

4.6 International Considerations

[Return to Common Elements](#)

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:¹⁾

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”²⁾ 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” to 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 [45_privacy](#).

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 1 provides some insight into data governance the CBDC needs as part of a **Data Strategy**.

Table 1: Governance issues associated with “data storage”

Data Residency ‡	Data Residency 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 ³⁾
Data Sovereignty	Data Sovereignty 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.
Data Localization ‡	Data Localization 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.⁴⁾

Governance Issues Associated with Data Storage

this namespace doesn't exist: cbbc:private:cbbc_omg:04_doc:15_common:50_international

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

Category	Desirements
Benefits	B0009, B0015, B0035, B0036, B0041, B0052
Policies	P0004, P0005, P0006, P0012, P0023, P0024, P0028
Risks	R0014
Design	D0013, D0015, D0016, D0017

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

Example Discussion

[Return to Top](#)

Table 3: “Desirements” identified in the **White Paper** that have potential international impacts.

Statement No.	Statement	Comment
B0009	Provide faster and cheaper payments (including cross-border payments)	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: B0016, B0017, P0015, P0016, R0022. These promises of a a global and international game changer has performance and cost issues. <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.⁵⁾</i> In addition to the speed issues, there are huge costs associated with consensus. See the OMG DIDO-RA discussion on Consensus Platforms. Note: However, this does not mean the Federal Reserve should not continue to have Research Development Test & Evaluation (RDT&E) Funding into Blockchains or Stablecoin. Note: See: B0041.
B0015	Reduce cross-border costs to benefit: 1. NO economic growth 2. enhance global commerce 3. improve international remittances 4. NO reduce inequality	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.⁶⁾</i> However, even though the U.S. Dollar is the de facto world currency, that 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.</i> <i>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, Why the US Dollar Is the Global Currency, The Balance 16 March 2022, Accessed: 10 April 2022, https://www.thebalance.com/world-currency-3305931)) Part of the reservation about the U.S. Dollar is also attributable to the Snowden revelation. See: Data Sovereignty and MacAskill and Dance.⁷⁾

Statement No.	Statement	Comment
B0035	Streamline cross-border payments by using: 1. NO new technologies 2. introducing simplified distribution channels 3. creating additional opportunities for cross-jurisdictional collaboration and interoperability	See B0015.
B0036	Preserve the dominant international role of the U.S. dollar	See B0015.
B0041	Support streamlining cross-border payments	The Bank for International Settlements (BIS) has produced a paper for the G20 on Central bank digital currencies for cross-border payments⁸⁾ <i>Cross-border payments with CBDCs can be envisioned in two fundamentally different ways:</i> 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> 2. <i>Access and settlement arrangements are established among different retail and/or wholesale CBDCs, built on strong cooperation among central banks</i> <i>In the <u>first scenario</u> 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> <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.¹² 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>
B0042	Preserve the dominant international role of the U.S. dollar	See B0015.

