Infrastructure and Design of Central Bank Digital Currencies

#SALMANQADIR

A RESEARCH REPORT BY BISON TRAILS

Infrastructure and Design of Central Bank Digital Currencies

Exploring the core design choices of CBDCs, along with the infrastructure and development needed to support them.

By Bison Trails • May 2021

ACKNOWLEDGEMENTS

This report would not exist without the support of the entire Bison Trails herd, and the expertise of the authors, editors, reviewers, and researchers who joined us along the way.

We thank Jemayel Khawaja for his large contributions to the body of this work. We would also like to thank Helen Rhee and Philippe Bungabong for their contributions, and to acknowledge the support of Monica Desai of Kleiner Perkins, and Arti Villa Chandok, Viktor Bunin, Erin Nolan, Evan Weiss, Liz Ralston, Serra Saridereli, Melissa Nelson, Casson Rosenblatt, and Mark Forscher of Bison Trails.

Contents

I. Introduction

Central Bank Digital Currencies, commonly known as CBDCs, are gradually moving towards global implementation with complex implications for international financial systems. CBDCs represent not only currencies in digital formats, but also a new digital medium of exchange, settlement, and payment verification—one with the potential to restructure the global financial system and the way trades are settled.

Competition for fiscal sovereignty from decentralized digital currencies and calls to update public monetary infrastructure have increased the pressure on central banks to develop CBDCs. Often built on distributed ledger technologies (DLTs), most prominently blockchains, a successful CBDC must strike the delicate balance between the needs of the government and its citizens by maximizing the benefits of technology for financial systems and limiting the potential threats to users' privacy. There is no off-the-shelf solution. Central banks must prioritize their goals for this new system and design their CBDC from there.

According to the International Monetary Fund's 2020 Working Paper report[1] on the central bank and monetary law considerations of CBDCs, there are four critical axes of consideration for the design features of all CBDCs:

- whether the network will be account-based or token-based;
- whether the CBDC will be issued for wholesale, retail, or general use;
- whether the currency will have direct, indirect, or hybrid issuance;
- and whether the network will operate in a centralized or decentralized manner.

This report analyzes each of these four axes and the implications each choice has on the infrastructure needed to support them.

1 Bossu, W., Itatani, M., Margulis, C., Rossi, A., Weenik, H. and Yoshinaga, A., 2020. Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations. International Monetary Fund Working Papers, [online] Available at: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827> [Accessed 17 December 2020].

II. The current state of CBDC development

A central bank's foundational role in its economy hinges upon a legal monopoly over the supply of domestic currency—cash, fiat, paper reserves. However, over the last decade, global trends have shifted away from traditional finance towards decentralization and digital currencies, and mainstream adoption of alternative payment methods appears imminent. The growing pressure for faster, more efficient payment rails and technological evolution portends a challenge to central banks' monetary sovereignty.

Central Bank Digital Currencies are an answer to this challenge. Around 80% of central banks across the globe have begun to explore CBDCs, with 40% already testing proofs-of-concept. Along with protecting monetary sovereignty, CBDCs are seen as a new means of spurring technological innovation and promoting economic inclusion within a nation and globally. Almost 2 billion people worldwide remain unbanked and outside the financial system; almost 25% of the United States is considered to be at least underbanked. Optimistically, CBDCs represent an opportunity to broaden this population's access to financial services while radically updating public monetary infrastructure.

"CBDCs can improve on existing currency models by using permissionless systems to enhance trust between constituents and their governing bodies," explains Bison Trails' Co-Founder and CEO Joe Lallouz. "While constituents maintain access, and utility of their money, the governing body retains management of the monetary supply—likely with highly updated and powerful new levers for asserting monetary policy. This combines defining elements of public cryptocurrencies and central banks into a very beneficial, happy medium."

The blockchain and DLT solutions used in CBDC prototypes to manage ledgers represent varying levels of decentralization. Most projects so far have chosen private, permissioned iterations of open-source and public blockchain technology to furnish pilots. In particular, Corda, Fabric, and Quorum have successfully proven that blockchain is a formidable technology for the development of CBDCs, at least as a prototype. More recently, next-generation public networks are being used for high profile CBDC projects, like Banque de France's Digital Euro program, built on Tezos, and the Marshall Islands' pioneering Sovereign currency, built on Algorand.

"While neither blockchain technology nor a decentralized architecture is a requirement for a functional CBDC infrastructure, either will provide substantial benefits in creating greater trust through permissionless access and distributed, peer-to-peer systems," explains Joe Lallouz. "While some banks will choose to roll out what is essentially a digital version of cash with a structure that mimics current financial models, innovation will hopefully trend towards currencies that interoperate with other currencies, financial systems, and the emerging global, decentralized digital asset landscape. In such a case, a CBDC's level of interoperability will be a key value proposition of the asset."

Expertise in the infrastructural components of multiple blockchains is critical for successful CBDC development as the ability to interoperate with different chains is becoming more of a requirement for the successful implementation of a CBDC. Additionally, exploring how different chains interact with each other can help to illuminate aspects of how the diverse players in traditional financial infrastructure—banks, retail users, and private companies, each with their own proprietary systems—can in turn become interoperable with a CBDC network and each other.

A specific understanding of diverse protocols' infrastructures—how the Algorand network supports multisignature algorithms, for example, or how running different daemons on a Tezos Baker can help process information about the state of the chain—is not only a primary element of the models utilized by CBDC proofs-of-concept, but is also a key aspect for considering how diverse stakeholders such as banks, retail users, and private companies will interact with CBDC technology.

It's difficult to become proficient in building for the abundance of protocols leading the ecosystem today, due to their widely varying governance forms, algorithmic mechanisms, and application interfaces. However, having expertise in how multiple protocols work provides essential knowledge of the entire ecosystem's interoperability, a key aspect through which to prepare for the diverse obstacles facing the development of CBDCs.

Global Landscape of CBDC Implementation

Countries around the world, from Canada and Singapore to Saudi Arabia and Uruguay, have begun dedicating resources to developing a digital financial system to update central banks. They have initiated proof-of-concept (PoC) projects exploring the application of distributed ledger technology (DLT) in payment systems to improve performance and accessibility.

1 SWEDEN *(e-Krona)* Initiated in 2017, the pioneering e-Krona program accommodates the rapid digitization of Sweden's economy with payment, deposit, and transfer capabilities for a digitized Krona utilizing R3 Corda DLT technology. The Swedish Riksbank's study of transitioning the country entirely to a digital currency is expected to be completed in November of 2022. Sweden is on course to be cashless by 2025.

2 URUGUAY *(e-Peso)* A successful pilot of the e-Peso concluded in early 2018; it issued and distributed digital banknotes for use in P2P, B2B, and B2C payments. Eschewing DLT for digital wallet tech operated via a state-owned telecom provider, the system included anonymous P2P transactions, offline transfer capability via mobile phones, and unique cryptographic signatures that include all information normally captured on a physical banknote (serial number, guarantee, etc.). Reportedly, the Uruguayan Central bank is waiting on other countries to launch their own CBDC solutions prior to fully implementing the e-Peso.

