - [b\) Cyber Resiliency](#)
- [2. What operational or cyber risks might be unavoidable?](#)

From:  
<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:  
[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:brp:q13:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:brp:q13:start)

Last update: **2022/05/16 21:47**





# 1. How could a CBDC be designed to foster operational and cyber resiliency?

[Return to Question 13](#) [Provide Feedback](#)

Although Operational and Cyber Resiliency are affected by the entire system's Resiliency, the two topics are treated separately for this discussion.

The Oxford Dictionary definition of **Resiliency**:

1. the capacity to recover quickly from difficulties; toughness.  
*"the often remarkable resilience of so many British institutions"*
2. the ability of a substance or object to spring back into shape; elasticity.  
*"nylon is excellent in wearability and resilience"*

The answer to this question is further divided into Operational and Cyber :

- [a\) Operational Resiliency](#)
- [b\) Cyber Resiliency](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q13:sb\\_01:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q13:sb_01:start)

Last update: **2022/05/16 21:48**



# a) Operational Resiliency

[Return to Question 13-1](#) [Provide Feedback](#)

## Overview

[Return to Top](#)

Within the context of CBDC, [Operational Resilience](#) needs to address things which can not be added on *post facto* or “*bolted on*” easily after the CBDC is deployed. In other words, it must be “*baked in*” so to speak. This means that for something new, like the CBDC, it starts with specifying both [non-Functional](#) and [Functional Requirements](#). The specification of requirements needs to be done as soon as possible. Granted, the system must be agile and adapt to unforeseen changes in the deployment environment, [threats](#), [exploits](#), etc. However, there is a fine line between being “agile” and [Scope Creep](#). Agile should not be defining or redefining major functional or non-functional requirements, but rather defining or refining Software Requirements such as Business Requirements, User Requirements. Granted, some functional and non-functional can evolve over time, but usually as a result of a discovery process conducted during [Research Development Test & Evaluation](#) phases of a project, not during the production of a deployable system. Sometimes a [Proof-of-Concept](#) or Prototype Model<sup>150</sup>. The Prototype model can work in areas such as Web Development, but not in the development of [Mission Critical Systems](#). For Mission Critical Systems, the prototype is used as “throwaway” code used to capture and refine more formalized requirements.

Operational Resiliency also means once the CBDC is up and operational, it needs to respond to internal issues requiring continuous monitoring and adaptation of the CBDC in order to ensure it continues to have Operational Resiliency and that it can evolve and live beyond any existing software or hardware component that comprises the CBDC. In the U.S. Navy, this is referred to as “reboot the Navy” In other words, it is not possible to reboot all the systems on a ship or within a fleet at the same time and still maintain operational purpose. Likewise, in distributed systems, it is not possible to update all the parts at one time; sometimes older parts may take years to update. Also, see the OMG DIDO-RA sections on:

- [Reboot the World Problem](#)
- [Software Interfaces](#)
- [Replaceability](#)
- [Extensible and Dynamic Topic Types for DDS \(DDS-XTypes\)](#)

Operational Resiliency also means a system must continue to adapt to the threats (i.e., hostile cyber threats and physical threats like hurricanes, earthquakes, and fire), as well as, evolving national and geopolitical situations. The current Ukraine-Russian conflict is a prime example. This type of flexibility needs to be planned into the CBDC and not done as an *impromptu* reaction. See **Reboot the World Problem** above.

In other words, Operational Resiliency for the CBDC is not a “*done and dusted*” sort of problem, rather, it is a continuous process that covers the entire [lifecycle](#) of the CBDC or follow-on efforts.

# Understanding the "What ifs"

## [Return to Top](#)

A key aspect of obtaining **Operational Resiliency** is to develop "*what-if*" scenarios to validate the resilience of the system against functional and non-Functional requirements. Some possible scenarios might be:

- What if there is an upgrade to an Operating System?
- What if a key component of the CBDC system is obsolete and no longer available?
- What if there is a network outage in the NE U.S.?
- What if there is a network failure crossing the Atlantic?
- What if there is a breach of security from personnel?
- What if there is a compromise in the data access?
- What if there is a 10-fold demand for access to CBDC infrastructure?
- What if the value of the U.S. Dollar goes up or down against the rest of the world currencies?
- What happens if there is a war?

A well-defined Resilience Plan addressing the specific Functional and non-Functional requirements is essential. Trying to reverse engineer these requirements from an existing system adds a lot of risks and indicates the system is not designed but the result of Organic Development<sup>151</sup>. While this makes sense for products with a short life span and is not **Mission Critical**, it is not going to:

- Instill confidence (i.e., **B0020**)
- Preserve the dominant role of the U.S. Dollar (i.e., **B0036**)
- Provide broad support from CBDC Stakeholders (i.e., **B0006**)
- Provide trusted central bank money (i.e., **B0027**).

# Understanding the Requirements

## [Return to Top](#)

The following is an outline from the OMG's DIDO-RA for **non-Functional Requirements** and should be reviewed and assessed for applicability to the CBDC. In essence, each of the **non-functional** requirements should be considered carefully and tailored to the needs of the Federal Reserve and the CBDC.

### 1. **Portability**

- **Adaptability**
- **Installability**
- **Replaceability**

### 2. **Reliability**

- **Maturity**

- Availability
- Fault Tolerance
- Recoverability

### 3. Maintainability

- Modularity
- Reusability
- Analysability
- Modifiability
- [https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4\\_req:2\\_nonfunc:20\\_maintainability:testabilityTestability](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4_req:2_nonfunc:20_maintainability:testabilityTestability)

### 4. Security

- Confidentiality
- Data Integrity
- Non-Repudiation
- Authenticity
- Accountability

### 5. Manageability

- Types of Manageability Functions
- Manageability Costs
- System Manageability Issues
- Software Manageability Issues

### 6. Usability

- Effectiveness Metrics
- Efficiency Metrics
- Attitude / Satisfaction Metrics

### 7. Performance

- Platform Performance
- Application Performance
- Network Performance

### 8. Interoperability

### 9. Elasticity

### 10. Scalability

The following is an outline from the OMG's DIDO-RA for [Functional Requirements](#), and should be reviewed and assessed for applicability to the CBDC. In essence, each of the **functional** requirements should be considered carefully and tailored to the needs of the Federal Reserve and

the CBDC. For example, making a decision as to which **Hardware Platform(s)** or **Operating System Platform** to use has huge long range impacts on the CBDC and can ultimately negatively impact some non-Functional requirements such as **Portability, Replaceability, Manageability Costs** (See: [Vendor Lock-In](#)).

## 1. Platforms

- [Hardware Platform](#)
- [Operating System Platform](#)
- [Runtime Platforms](#)
- [Network Platforms](#)
- [Virtualized Nodes](#)

## 2. Access Control

# Steps to Achieving Operational Resilience

## [Return to Top](#)

The following is an excerpt is from a blog from Matt Kunkel on “*What is Operational Resilience?*”<sup>152)</sup>

1. **Take a holistic view of organizational risk.** Consider internal and external factors that impact your organization including business lines, assets, systems, processes, third parties, and people. Building a resilient operation means seeing the interconnection and interdependence of risk throughout the organization. Effective enterprise risk management systems must look across divisions and operations to holistically assess and account for potential threats.
2. **Design systems that take a comprehensive approach to risk assessment.** This starts with translating risk into a language that everyone at the firm understands. Having common vernacular permits a more comprehensive analysis and documentation of potential risks throughout the organization. It also allows for a more robust discussion around risk and returns as organizations consider how to adapt to changing conditions. Moreover, a shared language permits greater collaboration and cooperation, both critical to building a deeper understanding of the interdependence of risk in the organization and building operational resilience.
3. **Assess for critical points of failure to inform robust processes, ensure systems capabilities, and cultivate adaptable practices.** Although no market disruption or business interruption is the same, much can be learned from each. Knowing where the key risks lie across the organization and proactively implementing potential workarounds can help organizations better adapt to evolving conditions. The key is having robust systems and flexible processes, as well as cultivating a collaborative and resilient culture.

# Strengthening Operational Resilience

## [Return to Top](#)

Another blog post from Dominick Campagna defines five ways to strengthen **Operational Resilience** in the Financial Services Sector<sup>153)</sup> and should include the CBDC.

*For any financial services company, big or small, failure is not an option. Financial services play a critical, foundational role in almost every sector of the economy, and robust customer service is expected through technology failures, market disruption, systemic risk events, natural disasters, and even pandemics.*

*Companies that can deliver robust services through unexpected disruptions are considered operationally resilient. The critical importance of operational resilience in financial services is evidenced by the flurry of guidance from global financial regulators detailing expectations and mandating best practices on how providers and supporting infrastructure can improve their operational resilience.*

*Operational resilience, as **defined by the Federal Reserve Board (FRB)**, is the ability to deliver operations, including critical operations and core business lines, through disruption from any hazard. Last October, the FRB, in partnership with the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation, issued an interagency paper on Sound Practices to Strengthen Operational Resilience. This guidance, specifically written for banks and savings and loan companies with at least \$100 billion in assets, can be adapted and applied to financial services companies of any size.*

*In short, operational resilience is built through “effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.” More than business continuity, which is focused on uninterrupted operations, operational resilience considers how to best adapt a firm’s operations to deliver services through any disruption.*

5 Ways to Strengthen Operational Resilience in the Financial Services Sector.<sup>154)</sup>

Table 97:

<b>Step</b>	<b>Description of Activities</b>
<b>1. Establish Effective Governance</b>	Effective governance at the board and senior management level are critical to strengthening operational resilience. A strong risk management culture—the foundation of operational resilience—can only happen when there is top-down, organizational commitment. Board and executive responsibilities lay the groundwork and accountability for an operationally resilient mindset and commitment to supporting practices throughout the organization.

<b>Step</b>	<b>Description of Activities</b>
<b>2. Identify Critical Assets</b>	<p>Disruption, by its nature, is unpredictable. Operational resilience is not about identifying and measuring risks and uncertainty, as the impact of evolving technology and market changes can rarely be predicted. It is instead a framework for protecting the core business.</p> <p>The identification of critical assets and functions and core business lines should be done with the intention of protecting those assets and operations regardless of the source of disruption. Whether impacted by an unexpected technology failure, pandemic, cybersecurity incident, or any other cause, and the operationally resilient firm will have the policies, procedures, and practices in place to guide them through any disruption.</p> <p>To do this systematically, the board must determine and approve the risk appetite and risk tolerance for operational disruption, both at the enterprise level and for critical operations and core business lines. These explicit board parameters for the firm's acceptable level of risk from operational disruption can guide effective decision-making, appropriate investment in resilient systems and controls, and a consistent firm-wide approach to operational risk management.</p>
<b>3. Consider Key Dependencies and Interconnections</b>	<p>After identifying the core business lines and critical assets and functions, consider the key personnel, technology, processes, data, and physical infrastructure facilities required to protect them. Understanding those inputs and mapping out the dependency and interconnection of those assets on other internal functions, external parameters, or third parties will support a robust plan for business continuity and operational resilience.</p> <p>Managing third-party risk is critical for operational resilience, given the growing dependence on third parties to maintain specific functions and services of core business lines. This risk must also be accounted for within the approved risk tolerance.</p> <p>An understanding of the entire picture is necessary for recovery planning and the build-out of appropriate redundancies and alternate availability of essential resources, personnel, technology capability, and, if necessary, physical infrastructure. Recovery planning should also be consistent with existing risk management practices to ensure that there are no gaps in providing service or meeting regulatory requirements.</p>
<b>4. Proactively Review and Audit Plans</b>	<p>Operational resilience is a dynamic process requiring periodic review, testing, and auditing. As systems and processes evolve, so should your plans. Regularly employing an internal or external audit function to assess the design and effectiveness of operational resilience efforts will help to keep your plans relevant, identify shortcomings due to process or policy changes, and support a firm-wide culture of risk management and operational resilience.</p> <p>As new infrastructure and technology are adopted, your plans should be revisited and tested. Any digital transformation efforts should include planning for and adopting policies to address digital risks, such as disruption due to an internal failure, cybersecurity incident, or processing error.</p> <p>Consistent testing of your operational resilience plans, including dependencies and interconnections, will prepare your firm to pivot and adapt quickly to a disruption.</p>

Step	Description of Activities
<p><b>5. Form a Collaborative Approach to Operational Risk Management</b></p>	<p>An operational risk management function is responsible for determining and managing exposure related to internal processes, people, and systems as well as external threats and third parties. However, they cannot do this in a <b>silo</b>. Effective operational risk management requires a collaborative approach between senior management, business units, the operational risk management function or designees, and the internal or external audit function.</p> <p>A cross-functional approach supports effective identification, mitigation, and resolution of operational risk, including technology and third-party risk, within the risk appetite and risk tolerance defined by the board while collaboration ensures a consistent, firm-wide approach and commitment to operational resilience.</p>

150)

The prototyping model is a software development model in which a prototype is built, tested, and reworked until an acceptable prototype is achieved. It also creates a base to produce the final system or software. It works best in scenarios where the project's requirements are not known in detail. It is an iterative, trial and error method that takes place between developer and client. Matthew Martin, Prototyping Model in Software Engineering: Methodology, Process, Approach, Guru99, 5 March 2022, Accessed: 17 May 2022,

<https://www.guru99.com/software-engineering-prototyping-model.html>

151)

**Organic Development** is the internal growth based on adjusting and adapting to the situations at hand. For example, new information systems might evolve incrementally based on user feedback rather than starting anew with a system from a third party.

152)

Matt Kunkel, What is Operational Resilience?, Logicgate, 17 September 2020, Accessed: 11 April 2022, [What is Operational Resilience?](#)

153) 154)

Dominick Campagna, 5 Ways to Strengthen Operational Resilience in the Financial Services Sector, Logicgate, 22 January 2021, Accessed: 11 April 2022,

<https://www.logicgate.com/blog/5-ways-to-strengthen-operational-resilience-in-the-financial-service-s-sector/>

From:

<https://www.omgwiki.org/CBDC/> - OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:brp:q13:sb\\_01:prt\\_a:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:brp:q13:sb_01:prt_a:start)

Last update: 2022/05/18 00:12





## b) Cyber Resiliency

[Return to Question 13-1](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

**Cyber Resiliency** is tied to the **Securability** of the system. Securability is not a single “thing” that can be added to a system. To be truly secure, the entire **End-to-End Solution (E2ES)** needs to be secure and needs to be considered during the entire **System Lifecycle**. As shown in Figure 40, a layered approach is used to help isolate the security needs. Each layer represents a portion of the **Information Technology (IT)** stack, including the people who use and have access to the IT stack.



The layers of security.

Figure 40:

In many ways, **Cyber Resiliency** is the **Security non-functional** requirement in **Operational Resiliency**.

The **Security non-Functional Requirement** includes the following sub-requirements.

The sub-requirements of the Security non-Functional Requirement.

Table 97:

<b>Confidentiality</b>	<p><b>Confidentiality</b> is usually covered by using a <a href="#">Confidentiality Agreement</a> or <a href="#">Non-Disclosure Agreement (NDA)</a>, which defines a set of rules or a promise limiting access or places restrictions on certain types of information. Areas that have legal agreements covering confidentiality are:</p> <ol style="list-style-type: none"> <li>1. Legal Confidentiality</li> <li>2. Medical Confidentiality</li> <li>3. Clinical and Counseling Psychology</li> <li>4. Commercial Confidentiality</li> <li>5. Banking Confidentiality</li> <li>6. Public Policy Concerns</li> <li>7. Religious Confidentiality</li> </ol> <p>As a rule of thumb, it is best to treat all <a href="#">Personal Identifiable Information (PII)</a> as confidential and to secure it (i.e., require <a href="#">authentication</a> both to access the data and log access to the data).</p>
<b>Data Integrity</b>	<p><b>Data Integrity</b> is the completeness, accuracy and consistency of data throughout the entire data lifecycle of the data as well as when the <a href="#">Data is at Rest</a>, <a href="#">Data-in-Motion</a> and <a href="#">Data-in-Use</a>.<sup>156)</sup></p>
<b>Non-Repudiation</b>	<p>Non-Repudiation, (<a href="#">Computer Security Resource Center (CSRC)</a> Accessed 14 August 2020, <a href="#">Non-Repudiation</a>) means that it is not possible to repudiate (i.e., deny) that an action has been taken. For example, the signed contract witnessed by two people could not be repudiated. In other words, the contract now has Non-Repudiation.</p> <p>Non-Repudiation is about providing <a href="#">assurance</a> using <a href="#">evidence</a> that an action has been done. For example, a data sender is provided evidence (i.e., proof) of delivery while the receiver is provided evidence (i.e., proof) of the sender's identity. As a consequence, neither the sender nor the receiver can deny having processed the data.</p>
<b>Authenticity</b>	<p><b>Authenticity</b> is a property indicating the source and origin of the information<sup>157)</sup>. The process of authenticating a source starts when an <a href="#">entity</a> (i.e., user, remote process, intelligent agent, etc.) attempts to access resources on a <a href="#">Computer Platform</a>. The entity proves its identity in order to gain access rights. For example, traditionally when logging into a computer, users use <a href="#">Single-Factor Authentication (SFA)</a> , providing a username and password to confirm their identity and allow <a href="#">authentication</a> for future access to resources. However, the username and password login combination is no longer considered secure enough, especially if the <a href="#">Security Culture</a> is poor. As a consequence, many systems have added <a href="#">Two-Factor Authentication (2FA)</a> that require <a href="#">Biometrics</a> (i.e., facial recognition, fingerprints, etc.) or <a href="#">One-Time PIN (OTP)</a> . These 2FA methods generally require the user to be physically present to successfully log in.</p>
<b>Accountability</b>	<p><b>Accountability</b> is the <a href="#">principle</a> of holding an individual entrusted to safeguard and control <a href="#">key</a> components of a system or program (i.e., equipment, keying material, and information) answerable to proper authority for the loss or misuse of that component.<sup>158)</sup></p> <p>Accountability is a security <a href="#">goal</a> outlined in <a href="#">ISO/IEC 24010</a><sup>159)</sup> requiring the actions of an <a href="#">entity</a> to be traced uniquely to that entity. Accountability directly supports <a href="#">Non-Repudiation</a>. It also provides deterrence, helps with fault isolation, and is useful in intrusion detection and prevention. In many cases, it is a key source of the <a href="#">evidence</a> used in an <a href="#">After Action Review (AAR)</a> and can ultimately, if needed, support legal actions.</p>

The first step in designing for [Cyber Resiliency](#) is to begin with a [Systems Engineering](#) approach and to survey CBDC [Stakeholders](#) in order to refine the definitions and expectations of Cyber Resiliency. See [CBDC Stakeholders](#) for a more detailed discussion.

## Guidelines for Developing Cyber-Resilient Systems

[Return to Top](#)

An important first step is to follow the NIST Special Publication SP 800-16 volume 2 guidelines for developing cyber-resilient systems.<sup>160</sup> Skipping this step and going right to design and implementation often ends with the problem space (i.e., CBDC) being defined by the product(s) it chooses to use rather than by stakeholder requirements. A product-based solution can work, but it often misses many key requirements important to the stakeholders. For example, the design must be [Quantum Computing](#) “safe” or resistant.

SP 800-16 provides a framework for conducting cyber resiliency engineering. It starts with defining and setting the goals, objectives, techniques, implementation approaches, and design principles. Table 98 summarizes the definition and purpose of each construct, and how each construct is applied at the system level. **Note:** The framework is applicable to levels beyond the system level (e.g., mission or business function level, organizational level, or sector level).

Cyber Resiliency Constructs<sup>161</sup>)

Table 98:

Construct	Definition, Purpose, and Application at the System Level
<b>Goal</b>	A high-level statement supporting (or focusing on) one aspect (i.e., anticipate, withstand, recover, adapt) in the definition of cyber resiliency. <b>Purpose:</b> Align the definition of cyber resiliency with definitions of other types of resilience. <b>Application:</b> Can be used to express high-level stakeholder concerns, goals, or priorities.
<b>Objective</b>	A high-level statement (designed to be restated in system-specific and stakeholder-specific terms) of what a system must achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security. The objectives are more specific than goals and more relatable to threats. <b>Purpose:</b> Enable stakeholders and systems engineers to reach a common understanding of cyber resiliency concerns and priorities; facilitate the definition of metrics or <a href="#">Measures of Effectiveness (MoEs)</a> . <b>Application:</b> Used in scoring methods or summaries of analyses (e.g., cyber resiliency posture assessments).
<b>Sub-Objective</b>	A statement, subsidiary to a cyber resiliency objective, that emphasizes different aspects of that objective or identifies methods to achieve that objective. <b>Purpose:</b> Serve as a step in the hierarchical refinement of an objective into activities or capabilities for which performance measures can be defined. <b>Application:</b> Used in scoring methods or analyses; may be reflected in system functional requirements.

Construct	Definition, Purpose, and Application at the System Level
<b>Activity or Capability</b>	<p>A statement of a capability or action that supports the achievement of a sub-objective and, hence, an objective.</p> <p><b>Purpose:</b> Facilitate the definition of metrics or <b>MoE</b>. While a representative set of activities or capabilities have been identified in [Bodeau18b], these are intended solely as a starting point for selection, tailoring, and prioritization.</p> <p><b>Application:</b> Used in scoring methods or analyses; reflected in system functional requirements.</p>
<b>Strategic Design Principle</b>	<p>A high-level statement that reflects an aspect of the risk management strategy, which informs systems security engineering practices for an organization, mission, or system.</p> <p><b>Purpose:</b> Guide and inform engineering analyses and risk analyses throughout the system life cycle. Highlight different structural design principles, cyber resiliency techniques, and implementation approaches.</p> <p><b>Application:</b> Included, cited, or restated in system non-functional requirements (e.g., requirements in a Statement of Work [SOW] for analyses or documentation).</p>

Once the Systems Engineering is completed, a design can be achieved to foster cyber resiliency.

156)

What is Data Integrity, Accessed 8 July 2020,

<https://www.talend.com/resources/what-is-data-integrity/>

157)

Authenticity, Computer Security Resource Center (CSRC) Accessed 14 August 2020, [Authenticity](#)

158)

Accountability, Computer Security Resource Center (CSRC) Accessed 14 August 2020,

<https://csrc.nist.gov/glossary/term/accountability>

159)

Accessed 15 August 2020,

<https://iso25000.com/index.php/en/iso-25000-standards/iso-25010?limit=3&start=6>

160) 161)

Ron Ross, Victoria Pillitteri, Richard Graubart, Deborah Bodeau, Rosalie McQuaid, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, National Institute for Standards and Technology (NIST), NIST Special Publication 800-160, Volume 2, Revision 1, December 2021, Accessed: 11 April 2022,

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf>

From:

<https://www.omgwiki.org/CBDC/> - OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:brp:q13:sb\\_01:prt\\_b:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:brp:q13:sb_01:prt_b:start)

Last update: 2022/05/18 21:38



## 2. What operational or cyber risks might be unavoidable?

[Return to Question 13](#) [Provide Feedback](#)

### Overview

[Return to Top](#)

The biggest [Risks](#) to the CBDC is related to the [Information Technology\(IT\)](#) infrastructure for the CBDC and the need to ensure the CBDC meets the quality expectations of the U.S. Federal Reserve and the public. For example, the White Paper Desirements

- **B0020** is about establishing maintaining public confidence as a priority
- **B0027** and **B0050** are about establishing a priority on safe and trusted central bank money
- **R0011** is concerned about loss, theft, and fraud

These are unique problems for The Federal Reserve or to U.S. CBDC. These problems have been addressed by standards aimed at minimizing risk to projects heavily dependent on Software:

See the the OMG DIDO-RA section on:

- [Quality](#)
- [Open Source Paradigm](#)
- [Assurance](#)

### Specification versus Standards

[Return to Top](#)

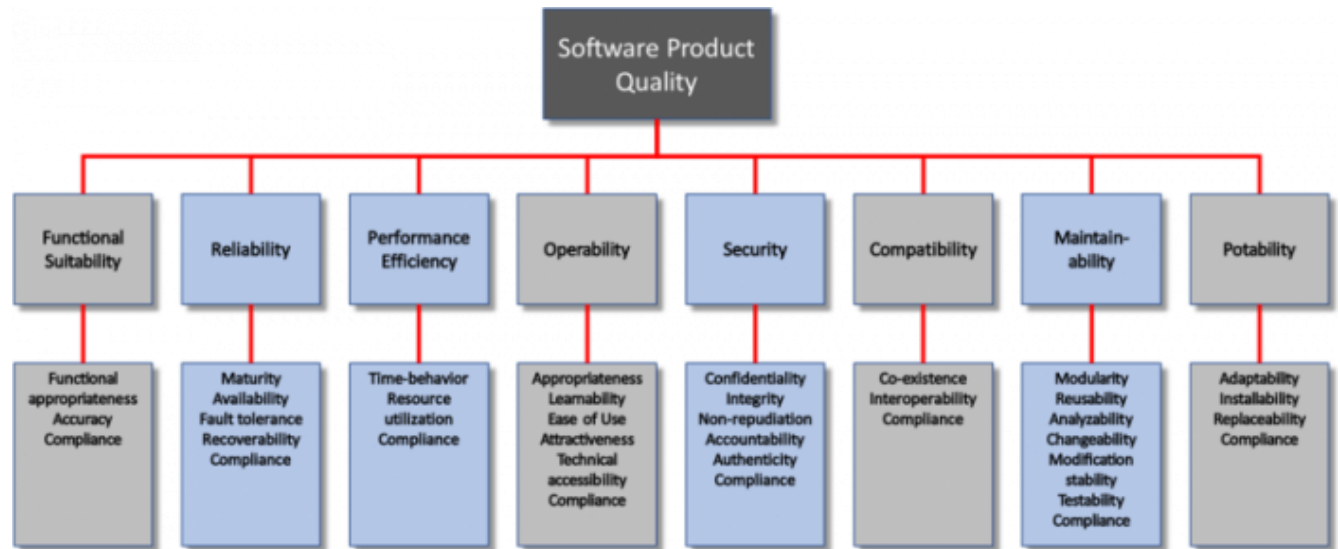
The difference between [Specification](#) and [Standard](#) is a specification is an explicit set of requirements to be satisfied by a material, product, or service. A Standard is a principle or example or measure used for comparison.

A [Specification](#) are statements detailing the requirements of a system or product that **should** or **must** be satisfied depending on the regulatory or contractual context. The Specification includes work products such as the definition of Protocols, Application Programming Interfaces (API), or the definition of processes. A [Standard](#) is a specification established by institutions such as [Standards Developing Organization \(SDO\)](#) or a [Voluntary Standards Consensus Body \(VSCB\)](#). Standards can be classified as [Technical](#) or *de facto* Standards.

### ISO, IEC, IEEE Standards

[Return to Top](#)

The purpose of ISO/IEC 25000 is to provide a general overview of SQuaRE contents, common reference models, and definitions, as well as, the relationship among the documents, and allow users of the Guide to gain a good understanding of how to use this series of standards. It also contains an explanation of the transition process between the old ISO/IEC 9126 and the newer ISO/IEC 14598 series and SQuaRE.



Quality Characteristics and Measures Specifications

Figure 41:

- [ISO 9001:2015 Quality management](#)
- [ISO/IEC/IEEE 90003:2018 Software engineering – Guidelines for the application of ISO 9001:2015 to computer software](#)
- [ISO/IEC/IEEE 25000:2014 SQuaRE -- Guide to SQuaRE](#)
- [ISO/IEC 25001:2014 SQuaRE -- Planning and Management](#)
- [ISO/IEC 25010:2011 SQuaRE -- System and Software Quality Models](#)
- [ISO/IEC 25012:2008 SQuaRE -- Data Quality Model](#)
- [ISO/IEC 25020:2007 SQuaRE -- Measurement Reference Model and Guide](#)
- [ISO/IEC 25021:2012 SQuaRE -- Quality Measure Elements](#)
- [ISO/IEC 25022:2016 SQuaRE -- Measurement of Quality in Use](#)
- [ISO/IEC 25023:2016 SQuaRE -- Measurement of System and Software Product Quality](#)
- [ISO/IEC 25024:2015 SQuaRE -- Measurement of Data Quality](#)
- [ISO/IEC 25030:2007 SQuaRE -- Quality Requirements](#)
- [ISO/IEC 25040:2011 SQuaRE -- Evaluation Process](#)
- [ISO/IEC 25041:2012 SQuaRE -- Evaluation Guide for Developers, Acquirers and Independent Evaluators](#)
- [ISO/IEC 25045:2010 SQuaRE -- Evaluation Module for Recoverability](#)
- [ISO/IEC/IEEE 15288:2015 Systems and software engineering -- System life cycle processes](#)

## Object Management Group (OMG) Standards and Consortium for Information & Software Quality (CISQ)

[Return to Top](#)

The Consortium for Information & Software Quality (CISQ) develops international standards to

automate the measurement of software from source code. The industry needs standard, low-cost, automated measures for evaluating software size and structural quality that can be used to control the quality, cost, and risk of software produced internally or by third parties.

Automation is critical because the manual review is infeasible for large multi-layer, multi-language, multi-platform systems. Additionally, [DevOps](#) greatly speeds up the deployment of applications, some changing on a daily or even hourly basis, which may result in unintended vulnerabilities without review.

- [OMG: Automated Source Code CISQ Maintainability Measure \(ASCMM\)](#)
- [OMG: Automated Source Code CISQ Measures \(ASCQM\)](#)
- [OMG: Automated Source Code CISQ Performance Efficiency Measure \(ASCPEM\)](#)
- [OMG: Automated Source Code CISQ Reliability Measure \(ASCRM\)](#)
- [OMG: Automated Source Code CISQ Security Measure \(ASCSM\)](#)
- [OMG: CISQ Automated Enhancement Points \(AEP\)](#)
- [OMG: CISQ Automated Function Points \(AFP\)](#)
- [OMG: CISQ Automated Technical Debt Measure \(ATDM\)](#)

The Case Management Model and Notation (CMMN) specification defines a common meta-model and notation for modeling and graphically expressing a Case, as well as an interchange format for exchanging Case models among different tools. The specification is intended to capture the common elements that Case management products use, while also taking into account current research contributions to Case management. It is to case management products what the OMG Business Process Model and Notation (BPMN) specification is to business process management products. This specification is intended to be consistent with and complementary to BPMN.

