Question: 10. How should decisions by other large economy nations to issue CBDCs influence the decision whether the United States should do so?

Return to CBDC Benefits, Risks, and Policy Considerations | **Provide Feedback**

Question

Return to Top

How should decisions by other large economy nations to issue CBDCs influence the decision on whether the United States should do so?

Answer

Return to Top

No “desirements” are expressed about needing or wanting to be the first among the other large economy nations to issue a CBDC. In many ways, building a CBDC is like landing a man on the moon. It is an extremely complicated undertaking, with lots of parts and lots of requirements. See section 3.0 White Paper Analysis for the “desirements” called out in the **White Paper**.

Beyond the **White Paper** there is a lot of discussion about CBDC, large systems engineering projects, and what works and does not work for large systems. Probably the most important “implied” requirement is that the CBDC is a Mission-Critical System with a long Lifespan.

A major difference between a cryptocurrency and a national currency is that people's lives and the viability of the country depend and rely on its currency, whatever form its form. Built around the currency is a complex monetary system as well as an entire national economy that includes financial resources and management. The national economy encompasses the value of all goods and services manufactured within a nation. In essence, the national economy is the backing behind the U.S. Dollar. Adding to the complexity of the U.S. currency issues is that “The dollar has been the world's reserve currency since the U.S. and its allies agreed at the 1944 Bretton Woods conference to peg it to a rate of $35 per ounce of gold. According to the International Monetary Fund, the dollar's share of global reserves stands at 59%, far above the euro at 20.5%.”[1)]. This extends the U.S. Currency and, by proxy, the U.S. CBDC well beyond the boundaries of a national economy.

These are some of the reasons why a U.S. CBDC is much larger, complex, and trickier to create than any other national CBDC, let alone any simplistic cryptocurrency or large products offered to the public by large corporations. The following example is meant to highlight the difference between large commercial

complex products and a CBDC.

Example: If a commercial, very large, complex system (such as Facebook) has a failure or has a temporary outage, there are probably very few lives at stake (if any) or even placed in jeopardy as a result of the loss of commercial service. This is because the commercial system is **NOT** mission-critical. However, when a CBDC is deployed and there is a failure or a temporary outage – people's lives, livelihoods, or life savings could be wiped out – making the CBDC a Mission Critical system. Over and above the criticality of a CBDC to a nation and its people, the use of this currency as a Reserve Currency throughout the world makes it obvious that the breadth and scope of the U.S. CBDC are more critical than other CBDCs.

An excellent place to start understanding the U.S. CBDC is to first understand money as it currently is and how it works. Daniel Kurt[2] describes how money works as follows:

> *Whether we pull out paper bills or swipe a credit card, most of the transactions we engage in daily use currency. Indeed, money is the lifeblood of economies around the world. Currency refers to paper money or coins that are in circulation. But currency is actually only a small piece of the monetary economy and is just one consideration when looking at the total money supply.*
>
> *Indeed, most money today exists as credit money or as electronic records stored in databases in banks or financial institutions. But still, the bread and butter of everyday transactions is currency, and that is what we will look more closely at here.*

- *Currency is the physical money in an economy, comprising the coins and paper notes in circulation.*
- *Currency makes up just a small amount of the overall money supply, much of which exists as credit money or electronic entries in financial ledgers.*
- *While early currency derived its value from the content of precious metal inside it, today's fiat money is backed entirely by **social agreement** and **faith in the issuer**.*
- *For traders, currencies are the units of account of various nation-states, whose exchange rates fluctuate between one another.*

An important part of the explanation of how money works comes down to **faith in the issuer** and **social agreement**. This is underpinned by the Executive Summary provided in the Money, and Payments: The U.S. Dollar in the Age of Digital Transformation **White Paper**:

> *For a nation's economy to **function effectively**, its citizens must have **confidence in its money and payment services**. The Federal Reserve, as the nation's central bank, works to maintain the public's **confidence by fostering monetary stability**, **financial stability**, and a **safe and efficient payment system**.*