3 UKRAINE *(e-Hryvnia)* The exploratory e-Hryvnia ran throughout 2018, and experimented with both centralized and decentralized infrastructure models. The pilot operated on a private version of the Stellar blockchain, concluding that private-public sector collaboration is key to innovation and successful implementation. In January of 2021 the Ministry of Digital Transformation of Ukraine signed a MOU with the Stellar Development Foundation for Stellar to help Ukraine develop their official CBDC, noting the protocol's ability to achieve consensus with issuer-enforced finality as one of its benefits.

4 BAHAMAS *(Sand Dollar)* The Bahamanian Project Sand Dollar initiative was announced in 2017, and is the first officially circulated CBDC in the world following its full launch in October of 2020. The Sand Dollar's heavily centralized infrastructure incorporates compliance mechanisms, retail banks, merchant services, B2B payments, and a mobile-first interface (the Island Pay wallet). Its underlying technology integrates a DLT framework with blockchain hardware nodes and wireless communication networks. In February of 2021 Mastercard launched full support for the Sand Dollar, a huge leap for CBDCs announced alongside an update to Island Pay that furthers financial integration by allowing users to toggle between Sand Dollars or regular dollars when sending transactions.

5 EASTERN CARIBBEAN *(DCash)* The Eastern Caribbean Central Bank (ECCB)—which issues the USD-pegged Eastern Carribean Dollar to eight member states—initiated the DXCD Caribe in 2019, its Hyperledger Fabric-built CBDC developed in partnership with solution provider Bitt. The Eastern Carribbean's relatively small population, distributed set of island economies, and physical detachment from financial infrastructure presents a prime landscape for CBDC deployment to offset the difficulties of distributing and managing cash. The CBDC's architecture is divided into two parts: the Numa layer and Commerce layer. The Numa layer contains the ledger and can only be accessed via API, enabling merchants, wallets, and applications to connect to the CBDC, while the commerce layer includes a private network for central banks and financial institutions.

6 EU & JAPAN *(Project Stella)* The comprehensive, 2-year 4-phase collaborative proof-of-concept initiative covered four key phases of wholesale payment networks, via a DLT framework utilizing a number of platforms: large-scale payments, securities settlement, cross-border payments, and confidentiality/auditability. The findings unequivocally confirmed the viability of the technology, but noted that DLT technology must mature before being implemented on such a large scale in developed economies. While the Bank of Japan and European Central Bank continue to disseminate their learnings from Project Stella globally, the Bank of Japan has announced they will begin building upon Project Stella's findings to develop their own CBDC.

7 SINGAPORE *(Singapore Dollar)* Singapore provides a unique case study for CBDCs due to its size, development, and history of tech-forward governance. The extensive Project Ubin tokenized the Singapore Dollar for interbank payments, real-time gross settlements and blockchain interoperability, and also prototyped multi-currency, cross-border payments via commercial blockchains.

8 CHINA *(Digital Yuan)* Of all CDBC initiatives around the world, China's appears to be the most developed and closest to deployment on the largest scale. In development since 2014, the Digital Yuan is managed by the People's Bank of China and distributed to 9 state-owned banking and telecom giants. Large-scale public tests have included payment to municipal government workers in Suzhou, and a trial with Didi Chuxing, China's largest rideshare provider. More public tests are expected—including the 2022 Beijing Olympics—while China's state control and need for a monetary infrastructural update suggest that the rollout of the Digital Yuan is nearing imminent and will be a watershed moment for CBDC.

9 MARSHALL ISLANDS *(SOV)* Marshall Islands is moving towards the first public tokenized offering of its CBDC SOV, making the island nation the first to open participation for securing rights to a CBDC. Its bespoke Sovereign (SOV) blockchain is uniquely decentralized, though compliance is overseen by the government via the SOV Foundation, and is run on the Algorand network using smart contract governance.

10 AUSTRALIA *(RBA DLT)* A collaborative wholesale CBDC project between the Reserve Bank of Australia, Commonwealth Bank of Australia, National Australia Bank, and Australian-based financial services firm Perpetual was announced in October of 2020. The proof-of-concept will be run on an Ethereum-based DLT and developed in partnership with Consensys, utilizing a tokenized CBDC for syndicated loan processes. Specifically, the project is targeted at wholesale participants and their settlements, potentially enabled by cross-chain atomic swaps.

11 THAILAND, HONG KONG, UAE, CHINA *(m-CBDC Bridge)* The Multiple CBDC Bridge (m-CBDC Bridge) project is considered phase two of Project Inthanon-LionRock CBDC, a proof-of-concept executed by the Bank of Thailand and the Hong Kong Monetary Authority, which explored a Thai Baht/Hong Kong dollar cross-border payment network. Announced in February of 2021, m-CBDC Bridge brings the UAE and China into the group in the aim of creating a DLT-based real-time 24-hour payment and settlement bridge between the Middle East and Asia.

“While neither blockchain technology nor a decentralized architecture is a requirement for a functional CBDC infrastructure, either will provide substantial benefits in creating greater trust through permissionless access and distributed, peer-to-peer systems,” explains Joe Lallouz. “While some banks will choose to roll out what is essentially a digital version of cash with a structure that mimics current financial models, innovation will hopefully trend towards currencies that interoperate with other currencies, financial systems, and the emerging global, decentralized digital asset landscape. In such a case, a CBDC’s level of interoperability will be a key value proposition of the asset.”

Expertise in the infrastructural components of multiple blockchains is critical for successful CBDC development as the ability to interoperate with different chains is becoming more of a requirement for the successful implementation of a CBDC. Additionally, exploring how different chains interact with each other can help to illuminate aspects of how the diverse players in traditional financial infrastructure—banks, retail users, and private companies, each with their own proprietary systems—can in turn become interoperable with a CBDC network and each other.

A specific understanding of diverse protocols’ infrastructures—how the Algorand network supports multisignature algorithms, for example, or how running different daemons on a Tezos Baker can help process information about the state of the chain—is not only a primary element of the models utilized by CBDC proofs-of-concept, but is also a key aspect for considering how diverse stakeholders such as banks, retail users, and private companies will interact with CBDC technology.

It’s difficult to become proficient in building for the abundance of protocols leading the ecosystem today, due to their widely varying governance forms, algorithmic mechanisms, and application interfaces. However, having expertise in how multiple protocols work provides essential knowledge of the entire ecosystem’s interoperability, a key aspect through which to prepare for the diverse obstacles facing the development of CBDCs.

Private solutions as a motivator

Central banks are also motivated to develop CBDCs because of the creation of digital assets by private entities, most notably Diem[2] (formerly known as Libra). Diem offers a whole new paradigm in economics: a diverse association of enterprise and social impact stakeholders developing digital currencies on a permissioned, open-source chain built with the most cutting edge tech—with a built-in global market and limited barriers for growth once live.