- [OMG: Case Management Model and Notation \(CMMN\)](#)

The Structured Assurance Case Metamodel (SACM) specification defines a metamodel for representing structured assurance cases. An Assurance Case is a set of auditable claims, arguments, and evidence created to support the claim that a defined system/service will satisfy the particular requirements. An Assurance Case is a document that facilitates information exchange between various system stakeholders such as suppliers and acquirers, and between the operator and regulator, where the knowledge related to the safety and security of the system is communicated in a clear and defensible way. Each assurance case should communicate the scope of the system, the operational context, the claims, the safety and/or security arguments, along with the corresponding evidence.

- [OMG: Structured Assurance Case Metamodel \(SACM\)](#)

The Test Information Interchange Format (TestIF) goal is to achieve a specification that defines the format for the exchange of test information among tools, applications, and systems that utilize it. The term “test information” is deliberately vague, because it includes the concepts of tests (test cases), test results, test scripts, test procedures, and other items that are normally documented as part of a software test effort. The long term goal is to standardize the exchange of all test-related artifacts produced or consumed as part of the testing process,

- [OMG: Test Information Interchange Format \(TestIF\)](#)

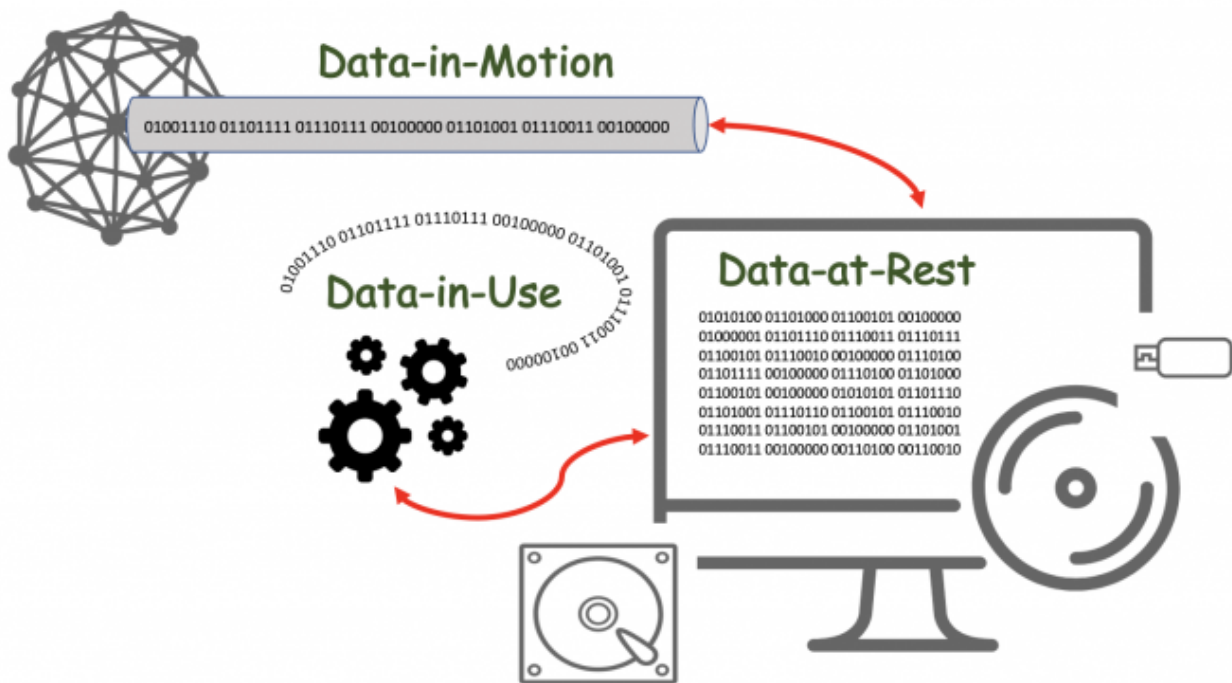


# State of Data

[Return to Top](#)

Data can exist in many states depending on how it is being used. The risks and concerns about Data in each of its different states are also important. Often, the primary focus for understanding data is to concentrate on **Data-at-Rest** . Even though data tends to remain relatively static, it can change over time. In the past, there was little concern for **Data-in-Motion** , which can have serious effects on **Reliability, Maintainability, and Availability (RAM)**, as well as, **Securability** and can leave a system vulnerable to breaches. With the advent of HTTPS, these vulnerabilities are mitigated. The latest issue has become the need to secure **Data-in-Use**. A recent WhatsApp data breach<sup>162)</sup> found that switching data between image filters could cause memory corruption followed by a crash that left data exposed.

Figure 39 graphically represents the different Data States within a system. Most systems are now able to handle Data-in-Motion and Data-at-Rest issues but have traditionally relied on physical security to protect Data-in-Use.



The various States of Data  
Figure 42:

Table 99 provides a quick overview of the various data states. These data states are described in detail in the [OMG DIDO-RA](#).

Data can exist in the following different states

Table 99:

<b>Data-at-Rest</b>	<b>Data-at-Rest</b> refers to all data in computer storage. It excludes data while it is moving across or within a network, and it excludes data that is temporarily residing in computer memory.
---------------------	---



<b>Data-in-Motion</b>	<a href="#">Data-in-Motion</a> , also referred to as <b>Data in Transit</b> or <b>Data in Flight</b> , is a <a href="#">Digital Asset</a> transmitted between locations (i.e., between computers or computer components). Data-In-Motion also describes data within <a href="#">Random Access Memory (RAM)</a> .
<b>Data-in-Use</b>	<a href="#">Data-in-Use</a> covers data being processed (i.e., updated, processed, erased, accessed or read) by a system. Data-In-Use is not passively stored, but is actively moving through parts of a <a href="#">Computing Platform</a> (i.e., <a href="#">Central Processing Unit (CPU)</a> , <a href="#">Dynamic Random Access Memory (DRAM)</a> ,, <a href="#">Data Bus</a> , etc.). <b>Data-In-Use</b> is one of three states of digital data - the other states are <a href="#">Data-at-Rest</a> and <a href="#">Data-in-Motion</a> .

## Examples

[Return to Top](#)

Some “desirements” in the [Money and Payments: The U.S. Dollar in the Age of Digital Transformation White Paper](#) and relating to **Operational or Cyber Risks** are summarized in the [White Paper Analysis](#) done by the [Object Management Group](#) and listed in [Table 100](#).

List of Operational or Cyber Risks Desirements identified in the White Paper  
Table 100:

Category	Desirements
<b>Benefits</b>	B0020, B0027, B0048, B0050, B0053, B0054
<b>Policy Considerations</b>	P0012, P0017, P0020, P0021, P0025, P0027, P0028
<b>Risks</b>	R0011
<b>Design</b>	D0015, D0016, D0017

## Discussion of Examples

[Return to Top](#)

[Table 101](#) comments on those “desirements” identified by the [White Paper](#) and the [OMG's White Paper Analysis](#) relating to [Central Bank Digital Currency \(CBDC\)](#) Operational or Cyber Risks. See: [Table 5](#) in [Section 4.1 Stakeholders](#).

List of “*desirements*” that allude to **stakeholders**  
Table 101:

Desirement No.	Desirement Text	Comment
B0020	<p><b>Maintain public confidence by not requiring mechanisms, such as deposit insurance</b></p>	<p>This is highly dependent on the <a href="#">Currency Model</a> used for the CBDC. If it is <a href="#">Digital Cash Model</a> then the need for deposit money is nil, since there are no deposits (i.s., just like there is no insurance on U.S. Dollars).</p> <p>However, if it is based on a <a href="#">Digital Account Model</a>, then by definition there are accounts, and by experience, deposit insurance is required to stabilize (See: <b>R0012</b>) the assets stored in those accounts. Deposit insurance provides three important benefits to the economy:<sup>163)</sup></p> <ol style="list-style-type: none"> <li>1. It assures small depositors that their deposits are <b>safe</b> and will be immediately available to them if their bank fails.(See: <b>B0007, B0019, B0027, B0050</b>)</li> <li>2. It maintains public <b>confidence</b> in the banking system, thus fostering economic stability. Without the confidence of the public, banks could not lend money but would have to keep depositors' money on hand in cash at all times. (See: <b>R0009, R0012</b>)</li> <li>3. It <b>supports the banking structure</b>. Deposit insurance makes it possible for the United States to have a system of both large and small banks. If there were no deposit insurance, the banking industry would probably be concentrated in the hands of a very few enormous banks. (See: <b>R0001, R0003, R0018</b>)</li> </ol>
B0027	<p><b>Maintain the centrality of safe and trusted central bank money</b></p>	<p>Safety and trust are both about perceived risk.</p> <ol style="list-style-type: none"> <li>1. Safety is defined as freedom from risk and risk is the possibility of suffering harm or loss. Both controllable and uncontrollable factors affect risk<sup>164)</sup>.</li> <li>2. Risk and trust are inextricably intertwined and loss of trust is possibly the biggest risk an endeavor can encounter since trust is the basis of all interactions.</li> </ol> <p>Therefore, the key is to manage <a href="#">risk</a>, which is the probability or threat of damage, injury, liability, loss, or any other negative occurrence caused by external or internal vulnerabilities, and that may be avoided through preemptive action.</p> <p>The goal of <a href="#">Systems Engineering</a> is to manage the risk, including the risk of not delivering what the customer wants and needs, the risk of late delivery, the risk of excess cost, and the risk of negative unintended consequences. One measure of the utility of Systems Engineering activities is the degree to which such risk is reduced. Conversely, a measure of acceptability of the absence of a System Engineering activity is the level of excess risk incurred as a result.</p>

<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>B0048</b>	<b>Provide a secure way for people to save</b>	In the U.S., savings accounts are a safe place since deposits (with limits) are guaranteed by Federal Deposit Insurance Corporation (FDIC) or the National Credit Union Administration (NCUA). Additionally, Certificates of Deposit (CDs) and U.S. government securities are also considered safe savings places. Both of these options offer some return on money. However, money safety is often associated with a high degree of liquidity, and relatively low fees.
<b>B0050</b>	<b>Extend Public Access to Safe Central Bank Money</b>	1. The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals See: <b>P0018</b> 2. Federal Reserve accounts for individuals represent a significant expansion of the Federal Reserve's role in the financial system and the economy. See: <b>P0019</b>
<b>B0053</b>	<b>Provide resiliency to threats to existing payment services—including:</b> <b>1. operational disruptions</b> <b>2. cybersecurity risks</b>	See the <a href="#">Overview of "What operational or cyber risks might be unavoidable?"</a>
<b>B0054</b>	<b>Attract risk-averse users to CBDC</b>	The term <b>Risk-Averse</b> describes the investor who chooses the preservation of capital over the potential for a higher-than-average return. In investing, risk equals price volatility. A volatile investment can make you rich or devour your savings. A conservative investment will grow slowly and steadily over time. <a href="https://www.investopedia.com/terms/r/riskaverse.asp">https://www.investopedia.com/terms/r/riskaverse.asp</a>
<b>P0012</b>	<b>The firms that operate interbank payment services are subject to federal supervision</b>	See the detailed discussion in section <a href="#">4.5 National Security Considerations</a> .
<b>P0017</b>	<b>The PWG report recommends CBDC complement existing authorities regarding:</b> <b>1. market integrity</b> <b>2. investor protection</b> <b>3. illicit finance</b>	See: 1. <a href="#">4.1 Stakeholders</a> 2. <a href="#">4.4 National Privacy Considerations</a> 3. <a href="#">4.5 National Security Considerations</a>

Desirement No.	Desirement Text	Comment
P0020	<p><b>The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments</b></p>	<p>Although the private sector is more than willing to take on this role, without some assurance that the wallets cannot be hacked and any losses will be covered by insurance, achievement of this desirement will probably have limited success.</p> <p>Hacks and data breaches happen almost daily. Cryptocurrency exchange hacks are particularly damaging because it affects thousands of users and involves the loss of funds. <sup>165)</sup></p> <p><i>Cryptocurrency exchanges come and go, and it's almost inevitable that an exchange will get hacked at one point or another. While cryptocurrencies themselves are very secure, exchanges can be affected by a variety of vulnerabilities, making them a prime target for malicious actors.</i></p> <p><i>State of the industry - February 2020: As it stands, 2019 saw a record number of twelve crypto exchanges being hacked. That being said, across the board the amounts of crypto stolen were worthless. In total, <b>\\$292,665,886 worth of cryptocurrency and 510,000 user logins were stolen from crypto exchanges in 2019.</b> One would hope that as time goes on cryptocurrency exchanges would become more secure. The unfortunate reality is that more exchanges are hacked every year. As cryptocurrency and exchanges remain largely unregulated, it is unclear who has jurisdiction over cryptocurrency markets.</i></p> <p>in 2019, there was a hack of a South Korean exchange that suffered a \\$51 million dollar breach. The stolen crypto has been on the move. It is moving between wallets, although it is unclear what purpose this will serve.</p> <p>At the current time, it is easy for exchanges or wallets to make lots of claims about security, but until there is a detailed assurance claim model to substantiate the claims, the promises are hollow.</p> <p>See:</p> <ol style="list-style-type: none"> <li>1. <a href="#">OMG: Structured Assurance Case Metamodel (SACM)</a></li> <li>2. <a href="#">OMG: Test Information Interchange Format (TestIF)</a></li> <li>3. <a href="#">OMG: Case Management Model and Notation (CMMN)</a></li> </ol>

Desirement No.	Desirement Text	Comment
P0021	<b>The intermediaries would operate in an open market for CBDC services</b>	<p>The lion's share of U.S. CBDC intermediaries will be building, delivering, and offering the services of software applications. This is not unlike the current situation in the smartphone world. However, the intermediary's applications will have to run not just on smartphones, but also on personal computers, servers, and mainframes. The Federal Reserve and a U.S. CBDC must be able to achieve and retain the confidence of consumers that these applications are sufficiently robust and provide reliable security to hold their vital assets.</p> <p>Therefore, there is a need for a U.S. CBDC “application store” to act as a web portal through which end users can access, download and install U.S. CBDC-approved software applications that rigorous Assurance Case Models with which the quality and security of these applications are validated.</p> <p>See:</p> <ol style="list-style-type: none"> <li>1. <a href="#">OMG: Structured Assurance Case Metamodel (SACM)</a></li> <li>2. <a href="#">OMG: Test Information Interchange Format (TestIF)</a></li> <li>3. <a href="#">OMG: Case Management Model and Notation (CMMN)</a></li> </ol>
P0025	<b>CBDC intermediary would need to verify the identity of a person accessing CBDC</b>	<ol style="list-style-type: none"> <li>1. If the <a href="#">Digital Cash Model</a> is used, then just like physical cash, there should be no IDs required.</li> <li>2. If the <a href="#">Digital Account Model</a> is used, it might depend on the rules placed on the intermediaries, Here are the rules for cashing checks in the U.S.: <ol style="list-style-type: none"> <li>a. When cashing a check, people use an ID to complete the transaction. Banks are required to have an identity verification policy by the Federal Deposit Insurance Corporation, which is why an ID is necessary<sup>166)</sup> <ol style="list-style-type: none"> <li>i. Ways of not showing an ID for cashing checks are: <ol style="list-style-type: none"> <li>1. <i>Signing it over to another individual</i></li> <li>2. <i>Using ATM check to cash if it's offered by your bank</i></li> <li>3. <i>Depositing it into your own account using a bank ATM</i></li> </ol> </li> <li>b. When using Credit Cards, the major Credit Cards (i.e., Visa and Mastercard) do not require an ID to complete a transaction. <p><i>They both have rules that limit stores from requiring you to show your ID as a condition of purpose. These rules also make them accept your card even if you refuse to show your ID.</i><sup>167)</sup></p> </li> </ol> </li> </ol> </li> </ol>
P0027	<b>CBDC a risk-free asset</b>	<p>The risk-free rate of return is the theoretical rate of return of an investment with zero risk. The risk-free rate represents the interest an investor would expect from an absolutely risk-free investment over a specified period of time.</p> <p>The so-called “real” risk-free rate can be calculated by subtracting the current inflation rate from the yield of the Treasury bond matching your investment duration.</p> <p><a href="https://www.investopedia.com/terms/r/risk-freerate.asp">https://www.investopedia.com/terms/r/risk-freerate.asp</a></p>

Desirement No.	Desirement Text	Comment
P0028	<p><b>Require significant international coordination to address issues such as:</b></p> <ol style="list-style-type: none"> <li><b>1. common standards</b></li> <li><b>2. infrastructure,</b></li> <li><b>3. the types of intermediaries able to access any new infrastructure,</b></li> <li><b>4. legal frameworks</b></li> <li><b>5. preventing illicit transactions</b></li> <li><b>6. the cost and timing of implementation</b></li> </ol>	<p>See: <a href="#">4.6 International Considerations</a></p>
R0011	<p><b>Increased Risk to consumer's vulnerability to:</b></p> <ol style="list-style-type: none"> <li><b>1. loss</b></li> <li><b>2. theft</b></li> <li><b>3. fraud</b></li> </ol>	<p>If the U.S. CBDC avoids most of the safeguards built into the current U.S. financial system, then there is an increased risk of <b>loss</b>, <b>theft</b>, and <b>fraud</b>. Most of the laws and regulations outlined in section <a href="#">4.5 National Security Considerations</a> have evolved over time in response to consumer demand for protection. Although it seems appealing, more efficient, and even “modern”, consumers should demand the same level of protection from a U.S.-based CBDC.</p> <p>According to Ryan Browne of CNBC<sup>168)</sup></p> <ul style="list-style-type: none"> <li>• <i>Overall losses caused by <a href="#">Decentralized Finance (DeFi)</a> exploits have totaled \ \$12 billion so far in 2021, according to a report from Elliptic.</i></li> <li>• <i>Fraud and theft accounted for \ \$10.5 billion of that sum — a sevenfold increase from last year.</i></li> </ul>

<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>D0015</b>	<b>Design should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks</b>	In order to protect data during all aspects of data handling and processing, there will most likely need to be new network hardware, computer processors, and even new encryption algorithms based on Quantum Computing's ability to crack encryption. See: <ol style="list-style-type: none"> <li>1. <a href="#">State of Data</a></li> <li>2. <a href="#">OMG DIDO-RA Network Devices</a></li> <li>3. <a href="#">Data in Use</a></li> <li>4. <a href="#">Access Control List (ACL)</a></li> <li>5. <a href="#">Zero Trust Security Model</a></li> <li>6. <a href="#">Zero Trust Architecture (ZTA)</a></li> <li>7. <a href="#">The Onion Router (Tor)</a></li> <li>8. <a href="#">Secure Memory Encryption (SME)</a></li> <li>9. <a href="#">Full Memory Encryption (FME)</a></li> <li>10. <a href="#">Total Memory Encryption (TME)</a></li> <li>11. <a href="#">Software Guard Extensions (SGX)</a></li> <li>12. <a href="#">Multi-Party Computation (MPC)</a></li> <li>13. <a href="#">TRESOR</a></li> <li>14. <a href="#">Homomorphic Encryption (HE)</a></li> </ol>
<b>D0016</b>	<b>Design should include offline capabilities to help with the operational resilience of the payment system</b>	See: <a href="#">Question: 18. Should a CBDC have "offline" capabilities? If so, how might that be achieved?</a>
<b>D0017</b>	<b>Design should include digital payments in areas suffering from large disruption, such as natural disasters</b>	See: <a href="#">Question: 18. Should a CBDC have "offline" capabilities? If so, how might that be achieved?</a>
<b>B = <a href="#">Benefit Considerations</a></b>		
<b>P = <a href="#">Policy Considerations</a></b>		
<b>R = <a href="#">Risk Considerations</a></b>		
<b>D = <a href="#">Design Considerations</a></b>		

162)

Czarina Grace, [WhatsApp Data Breach 2021 Could Expose 2 Billion Users: Update Now on Android, iOS to Fix Security Risk](#), iTechPpost, 6 September 2021, Accessed 6 October 2021, <https://www.itechpost.com/articles/106929/20210906/whatsapp-data-breach-2021-expose-2-billion-users-update-now.htm>

163)

State of Connecticut, Department of Banking, [ABC's of Banking](#), Accessed: 13 April 2022, <https://portal.ct.gov/DOB/Consumer/Consumer-Education/ABCs-of-Banking---Deposit-Insurance>

164)

Derek Lann, [What is the Relationship Between Safety and Risk?](#) Accessed: 13 April 2022, <https://avatarms.com/safety-risk/>

165)

Selfkey Blog, [A Comprehensive List of Cryptocurrency Exchange Hacks](#), 13 February 2020, Accessed: 13 April 2020, <https://selfkey.org/list-of-cryptocurrency-exchange-hacks/>  
<sup>166)</sup>

Frank Gogol, Stilt, [How to Cash a Check Without an ID](#), 18 March 2022, Accessed: 13 April 2022, [https://www.stilt.com/blog/2021/05/how-to-cash-a-check-without-an-id/#3\\_Ways\\_to\\_Cash\\_a\\_Check\\_Without\\_an\\_ID](https://www.stilt.com/blog/2021/05/how-to-cash-a-check-without-an-id/#3_Ways_to_Cash_a_Check_Without_an_ID)  
<sup>167)</sup>

Privacy Rights Clearing House, [Do I have to show my ID when I buy something with a credit card?](#), 15 July 2019, Accessed: 13 April 2022, <https://privacyrights.org/resources/do-i-have-show-my-id-when-i-buy-something-credit-card>  
<sup>168)</sup>

Ryan Browne, CNBC, 19 November 2021, Accessed: 13 April 2022, <https://www.cnbc.com/2021/11/19/over-10-billion-lost-to-defi-scams-and-thefts-in-2021.html>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:brp:q13:sb\\_02:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:brp:q13:sb_02:start)

Last update: **2022/05/19 01:30**





# Question: 14. Should a CBDC be legal tender?

[Return to CBDC Benefits, Risks, and Policy Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**Should a CBDC be legal tender?**

## Answer

[Return to Top](#)

## Overview

[Return to Top](#)

In general, a United States CBDC should be designated as legal tender, thereby matching the current physical US currency. Such a characterization is necessary for a Digital Dollar to exist alongside and eventually replace physical notes and coins, particularly in relatively small “retail” transactions like the acquisition of food, energy, and/or personal services. With the wide adoption of a Digital Dollar, the reduction in costs associated with producing, transferring, securing, and destroying physical currency notes and coins would be quite considerable.

The arguments against designating a US Digital Dollar as a legal tender are more operational in nature. Consider, for instance, the various types of fraud that might be attempted with Digital Dollars. Currently, the largest US note in general circulation is one hundred dollars. It is thus difficult to gather sufficient physical notes to exchange for substantial physical assets like an automobile or a housing unit. How would similar “speed bumps” be implemented with a United States CBDC where the transaction size might be unbound?

Currently, financial institutions are key points of control in implementing Anti-Money Laundering (“AML”) / Combating the Financing of Terrorism (“CMT”) policies and procedures. If a United States CBDC is considered legal tender, presumably it will also be convertible with both physical currency and/or account balances with financial institutions. What entities, potentially with geographic or other constraints, will be permitted to perform these conversions, particularly the physical currency / CBDC type where counterfeit tender might be involved?

The design features of a United States CBDC will necessitate trade-offs along four axes:

1. account-based versus token-based
2. institutional versus retail
3. direct versus indirect obligation
4. centralized versus decentralized.

As the design evolves, OMG recommends further consultations that include Use Case analysis and solicitation of scenarios that test the limits of the contemplated CBDC design.

According to the U.S. Code, Title 32, Subtitle IV, Chapter 51, Subchapter I Section § 5103, **Legal Tender** in the U.S. is:

*United States coins and currency (including [Federal Reserve Notes](#) and circulating notes of Federal Reserve Banks and national banks) are legal tenders for all debts, public charges, taxes, and dues. Foreign gold or silver coins are not legal tender for debts.* <https://www.law.cornell.edu/uscode/text/31/5103>

According to the Statutes, yes if the U.S. CBDC is considered a form of the [Federal Reserve Note](#).

The U.S. CBDC could offer another mechanism to the existing non-cash mechanisms such as debit cards, credit cards, electronic transfers, and checks. However, in order to offer real-time settlements, it may need to use a different mechanism than the existing [Automated Clearing House \(ACH\) Network](#) currently in use to electronically move money between banks accounts across the U.S. The current ACH network is run by an organization called Nacha, formerly the [National Automated Clearing House Association \(NACHA\)](#).

There definitely would need to be a **bridge** between the existing ACH-NACHA payment network and a U.S. CBDC, its associated Consensus Algorithms, and the network of nodes. However, in addition to the bridge between the two, there probably needs to exist a new consolidated frontend ( [Application Programming Interface \(API\)](#)?) that abstracts the type of payment from the participants in the transactions. In other words, the transaction should be agnostic to non-cash mechanisms such as debit cards, credit cards, electronic transfers, checks, and CBDC.

The U.S. CBDC needs to support basic purchases of:

1. goods
2. services
3. pay bills
4. pay taxes

U.S. CBDC should be treated like any other payment form, even though under the hood, it might use a different payment network than the [National Automated Clearing House Association \(NACHA\)](#) network.

## Examples

[Return to Top](#)

The following “Desirements” are from the [White Paper](#) as identified by the [Object Management Group's](#) report called [White Paper Analysis](#):

Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG

Table 102:

<b>Benefits</b>	B0025, B0026, B0029, B0034, B0038, B0040, B0044, B0045, B0046, B0047, B0049
<b>Policies</b>	P0003, P0018, P0019, P0020, P0021
<b>Risks</b>	
<b>Design</b>	D0004

## Example Discussion

[Return to Top](#)

“Desirements” identified in the **White Paper** that have potential monetary policy impacts.

Table 103:

<b>Statement No.</b>	<b>Statement</b>	<b>Comment</b>
<b>B0025</b>	<b>Serve as a new foundation for the payment system</b>	The CBDC could offer another mechanism to the existing non-cash mechanisms such as debit cards, credit cards, electronic transfers, and checks. However, in order to offer real-time settlements, it may need to use a different mechanism than the existing Automated Clearing House Network (ACH) network currently to electronically move money between bank accounts across the U.S. The current ACH network is run by an organization called Nacha, formerly the <a href="#">National Automated Clearing House Association (NACHA)</a> .
<b>B0026</b>	<b>Provide a bridge between legacy and new payment services</b>	There definitely would need to be a bridge between the existing ACH-NACHA payment network and a U.S. CBDC, its associated Consensus Algorithms, and the network of nodes. However, in addition to the bridge between the two, there probably needs to exist a new consolidated frontend ( <a href="#">Application Programming Interface (API)</a> ?) that abstracts the type of payment from the participants in the transactions. In other words, the transaction should be agnostic to non-cash mechanisms such as debit cards, credit cards, electronic transfers, checks, and CBDC.
<b>B0029</b>	<b>Support basic purchases of:</b> <b>1. goods</b> <b>2. services</b> <b>3. pay bills</b> <b>4. pay taxes</b>	See the answer to <b>B0026</b> above. CBDC should be treated like any other payment form, even though under the hood, it might use a different payment network than the <a href="#">National Automated Clearing House Association (NACHA)</a> network.

Statement No.	Statement	Comment
<b>B0038</b>	<b>Allow private-sector innovators to focus on:</b> <b>1. new access services</b> <b>2. distribution methods</b> <b>3. related service offerings</b>	By defining a new standardized <a href="#">Application Programming Interface (API)</a> as in <b>B0026</b> above, a marketplace of products can be developed by the private sector to help innovate the current payment ecosystem.
<b>B0044</b>	<b>Facilitate access to digital payments</b>	See answers to <b>B0011, B0018, B0020, B0024, B0025, B0026</b> above.
<b>B0046</b>	<b>Enable rapid and cost-effective delivery of:</b> <b>1. wages,</b> <b>2. tax refunds</b> <b>3. other federal payments</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>B0047</b>	<b>Lower transaction costs</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>B0049</b>	<b>Promote access to credit</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>P0003</b>	<b>Complement current forms of money and methods for providing financial services</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>P0018</b>	<b>The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals</b>	The easiest solution is to allow current intermediaries to process CBDC transactions using an upgraded payment system. See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>P0020</b>	<b>The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>P0021</b>	<b>The intermediaries would operate in an open market for CBDC services</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>D0004</b>	<b>Design should influence how the Federal Reserve might affect monetary policy</b>	See answer <b>B0025, B0026, B0029, B0038, B0040</b> above.
<b>B = <a href="#">Benefit Considerations</a></b>		
<b>P = <a href="#">Policy Considerations</a></b>		
<b>R = <a href="#">Risk Considerations</a></b>		
<b>D = <a href="#">Design Considerations</a></b>		

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:brp:q14:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:brp:q14:start) 

Last update: **2022/05/19 01:38**

# 5.2 Design

[Return to Public Questions](#) **Provide Feedback**

## Specific Questions

[Return to Top](#)

- Question: 15. Should a CBDC pay interest? If so, why and how? If not, why not?
- Question: 16. Should the amount of CBDC held by a single end user be subject to quantity limits?
- Question: 17. What types of firms should serve as intermediaries for CBDC? What should be the role and regulatory structure for these intermediaries?
- Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?
- Question: 19. Should a CBDC be designed to maximize ease of use and acceptance at the point of sale? If so, how?
- Question: 20. How could a CBDC be designed to achieve transferability across multiple payment platforms? Would new technology or technical standards be needed?
- Question: 21. How might future technological innovations affect design and policy choices related to CBDC?
- Question: 22. Are there additional design principles that should be considered? Are there tradeoffs around any of the identified design principles, especially in trying to achieve the potential benefits of a CBDC?