The main takeaways from the Executive Summary are the U.S. CBDC must:

- function effectively
- instill confidence in its money and payment services
- instill confidence by fostering monetary stability

- offer financial stability
- Be a safe and efficient payment system

For these reasons, the U.S. CBDC must be more than a Cryptocurrency or even **Stablecoin**. It can not be organically grown and evolved using a bottom-up approach. Having a Dollar be a National Currency with a major role in the National and International economies requires a systematic, pedantic, system engineering approach. This does not mean that it has to follow the traditional Water Fall Model but can also use an Agile Model when and where appropriate. For example, if a Blockchain model is adopted for use within the CBDC, which uses a series of Smart Contracts to accomplish portions of its overall requirements, these can be developed using an **Agile Model** working within the framework of requirements set at the onset of the CBDC.

Mark Zuckerburg is quoted as saying, *"We used to have this famous mantra ... and the idea here is that as developers, moving quickly is so important that we were even willing to tolerate a few bugs in order to do it. What we realized over time is that it wasn't helping us to move faster because we had to slow down to fix these bugs and it wasn't improving our speed."* [3] As stated earlier, there is a big difference between working on a large, commercially available product that is not Mission Critical and a product that is Mission Critical. In Mission Critical Systems, any bug can have devastating consequences. Who wants to be in an operating room when a major piece of equipment has a bug? How about an airplane flying over your head? It is expected there will be bugs in any software, but in Mission Critical systems many can be found and corrected earlier on in the product lifecycle and especially during product testing. It is not acceptable to "let the End Users" do the testing on these kinds of systems.

So, back to the fundamental question. Should the U.S. CBDC be worried about being first to market among the other large economies? Not if it means the Federal Reserve has to take shortcuts to race to market and ultimately accumulate Technical Debt, which like all debt, must be paid back in the future.

> *The term "technical debt" was coined by Ward Cunningham, when he described the phenomenon of meeting a release deadline by making adaptations and concessions to a product. He also outlined how the effects felt afterward were analogous to those associated with the incurring of financial debt. Cunningham acknowledged that, most often, technical debt required payback, while the inability to manage assets could lead to a complete stand-still as the interest and effects of the adaptations (or lack thereof) become unbearable.*[4]

Chris Cairns and Sarah Allen proposed a quadrant as a way to classify the various types of Technical Debt (See Figure 1). Across the top of the quadrant, they divided the behavior that leads to Technical Debt as being **Reckless** or **Prudent**. Down the left side of the quadrant, they divided the mechanisms that led to the debt as being **Deliberate** or **Inadvertent**. Each cell in the quadrant is used to classify Technical Debt and is described in Table 1.

Figure 1: A classification of Technical Debt show in quadrants. [5]
Table 1: Each quadrant in Figure 1 is a different type of Technical Debt.[6]

Type of Technical Debt	Description
Reckless/Deliberate Debt	The team feels time-pressured and knowingly violates best practices without any forethought into how to address the consequences. Another scenario: management lacks sufficient funding to hire enough senior experts to direct and review the work of junior programmers, but decides to take the risk anyway.
Prudent/Deliberate Debt	The team decides that the value of shipping a “quick and dirty solution” now is worth the cost of incurring debt. They’re fully aware of the consequences, however, and have a plan in place to address them.
Reckless/Inadvertent	The team is ignorant of best practices and makes a big mess of the codebase.
Prudent/Inadvertent	Even with great programmers, the team delivers an extrinsically valuable solution, only to realize how they should have (intrinsically) designed it. (Often the process of software development is as much learning as it is coding.)

Mark Zuckerberg used the motto “Move fast and break things” in 2014.

“Move fast and break things” has come back to haunt Facebook/Meta over the years. As the company has faced wave after wave of scandals over privacy, misinformation, and harmful content, critics have held its original motto up as evidence of a tendency towards collateral damage.

