Question: 11. TBD Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?

Return to CBDC Benefits, Risks, and Policy Considerations

Question

Return to Top

Are there additional ways to manage potential risks associated with CBDC that were not raised in this paper?

Answer

Return to Top

By all descriptions, the U.S. CBDC is primarily a large System-of-Systems (SoS) or even an SoS of SoSs. Some of these would ideally already exist and some will need to be created. The new systems are predominately a Software (SW) effort. Yes, there will be some specialized Hardware(HW) required, but the primary focus appears to be Software (including Commercial-Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), or Modified Off-The-Shelf (MOTS). This software will ultimately need to be Managed and Modified.

1. Risk of a Software Crisis

Return to Top

2. Risk of Lack of Stakeholder Buy-In

Return to Top

3. Risk due to Poor Community of Interest (CoI) Governance

Return to Top

Governance of a Community of Interest (CoI) just does not happen by chance. It must be a well-thought-out formal organization with strict Policies and Procedures in place to guarantee the whole community is represented and can help formulate the solution or in this case, solutions to solving the Communities problem (i.e., U.S. CBDC). Too often, the Governance is considered by using Open Source Software (OSS). Although having OSS Projects can have an important role in the Governance of a project, it is primarily focused on the development of Software. Yes, the CBDC will be predominately software, but there is much more that needs to be governed than just software.

Table 1: Examples of non-Software things the U.S. CBDC Community of Interest might need to control. For example,

- Legal Documents such as
  - Charters
  - By-Laws
  - Policies and Procedures (P&P)
2. Guides
3. System and Software Engineering documents such as
   - Requirements
     - Non-Functional
     - Functional
   2. Models
   3. Interface Specifications
   4. Assurance and Assurance Models
   5. Testing regime
      1. Unit Testing
      2. Integration Testing
      3. End-to-End Testing (E2E Testing)
      4. Smoke Testing
      5. Sanity Testing
      6. Regression Testing
      7. Acceptance Testing
      8. White Box Testing
      9. Black Box Testing
      10. Interface Testing
      11. Interoperabiloity Testing
      12. Test Data
      13. Test Plans

14. Test Results

In addition to all these requirements for Governance, the Governance Model itself must reflect the *"distributed nature"* of the participants in the CoI itself. So far, we have identified 33 different Oversight Authorities that could be part of the CoI (see Table ##REF:summaryStakeReg##, and each one needs to be able to have a voice at the CoI forum or Consortium. See the OMG DIDO-RA discussion of Governance.

The U.S. CBDC will most likely be a System-of-Systems (SoS) or even an SoS of other SoSs. This means that there probably needs to be a hierarchy of CoI not unlike that of the Federal Reserve itself. For example:

- The U.S. CBDC CoI might be an Ecosphere
- The development of U.S. CBDC ATM equivalents might be an Ecosystem
    - The Development of a U.S. CBDC ATM machine itself might be a Domain
    - The Development of a U.S. CBDC ATM network might be a Domain
3. The Development of a Bridge between the ACH and the U.S. CBDC might be an Ecosystem
    - The Development of a U.S. CBDC Bridge Hardware might be a Domain
    - The Development of a U.S. CBDC Application Programming Interface (API) might be a Domain

Table 2: Overview of the different kinds of Communities of Interest (CoIs)

CoI Type	Description
Ecosphere Community	**Ecosphere Community is the highest level Community of Interest (COI) that encapsulates DIDO Ecosystem Communities and DIDO Domain Communities. The Ecosphere usually provides high-level requirements and some funding for the administration of the other CoIs. The Ecosphere's role is to act as a coordinator of the Ecosystems and to provide a framework for all other CoIs to establish working agreements such as Memorandum of Agreement (MoA) or Memorandum of Understanding (MoU). The Ecosphere is often the only CoI that is recognized as a Legal Entity with legally binding Charter, Bylaws and official Policies and Procedures. Often the Ecosphere control Intellectual Property (IP) rights and allowable Copyrights that are acceptable for the Ecosphere and the Domain.**

Ecosystem Community	**Ecosystem Community is the midlevel level Community of Interest (COI) that encapsulates Domain Communities. The Ecosystem has a Sub-Charter approved by the Ecosphere CoI. The Ecosystem usually relies on the Ecosphere for By-Laws and Policy and Procedures (P&P) but can provide addendums that do not conflict with the Ecosphere. The primary role of the Ecosystem is to coordinate the activities of the Domains which fall under its jurisdiction. As a general rule, the Ecosystem does not actually create anything but acts as the integrator and coordinator of all the Domains it is responsible for. The Ecosystem may have more restrictive Intellectual Property (IP) Rights than the Ecosphere. It can only subset the Copyrights allowed by the Ecosphere. The Ecosphere's role is to act as a coordinator of the Domains, however, one Ecosystem can also have a Sub-Ecosystem that it is responsible for. The Ecosystem can have its own bug tracking system that covers integration issues. The Ecosystem is responsible for all Integration Testing.**
Domain Community	**Domain Community is the lowest level Community of Interest (COI). The Domain has a Sub-Charter approved by the Ecosystem Community. The Domain usually relies on the Ecosphere for By-Laws and Policies and Procedure (P&P) but can provide addendums that do not conflict with the Ecosphere. The primary role of the Domain is to produce a product that meets the Functional and Non-Functional Requirements of the Ecosystem and the Ecosphere. As a general rule, the Domain actually builds or deploys things to be integrated into the Ecosystem. The Domain may have more Intellectual Property (IP) Rights than the Ecosystem. It can have a subset of the Copyrights allowed by the Ecosystem. The Domain's role is to build products as per the requirements and maintain products according to the Bug Tracking System. The Domain is responsible for all testing at the Domain level (See: Testability).**