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:dsn:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:dsn:start)

Last update: **2022/05/17 01:49**



# Question: 15. Should a CBDC pay interest? If so, why and how? If not, why not?

[Return to Design Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

1. **Should a CBDC pay interest?**
2. **If so, why and how?**
3. **If not, why not?**

## Answer

[Return to Top](#)

The answer depends on the architecture, design and implementation. (See: [4.0 Common Elements](#)).

1. If it is a replacement for cash: **NO**
2. If it is a replacement for a bank account or equivalent such as [Payment Cards](#) savings, checking, investment, direct pay, credit, debit cards, etc. ): **YES**

## Overview

[Return to Top](#)

Before an answer can be provided about paying interest on CBDC, it is essential to clearly state the purpose and goals of the CBDC. Based on the information in the White Paper, it is not clear if the CBDC should be a replacement for Physical Money, a replacement for bank accounts, or a hybrid combination of the two. Currently, there is no interest paid in cash. In fact, that is a motivation for not hoarding cash, but putting it into an account. The interest paid on the account depends on the kind of account (i.e., checking, savings, certificate of deposit, money market, etc.).

1. Is the CBDC suppose to be an alternative to existing physical dollar bills? If so:

- What denominations are to be created (\\$1, \\$2, \\$5, \\$10, \\$20, \\$50, \\$100)?
- What about coins? (i.e., penny, nickel, dime, quarter, half-dollar)
- Will it be able to be used everywhere physical money is used?
- Can transactions be made using a combination of CBDC and Physical Money?
- Can CBDC and Physical Money be interchanged? Where? Fees?

2. Is it supposed to be the equivalent of a financial account (i.e, savings, checking, investment, direct pay, credit, debit cards, etc. )? If so:

- How many accounts can an individual have?
- Is there a cost for maintaining the accounts?
- How will rules such as Know-Your-Customer(KYC) be applied?
- Can the accounts be garnered for taxes? Child support? Student debt? Other debt?
- Does it require a court order or warrant to review the account activity?
- Is there an age limit on who can have an account?
- Do you have to be a US Resident to have an account?
- What IDs need to be associated with the account?
- Do you need a taxpayer ID?
- Do you need to have a current street address?

3. Has a trade study been conducted to determine the best solution?

## Examples

[Return to Top](#)

There are three categories of requirements alluded to in the [White Paper](#) as identified by the [Object Management Group White Paper Analysis](#):

There are three Currency Models that are applicable to the CBDC.

- **4.2.1 Digital Cash Model** - is a model representing the CBDC using cash (i.e., coins, \ \$1, \ \$2, \ \$5, \ \$10, \ \$20, \ \$50 and \ \$100 bills)) as the basis of the CBDC
- **4.2.2 Digital Account Model** - is a model that represents the CBDC in using digital accounts (i.e, Savings, Checking, Investment, Direct Pay, Credit Cards, Debit Cards, etc.)
- **4.3 Stablecoins** - is a currency model tying a cryptocurrency to a real world asset such as a fiat currency, gold, indexed funds. etc.

Table 94 provides a list of requirements associated with each of the CBDC model taxonomy.

Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG

Table 104:

Topic	Requirements
<b>Digital Cash Model</b>	B: B0003, B0004, B0007, B0009, B0013, B0018, B0020, B0022-1, B0022-2, B0022-3, B0024, B0028, B0029, B0034, B0036, B0040, B0042 P: P0004, P0027, P0029 R: R0013 D: D0001, D0006, D0007, D0009
<b>Digital Account Model</b>	B: B0005, B0010, B0022-4, B0038, B0047, B0048, B0049, B0051, B0054 P: P0002, P0012, P0013, P0017, P0018, P0019, P0020, P0021, P0023, P0024, P0025, P0017, P0028, P0030 R: R0002, R0009, R0012, R0015, R0020, R0023 D: D0001, D0002, D0003, D0005, D0008, D0010, D0012, D0013,



Topic	Requirements
<a href="#">Stablecoin / Research</a>	B: B0016, B0017, B0021 P: P0008, P0015, P0016 R: R0010, R0017, R0019, R0020, R0021, R0022

## Discussion of Examples

[Return to Top](#)

The following discussion of the three models identified in the requirements. Each section is independent of the other sections and can be read *as-is*.

### Digital Cash Model

[Return to Top](#)

Many of the OMG-identified “desirements” found in the [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation White Paper](#) during the [White Paper Analysis](#) appear to be appropriate of a CBDC “Cash Model”. The “Cash Model” uses Digital Money in an analogous model as Cash for CBDC. For example, the requirements **B0004** which is a requirement to “*Protect consumer privacy*” is more closely related to a “cash mode” rather than a bank account model. There are no bank accounts required in order to complete a transaction, just “cash” in exchange for goods and services. This is in contrast to checkbooks, debit, or credit card transactions, which are associated with an account offered by intermediary commercial banks and directly tied to an Identity.

List of requirements (i.e., desirements) identified in the **White Paper** indicating a **Cash Model**.  
Table 105:

Requirement	Statement	Comment
<b>B0003</b>	<b>Complement, rather than replace, current forms of money and methods for providing financial services</b>	A “digital cash” is complementary to the existing cash money, just without the need for physical money.
<b>B0004</b>	<b>Protect consumer privacy</b>	There are no identities required for cash transactions.
<b>B0007</b>	<b>Provide households and businesses a: 1. convenient 2. an electronic form of central bank money with a. safety b. liquidity</b>	1. Cash probably represents the epitome of liquidity, that is, unless the size of the transaction gets too big, then US Federal law requires a person to report cash transactions of more than \ \$10,000 by filing IRS Form 8300 PDF, Report of Cash Payments Over \ \$10,000 received in a Trade or Business. <sup>169)</sup> 2. With cash, your spending is straightforward and there is less risk of identity theft. Ultimately, it's up to each individual to make the best decisions based on their financial health, what they are purchasing, and the risks they are willing to incur <sup>170)</sup> .
<b>B0009</b>	<b>Provide faster and cheaper payments (including cross-border payments)</b>	US Dollars in the form of cash are used in many parts of the world. As of 2018, the U.S. had \$1,671 billion in circulation. As much as half that value is estimated to be in circulation abroad. <sup>171)</sup> Many of these bills are in the former Soviet Union countries and in Latin America. They are often used as hard currency in day-to-day transactions. <a href="https://www.thebalance.com/world-currency-3305931#citation-12">https://www.thebalance.com/world-currency-3305931#citation-12</a>
<b>B0013</b>	<b>Provide immediate access to transferred funds</b>	Sine the digital cash is for all intents and purposes cash, the same accessibility as cash should apply
<b>B0018</b>	<b>Allow the general public to make digital payments</b>	Digital cash should be immediately transferrable to traditional cash, and therefore, it should be at least as usable for digital payments as actual cash, but can also be used online just like Direct Pay, Credit, or Debit Cards.

Requirement	Statement	Comment
B0019	<b>Provide the safest digital asset available to the general public, with no:</b> 1. associated credit 2. liquidity risk	With cash, there is no need for credit and by definition it is liquid. See <a href="#">Liquidity Risk</a>
B0020	<b>Maintain public confidence by not requiring mechanisms, such as deposit insurance</b>	The only need for <a href="https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend_a_glossary:d:deposit_insurance">https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend_a_glossary:d:deposit_insurance</a> is when there is not enough cash in hand to pay for liabilities. By definition, a cash-based CBDC would have enough cash.
B0022	<b>Provide a CBDC that is:</b> 1. <b>Privacy-Protected</b> 2. <b>NOT Intermediated</b> 3. <b>Widely Transferable</b> 4. <b>NOT Identity-Verified</b>	By definition, cash is considered private and is widely transferable unless the quantity of cash makes it too onerous.
B0024	<b>Provide transactions finalized and completed in real-time</b>	Since there is no need to do a background check on the participants in a cash transaction, the transaction is real-time.
B0028	<b>Offer the general public broad access to digital money:</b> 1. free from credit risk 2. liquidity risk	Cash is by definition does not require credit and inherently no <a href="#">Liquidity Risk</a> .
B0029	<b>Support basic purchases of:</b> 1. goods 2. services 3. pay bills 4. pay taxes	There is no federal statute mandating that a private business, a person, or an organization must accept currency or coins as payment for goods or services. Private businesses are free to develop their own policies on whether to accept cash unless there is a state law that says otherwise. <a href="https://www.federalreserve.gov/faqs/currency_12772.htm">https://www.federalreserve.gov/faqs/currency_12772.htm</a> , Therefore, the same can be applied to Digital Cash. Although it is currently possible to pay Federal taxes in cash, it is more difficult than paying online with Direct Pay, Credit, or Debit Cards.
B0034	<b>Generate new capabilities to meet the speed and efficiency requirements of the digital economy</b>	Although cash is quick and efficient during face-to-face transactions, it is difficult over long distances or when the payments become large.
B0036	<b>Preserve the dominant international role of the U.S. dollar</b>	See: <b>B0009</b>
B0040	<b>Provide micropayment support</b>	As long as the micropayment is larger than the cost of conducting the transaction, micropayments are feasible. However, if the cost of the micropayment is very small, then there is probably a need for an account for accumulating the micropayments until it becomes financially viable to process the micropayment.
B0042	<b>Preserve the dominant international role of the U.S. dollar</b>	See: <b>B0009</b>
P0004	<b>Protect consumer privacy</b>	Since there is no need for an account or identification with cash, consumers' privacy is protected.
P0027	<b>CBDC a risk-free asset</b>	As long as the CBDC is tied to the US Dollar, it will have the same risk as to the US Dollar.
P0029	<b>The Federal Reserve is committed to ensuring the continued safety and availability of cash</b>	The Cash Model for CBDC treats the CBDC as a form of cash when the cash model is used.
R0013	<b>CBDC offers no associated credit or Liquidity Risk</b>	In the cash model of the CBDC, this is definitely true.

Requirement	Statement	Comment
D0001	Design should be for a non-interest-bearing CBDC, for example, would be less attractive as a substitute for commercial bank money	CBDC using the cash model would be just another form of cash, and therefore should not offer interest
D0006	Design should allow an increase in CBDC supply to provide an adequate buffer, so there is little effect on the federal funds rate	The same rules would apply as used with traditional cash
D0007	Design should allow the Federal Reserve to increase the level of reserves on average, in order to provide an adequate buffer against unanticipated increases in CBDC	Under the CBDC cash model, the Federal Reserve would treat CBDC reserves similarly to cash reserves
D0009	Design should allow for significant foreign demand for CBDC, furthering complicate monetary policy implementation	See: B0009
B = <a href="#">Benefit Considerations</a>		
P = <a href="#">Policy Considerations</a>		
R = <a href="#">Risk Considerations</a>		
D = <a href="#">Design Considerations</a>		

## Digital Account Model

### [Return to Top](#)

Many of the OMG identified requirements found in the [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation White Paper](#) during the [White Paper Analysis](#) appear to be appropriate of a CBDC **“Account Model”**. The **“Account Model”** uses Digital Money in an analogous model as Accounts for CBDC. For example, the requirement **B0005** is a requirement to *“Protect against criminal activity| In this context, criminal activity is either Money Laundering or Fraud. Fraud is an intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim. Types of fraud include tax fraud, credit card fraud, wire fraud, securities fraud, and bankruptcy fraud. Fraudulent activity can be carried out by one individual, multiple individuals, or a business firm as a whole”* is easily associated with **Accounts**.

List of requirements (i.e., desirements) identified in the **White Paper** indicating a **Account Model**.  
Table 106:

Requirement	Statement	Comment
B0005	<b>Protect against criminal activity</b>	In this context, criminal activity is either Money Laundering or Fraud. Fraud is an intentionally deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim. Types of fraud include tax fraud, credit card fraud, wire fraud, securities fraud, and bankruptcy fraud. Fraudulent activity can be carried out by one individual, multiple individuals, or a business firm as a whole.
B0010	<b>Expand consumer access to the financial system</b>	A financial system is the entire set of non-cash-based institutions (i.e., banks, thrifts, insurance companies, stock exchanges, etc.) permitting and facilitating the exchange of funds. The expansion would entail adding people to these institutions
B0022	<b>Provide a CBDC that is:</b> 1. NOT Privacy-Protected 2. Intermediated 3. NOT Widely Transferable 4. Identity-Verified	Intermediated generally implies accounts or digital wallets. Identity-Verified generally implies validating and verifying a person's identity to gain access to their accounts
B0038	<b>Allow private-sector innovators to focus on:</b> 1. new access services 2. distribution methods 3. related service offerings	These innovations would predominately be account-based.
B0047	<b>Lower transaction costs</b>	Normally, there are no transaction costs for using cash
B0048	<b>Provide a secure way for people to save</b>	People save money in accounts unless we are offering piggy banks
B0049	<b>Promote access to credit</b>	Credit is, by definition, using cash you do not have access to.
B0051	<b>Generate data about users' financial transactions similar to the current Commercial Bank<sup>172)</sup> and Nonbank Money</b>	This kind of data is collected on the activity in accounts.
B0054	<b>Attract risk-averse users to CBDC</b>	Risk Averse investments usually pay little to no incentive to investors, but their value remains constant. Cash represents that kind of investment

<b>Requirement</b>	<b>Statement</b>	<b>Comment</b>
<b>P0002</b>	<b>Provide Yield benefits more effectively than alternative methods</b>	Cash generally offers no yield; therefore, this would require accounts
<b>P0005</b>	<b>Protect against criminal activity</b>	See: <b>B0005</b>
<b>P0012</b>	<b>The firms that operate interbank payment services are subject to federal supervision</b>	These services typically use accounts to move payments unless it is referring to armored guards and vehicles
<b>P0013</b>	<b>Systemically important payment firms are subject to</b> <b>1. heightened supervision</b> <b>2. regulation</b>	Refers to the accounting practices used by the payment firms
<b>P0017</b>	<b>The PWG report recommends CBDC complement existing authorities regarding</b> <b>1. market integrity</b> <b>2. investor protection</b> <b>3. illicit finance</b>	Refers to the accounting practices for CBDC accounts
<b>P0018</b>	<b>The Federal Reserve Act does not authorize direct Federal Reserve accounts for individuals</b>	Refers to accounts
<b>P0019</b>	<b>Federal Reserve accounts for individuals represent a significant expansion of the Federal Reserve's role in the financial system and the economy</b>	Refers to accounts
<b>P0020</b>	<b>The private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments</b>	Refers to accounts
<b>P0021</b>	<b>The intermediaries would operate in an open market for CBDC services</b>	Refers to accounts
<b>P0023</b>	<b>CBDC would need to be readily transferable between customers of different intermediaries</b>	Intermediaries imply accounts
<b>P0024</b>	<b>CBDC would need to comply with the U.S. robust rules</b>	Implies accounting and oversight rules
<b>P0025</b>	<b>CBDC intermediary would need to verify the identity of a person accessing CBDC</b>	Intermediaries imply accounts
<b>P0027</b>	<b>CBDC a risk-free asset</b>	See: <b>B0054</b>
<b>P0028</b>	<b>Require significant international coordination to address issues such as:</b> <b>1. common standards</b> <b>2. infrastructure,</b> <b>3. the types of intermediaries able to access any new infrastructure,</b> <b>4. legal frameworks</b> <b>5. preventing illicit transactions</b> <b>6. the cost and timing of implementation</b>	

Requirement	Statement	Comment
P0030	The Federal Reserve will only take further steps toward developing a CBDC if: 1. Research points to benefits for households, businesses, and the economy overall that exceed the downside risks 2. Indicates that CBDC is superior to alternative methods	See: B0054
R0002	Risk to the cost and availability of credit	See: B0054
R0009	Increased Risk of “runs” or other instabilities to the financial system	
R0012	Risk of increased concern related to the potential for: 1. destabilizing “runs” 2. disruptions in the payment system 3. concentration of economic power	See: B0054
R0013	CBDC offers no associated credit or liquidity Risk	See: B0054
R0015	Require mechanisms to reduce liquidity Risk	See: B0054
R0016	Require mechanisms to reduce credit Risk	See: B0054
R0020	Risk that interest-bearing CBDC could result in a shift away from other low-risk assets, such as shares in money market mutual funds, Treasury bills, and other short-term instruments.	See: B0054
R0023	Risk of financial panic causing outflows from Commercial Banks to CBDC without prudential supervision, government deposit insurance, and access to central bank liquidity	See: B0054
D0001	Design should be for a non-interest-bearing CBDC, for example, would be less attractive as a substitute for commercial bank money	Commercial bank money implies accounts
D0002	Design should allow the central bank to limit the amount of CBDC an end-user could hold	These restrictions imply accounts
D0003	Design should allow a limit on the amount of CBDC an end-user could accumulate over short periods	These restrictions imply accounts
D0005	Design could affect monetary policy implementation and interest rate control by altering the supply of reserves in the banking system	These restrictions imply accounts
D0008	Design should allow for interest-bearing at levels of the CBDC to be controlled independently of other safe assets	These restrictions imply accounts
D0010	Design should consider the potential for interest-bearing CBDC as a new policy tool on the channels of influence in monetary policy	These restrictions imply accounts

Requirement	Statement	Comment
<b>D0011</b>	<b>Design should generate data about users' financial transactions in the same ways that commercial bank and nonbank money generates data today</b>	These restrictions imply accounts
<b>D0012</b>	<b>Design should address privacy concerns by leveraging existing tools already in use by intermediaries</b>	These restrictions imply accounts
<b>D0013</b>	<b>Design should facilitate compliance with a robust set of rules already intended to combat</b> <b>1. money laundering</b> <b>2. the financing of terrorism</b> <b>3. customer due diligence</b> <b>4. record-keeping</b> <b>5. reporting requirements</b>	These restrictions imply accounts
<b>B = <a href="#">Benefit Considerations</a></b>		
<b>P = <a href="#">Policy Considerations</a></b>		
<b>R = <a href="#">Risk Considerations</a></b>		
<b>D = <a href="#">Design Considerations</a></b>		

## Stablecoin / Research

### [Return to Top](#)

The [White Paper](#) and summarized by the [Object Management Group's White Paper Analysis](#) provide some insight as to “what's next” with CBDC. The **White Paper** is not intended to advance a specific policy outcome and takes no position on the ultimate desirability of a U.S. CBDC [**P0008**]. Furthermore, the Federal Reserve will only take further steps toward developing a CBDC if [**P0030**]:

1. Research points to benefits for households, businesses, and the economy overall that exceed the downside risks
2. Indicates that CBDC is superior to alternative methods

In addition, the Federal Reserve does not intend to proceed with the issuance of a CBDC without explicit support from [**P0011**]:

1. the Executive Branch
2. Legislative Branch
3. ideally in the form of a specific authorizing law

The following topics are covered in the **White Paper**, which would require further research in order to garner broad public and cross-governmental support [**P0031**]:

**Note:** Also see: [4.3 Stablecoins](#) in context of Currency Models.

List of requirements (i.e., desirements) identified in the **White Paper** that require further research Table 107:

Requirement	Statement	Comment
<b>B0016</b>	<b>Provide Stablecoins that are:</b> <b>1. well-designed</b> <b>2. appropriately regulated</b>	Stablecoin is a specific solution
<b>B0017</b>	<b>Provide Stablecoins that are:</b> <b>1. faster</b> <b>2. more efficient</b> <b>3. more inclusive payment</b>	Stablecoin is a specific solution
<b>B0021</b>	<b>Maintain value by not using backing by an underlying asset</b>	<b>Conflict with B0017</b>
<b>P0015</b>	<b>The PWG report recommends that Congress act promptly to enact legislation that would ensure payment of Stablecoins</b>	Stablecoin is a specific solution
<b>P0016</b>	<b>The PWG report recommends payment Stablecoin arrangements are subject to a consistent and comprehensive federal regulatory framework</b>	Stablecoin is a specific solution
<b>R0010</b>	<b>CBDC has Risk of significant energy footprint similar to Cryptocurrencies</b>	Very different answers depending on CBDC mode, <b>Cash</b> rather than on <b>Accounts</b>
<b>R0017</b>	<b>Using private digital money could present Risks to both individual users and the financial system as a whole</b>	Requires Research
<b>R0019</b>	<b>Risk of reducing the aggregate amount of deposits in the banking system, which could in turn increase bank funding expenses, and reduce credit availability or raise credit costs for households and businesses.</b>	Requires Research
<b>R0020</b>	<b>Risk that interest-bearing CBDC could result in a shift away from other low-risk assets, such as shares in money market mutual funds, Treasury bills, and other short-term instruments.</b>	Requires research
<b>R0021</b>	<b>Risk of reducing credit availability or raising credit costs for businesses and governments</b>	Requires Research
<b>R0022</b>	<b>Risk of Stablecoins and other types of nonbank money shifting deposits away from banks even without a CBDC</b>	Stablecoin is a specific solution
<b>B = Benefit Considerations</b>		
<b>P = Policy Considerations</b>		
<b>R = Risk Considerations</b>		
<b>D = Design Considerations</b>		

169)

Internal Revenue Service, [Cash payment report helps government combat money laundering](https://www.irs.gov/newsroom/cash-payment-report-helps-government-combat-money-laundering), Accessed 2 March 2022,

<https://www.irs.gov/newsroom/cash-payment-report-helps-government-combat-money-laundering>

170)

Andrew Beattie, Investopedia, 21 August 2021, Accessed 2 March 2022,

<https://www.investopedia.com/articles/pf/08/pay-in-cash.asp>

171)



U.S. Currency Education Program. U.S. Currency in Circulation. Accessed 2 March 2022.

<https://www.uscurrency.gov/life-cycle/data/circulation>

172)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG)**  
**Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:dsn:q15:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:dsn:q15:start)

Last update: **2022/05/19 01:34**



# Question: 16. Should the amount of CBDC held by a single end user be subject to quantity limits?

[Return to Design Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**Should the amount of CBDC held by a single end-user be subject to quantity limits?**

## Answer

[Return to Top](#)

The answer depends on the architecture, design and implementation. (See: [4.0 Common Elements](#)).

1. If it is a replacement for cash: **NO**
2. If it is a replacement for a bank account or equivalent (i.e, savings, checking, investment, direct pay, credit, debit cards, etc. ): **YES**

**Note:** The answer is almost identical to [Question: 15. Should a CBDC pay interest? If so, why and how? If not, why not?](#)

## Overview

[Return to Top](#)

Before an answer can be provided about **CBDC quantity limits** for end-users, it is essential to clearly state the purpose and goals of the CBDC. The answer to [Question: 15. Should a CBDC pay interest? If so, why and how? If not, why not?](#) Sets the stage for this question, too. Basically, it depends on which model is used for the CBDC:

- **4.2.1 Digital Cash Model** - is a model representing the CBDC using cash (i.e., coins, \ \$1, \ \$2, \ \$5, \ \$10, \ \$20, \ \$50 and \ \$100 bills)) as the basis of the CBDC
- **4.2.2 Digital Account Model** - is a model that represents the CBDC in using digital accounts (i.e, Savings, Checking, Investment, Direct Pay, Credit Cards, Debit Cards, etc.)

## Example

[Return to Top](#)

There is only one requirement in the [White Paper](#) as identified by the identified by the [Object Management Group's](#) report called [White Paper Analysis](#):

Requirements identified in [White Paper Analysis](#) related to limiting CBDC quantity of CBDC for an End User.

Table 108:

Statement No.	Page No.	Statement
<b>D0003</b>	<b>18</b>	Design should allow a limit on the amount of CBDC an end user could accumulate over short periods

## Discussion of Example

[Return to Top](#)

### Digital Cash Model

[Return to Top](#)

The Digital Cash Model

List of requirements (i.e., desirements) identified in the **White Paper** indicating a Digital Cash Model.

Table 109:

Requirement	Statement	Comment
<b>D0003</b>	<b>Design should allow a limit on the amount of CBDC an end user could accumulate over short periods</b>	Digital Cash should be considered similarly as physical cash. It is impractical to have large amounts of physical cash. For security and safety, rarely does an End User hoard large amounts of physical cash. Using large amounts of cash to make purchases require time to count and validate the cash, and the same limits should be the same for Digital Cash.
<b>B</b> = <a href="#">Benefit Considerations</a>		
<b>P</b> = <a href="#">Policy Considerations</a>		
<b>R</b> = <a href="#">Risk Considerations</a>		
<b>D</b> = <a href="#">Design Considerations</a>		

### Digital Account Model

[Return to Top](#)

List of requirements (i.e., desirements) identified in the **White Paper** indicating a Digital Account

Model.

Table 110:

Requirement	Statement	Comment
<b>D0003</b>	<b>Design should allow a limit on the amount of CBDC an end user could accumulate over short periods</b>	Digital Accounts should be considered similar to current intermediary accounts (i.e., checking, savings, certificate of deposit, money market, etc.) held by End Users.
<b>B</b> = <a href="#">Benefit Considerations</a>		
<b>P</b> = <a href="#">Policy Considerations</a>		
<b>R</b> = <a href="#">Risk Considerations</a>		
<b>D</b> = <a href="#">Design Considerations</a>		

## Stablecoins

[Return to Top](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:dsn:q16:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:dsn:q16:start)

Last update: **2022/05/19 01:37**



# Question: 17. What types of firms should serve as intermediaries for CBDC? What should be the role and regulatory structure for these intermediaries?

[Return to Design Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

1. **What types of firms should serve as intermediaries for CBDC?**
2. **What should be the role and regulatory structure for these intermediaries?**

## Answer

[Return to Top](#)

The answer depends on:

- Currency Model(s) are adopted, see section [4.2 Currency Models](#))
- Architectural choices, see section [4.7 Dual Payment Networks](#)
- Design considerations, see section [4.3 Stablecoins](#)

## Currency Model Considerations

### Digital Cash Model

[Return to Top](#)

Using a [Digital Cash Model](#) it would be expected that all the existing Intermeidaires types continue to serve in their existing roles, however, these would have to be extended to support the new form of cash. There may need to be new intermediaries that exclusively use the new Digital Cash in ways yet to be determined but mostly like online services.

### What should be the role and regulatory structure for these intermediaries?

The regulatory structure should be the same as the current system for both the current Intermediaries types as well as any new Intermediaries types unless new laws and regulations are enacted to specifically exempt the CBDC from existing 60+ laws and regulations governing:

1. [National Privacy Considerations](#)
2. [National Security Considerations](#)
  - [Human Trafficking](#)
  - [Drug Trafficking](#)
  - [Corruption](#)
  - [Money Laundering](#)
3. [International Considerations](#)
  - [Data Residency](#)
  - [Data Sovereignty](#)
  - [Data Localization](#)

## Digital Account Model

[Return to Top](#)

Using a [Digital Account Model](#) it would be expected that all the existing Intermeidaires types continue to serve in their existing roles, however, these would have to be extended to support the new form of cash most likely offering the ability to keeps account balances denominated in either U.S. Dollars or in U.S. CBDC. The main benefit of using U.S. CBDC would be to use the CBDC Network to transfer money in near real-time versus using the traditional [Automated Clearing House \(ACH\) Network](#) .

### What should be the role and regulatory structure for these intermediaries?

The regulatory structure should be the same as the current system for both the current Intermediaries types as well as any new Intermediaries types unless new laws and regulations are enacted to specifically exempt the CBDC from existing 60+ laws and regulations governing:

1. [National Privacy Considerations](#)
2. [National Security Considerations](#)
  - [Human Trafficking](#)
  - [Drug Trafficking](#)
  - [Corruption](#)
  - [Money Laundering](#)
3. [International Considerations](#)
  - [Data Residency](#)
  - [Data Sovereignty](#)
  - [Data Localization](#)

## Dual Payment Model

[Return to Top](#)

Using a Dual Payment Network Model of [Automated Clearing House \(ACH\) Network](#) and a U.S.

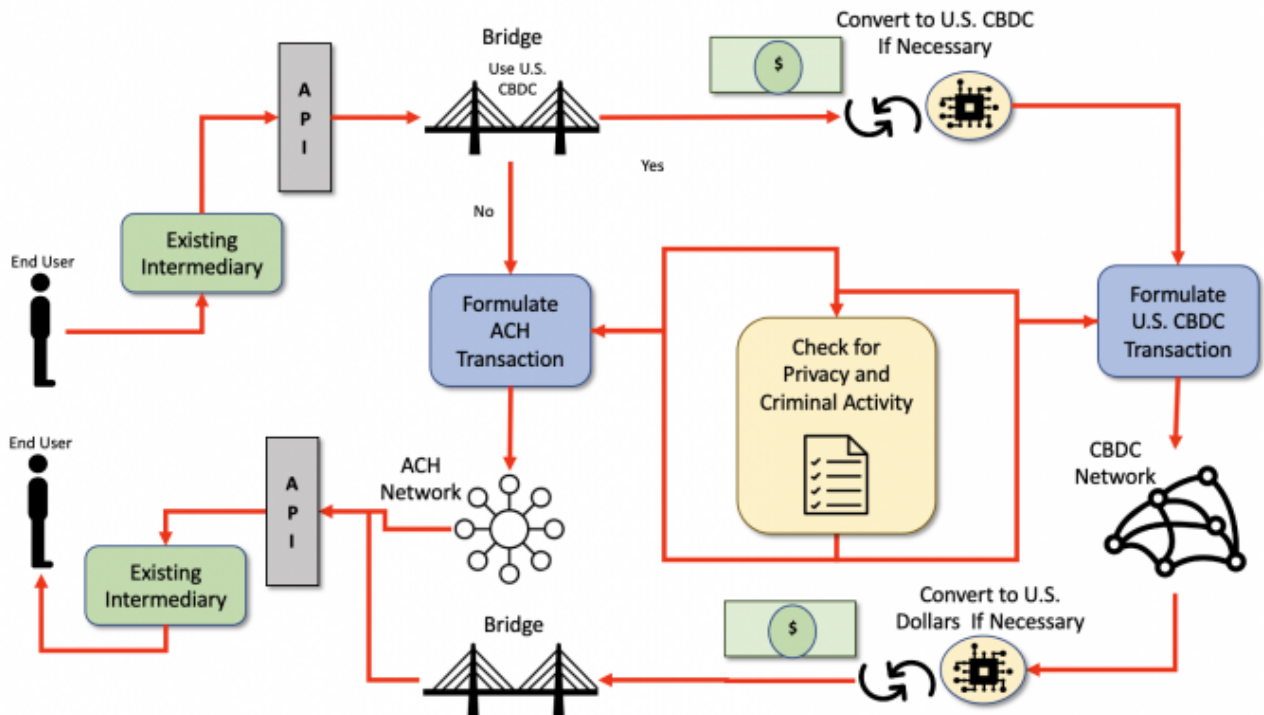
CBDC Network as described in Figure 33, the existing Intermediaries would continue to play a role, however, they would have to adapt their existing policies and procedures to allow for the use of both the U.S. Dollar based ACH and to support the use of the near real-time U.S. CBDC network while using CBDC.