Although famously reticent to develop a US digital dollar, Federal Reserve Chairman Jerome Powell acknowledged the inevitability of a CBDC given the highly technical private option Diem will provide, stating that "[Diem] was a bit of a wakeup call that this is coming fast, and could come in a way that is widespread and systemically important fairly quickly—if you use one of these big tech networks like [Diem] did."[3] In October 2020, Powell announced the US Federal Reserve was in the midst of extensive research and public consultation regarding a digital dollar that will complement existing cash systems, and in March of 2021 he spoke to the COVID-19 virus further increasing the speed of executing that endeavor.

Similarly, the development of Diem is considered a catalyst for the Chinese government to accelerate its plans for its Digital Currency Electronic Payment (DCEP), also abbreviated as the digital RMB or e-CNY, the country's forthcoming national digital currency issued by the state bank People's Bank of China (PBoC). Acknowledging the new reality of Bitcoin and blockchain-driven ICOs, the Chinese government remains intent on establishing itself as a central player in the emerging global digital currency market.

In turn, the accelerated rollout of the DCEP has driven other nations to redouble efforts around their own research and development on CBDCs.

2 Bison Trails and its parent company Coinbase Global, Inc. are members of the Diem Association and, as such, have a financial interest in the Diem Network.

3 U.S. Congressman French Hill. 2020. Transcript: US Congressman Raises Spectre Of Threat Of Digital Renminbi CBDC To US Dollar. Fed Governor Responds. [online] Available at: <https://hill.house.gov/news/documentsingle.aspx?DocumentID=6651> [Accessed 17 December 2020].

These developments have significantly shortened the time frame for execution needed to achieve early mover status.

This early mover status may be an important factor in the competitiveness of a given nation's currency. Given the advantages that CBDCs hold over their fiat comparisons—and potentially over other CBDCs—including speed and more efficient reserve settlement, early adoption of a functional CBDC has the potential to edge up a currency's competitive advantage. As Diem and China's DCEP each near rollout, pundits increasingly are questioned in the media regarding whether these digital currencies will dismantle the USD's status as the primary international reserve currency.

Although the mere existence of Diem has pushed the international race to develop a CBDC forward, it is the strategic manner in which the network is being built that may have the biggest influence on the international financial sector. As a founding member of the Diem Association and member of its Technical Steering Committee, Bison Trails has participated in the development of the technical infrastructure of the Diem network.

"Diem has done a good job in the way that they built their technology stack, for example how permissioning works and the way that the chain is architected from its base layer to include auditing and smart contracting for consensus," explains Bison Trails' co-founder and CTO Aaron Henshaw. "It ensures that all transactions run through checks that are audited and controlled, that you don't create opportunities for smart contract bugs to introduce certain types of risk to the system. It's built into how the consensus works, how it creates state, and how things come in and out of the state machine."

The intense focus on the base architecture and design of Diem underscores the fact that these decisions are critical to the success of CBDC execution. It is clear that countries currently testing CBDC options are not only driven by time-based pressure, but more importantly by the desire to implement the strongest and most secure technological product possible.

III. CBDC design choices and their infrastructural considerations

With CBDC development still in the proof-of-concept stage, CBDC design is in the discovery phase. The models discussed below are best considered as a starting point rather than a rigidly prescribed framework. In addition, no design choice is made in a vacuum. Each choice impacts the next, often with one design option precluding the opportunity to use another.

For example, the decision of whether a CBDC network will be account-based or token-based may rely heavily on its choice to enable retail rather than wholesale use, which in turn may determine if the network will be better suited to operate in a centralized or decentralized manner, and so on. They are also not binary choices. Most CBDC proofs-of-concept have designed protocols somewhere in the middle of these axes. However, analyzing these four key choices independently provides an important introductory lens to understand the infrastructure needs of CBDCs.

Account-based or token-based

A CBDC network can be account-based or token-based; this choice is primarily about whether the network will carry digital balances in accounts held by a central bank, or if the central bank will issue a digital token that does not have an account-based relationship with the end user.

According to an August 2020 publication from the Federal Reserve Bank of New York, the legal distinction between these options is that "an account-based system requires verifying the identity of the payer, while a token-based system requires verifying the validity of the object used to pay."[4] Each option requires a distinct set-up for know-your-customer (KYC), anti-money-laundering (AML), and counter-terrorist-financing (CTF) checks as well as ownership and key management within the CBDC network.

Technological requirements for verifying identity

Account-based CBDCs can use smart contracts to verify account holder identity in compliance with KYC, AML, and CTF regulation. A smart contract is a self-executing program on a blockchain; it controls and/or documents events or actions according to preset terms. Smart contracts define the rules and penalties of an agreement, and also enforce compliance. Because smart contacts are automatic, much of the cost and capacity burden of imposing KYC for an account-based CBDC can be removed—as they execute immutably, it's possible to build AML/KYC controls and checks into the account structure, thus reducing the associated operational costs.

As Dan Doney, CEO of digital currency-focused financial logistics company Securrency, said to American Banker in his analysis of CBDC development, "Banks spend $270 billion a year on compliance functions. We believe you can automate

4 Garratt, R., Lee, M., Malone, B. and Martin, A., 2020. Token- or Account-Based? A Digital Currency Can Be Both - Liberty Street Economics. Federal Reserve Bank of New York, [online] Available at: <https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both.html> [Accessed 17 December 2020].

most of those through smart digital currencies."[5]

Implementing smart contract functionality is not, however, a simple task. A survey of over 200 developers and stakeholders on smart contract script development delineate a few of the key challenges as: the complexities of secure smart contract code; the limitations of current programming languages and virtual machines in this nascent ecosystem; and the difficulty moderating performance of smart contracts under resource-constrained operating environments.[6]

CBDC proof-of-concept developers interested in using smart contracts will likely want to partner with established players in the blockchain space, such as existing infrastructure providers, smart contract auditing teams, and development teams, to ensure their smart contract's code not only fits in the CBDC's parameters but can be executed effectively and securely.

"If you only make a ledger without the primitives that make all of these other networks so powerful, like an actual, proper smart contracting language and platform, you'll miss out on a tremendous amount of the benefits."

— AARON HENSHAW, BISON TRAILS CTO

Smart contracts can also induce consumer adoption because of their value for decentralized finance applications, commonly known as DeFi apps, and inter-chain operability. To be competitive against public blockchains CBDCs will want to consider this possibility as an important feature. As Aaron Henshaw explains, "If you only make a ledger without the primitives that make all of these other

5 Lang, H., 2020. A Fed Digital Currency Looks Inevitable. So Do The Problems.. [online] American Banker. Available at: <https://www.americanbanker.com/podcast/a-fed-digital-currency-looks-inevitable-so-do-the-problems> [Accessed 18 December 2020].

6 ZOU, Weiqin; LO, David; KOCHHAR, Pavneet Singh; LE, Xuan-Bach D.; XIA, Xin; FENG, Yang; CHEN, Zhenyu; and XU, Baowen. Smart contract development: Challenges and opportunities. (2019). IEEE Transactions on Software Engineering. 1-20. Research Collection School Of Information Systems. Available at: <https://ink.library.smu.edu.sg/sis_research/4496> [Accessed 18 December 2020]

networks so powerful, like an actual, proper smart contracting language and platform, you'll miss out on a tremendous amount of the benefits and potential for powerful and scalable applications to be built on top of the Diem network."

