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

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

Return to Top

5. Risk of Data being hacked due weak Security Infrasture

Return to Top

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:*[1)]
>
> - *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:[2)]

> *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).[3)]

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.*[4)]

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)
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/
2)
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
3)
Jacob Dayan, IRS Audits: 10 Common Myths Debunked, Accessed: 24 April 2022, https://articles.bplans.com/irs-audits-10-common-myths-debunked/
4)
Stahl Criminal Defense Lawyers, Accessed: 24 April 2022, https://stahlesq.com/irs-artificial-intelligence-detects-tax-evaders/