**What should be the role and regulatory structure for these intermediaries?** The role and regulatory structure for these intermediaries would remain largely unchanged except for having to account for U.S. CBDC as part of the Banking Reserves.

The regulatory structure should be the same as the current system for both the current Intermediaries types as well as any new Intermediaries types unless new laws and regulations are enacted to specifically exempt the CBDC from existing 60+ laws and regulations governing:

1. National Privacy Considerations
2. National Security Considerations
  - Human Trafficking
  - Drug Trafficking
  - Corruption
  - Money Laundering
3. International Considerations
  - Data Residency
  - Data Sovereignty
  - Data Localization

There would also be a need for Intermediaries that exclusively use a new U.S. CBDC. These intermediaries would need to also participate in having Banking Reserves, be subject to auditing and follow all the existing Laws and Regulations such as, [Privacy](#), [Security](#), and [International Agreements](#)



Theoretical Very Simplified Dual ACH-CBDC Network Concept.

Figure 43:

## Design Considerations

[Return to Top](#)

A [Stablecoin](#) is a class of cryptocurrencies attempting to offer price stability by backing the Coins with a reserve asset, such as U.S. Dollars. Stablecoins have gained traction as they attempt to offer the best of both worlds—the instant processing and security or privacy of payments of cryptocurrencies, and the volatility-free stable valuations of fiat currencies.

The only Design Consideration presented in the **White Paper** are described in the Sections on [Stablecoin Examples](#) and in [Stablecoin Discussion of Examples](#) .

Section [4.3 Stablecoins](#) describes four types of Stablecoins with the **Fiat-Collateralized Stablecoins** as the most likely relevant to a U.S. CBDC. These are collateralized, or backed, by a [Fiat Currency](#) and are generally backed at a 1:1 ratio, meaning 1 Stablecoin is equal to 1 unit of currency. So for each Stablecoin that exists, there is (theoretically) one real Fiat Currency being held in a bank account to back it up.

Stablecoins could work with either [Digital Currency Model](#) (i.e., [Digital Cash Model](#) or the [Digital Account Model](#)). Regardless of which Digital Currency Model used, a Stablecoin Design will probably support all the existing Intermediaries as well as any new CBDC-only Intermediaries, especially if a [\[\[cbdc:public:cbdc\\_omg:04\\_doc:15\\_common:70\\_dualnets:start | Dual Payment Network](#) is adopted.

### What should be the role and regulatory structure for these intermediaries?

The regulatory structure should be the same as the current system for both the current Intermediaries types as well as any new Intermediaries types unless new laws and regulations are enacted to specifically exempt the CBDC from existing 60+ laws and regulations governing:

1. [National Privacy Considerations](#)
2. [National Security Considerations](#)
  - [Human Trafficking](#)
  - [Drug Trafficking](#)
  - [Corruption](#)
  - [Money Laundering](#)
3. [International Considerations](#)
  - [Data Residency](#)
  - [Data Sovereignty](#)
  - [Data Localization](#)



From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:dsn:q17:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:dsn:q17:start)

Last update: **2022/05/19 01:41**



# Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?

[Return to Design Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

1. **Should a CBDC have “offline” capabilities?**
2. **If so, how might that be achieved?**

## Answer

[Return to Top](#)

The answer is yes.

## Overview

[Return to Top](#)

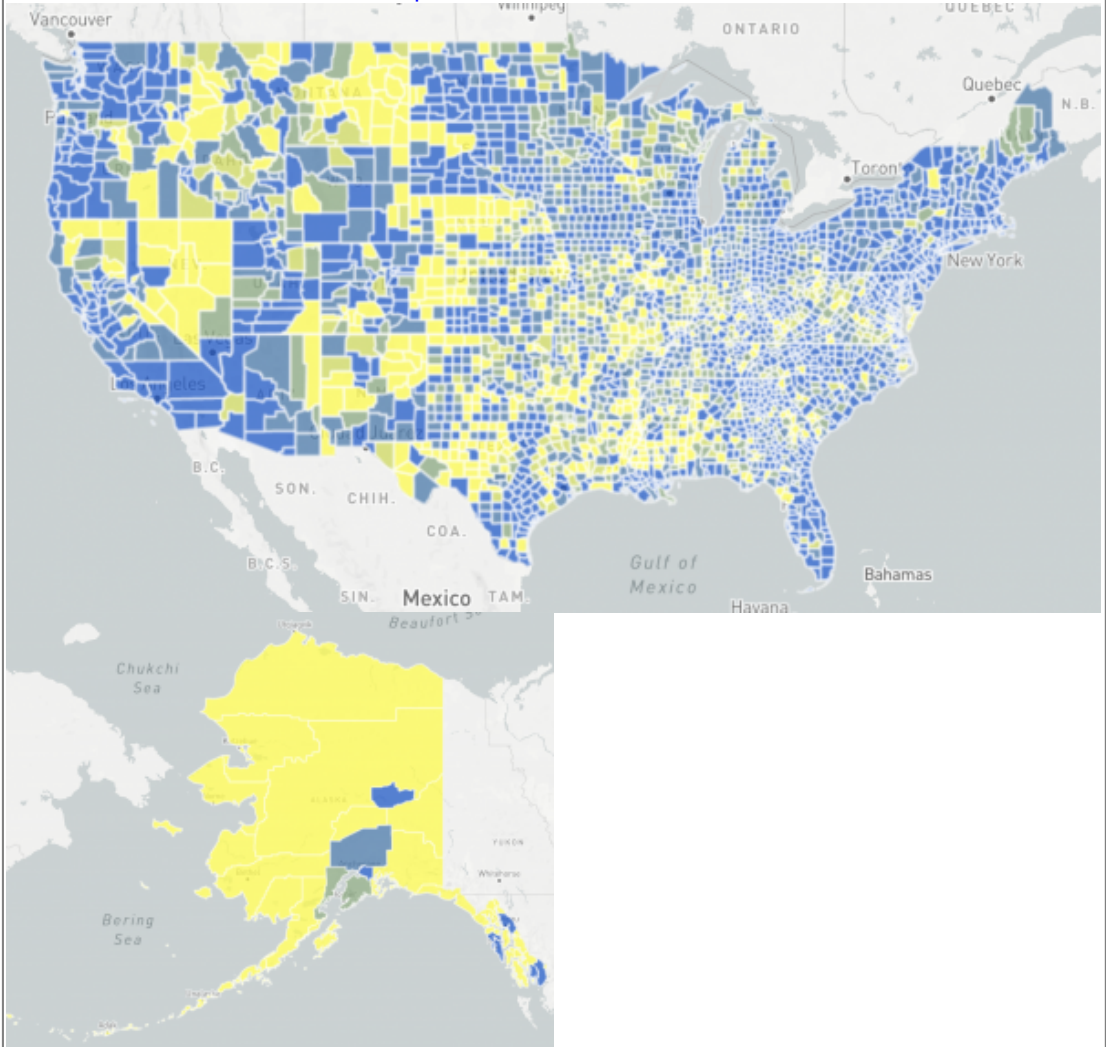
At the heart of this problem are [Disconnected, Intermittent, and Limited \(DIL\)](#) links.

*Disconnected, Intermittent, and Limited (DIL) occur in wireless/mobile networking environments, e.g. rural area networks, vehicular networks, battlefield networks, and other resource-constrained or disadvantaged networks. Efficient and effective [interoperability](#) in these networks are highly demanded various [mission-critical](#) systems and [application](#) scenarios such as disaster relief in ravaged regions, search and rescue in remote areas and military/tactical operations in hostile environments. ( [DIDO-RA](#) and [IEEE](#) )*

A DIL can occur whenever a network becomes unavailable. The definition of a DIL elaborates on three cases: disaster relief in ravaged regions, search and rescue in remote areas, and military/tactical operations in hostile environments. A fourth case, Network Outages is added to highlight just how fragile the reliance on networks can be.

Situations where Disconnected, Intermittent and Limited (DIL) occur and have an impact on CBDC. Table 111:

<b>Situation</b>	<b>Description</b>
<b>Disaster relief in ravaged regions</b>	<p data-bbox="415 163 1463 195"><a href="#">FEMA Led Historic Pandemic Response, Supported Record Number of Disasters in 2020</a></p> <ol style="list-style-type: none"> <li data-bbox="415 199 1500 289">1. FEMA responded to the most active Atlantic hurricane season in history. More than 5,000 FEMA employees deployed to support both Atlantic and Pacific hurricane responses in 2020.</li> <li data-bbox="415 294 1500 352">2. 2020 saw 30 record named storms, with the previous record of 27 named storms in the 2005 hurricane season. <ol style="list-style-type: none"> <li data-bbox="415 357 1463 420">a. Twelve of these storms made landfall in the U.S., surpassing the 1916 record of nine storms making landfall in the U.S.</li> <li data-bbox="415 424 1500 514">b. September 2020 set a record with 10 named storm formations. On Sept. 18, three Atlantic storms formed within six hours, which previously occurred only one other time in 1893.</li> </ol> </li> <li data-bbox="415 518 1081 550">3. Five of the named storms made landfall in Louisiana. <ol style="list-style-type: none"> <li data-bbox="415 554 1479 613">a. As of Jan. 4, 2021, FEMA has provided over \ \$245 million in grants and \ \$1.2 million in flood policy payments to survivors in Louisiana.</li> <li data-bbox="415 617 1500 676">b. FEMA also provided more than \ \$2.3 million in grants to governments and nonprofits to assist with response efforts and rebuild infrastructure.</li> </ol> </li> <li data-bbox="415 680 1463 739">4. FEMA responded to the most active West Coast wildfire season on record. More than 1,200 employees were deployed to support the response to western wildfires. <ol style="list-style-type: none"> <li data-bbox="415 743 1468 802">a. These included the largest wildfire in Colorado’s recorded history, the Cameron Peak fire, and five of the 10 largest fires in California’s history.</li> </ol> </li> <li data-bbox="415 806 1143 833">5. FEMA processed three major declarations due to wildfires.</li> </ol>

Situation	Description
<p data-bbox="191 762 378 856"><b>Search and rescue in remote areas</b></p>	<p data-bbox="410 163 1502 321">While the nation continues to make progress in broadband deployment, millions of Americans still lack access to adequate broadband, especially in rural areas and on Tribal lands. This baseline map visualizes broadband access at the county level and identifies connectivity gaps — the lighter the color, the lower the percentage of households with broadband access. <a href="#">Broadband Gaps in the USA</a></p>  <p data-bbox="410 1360 795 1392">Broadband coverage in the USA</p> <p data-bbox="410 1392 540 1423">Figure 44:</p> <p data-bbox="410 1423 979 1455"><b>Note:</b> This does not include “at sea” coverage</p>

Situation	Description
<b>Military/tactical operations in hostile environments</b>	<a href="#">Communication with submarines</a> is a field within military communications that presents technical challenges and requires specialized technology. Because radio waves do not travel well through good electrical conductors like saltwater, submerged submarines are cut off from radio communication with their command authorities at ordinary radio frequencies. Submarines can surface and raise an antenna above the sea level, then use ordinary radio transmissions, however, this makes them vulnerable to detection by anti-submarine warfare forces. Early submarines during World War II mostly traveled on the surface because of their limited underwater speed and endurance; they dived mainly to evade immediate threats. During the Cold War, however, nuclear-powered submarines were developed that could stay submerged for months. In the event of a nuclear war, submerged ballistic missile submarines have to be ordered quickly to launch their missiles. Transmitting messages to these submarines is an active area of research. Very low frequency (VLF) radio waves can penetrate seawater a few hundred feet (10–40 meters), and many navies use powerful shore VLF transmitters for submarine communications. A few nations have built transmitters that use extremely low frequency (ELF) radio waves, which can penetrate seawater to reach submarines at operating depths, but these require huge antennas. Other techniques that have been used include sonar and blue lasers.
<b>Network Outages</b>	Wikipedia has identified 19 major internet outages ( see <a href="#">Table 111</a> that have occurred because of hardware or cabling, internet infrastructure, cyber-attacks, government censorship, and server overloads.

Many of these problems create a situation often referred to as the [Two Generals Problem](#) which for the most part is unsolvable. However, if each general can work independently of the other (i.e., disconnected or offline), then the number of occurrences of the **Two Generals Problem** is reduced.

**Note:** The Two Generals is related to, but distinct from [Byzantine General Problem](#). The Two Generals problem is about the weakness in the connectivity between the Generals. The Byzantine General Problem is about the weakness of a General.

List of [Internet outages](#) provided by Wikipedia.

Table 111:

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
16 Jul 1997	DNS TLD Outage	Worldwide		50,000,000	An Ingress database failure resulted in corrupt .com and .net zones, which were subsequently released to the DNS root servers. As the root servers were reloaded, they began to return failures for all domains in the .com and .net zones.	4 hours	DNS	Automation and Human Failure	InterNIC / Network Solutions	All .com and .net domains

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2008	2008 submarine cable disruption	Middle East and the Mediterranean Sea			Three separate incidents of major damage to submarine optical communication cables around the world occurred in 2008. The first incident caused damage involving up to five high-speed Internet submarine communications cables in the Mediterranean Sea and the Middle East from 23 January to 4 February 2008, causing internet disruptions and slowdowns for users in the Middle East and India. In late February there was another outage, this time affecting a fiber optic connection between Singapore and Jakarta. On 19 December, FLAG FEA, GO-1, SEA-ME-WE 3, and SEA-ME-WE 4 were all cut.		submarine cables	Unknown	Unknown	
2011	2011 submarine cable disruption	South Asia and the Middle East			Two incidents of submarine communications cables cut off on 25 December 2011. The first cut-off occurred to SEA-ME-WE 3 at Suez Canal, Egypt and the second cut-off occurred to i2i which took place between Chennai, India, and Singapore line. Both the incidents had caused Internet disruptions and slowdowns for users in South Asia and the Middle East in particular UAE.		submarine cables	Unknown	Unknown	
2011		Armenia		3,000,000	A woman digging for scrap metal damaged land cables and thereby severed most connectivity for the nation of Armenia.	5 hours	land cables	digging		Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2011		Egypt			The Internet in Egypt was shut down by the government, whereby approximately 93% of networks were without access in 2011 in an attempt to stop mobilization for anti-government protests.		ISPs	government censorship	Egypt	Full
2012		2012 Syrian internet outage	Syria		On 29 November 2012, the Syrian Internet was cut off from the rest of the world. The autonomous system (AS29386) of the Syrian Telecommunication Establishment (STE) was cut off completely at 10:26 UTC. Five prefixes were reported to have remained up, this is why Dyn reports an outage in 92% of the country. Responsibility for the outage has somewhat speculatively been blamed on various organizations.			Unknown	Unknown	
2016		Germany	Deutsche Telekom	900,000	At the end of November 2016 0.9 million routers, from Deutsche Telekom and produced by Arcadyan, were crashed due to failed TR-064 exploitation attempts by a variant of Mirai, which resulted in Internet connectivity problems for the users of these devices. While TalkTalk later patched their routers, a new variant of Mirai was discovered in TalkTalk routers.	1 day	Internet routers	cyberattack	Unknown	Full
2016		Liberia		Unknown	Mirai has also been used in an attack on Liberia's Internet infrastructure in November 2016.			cyberattack	Unknown	Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2016	DDoS attack on Dyn	United States	Dyn (company)		The cyberattack took place on October 21, 2016, and involved multiple distributed denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn, which caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America. As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name—when, for instance, entered into a web browser—to its corresponding IP address. The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses. The activities are believed to have been executed through a botnet consisting of a large number of Internet-connected devices—such as printers, IP cameras, residential gateways and baby monitors—that had been infected with the Mirai malware. With an estimated throughput of 1.2 terabits per second, the attack is, according to experts, the largest DDoS attack on record.	1 day	Domain Name System (DNS) provider	cyberattack	Unknown	Major websites



Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2017		Cameroon	South-West and North-West of Cameroon	20% of the country's population	On January 17, around 20 percent of the people in Cameroon had their Internet blocked due to recent anti-government protests.	270 days or 8 months		government censorship	Cameroon	Full
2017		North Korea			On October 1, The autonomous system (AS131279) of Star JV was cut off completely, due to alleged US cyber attack	9 hours and 31 minutes		cyberattack	United States	Full
2019	Verizon and BGP Optimizer	United States	Verizon (company)		On June 24, 2019, many parts of the Internet faced an unprecedented outage as Verizon, the popular Internet transit provider accidentally rerouted IP packages after it wrongly accepted a network misconfiguration from a small ISP in Pennsylvania, USA. According to The Register, systems around the planet were automatically updated, and connections destined for Facebook, Cloudflare, and others, ended up going through DQE and Allegheny, which buckled under the strain, causing traffic to disappear into a black hole.	3 hours	Internet transit provider	misconfiguration	Unknown	Major websites
2019	Iranian internet shutdown	Iran			The Internet in Iran was shut down by the government, whereby approximately 96% of networks were without access in an attempt to stop mobilization for anti-government protests.	7 days	ISPs	government censorship	Iran	Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2019	Internet shutdown in India	India		50,000,000	The Government of India passed the Citizenship Amendment Act, 2019 which caused huge controversy and mass protest in various parts of India. In order to prevent protests and outrage on social media, various state governments including those of Assam, Tripura, Meghalaya, Arunachal Pradesh, West Bengal, and Uttar Pradesh decided to shut down internet access.	Up to 9 days Over one year (Kashmir)		government censorship	Various State governments of India	Full
2019	2019 Burmese internet shutdown	Myanmar			On June 21, the Internet in Burma was shut down by the government. The Burmese government shut down the internet connection in nine townships of the northern Arakan State and one single township in the Southern Chin State, which was proposed by Burmese Military officers. The shutdown is ongoing and has become the world's longest internet shutdown.			Government censorship	Burma	Full
2019	2019 Papua protests	Indonesia			To curb the escalating protests that occurred in the Indonesian provinces of Papua and West Papua, the Indonesian authority imposed an internet blackout on both provinces on 21 August 2019. The blackout continues until the authority partially lift the blackout on 4 September in several regions, with the complete lifting of the restriction only occurring on 9 September.	19 days		Government censorship	Indonesia	Full

Year	Name	Country or region	Affected users	Number of affected users (rough)	Description	Duration (rough)	Internet component	Cause	Entity responsible	Type
2021		North Korea			On October 21st, North Korean internet infrastructure dropped off the internet, including public-facing websites and email servers. All servers which were subject to monitoring were found to be offline.	At least 14 minutes		Unknown	Unknown	
2021	Facebook Outage	Worldwide	LAN Internet Connection	2,850,000,000	On October 4, 2021, at around 11:45 AM EST, the online social media site Facebook went down, as well as Facebook subsidiaries including Instagram and Whatsapp. Around 4:00 PM EST, people reported other sites were not working via Downdetector, including Gmail and Twitter, the latter possibly caused by Facebook users reporting the outage. The outage came less than a day after a whistleblower had been on 60 Minutes. For a short period of time, no Facebook employee could access the building to investigate the issue due to their "keycards not working.". At around 6:30 PM EST, Facebook reported that all their sites were up. Facebook CEO Mark Zuckerberg lost around \ \$7B dollars after the outage. For more info, see 2021 Facebook outage	7 hours	LAN connection	BGP Withdrawal of IP Address (Facebook), Server overwhelming (other sites)	Unknown	Major websites
2022	2022 Kazakhstan internet shutdown	Kazakhstan			On 4 January 2022 the Internet in Kazakhstan was shut down on account of anti-government protests against sudden energy price rises.[75]	5 days		Government censorship	Kazakhstan	mobile internet

## Examples

[Return to Top](#)

Some of these [Disconnected, Intermittent and Limited \(DIL\)](#) requirements were alluded to in the White Paper, but not directly specified or defined. The Table 112 provides an example of cross-referencing the DIL Requirements to the Benefits, Policy Considerations, Risks and Design requirements identified in the [White Paper Analysis](#) done by the [Object Management Group](#) .

Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG

Table 112:

Topic	Requirements
<b>Disaster relief in ravaged regions</b>	B: B0008, B0010, B0013, B0014, B0024, B0030, B0035, B0036, B0039, B0040, B0043, B0044, B0053 P: P0023, P0026 R: R0011 D: D0016, D0017
<b>Search and rescue in remote areas</b>	D: D0016, D0017
<b>Military/tactical operations in hostile environments</b>	B: B0013, B0018, B0030, B0024, D: D0016, D0017, B0030
<b>Network Outages</b>	B: B0018, B0030, B0024 D: D0016, D0017
B = <a href="#">Benefit Considerations</a>	
P = <a href="#">Policy Considerations</a>	
R = <a href="#">Risk Considerations</a>	
D = <a href="#">Design Considerations</a>	

## Discussion of Example

[Return to Top](#)

The benefit specified **B0030** and the design specified **D0017**:

<b>B0030</b>	<b>14</b>	Support benefit payments directly to citizens
<b>B0039</b>	<b>15</b>	Provide a programmable CBDC to deliver payments at certain times
<b>D0017</b>	<b>20</b>	Design should include digital payments in areas suffering from large disruption, such as natural disasters
B = <a href="#">Benefit Considerations</a>		
P = <a href="#">Policy Considerations</a>		
R = <a href="#">Risk Considerations</a>		
D = <a href="#">Design Considerations</a>		

Both of these can be mapped to **Disaster relief in ravaged regions**. When a disaster occurs **D0017**, the US government can provide disaster relief through the Federal Emergency

Management Agency (FEMA). The relief is often in the form of loans with payments, generally made through the US Small Business Administration (SBA). The [assistance loans](#) can be for businesses of all sizes, homeowners, and renters. CBDC needs to provide the payments directly to the recipients (i.e., **B0030** of the loans since many of the physical facilities of the existing financial institutions have also been damaged).

In addition, FEMA can offer assistance for Temporary Housing Assistance, Lodging Expenses Reimbursement<sup>173)</sup>, which are recurring expenses. **B0039** would allow these payments to be made on a schedule and perhaps be made directly to the landlords or programmed to allow recipients to transfer the money to the landlord but nowhere else.

When access to the Internet becomes a [Disconnected, Intermittent and Limited \(DIL\)](#), often a [Peer-to-Peer \(P2P\)](#) network can be very effective, especially when other [Network Platforms](#) are used instead of just [Ethernet](#) with nodes connected over [Local Area Network \(LAN\)](#) and/or a [Wide Area Network \(WAN\)](#) using a [Traditional Network Device](#). For example:

- [Bluetooth](#)
- [Zigbee](#)
- [Near-Field-Communication \(NFC\)](#)

Consequently, it is important to identify the kinds of connections that are required to support the CBDC. Some examples are:

- Many contactless payments systems use [Radio Frequency Identification \(RFID\)](#) and NFC
- Many supply chains use RFID
- Many smart home efforts use WiFi and Zigbee
- Many automobiles use Bluetooth to connect phones, make queries, play music, etc.

Another alternative is to establish a [Wireless Fidelity \(Wi-Fi\)](#) LAN that has no or very limited access to the Internet but can be used to connect local devices together.

Regardless of how the CBDC nodes connect, the information that flows between the nodes must be secure (See: [OMG DIDO-RA Secure Messaging](#) for a set of Technical and \de Facto Standards for secure messaging).

The [OMG DIDO-RA](#) provides a detailed discussion on [Networks](#), and we recommend that this be used when formulating further requirements for the CBDC. Some topics covered in the [OMG DIDO-RA](#) are:

- [Secure Messaging](#)
- [Transport](#)
- [Security](#)
- [Protocol](#)
- [Distribution Software](#)

<sup>173)</sup>

<https://www.fema.gov/assistance/individual/housing>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:dsn:q18:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:dsn:q18:start)

Last update: **2022/05/18 21:38**



# Question: 19. Should a CBDC be designed to maximize ease of use and acceptance at the point of sale? If so, how?

[Return to Design Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

1. **Should a CBDC be designed to maximize ease of use and acceptance at the point of sale?**
2. **If so, how?**

## Answer

[Return to Top](#)

By using a system designed roughly as outlined in section [4.7 Dual Payment Networks](#), much of the current infrastructure would remain in place and the **ease of use and acceptance at the point of sale** would be very little different than the current system since the End User Front End would be done by existing Intermediaries or newly specialized U.S. CBDC Intermediaries.

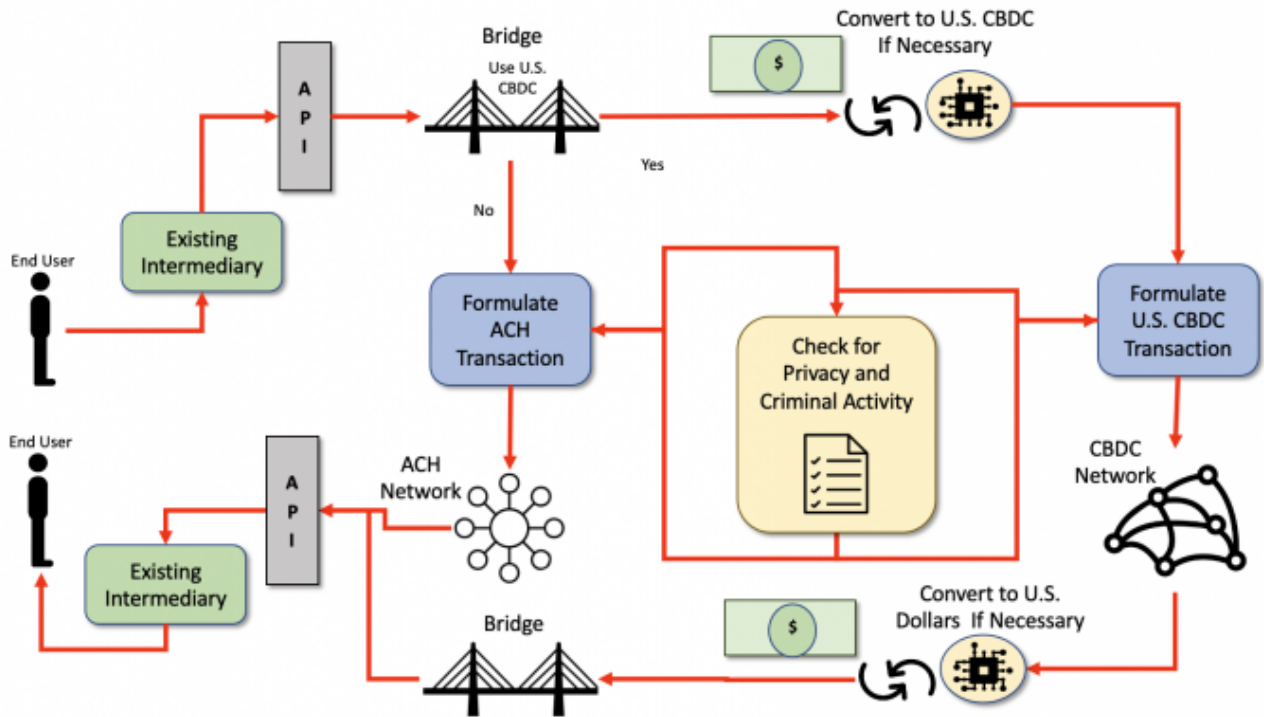
Table [113](#) provides the system components of a very simplified, theoretic ACH / CBDC network. Figure [43](#) graphically shows a theoretical, very simplified, dual ACH-CBDC Network Concept.

Theoretical components of a Dual ACH / CBDC System

Table 113:

- Development of a U.S. CBDC is probably based on Stablecoin Model.
- Use of an energy-efficient [Consensus Algorithm](#)
- Development of a **bridge** between the existing [Automated Clearing House \(ACH\) Network](#) and the new U.S. CBDC Network
- Development of a new standardized [Application Programming Interface \(API\)](#) to connect the outside world to the newly enhanced combined ACH Network and CBDC Network for the existing intermediaries to use for transfers

**Note:** The [API](#) could be in the form of [Web Services](#), [Remote Procedure Calls \(RPC\)](#), [Common Object Request Broker Architecture \(CORBA\)](#), [Data Distribution Service \(DDS\)](#) or other interprocess communication mechanisms defined using [ISO/OMG Interface Definition Language \(IDL\)](#), [standardized Web Services Interface Language \(WSDL\)](#), etc.



Theoretical Very Simplified Dual ACH-CBDC Network Concept.  
Figure 45:

## Examples

[Return to Top](#)

The “desirements” specified in [White Paper](#) and identified by the [OMG's White Paper Analysis](#) as **ease of use and acceptance at the point of sale** are listed in Table 114.

