bitt

CBDCs, Stablecoins & Crypto

Author: Simon Chantry,
Co-Founder and Chief Information Officer, Bitt

The Future Composite Financial System is Evolving

Getting digital currency right is a challenge faced by both public and private sectors. The private sector has been building unique fintech products for over a decade now – some of which have led to tremendous economic growth, others outright scams, and many yet to be determined. Policy makers have faced increasing challenges given the complexity innate in this novel asset class. Digital currency regulation is a contentious issue and significant challenge for legislators of our time. The task of designing and enacting legislation that will protect investors, foster development and growth, keep talent and businesses in-country, enable tax collection, minimize criminal activity, and mitigate financial stability risk is a complicated challenge. Considering how the financial system has evolved, and how crises developed and were dealt with in the past, our modern day composite financial system — with all its novel capabilities and interconnected stakeholders — offers significant opportunities and risks for those taking part in the exchange of value. As a builder working at the intersection of technology and policy — building stablecoin and Central Bank Digital Currency (CBDC) systems since 2016 — it has been fascinating to both witness and participate in significant digital currency efforts in multiple countries. This piece is meant to provide an overview of regulatory and social perceptions of financial technologies — linking key moments that have contributed to current events — and offer commentary on how the industry may evolve. The financial system of the future will be shaped by the efforts of both builders and regulators who desperately need to collaborate to ensure optimal outcomes for future generations.

“Digital currency regulation is a contentious issue and a significant challenge for legislators of our time. The task of designing and enacting legislation that will protect investors, foster development and growth, keep talent and businesses in-country, enable tax collection, minimize criminal activity, and mitigate financial stability risk is a complicated challenge.”

With most people on the planet now connected to the instant data exchange network that we call the internet, a growing recognition that money is simply data, and with digital currencies and assets gaining significant traction over the past few years — with powerful permissionless decentralized foundations — regulators have their hands full. As if the challenge wasn't significant enough, this novel asset class has multiple regulators fighting over jurisdiction in the US with the Securities and Exchange Commission (SEC), Commodity Futures Trading Commission (CFTC), the Office of the Comptroller of the Currency (OCC) all participating in regulatory actions. In some countries, the central bank itself is passing digital currency legislation and enforcement actions. Some nations were quick to implement regulation during and after the Initial Coin Offerings (ICO) boom of 2016/2017, with Bermuda introducing the Digital Asset Business Act[1], Malta with their Virtual Financial Assets Act[2], and the Monetary Authority of Singapore[3]. However, this legislation was largely meant to attract companies to their jurisdiction to benefit from the increase in tax revenues and employment. The exception perhaps was the New York State Department of Financial Services (NYDFS), passing the so called "BitLicense" regulation in 2015[4]: a particularly burdensome piece of legislation that would lead to the outflow of digital currency companies from New York. At this point, all eyes are on the US to implement comprehensive and sensible regulations.

[1] *Digital Assets Supervision and regulation in Bermuda*. Bermuda Monetary Authority. (2018, September). https://www.bma.bm/digital-assets-supervision-regulation

[2] *Virtual Financial Assets Act.* Malta Financial Services Authority. (2018, November). https://www.mfsa.mt/wp-content/uploads/2018/12/fintech-main-legislation.pdf

[3] *MAS clarifies regulatory position on the offer of digital tokens in Singapore.* Monetary Authority of Singapore. (2017, August). https://www.mas.gov.sg/news/media-releases/2017/mas-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-singapore

[4] *Virtual Currency Businesses*. Department of Financial Services of New York State. (2015, June). https://www.dfs.ny.gov/virtual_currency_businesses

On the CBDC side of things, solutions are evolving to service the multifaceted financial system of the future, ensuring this next iteration of national currency is interoperable with both legacy and new transaction and settlement systems. This task remains a challenge given that there will certainly be currency and other instruments of value circulating on multiple types of "layer 1" networks (see our previous piece titled "The Importance of Interoperability in CBDCs" for more on this). However, aside from the technical challenges associated with building interconnected systems that can securely exchange and settle value, regulation will impact the extent to which these technologies' value propositions can be truly realized, which applies not only to decentralized crypto assets but also to CBDCs. Furthermore, regulation could impact **where** on the planet the most successful progressive financial technology companies' domicile, grow, and prosper, which could also have a direct impact on nations' economic futures.