Statement No.	Statement	Comment												
B0052	Prevent Financial money laundering crimes	There is already a rich legal framework in place to cope with Money Laundering within the U.S.; many of these can help prevent money laundering across U.S. borders. One example is the US Patriot Act, Title III: Anti-money-laundering to prevent terrorism of 2001, especially the • The First Subtitle deals primarily with strengthening banking rules against money laundering, especially on the international stage • The Third Subtitle deals with currency smuggling and counterfeiting, including quadrupling the maximum penalty for counterfeiting foreign currency. Also, 18 U.S. Code § 1956 - Laundering of monetary instruments has provisions for international situations: • Unlawful activity, certain offenses against foreign nations • The defendant knew that the property involved was the proceeds of any felony under State, Federal or foreign law • Defines “<i>financial transactions</i>” to include interstate or foreign commerce Note: 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.												
P0004	Protect consumer privacy	Internationally, a major method of protecting consumer privacy is referred to as Data Localization. This section includes examples from Russia, China, India, European Union, and Brazil. Data Localization policies classification ⁹⁾ is summarized below: Local-only Storing, Transmission, and Processing: 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. Local Copy Required: 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. Narrower, conditional restrictions: Transfers of data outside the country are only permitted if certain conditions are met by the transferee and/or by the recipient country.												
P0005	Protect against criminal activity	There is already a rich legal framework within the U.S. to protect against criminal activity, which includes international activities (see the Details of National Security Considerations). Many of these laws and regulations are already well established and operational on the international level. Some examples: Human Trafficking: Intelligence Reform and Terrorism Prevention Act of 2004 The Intelligence Reform and Terrorism Prevention Act, section 7202 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. Drug Trafficking: 18 U.S. Code § 1952 - Interstate and foreign travel or transportation in aid of racketeering enterprises Five year maximum for traveling or using the mail or instruments of interstate commerce (telephone/internet) with intent to facilitate drug trafficking. Table 3: Summary of the number of laws and regulations covering National Security Considerations. <table><tr><th>National Security Consideration</th><th>No. of Laws and Regulations</th></tr><tr><td>Human Trafficking</td><td>14</td></tr><tr><td>Drug Trafficking</td><td>9</td></tr><tr><td>Corruption</td><td>10</td></tr><tr><td>Money Laundering</td><td>11</td></tr><tr><td>Total</td><td>44</td></tr></table> Note: 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	National Security Consideration	No. of Laws and Regulations	Human Trafficking	14	Drug Trafficking	9	Corruption	10	Money Laundering	11	Total	44
National Security Consideration	No. of Laws and Regulations													
Human Trafficking	14													
Drug Trafficking	9													
Corruption	10													
Money Laundering	11													
Total	44													
P0006	Garner broad support from key stakeholders	See 05_stakeholder. The primary international stakeholders in the CBDC effort are identified in non-U.S. Federal Government Oversight Authorities. This is a minimum set and could include more countries and specific agencies within these countries.												

Statement No.	Statement	Comment
P0012	The firms that operate interbank payment services are subject to federal supervision	This is highly dependent on the Currency Model or mix of currency models chosen to implement the U.S. CBDC. Existing intermediaries must already follow: • Know Your Customer (KYC) • Customer Due Diligence As well as take steps to prevent Money Laundering, such as: 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 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. ¹⁰⁾ Note: 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.
P0023	CBDC would need to be readily transferable between customers of different intermediaries	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.
P0024	CBDC would need to comply with the U.S. robust rules	Most of the international agreements have to do with detection and prevention of National Security 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: • Human Trafficking • Drug Trafficking • Corruption • Money Laundering

Statement No.	Statement	Comment
P0028	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	1. Common Standards: There are lots of “common standards” that apply to Blockchains and Blockchain technology. The following provides (and describes) standards or lists of standards that apply: • DIDO RA - Technical Standard Bodies • DIDO RA - de facto Standards Bodies 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 “<i>standard</i>”. However, often these projects lack the rigor needed to be considered a “<i>standard</i>”. Also, see the discussion in the DIDO RA on Talk Openly Develop Openly (TODO). As a contrast, look at the DIDO RA definition of a Standards Developing Organization (SDO). 2. Infrastructure: The CBDC Infrastructure needs to be considered Mission Critical since any loss of functionality could be considered a threat to survival. This is why the Desirements: B0053, D0015, D0016, D0017 are in the White paper. 3. Types of Intermediaries able to access any new infrastructure: B0026 specifies bridges between legacy and new payment services and will require new infrastructure. D0012 specifies leveraging existing tools already in use by intermediaries 4. Legal Frameworks: There are already legal frameworks in place to handle: • National Privacy Considerations • National Security Considerations 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 creating new frameworks. 5. Preventing Illicit Transactions: There are two areas within the existing legal frameworks covering Illicit transactions: • Money Laundering • Corruption 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 create new frameworks. 6. Cost and Timing of Implementation: 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 (B0020).
R0014	Risk of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity	This has to be accomplished understanding international treaties, laws and regulations on • Criminal Activity. • Data Residency • Data Localization • Data Sovereignty
D0002	Design should allow the central bank to limit the amount of CBDC an end user could hold	The U.S. CBDC would need to work within the confines of the individual country's laws and regulations on: • Data Residency • Data Localization • Data Sovereignty