Smart contract security at creation is of the utmost importance, particularly because once a smart contract is executed it cannot be changed. In particular, the valuable "honeypot" of those CBDCs with large adoption will likely make their smart contracts alluring targets for attacks from all angles. CBDC developers can learn a lot from audits of existing smart contract implementations on topics such as preventing re-entrance or front-running. Countries with limited resources could potentially integrate existing smart contract code into their project, but the use of existing codebases requires additional diligence in order to ensure vulnerabilities are not passed on.

Another facet of verifying identity, both account ownership and key management differ for account-based and token-based CBDCs. The IMF frames this concept as 'I am therefore I own' vs. 'I know therefore I own'. In account-based CBDC implementations, the identity of a user allows the user to access their funds—'I am therefore I own.'[7] Just as this framework allows for the use of smart contracts to prove user identity for account creation, smart contracts can also be used to verify the identity of a user who has lost access to their account and needs to regain access to their funds.

Although this method is likely a better user experience, CBDCs will need to account for the structure of account storage in their design. Some account-based networks, such as Ethereum, record a combination of permanent and transient data using tries data structures that include transaction data, account balances (referred to as the network's global state), and receipts. The smart contract data is tied to each account address, referenced in the global state itself, thus reducing the need for on-chain processing and storage. These models require the development of adjoining tools to allow interfacing products to query the status of accounts in the network.

7 Bossu, W., Itatani, M., Margulis, C., Rossi, A., Weenik, H. and Yoshinaga, A., 2020. Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations. International Monetary Fund Working Papers, [online] Available at: <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827> [Accessed 17 December 2020].

Generally, in token-based DLT networks, users hold a private key which enables them to send or sign their funds—'I know therefore I own.' The use of self-custodied private keys in a token-based CBDC could help preserve some of the privacy of cash, but carries the added risk that a user could lose access to their funds if their key is lost—or that their funds could be stolen if their key is compromised.

Token-based networks generally do not provide any custody options for private keys, as any storage or transfer of the private key opens up the associated funds to security concerns. This lack of consideration for KYC and AML mirrors the use of cash, where the burden is moved to the transactional level. Token-based networks also open up opportunities for private-sector development of key management tools and wallets.

There are pros and cons to these opportunities. On the one hand, token-based CBDCs moving the responsibility of key management and KYC compliance to the private sector reduces the CBDC issuer's operational overhead, including the development of ways for third-party financial applications to interact with the network's stored account data. On the other hand, it raises issues around legal implications of currency ownership, including how third-party key management services and digital wallets could be regulated for consumer protection and AML compliance purposes.

QUERY & TRANSACT BY BISON TRAILS

Developing retail for account-based CBDCs

Query & Transact by Bison Trails allows applications to connect to real-time blockchain data, providing a robust link between off-chain systems and blockchain networks.

Enterprises developing financial tools to interface with account-based CBDCs can use Query & Transact to read data, monitor address balances, monitor transactions to make sure they make it onto the chain, and more.

Building with Query & Transact can enable financial institutions and enterprises to interact with CBDCs 24/7, without investing to develop capabilities in-house. Our Query & Transact read/write infrastructure processes billions of transactions per month, with the ability to supercharge adoption by making it incredibly easy to integrate and add support for CBDCs, regardless of what form they take.

Learn more at bisontrails.co/QT

CBDC in action: Account-based model

The Bahamanian Sand Dollar was the first CBDC in the world to launch following its full rollout in October of 2020. Its circulation in the Bahamas has been bolstered by early 2021 upgrades to the network, including full Mastercard support for Sand Dollar payments and an update allowing users of the central bank's mobile wallet to toggle between using Sand Dollars or USD for digital transactions. The speed and acceptance of the digital Sand Dollar is in no small part due to the difficulty of circulating cash and settling transactions between the remote auxiliary islands of the nation.

Very few details about the Bahamanian DLT network have been shared by the lead infrastructure development partner, NZIA. However, it is believed to be an account-based model given NZIA's acknowledgement of working with the teams powering IBM's Hyperledger Fabric and the Cortex network, both of which operate in a limited account-based manner.

FABRIC

IBM's Fabric is a permissioned blockchain that features a modular design with "pluggable" features that allow flexibility for customers and developers. The platform is composed of a network of bilateral, overlapping channels that connect each participant to one another. There is one ledger within each channel to maintain data privacy. Settlement finality within Fabric is reached after the transaction is validated against system rules set by predetermined, containerized smart contracts called chaincode. Container technology allows smart contracts to be pluggable and isolated from the rest of the system.

Retail users of the Bahamanian Sand Dollar can create a mobile or card-based wallet via their existing bank account, or, instead, may create a wallet directly with the Bahamanian Central Bank via the central bank-issued mobile app Island Pay. NZIA describes the network as using a combination push-pull payment rail system[8] which indicates there are accounts on the network that use smart contract infrastructure to verify that a merchant transaction was both requested by the merchant and sent by the user prior to a retail transfer of funds.

The choice to use an account-based model may be in part due to the Bahamas'

8 https://nzia.io/ [accessed 21 December 2020]

relatively small population; the developers would have less concern over the storage and CPU implications of a massively-expanding account set. In addition, it is likely the nation desired to use smart contracts to enable interchain operability, lower retail transaction speeds, and reduce the famously-high transaction fees faced by Bahamanian residents.

Perhaps most importantly to their use of the account-based model is the Central Bank of the Bahamas' stated goal of "universal access to banking services of a deposit account maintenance nature."[9] Currently, traditional banks lack the economic incentive to operate branches in remote regions of the Bahamas due to the cost of cross-island operation. Adoption of an account-based CBDC is an important opportunity for the Bahamas, and other island nations such as the Marshall Islands, to leapfrog generations worth of building physical financial infrastructure by providing digital account access directly to residents. Doing so has the potential of strengthening native economies and expanding financial inclusion by providing essential financial services to residents of the nation, while also permitting interoperability with the existing financial system via smart contract enablement.

Retail, general use, or wholesale

In order to determine if a CBDC is better implemented as an account-based or token-based model, developers will want to decide if it will be used for wholesale use, retail use, or both (referred to as general use).

- The retail model has the central bank issue currency directly to consumers for retail use. These models align well with account-based models, as individual users are effectively able to create accounts with the central bank and receive the CBDC directly from them. Retail models are generally considered to be the form of CBDC most widely available for use, and are primarily targeted at retail transactions rather than loans or settlements.

9 Central Bank of the Bahamas, 2019. Project Sand Dollar: A Bahamas Payments System Modernisation Initiative. Available at: <https://cdn.centralbankbahamas.com/download/022598600.pdf> [Accessed 22 December 2020].