Examples of **ease of use and acceptance at the point of sale** identified during the White Paper Analysis conducted by the OMG

Table 114:

Category	Desirements
Benefits	B0003, B0007, B0009, B0011, B0012, B0013
Policies and Considerations	
Risks	R0007
Design	

**Note:** B = Benefit, P = Policy, R = Requirement, D = Design.

## Discussion of Examples

[Return to Top](#)



Table 115 provides discussion points for each of the “desirements” identified by the [OMG's White Paper Analysis](#) which apply to **ease of use and acceptance at the point of sale**.

Table 115:

<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>B0003</b>	<b>Complement, rather than replace, current forms of money and methods for providing financial services</b>	The proposed Dual ACH/CBDC networks would do exactly that. The existing Intermediaries would be allowed to expand their services to include U.S. CBDC by basically making it a consumer choice.
<b>B0007</b>	<b>Provide households and businesses a convenient and electronic form of central bank money with:</b> <b>1. safety</b> <b>2. liquidity</b>	In all accounts, U.S. money could be kept as U.S. Dollars or as U.S. CBDC. Since the U.S. CBDC would probably be backed by a U.S. Dollar Stablecoin, there should be no advantage or disadvantage to either. The main difference is the End User's choice to use the real-time CBDC or the existing ACH Network. Note: There may be a cost associated with converting between the two currencies.
<b>B0009</b>	<b>Provide faster and cheaper payments (including cross-border payments)</b>	If the U.S. CBDC network is selected by the End User, the transactions will most likely be faster but not necessarily cheaper. There is a cost associated with using the <a href="#">Consensus facilities</a> of the U.S. CBDC as well as the possibility of costs associated with converting U.S. Dollars to U.S. CBDC.
<b>B0011</b>	<b>Make payments:</b> <b>1. faster</b> <b>2. cheaper</b> <b>3. more convenient</b> <b>4. more accessible</b>	Using the Dual Network, the End User can decide how fast they want the payments to be made. The cost of using a U.S. CBDC is still unknown. There is a cost associated with using the <a href="#">Consensus facilities</a> of the U.S. CBDC as well as the possibility of costs associated with converting U.S. Dollars to U.S. CBDC. It is up to the free market and the entrepreneurs to make it more convenient and accessible.
<b>B0013</b>	<b>Provide immediate access to transferred funds</b>	If an End User chooses to use the U.S. CBDC network, the funds will be available as fast as the U.S. CBDC infrastructure permits. Usually within minutes. See <a href="#">Consensus Algorithms</a> for more information.
<b>R0007</b>	<b>Risk CBDC is difficult to use without service providers</b>	At a minimum, the existing Intermediaries would be able to use most of their existing infrastructure to use the U.S. CBDC. In the Workflow for creating a payment transaction: 1. Need to ask if it is going to use a CBDC transfer. a. If yes, they need to make sure the End Users account has the correct amount of CBDC Stablecoins i. If not, they need to convert U.S. Dollars to U.S. CBDC Stablecoins ii. formulate a standardized U.S. CBDC transaction and all the required data b. If not, do ACH Network business as usual
<b>B = <a href="#">Benefit Considerations</a></b>		

<b>Desirement No.</b>	<b>Desirement Text</b>	<b>Comment</b>
<b>P</b>	= Policy Considerations	
<b>R</b>	= Risk Considerations	
<b>D</b>	= Design Considerations	

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:20\\_comments:dsn:q19:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:20_comments:dsn:q19:start)

Last update: **2022/05/19 01:43**



# Question: 20. How could a CBDC be designed to achieve transferability across multiple payment platforms? Would new technology or technical standards be needed?

[Return to Design Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

- **How could a CBDC be designed to achieve transferability across multiple payment platforms?**
- **Would new technology or technical standards be needed?**

## Answer

[Return to Top](#)

By using a system designed roughly as outlined in section [4.7 Dual Payment Networks](#), much of the current infrastructure would remain in place and to **achieve transferability across multiple payment platforms** would be very little different than the current system.

Table [113](#) provides the system components of a very simplified, theoretic ACH / CBDC network. Figure [45](#) graphically shows a theoretical, very simplified, dual ACH-CBDC Network Concept. A newly developed Application Programming Interface (API) and a specialized bridge going between the existing ACH Network and the new U.S. CBDC network would allow the existing platforms to work fairly seamlessly.

The existing Intermediaries would have time to adopt and adapt to the new API and use a “stubbed out” bridge as a first step toward the support of the U.S. CBDC in the future. The API and “stubbed out” bridge would connect to the existing ACH Network. As the CBDC network comes online, the existing Intermediaries would be able to join. This would allow a phased roadmap for the transition. New Intermediaries would start using the new API and the new U.S. CBDC network when it becomes available.

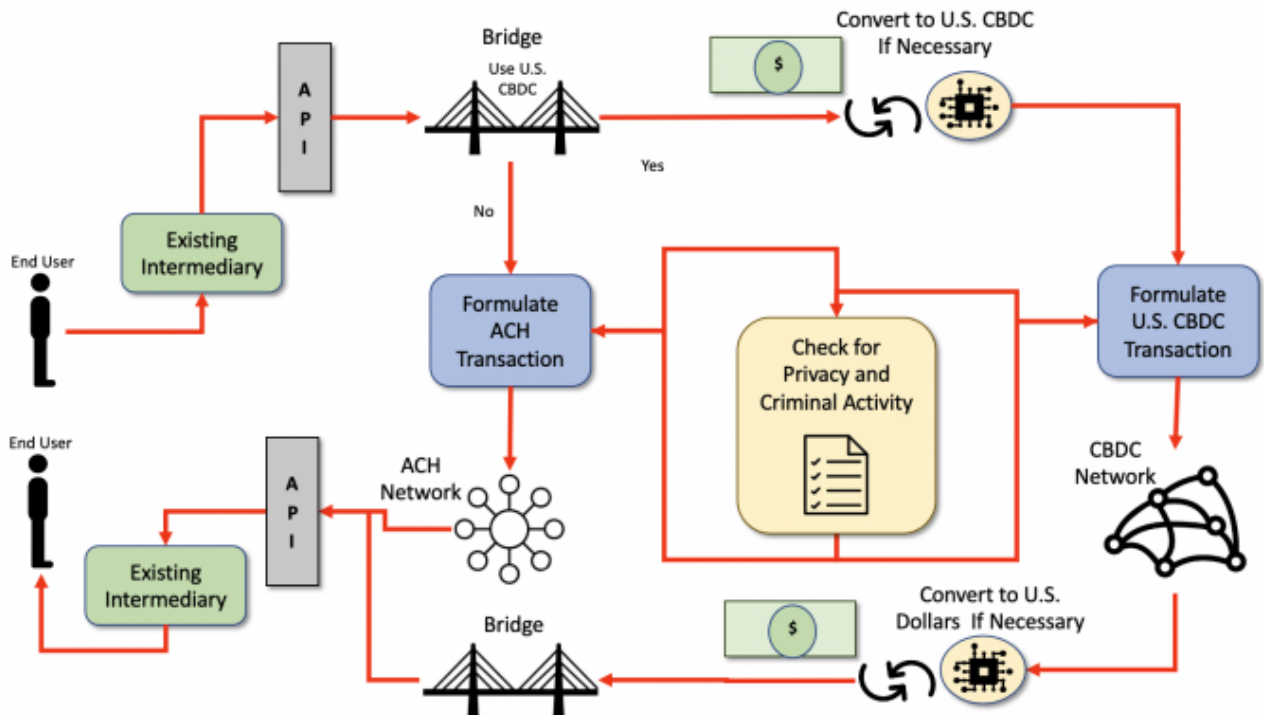
Theoretical components of a Dual ACH / CBDC System

Table 116:

- Development of a U.S. CBDC is probably based on Stablecoin Model.
- Use of an energy-efficient [Consensus Algorithm](#)

- Development of a **bridge** between the existing [Automated Clearing House \(ACH\) Network](#) and the new U.S. CBDC Network
- Development of a new standardized [Application Programming Interface \(API\)](#) to connect the outside world to the newly enhanced combined ACH Network and CBDC Network for the existing intermediaries to use for transfers

**Note:** The [API](#) could be in the form of [Web Services](#), [Remote Procedure Calls \(RPC\)](#), [Common Object Request Broker Architecture \(CORBA\)](#), [Data Distribution Service \(DDS\)](#) or other interprocess communication mechanisms defined using [ISO/OMG Interface Definition Language \(IDL\)](#), [standardized Web Services Interface Language \(WSDL\)](#), etc.



Theoretical Very Simplified Dual ACH-CBDC Network Concept.  
Figure 46:

## Examples

[Return to Top](#)

The “desirements” specified in [White Paper](#) and identified by the [OMG's White Paper Analysis](#) as **achieving transferability across multiple payment platforms** are listed in Table 117.

Examples of **achieving transferability across multiple payment platforms** identified during the White Paper Analysis conducted by the OMG

Table 117:

Category	Desirements
Benefits	B0026, B0045, B0046
Policies and Considerations	P0021

Category	Desirements
Risks	
Design	D0015

**Note:** **B** = Benefit, **P** = Policy, **R** = Requirement, **D** = Design.

## Discussion of Examples

[Return to Top](#)

Table 115 provides discussion points for each of the “desirements” identified by the [OMG's White Paper Analysis](#) which apply to **achieving transferability across multiple payment platforms**.

Table 118:

Desirement No.	Desirement Text	Comment
<b>B0026</b>	<b>Provide a bridge between legacy and new payment services</b>	The Dual ACH Network and U.S. CBDC Networks presented provides a bridge between the two networks. In order to be used effectively, the use of a standardized <a href="#">Application Programmer Interface (API)</a> is also recommended. <b>Note:</b> The <a href="#">API</a> could be in the form of Web Services, Remote Procedure Calls (RPC), <a href="#">Common Object Request Broker Architecture (CORBA)</a> , <a href="#">Data Distribution Service (DDS)</a> or other interprocess communication mechanisms defined using <a href="#">ISO/OMG Interface Definition Language (IDL)</a> , <a href="#">standardized Web Services Interface Language (WSDL)</a> , etc.
<b>B0045</b>	<b>Enable rapid and cost-effective payment of taxes</b>	The Internal Revenue Service (IRS) would be required to support the ACH/CBDC API and Bridge to make this happen. It is beyond the control of the Federal Reserve.
<b>B0046</b>	<b>Enable rapid and cost-effective delivery of:</b> <b>1. wages,</b> <b>2. tax refunds</b> <b>3. other federal payments</b>	This would require the employers, the U.S. Benefits agencies, and the Internal Revenue Service (IRS) to support the ACH/CBDC API and Bridge to make this happen.

Desirement No.	Desirement Text	Comment
P0021	<b>The intermediaries would operate in an open market for CBDC services</b>	<p>Currently, the Intermediaries operate in an open market that is confined by the Laws and Regulations of the U.S. and Foreign governments when applicable.</p> <p>The proposed Dual ACH/CBDC networks would allow the existing Intermediaries to participate in the CBDC services as long as they are compliant with the standardized <a href="#">Application Programmer Interface (API)</a> and Bridge.</p> <p>The proposed Dual ACH/CBDC networks would also allow new Intermediaries to only offer CBDC services.</p>
P0023	<b>CBDC would need to be readily transferable between customers of different intermediaries</b>	<p>As long as the Intermediaries use the standardized <a href="#">Application Programmer Interface (API)</a> and Bridge, all transfers between Intermediaries is possible.</p>
D0015	<b>Design should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks</b>	<p>The Dual ACH/CBDC Networks would require the new infrastructure for the <a href="#">Application Programmer Interface (API)</a>, the bridges, and the building out of a Distributed Network of Nodes to handle the CBDC transactions and <a href="#">Consensus</a>. The network of nodes might have any number of node types. Figure 21 describes the taxonomy of DIDO Node Types. See <a href="#">OMG DID-RA Node Taxonomy</a> for a discussion on the different kinds of nodes.</p>
<p><b>B</b> = <a href="#">Benefit Considerations</a></p>		
<p><b>P</b> = <a href="#">Policy Considerations</a></p>		
<p><b>R</b> = <a href="#">Risk Considerations</a></p>		
<p><b>D</b> = <a href="#">Design Considerations</a></p>		

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:dsn:q20:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:dsn:q20:start)

Last update: **2022/05/19 01:44**



# Question: 21. How might future technological innovations affect design and policy choices related to CBDC?

[Return to Design Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

**How might future technological innovations affect design and policy choices related to CBDC?**

## Answer

[Return to Top](#)

### Quantum Computing

[Return to Top](#)

One of the riskiest predictions for the U.S. CBDC is the advent of a real [Quantum Computing](#). These machines are not mature at the present but will be able to “crack” most of the existing encrypted data when it happens. This kind of power will render most “private” as “clear text” and reveal all the secrets hidden within (i.e., private communications, company data, government data, and military classified data). In addition, most of the currently encrypted digital signatures are vulnerable to “cracking”. Therefore, although most encrypted data currently stored in public datastores (i.e. blockchains, distributed ledgers, Directed Acyclical Graphs (DAGs) ) may become vulnerable in the future. That is why it is important for a U.S. CBDC only encrypt data in public ledgers that have a shelf life (i.e., it only needs to be kept private for a short period of time).

*Quantum-safe encryption will come into your life through upgraded laptops, phones, web browsers, and other products. But most of the burden for quantum-safe encryption rests on the shoulders of businesses, governments, and cloud computing services that must design and install the technology. It's an extraordinarily complex change that's on par with fixing Y2K bugs or upgrading internet communications from IPv4 to IPv6.<sup>173)</sup>*

While quantum computers will have an impact on the current [Advanced Encryption Standard \(AES\)](#) encrypted data, it does not mean they will break it.

*We [NIST] believe that AES will be secure for decades at least — with the caveat that new research discoveries could change this view. It is generally agreed that doubling the key length will suffice to provide the same level of security as in the pre-quantum era. Thus, a user who is using AES-128 could **switch to AES-256 to ensure the same level of security**.*<sup>174)</sup>

## Overly Simplistic Blockchain Technology

### [Return to Top](#)

The current set of [DIDO Platforms](#) (i.e. [Ethereum](#), [Hyperledger](#), [Iota](#), [Hedera](#), etc.) are very simplistic, even though they have made great strides since their inception. It is much like the early days of databases when all the data were stored in a single hierarchy. As the [Databases](#) evolved, they became more sophisticated moving toward [DataBase Management System \(DBMS\)](#). Some examples of DBMSs are:

- [Relational DataBase Management Systems \(RDBMSs\)](#) with tables, relationships, indexes, triggers, and stored procedures
- [Graph DataBase \(GDB\)](#) with nodes, edges, properties
- [Object-Oriented Database \(OOD\)](#) , with objects, classes, and inheritance

For example, DIDO Platforms currently are very good at building “accounts” and keeping tallies on the accounts (i.e. account ledgers). However, this is basically just bookkeeping. Granted, bookkeeping is a cornerstone of the financial systems, but there is so much more which requires far more sophistication.

*Bookkeeping is a transactional and administrative role that handles the day-to-day tasks of recording financial transactions, including purchases, receipts, sales, and payments. Accounting is more subjective, providing business owners with financial insights based on information gleaned from their bookkeeping data.*<sup>175)</sup>

Accounting focuses on the day-to-day flow of money in and out of accounts which DIDO Platform can do when used as a bookkeeper. However, Accounting has far more rules that are not done within the current DIDO Platforms. See [Generally Accepted Accounting Principles \(GAAP\)](#).

Individuals, corporations, and institutions accounting systems are far more complex than a simple account or even accounting. They may have hundreds if not thousands of accounts that need to be managed. The management of the accounts not only includes a tally of money in each account but its color (the different categories of money and the specific uses on which those funds may be spent). There are usually strict laws, regulations, or even accounting rules which prevent money from being [comingled](#) in the accounts. The current DIDO Platforms are basically only keeping the tallies on accounts and leaving the enforcement of laws, regulations, and rules to the individuals that have control over the account.

For example, if a University collects tuition, there may be rules on the tuition money that may allow it to be spent only on educators, staff, and supplies directly tied to the teaching of the students.



Finance, a broader term than accounting, is the management of assets and liabilities and the planning of future growth. It also implies the adherence to Laws and Regulations. See the following sections:

- [4.4 National Privacy Considerations](#)
- [4.5 National Security Considerations](#)
- [4.6 International Considerations](#)

The next generations of DIDO Platforms will most likely be more sophisticated and cover concepts such as:

1. More of a Systems or [System-of-Systems \(SoS\)](#) approach 2. Better Business Process mechanisms that use high-level languages rather than simple procedural programming languages such as [Solidity](#). Some examples are:

- [Visual Programming Language \(VPL\)](#)
- [Business Process Modeling Notation \(BPMN\)](#)

3. Better formalism of data sources inside and outside the blockchain including other blockchains.

4. More sophisticated constructs for the relationships between the data

- Association
- Directed Association
- Reflexive Association
- Multiplicity
- Aggregation
- Composition
- Inheritance/Generalization
- Realization

5. Snapshotting 6. More sophisticated event processing and handling based on things like time, geographic location, the quantity of transfer, etc 7. More Sophisticated sharding to support geographic locations and time

- [4.6.1 Data Residency](#)
- [4.6.2 Data Localization](#)
- [4.6.3 Data Sovereignty](#)

8. More integration of Artificial Intelligence(AI) and Intelligent Agents

- [4.4 National Privacy Considerations](#)
- [4.5 National Security Considerations](#)

9. Blacklisting

The Federal Reserve would be well-advised to fund

[https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a\\_glossary:r:rtd\\_e](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:r:rtd_e) |

Research Development Test & Evaluation (RDT&E) Funding]] projects to accelerate these

developments before embarking on U.S. CBDC. Also see [Appendix C: Other Transaction Authority](#)

(OTA)

173)

Stephen Shankland, Quantum computers could crack today's encrypted messages. That's a problem, C/net, 24 May 2021, Accessed: 25 May 2022,  
<https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/>

174)

Dustin Moody, NIST, Federal government leads the way with encryption standards, Samsung Insights, 12 January 2022, Accessed 25 April 2022,  
<https://insights.samsung.com/2022/01/12/federal-government-leads-the-way-with-encryption-standards/>

175)

Donna Fuscaldo, What's the Difference Between Accountants and Bookkeepers?, Business Daily, 8 March 2022, Accessed: 25 April 2022,  
<https://www.businessnewsdaily.com/15357-15-accountant-bookkeeper-differences.html>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:dsn:q21:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:dsn:q21:start)

Last update: **2022/05/18 00:40**



# Question: 22. Are there additional design principles that should be considered? Are there tradeoffs around any of the identified design principles, especially in trying to achieve the potential benefits of a CBDC?

[Return to Design Considerations](#) [Provide Feedback](#)

## Question

[Return to Top](#)

1. **Are there additional design principles that should be considered?**
2. **Are there tradeoffs around any of the identified design principles, especially in trying to achieve the potential benefits of a CBDC?**

## Answer

[Return to Top](#)

## Non-Functional Requirements Design Principles

[Return to Top](#)

### Overview

[Return to Top](#)

Some major design principles missing from the [White Paper](#) are the specification of [Non-Functional Requirements](#). The [Distributed Immutable Data Objects - Reference Architecture \(DIDO-RA\)](#) provides a list of [Non-Functional Requirements](#) applicable to the CBDC. The following is an outline of the **Non-Functional Requirements**:

1. [Portability](#)
  - [Adaptability](#)
  - [Installability](#)
  - [Replaceability](#)

## 2. Reliability

- Maturity
- Availability
- Fault Tolerance
- Recoverability

## 3. Maintainability

- Modularity
- Reusability
- Analysability
- Modifiability
- Testability

## 4. Security

- Confidentiality
- Data Integrity
- Non-Repudiation
- Authenticity
- Accountability

## 5. Manageability

- Types of Manageability Functions
- Manageability Costs
- System Manageability Issues
- Software Manageability Issues

## 6. Usability

- Effectiveness Metrics
- Efficiency Metrics
- Satisfaction Metrics

## 7. Performance

- Platform Performance
- Application Performance
- Network Performance

## 8. Interoperability

## 9. Elasticity

## 10. Scalability

## Examples

[Return to Top](#)

Some of these **Non-Functional** requirements were alluded to in the White Paper, but not directly specified or defined. Table 117 provides an example of cross-referencing the Non-Functional Requirements to the Benefits, Policy Considerations, Risks and Design requirements identified in the [White Paper Analysis](#) done by the [Object Management Group](#) .

Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG.

Table 117:

Non-Functional Requirement	Benefits, Policy Considerations, Risks and Design requirements
<a href="#">Adaptability</a>	B: B0008, B0016, B0025, B0026, B0029, B0032, B0033, B0035, B0037, B0038, B0039, B0048, P: P0007
<a href="#">Performance</a>	B: B0009, B0011-1, B0011-2, B0017-1, B0017-2, B0024, B0034, B0045, B0047, P: P0026, P0028-6
<a href="#">Availability</a>	B: B0012, B0013 B0053, D: D0016
<a href="#">Confidentiality</a>	B: B0004, B0022-1, B0051
<a href="#">Efficiency Metrics</a>	B: B0001, B0002, B0009, B0011, B0014, B0047, B0051, P: P0023, P0026, P0028-6
B = <a href="#">Benefit Considerations</a>	
P = <a href="#">Policy Considerations</a>	
R = <a href="#">Risk Considerations</a>	
D = <a href="#">Design Considerations</a>	

**Note:** There should be no tradeoffs between **Non-Functional Requirements** and any existing requirements identified in [White Paper](#) as determined by the OMG [White Paper Analysis](#)

## Discussion of Example

[Return to Top](#)

The first requirement listed under [Adaptability](#) is Benefit **B0008**:

<b>B0008</b>	3 Provide entrepreneurs a platform on which to create new financial products and services
B = <a href="#">Benefit Considerations</a>	
P = <a href="#">Policy Considerations</a>	
R = <a href="#">Risk Considerations</a>	

## D = Design Considerations

In order to realize **B0008**, the CBDC needs to be considered a system that can support both:

- **Software Adaptability** - A software component with a well-defined, stable **Application Programming Interface (API)** can be exchanged using another component with minimal effort, as long as that component adheres to the API. For example, **SQL** describes an API for a database component. As long as the software adheres to the standard SQL API, the **Database Management System (DBMS)** can be exchanged between, for example, **Oracle | Oracle** and **PostgreSQL**, with no to minimal impact.
- **Architecture Adaptability** - Connectors between software components change without having to change the components. This again comes down to having well-defined, stable APIs for the connectors. For example, the **Unix File System (UnixFS)** is a connector between software components and the physical filesystem. The associated UnixFS library can be exchanged for the **InterPlanetary File System (IPFS)** UnixFS connector and the software component should have no to minimal impact.

Obviously, this is just an example, and the Federal Reserve should adopt the information and update the information in the **White Paper Analysis** and also perform their own assessment a similar to that presented in Table 117. The discussions and justifications for each requirement need to be captured for future reference. For example, **B00008** would have its own discussion area within the CBDC requirements document.

## Functional Requirements Design Principles

[Return to Top](#)

### Overview

[Return to Top](#)

Some major design principles missing from the **White Paper** are the specification of [https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a\\_glossary:f:funcreq](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:f:funcreq). The **Distributed Immutable Data Objects - Reference Architecture (DIDO-RA)** provides a list of **Functional Requirements** applicable to the CBDC. The following is an outline of the **Functional Requirements**:

#### 1. Platforms

- **Hardware Platforms**
- **Operating System Platforms**
- **Runtime Platforms**
- **Network Platforms**
- **Virtualization Platforms**

#### 2. Access Control

Some of these **Functional Requirements** were alluded to in the White Paper, but not directly specified or defined. The Table 118 provides an example of cross-referencing the **Functional Requirements** to the Benefits, Policy Considerations, Risks and Design requirements identified in the [White Paper Analysis](#) done by the [Object Management Group](#).

## Examples

### [Return to Top](#)

Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG.

Table 118:

Functional Requirement	Benefits, Policy Considerations, Risks and Design requirements
<b>Hardware Platforms</b>	B: B0007, B0008, B0011, B0014, B0015, B0018, B0022-3, B0024, B0025, B0029, B0030, B0032, B0033, B0037, B0038, B0039, B0040, B0041, B0043, B0044, B0047, B0049, B0053, P: P0007, P0013, P0020, P0026, P0028, R: R0007, R0008, R0010, R0011, D: D0009, D0012, D0015, D0016, D0017
<b>Access Control</b>	B: B0004, B0005, B0007, B0009, B0010, B0011, B0015, B0018, B0022, B0025, B0029, B0033, B0035-2, B0038, B0041, B0044, B0045, B0046, B0049, B0050, P: P0004, P0005, P0007, P0020, P0021, P0023, P0025, P0029, R: R0001, R0003, R0007, R0008, R0011, R0014,
<b>B = Benefit Considerations</b>	
<b>P = Policy Considerations</b>	
<b>R = Risk Considerations</b>	
<b>D = Design Considerations</b>	

## Discussion of Example

### [Return to Top](#)

The one of the first requirements listed under [Platforms](#) is Benefit **B00011**:

<b>B0011</b>	Make payments: 1. faster 2. cheaper 3. more convenient 4. more accessible
<b>B = Benefit Considerations</b>	

Requirement **B0011** is a compound requirement, and the selection of a Platform can have an impact on:

- **B00011-1** - Faster
- **B00011-2** - Cheaper

- **B00011-3** - More Convenient
- **B00011-4** - More Accessible

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:20\\_comments:dsn:q22:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:20_comments:dsn:q22:start)

Last update: **2022/05/17 18:40**





# 6.0 Recommendations

[Return to Main Document](#) [Provide Feedback](#)

The OMG members wanted to make recommendations to the Federal Reserve for future activities in the area of a U.S. CBDC. They propose 12 different direct actions or activities. One of these activities involves the use of RDT&E funding to explore eight specific Research Development Test & Evaluation (RDT&E) topics.

The **Object Management Group® (OMG®)**, founded in 1989, is an international not-for-profit software consortium (aka [Standards Developing Organization \(SDO\)](#) or a [Voluntary Standards Consensus Body \(VSCB\)](#)) that sets standards in the many areas including distributed object computing. This means the OMG organization plans, develops, establishes, or coordinates voluntary consensus standards using agreed-upon [Policies and Procedures \(P&P\)](#). The P&P provides a framework for openness and transparency to aid in balancing the interests of the Stakeholders, providing due process for disagreements, and building consensus.

The OMG is not a financial institution, a government institution, or a provider of goods, services, or technology. The main goal of the OMG is to produce standard technical specifications for use by the national and international communities with a proven track record, see the [Introduction](#)). Based on our experience in formulating the responses to the questions posed in the **White Paper**, our members have formulated a set of recommendations to help aid the Federal Reserve to move forward with a U.S. CBDC. The OMG members are very active in 26 vertical markets, including Business, Finance, Government, Healthcare, Manufacturing, Military, Robotics, Space, and Telecoms.

- [6.01 Elaborate the Newly Known Risks](#)
- [6.02 Move from Desirements to Requirements](#)
- [6.03 Establish a Consortium](#)
- [6.04 Formally Define Stakeholders](#)
- [6.05 Formally Define Non-Functional Requirements](#)
- [6.06 Formally Define Functional Requirements](#)
- [6.07 Refine Applicable Laws and Regulations](#)
- [6.08 Instill Confidence in the CBDC](#)
- [6.09 Baked-in Security](#)
- [6.10 Adopt a Model-Based Systems Engineering \(MBSE\) Approach](#)
- [6.11 Perform Research Development Test & Evaluation \(RDT&E\)](#)
  - [6.11.1 Consensus Algorithms](#)
  - [6.11.2 Artificial Intelligence \(AI\)](#)
  - [6.11.3 Ontologies](#)
  - [6.11.4 Smart Contracts](#)
  - [6.11.5 Complex Data Models](#)
  - [6.11.6 Understanding Gas Implications](#)
  - [6.11.7 Simulation, Training and Testing Environment](#)
  - [6.11.8 Build Reference Implementation \(RI\)](#)
- [6.12 Defining the Appropriate Standards or Specifications](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc\\_omg:04\\_doc:90\\_recommend:start](https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:04_doc:90_recommend:start)

Last update: **2022/05/16 22:14**



## 6.01 Elaborate the Newly Known Risks

[Return to Recommendations](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve define a task for exploring and understanding the risks which were **Unknown** or not elaborated in the **White Paper**.

The answer to [Question: 11. Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?](#), asked about these **Unknown Risks** for the CBDC. The OMG has responded as follows. Many of the responses are basically “Recommendations” for future CBDC efforts. The **“Unknown Risks”** identified by OMG members are:

- 1. Risk of a Software Crisis
- 2. Risk of Lack of Stakeholder Buy-In
- 3. Risk Due to Poor Community of Interest (CoI) Governance
- 4. Risk Due to lack of Broad, Wide Ranging Security Planning
- 5. Risk of Data being hacked due weak Security Infrastructure
- 6. Risk of Meta-Data being hacked due weak Security Infrastructure
- 7. Risk of Business Processes Being Hacked
- 8. Risk of competing Currency Models for the CBDC

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:90\\_recommend:10\\_recommend:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:90_recommend:10_recommend:start)

Last update: **2022/05/16 22:17**



## 6.02 Move from Desirements to Requirements

[Return to Recommendations](#) | [Provide Feedback](#)

The OMG members recommend the Federal Reserve define a task for developing and perfecting the Requirements for the U.S. CBDC.

The **White Paper** did a good job of describing what a U.S. CBDC could be and identifying, in prose form, the issues and expectations surrounding a CBDC. The OMG members took the first step in trying to formalize these issues and expectations as a set of Desirement<sup>34)</sup> considerations categorized according to the four major objectives identified in the **White Paper**:

- [Benefit Considerations](#),
- [Policy Considerations](#),
- [Risk Considerations](#)
- [Design Considerations](#)

The next step is to start capturing real Requirements<sup>35)</sup> for a U.S. CBDC. The OMG DIDO-RA has an extensive discussion on [Specifying Requirements](#) which is particularly appropriate for Distributed Systems.