In the article on the biggest cryptocurrency hacks of all time by Tech Monitor[7] they highlight that Multi-million dollar crypto heists reveal that the crypto industry is learning cybersecurity lessons the hard way, one hack at a time. The article provides the following quotes:

> *Proponents argue that the crypto ecosystem is having to learn in a few years, lessons the conventional finance sector has had centuries to perfect. But the biggest crypto hack by value is also the most recent, suggesting there be many more lessons left to learn.*
>
> *“Traditional financial companies have grown up knowing that you have to have layers of protection… in order for folks to entrust you with their money,” says Chris Caruana, VP of AML solutions at financial crime solutions platform Feedzai.*
>
> *“Cryptocurrency exchanges, and the actual ecosystem itself, haven’t had to go through those growing pains yet,” Caruana says. “Even the most adult in the room still has some ways to go.”*

Figure 2 highlights the top biggest losses from hacks in Cryptos. The graph highlights the ever-increasing magnitude in the amount lost in each hack. This indicates that instead of getting things under control, things are only getting worse, which does not bode well for the adoption of the current technology by the CBDC.

Figure 2: Top nine biggest cryptocurrency thefts by estimated losses as of March 2022[8]

> **Note:** Total is \$2,905M

Note: Values calculated according to cryptocurrency prices at time of theft
Source: Statista/Bloomberg, Business Insider, TechCrunch, CNBC

Table 2 goes through the five top biggest crypto hacks of all time and provides a detailed explanation of the current knowledge about each hack.

Table 2: The top biggest biggest crypto hacks of all time[9)]

Rank Of Biggest to Smallest	Amount Lost	Year	Cryptocurrency	Explanation
1	**\$614M**	**2021**	**Ronin Network**	The biggest cryptocurrency theft of all time, calculated using the value of the crypto assets at the time they were stolen, was March 2022's raid on Ronin Network, an exchange that allows players of the Axie Infinity videogame to exchange their in-game tokens for another cryptocurrency. On 30th March, the network revealed that an attacker had stolen the private keys required to authenticate transactions and had transferred 173,600 Ethereum and 25.5m USDC, a **Stablecoin** pegged to the US dollar, to their own wallets. Using the conversion rate at the time, this values the heist at \$614m. The theft was discovered when a customer tried to make a legitimate withdrawal. Sky Mavis, the company behind Axie Infinity, said it is working with "law enforcement officials, forensic cryptographers, and our investors to make sure there is no loss of user funds. *"We know trust needs to be earned and are using every resource at our disposal to deploy the most sophisticated security measures and processes to prevent future attacks,"* the company statement said.

2	**\$611M**	**2021**	**Poly Network**	The second biggest crypto theft of all time, calculated using the value of the crypto assets at the time they were stolen, is last year's \$611m theft from Poly Network, a smart contract platform that allows users to exchange tokens between disparate blockchains, such as Bitcoin and Ethereum. On August 10th, 2021, a hacker transferred \$611m-worth of Poly Network tokens to three wallets under their control. According to an analysis by security researcher Mudit Gupta, the attacker had found a way to 'unlock' (ie buy) tokens on the Poly Network protocol without 'locking' (ie selling) the corresponding tokens on other blockchains. Fortunately for Poly Network, the attacker began returning the tokens the next day. While some speculated that they may have struggled to sell the tokens, someone claiming to be the attacker said they had only stolen them “for fun”. By the end of the week, all assets were returned, Poly Network said, except \$33m-worth of **'Stablecoin'** Tether, which had been frozen immediately after the attack. Shortly after the theft, Steven Dickens, senior analyst at technology research company Futurum, wrote that it was likely to bolster the security of decentralized finance (DeFi) systems in the long run, but discredit them in the short term. *“While lessons need to be learned for sure,”* he wrote, *“we need to be aware of the progress made so far by the DeFi community [which is for all] intents and purposes less than a decade old.”*
3	**\$547M**	**2018**	**Coincheck**	In January 2018, Japanese crypto exchange Coincheck revealed that \$547m in lesser-known cryptocurrency NEM had been stolen. The company admitted that it had stored the assets in a 'hot wallet', meaning a cryptocurrency store that is connected to the internet and therefore vulnerable to cybersecurity breaches. Shortly after the incident, 16 of Japan's crypto exchanges merged to form a self-regulatory body. The country's financial regulator, the Financial Services Association, ordered all exchanges to report on their cybersecurity defenses. At the time of the attack, Coincheck was one of the most high-profile exchanges in Japan, which was then among the biggest markets for crypto trading. A few months later, Coincheck was acquired by financial services provider Monex Group. It is still unknown who undertook the attack, but more than 30 people have been arrested in Japan in connection with selling the stolen assets.

