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

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)[1)] 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.*[2)]

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.*[3)]

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 1: 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

Task	Gas required	Cost (ETH)	Cost (USD)	Ops per ETH	Ops per USD	Ops per Block	Blocks to complete OP
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

1)

“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

2)

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

3)

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