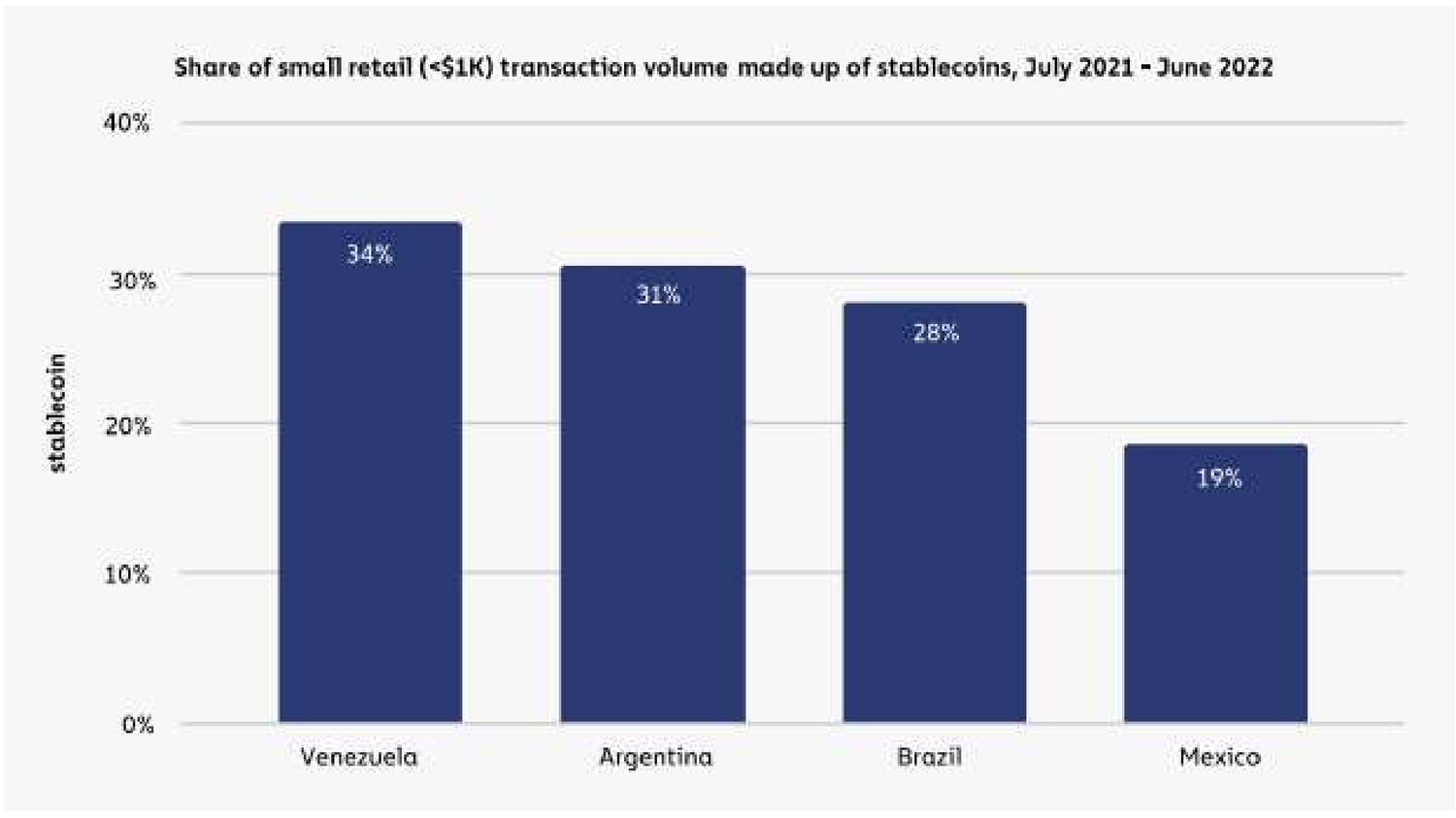
Whenever we engage with a central bank, financial institution, or regulator, many questions emerge regarding the nature of the underlying technology, the proximity or association with crypto and stablecoins, and how to effectively address the challenges and maximize the opportunities posed by each type of asset. CBDCs, stablecoins, and crypto assets all possess unique features and functions that serve a multitude of use-cases. Let's unpack each of them briefly:

Crypto

Cryptocurrency: the first of such assets – Bitcoin — launched in 2009, offering an algorithmically-governed limited supply cryptographic currency circulating on its own layer 1 network, operating in a decentralized manner with game theory woven into the protocol to incentivize a variety of stakeholders to operate, hold, and transact in the native token BTC. The use of proof-of-work to secure the network, settle transactions, and earn a reward incentivized miners to run the protocol, and public-private key cryptography enabled users to transact BTC as a digital bearer instrument. Bitcoin would go on to inspire other digital currencies such as Ethereum, Stellar, and others with unique value propositions (smart contracts enabling additional tokens to be issued on the same network, and more) ultimately serving people who wish to transact in a permissionless manner without intermediaries, having significant risk tolerance for this volatile asset class.

Stablecoins

Stablecoin: first entered the space to service crypto users seeking to hold USD in a permissionless manner, and to balance their portfolio and enable more efficient trading to and from crypto and USD. Stablecoins in their current form are tokens issued primarily on public permissionless networks such as Ethereum, with the issuer maintaining 1:1 reserves[5] for all tokens in circulation. Post 2020, as DeFi protocols like Curve and Aave advanced in functionality and experienced significant growth in active users — alongside the growth of NFT marketplaces like OpenSea — stablecoins serviced a multitude of use-cases including liquidity provision in automated market makers, lending, and atomic exchange and settlement on decentralized exchange platforms. Stablecoins have also been increasingly used by people in countries seeking to protect themselves from currency inflation; the currencies of Venezuela (25,735,658 %), Argentina (851%), and Turkey (340%), have all devalued the past five years relative to the US dollar. This devaluation has in-turn forced their citizens to pivot in-part to USD stablecoins as hedges against their local currency devaluation. According to Chainalysis[6], consumers seeking a vehicle capable of storing value have flocked to stablecoin alternatives in Venezuela, Argentina, and Brazil where nearly a third of all small retail transaction volume is now made up of stablecoins. A similar situation has occurred in Turkey, where, due to the depreciation of the Lira, The Financial Times reported in early 2022[7], that as the Lira depreciated, trading volumes surged by 360% towards USDT. Today, USDT accounts for 20% of all crypto volume in Turkey, peaking at 46% earlier this year[8].



According to Chainalysis, as Latin American currencies devalued, consumers increasingly resorted to USD stablecoins in order to preserve the value of their savings.