Note: One way within the U.S. Government to create an Ecosphere, might be to use the Other Transaction Authority provisions within the U.S. Code.

4. Risk due to lack of Broad, Wide Ranging Security Planning

Return to Top

An important way to make sure the Security Planning is adequate is to design it into the U.S. CBDC from the onset, especially if the U.S. CBDC adopts the use of Distributed Technologies currently in wide use in cryptocurrencies. First, it is important to detail what needs to be secure and why. See Table 3.

For a more detailed discussion, see the OMG DIDO-RA section on Non-Functional

requirements for Securability.

Table 3: Main reasons why data needs to be secure.

- Confidentiality
- Data Integrity
- Non-repudiation
- Authenticity
- Accountability

All too often, projects try to “bolt-on” security after products are built. When building as essential and critical to the U.S. as a new financial mechanism such as CBDC, it is essential to think about it at every stage of the development, starting at the specification of requirements and at each layer of securability. See Figure 1 and Table 4

Securability is also a layered stack. At each layer, there are different steps that need to be taken to secure the system. For example, **Culture Security** it may just mean having employees hold a security clearance and/or take Drug Tests. For **Physical Security** it may mean having a locked facility to house the computers and network devices. Data Security might be software and cultural procedures such as encrypting all data stored in a disk drive and using software to access the data.

Figure 1: The layers of Security.

Table 4: The layers of Security.

1. Physical Security
2. Data Security
3. Network Security
4. Platform Security
5. Application Security
6. Culture Security

5. Risk of Data being hacked due weak Security Infrasture

Return to Top

> *When Senator Mark Warner (D-VA) questioned witness Dr. Neha Narula, Director of the Digital Currency Initiative at MIT, on security risks associated with cryptocurrencies, she responded that, with respect to ransomware attacks, the issue is that valuable data has not been properly secured, and suggested that a CBDC could have built-in safeguards. She also believed that open source software is critical for security.*[1)]

Data can exist in many states depending on how it is being used. Each of the different Data States poses its own risks of compromising data. The primary concern with data is that it compromises End User Privacy. See section 45_privacy.

The risks and concerns about Data in each of the different states are also important. Often, the primary focus for understanding data is to concentrate on Data-at-Rest. Although this data is relatively static, it can change over time. In the past, there was little concern for Data-in-Motion , which can have serious effects on Reliability, Maintainability, and Availability (RAM), as well as, Securability and can leave a system vulnerable to breaches. With the advent of HTTPS, these vulnerabilities are mitigated. The latest issue has become the need to secure Data-In-Use. A recent WhatsApp data breach [2)] found that switching data between image filters could cause memory corruption followed by a crash that left data exposed.

Figure 2 graphically represents the different Data States within a system. Most systems are now able to handle the Data-in-Motion and the Data-at-Rest issues but have traditionally relied on physical security to protect Data-in-Use.

Figure 2: The Various States of Data.

Any risk assessment must include the Security Infrasture and the state of data:

- Data-at-Rest
- Data-in-Motion
- Data-In-Use

6. Risk of Meta-Data being hacked due weak Security Infrasture

Return to Top

Metadata is data about data. Although this data can provide specific insight into personal data such as Personal Identifiable Information (PII) (see Privacy Concerns), there is also a problem with hackers gaining access to Metadata.

For example, knowing your name, address, phone number, and credit card details can be used to make illegal purchases in your name. This is a Criminal Activity in itself, but gaining information about your behavior and habits is a different kind of privacy violation. This information can be used to target you for advertisements or more nefariously specific scams. For instance, the metadata can now be used to determine that an individual is visiting a well-known cancer clinic and target the person for “miracle cures”.

Another example might be the discovery that a well-known founder and CEO of a publicly-traded company has visited the same well-known cancer clinic. This information is then used to in essence glean insider information about the company and make stock trades.

The use of Metadata is the primary engine for companies such as Google, Facebook, Microsoft, Apple, etc. However, this is done using their own mechanism to collect the data and users sign their rights away with the Service Level Agreements (SLAs), etc

they “sign” when they choose to use these products. It is another thing to use government-provided data.

Therefore, Metadata not only contains Data about Data, but it can also contain information about the association of data elements together. Sometimes this activity is referred to as Triangulation.