[Requirements](#) are captured in many ways. In the government realm, this is usually done through codification into laws, regulations, and contracts including [Performance](#) and [Conformance Specification](#).

Regardless of where the requirements are captured or by what organizations, they can in general be considered governing statements. The following are some guidance on how to write healthy governing statements and consequently also requirements.

A [Governance](#) Statement based on an [Engineering Governance](#) Model developed at US Navy SPAWAR<sup>36)</sup> is defined as atomic, succinct, absolute, and definitive in nature. It contains specific instructions which can be validated through observation, measurement, or testing.

- **Atomic** - A Governance Statement only addresses a single topic. Indicators of non-atomic guidance are the use of highly complex sentences, multiple sentences, or conjunctions such as and, or, etc.
- **Succinct** - A Governance Statement is short and to the point. The definition of terms or caveats that explain when a statement is applicable is not acceptable as part of the Governance Statement. Indicators of non-succinct statements are the use of words or expressions such as: consider, when possible, if, etc.
- **Absolute** - A Governance Statement is valuable with one or more non-subjective questions. Indicators of non-absolute statements are those which are subject to the interpretation of the evaluator. For example, "All menus must be user-friendly". No one produces menus that they feel are user-hostile.
- **Definitive** - A Governance Statement is precisely worded and explicit in nature. Their words, terms, and expressions need to be defined and not subject to interpretation. Indicators of

non-definitive guidance are words that are not intuitively obvious to an outside reader. Some words that are examples of non-explicit words are: object, service, and function.

Another issue or controversy with specifying requirements is how the statements use imperatives originally defined in [RFC2119 - Key words for use in RFCs to Indicate Requirement Levels](#), words like:

- [Shall \(Requirement\)](#)
- [Must \(Requirement\)](#)
- [Will \(Requirement\)](#)
- [Should \(Requirement\)](#)

There is an excellent reference in [How to Write and Exceptionally Clear Requirements Document](#)<sup>37)</sup> and it is up to the Federal Reserve and the CBDC effort to settle on the form of requirements.

One of the best ways to analyze **Non-Functional Requirements** is to perform an evaluation of proposed or existing systems, subsystems, components, etc. The [Distributed Immutable Data Objects - Reference Architecture \(DIDO-RA\)](#) provides a starting point for conducting such an evaluation. [Creating a Trade Study](#). Obviously, the DIDO-RA Trade Study is to be used as a reference and perhaps a starting point.

<sup>34)</sup>

A **Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired, but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)<sup>35)</sup>

A **Requirement** specifies a capability or [condition](#) that must (or should) be satisfied. A requirement may specify a function that a system must perform or a [performance](#) condition a system must achieve.

<sup>36)</sup>

Stavros, Robert W. and Albrant, Jeremiah; [Engineering Governance](#), SPAWAR, October 9, 2007,<sup>37)</sup>

QRA, [How to Write and Exceptionally Clear Requirements Document](#), Accessed 5 March 2021, [https://qracorp.com/write-clear-requirements-document/#elementor-toc\\_heading-anchor-1](https://qracorp.com/write-clear-requirements-document/#elementor-toc_heading-anchor-1)

From:

<https://www.omgwiki.org/CBDC/> - OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:20\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:20_recomend:start)

Last update: **2022/05/16 22:18**



## 6.03 Establish a Consortium

[Return to Recommendations](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve define a task for establishing a Stakeholders Consortium which would be a fulfillment of **P0011** and **P0030** Desirements<sup>174</sup>. These are provided in Table 119 for convenience.

The Policy Considerations identified in the **White Paper**  
Table 119:

Statement No.	Page No.	Desirement
<b>P0011</b>	<b>3</b>	The Federal Reserve does not intend to proceed with the issuance of a CBDC without clear support from: <ol style="list-style-type: none"> <li>1. Executive Branch</li> <li>2. Legislative Branch</li> <li>3. Ideally in the form of a specific authorizing law</li> </ol>
<b>P0030</b>	<b>21</b>	The Federal Reserve will only take further steps toward developing a CBDC if: <ol style="list-style-type: none"> <li>1. Research points to benefits for households, businesses, and the economy overall that exceed the downside risks</li> <li>2. Indicates that CBDC is superior to alternative methods</li> </ol>

Each of the two Desirements needs to be pursued separately. The Federal Reserve should continue to pursue garnering support from the Executive and Legislative Branches of Government for a CBDC as stated in **P0011** and also pursue obtaining an authorizing law. However, while pursuing these avenues, it is important to present [Data, Information, Knowledge, Understanding, and Wisdom](#) based on the findings from [Research Development Test & Evaluation \(RDT&E\)](#).

The purpose of a Consortium would be to help initiate, guide, oversee, and coordinate RDT&E efforts. These efforts would be used to help formulate an authorizing law and provide evidence to the Executive and Legislative branches of government.

The CBDC is a large problem with many moving parts, all of which require a lot of systems analysis, engineering, testing, and simulation in order to ensure public confidence:

*For a nation's economy to function effectively, its citizens must have confidence in its money and payment services. The Federal Reserve, as the nation's central bank, works to maintain the public's confidence by fostering monetary stability, financial stability, and a safe and efficient payment system. from the **Executive Summary** provided in the [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#) White Paper*

Pursuing a CBDC that is flawed or not having stakeholder buy-in could ultimately inflict more

damage than it is worth.

The OMG further recommends that an **Other Transaction (OT) Consortium** be considered and the stakeholders are invited to join. An OT Consortium is a formal relationship between a government sponsor (i.e., Federal Reserve), an OT Administrator, and a collection of traditional and non-traditional vendors, non-profit organizations, and academia aligned to a technology domain area (i.e., cyber, space, undersea, propulsion) that are managed by a single entity, and focused on innovative solutions to government technology challenges that meet the intended scope and purpose of other transactions.

OT Consortium is based on the following [OT Consortium Model](#):



The Existing OT Constoria Model  
Figure 47:

Generally, an OT Consortium has three components:

- Government Sponsor
- Government Contracting Office
- Consortium Manager
- Consortium (i.e., Stakeholders)

**Note:** Sometimes the government sponsors prefer to manage a consortium in-house rather than hire an industry Consortium Manager or Consortium Management Firm.

The Consortium Manager is awarded an OT agreement by the government (base OT agreement) and manages OTs awarded to its consortium member organizations (project OT agreements) under the base agreement. In the [OMG Distributed Immutable Data Object Reference Architecture \(DIDO-RA\)](#), this highest level (i.e., OT Consortium) is referred to as the [Ecosphere](#) which would roughly follow the steps outlined in [Steps for Establishing an Ecosphere](#). The OT Consortia (ie., Ecosphere) can create any number of Ecosystems and Domains as is needed. It is recommended that the Ecosystems create and are responsible for Domains that fall under their auspices, however, the Policy and Procedures (P&P) may require the Ecosphere's approval for creation.

174)

A **Desirement** is a blended word combining the word **Desire** and **Requirement**. **Desirement** is something that is desired, but not absolutely required and is often used to caption the capabilities of a product or system before it has reached the formal requirements phase. Source: [Desirement](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:30\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:30_recomend:start)

Last update: **2022/05/18 21:38**





## 6.04 Formally Define Stakeholders

[Return to Recommendations](#) | [Provide Feedback](#)

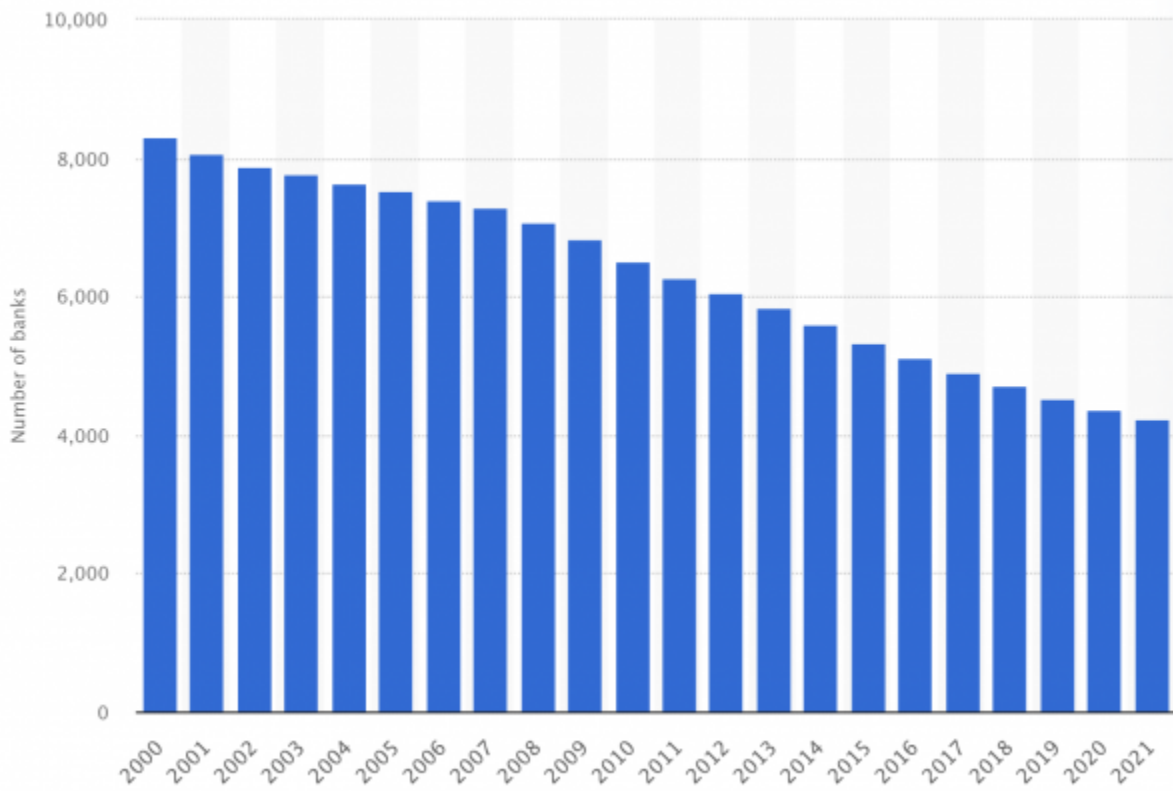
The OMG members recommend the Federal Reserve define a task for establishing a U.S. CBDC Consortium that has well defined [Charter](#), [ByLaws](#), [Policy and Procedures \(P&P\)](#), and [Guidance](#) allowing all stakeholders to participate and have a voice in the final U.S. CBDC.

The OMG members recommend the Federal Reserve establish a formal list of Stakeholders in the U.S. CBDC. Obviously, when it comes to determining the Stakeholders it might be fair to include every U.S. Resident, or at least those having banking or credit union accounts. Obviously, this would be unwieldy. All these individuals are supposedly represented in government through elected officials in Congress and the President. These elected officials have taken the problem and made various departments or agencies that should be representing these people. Based on a cursory review, it appears that there are at least 33 different Oversight authorities in the U.S., see [Table 90](#).

Summary of the estimated number of Government Stakeholders for the CBDC.  
Table 120:

<b>Potential Oversight Authorities</b>	<b>No. of Stakeholders</b>
<a href="#">U.S. Federal Government Oversight Authorities</a>	14
<a href="#">non-U.S. Federal Government Oversight Authorities</a>	19
<b>Total</b>	<b>33</b>

However, this does not include the roughly 4,200 Commercial Banks insured by the FDIC, see [Figure 48](#) or the largest Banking Association in the U.S., The American Banking Association (ABA), or its competitors, nor the roughly 5,300 Credit Unions.



Number of FDIC-insured commercial banks in the United States from 2000 to 2021.<sup>175)</sup>  
 Figure 48:

**Note:** In 2021, there were 4,236 FDIC-insured commercial banks in the United States.

It does not represent all the retail outlets, service providers, landlords, etc that all have a “stake” in the U.S> Dollar and consequently a U.S. CBDC. For more on the Stakeholders identified in the OMG analysis, please refer to section 4.1 Stakeholders.

<sup>175)</sup>

Statista, Number of FDIC-insured commercial banks in the United States from 2000 to 2021,  
 Accessed: 8 May 2022,  
<https://www.statista.com/statistics/184536/number-of-fdic-insured-us-commercial-bank-institutions/>

From:  
<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**  
 Permanent link:  
[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:40\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:40_recomend:start)  
 Last update: 2022/05/19 01:49



# 6.05 Formally Define Non-Functional Requirements

[Return to Recommendations](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve define a task for defining, developing, and perfecting the [Non-functional requirements](#) that are acceptable to the Federal Reserve and its Stakeholders.

Non-Functional Requirements are often incorrectly assumed rather than explicitly defined by users. This can lead to problems towards the end of a project as the user expectations for non-functional requirements are not met. Many times, the developers dismiss non-functional requirements as non-testable and therefore not enforceable.

This lack of specificity in non-functional requirements sets the stage for conflicts between the users, system architects, systems engineers, and developers. For example, users expect software to start and run every time it is used however, the non-functional requirement of reliability may never have been explicitly specified.

Users expect new features to be added to a system and tested before they use them. Users assume the software is maintainable without an explicit declaration for “[maintainability](#)”. In many ways, they expect it to be an unwritten requirement and or [goal](#). In other words, users expect the system to be analyzable, changeable, stable, and testable<sup>176)</sup>. For example, smartphone users will switch apps to other apps if the energy consumed by the app is not efficient. Efficiency is therefore a non-functional requirement. Energy consumption may also be a [functional requirements](#) (i.e., An [application](#) can not use more than 1040 mW (milli-Watt) per [Short Message Service \(SMS\)](#) message.<sup>177)</sup>.

It is recommended the Federal Reserve consider reviewing and specifying values for each of these Non-FUunctional Requirements.

## 1. [Portability](#)

- [Adaptability](#)
- [Installability](#)
- [Replaceability](#)

## 2. [Reliability](#)

- [Maturity](#)
- [Availability](#)
- [Fault Tolerance](#)
- [Recoverability](#)

## 3. [Maintainability](#)

- [Modularity](#)

- Reusability
- Analysability
- Modifiability
- Testability

#### 4. Security

- Confidentiality
- Data Integrity
- Non-Repudiation
- Authenticity
- Accountability

#### 5. Manageability

- Types of Manageability Functions
- Manageability Costs
- System Manageability Issues
- Software Manageability Issues

#### 6. Usability

- Effectiveness Metrics
- Efficiency Metrics
- Satisfaction Metrics

#### 7. Performance

- Platform Performance
- Application Performance
- Network Performance

#### 8. Interoperability

#### 9. Elasticity

#### 10. Scalability

<sup>176)</sup>

Prolifics Testing, [Achieving Requirements Testability](https://www.prolifics-testing.com/news/achieving-requirements-testability), 10 October 2018, Accessed 10 November 2020, <https://www.prolifics-testing.com/news/achieving-requirements-testability>

<sup>177)</sup>

Sai Suren Kumar Kasireddy and Vishnuvardhan Reddy Bojja, [Measurements of Energy Consumption in Mobile Applications with respect to the quality of Experience](https://www.diva-portal.org/smash/get/diva2:829733/FULLTEXT01.pdf), School of Computing, Blekinge Institute of Technology, 37179 Karlskrona, Sweden, March 2012, Accessed: 10 November 2020, <https://www.diva-portal.org/smash/get/diva2:829733/FULLTEXT01.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:50\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:50_recomend:start)

Last update: **2022/05/18 00:44**



## 6.06 Formally Define Functional Requirements

[Return to Recommendations](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve define a task for defining, developing, and perfecting the [Functional Requirements](#) that are acceptable to the Federal Reserve and its Stakeholders.

Functional Requirements define the basic system behavior. Essentially, they are requirements stating what the system must do or must not do, and can be thought of in terms of how the system responds to inputs. Functional requirements usually define if/then behaviors and include calculations, data input, and business processes.

Functional Requirements (sometimes referred to as Performance Requirements) are features that allow the system to function as it was intended. Put another way, if the functional requirements are not met, the system will not work. Functional requirements are product features and focus on user requirements. Functional Requirements can be used during all phases of a project [Lifecycle](#) independent of the development model (i.e., [Waterfall](#) or [Agile](#)). In the Waterfall method, these requirements are generally specified early on in the process. In the Agile method, they can be applied derived during each [Sprint](#) or applied during specific Sprints.

### 1. Platforms

- [Hardware Platforms](#)
- [Operating System Platforms](#)
- [Runtime Platforms](#)
- [Network Platforms](#)
- [Virtualization Platforms](#)

### 2. Access Control

- [Permissionless Networks](#) and [Public Network](#) - public and open
- [Permissionless Networks](#) and [Private Network](#) - public and closed
- [Permissioned Networks](#) and [Public Network](#) - private and open
- [Permissioned Networks](#) and [Private Network](#) - private and closed

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:55\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:55_recomend:start)

Last update: **2022/05/17 01:37**



## 6.07 Refine Applicable Laws and Regulations

[Return to Recommendations](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve define a task for reviewing and assessing the current Laws and Regulations for applicability to a U.S. CBDC and making recommendations on how to update the laws and regulations to accommodate the CBDC.

The members of the OMG have compiled a list of the Laws and Regulations within the U.S. that applicable to the Financial System covering:

- [Privacy](#) see Table 16 for summary
- [Security](#) see Table 8 for a summary

These laws were passed by the Legislative and the Executive Branches of the Government and have been upheld by the Supreme Court. Therefore, this can be considered as part of the will of the people ( see Stakeholders).

Table 16: Summary of the number of laws and regulations covering National Security Considerations.

<b>U.S. Privacy Consideration</b>	<b>No. of Laws and Regulations</b>
<a href="#">U.S. Federal Laws and Regulations</a>	10
<a href="#">U.S. State Laws and Regulations</a>	6
<b>Total</b>	<b>16</b>

Table 17: Summary of the number of laws and regulations covering National Security Considerations.

<b>National Security Consideration</b>	<b>No. of Laws and Regulations</b>
<a href="#">Human Trafficking</a>	14
<a href="#">Drug Trafficking</a>	9
<a href="#">Corruption</a>	10
<a href="#">Money Laundering</a>	11
<b>Total</b>	<b>44</b>

It appears that a U.S. CBDC would have to adhere to these laws if it is going to be considered valid. Not doing so would be considered arbitrary and capricious. In addition, since the CBDC would most likely rely on new technology, each of these laws would need to be evaluated by a legal team to assess how the laws and regulations need to be reinterpreted, amended, or extended to remain current. Further discussions are well beyond the skills of the authors but it is recommended The Federal Reserve take this on as a serious part of the whole CBDC effort.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc\\_omg:04\\_doc:90\\_recommend:60\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:04_doc:90_recommend:60_recomend:start)

Last update: **2022/05/17 01:38**





## 6.08 Instill Confidence in the CBDC

[Return to Recommendations](#) [Provide Feedback](#)

The [Object Management Group \(OMG\)](#) recommends the Federal Reserve uses a Model-Based Systems Engineering (MBSE) and Unified Architecture Framework (UAF) approach for future CBDC efforts. The CBDC is a complex issue that, once released, could have a life expectancy of many, many years. Only through extensive Systems Analysis, Engineering, Design, and testing will CBDC have the stability it needs to instill confidence from the public.

Some of the potential requirements in the [White Paper](#) as summarized by the [Object Management Group's White Paper Analysis](#) reflect the need to instill public confidence (See Table 71)

Some requirements in the White Paper that require the confidence of the public.

Table 119:

Statement No.	Page No.	Statement
<b>B0020</b>	<b>13</b>	Maintain public confidence by not requiring mechanisms, such as deposit insurance
<b>R0003</b>	<b>3</b>	<b>Risk</b> to the safety and stability of the financial system
<b>R0004</b>	<b>3</b>	<b>Risk</b> to the efficacy of monetary policy
<b>R0005</b>	<b>7</b>	New payment services could pose <b>Risks</b> to: <ol style="list-style-type: none"> <li>1. financial stability</li> <li>2. payment system integrity</li> <li>3. other <b>Risks</b></li> </ol>
<b>R0011</b>	<b>11</b>	Increased <b>Risk</b> to consumer's vulnerability to: <ol style="list-style-type: none"> <li>1. loss</li> <li>2. theft</li> <li>3. fraud</li> </ol>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:70\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:70_recomend:start)

Last update: **2022/05/18 00:46**



## 6.09 Baked-in Security

[Return to Recommendations](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve define a task to ensure that Security is baked into the U.S. CBDC rather than trying to *post facto* add it later (i.e bolted-on).

Also see the answers to:

1. [1. How could a CBDC be designed to foster operational and cyber resiliency?](#)
  - [b\) Cyber Resiliency](#)
2. [Question: 07. What tools could be considered to mitigate any adverse impact of CBDC on the financial sector? Would some of these tools diminish the potential benefits of a CBDC?](#)
  - [Lack of Reporting and Oversight](#)
3. [Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?](#)
4. [Question: 02. Could some or all of the potential benefits of a CBDC be better achieved in a different way?](#)

Cryptocurrency skirts near the edges of illegal, illicit, or shady interactions and transactions. The Chainalysis Team recently published their 2021 findings<sup>176)</sup> which highlights some security issues associated with the unregulated or poorly regulated Cryptocurrency realm. The following is an excerpt from the report:

*Overall, going by the amount of cryptocurrency sent from illicit addresses to addresses hosted by services, **cybercriminals laundered \$8.6 billion worth of cryptocurrency in 2021.***

*That represents a **30% increase in money laundering activity over 2020**, though such an increase is unsurprising given the significant growth of both legitimate and illicit cryptocurrency activity in 2021. We also need to note that these numbers only account for funds derived from “cryptocurrency-native” crime, meaning cybercriminal activity such as [Dark Web](#) market sales or ransomware attacks, in which profits are virtually always derived in cryptocurrency rather than fiat currency. It’s more difficult to measure how much fiat currency derived from offline crime — traditional drug trafficking, for example — is converted into cryptocurrency to be laundered. However, we know anecdotally this is happening, and later in this section provide a case study showing an example of it.*

Therefore, security needs to be “baked into” the CBDC from the onset and can not be an afterthought; however, it is hard to balance the tightrope between the need for **Privacy** and the need for **Security**. This difficulty in achieving a balance has been captured in Desirement **R0014**:

<b>R0014</b>	<b>Risk of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity</b>
--------------	--

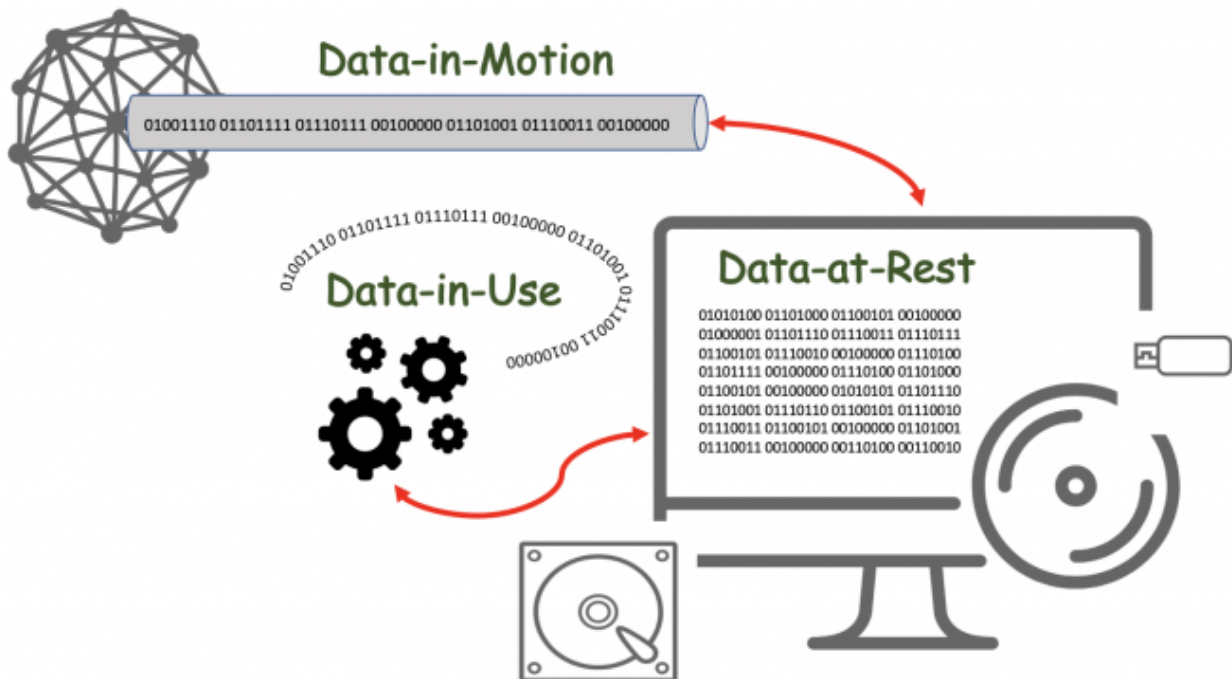
It appears that the [Digital Cash Model](#) is less vulnerable than the [Digital Account Model](#). The use of Stablecoins could help with maintaining the value of CBDC, but would not add any security.

Regardless of which model ( [Digital Accounts](#), [Stablecoins](#), [Digital Cash](#)) is used for the CBDC, the [Object Management Group](#) recommends that the Federal Reserve consider Security of the system from the earliest phases of the U.S. CBDC. This means having the Non-Functional requirement of Security be well defined and formal.

One way to accomplish this is through the use of a Model-Based Systems Engineering (MBSE) and Unified Architecture Framework (UAF) to model all aspects of the CBDC before it is built. Since the requirements for the security of the system are a moving, ever-changing target, this does not mean that every security issue must be fully understood or specified before work can begin. It means that at every step, the Security question needs to be raised. The CBDC is a complex issue that, once released, could have a life expectancy of many, many years. Only through extensive Systems Analysis, Engineering, and Design will the CBDC have the stability it needs to instill confidence in the public.

During system development, MBSE and UAF models of the system are used along with Use Scenarios and Use Cases to flush out potential problems. This means thinking about all aspects of the State of Data throughout its lifecycle. The OMG DIDO-RA has detailed discussions of the various states of data and how it relates to a distributed system.

Figure 42 graphically represents the different Data States within a system. Most systems are now able to handle Data-in-Motion and Data-at-Rest issues but have traditionally relied on physical security to protect Data-in-Use.



The various States of Data  
Figure 49:

Table 99 provides a quick overview of the various data states. These data states are described in

detail in the [OMG DIDO-RA](#).

Data can exist in the following different states

Table 121:

<b>Data-at-Rest</b>	<b>Data-at-Rest</b> refers to all data in computer storage. It excludes data while it is moving across or within a network, and it excludes data that is temporarily residing in computer memory.
<b>Data-in-Motion</b>	<b>Data-in-Motion</b> , also referred to as <b>Data in Transit</b> or <b>Data in Flight</b> , is a <b>Digital Asset</b> transmitted between locations (i.e., between computers or computer components). Data-In-Motion also describes data within <b>Random Access Memory (RAM)</b> .
<b>Data-in-Use</b>	<b>Data-in-Use</b> covers data being processed (i.e., updated, processed, erased, accessed or read) by a system. Data-In-Use is not passively stored, but is actively moving through parts of a <b>Computing Platform</b> (i.e., <b>Central Processing Unit (CPU)</b> , <b>Dynamic Random Access Memory (DRAM)</b> , <b>Data Bus</b> , etc.). <b>Data-In-Use</b> is one of three states of digital data – the other states are <b>Data-at-Rest</b> and <b>Data-in-Motion</b> .

White Paper Desiresments related to disruption and security

Table 122:

<b>Statement No.</b>	<b>Page No.</b>	<b>Statement</b>
<b>B0004</b>	<b>2</b>	Protect consumer privacy
<b>B0005</b>	<b>2</b>	Protect against criminal activity
<b>B0053</b>	<b>20</b>	Provide resiliency to threats to existing payment services—including: 1. operational disruptions 2. cybersecurity risks
<b>R0011</b>	<b>11</b>	Increased <b>Risk</b> to consumer's vulnerability to: 1. loss 2. theft 3. fraud
<b>D0015</b>	<b>20</b>	<b>Design</b> should include any dedicated infrastructure required to provide a resilience to threats such as operational disruptions and cybersecurity risks
<b>D0016</b>	<b>20</b>	<b>Design</b> should include offline capabilities to help with operational resilience of the payment system
<b>D0017</b>	<b>20</b>	<b>Design</b> should include digital payments in areas suffering from large disruption, such as natural disasters

<sup>176)</sup>

DeFi Takes on a Bigger Role in Money Laundering, But a Small Group of Centralized Services Still Dominate, Chainalysis Team, 26 January 2022, Accessed: 4 April 2022, <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:80\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:80_recomend:start)

Last update: **2022/05/19 01:51**



## 6.10 Adopt a Model-Based Systems Engineering (MBSE) Approach

[Return to Recommendations](#)

The OMG members recommend the Federal Reserve define a task to define a methodology for proceeding with a [Greenfield](#) U.S. CBDC. There is a lot of risk in trying to organically define the development process.

For more than forty years, the practice of systems engineering followed a linear path: requirements are documented first, followed by analysis then conceptual design—through the development life cycle. However, regardless of the engineering process employed—waterfall, incremental, iterative, spiral, and even sprint-based—the lack of integration from one phase to another in the cycle results in longer delivery times and increases costs to correct errors introduced at transition points.

**Model-Based Systems Engineering (MBSE)**<sup>178</sup> is an initiative in the systems engineering community that uses model-based descriptions and transformations so that work occurs concurrently. Requirements collection, analysis, and specifications are performed at the same time as conceptual design. MBSE is practiced across many industries around the globe. For example, it was used to develop the world's largest telescopes, propulsion engines for fighter jets, autonomous driving cars, software solutions to include software-defined radios, and space applications (hardware and software).