Source: *Chainalysis 2022 "Geography of Cryptocurrency Report"* *https://go.chainalysis.com/geography-of-crypto-2022-report.html*

---

[5] Baughman, G., Carapella, F., Gerszten, J., & Mills, D. (2022, May). *The stable in stablecoins*. The Federal Reserve of the United States. *https://www.federalreserve.gov/econres/notes/feds-notes/the-stable-in-stablecoins-20221216.html* "With respect to the commitment to stabilize their value relative to another asset, stablecoin issuers are similar to a currency board, which is required to maintain a fixed exchange rate with a foreign currency and holding that foreign currency in reserves"

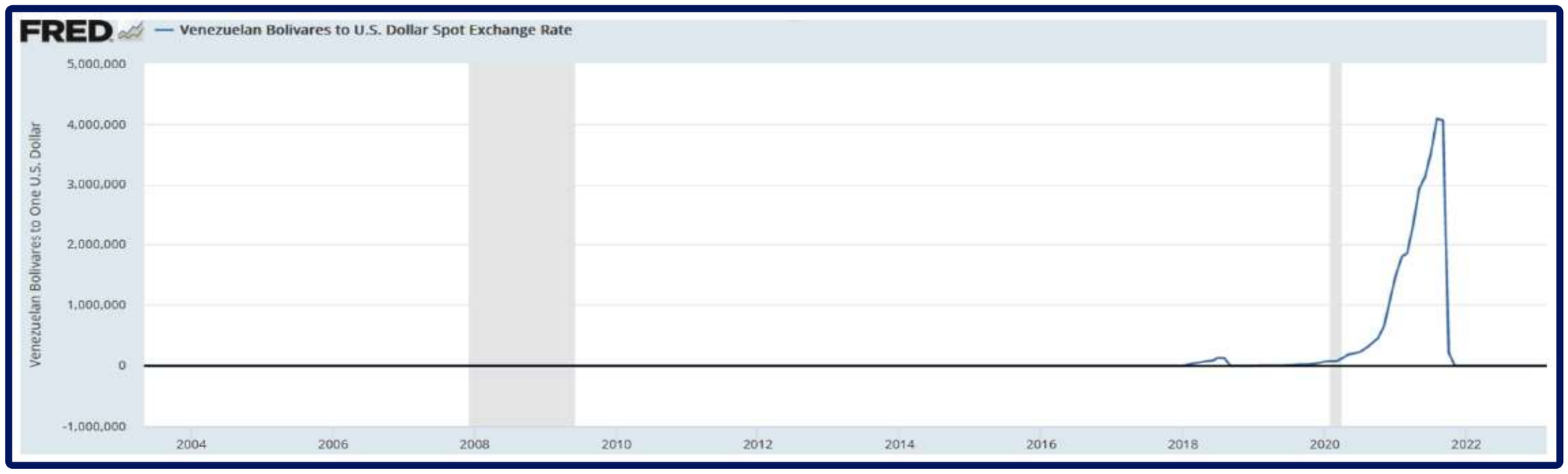
[6] *Chainalysis 2022 "Geography of Cryptocurrency Report"* *https://go.chainalysis.com/geography-of-crypto-2022-report.html*

[7] *Financial Times, "Turks flock to Cryptocurrencies in search of stability"* *https://www.ft.com/content/02194361-a5b9-4bf0-9147-f36ba7759cf1*

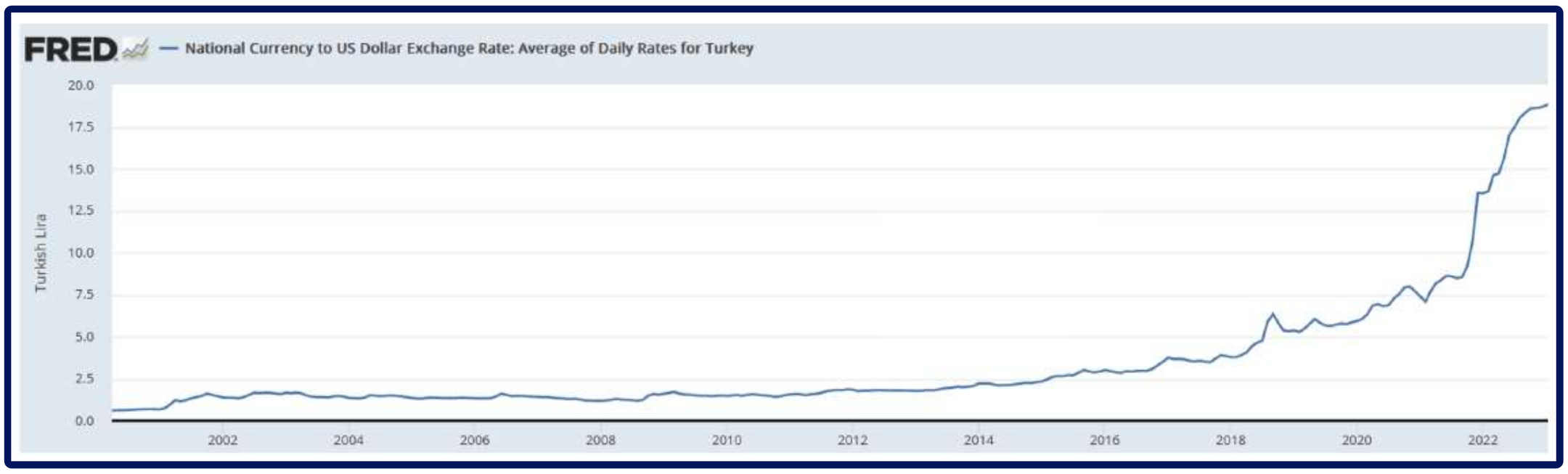
[8] Fries, T. (2023, May). *Turkey turns to crypto amid high inflation and political instability*. The Tokenist. *https://tokenist.com/turkey-turns-to-crypto-amid-high-inflation-and-political-instability/*

"Whenever we engage a central bank, financial institution, or regulator, many questions emerge regarding the nature of the underlying technology, the proximity or association with crypto and stablecoins, and how to effectively address the challenges and maximize the opportunities posed by each type of asset. CBDCs, stablecoins, and crypto assets all possess unique features and functions that serve a multitude of use cases."

