6.0 Recommendations

OMG Responses to Federal Reserve Discussion Paper

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.

this namespace doesn't exist: cbdc:private:cbdc_omg:04_doc:90_recommend

Defining the Stakeholders

Return to Top of Recommendations

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 1.

Table 1: Summary of the estimated number of Government Stakeholders for the CBDC.

Potential Oversight Authorities	No. of Stakeholders
U.S. Federal Government Oversight Authorities	14
non-U.S. Federal Government Oversight Authorities	19
Total	**33**

However, this does not include the roughly 4,200 Commercial Banks insured by the FDIC, see Figure 1 or the largest Banking Association in the U.S., The American Banking Association (ABA), or its competitors, nor the roughly 5,300 Credit Unions.

Figure 1: Number of FDIC-insured commercial banks in the United States from 2000 to 2021.[1)]

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 05_stakeholder.

Defining Applicable Laws and Regulations

Return to Top of Recommendations

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 2 for summary
- Security see Table 3 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 2: Summary of the number of laws and regulations covering National Security Considerations.

U.S. Privacy Consideration	No. of Laws and Regulations
U.S. Federal Laws and Regulations	10
U.S. State Laws and Regulations	6
Total	**16**

Table 3: Summary of the number of laws and regulations covering National Security Considerations.

National Security Consideration	No. of Laws and Regulations
Human Trafficking	14
Drug Trafficking	9
Corruption	10
Money Laundering	11
Total	**44**

A U.S. CBDC would have to adhere to these laws if it 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.

Instilling Confidence in the CBDC

Return to Top of Recommendations

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 of 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 4)

Table 4: Some requirements in the White Paper that require the confidence of the public.

Statement No.	Page No.	Statement
B0020	**13**	Maintain public confidence by not requiring mechanisms, such as deposit insurance
R0003	**3**	**Risk** to the safety and stability of the financial system
R0004	**3**	**Risk** to the efficacy of monetary policy
R0005	**7**	New payment services could pose **Risks** to: 1. financial stability 2. payment system integrity 3. other **Risks**
R0011	**11**	Increased **Risk** to consumer's vulnerability to: 1. loss 2. theft 3. fraud

Adopting a Model-Based Systems Engineering (MBSE) Approach

Return to Top of Recommendations

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)[2)] 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.

Defining the Appropriate Standards or Specifications

Return to Top of Recommendations

Perform Research Development Test & Evaluation (RDT&E)

Return to Top of Recommendations

Research Development Test & Evaluation (RDT&E) Funding

Consensus Algorithms

Return to Top of Recommendations

> *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.*[3)]

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 of the Mining Operations have moved from being distributed to being centralized and operated be 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.*[4)]

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.

Artifical Intelligence (AI)

Return to Top of Recommendations

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.

Ontologies

Return to Top of Recommendations

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.

Smart Contracts

Return to Top of Recommendations

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.

Figure 2: Creating a Platform Indepenent Model (PIM) and transforming it into various Platform Specific Models (PSMs)

Complex Data Model

Return to Top of Recommendations

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.

TBD TBD TBD

Most of the data models underlying cryptocurrencies are pretty simple. Generally, it's a balance.

The OMG members recommend There needs to be a comprehensive study of what needs to be stored in addition to the simple balance, especially if the “ledger” is going to try and prevent criminal activity and protect privacy. It also means that there will most likely be a confederation of blockchains and the need to link these together with the blockchains. some examples of concepts not covered in the existing models are association and composition. However, this extra data comes at a cost.

Understanding Gas

Return to Top of Recommendations

> *A gas is worth of 0.00000005 ETH and if you planning to store data or let’s say a 256-bit word it will cost you 20,000 gas. A kilobyte is thus 640k gas or 0.032 ETH or 16.70 USD as per the current rate of Ethereum which is $528.3 Dollar.*
>
> *Now calculate the price of storing one GB of data on a blockchain decentralized ledger and blow your mind away with an enormous amount that will come up. As per the current price of Ethereum, 1MB of data will cost you up approx. 17,100 USD. Calculate the price you will need to pay to store 1GB data of data on the blockchain.* Though the facts mentioned above is only true for public Ethereum blockchain while the case can be totally different if we focus on a few private or permissioned blockchain. One will, after reading the solution, definitely conceive the idea of using blockchain as the secured database is far way better than using the traditional database.

- 1 Gwei equals 0.000000001 ETH)
- median gas price (28 Gwei)
- USD/ETH exchange rate ($295/ETH)

Task	Gas required	Cost (ETH)	Cost (USD)	Ops per ETH	Ops per USD	Ops per Block	Blocks to complete OP
Add or subtract two integers	3	0.000000009	0.000002655	11111111.11	37664.78343	1566666.667	0.0000006382978230
Add two Integers, 1 Million times	3000000	0.09	26.550000000	11.1111111	0.037664783	1.566666667	0.638297872

Task	Gas required	Cost (ETH)	Cost (USD)	Ops per ETH	Ops per USD	Ops per Block	Blocks to complete OP
Save a 256-bit word to Storage	20000	0.0006	0.171	1666.666667	5.649711751	243	0.004255319
Save 1MB to Storage (31250 256-bit words)	625000000	18.75	5531.25	0.053333333	0.000180791	0.00752	132.9787234
Save 1GB to Storage (31250 256-bit words)	6250000000000	18750	5531250	0.00005333333	0.00000018079	0.00000752	132978.7234

Security Baked-in not Bolted-on

Return to Top of Recommendations

Also see the answers to:

- sb_01
  - prt_b
2. q07
   - Lack of Reporting and Oversight
3. q18
4. q02

Cryptocurrency skirts near the edges of illegal, illicit, or shady interactions and transactions. The Chainalysis Team recently published their 2021 findings[5)] 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**:

R0014	**Risk of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity**

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 Seurity 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 3 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.

Figure 3: The various States of Data

Table 5 provides a quick overview of the various data states. These data states are described in detail in the OMG DIDO-RA.

Table 5: Data can exist in the following different states

Data-at-Rest	Data-at-Rest 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.
Data-in-Motion	Data-in-Motion , also referred to as **Data in Transit** or **Data in Flight**, is a Digital Asset transmitted between locations (i.e., between computers or computer components). Data-In-Motion also describes data within Random Access Memory (RAM).
Data-in-Use	Data-in-Use 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 Computing Platform (i.e., Central Processing Unit (CPU), Dynamic Random Access Memory (DRAM),, Data Bus, etc.). **Data-In-Use** is one of three states of digital data – the other states are Data-at-Rest and Data-in-Motion.

Table 6: White Paper Desirements related to disruption and security

Statement No.	Page No.	Statement
B0004	**2**	Protect consumer privacy
B0005	**2**	Protect against criminal activity
B0053	**20**	Provide resiliency to threats to existing payment services—including: 1. operational disruptions 2. cybersecurity risks
R0011	**11**	Increased **Risk** to consumer's vulnerability to: 1. loss 2. theft 3. fraud
D0015	**20**	**Design** should include any dedicated infrastructure required to provide a resilience to threats such as operational disruptions and cybersecurity risks
D0016	**20**	**Design** should include offline capabilities to help with operational resilience of the payment system

Statement No.	Page No.	Statement
D0017	**20**	**Design** should include digital payments in areas suffering from large disruption, such as natural disasters

1)

Statistica, 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/

2)

“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

3)

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

4)

Sunbird, Largest Bitcoin Mining Farms in the World, Accessed: 9 May 2022, https://www.sunbirddcim.com/sites/default/files/Sunbird_InfoGraphic_Bitcoin.pdf

5)

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/