- The wholesale model uses tokenized fiat to create a wholesale payment network, to increase efficiency within the existing current national finance infrastructure. The CBDC is issued to the existing account holders at central banks, such as real time gross settlement clients, clearinghouses, and foreign reserves managers.

Retail

Retail models require broader adoption than wholesale models; the CBDC must be accepted as a valid and accessible means of payment and an appropriate store of value by residents and businesses in addition to government agencies. This is in contrast to wholesale, permissioned networks, which only need the buy-in of participating members.

Given the need for wide adoption of a retail CBDC, its design must be accessible and easy to use in addition to having lower transaction fees and times than traditional financial networks. A CBDC's associated wallet technology can not be excessively technical for a user to operate; the infrastructure must be built to overcome technological barriers to entry, for example, by allowing SMS-based account access.

Most believe the infrastructure of retail CBDCs should be open rather than permissioned, allowing private enterprises to develop products and services on top of the CBDC network more easily. Single-click node infrastructure providers can provide enterprises and other private sector actors the opportunity to interact with and develop on the DLT without needing technical infrastructure knowledge in-house.

General use

General use models are designed so that the CBDC network can be used for both interbank wholesale transactions and direct retail issuance. The Bahaminian Sand Dollar, discussed in the previous section, can be considered a general use model, allowing both existing financial institutions to issue or settle with the central bank

using wholesale transactions and individual users to create accounts directly with the central bank.

Both retail and general models must consider how consumers and existing financial institutions will interact with the ledger. Secure read/write node infrastructure would allow financial institutions, and consumers through an enterprise or institution, to connect off-chain systems, such as traditional financial products and services, to the CBDC's DLT data.

Entities that build applications for the CBDC network can use read/write nodes to validate transactions, obtain information about said transactions, or to write data such as transfers or smart contract interactions to the chain. These types of interactions are critical for building third-party applications which can spur the expansion of retail uses. CBDC operators can benefit from using private sector partners to run and manage the read/write nodes they offer to these third-party institutions.

For example, while the Diem Network is a permissioned network operated by a secured and validated number of active association members, outside developers and financial institutions can access read/write node infrastructure on the Diem Network directly or via a private partner like Bison Trails. Providing read/write nodes increases opportunities to participate in the network without opening validation to the public sphere. However, financial institutions will still need to ensure any third-party provider operates their read/write node infrastructure with the proper security, regional redundancy, and authenticated API access.

Wholesale

The wholesale model, on the other hand, is a blockchain-based interbank settlement layer to digitize global backend financial infrastructure without the regulatory, adoption, and scaling complexities of retail or general models. Interbank prototypes are proving productive ground for substantive application of blockchain technology currently, or close to, available for production and release.

Wholesale settlement prototypes began in earnest in 2016. A trio of Quorum-inclusive projects all featuring ConsenSys as a partner—Project Khokha in South Africa (2018), Project Ubin in Singapore (2016-2010), and Project i2i in the Philippines (2019)—alongside Thailand's Project Inthanon (built on Corda), are building wholesale payment networks between currency-issuing central banks and financial institutions with a focus on interbank settlements.

Improving interbank settlements is one of the greatest benefits of upgrading to a DLT within the financial sector. Overnight processing of interbank payment settlements is no longer considered sufficient to meet the needs of the digital economy, but real-time interbank settlements create liquidity issues that can prevent central bank systems from settling. As banks within Real Time Gross Settlement (RTGS) generally settle with one another in the order in which payments come through instead of settling amongst each other multilaterally, banks can face backlogs of payments (referred to as gridlock) that they may have the liquidity for after settling with another bank, but not in the moment their payment needs to be made.

One solution to this problem is to build protocols with decentralized netting systems in place. Blockchain-based decentralized netting protocols are systems of smart contracts allowing trustless settlement between users of permissioned central networks, with transactions settled individually on a triaged basis.[10] Participants' payments can be settled immediately as long as the party sending the payment has sufficient funds and there are no higher-priority payments in their outgoing payment queue. After a defined validation period all interconnected nodes on the network will conduct multilateral settlement amongst each other, thus removing the conditions leading to gridlock while enabling real-time settlement.

Given the centrality of the interbank settlement processes to a central bank's function, any wholesale CBDC projects must ensure their node communication environments have adequate security contracts and have fail-proof distribution.

10 Cao, S., Yuan, Y., De Caro, A., Nandakumar, K., Elkhijaoui, K. and Hu, Y., 2020. Decentralized Privacy-Preserving Netting Protocol on Blockchain Payment Systems. Twenty-Fourth International Conference of Financial Cryptography and Data Security Preproceedings, [online] Available at: <https://fc20.ifca.ai/preproceedings/27.pdf> [Accessed 21 December 2020].

The use of zero-knowledge proofs within decentralized netting systems are an option for preserving account-holder privacy while still enabling interbank settlements.

CBDC in action: Wholesale

South Africa's Project Khokha provides an excellent case study of wholesale interbank settlement improvements via CBDC. A single interbank payment settlement in South Africa currently takes four steps to complete due to notification, confirmation, and reconciliation processes. The adoption of blockchain technology within Project Khokha reduces this process to a single step.

Project Khokha ran a decentralized, permissioned network to focus on interbank clearing and settlements between the South African Reserve Bank, seven central-bank appointed intermediary nodes, and ConsenSys, the technical partner. The project met its goal by improving the standards for transaction speed, block propagation times, and confidentiality.

The project also implemented a number of notable infrastructural innovations. First, each bank operated its own nodes and had the freedom to determine node architecture as long as it adhered to minimum specifications. This freedom resulted in both on-premise and cloud-based nodes in the network. A developed node infrastructure reduces the network's vulnerability to a single point of failure as exists in more centralized notary node models; it also improves the resiliency of

QUORUM

Quorum is a permissioned, private enterprise blockchain platform built on Ethereum using the Geth client. Quorum uses zero-knowledge proof transactions, allowing parties to transfer assets without revealing the sender, receiver, or quantity of the asset. The consensus mechanisms used for finality are the Raft algorithm or the Istanbul Byzantine Fault Tolerant (IBFT) algorithm. The main difference between the two algorithms is that IBFT can tolerate up to 33% of faulty parties in a network, while Raft assumes there are no malicious actors in a network. While Quorum excels in transaction privacy, distributed security, censorship resistance, and network resiliency, critics of its use in CBDC tech note its intrinsic decentralization means that it lags in transactional capacity due to the wider degree of consensus required.

the network by protecting against outages and common node failure.

Project Khokha was also acclaimed for the combinations of technological algorithms used to achieve resilience, confidentiality, and settlement finality in the system. For example, its implementation of a multi-tenant Istanbul Byzantine Fault Tolerance (IBFT) consensus mechanism proved successful in adding substantive technical decentralization to the architecture; a validator in a network utilizing IBFT consensus never needs to assume a block proposer is honest or correct as it requires multiple rounds of voting on each block by a set of validators instead. As a result, IBFT networks remain fault tolerant with a threshold of up to 33% of faulty parties in the network. In regards to privacy, Khokha's application of transaction hashing Pedersen Commitments and zero-knowledge range proofs showed promise in maintaining privacy in transactions.