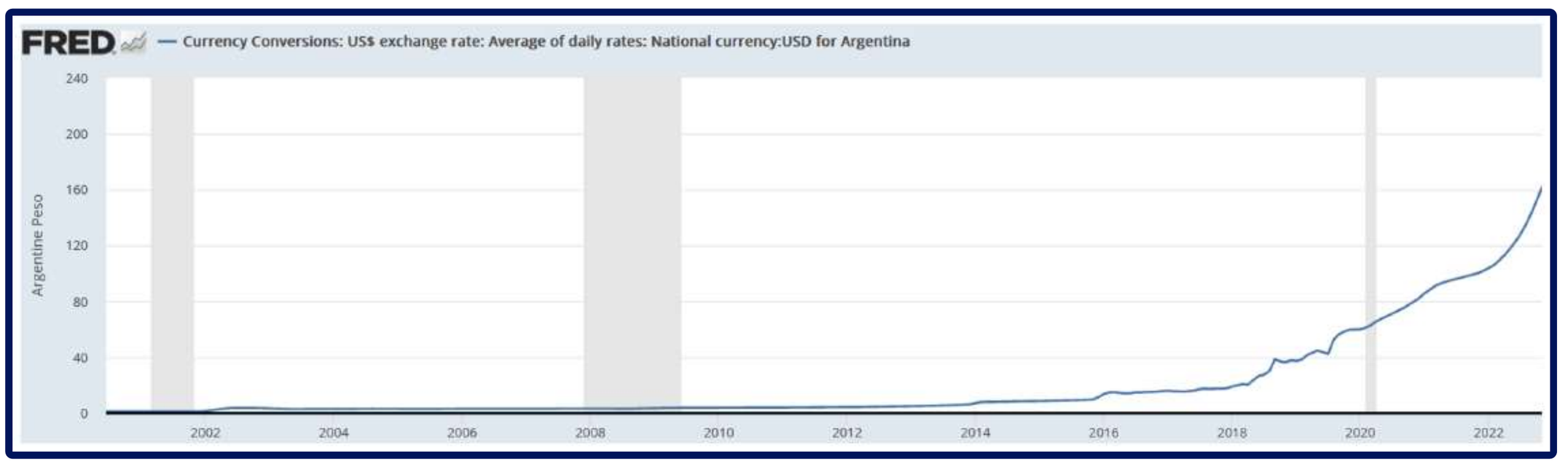
Venezuelan Bolivar



Turkish Lira



Argentinian Peso



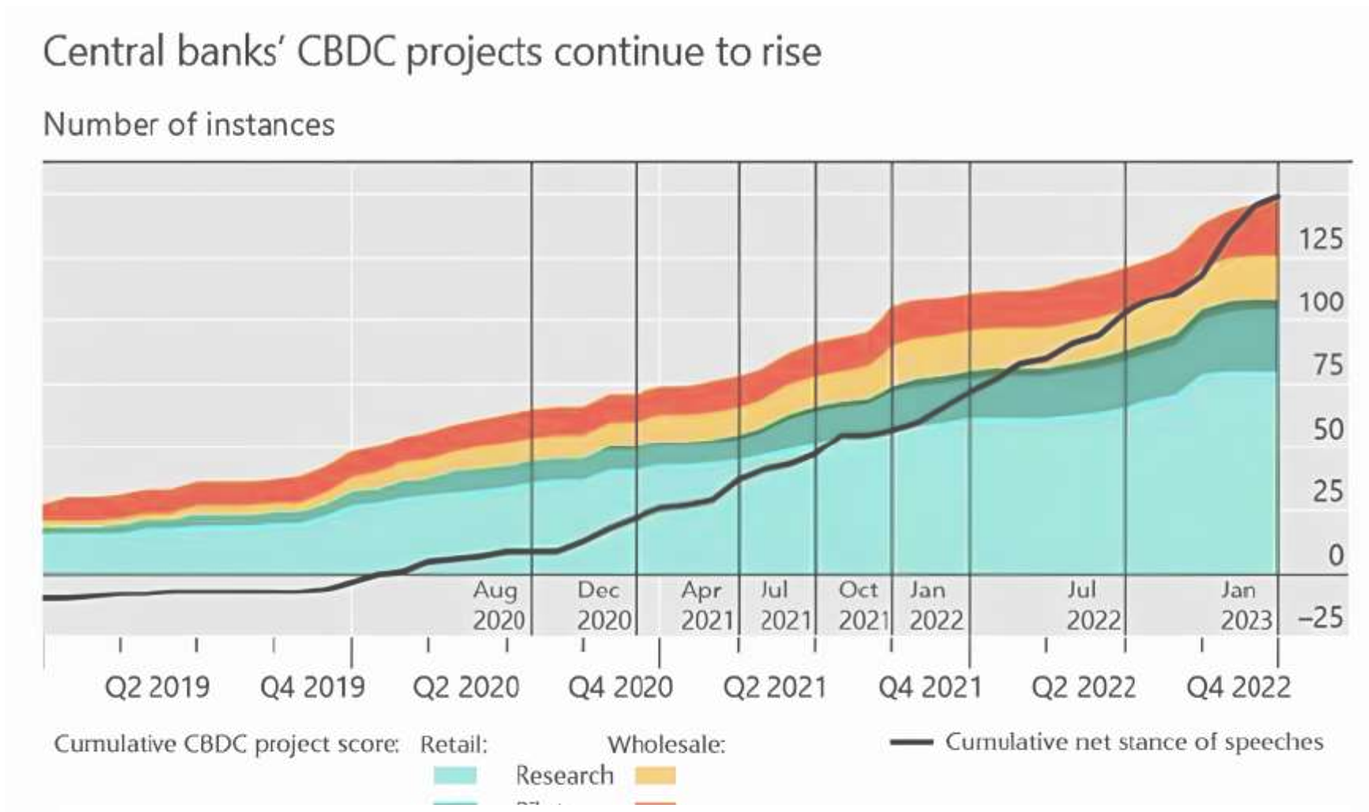
In the past, these same people would go to great lengths to save physical USD for the same purpose. With USD stablecoins transacting on open networks, it was and is now markedly easier for individuals and businesses to receive and manage digital USD with less physical security risk and with an increase in mobility and payment options.