> ***Metadata Triangulation*** *describes taking two pieces of metadata to infer a great deal more. Let me give you an example. You take a picture of something with your iPhone. That picture has both a date/time stamp and a GPS location tag. Two different pieces of information that, when combined, can lead to so much more. Some examples of information that can be inferred are:*[3)]
> - *The weather*
> - *Top news stories (including the content of those stories)*
> - *Local objects, buildings, structures, etc.*
> - *Natural disasters*
> - *Nearby housing prices*
> - *Stock prices, economic conditions, inflation, etc.*
> - *Flights overhead, traffic conditions*

There is an assumption that Bitcoin transactions are anonymous, the reality is that they are anonymized. The following article by John Bohannon highlights the issue:[4)]

> *Bitcoin, the Internet currency beloved by computer scientists, libertarians, and criminals, is no longer invulnerable. As recently as 3 years ago, it seemed that anyone could buy or sell anything with Bitcoin and never be tracked, let alone busted if they broke the law. “It's totally anonymous,” was how one commenter put it in Bitcoin's forums in June 2013. “The FBI does not have a prayer of a chance of finding out who is who.”*
>
> *The Federal Bureau of Investigation (FBI) and other law enforcement begged to differ. Ross Ulbricht, the 31-year-old American who created Silk Road, a Bitcoin market facilitating the sale of \$1 billion in illegal drugs, was sentenced to life in prison in February 2015. In March, the assets of 28-year-old Czech national Tomáš Jiříkovský were seized; he's suspected of laundering \$40 million in stolen Bitcoins. Two more fell in September 2015: 33-year-old American Trendon Shavers pleaded guilty to running a \$150 million Ponzi scheme—the first Bitcoin securities fraud case—and 30-year-old Frenchman Mark Karpelès was arrested and charged with fraud and embezzlement of \$390 million from the now shuttered Bitcoin currency exchange Mt. Gox.*

In this case, it was the “good guys” who used the Metadata, but this could also have been used for nefarious activities and a U.S. CBDC needs to protect this kind of data.

7. Risk of Business Processes Being Hacked

Return to Top

Some government business processes need to be kept confidential, secret, or even top-secret when it comes to trying to audit or discover illegal or criminal activities. The reason is that if the processes were made readily available to the public, then the business process can be "gamed" to avoid detection. In these situations, the government is involved in an "arms race" so to speak with those who want to avoid detection. The government business processes are continuously refined and honed to detect illegal or criminal activity, while the "bad guys" continuously test the system to find its weaknesses.

As an example, the process of trying to "reverse engineer" the "rules" of a government business process for determining if an individual return gets audited run rampant when it comes to triggering an audit by the Internal Revenue Service (IRS).[5)]

More and more government business processes are using Artificial Intelligence (AI) to aid in the flow of the business process. Many of these AI processes are data-driven either through parameters or by using learning datasets continuously refined based on previous runs through the process. This means that either the original parameters or the learning data sets are subject to hacking attempts.

> *Budget cuts and a significant drop in Special Agents that investigate criminal tax crimes have led the IRS to use Artificial Intelligence (AI) to uncover criminal tax activities. In a recent webcast hosted by the American Bar Association, the IRS revealed that research and investigative techniques that used to take weeks or months may now be accomplished in minutes with technology the IRS is rolling out to detect taxpayer noncompliance.*
>
> *These computer tools are able to detect fraud, identity theft, money laundering, and hidden assets that Revenue Agents and Special Agents typically look for manually. The speed and sophistication of these computer data-mining programs have greatly increased the IRS' efficiency.*[6)]

If the government business processes are hacked, then the ability for illegal or criminal activities to go undetected is advanced.

Another problem would be if the government's business processes themselves were "hacked" to disable the government process or change the algorithms or parameters of the process to provide an unfair advantage. A simple example might be adding an exclusion for a certain individual within the process.

1)

Buckley Firm, Senate holds hearing on central bank digital currency, 16 June 2022, Accessed: 24 April 2022,

https://buckleyfirm.com/blog/2021-06-16/senate-holds-hearing-central-bank-digital-currency
2)

Czarina Grace, WhatsApp Data Breach 2021 Could Expose 2 Billion Users: Update Now on Android, iOS to Fix Security Risk, iTechPpost, 6 September 2021, Accessed 6 October 2021, https://www.itechpost.com/articles/106929/20210906/whatsapp-data-breach-2021-expose-2-billion-users-update-now.htm
3)

Aaron Edell, Coining a term: metadata triangulation, 11 February 2016, Accessed: 24 April 2022, https://www.linkedin.com/pulse/coining-term-metadata-triangulation-aaron-edell/
4)

John Bohannon, Why criminals can't hide behind Bitcoin - Even with cryptocurrency, investigators can follow the money, Science, 9 March 2016, Accessed: 24 April 2022, https://www.science.org/content/article/why-criminals-cant-hide-behind-bitcoin
5)

Jacob Dayan, IRS Audits: 10 Common Myths Debunked, Accessed: 24 April 2022, https://articles.bplans.com/irs-audits-10-common-myths-debunked/
6)

Stahl Criminal Defense Lawyers, Accessed: 24 April 2022, https://stahlesq.com/irs-artificial-intelligence-detects-tax-evaders/