MBSE is often contrasted with a more traditional document-based approach to systems engineering, where system information is spread across many document-based artifacts (handwritten text documents, spreadsheets, and drawings). MBSE brings information together into a cohesive, integrated model of the system that:

1. Enhances precision, consistency, and traceability;
2. Includes behavioral analysis, system architecture, requirement traceability, performance analysis, simulation, test, etc.;
3. Formalizes the practice of systems development through the use of models;
4. Integrates information across discipline-specific engineering tools, including hardware and software design, analysis, simulation, and test; and
5. Facilitates shared understanding of the system among the development team, resulting in:
  - quality/productivity improvements and lower risk;
  - rigor and precision;
  - ongoing communications among development team and customer; and
  - management of complexity.

For more information on MBSE, please see:

- [MBSE Specifications at OMG](#);
- [MBSE Overview in Appendix](#).

The [Object Management Group \(OMG\)](#) also recommends that the Federal Reserve use the Unified

Architecture Framework (UAF) for future CBDC efforts. See [OMG Unified Architecture Framework \(UAF\)](#):

UAFP 1.0 supports the capability to:

- model architectures for a broad range of complex systems, which may include hardware, software, data, personnel, and facility elements;
- model consistent architectures for System-of-Systems (SoS) down to lower levels of design and implementation;
- support the analysis, specification, design, and verification of complex systems; and
- improve the ability to exchange architecture information among related tools that are SysML-based and tools that are based on other standards.

The intent of UAF is to provide a standard representation for describing enterprise architectures using a Model-Based Systems Engineering (MBSE) approach.

The [Object Management Group](#) also recommends that the Federal Reserve use the Unified Architecture Framework (UAF) for future CBDC efforts. See [OMG Unified Architecture Framework \(UAF\)](#); it is summarized here:

*UAF Profile (UAFP) 1.0 supports the capability to:*

- *Model architectures for a broad range of complex systems, which may include hardware, software, data, personnel, and facility elements;*
- *Model consistent architectures for System-of-Systems (SoS) down to lower levels of design and implementation;*
- *Support the analysis, specification, design, and verification of complex systems; and*
- *Improve the ability to exchange architecture information among related tools that are SysML based and tools that are based on other standards.*

*The intent of UAF is to provide a standard representation for describing enterprise architectures using a Model-Based Systems Engineering (MBSE) approach.*

178)

“Model-based systems engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases.”  
INCOSE SE Vision 2020 (INCOSE-TP-2004-004-02), Sept 2007 MBSE

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:90\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:90_recomend:start)

Last update: **2022/05/18 00:49**



# 6.11 Perform Research Development Test & Evaluation (RDT&E)

[Return to Recommendations](#) [Provide Feedback](#)

## Overview

[Return to Top](#)

There are a couple of ways that the OMG members recommend pursuing a U.S. CBDC [Research Development Test & Evaluation \(RDT&E\)](#) effort.

- Either the Federal Reserve directly funds the RDT&E effort
- Partner with a U.S. Federal Department with an existing [Small Business Innovation Research \(SBIR\)](#) / [Small Business Technology Transfer \(STTR\)](#) process in place (see [Table 123](#)) to conduct the research.

**Note:** Under the SBIR/STTR processes, there can be multiple award teams working to solve the same problem at the same time. The solutions proposed could be merged together later. This gives some competition and helps avoid *group think* on the *best solution*.

List of U.S. Federal Eleven Federal Agencies participating in the SBIR program<sup>177)</sup>  
Table 123:

1. Small Business Administration
2. Department of Agriculture
3. Department of Commerce
  - National Institute of Standards and Technology (NIST)
  - National Oceanic and Atmospheric Administration (NOAA)
4. Department of Defense<sup>‡</sup>
5. Department of Education
6. Department of Energy<sup>‡</sup>
7. Department of Health and Human Services<sup>‡</sup>
8. Department of Homeland Security
9. Department of Transportation
10. Environmental Protection Agency
11. National Aeronautics and Space Administration<sup>‡</sup>
12. National Science Foundation<sup>‡</sup>

<sup>‡</sup> - *participate in the STTR Program*




# Limitations of Blockchain Technology

[Return to Top](#)

Orla Ward and Sabrina Rochemont presented a list of Limitations to Blockchain Technologies to the Institute and Faculty of Actuaries.<sup>178)</sup> Table 124 presents a summary of the limitations outlined by Orla et al. Many of these are issues are similar to those proposed by the OMG members in [Possible SBIR STTR Topics](#).

Limnitations of Blockchain Technology.<sup>179)</sup>

Table 124:

Paragraph Number	Title	Description
4.7.1	Slow transactions	<p>Physical performance affecting public Blockchains is a major limitation and barrier to adoption, as this comparative chart illustrates.</p> <p><b>Cryptocurrencies Transaction Speeds Compared to Visa &amp; Paypal</b></p>  <p>Article &amp; Sources:  <a href="https://howmuch.net/articles/crypto-transaction-speeds-compared">https://howmuch.net/articles/crypto-transaction-speeds-compared</a>  <a href="https://howmuch.net/sources/crypto-transaction-speeds-compared">https://howmuch.net/sources/crypto-transaction-speeds-compared</a></p> <p><a href="#">Cryptocurrencies Transactions Speeds compared to Visa and Paypal</a><sup>180)</sup>  Figure 50:</p>
4.7.2	Consensus time delay	<p>The mining process (“Proof of Work”) requires vast amounts of computing power to record transactions and because all payments require miner approval, there is a limit on the number of transactions that can be processed at any time. Once a transaction has been completed, it is irreversible. Miners are critical to ensuring the validity of each transaction and are rewarded by receiving newly created digital currency units. The alternative “Proof of Stake” attributes mining power to the proportion of tokens held by the miner and may help improve performance in the future.</p>

<b>Paragraph Number</b>	<b>Title</b>	<b>Description</b>
<b>4.7.3:</b>	<b>Scalability</b>	Most digital currencies have a source code that outlines the precise number of units that can and will ever exist and so there is a finite supply. Over time, it becomes more difficult for miners to produce digital currency units until the upper limit is reached. Digital currency's finite supply makes them inherently deflationary, more akin to gold and other precious metals than fiat currencies. This too places pressure on the price of digital currencies, unlike fiat currencies for which Central Banks can, in theory, produce an unlimited supply
<b>4.7.4</b>	<b>Design</b>	It has been suggested that many issues with the performance of public Blockchain stem from excessive decentralization, leading to inefficiency. Further research and development activity will likely resolve the trade-off between decentralization and performance.
<b>4.7.5</b>	<b>Link into the real economy</b>	The environment within Blockchain cannot be extrapolated outside of Blockchain, for instance, to translate "proof of ownership" into "proof of possession" (e.g. of a house). Blockchain must solve the real-life trust problem and needs to interface with a trusted central mechanism outside of Blockchain.
<b>4.7.7</b>	<b>Security</b>	Blockchain is trusted for being a highly secure, impenetrable technology as all users share the same information that has been verified by the miner. The security of a Blockchain is guaranteed through the use of cryptographic functions that are deemed to be relatively secure because breaking them requires huge computing resources, which are not generally available. However, it has been suggested that they are not completely immune from advances in technology, namely the rise of quantum computing. Unlike ordinary computers that operate on a binary system accepting bites of the form 0 or 1, a quantum computer works with particles that can be in superposition. Rather than representing bits of value 0 or 1, quantum computers would have particles represented by qubits, which can take on the value 0, or 1, or both simultaneously. Quantum computing may have the potential to break the cryptography that conventional Blockchain relies upon as they are much more powerful. However, such an issue may be solved using next-generation technology by using quantum cryptography in Blockchain and so the entire Blockchain may be a quantum phenomenon
<b>4.7.8</b>	<b>Vulnerability</b>	All Blockchain systems have to address the inherent problems of double-spend, and issues such as blocks that have detached from the chain, accidentally or through attacks. As Blockchains are implemented in software, any number of software vulnerabilities can also exist due to poor code implementations.

## Possible SBIR/STTR Topics

[Return to Top](#)

The following subsections are provided by the OMG members on some possible RDT&E topics and some discussions the Federal Reserve can pursue with a partnering Federal Agency (see [123](#) for a list of possible Federal Government Department SBIR/STTR partners).

- [6.11.1 Consensus Algorithms](#)
- [6.11.2 Artificial Intelligence \(AI\)](#)
- [6.11.3 Ontologies](#)
- [6.11.4 Smart Contracts](#)
- [6.11.5 Complex Data Models](#)
- [6.11.6 Understanding Gas Implications](#)
- [6.11.7 Simulation, Training and Testing Environment](#)
- [6.11.8 Build Reference Implementation \(RI\)](#)

177)

The Department of Interior, [Small Business Innovation Research Programs \(SBIR\)](#), Accessed: 12 May 2022, <https://www.doi.gov/pmb/osdbu/small-business-innovation-research-programs-sbir>

178) 179)

Orla Ward, Sabrina Rochemont, [An addendum to “A Cashless Society- Benefits, Risks and Issues \(Interim paper\)” - Understanding Central Bank Digital Currencies \(CBDC\)](#), Institute and Faculty of Actuaries, page 17-18, March 2019, Accessed: 18 May 2022, <https://www.actuaries.org.uk/system/files/field/document/Understanding%20CBDCs%20Final%20-%20disc.pdf>

180)

HowMuch.net, [Transactions Speeds: How Do Cryptocurrencies Stack Up To Visa or PayPal?](#), Accessed: 15 May 2022, <https://howmuch.net/articles/crypto-transaction-speeds-compared>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:90\\_recommend:93\\_recomend:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:90_recommend:93_recomend:start)

Last update: **2022/05/18 21:38**



## 6.11.1 Consensus Algorithms

[Return to RDT&E](#) [Provide Feedback](#)

*Consensus algorithms are the basis of all the blockchains/DAGs. They are the most important part of the blockchain/DAG platforms. Without them(consensus algorithms) we will be left with just a dumb, immutable database.*<sup>183)</sup>

The OMG members recommend the Federal Reserve invest [Research Development Test & Evaluation \(RDT&E\) Funding](#) in developing and perfecting any [Consensus Algorithms](#) required by the CBDC since they are an essential part of any DIDO implementation such as [Blockchain](#), [Distributed Ledger](#), [Directed Acyclical Graphs](#), etc).

There are a few consequences to not having “the best” Consensus Algorithms for the CBDC:

- Loss of confidence in the Federal Reserve and the CBDC by the Stakeholders
- Cost of operating the CBDC
- Unavailability during disasters
- Vulnerability during Cyberattacks

Currently, in the Cryptocurrency world, most Mining Operations have moved from being distributed to being centralized and operated by a few select organizations in highly centralized locations. For example,

*Fundamentally, Bitcoin mining operations ad traditional data centers are similar in the basic design and operational principles. Power must be brought into the building and distributed to the requirement, air distribution systems cool the equipment, and the building provides protection from outdoor conditions and security threats.*<sup>184)</sup>

If this is true for a U.S. CBDC, then what advantage does the CBDC have over the [Real-Time Payments \(RTP\)](#) developed by the [Automated Clearing House \(ACH\) Network](#).

<sup>183)</sup>

Vaibhav Saini, [hackernoon.com](#), [ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms, A complete list/comparison of all Consensus Algorithms](#), 26 June 2-18, Accessed: 7 September 2021 <https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f>

<sup>184)</sup>

Sunbird, [Largest Bitcoin Mining Farms in the World](#), Accessed: 9 May 2022, [https://www.sunbirddcim.com/sites/default/files/Sunbird\\_InfoGraphic\\_Bitcoin.pdf](https://www.sunbirddcim.com/sites/default/files/Sunbird_InfoGraphic_Bitcoin.pdf)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:93\\_recomend:10\\_consensus](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:93_recomend:10_consensus)

Last update: **2022/05/18 00:52**



## 6.11.2 Artificial Intelligence (AI)

[Return to RDT&E](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve use [Research Development Test & Evaluation \(RDT&E\) Funding](#) in developing and perfecting Artificial Intelligence (AI) for use with and alongside a U.S. CBDC. The AI could help in detecting suspicious security and criminal activities. When combined with [Biometrics](#) and [Biometric Authentication](#).

AI could also consider time and geospatial data to make informed decisions about the validity of a proposed transaction.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:93\\_recomend:20\\_ai](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:93_recomend:20_ai)

Last update: **2022/05/17 01:43**



## 6.11.3 Ontologies

[Return to RDT&E](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve use [Research Development Test & Evaluation \(RDT&E\) Funding](#) in developing and perfecting glossaries, taxonomies, and ontologies used to represent the U.S. CBDC, the Intermediaries, and the needs of the Stakeholders. There already exists an OMG Ontology, [Financial Industry Business Ontology \(FIBO\)](#) that probably needs to be extended or updated to handle a U.S. CBDC.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:90\\_recommend:93\\_recomend:30\\_onto](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:90_recommend:93_recomend:30_onto)

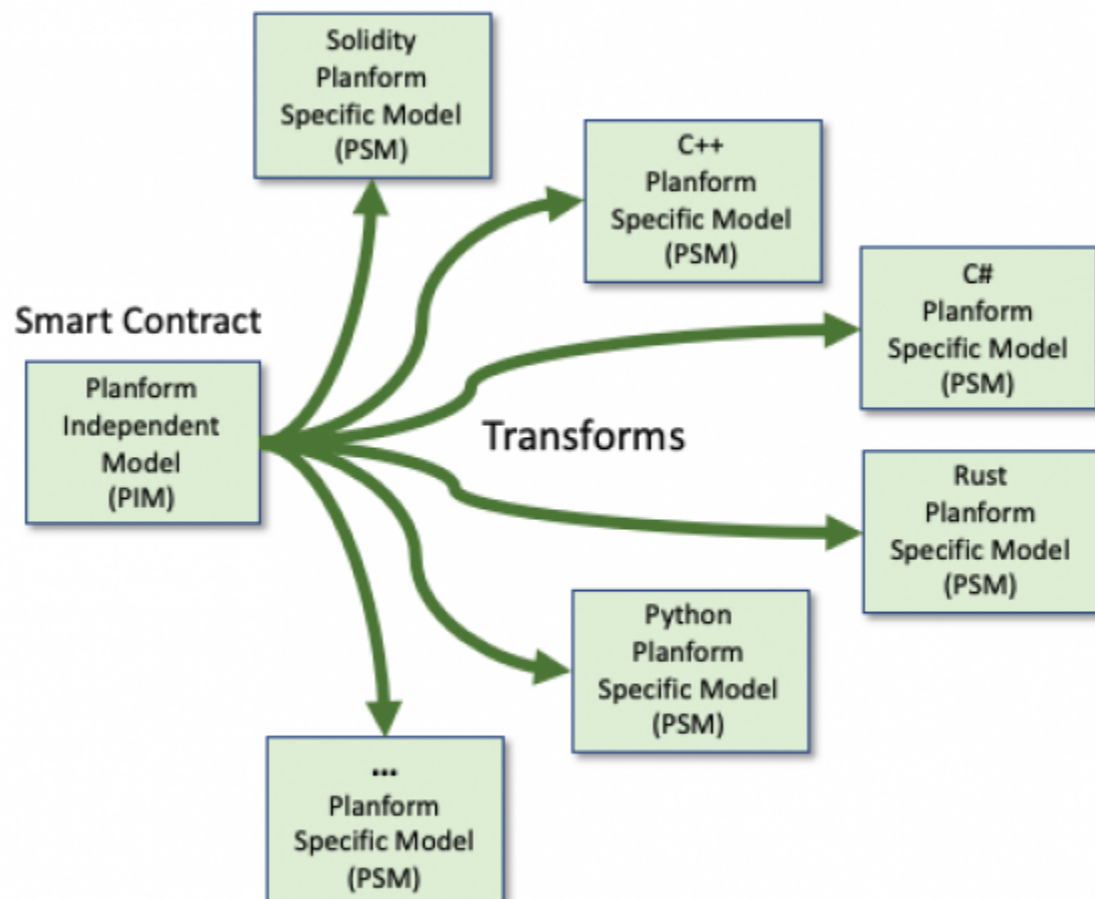
Last update: **2022/05/17 01:43**



## 6.11.4 Smart Contracts

[Return to RDT&E](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve use [Research Development Test & Evaluation \(RDT&E\) Funding](#) in developing and perfecting [Smart Contracts](#). Currently, the *de facto* standard for Smart Contracts is the [Ethereum](#) language called [Solidity](#). See the [Ethereum Solidity Language Specification](#). However, there are shortcomings in the language which could either be updated or replaced with a more comprehensive language and may not even be procedural in nature. For example, the graphically based [Business Process Model And Notation \(BPMN\)](#). Another possibility would be to develop a standardized, [Platform-Independent Model](#) for a Smart Contract [Application Programming Interface \(API\)](#) which could have multiple [Platform Specific Models](#) developed from the PIM.



Creating a Platform Independent Model (PIM) and transforming it into various Platform Specific Models (PSMs)

Figure 51:



From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:93\\_recomend:40\\_smart](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:93_recomend:40_smart)

Last update: **2022/05/18 21:38**



## 6.11.5 Complex Data Models

[Return to RDT&E](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve use [Research Development Test & Evaluation \(RDT&E\) Funding](#) in developing and perfecting how to model data on a blockchain and especially what data to store on a blockchain, what data to store off the blockchain, how to access off-blockchain data (i.e., Oracles).

Most of the data models underlying cryptocurrencies are pretty simple. Generally, it's a balance expressed as a simple unsigned, 256-bit integer. However, the cost of storing data on a blockchain is extremely high in comparison to other methods ( see [OMG DIDO-RA Understanding Gas](#))). The restricted or reduced data storage and processing capability on a Blockchain mean that it will be more difficult to detect Criminal Activity directly on the blockchain. Consequently, it will have to rely on off-block data and processing to be successful. The question is: How will the on-block / off-block data and processes be modeled.

Another issue might be the need for Blockchains to be joined as a federation of blockchains or even a confederation of blockchains. For example, there may be two separate blockchains, one for domestic use and one for international use. The problem might get more complicated than that. There may need to be a blockchain for the purchasing and selling of stocks which is different than one used for retail.

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:93\\_recomend:50\\_test](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:93_recomend:50_test)

Last update: **2022/05/17 01:44**



## 6.11.6 Understanding Gas Implications

[Return to RDT&E](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve invest [Research Development Test & Evaluation \(RDT&E\) Funding](#) in developing and perfecting the concept of [Gas](#) that is a measurement roughly equivalent to computational steps (for Ethereum). Every transaction is required to include a gas limit and a fee that it is willing to pay per gas; miners have the choice of including the transaction and collecting the fee or not. Every operation has a gas expenditure; for most operations, it is ~3-10, although some expensive operations have expenditures up to 700 and a transaction itself has an expenditure of 21000.

For an explanation of what Gas is, how Gas price is determined for processing and for Data Storage, and a detailed example of how the actual costs are calculated, see the OMG DIDO-RA section on [Understanding Gas](#)

In order to successfully operate the U.S. CBDC based on Cryptocurrencies, even if they are [Stablecoins](#), it is important to determine if Gas is necessary and if so how much it will cost and who will pick up the cost of processing. Based on the example provided in the DIDO-RA on Gas costs on Ethereum, the cost is about is approximately 40 Million to 400 Million times more expensive than using [Amazon Web Services \(AWS\)](#).

From:

<https://www.omgwiki.org/CBDC/> - [OMG Central Bank Digital Currency \(OMG-CBDC\) Working Group \(WG\) Wiki](#)

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:90\\_recommend:93\\_recomend:60\\_test](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:90_recommend:93_recomend:60_test)

Last update: **2022/05/17 01:45**



## 6.11.7 Simulation, Training and Testing Environment

[Return to RDT&E](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve invest [Research Development Test & Evaluation \(RDT&E\) Funding](#) in developing and perfecting a Simulation, Training, and Test environment.

This environment should allow for the creation and running of thousands of Distributed Nodes of different types to simulate a real distributed environment in a matter of seconds or at most minutes. The Testing Environment (TE) needs to be able to start from a known starting point each time it is run, especially to support [Regression Testing](#).

This kind of Testing Environment (TE) is different than the [Sandboxes](#) most Cryptocurrencies currently offer. These cryptocurrency sandboxes work on actual distributed systems with a set of collective nodes running on actual networks. This means the rigor of the testing is compromised since the state of the sandbox is a moving target (i.e., it is not the same this time it is run as it was the last time it was run). Additionally, Sandbox testing means the ability to release hostile agents into the environment is extremely limited (who wants to have a hostile agent accidentally release a malicious agent into the wild?). It also limits the testing of the [Network Devices](#) (i.e., hub, switch, etc.) and the use of [HTTP Sniffers](#).

A Testing Environment (TE) can support simulation by allowing the morphology (number and kinds of nodes) of the Environment to be altered and rerun. Although the performance metrics collected during each run would not necessarily reflect the actual metrics during a real deployment, they would be useful relative to each other allowing for an informed decision-making process.

Training Environment leverages the TE by using the Testing Environment as a platform for training people and AI on different well-known scenarios. The TE would be started at a known point each time and the people or the intelligent agents could learn through the use of “what happens if” scenarios. The metrics collected could be used to assess the results.

Using a Testing Environment (TE) from the onset of the CBDC helps fulfill the Non-Functional Requirement for Testability.

**Note:** [Testability](#), Testable, Testing, and Test are not synonyms for each other. Just because a system or program is undergoing testing using various tests does not necessarily mean that the system or program is actually Testable. See section [6.05 Formally Define Non-Functional Requirements](#).

The following sections from the [OMG DIDO Reference Architecture \(DIDO-RA\)](#) could be helpful in understanding the creation of a Test Environment.

- [Detailed discussion of types of Tests](#)
- [Testability](#) Non-Functional Requirement

- [Securability](#) Non-Functional Requirement

Table 121 lists an overview of the types of tests defined by the OMG DIDO-RA. All systems should have [Policies and Procedures](#) in place to improve the quality of the system and increase reliability. Follow the links to get more detail on each test.

The different kinds of tests.

Table 121:

- [Unit Testing](#)
- [Integration Testing](#)
- [End-to-End Testing \(E2E Testing\)](#)
- [Smoke Testing](#)
- [Sanity Testing](#)
- [Regression Testing](#)
- [Acceptance Testing](#)
- [White Box Testing](#)
- [Black Box Testing](#)
- [Interface Testing](#)
- [Interoperability Testing](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:90\\_recommen:93\\_recomend:70\\_test](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:90_recommen:93_recomend:70_test)

Last update: **2022/05/18 00:54**



## 6.11.8 Build Reference Implementation (RI)

[Return to RDT&E](#) [Provide Feedback](#)

The OMG members recommend the Federal Reserve invest [Research Development Test & Evaluation \(RDT&E\) Funding](#) in developing and perfecting a [Reference Implementation \(RI\)](#) for all standards developed for the U.S. Based CBDC.

See: [6.12 Defining the Appropriate Standards or Specifications](#)

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:04\\_doc:90\\_recommend:93\\_recomend:80\\_test](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:04_doc:90_recommend:93_recomend:80_test)

Last update: **2022/05/17 01:46**



# 6.12 Defining the Appropriate Standards or Specifications

[Return to Recommendations](#) [Provide Feedback](#)

The OMG members recommend to the Federal Reserve:

- Rely on formal, accredited [Standard](#) and [Specifications](#) in developing and perfecting a U.S. based CBDC. Although it is possible to use *de facto standards*, these are generally tied to implementations rather than to the concepts and agreements of how to work together. This can be a form of [Vendor Lock-in](#).
- Consider the [Non-Functional Requirements](#) of [Portability](#) and specifically [Replaceability](#)
- Create Standards and Specifications within a [Standards Developing Organization \(SDO\)](#) or a [Voluntary Standards Consensus Body \(VSCB\)](#).
- Using [Open Source Software \(OSS\)](#) to be used as a [Reference Implementation\(RI\)](#).
- Provide Reference Implementations(RIs) by using [Research Development Test & Evaluation \(RDT&E\)](#) process of [Small Business Innovation Research \(SBIR\)](#) and/or [Small Business Technology Transfer \(STTR\)](#) process.

The following definitions are provided here as a convenience.

<b>Standard</b>	A <b>Standard</b> is a set of technical definitions and guidelines. In essence, it is a <i>how-to</i> instructions for designers, manufacturers, and users. Standards promote safety, reliability, productivity, and efficiency in almost every industry that relies on engineering components or equipment. Standards can run from a few paragraphs to hundreds of pages and are written by experts with knowledge and expertise in a particular field who sit on many committees.
<b>Specification</b>	A <b>Specification</b> is a document stating requirements. A specification can be related to activities (e.g. procedure document, process Specification, and test Specification), or products (e.g. product Specification, performance Specification, and drawing).

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:04\\_doc:90\\_recommend:92\\_stds](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:04_doc:90_recommend:92_stds)

Last update: 2022/05/19 01:54



# Appendix A: Acronyms

<a href="#">Return to Appendices</a> <a href="#">Provide Feedback</a>	
Acronym	Expansion
ACH	Automated Clearing House
AI	Artificial Intelligence
AMF	Autorité des marchés financiers
AML	Anti-Money Laundering
API	Application Programming Interface
BaFin	Federal Financial Supervisory Authority
BoE	Bank of England
CAFRA	Civil Asset Forfeiture Reform Act
CBDC	<a href="#">Central Bank Digital Currency</a>
CBRC	China Banking Regulatory Commission
CCCRA	California Consumer Credit Reporting Agencies Act
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CHIP	Children's Health Insurance Program
CIRC	China Insurance Regulatory Commission
CSRC	China Securities Regulatory Commission
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIDO	Distributed Immutable Data Object
DPPA	Driver's Privacy Protection Act of 1994
Doj	U.S. Department of Justice
EU	European Union
FACTA	Fair and Accurate Credit Transactions Act
FAR	Federal Acquisition Regulation
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCA	Financial Conduct Authority
FCPA	Foreign Corrupt Practices Act
FCRA	Fair Credit Reporting Act
FDCPA	Fair Debt Collection Practices Act
FDIC	Federal Deposit Insurance Corporation
FEMA	Federal Emergency Management Agency
FINMA	Swiss Financial Market Supervisory Authority
FINRA	Financial Industry Regulatory Authority
FSA	UK Financial Services Agency
GDPR	General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act
GSC	Global StableCoin



<b>Acronym</b>	<b>Expansion</b>
IBBI	Insolvency and Bankruptcy Board of India
IRDAI	Insurance Regulatory and Development Authority of India
IRS	Internal Revenue Service
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
MBSE	Model-Based Systems Engineering
MCLA	Money Laundering Control Act of 1986
MiFID II	Markets in Financial Instruments Directive II
NAIC	National Association of Insurance Commissioners
NIST	National Institute of Standards and Technology
NCUA	National Credit Union Administration
NOAA	National Oceanic and Atmospheric Administration
OCC	Office of the Comptroller of the Currency
OMG	Object Management Group
OTA	Other Transaction Authority
P&P	Policies and Procedures
PFRDA	Pension Fund Regulatory and Development Authority
PRA	UK Prudential Regulation Authority
PWG	President's Working Group on Financial Markets
RA	Reference Architecture
RBI	Reserve Bank of India
RFPA	Right to Financial Privacy Act of 1978
RI	Reference Implementation
RICO	Racketeer Influenced and Corrupt Organizations Act of 1970
RDT&E	Research Development Test & Evaluation
RTP	<a href="#">Real-Time Payments</a>
SBIR	Small Business Innovation Research
SDO	Standards Development Organization
SEBI	Securities and Exchange Board of India
SEC	U.S. Securities and Exchange Commission
SIG	Special Interest Group
SMS	Short Message Service
STTR	Small Business Technology Transfer
SUA	Specified Unlawful Activity
TANF	Temporary Assistance for Needy Families
TODO	Talk Openly Develop Openly
TVPA	Trafficking Victims Protection Act
TVPRA	Trafficking Victims Protection Reauthorization Act
UAF	Unified Architecture Framework
UK	United Kingdom
UNDP	United Nations Development Programme
UNODC	United Nations Office on Drugs and Crime

<b>Acronym</b>	<b>Expansion</b>
VPPA	Video Privacy Protection Act
VSCB	Voluntary Standards Consensus Body

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:8\\_append:10\\_acronyms:start](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:8_append:10_acronyms:start)

Last update: **2022/05/17 06:42**



# Appendix B: Glossary

[Return to Apedices](#) [Provide Feedback](#)

**Note:** If you need a definition of terms not found within this Glossary, please refer to the [OMG DIDO-RA Glossary](#).