CBDCs:

CBDC's started to gain more traction over the past few years, with the Bank for International Settlements (BIS) reporting growth in the number of projects and positive sentiment in central bank governors' speeches (see figure X below). CBDCs are an extension of central bank money in digital form ¬– an addition to the two existing types of central bank money: physical notes and coins, and reserves (which are only held by commercial banks). CBDCs are considered a technology upgrade to national currency; a tool that could enable central banks to monitor economic activity in real time and transmit monetary policy in a more direct manner. For users, CBDCs provide people and businesses with access to risk-free central[9] bank money, especially as cash use is declining in many nations. CBDCs should also provide financial institutions of all shapes and sizes with access to a common transaction and settlement network at very low cost, enabling co-opetition in the payments space. While most central banks are considering private permissioned ledgers for issuing CBDCs, it is technically possible for central banks to issue digital versions of their currency on multiple layer 1s, including open networks like Ethereum and Stellar, for example. In the wholesale context, CBDCs represent a technological upgrade for real-time gross settlement (RTGS) networks and could drastically improve settlement time and cost, especially in cross-currency use-cases, freeing up significant liquidity for many players worldwide. Overall, central banks require a technology upgrade to continue to achieve their mandate in a fast-evolving fintech world – see below quote from the European Central Bank's (ECB) Fabio Panetta for more on this point.

"However, regulation and taxation alone will not be sufficient to address the shortcomings of cryptos. To build solid foundations for the digital finance ecosystem, we need a risk-free and dependable digital settlement asset, which can only be provided by central bank money. That is why the ECB and central banks around the world are working on both retail and wholesale central bank digital currencies. By preserving the role of central bank money as the anchor of the payment system, central banks will safeguard the trust on which private forms of money ultimately depend."

- Fabio Panetta



Source: Kosse, A., & Mattei, I. (2022, May). *Gaining momentum – results of the 2021 BIS survey on Central Bank Digital Currencies*. The Bank for International Settlements. https://www.bis.org/publ/bppdf/bispap125.htm

[9] Panetta, F. (2022, February). *Central Bank Digital Currencies: Defining the problems, designing the solutions*. European Central Bank. https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220218_1~938e881b13.en.html#:~:text=Confidence%20in%20private%20means%20of,%2C%20its%20credibility%2C%20its%20authority

Controversy

Of the three assets mentioned above, crypto and stablecoins have predominantly been the recipients of criticism and are hotbeds for controversy for the past few years. From allegations of terrorism financing, money laundering and drug trafficking[10], to slanderous comments from financial magnates[11], crypto and stablecoins are regularly featured in the news in a negative light, exacerbated by the significant cases of fraud perpetrated by private sector players that came to light throughout 2022[12]. Even though there are a growing number of revered academics and investors who are supportive of the growth and development of crypto and stablecoins[13], opposition to the asset class also continues to grow, with the SEC and CFTC now in a turf war to regulate the space while initiating lawsuits against multiple private sector players[14] [15] .

More recently, CBDCs have come under scrutiny with several American politicians introducing bills that would ban the central bank from deploying CBDCs to the market[16] [17]. Critics say that CBDCs could shift more power into the hands of the government to control and surveil transactions, program money in ways that do not serve the public interest and put commercial bank funding at risk which could decrease their capacity to lend.

While these concerns are valid, the people focused on building and deploying CBDC platforms today are establishing both technical and policy-driven solutions to address and mitigate the risks, while still delivering the benefits that have been discussed in the extensive research released over the past ~7 years. While it is still early for CBDCs, with only five CBDCs live today (Nigeria, the Eastern Caribbean, The Bahamas, Jamaica, and China) and most G20 economies still years away from deploying, standards and best practices should be developed, scrutinized, refined, and tested to provide citizens and businesses with the assurances they require to feel comfortable using this next iteration of national currency.

---

[10] BBC. (2022, January 26). *Crypto money laundering rises 30%, report finds*. BBC News. https://www.bbc.com/news/technology-60072195

[11] King, T. (2018, May). *Warren Buffett says Bitcoin is "probably rat poison squared."* CNBC. https://www.cnbc.com/2018/05/05/warren-buffett-says-bitcoin-is-probably-rat-poison-squared.html

[12] Olinga, L. (2022, December). *FTX, Luna, Celsius, voyager: The year of crypto bankruptcies*. The Street Crypto. https://www.thestreet.com/cryptocurrency/ftx-luna-celsius-voyager-the-year-of-crypto-bankruptcies

[13] Nasdaq *Peter Diamandis says Bitcoin Equals Abundance for the world*. Nasdaq. (2022, February). https://www.nasdaq.com/articles/peter-diamandis-says-bitcoin-equals-abundance-for-the-world

[14] *Crypto Assets and Cyber Enforcement Actions*. U.S. Security and Exchange Commission. (2017, June). https://www.sec.gov/spotlight/cybersecurity-enforcement-actions

[15] *CFTC Charges Binance and Its Founder, Changpeng Zhao, with Willful Evasion of Federal Law and Operating an Illegal Digital Asset Derivatives Exchange*. The Commodity Futures Trading Commission of the United States. (2023, March). https://www.cftc.gov/PressRoom/PressReleases/8680-23

[16] *Sen. Cruz introduces legislation to prohibit the Fed from establishing a central bank digital currency*. Office of Senator Ted Cruz. (2023, March). https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-introduces-legislation-to-prohibit-the-fed-from-establishing-a-central-bank-digital-currency

[17] Blasi, W. (2023, March). *Ron DeSantis proposes law to ban a 'centralized digital dollar' in Florida.* MarketWatch. https://www.marketwatch.com/story/ron-desantis-proposes-law-to-ban-a-centralized-digital-dollarin-florida-43a3c27c

How can we ensure CBDCs are designed correctly?