4	**\$480M**	**2014**	**Mt. Gox**	The first widely publicized - and perhaps still the best-known - crypto heist was the theft of \$480m in Bitcoin from another Japanese exchange, Mt. Gox, in 2014. Founded in 2010 as a site for trading '*Magic the Gathering* game cards, by 2014 Mt. Gox was handling over 70% of all Bitcoin transactions. In February of that year, it abruptly suspended trading, closed its exchange services, and filed for bankruptcy protection. Soon after, it revealed that up to 850,000 Bitcoins had gone missing, presumed stolen. Around 7% of all Bitcoin was in circulation at the time, the haul was then worth around \$480m. Today, it would be closer to /\$35bn. Mark Karpeles, CEO of Mt. Gox at the time of the theft, was later arrested on unrelated charges and, he claims, interrogated for eight hours a day. “I was asked about the missing Bitcoins,” he told reporters. “I was even asked if I was Satoshi Nakamoto, the creator of Bitcoin.” But in 2016, a US investigation concluded that Mt. Gox had been hacked by an outsider.
5	**\$285M**	**2020**	**KuCoin**	In September 2020, Singapore-headquartered crypto exchange KuCoin revealed that \$275m worth of cryptocurrency had been stolen, including \$127m in ERC20 tokens, which are used in Ethereum smart contracts. CEO Johnny Lyu revealed that hackers had obtained the private keys to the exchange's 'hot wallets'. The majority of the stolen tokens were recovered, and the remaining 16% in stolen funds was covered by KuCoin's insurance, the company said in February 2021, so all customers were reimbursed.
Total	**\$2,537M**			

Examples

Return to Top

The following “desirements” are from the White Paper as identified by the Object Management Group's CBDC WG report called White Paper Analysis:

Table 3: Example of mapping a subset of requirements identified during the White Paper Analysis conducted by the OMG's CBDC WG.

Benefits	B0020, B0027, B0036, B0050
Policies	P0006, P0009, P0010, P0014, P0015, P0016, P0017, P0025, P0031
Risks	R0001, R0003, R0005, R0006, R0009, R0012, R0014, R0023,
Design	D0011, D0012, D0015

Example Discussion

Return to Top

Table 4: “Desirements” identified in the **White Paper** that have potential international impacts.