South Africa announced a second proof-of-concept project, Project Khokha 2, in February of 2021. This second trial is targeted at exploring use of a wholesale settlement token to settle wholesale bond and debenture transactions on a permissioned blockchain.

In 2020, the Singapore Central Bank, alongside JP Morgan and Accenture, completed the 5th and final phase of a four year endeavor, Project Ubin. The project established standards for an international wholesale settlement network using smart contracts that were interoperable between multiple currencies and tokens across blockchain networks. The final report notably stated that blockchain technology has reached the maturity to bring such a project to market.

Interoperability in the design of wholesale settlement infrastructure will become a particularly key feature of future CBDC development, in light of the United States' Office of the Comptroller of the Currency's announcement that the national banking sector may use private blockchain networks to conduct interbank settlement and other banking activities.

Given their more limited roll-out considerations, there are many examples of wholesale model infrastructure from which to learn, even for retail and general

model CBDCs. For instance, a smaller nation interested in a retail model may learn from, for example, the innovative nodal infrastructure of Project Khokha to inform the development of a retail system using a network of existing financial institutions. An investigation of the different models of offering CBDCs to the public, either directly or via institution, can help a central bank to envision scaling a wholesale model to a retail offering.

Indirect (2-tier), direct (1-tier), or hybrid distribution

Central banks must consider whether the network will be designed with direct (or 1-tier) issuance, indirect (or 2-tier) issuance, or use a hybrid distribution architecture. Generally, only retail or general use networks will need to consider this choice extensively, but wholesale CBDCs may also consider how end users will access and use digital currencies.

In direct models of CBDC distribution architecture, central banks retain control of the underlying CBDC network and distribute currency directly to citizen accounts. Also referred to as the 'fed accounts' model, this model is essentially one in which central banks act as the national retail bank, handling all currency distribution and managing all ledgers. Direct models utilizing the account-based model would also manage all of the accounts in the network, whereas direct models utilizing a token-based model would manage token distribution. With indirect models, digital currency is distributed to citizens via commercial banks, with central banks backing the liabilities. Hybrid models of retail issuance may take many forms, but, in general, claims are made to a central bank with commercial banks handling payments.

Indirect

The indirect system is the most popular and has proven to be effective in this nascent phase, largely due to its resemblance to current financial systems and its

modular functionality. Indirect retail systems are defined by three levels of financial institutional interaction:

- Central banks are the primary source of CBDC minting and maintain ownership rights over the distributed network.
- Financial institutions directly interact with central banks, conducting wholesale transactions to release large sums of funds into the wider banking ecosystem.
- Retail institutions use layer-2 applications, i.e. applications built on top of the existing network, and potentially layer-2 blockchain solutions, to serve as the go-between for financial institutions and end-users.

In indirect models, users can interact with any decentralized application, decentralized finance solution, or other private investment opportunity they choose, as opposed to only using those provided by the central bank—just as there are a plethora of private financial integration options available in the traditional financial system. The free market can determine which solutions and networks provide users the most utility, thus spurring innovation and potentially greater commercial use of the CBDC.

The risk of hacks to the network is also reduced in the indirect model, as offering multiple retail options for CBDC users diversifies the custody options for the digital currency in circulation. The more retail options offered, the less of a lucrative target any one offering provides to a potential hacker. Central banks will likely enforce strict guidelines for the security of any retail distribution system in order to protect consumers, such as implementing security audits of code bases before launch.

The wholesale tier of an indirect CBDC must be designed to ensure the security of the lower issuance tiers, so that hacking into the wholesale portion of the network does not create a backdoor to a commercial bank's system or allow a hacker to ransom any keys they find.

Although these security measures are of utmost importance, an indirect CBDC

network is not a truly decentralized network, any centralized system is, at its core, a single point of failure should there be an issue with the central authority. This is as opposed to decentralized systems, which maintain security in part due to their inherent spread of authority cross-participant.

Additionally, retail solutions will have their functionality limited by the design and build of the underlying CBDC protocol; private development will need to make concessions around privacy, scalability, and cross-chain interoperability based on those limitations. KYC enforcement on the retail side would make the use of many current decentralized financial applications difficult. As such, one would not expect an indirect CBDC to lead to the same flourishing of DeFi seen in the decentralized blockchain ecosystem.

Due to their indirect-issuance, central banks building CBDC networks with indirect distribution models will have limited ability to directly control the design of payment rails. This circumstance is not entirely dissimilar to the traditional financial system—in which central banks are primarily concerned with inflation and liability rather than payment operations—but not having that level of control over the CBDC payment rail is a trade-off for central banks whose mission is to provide specific financial solutions to their countries (such as free account access). One way that a central bank can influence the availability of desired retail payment solutions is through the development and distribution of permissioned APIs. Concessions, however, must be made.

Developers of indirect models must also consider how to design DLT-specific procedures to inform network stakeholders, including retail and commercial banks and risk management operators, about updates, patches, items in need of escalation, and other events on the network. Participation platforms could be used to share metrics to help monitor infrastructure performance, such as node uptime, CPU usage, interconnected peers, and block height.

Of particular concern is the development of permissioned systems to inform financial institutions that operate nodes in the network of needed patches and upgrades without opening the network to attack by broadcasting those issues needing to be patched. Permissioned commercial banks and retail institutions will

also need a communication channel for testing on the network, asking central bank development teams questions about the CBDC codebase, and other support needs as the technology develops, as they will need to operate either participatory or read/write nodes in order to settle and interact with the CBDC network.

Additionally, indirect CBDCs will need to consider the additional processing and network capacity needed to interface their blockchain application with existing enterprise financial applications. For example, a recent spike in the popularity of DeFi applications on the Ethereum network led to an untenable rise in network gas prices; central banks will need to build infrastructural systems that can scale appropriately to compensate for an exponentially growing number of applications as central banks and retail issuers enable fiat or interchain swaps, develop composable financial applications built on top of the initial layer, and generally drive the tide of commercial adoption forward.

Overall, although CBDC networks using the indirect model must build internal processes, business logic, and controls for currency management and private-solution integration, the central bank is not responsible for ensuring that the retail distribution options themselves are operational. A central bank's system needs to be designed to enable the participation of commercial banks, retail institutions, and other financial networks, and to help them succeed. However, at the end of the day the central bank does not ultimately need to maintain the daily operation of the distribution functions.

CBDC in action: Indirect model

The most developed instance of an indirect system is China's DCEP, or "digital Yuan." The digital Yuan is conceptualized by the People's Bank of China (PBoC) as a digitized fiat and a government-backed electronic payment system rather than a cryptocurrency. While many details are a mystery, we do know that DCEP is pegged 1:1 to the Renminbi (RMB), legally tendered by the PBoC, and will be distributed in an indirect/two-tier system through nine state owned banks and telecom providers. Although running on cryptography and DLT, the DCEP makes no overtures towards decentralization as it is issued centrally by PBoC.