What's clear from discussions and surveys surrounding the topic of CBDCs is that citizens are primarily concerned with privacy.

> *"The European Central Bank (ECB) has published today a comprehensive analysis of its public consultation on a digital euro. The analysis confirms, by and large, our initial findings: what the public and professionals want the most from such a digital currency is privacy (43%), followed by security (18%), the ability to pay across the euro area (11%), no additional costs (9%) and offline usability (8%)."*[18]

European concerns are consistent with the latest American opposition to CBDCs, which should come as no surprise. Thankfully, privacy can be solved for by implementing similar data segregation tactics used in financial services today, with additional technological solutions for privacy protection at the transaction network layer, including:

Zero Knowledge Proofs as discussed in "Designing a Central Bank Digital Currency with Support for Cash Like Privacy" (Gross et al, 2021)

Storing only transaction hashes on chain as done in Project Hamilton and detailed in "A High-Performance Payment Processing System Designed for Central Bank Digital Currencies." (Brownworth, et al, 2022)

Transaction channels created between the central bank and each intermediary, and each intermediary with one another, utilizing Hyperledger Fabric, detailed in the "Project Aber" report. (Saudi Central Bank, Central Bank of the UAE, 2020)

Chaumian blind signatures as detailed in "eCash 2.0: Inalienably private and quantum-resistant to counterfeiting" (Chaum & Moser, 2020)

Homomorphic encryption could also be used and was mentioned in the Bank of Canada's "Privacy in CBDC Technologies" (Darbha and Arora, 2020).

The difficulty that central banks face in assuring their populations that CBDCs have guaranteed privacy is not just a function of the technology used, but the degree to which they can be transparent about said technology – for national security and other reasons. One of the takeaways from the unprecedented growth of defi and web3 ecosystems includes the transparency of both policy and technical design. With CBDCs, policy is dynamic and decided by authorities at the central bank in response to economic conditions and expectations. The technical design, however, could be transparent through open-sourcing and other methods, provided they do not betray critical details of the system that could render it vulnerable to attack. Ultimately, standards need to be established that address critical privacy concerns, in addition to practical elements of operating critical national financial infrastructure.

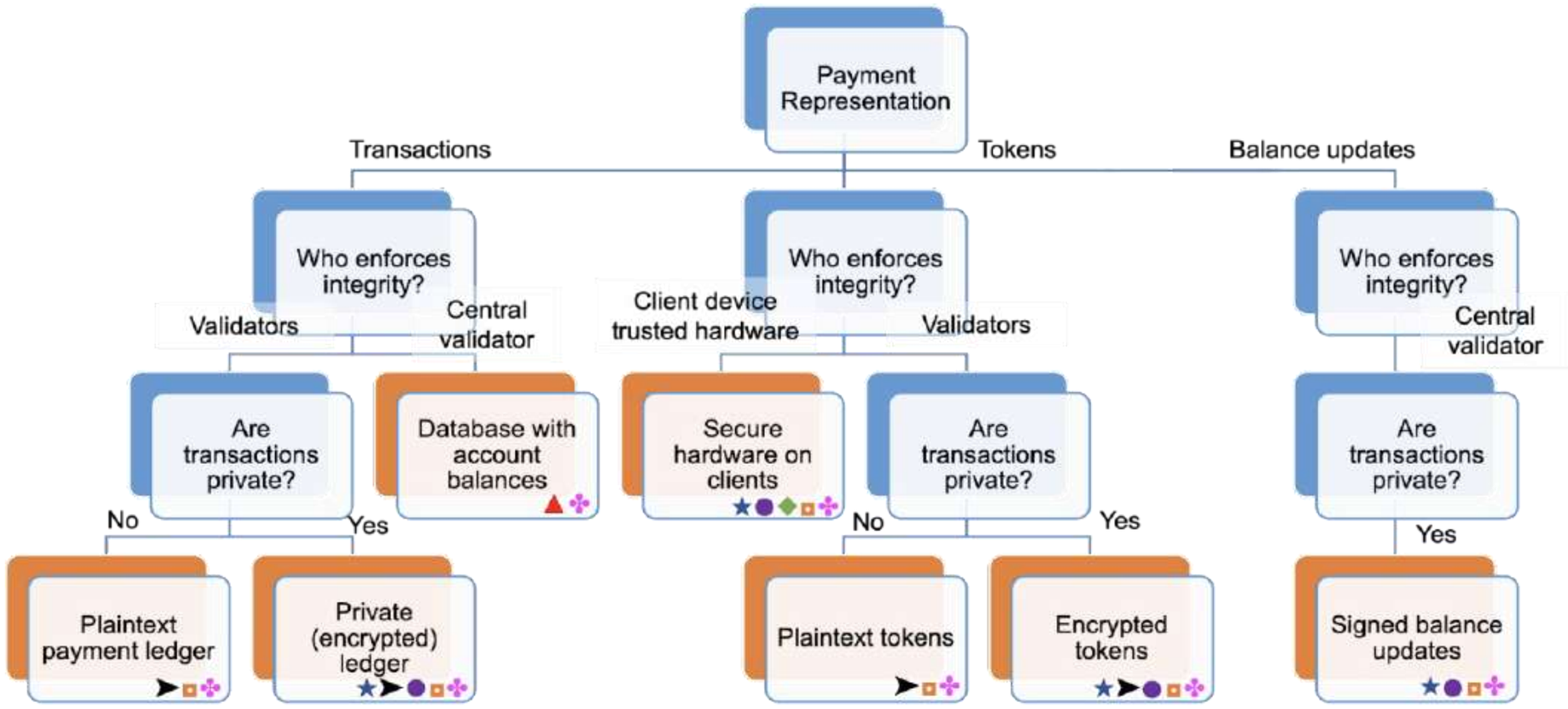
[18] European Central Bank. (2021, April). *ECB publishes the results of the public consultation on a digital euro*. European Central Bank. https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html