Statement No.	Statement	Comment
B0020	**Maintain public confidence by not requiring mechanisms, such as deposit insurance**	Even in the current Crypto world, there is a need for “deposit insurance”. *The 2020 KuCoin hack cost \$285M. The majority of the stolen tokens were recovered, and the remaining 16% in stolen funds was covered by KuCoin's **insurance**, the company said in February 2021, so all customers were reimbursed.* *Despite the hack, KuCoin remains the fifth most popular crypto exchange, according to the CoinMarketCap website.*[10)]
B0027	**Maintain the centrality of safe and trusted central bank money**	
B0036	**Preserve the dominant international role of the U.S. dollar**	The U.S. CBDC will be a target not just from hackers who want to profit from an attack, but also as a symbol of the U.S. making it a target of espionage.
B0050	**Extend Public Access to Safe Central Bank Money**	By extending public access to the “safe Central Bank Money”, there is also an extension of risk to the “safe central bank money”. Currently, the separation between the “safe central bank Money” and the regular money acts as a firewall. By granting direct access to the Central Bank Money, that firewall is no longer in place and safeguards need to be added to protect the Central Bank Money.
P0006	**Garner broad support from key stakeholders**	In order to garner support from within the U.S. and from the rest of the world, the CBDC needs to uphold the laws against Human Trafficking , Drug Trafficking , Corruption , and Money Laundering just as the U.S. has done with the U.S. Dollar and numerous laws we now enforce to prevent or interrupt these illegal activities.
P0009	**CBDC would be a liability of the Federal Reserve, not of a commercial bank**	When the Federal Reserve assumes liability for the CBDC, any negative news regarding hacks, breaches, or criminal activity associated with the CBDC will be a direct reflection on The Federal Reserve.

Statement No.	Statement	Comment
P0010	**CBDC would be a liability not of a commercial bank**[11)]	See **P0009**
P0014	**The PWG report highlights gaps in the authority of regulators to reduce these risks**	This is why all the Stakeholders need to be involved in the U.S. CBDC development, not just guide the CBDC system, but also to guide the administrators and the legislators to make the appropriate updates and amendments to the laws.
P0015	**The PWG report recommends that Congress act promptly to enact legislation that would ensure payment Stablecoins**	Stablecoins are just the same as any other cryptocurrency with the exception that their value is pegged to the U.S. Dollar. If the Stablecoin software is not properly engineered and tested before deployment just to be “the first” major economy with a CBDC, it seems it will be an expensive proposition.
P0016	**The PWG report recommends payment Stablecoin arrangements are subject to a consistent and comprehensive federal regulatory framework**	See **P0014**
P0017	**The PWG report recommends CBDC complement existing authorities regarding:** **1. market integrity** **2. investor protection** **3. illicit finance**	See **P0014**
P0027	**CBDC a risk-free asset**	The CBDC will be a large project that produces many lines of code. It is not possible for it to be “risk-free”. The risk to the end-user can be alleviated with insurance, but that does not mitigate the risk. See Figure 2 and Table 2 above.
P0031	**The Federal Reserve would only pursue a CBDC in the context of broad public and cross-governmental support**	See **P0014**
R0001	**Risk of affecting financial-sector market structure**	If there is a major hack to the CBDC, this could trigger a “lack of confidence” not just in the CBDC, but in the U.S. Dollar and perhaps The Federal Reserve.
R0003	**Risk to the safety and stability of the financial system**	See **R0001**
R0004	**Risk to the efficacy of monetary policy**	See **R0001**
R0005	**New payment services could pose Risks to:** **1. financial stability** **2. payment system integrity** **3. other Risks**	See **R0001**

Statement No.	Statement	Comment
R0006	**Risk of extreme price volatility**	See **R0001**
R0009	**Increased Risk of "runs" or other instabilities to the financial system**	See **R0001**
R0012	**Risk of increased concern related to the potential for: 1. destabilizing "runs" 2. disruptions in the payment system 3. concentration of economic power**	See **R0001**
R0014	**Risk of not achieving an appropriate balance between safeguarding the privacy rights of consumers and affording the transparency necessary to deter criminal activity**	Not only does the CBDC have to worry about hacks that can steal value from the CBDC, but it also needs to worry about hacks that steal private information. Once there is a hack of private information, confidence in the CBDC will be undermined.
R0023	**Risk of financial panic causing outflows from Commercial Banks to CBDC without prudential supervision, government deposit insurance, and access to central bank liquidity**	This is a dangerous two-way street. Not only could there be a "flight to value" towards the CBDC, but there could also be a "flight to value" away from the CBDC.
D0011	**Design should generate data about users' financial transactions in the same ways that commercial bank and nonbank money generates data today**	If the CBDC is rushed to be the first major economy in the world with a CBC, the design must assure the privacy of the end-users. See section 4.4 National Privacy Considerations. Also, see **P0009** where the CBDC would be a liability of the Federal Reserve, not of a commercial bank.
D0012	**Design should address privacy concerns by leveraging existing tools already in use by intermediaries**	There appears to be a conflict between **D0012** and **P0009**.