Binance Research reports[11] that the first interaction layer in this system is between the PBoC and commercial banks, since the former only issues and redeems DCEP through the latter. The second interaction layer involves commercial banks distributing DCEP to smaller businesses and the general public. The entire process mirrors the way cash is currently distributed in China and falls under the category of a two-tiered architectural model.

Sweden's e-Krona program is another example of indirect-issuance infrastructure. Initiated in 2017, the e-Krona program accommodates the rapid digitization of Sweden's economy with payment, deposit, and transfer capabilities for a digitized Krona utilizing R3 Corda DLT technology. R3 has drafted general CBDC implementations for a two-tiered retail currency distribution structure, adopted by a number of early mover CBDC prototypes likely including Sweden.

PARTICIPATE BY BISON TRAILS

Run secure, fully managed node clusters.

Participate by Bison Trails enables banks, retail institutions, and enterprises to run secure, fully managed node clusters to participate in a variety of networks and earn participatory rewards, without investing to develop capabilities in-house.

Our infrastructure platform features a 99% Participate Cluster uptime guarantee, real-time analytics and insights, and simple governance participation, with insights from our protocol experts on network changes, voting timeline, and technical tooling.

Learn more at bisontrails.co/participate

Over the past decade, cash use in Sweden has dwindled from 39% to 9%[12], and Sweden is on course to be cashless by 2025. The Swedish Riksbank generated multiple possible frameworks for distributing e-kronor in its pioneering pilot. The main technological architecture endeavor was a two-tiered financial model with intermediary nodes, using Corda's ledger system. The Riksbank node issues and redeems e-kronor and verifies the legality of transactions, but there is no centralized ledger maintained by the Riksbank node. Rather, there is one common infrastructure among all intermediaries, and each intermediary node only stores

11 Binance Research. 2020. First Look: China's Central Bank Digital Currency | Binance Research. [online] Available at: <https://research.binance.com/en/analysis/china-cbdc> [Accessed 21 December 2020].

12 de Best, R., 2020. Share Of Cash Payments In Sweden From 2010 To 2020. [online] Statista. Available at: <https://www.statista.com/statistics/1062036/paying-cash-for-most-recent-purchase-in-sweden/> [Accessed 21 December 2020].

information regarding its end-user's transactions.

In the first tier, the Riksbank distributes e-kronor to pre-approved financial institutions that maintain the security standards set by the central bank. Nodes on the network include the Riksbank node, participant nodes (run by each financial institution), and the notary node, a predetermined observer to protect against malicious activity. For the pilot, a singule notary node was used instead of the still experimental notary cluster model; having only one notary node could be vulnerable as a single point of failure.

In the second tier, the intermediary nodes distribute e-kronor to end-users, such as merchants and customers. Intermediaries obtain e-kronor by exchanging their RIX reserves into e-kronor tokens which can then be distributed. They store and receive e-kronor, as well as validate and forward transactions. End-users have a direct, contractual relationship with the intermediaries and access e-kronor by setting up digital wallet accounts at the intermediary. Because the Riksbank has no contractual relationship with the end-user, intermediaries are largely, if not completely, responsible for performing KYC, AML, and CTF checks.

Direct

In contrast, the direct CBDC model theoretically offers infrastructural simplicity with fewer junctures and stakeholders, allowing for efficiency, quality, and reliability improvements over the indirect model. Because governments must manage the distribution of currency, the financial infrastructure, and the retail-level accounting,

CORDA

Corda is a DLT that caters to financial institutions and offers transactions that ensure increased confidentiality. The platform executes smart contracts wherein only parties involved in a transaction are able to view its details. Consensus is achieved on the specific agreements that parties are involved in, and not on the state of the global ledger. The notary node, a predetermined observer, verifies consensus across the network. This process prevents actions related to double spending. The notary node can be run by a single node or multiple nodes that reach consensus through a specified consensus algorithm or contract code; multiple nodes provide additional resiliency against a single point of failure.

there are huge obstacles to success.

The direct model of issuance allows a central bank to retain total control of the overarching CBDC network and payment system. The central bank, as both the issuer and the payment rail, provides oversight of the financial access points for end users as well as controls the network's data. The central bank can develop insights into user behavior to help optimize the infrastructure as the network scales.

Given this level of control, the direct CBDC model is even further from a traditional decentralized network despite its use of DLT. Critics believe this total control could lead to political abuse, as well as increased privacy concerns over the access to data not available with non-digital currency. As with any system under one locus of control any privacy considerations present initially can be stripped away after broad market adoption.

The direct model of issuance allows central bank developers to build a specific set of end-user products, rather than rely upon banks or other second tier issuers to develop consumer implementations envisioned by the central bank. Central banks of smaller or more nationalized countries—or those central banks aiming to expand financial access for residents of their country, as the Bahamanian Central Bank aims to do—may be particularly interested in this level of control over financial products and solutions offered to their market.

However, distributing currency directly to citizen accounts could overburden governments by requiring them to create a financial services infrastructure and manage all ledgers; this additional work could create problems that outweigh potential efficiency gains.

Any issues that arise, including downtime or validation errors, could cause an 'egg on the face' situation for a central bank and could even prove harmful to the overall economy if the issues are large enough. Such problems could hamper use and adoption of a CBDC network. Experience in the existing blockchain ecosystem shows that protocols with prevalent performance issues at launch, such as bugs,

downtime, and a lack of interoperability, are often abandoned by the market at large.

Though one may imagine a direct-issuance CBDC as existing in total isolation, it is implemented within a broad ecosystem of existing commercial banks, financial institutions, and retail applications. A central bank's reluctance, when building a direct-issuance protocol, to design a participation network allowing retail institutions to connect to the CBDC network means that hundreds of proprietary systems could instead be built ad-hoc by existing enterprises to connect retail systems to the network, potentially leading to a large disparity in key security, consumer protections, and effective distribution. Similarly, privately developed bridges, which are often highly imperfect connectors with security risks, may be the only available interface with the broader ecosystem of digital currencies.

Experience in the existing blockchain ecosystem shows that protocols with prevalent performance issues at launch, such as bugs, downtime, and a lack of interoperability, are often abandoned by the market at large.

Regardless of these private connectors, central banks will need to shoulder the overhead costs and responsibilities of the network in the direct model, including systems monitoring, network patching, troubleshooting, and log capture for audit purposes. No part of the system is officially passed off to commercial banks and private business; the central bank must develop and maintain this infrastructure in-house in order to maintain the payment network.

One of the secondary prototypes furnished during Sweden's e-kronor pilot serves as an example of implementing the direct model. In this prototype, e-kronor is directly distributed by the central Riksbank without intermediaries. The Riksbank maintains all citizen account balances and directly disburses the currency via

their own network and wallet systems.This model envisions the Riksbank holding a direct, contractual relationship with the end-user and, because of this more involved role, managing KYC, AML, and CTF policies.

