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 “craking”. 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.*[1)].

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****.*[2)]

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.*[3)]

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 | 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)

1)

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/
2)

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/
3)

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