Statement No.	Statement	Comment
D0003	Design should allow a limit on the amount of CBDC an end user could accumulate over short periods	See: q16 The U.S. CBDC would need to work within the confines of the individual country's laws and regulations on: • Data Residency • Data Localization • Data Sovereignty
D0002	Design should allow the central bank to limit the amount of CBDC an end user could hold	The U.S. CBDC would need to work within the confines of the individual country's laws and regulations on: • Data Residency • Data Localization • Data Sovereignty
D0009	Design should allow for significant foreign demand for CBDC, furthering complicate monetary policy implementation	This depends on the Currency Model used for the CBDC. For • Digital Cash Model, it would follow all the same rules as the current physical Dollar models work today.
D0013	Design should facilitate compliance with a robust set of rules already intended to combat 1. money laundering 2. the financing of terrorism 3. customer due diligence 4. record-keeping 5. reporting requirements	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: • Human Trafficking • Drug Trafficking • Corruption • Money Laundering Customer due diligence and record keeping need to take into account: • Data Residency • Data Localization • Data Sovereignty

Statement No.	Statement	Comment
D0015	Design should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks	Often, threats and operational disruptions are not limited to the geographic location of a particular country or jurisdiction. Some recent international attacks on communications ¹⁾ listed below: March 2022: An attack on a satellite broadband service run by the American company Viasat disrupted internet services across Europe, including Ukrainian military communications at the start of the Russian invasion. The attackers hacked satellite modems belonging to thousands of Europeans to disrupt the company's service. March 2022: Hackers penetrated the websites belonging to multiple Russian agencies including the Energy Ministry, the Federal State Statistics Service, the Federal Penitentiary Service, and the Federal Bailiff Service. The websites displayed several anti-government and anti-invasion images and messages before the agencies were able to expel the attackers. March 2022: Hackers linked to the Chinese government penetrated the networks belonging to government agencies of at least 6 different U.S. states in an espionage operation. Hackers took advantage of the Log4j vulnerability to access the networks, in addition to several other vulnerable internet-facing web applications. February 2022: Researchers identified campaigns by two North Korean government-backed groups targeting employees across numerous media, fintech, and software companies. The hackers used phishing emails advertising fake job opportunities and exploited a vulnerability in Google Chrome to compromise the companies' websites and spread malware. February 2022: A Beijing-based cybersecurity company accused the U.S. National Security Agency of engineering a backdoor to monitor companies and governments in over 45 countries around the world. A Foreign Ministry spokesman said that operations like this may threaten the security of China's critical infrastructure and compromise trade secrets.
D0016	Design should include offline capabilities to help with the operational resilience of the payment system	See: D0015
D0017	Design should include digital payments in areas suffering from large disruption, such as natural disasters	See: D0015 See: https://www.omgwiki.org/CBDC/doku.php?id=cbdc:private:cbdc_omg:04_doc:20_comments:dsn:q18 , List of Internet outages provided by Wikipedia.
B = Benefit Considerations		
P = Policy Considerations		
R = Risk Considerations		
D = Design Considerations		

1)

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

2)

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](#)

3)

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>

4)

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

5)

Kai Sedwick, No, Visa Doesn't Handle 24,000 TPS and Neither Does Your Pet Blockchain, Bico.in April 10, 2022, Accessed 10 April 2022,

<https://news.bitcoin.com/no-visa-doesnt-handle-24000-tps-and-neither-does-your-pet-blockchain/>

6)

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>

7)

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>

8)

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>

9)

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>

10)

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>

11)

Center for Strategic and International Studies, Accessed: 10 April 2022,
<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>

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:50_international:start&rev=1652459886

Last update: **2022/05/13 12:38**