Standards Thus Far

The development and implementation of standards in CBDCs has not yet been achieved, however many helpful papers have been released to guide central banks in their CBDC journey, including reports from central banks that cover their efforts in testing CBDC technologies, many of which can be found on Bitt's CBDC News page. Papers from central bank adjacent institutions have been released over the past several years and include the World Economic Forum's Policymakers Toolkit, Privacy and Confidentiality Options for CBDCs, and the Digital Currency Governance Consortium White Paper, including a CBDC Technology Decisions Mindmap from Bitt. The Atlantic Council's Missing Key: The challenge of cybersecurity and central bank digital currency provided a deeper look at practical technical decisions that need to be considered in designing a CBDC solution, including the following decision tree

:

Figure Y: CBDC Design Variants



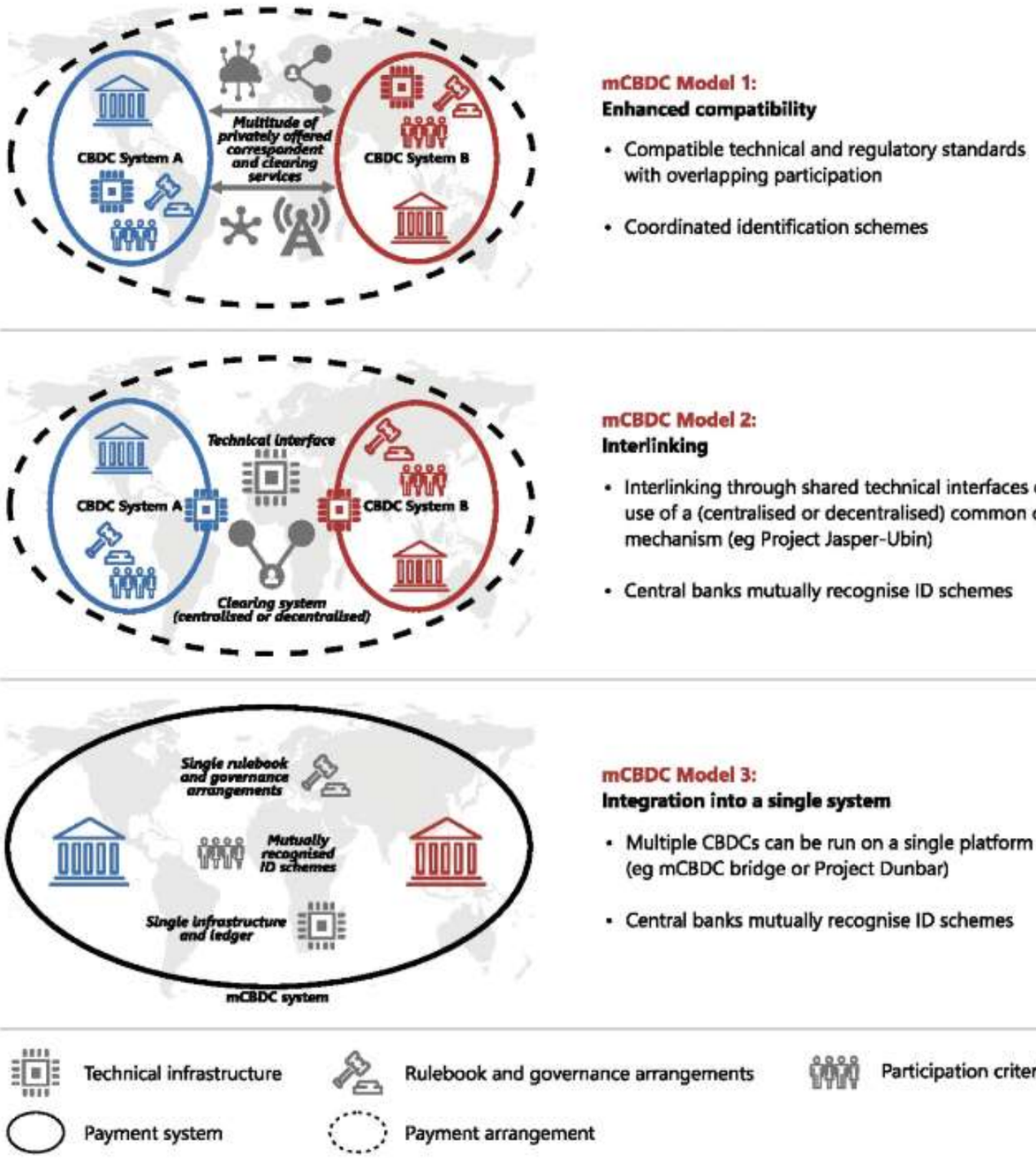
Source: Figure created by Giulia Fanti.
Note: Each variant is annotated with cybersecurity challenges that are new or elevated compared to the current financial system.

