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's CBDC WG 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 1) 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*.

Table 1: List of U.S. Federal Eleven Federal Agencies participating in the SBIR program[1)]

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‡
5. Department of Education
6. Department of Energy‡
7. Department of Health and Human Services‡
8. Department of Homeland Security
9. Department of Transportation
10. Environmental Protection Agency
11. National Aeronautics and Space Administration‡
12. National Science Foundation‡

‡ - *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. [2)]. Table 2 presents a summary of the limitations outlined by Orla et al. Many of these are issues are similar to those proposed by the OMG's CBDC WG members in Possible SBIR STTR Topics.

Table 2: Limnitations of Blockchain Technology.[3)]

Paragraph Number	Title	Description
4.7.1	**Slow transactions**	Physical performance affecting public Blockchains is a major limitation and barrier to adoption, as this comparative chart illustrates. Figure 1: Cryptocurrencies Transactions Speeds compared to Visa and Paypal[4)]
4.7.2	**Consensus time delay**	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.
4.7.3:	**Scalability**	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
4.7.4	**Design**	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.
4.7.5	**Link into the real economy**	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.

Paragraph Number	Title	Description
4.7.7	**Security**	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
4.7.8	**Vulnerability**	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's CBDC WG members on some possible RDT&E topics and some discussions the Federal Reserve can pursue with a partnering Federal Agency (see 1 for a list of possible Federal Government Department SBIR/STTR partners.

1)

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

2) , 3)

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
4)

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