6.09 Baked-in Security

Return to Recommendations | **Provide Feedback**

The OMG's CBDC WG members recommend the Federal Reserve define a task to ensure that Security is baked into the U.S. CBDC rather than trying to *post facto* add it later (i.e bolted-on).

Also see the answers to:

1. 1. How could a CBDC be designed to foster operational and cyber resiliency?
    - b) Cyber Resiliency
2. Question: 07. What tools could be considered to mitigate any adverse impact of CBDC on the financial sector? Would some of these tools diminish the potential benefits of a CBDC?
    - Lack of Reporting and Oversight
3. Question: 18. Should a CBDC have “offline” capabilities? If so, how might that be achieved?
4. Question: 02. Could some or all of the potential benefits of a CBDC be better achieved in a different way?

Cryptocurrency skirts near the edges of illegal, illicit, or shady interactions and transactions. The Chainalysis Team recently published their 2021 findings[1)] 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's CBDC WG 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 1 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 1: The various States of Data

Table 1 provides a quick overview of the various data states. These data states are described in detail in the OMG DIDO-RA.

Table 1: 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 2: White Paper Desirements related to disruption and security

Statement No.	Page No.	Statement

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
D0017	**20**	**Design** should include digital payments in areas suffering from large disruption, such as natural disasters

1)

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/