Many are looking to the BIS, who has been conducting CBDC research periodically since 2017, and more recently established and grew the Innovation Hub to experiment with components of CBDC systems. While the BIS released a document covering "Central bank digital currencies: foundational principles and core features," it stops short of technical standards that could be utilized by central banks and developers of CBDC technology. Others are looking to bodies like the International Organization for Standardization (ISO), who were quick to initiate a blockchain standard ISO/TC307 but hasn't covered the ins and outs of CBDCs.

While ISO20022 is relevant for interoperability efforts in CBDCs as a message formatting standard, it does not include deeper technology standards that are required to mitigate the many risks inherent in CBDC systems. Standards are required to ensure fundamental elements, including security and resiliency, are properly implemented in CBDC systems, but given the concerns stated above, standards that delineate the appropriate treatment of all system and user data have yet to be created and recognized by central banks worldwide. Ultimately, in a data-centric world we need data -centric standards for this next iteration of public money. A system that provides assurances regarding the creation, segregation, storage, and transfer of all types of data generated by its users is more likely to be trusted and trafficked by retail and enterprise users alike.

Perhaps as CBDCs become more advanced, bodies such as the World Wide Web Consortium (W3C), International Standards Organization (ISO), or others will propose standards that address the difficult and complex challenges posed by the introduction and adoption of CBDCs, especially across borders. This seems even more appropriate considering W3C's focus has consistently been on security, privacy, interoperability and accessibility. W3C's existing standards for web-based technologies are widely adopted throughout many industries and have significantly contributed to the advancement of online commerce, among many other areas. W3C's recent effort to standardize Decentralized Identifiers (DIDs) is also highly relevant in the discussion of CBDCs, aiming to provide individuals with a way to safeguard their identity with assurances of verifiability, portability, and privacy – each being fundamental elements in the context of CBDC systems.

Interoperability can be enabled via "multi-CBDC arrangements" Graph 6



Standards will not only enable consumer protection and privacy, but also highly valued interoperability for the efficient execution of cross currency exchange, as depicted in BIS Survey 116 CBDCs beyond borders: results from a survey of central banks.

Considerations for Composite Currency Systems

The value propositions, use-cases, and technological components of crypto and CBDCs differ substantially in their current form, and yet some of us see a composite financial system of the future taking shape where these assets coexist and interoperate to service users with a

Could CBDCs be used in DeFi? Yes, and under numerous configurations for multiple use cases. While most central banks have utilized private permissioned ledgers for their CBDC efforts to date, some have experimented with public permissionless ledgers, including Norges Bank's ERC20 token for the eKroner (not yet in circulation). Furthermore, central banks need not restrict the minting and issuance of CBDC to one network; CBDCs could be circulated on multiple underlying transaction networks, both decentralized and private. Furthermore, within the categories of "decentralized" and "private" exist other configurations, such as federated networks on decentralized ledgers (e.g., Liquid Network) and distributed private networks with multiple central bank administrators (mCBDC).

If central banks enable the circulation of their CBDC on permissionless, open L1s, they could easily be integrated with the most heavily trafficked platforms like Curve, Aave, OpenSea, and other DEXs and lending platforms for use in DeFi. If central banks do not issue on permissionless open L1s, but they allow stablecoin operators to hold CBDCs as collateral for permissionless stablecoins, bridges could be built that offer instant redemption between stablecoins and CBDCs therefore limiting bank-run scenarios for financial institutions holding stablecoin reserves, or the forced sale of other reserve assets such as t-bills. While holding CBDCs in reserve for stablecoins would limit the profitability of stablecoin operators to the interest rate applied to said reserve CBDCs, it could reduce the risk of financial stability brought on by mass stablecoin redemptions. In either case, robust and detailed technical standards need to be established to define and mitigate the risks associated with each design choice made by central banks and their technology providers.

Where do we go from here?

One thing is for sure: we require sensible regulations on all new forms of digital assets and currencies that enable growth and development of the space, while ensuring businesses and talent don't flee to areas with lacking or no regulation at all. We also need sensible transparent discussions regarding how to implement CBDCs in a way that can serve the market of enterprise and retail users while providing the central bank with the tools it needs to achieve its mandate in a more effective manner. The tendency for regulatory powers to grow and control an increasing number of activities, while hopefully rooted in good intention, could lead to undesirable outcomes for all who find themselves within their purview. Consider the development of the internet itself, when the TCP/IP standard was formalized and implemented for ARPANET, the Department of Defense warned of the risks of espionage and other threats to national security. There were even discussions about attempting to shut down the internet in the 80s, due to these concerns. The warnings were informed by the reality that TCP/IP would enable networks all over the globe to become interconnected for hosting and sharing all kinds of data. The outcome would be a network that was incapable of being governed in its entirety by the US government. It led to arguably the most significant development in the history of the human species, enabling instant connection worldwide and the creation of tremendous wealth. As new types of money emerge from this network, and national currencies evolve to properly leverage the internet, we hope to create and experience a financial system that meets the needs of all people in the years to come.

About Bitt

Bitt is a global financial technology company that provides digital currency solutions to central banks, financial institutions, and ecosystem participants worldwide. Bitt's Digital Currency Management System (DCMS) is the secure infrastructure that multiple monetary authorities use to deploy CBDCs, enables financial institutions to integrate a variety of digital currencies into their financial service offerings. Bitt's DCMS has been deployed in 12 countries across Africa, Central America, Europe, and the Caribbean. Bitt is a portfolio company of Medici Ventures, L.P., a blockchain-focused investment fund.

Contact Us

For media enquiries, contact marketing@bitt.com
For all other enquiries, contact info@bitt.com