• **Note:** You can add new questions [here](#)

- [Central Bank Digital Currency \(CBDC\)](#)
- [Central Bank Money](#)
- [Commercial Bank Money](#)
- [Consumer Privacy](#)
- [Financial Crimes](#)
- [Identity-verified](#)
- [Intermediated Model](#)
- [Nonbank Money](#)
- [Privacy-Protected](#)
- [Real-Time Payments \(RTP\)](#)
- [Transferable](#)

## Add a new term

[Return to Top](#)

Create a Glossary entry starting **Word or Expression** →

From: <https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link: [https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:8\\_append:20\\_glossary:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:8_append:20_glossary:start)

Last update: 2022/05/19 01:57



# Central Bank Digital Currency (CBDC)

[Return to Glossary](#)

**Central Bank Digital Currency (CBDC)** is defined as a digital liability of a central bank that is widely available to the general public. In this respect, it is analogous to a digital form of paper money.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc;public:cbdc\\_omg:8\\_append:20\\_glossary:cbdc](https://www.omgwiki.org/CBDC/doku.php?id=cbdc;public:cbdc_omg:8_append:20_glossary:cbdc)

Last update: **2022/05/16 18:21**



# Central Bank Money

[Return to Glossary](#)

**Central Bank Money** is a liability of the central bank. In the United States, central bank money comes in the form of physical currency issued by the Federal Reserve and digital balances held by commercial banks at the Federal Reserve.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc\\_omg:8\\_append:20\\_glossary:central\\_bank\\_money](https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:8_append:20_glossary:central_bank_money)

Last update: **2022/05/18 00:56**



# Commercial Bank Money

[Return to Glossary](#)

**Commercial Bank Money** is the digital form of money that is most commonly used by the public. Commercial bank money is held in accounts at commercial banks.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc\\_omg:8\\_append:20\\_glossary:commercial\\_bank\\_money](https://www.omgwiki.org/CBDC/doku.php?id=cbbc:public:cbbc_omg:8_append:20_glossary:commercial_bank_money)

Last update: **2022/05/16 18:21**



# Consumer Privacy

[Return to Glossary](#)

**Consumer Privacy** is a general-purpose CBDC that generates data about users' financial transactions in the same ways that [Commercial Bank](#) and [Nonbank Money](#) generates such data today. In the CBDC [Intermediated Model](#) that the Federal Reserve would consider, intermediaries would address privacy concerns by leveraging existing tools.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:8\\_append:20\\_glossary:consumer\\_privacy](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:8_append:20_glossary:consumer_privacy)

Last update: **2022/05/16 18:21**



# Financial Crimes

[Return to Glossary](#)

**Financial Crimes** are money laundering and the financing of terrorism. Financial institutions must comply with a robust set of rules that are designed to combat **Financial Crimes**. These rules include customer due diligence, record keeping, and reporting requirements.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:8\\_append:20\\_glossary:financial\\_crimes](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:8_append:20_glossary:financial_crimes)

Last update: 2022/05/16 18:21





# Identity-verified

[Return to Glossary](#)

**Identity-verified** is ...

Financial institutions in the United States are subject to robust rules that are designed to combat money laundering and the financing of terrorism. A CBDC would need to be designed to comply with these rules. In practice, this would mean that a CBDC intermediary would need to **verify** the **identity** of a person accessing CBDC, just as banks and other financial institutions currently verify the identities of their customers.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg\\_8\\_append:20\\_glossary:identity-verified](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg_8_append:20_glossary:identity-verified)

Last update: **2022/05/16 18:21**



# Intermediated Model

[Return to Glossary](#)

Under an **Intermediated Model**, the private sector would offer accounts or digital wallets to facilitate the management of CBDC holdings and payments. Potential intermediaries could include commercial banks and regulated **Nonbank** financial service providers, and would operate in an open market for **Central Bank Digital Currency (CBDC)** services. Although commercial banks and **nonbanks** would offer services to individuals to manage their CBDC holdings and payments, the CBDC itself would be a liability of the Federal Reserve.

An **Intermediated Model** would facilitate the use of the private sector's existing privacy and identity-management frameworks; leverage the private sector's ability to innovate; and reduce the prospects for destabilizing disruptions to the well-functioning U.S. financial system.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:8\\_append:20\\_glossary:intermediated](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:8_append:20_glossary:intermediated)

Last update: **2022/05/16 18:21**



# Nonbank Money

[Return to Glossary](#)

**Nonbank Money** is digital money held as balances at nonbank financial service providers. These firms typically conduct balance transfers on their own books using a range of technologies, including mobile apps.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:8\\_append:20\\_glossary:nonbank\\_money](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:8_append:20_glossary:nonbank_money)

Last update: **2022/05/16 18:21**



# Privacy-Protected

[Return to Glossary](#)

**Privacy-Protected** means that the [Central Bank Digital Currency \(CBDC\)](#) protecting consumer privacy is critical. Any CBDC would need to strike an appropriate balance, however, between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:8\\_append:20\\_glossary:privacy-protected](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:8_append:20_glossary:privacy-protected)

Last update: **2022/05/16 18:21**



# Real-Time Payments (RTP)

[Return to Glossary](#)

**Real-Time Payments (RTP)** is a network from The Clearing House. It is a real-time payments' platform that all federally insured U.S. depository institutions are eligible to use for payments innovation. With mobile technology and digital commerce driving the need for safer and faster payments in the U.S., financial institutions of all sizes are taking advantage of the RTP network's capabilities to create or enhance digital services for their corporate and retail customers.

Source: <https://www.theclearinghouse.org/payment-systems/rtp>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:8\\_append:20\\_glossary:rtp](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:8_append:20_glossary:rtp)



Last update: **2022/05/16 18:21**

# Transferable

[Return to Glossary](#)

For a CBDC to serve as a widely accessible means of payment, it would need to be readily **Transferable** between customers of different intermediaries. The ability to transfer value seamlessly between different intermediaries makes the payment system more efficient by allowing money to move freely throughout the economy.

Source: <https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc\\_omg:8\\_append:20\\_glossary:transferable](https://www.omgwiki.org/CBDC/doku.php?id=cdbc:public:cdbc_omg:8_append:20_glossary:transferable)

Last update: **2022/05/16 18:21**



# Appendix C: Other Transaction Authority (OTA)

[Return to Apedices](#) [Provide Feedback](#)

## Overview

[Return to Top](#)

**Other Transaction Authority (OTA)** is the authority of a US Agency to use [Other Transactions \(OTs\)](#). Once the agency has OTA, it can establish an Other Transaction Agreement (OTA)

The two terms are often incorrectly used synonymously.

1. The **Other Transaction Authority (OTA)** is granted to be able to use Other Transactions and is generally considered for use in RTD&E contracts.
2. The US Agency with OTA then can then appoint a Government Contracting Office as an **Agreement Officer**
3. The **Agreement Officer** then creates an **Open Transaction Agreement (OTA)** as the basis to conduct business
4. OTAs are awarded in several ways<sup>181)</sup>:
  - One way is through a direct award process such as a Request for Proposal (RFP), a Broad Agency Announcement (BAA), or through a follow-on to an existing OTA.
  - A second mechanism is through a consortium-based OTA. A consortium is an association formed by multiple parties for the purpose of participating in a common activity or pooling resources to achieve a common goal. Consortium-based OTAs allow multiple companies (traditional defense contractors and NDCs) and academia to collaborate with government customers and to partner with each other to accelerate innovation.

The most important aspect of an OTA is the [Other Transactions \(OTs\)](#) provisions, which are a legally binding, streamlined acquisition process. Only Congressionally-designated Federal agencies can use to procure innovative technology (e.g., prototypes and other [Research Development Test & Evaluation \(RDT&E\) projects](#)) while avoiding burdensome processes normally associated with government contracts, grants, and cooperative agreements such as the [Federal Acquisition Regulation \(FAR\)](#) and agency supplements, like the [Defense Federal Acquisition Regulation Supplement \(DFARS\)](#). This makes OTA efforts more similar to the commercial sector contracts in that they offer a flexible and less regulated approach to connect government with industry for innovative solutions.<sup>182)</sup>

The use of OTs and OTAs are specially designed for government departments and agencies to use and manage [Research Development Test & Evaluation \(RDT&E\) Funding](#).

Table 124 provides a list of Federal Agencies with Congressional OTAs.

**Note:** The inclusion of non-DoD Agencies.

Federal Agencies with Congressional OT Authorization<sup>183)</sup>

Table 124:

Agency	OT Authority	Agency Specific OT Requirements, Limitations, and Restrictions
<b>NASA</b>	51 U.S.C. § 20113(e)	No limitations or restrictions.
<b>DOD</b> <sup>184)</sup> , <sup>185)</sup>	1. 10 U.S.C. § 2371 2. 10 U.S.C. § 2371b	Authorizes Research OTs and Prototype OTs. See DoD Other Transactions for detailed requirements, limitations, and restrictions.
<b>DOE</b>	42 U.S.C. § 7256	1. Limited to RD&D projects. A cost-sharing agreement is required. 2. Authorized for RD&D and prototype projects.
<b>HHS</b>	42 U.S.C. § 247-7e	1. Limited to RD&D projects. A cost-sharing agreement is required. 2. Authorized for RD&D and prototype projects.
<b>DHS</b>	6 U.S.C. § 391	Prototype projects require a non-traditional contractor and cost sharing agreement.
<b>DOT</b>	49 U.S.C. § 5312	Limited to RD&D focused on public transportation.
<b>FAA</b>	49 U.S.C. § 106(l)	No limitations or restrictions.
<b>TSA</b>	49 U.S.C. § 114(m)	No limitations or restrictions.
<b>DNDO</b>	6 U.S.C. § 596	No limitations or restrictions.
<b>ARPA-E</b>	42 U.S.C. § 16538	No limitations or restrictions.
<b>NIH</b>	1. 42 U.S.C. § 285b-3 2. 42 U.S.C. § 284n 3. 42 U.S.C. § 287a	Limitations and restrictions differ based on specific research programs.

## Recommendations

[Return to Top](#)

The [Object Management Group](#) recommends the US Federal Reserve continues to pursue **P0011** and **P0030** but as two separate issues. It is essential the Federal Reserve pursues a CBDC (i.e., **P0011**) and makes recommendations based on using [Data, Information, Knowledge, Understanding and Wisdom](#) gathered during the RTD&E efforts (i.e., **P0030**). CBDC is a large problem with many moving parts, all of which require a lot of systems analysis, engineering, and simulation in order to ensure public confidence:

*For a nation's economy to function effectively, its citizens must have confidence in its money and payment services. The Federal Reserve, as the nation's central bank, works to maintain the public's confidence by fostering monetary stability, financial stability, and a safe and efficient payment system. from the **Executive Summary** provided in the [Money, and Payments: The U.S. Dollar in the Age of Digital Transformation](#) White Paper*

Pursuing a CBDC that is flawed could ultimately inflict more damage than it is worth.



After the Federal Reserve obtains OT Authority, the OMG further recommends that an **Other Transaction (OT) Consortium** be established. An OT Consortium is a formal relationship between a government sponsor (i.e., Federal Reserve) and a collection of traditional and non-traditional vendors, non-profit organizations, and academia aligned to a technology domain area (i.e., cyber, space, undersea, propulsion) that are managed by a single entity, and focused on innovative solutions to government technology challenges that meet the intended scope and purpose of other transactions.

OT Consortium is based on the following [OT Consortium Model](#):



The Existing OT Constoria Model  
Figure 52:

Generally, an OT Consortium has three components:

- Government Sponsor and Contracting Office
- Consortium Manager
- Consortium (i.e., Stakeholders)

**Note:** Sometimes, the government sponsors prefer to manage a consortium in-house rather than hire an industry Consortium Manager or Consortium Management Firm.

The Consortium Manager is awarded an OT agreement by the government (base OT agreement) and manages OTs awarded to its consortium member organizations (project OT agreements) under the base agreement. In the [OMG Distributed Immutable Data Object Reference Architecture \(DIDO-RA\)](#), this highest level (i.e., OT Consortium) is referred to as the [Ecosphere](#) which would roughly follow the steps outlined in [Steps for Establishing an Ecosphere](#). Also see [DIDO-RA on Legal Documents](#) for a discussion of how Ecosphere, Ecosystem, and Domain are related. The overall intent is the Ecosphere has the responsibility to external entities (i.e., sponsors). The OT Consortia (i.e., Ecosphere) can create any number of Ecosystems and Domains as is needed. It is recommended that the Ecosystems create and are responsible for Domains that fall under their auspices; however, the Policy and Procedures (P&P) may require the Ecosphere's approval for creation.

Table [125](#) summarizes the relationship between the Ecosphere, Ecosystem, and Domains. Some P&P may require every Ecosystem and Domain to have its own sub-charter which a narrower scope than the Ecosphere. See [OMG DIDO-RA, 3.2 Legal Documents](#)

Documents required to Create and Govern a DIDO CoI

Table 125:

<b>DIDO Col</b>	<b>Charter</b>	<b>Bylaws</b>	<b>Policies and Procedures</b>
<b>Ecosphere</b>	Yes(§)	Yes(†)	Yes(‡)
<b>Ecosystem</b>	Subcharter of Ecosphere	covered by Ecosphere	covered by Ecosphere + extensions
<b>Domain</b>	Subcharter of Ecosystem	covered by Ecosphere	covered by Ecosphere + extensions from Ecosystem + local

(§) Initially, a legal statement created by the founders of the organization that lays out the goals, missions, and officers for the organization

(†) Legal document reviewed by lawyers from all the participating parties

(‡) Some *Policies and Procedures* may be mandated by law (i.e., discrimination, ADA, Safety, etc. while others may be added by local governing boards and should be drafted/reviewed by lawyers of all participating parties

There are many existing examples of Other Transaction Authorities (OTAs) that are already in existence within the US Government. Table 126 provides a detailed list originally painstakingly developed by Capture 2 Proposal<sup>186)</sup>. There is an excellent article by Stephen Speciale<sup>187)</sup>

*OTAs are binding agreements between Defense Department organizations and industry partners that are different than Federal Acquisition Regulation contracts, grants, and cooperative agreements. While they are an innovative and flexible option that is not subject to all acquisition laws and regulations, they require vigorous program management. The intent of OTAs is to leverage commercial technologies for military purposes, improve the nation’s industrial base and allow for more cost-effective and affordable solutions without extreme bureaucracy. Opportunities are available to traditional defense industry partners and nontraditional defense contractors, such as academia, non-profits, and other small businesses.*

*Failing to plan is planning to fail. Since parties can negotiate and tailor many OTA elements, it is critical for all parties involved to complete sound planning efforts prior to execution. Also, because they promote “outside the box” business practices, risk management is not a choice, but the backbone of the effort from cradle to grave. Agencies should start planning with a clear needs statement or defined problem supporting a capability gap.*

List of Other Transaction Authorities (OTAs) developd by Capture 2 Proposal<sup>188)</sup>

Table 126:

<b>Consortium</b>	<b>Membership Firm</b>	<b>Description</b>
<b>Advanced Manufacturing, Materials, and Processes (AMMP)</b>	NCMS	Advance and enable additive manufacturing to create next-generation manufacturing breakthroughs
<b>American Metalcasting Consortium (AMC)</b>	ATI	An industry-led consortium developing new technologies and processes that support the DLA in the procurement of critical cast parts.

<b>Consortium</b>	<b>Membership Firm</b>	<b>Description</b>
<b>Aviation and Missile Research, Development and Engineering Center (AMRDEC)</b>	US Army Contracting Command	The development and maturation of guided-missile technologies, manufacturing, and enabling/disruptive technologies, and aviation technologies.
<b>Aviation and Missile Technology Consortium (AMTC)</b>	ATI	Develop and transition Army aviation and missile manufacturing technologies, and integrate advanced technologies, techniques and processes into future effective weapon systems.
<b>Border Security Technology Consortium (BSTC)</b>	ATI	Research, development, prototyping, and piloting initiatives to meet border security requirements and close capability gaps.
<b>Center for Naval Metalworking (CNM)</b>	ATI	To develop and deploy innovative metalworking and related manufacturing technologies to reduce the cost and time to build and repair key U.S. Navy ships and weapons platforms.
<b>Composites Manufacturing Technology Center (CMTC)</b>	ATI	An ONR Center of Excellence developing composites for advanced weapons systems.
<b>Consortium for Command, Control, and Communications in Cyberspace (C5)</b>	CMG	C5 is a consortium composed of leading companies and institutions in the C4ISR and cyber technology sectors.
<b>Consortium For Energy, Environment, And Demilitarization (CEED)</b>	CMG	CEED is a consortium composed of leading companies and institutions in the Energy, Environmental, and Demilitarization technology sectors.
<b>Consortium for Execution of Rendezvous and Servicing Operations (CONFERS)</b>	ATI	Research, develop, and publish non-binding, consensus-derived technical and operations standards for OOS and RPO. These standards would provide the foundation for a new commercial repertoire of robust space-based capabilities and a future in-space economy.
<b>Cornerstone</b>	Rock Island Arsenal	A modern Industrial Base that integrates traditional and emerging sectors to respond at will to National Security Requirements.
<b>Countering Weapons of Mass Destruction Consortium (CWMD)</b>	ATI	Developing technologies to detect, prevent, and protect against weapons of mass destruction.
<b>Cyber Apex Solutions Consortium</b>	Cyber Apex Solutions, LLC	Applied cybersecurity research focused on filling the security gaps of critical infrastructure in the United States of America.
<b>Defense Automotive Technologies Consortium (DATC)</b>	SAE International	Develop and transition advanced automotive technologies to all branches of military and government agencies.

<b>Consortium</b>	<b>Membership Firm</b>	<b>Description</b>
<b>Department of Defense Ordnance Technology Consortium (DOTC)</b>	ATI	Integrate the DoD Ordnance community to work collaboratively in RDT&E of prototype solutions to the advance and transition ordnance systems, subsystems, and component technologies.
<b>Forging Defense Manufacturing Consortium (FDMC)</b>	ATI	Teaming the US forging industry with the DoD to address supply chain challenges and research needs.
<b>Information Warfare Research Project (IWRP)</b>	ATI	Developing and implementing advanced Information Warfare technology solutions.
<b>Medical-Chemical Biological Radiological Nuclear (CBRN) Defense Consortium (MCDC)</b>	ATI	Supporting the DoD's medical, pharmaceutical, and diagnostic requirements to enhance the effectiveness of military personnel.
<b>Medical Technology Enterprise Consortium (MTEC)</b>	ATI	Provide cutting-edge technologies to help protect, treat and optimize Warfighters' health.
<b>Natick Soldier Research, Development, and Engineering Center (NSRDEC)</b>	US Army-Aberdeen Proving Ground	Maximize the Warfighter's Survivability, Sustainability, Mobility, Combat Effectiveness and Field Quality of Life by Treating the Warfighter as a System.
<b>National Advanced Mobility Consortium (NAMC)</b>	NAMC	To provide the Government with ready, quality access to the broadest population of U.S. ground vehicle system (GVS), sub-system, and component technology developers and providers.
<b>National Armaments Consortium (NAC)</b>	ATI	The focal point for armaments system technology research and development across the DoD.
<b>National Center for Manufacturing Sciences (NCMS)</b>	NCMS	A cross-industry technology development consortium, dedicated to improving the competitiveness and strength of the U.S. industrial base
<b>National Center for Simulation (NCS)</b>		Promote and support modeling, simulation, and training (MS&T). Registered as Training and Simulation Technology Consortium, Inc. (dba National Center for Simulation)
<b>National Shipbuilding Research Program (NSRP)</b>	ATI	A Navy-sponsored, industry-led collaboration of shipyards that is reducing the cost of building and repairing Navy ships.
<b>National Spectrum Consortium (NSC)</b>	ATI	Develop technologies that broaden access to and use of the electromagnetic spectrum.
<b>Naval Aviation Systems Consortium (NASC)</b>	CMG	Support the technology needs of the Naval Air Warfare Centers (NAWCs) and the Naval Air Systems Command (NAVAIR)

<b>Consortium</b>	<b>Membership Firm</b>	<b>Description</b>
<b>Naval Shipbuilding and Advanced Manufacturing Center (NSAMC)</b>	ATI	Developing and deploying advanced manufacturing technologies to reduce the cost and time required to build and repair Navy ships.
<b>SAE Industry Technologies Consortia (SAE ITC®)</b>	SAE International	Drive innovative solutions to key industry challenges.
<b>Sensors, Communications, and Electronics Consortium (SCEC)</b>	SOSSEC Inc.	Conduct research, development, and testing in cooperation with the Government, leading to technology demonstrations and prototype projects in the sensors, communications, and electronics sciences and other related fields.
<b>Space Enterprise Consortium® (SpEC)</b>	ATI	Reducing risk and increasing constellation refresh rates to improve the availability of new technology on-orbit and to enhance system responsiveness and survivability.
<b>System of Systems Consortium (SOSSEC)</b>	SOSSEC Inc.	Technology agnostic approaches that capture the best-of-breed solutions.
<b>Strategic &amp; Spectrum Missions Advanced Resilient Trusted Systems ((S2MARTS ))</b>	NSTXL	The S2MARTS OTA (pronounced “SMARTS”) is designed to refine strategies, management planning activities, and implement integrated, complementary solutions that enable broader Department of Defense (DoD) access to commercial state-of-the-art EMS technologies, advanced microelectronics, radiation-hardened (RAD-HARD) and strategic missions hardware.
<b>Training and Readiness Accelerator (TRex)</b>	NSTXL	To expedite the development, demonstration, and delivery of cutting edge technology capabilities in support of modeling, simulation, and training (MST) needs of the U.S. Department of Defense.
<b>Undersea Technology Innovation Consortium (UTIC)</b>	ATI	Rapid development, prototyping, and commercialization of innovative undersea and maritime technology.
<b>Vertical Lift Consortium (VLC)</b>	ATI	Develop and transition innovative vertical lift technologies to meet Warfighter needs.
<b>AFLCMC Consortium Initiative (ACI)</b>	SOSSEC Inc.	Prototyping projects might include any topic generally consistent with the research, development, test, and evaluation of within prototyping projects of the AFLCMC mission sets.
<b>Cyberspace Operations Broad Responsive Agreement (COBRA)</b>	SOSSEC Inc.	Establish defense-in-depth across the entirety of cyberspace by simultaneously combining DCO capabilities at global, regional and local levels using a layered and adaptive approach.

<b>Consortium</b>	<b>Membership Firm</b>	<b>Description</b>
<b>Defense Electronics Consortium (DEC)</b>	USPAE	The DEC identifies challenges, needs, and opportunities in defense electronics, which has been impacted by the contraction of U.S. electronics manufacturing and other factors.
<b>Defense Innovation Unit (DIU)</b>	DIU	DIU is the only DoD organization focused exclusively on fielding and scaling commercial technology across the U.S. military at commercial speeds.
<b>Defense Technological Information Center Energy OTA (DTIC)</b>	NSTXL	Technical areas germane to this OTA include cyber, advanced materials, sensors, and biomedical challenges. The ceiling on this OTA has been reached and it is no longer accepting new projects. It does however continue to execute on several prototype projects/Ceiling reached. No longer accepting new projects. which are nearing successful completion.
<b>DHS Silicon Valley Innovation Program (SVIP)</b>	DHS	Incentivize product developers to open the aperture of their development roadmaps to include homeland security solutions. Opportunities posted on sam.gov.
<b>Engineer, Research, and Development Center (ERDC)</b>	SOSSEC Inc.	Performs prototype projects within the following focus areas as they relate to Military Engineering.
<b>Expeditionary Warfare Consortium (EWC)</b>	ARA	Develop innovative products, prototypes, and solutions to meet the expeditionary warfare needs of the Naval Surface Warfare Center.
<b>Future Airborne Capability Environment (FACE™)</b>	The Open Group	Define an open avionics environment for all military airborne platform types.
<b>Govmates Consortium</b>	ATI	An enterprise solution to the Federal Government. Rather than specializing in technology silos, members of this consortium have capabilities spanning nearly every technology vertical.
<b>Nano-Bio Manufacturing Consortium (NBMC)</b>	SEMI	Raises the readiness levels of nano- and bio-technologies.
<b>National Geospatial-Intelligence Agency (NGA)</b>	SOSSEC Inc.	Drive innovative and transformational change into the National System for Geospatial-Intelligence (NSG) and Allied System for Geospatial-Intelligence (ASG) environments.
<b>National Offshore Wind Research and Development Consortium</b>		Reduce the Levelized cost of energy (LCOE) of offshore wind in the U.S. while maximizing other economic and social benefits.
<b>National Security Technology Accelerator (NSTXL)</b>	NSTXL	Support of the Warfighter mission. Management firm-level access to all of their OTAs (S2MARTS, TReX, SpEC).



<b>Consortium</b>	<b>Membership Firm</b>	<b>Description</b>
<b>Naval Surface Technology and Innovation Consortium (NSTIC)</b>	ATI	Supporting naval surface technology innovation across a broad range of technology areas and disciplines.
<b>Nuclear Science and Security Consortium (NSSC)</b>	NNSA	Develop a new generation of laboratory-integrated nuclear experts.
<b>Open System Acquisition Initiative (OSAI)</b>	SOSSEC Inc.	Produce prototypes in command, control, communications, and cyber, intelligence, surveillance, and reconnaissance (C4ISR) that increase the efficiency of Government, industry and academia capabilities in information systems proposed to be acquired or developed by the Department of Defense (DOD), and to reduce the cost of defense information systems technology.
<b>Propulsion Directorate Consortium Initiative (PCI)</b>	SOSSEC Inc.	Perform critical research, development, testing, and evaluation within prototyping projects addressing propulsion needs and the future of the propulsion enterprise.
<b>Sensor Open Systems Architecture (SOSA Consortium)</b>	SOSA	The SOSA Consortium is creating open system reference architectures applicable to military and commercial sensor systems and a business model that balances stakeholder interests.
<b>Supply Chain Consortium Initiative (SCCI)</b>	SOSSEC Inc.	Perform critical research, development, test, and evaluation within prototyping projects addressing 448th Supply Chain Management Wing (SCMW), to include other organizations in the Air Force Material Command (AFMC) or strategic partners, needs and the future of these enterprises.
<b>University Consortium for Applied Hypersonics (UCAH)</b>	UCAH	Deliver the innovation and workforce needed to advance modern hypersonic flight systems in support of the national defense.

181)

Benjamin Schwartz, and Bill Greenwalt, The Chertoff Group, OTHER TRANSACTION AUTHORITY AND THE CONSORTIA-BASED ACQUISITION MODEL: A VALUABLE TOOL FOR RAPID DEFENSE INNOVATION, 2020, Accessed: 14 March 2022, [https://www.chertoffgroup.com/hubfs/TCG\\_Other%20Transaction%20Authority%20r010821\\_REVISION\\_D.pdf](https://www.chertoffgroup.com/hubfs/TCG_Other%20Transaction%20Authority%20r010821_REVISION_D.pdf)

182)

American Council for Technology-Industry Advisory Council (ACT-IAC), Other Transaction Authority - Best Practices for Industry and Government, 10 July 2020, Accessed: 11 March 2022, [https://www.actiac.org/system/files/OTA\\_1.pdf](https://www.actiac.org/system/files/OTA_1.pdf)

183)

Other Transaction Authority (OTA), Acquisition in the Digital Age (AIDA), MITRE.org, Accessed: 27 February 2022, <https://aida.mitre.org/OTA/>

184)

Section 815 of the FY 2016 NDAA defines a non-traditional defense contractor as an entity that is

not currently performing and has not performed, for at least the one-year period preceding the solicitation of sources by the DoD for the procurement or transaction, any contract or subcontract for the DoD that is subject to the full coverage under the cost accounting standards prescribed pursuant to Section 1502 of title 41 and the regulations implementing such section.

<sup>185)</sup>

Section 815 of the FY 2016 NDAA replaced section 845 of the FY 1994 NDAA (repealed) and provided DoD with permanent authority for prototypes, as well as increased dollar threshold approval levels for prototype projects, the amended criterion for OTA eligibility, and allows a prototype project to transition to the award of a follow-on production contract.

<sup>186)</sup> , <sup>188)</sup>

Capture 2 Proposal, Accessed: 26 February 2022),

<https://capture2proposal.com/consortiums-supporting-government-other-transaction-authority-ota-opportunities/>

<sup>187)</sup>

Stephen Speciale, National Defense, Other Transactions – Best Practices to Enable Success, 15 April 2020, Accessed: 27 February 2022,

<https://www.nationaldefensemagazine.org/articles/2020/4/15/other-transactions-best-practices-to-enable-success>

From:

<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:

[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:8\\_append:50\\_other:start](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:8_append:50_other:start)



Last update: **2022/05/18 21:38**



# Appendix D: Model-Based Systems Engineering (MBSE)

[Return to Apedices](#) [Provide Feedback](#)

## Introduction

*For more than forty years, the practice of systems engineering followed a linear path: requirements are documented first, followed by analysis, and then conceptual design, a process repeated through the development life cycle. However, regardless of the engineering process employed—waterfall, incremental, iterative, spiral, and even sprint-based — the lack of integration from one phase to another in the cycle results in longer delivery times and increases costs to correct errors introduced at transition points.*

*Model-Based Systems Engineering (MBSE)<sup>193)</sup> is an initiative in the systems engineering community that uses model-based descriptions and transformations so that work occurs concurrently. Requirements collection, analysis, and specifications are performed at the same time as conceptual design. MBSE is practiced across many industries around the globe. For example, it was used to develop the world's largest telescopes, propulsion engines for fighter jets, and autonomous driving cars.*

## Value Proposition


*MBSE is often contrasted with a more traditional document-based approach to systems engineering where system information is spread across many document-based artifacts (hand-written text documents, spreadsheets, and drawings). MBSE brings information together into a cohesive integrated model of the system that:*

- *Enhances precision, consistency, and traceability;*
- *Includes behavioral analysis, system architecture, requirement traceability, performance analysis, simulation, test, etc.;*
- *Formalizes the practice of systems development through the use of models;*
- *Integrates information across discipline-specific engineering tools, including hardware and software design, analysis, simulation, and test; and*
- *Facilitates shared understanding of the system among the development team resulting in:*
  - a) *quality/productivity improvements and lower risk;*
  - b) *rigor and precision;*
  - c) *ongoing communications among development team and customer; and*
  - d) *management of complexity.*

<sup>193)</sup>

*“Model-based systems engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle phases.” INCOSE SE Vision 2020 (INCOSE-TP-2004-004-02), Sept 2007 MBSE*

From:  
<https://www.omgwiki.org/CBDC/> - **OMG Central Bank Digital Currency (OMG-CBDC) Working Group (WG) Wiki**

Permanent link:   
[https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc\\_omg:8\\_append:60\\_mbse](https://www.omgwiki.org/CBDC/doku.php?id=cbdc:public:cbdc_omg:8_append:60_mbse)

Last update: **2022/05/18 01:04**