Statement No.	Statement	Comment
D0015	**Design should include any dedicated infrastructure required to provide resilience to threats such as operational disruptions and cybersecurity risks**	A dedicated infrastructure takes time. As an indicator of how slow infrastructure can be, IPv6 has been underway since 1998 to address a shortfall of IPv4 addresses, yet the upgrade is still in progress as of 2022. [12] Another example is the slow adoption in the U.S. of the "Chip and Pin" Credit Cards. According to Heather Long: [13] *The credit card market in the US is complex (pdf). You have retailers, big banks, and then card associations like Visa and Mastercard. So you have to get three sectors of the market to work together to implement any new technology. US retailers and credit card companies have been at war for years over who pays what transaction fees. Now they're trying to sort out who will pay for the estimated $8bn costs (pdf) for chip and pin technology.* The adoption of infrastructure for CBDC needs to be thought out and planned, including who is paying for it.
B = Benefit Considerations		
P = Policy Considerations		
R = Risk Considerations		
D = Design Considerations		

1)
Robert Burgess, Bloomberg, 3 March 2022, Accessed: 16 April 2022, https://www.bloomberg.com/opinion/articles/2022-03-03/dethroning-the-dollar-as-the-world-s-reserve-currency-won-t-be-easy
2)
Daniel Kurt, How Currency Works, 24 June 2021, Accessed 15 April 2022, https://www.investopedia.com/articles/investing/092413/how-currency-works.asp
3)
Ramnath Kashikar, Technical Debt – Good or Bad?, 7 August 2020, Accessed: 15 April 2022, https://www.linkedin.com/pulse/technical-debt-good-bad-ramnath-kashikar/
4)
Johannes Holvitie, Sherlock A. Licorish, Rodrigo O. Spínola, Sami Hyrynsalmi, Stephen G. MacDonell, Thiago S. Mendes, Jim Buchan, Ville Leppänen, Technical debt and agile software development practices and processes: An industry practitioner survey, Information and Software Technology, Volume 96, 2018, Pages 141-160, ISSN 0950-5849, Accessed: 16 April 2022, https://www.sciencedirect.com/science/article/pii/S0950584917305098
5)
Chris Cairns , Sarah Allen , What is technical debt?, 18f.gsa.gov, 4 September 2015, Accessed 15 April 2022, https://18f.gsa.gov/2015/09/04/what-is-technical-debt/
6)
Chris Cairns , Sarah Allen , What is technical debt?, 18f.gsa.gov, 4 September 2015, Accessed 15 April 2022, https://18f.gsa.gov/2015/09/04/what-is-technical-debt/

7) , 8) , 9) , 10)

Tech Monitor, The biggest cryptocurrency hacks of all time, 17 March 2022, Accessed: 15 April 2022, https://techmonitor.ai/technology/cybersecurity/biggest-cryptocurrency-hacks-of-all-time

11)

Commercial banks include banks licensed either by federal or state banking agencies, credit unions, and thrifts from the **White Paper**.

12)

Josh Fruhlinger, What is IPv6, and why is its adoption taking so long?, Network World, 21 March 2022, Accessed 17 April 2022, https://www.networkworld.com/article/3254575/what-is-ipv6-and-why-aren-t-we-there-yet.html

13)

Heather Long, Why is the US a decade behind Europe on 'chip and pin' cards?, The Guardian, 27 January 2014, Accessed: 17 April 2022, https://www.theguardian.com/commentisfree/2014/jan/27/target-credit-card-breach-chip-pin-technology-europe