Without intermediaries to distribute the e-kronor, in this prototype the Riksbank must create a technical platform with a register containing information of all users and e-krona transactions. Any additional payment services such as cards, mobile applications, and settlement systems also must be managed by the Riksbank. This setup stands in contrast to the Riksbank's other more hybrid prototype, which maintained a direct relationship with end users by tracking all CBDC transactions in the bank's central ledger, but utilized intermediaries to disburse the CBDC to retail users via their own retail solutions—perhaps similarly to how decentralized apps, or dApps, can be built to transact on top of an existing chain. Ultimately, the Riksbank determined the direct model was not feasible to implement.

Generally speaking, it is extremely difficult to build a full solution that accounts for all use cases of parties interacting with a currency. In the development of a direct-issuance CBDC, it will be crucial for central banks to establish a clear divide between which functions, such as wallets and payment interfaces, will be developed by the central bank and which by private enterprise, while still building a validation infrastructure that can support the integration of alternative or competing retail currency options.

Hybrid models

A third model for CBDC implementation, hybrid distribution infrastructure combines the indirect and direct models by allowing intermediary institutions to offer retail banking products while central banks periodically access and record balances. While central banks retain issuance and distribution functions, third-party APIs can readily plug into the system.

The Bank of England explored a 'platform model' where the central bank controls a 'core ledger' and retains the right to create and destroy currency. In this hybrid model, the Bank of England would build and maintain the infrastructure to

"provide the minimum necessary functionality for CBDC payments," with private sector 'Payment Interface Providers' building overlay services to add customer-facing functionality beyond that of the Bank's core infrastructure offerings[13]. As such, these payment interface providers and technical service providers, which could feasibly be commercial banks or API-based applications, would perform KYC, interact with citizens in customer support scenarios, and provide secondary services to the CBDC's end users.

The Bank of England notes that the theoretical CBDC base protocol layer would be built to enable "programmable money, smart contracts and micropayments," but the development and execution of these Web3-centric applications would fall on private sector Payment Interface Providers. This setup provides a prime opportunity for the CBDC network to be interoperabile with existing blockchain protocols. Financial organizations already testing the waters of decentralized finance could establish partnerships with existing public protocol teams to develop secure and effective CBDC applications.

One way to implement this model is to allow existing financial institutions and private sector teams who meet the Payment Interface Provider standards, regardless of in-house technological ability, to operate nodes—participatory nodes on the core CBDC protocol and read/write nodes on the any layer-2 protocol solutions built to support customer-facing applications. This multi-level distribution model could prove highly resilient if built with effective failover and appropriate security architecture, with private sector providers strengthening the CBDC's settlement layer through network diversification.

While hybrid models may be more resilient than the indirect and direct models, they may also require significantly more intricate operational structures. The development of debt products and other financial instruments, as happened with the explosive growth of decentralized finance in 2020, not only adds value to a digital asset ecosystem but also complexity.

13 Bank of England, 2020. Discussion Paper: Central Bank Digital Currency Opportunities, Challenges And Design. [online] Available at: <https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=A71920A2FFB6511E43F787019C549262049CC7A8#page=21> [Accessed 30 December 2020].

Open source opportunities in blockchain

Open source has been prevalent in computer science since the 1950s, and was codified by the launch of Linux in 1991. But many governments were decades behind, including the US Government, which only launched an official Open Source Pilot Program in 2019. Prior to this time they spent upwards of $6 billion annually on proprietary code.

Infrastructure for blockchain, and decentralized finance in particular, is open source and written with composability in mind. When developing CBDCs, effective governments have an impetus to learn from the costly nature of slow adoption in the past and will benefit from being proactive in the use of open source code. Additionally, the blockchain ecosystem has developed a strong focus on interoperability, with open-source solutions like Substrate and Tendermint accelerating the development of interoperable blockchains tied to specific use cases.

No matter the design, central banks will want to determine what portion of the stack will be developed in-house vs. built with open-source components. Working with cryptography is a technical feat, so the benefits of participating and repurposing existing cryptographic innovations from the ecosystem currently working on these complicated tasks can be enormous.

For example:

- Zcash's innovations around zk-SNARKS are zero-knowledge proofs that have the ability to validate network transaction data without exposing information such as the address of the sender, receiver, or payment amount—a useful way for a CBDC network to allow third-party applications to validate account information without revealing users' personal information. Using Zcash's open-source cryptography innovations could prove an incredible boon for the scalability, security, and privacy of a CBDC network, all without having to create new cryptographic methodologies in-house.

- Substrate is a toolbox platform used to develop bespoke blockchain networks with a focus on interoperability and maximum technical freedom for those developing blockchains. It offers cross-language support with WebAssembly, a rapid consensus mechanism, integration of on-chain and off-chain elements, and the ability to upgrade without forks. All Substrate-based networks are natively compatible with Polkadot and its emerging ecosystem of projects and applications. Polkadot's proposition to connect the world's heterogeneous chains through collective validation and security modules is powerful, but possibly risky, for many CBDC-seeking nations. On the one hand, its scalability and speed, coding language-agnosticism, and non-forking upgrades could prove very valuable. On the other hand, it is a newcomer to the blockchain ecosystem, and remains in its early phase.
- The Tendermint ecosystem, like Substrate, enables building high-level protocol applications. However, Tendermint allows each chain to maintain its own sovereignty and security while interoperating, whereas Polkadot requires parachains to share security.

Regardless of which library is chosen, using already existing code, tech, developers, and markets as the basis for a CBDC network could help a nation leapfrog over other countries. Accommodating DeFi stakeholders aligns incentives between the government, the private sector, and end-users, resulting in a more complete product built by experienced developers available at a faster pace to a primed public.

Centralized or decentralized operation and security concerns

Determining whether a CBDC network will be centralized or decentralized is, at its core, a question of whether digital currency transfers will be settled internally by the central bank, or settled in a decentralized manner using a blockchain or DLT—either permissioned or open. It is a question of who will keep the CBDC's ledger running, and deciding the structure for validation and settlement is the elemental building block of a protocol's infrastructure.

Through this lens, one can see this decision is tightly linked to the decision of whether or not the CBDC will be designed with direct or indirect issuance. With the direct model, the central bank is entirely responsible for settling and validating transactions on the network, as the central bank controls the currency from issuance through to retail use. For indirect and hybrid models, other stakeholders, such as commercial banks and retail institutions, help keep the ledger running via operating nodes or other participatory functions of the network.

For these indirect and hybrid models, the use of dedicated blockchain infrastructure platforms such as Bison Trails can help institutions participate in and maintain the ledger without having to develop the engineering know-how to execute infrastructural code to specification in-house. Permissioned decentralized networks can do

TENDERMINT

Tendermint is software for securely and consistently replicating an application on many machines. At its core, Tendermint is made of two key components: a byzantine fault tolerant (BFT) blockchain engine that handles the networking and consensus, and a generic application interface (ABCI). Tendermint Core, the consensus layer of Tendermint, provides an out-of-the-box consensus design solution for teams that want to develop a new proof of stake protocol, while the ABCI allows for the deployment of application logic in any language. The next stage of evolution for the Tendermint ecosystem has the vision of interoperability between Tendermint chains at its core. To that end, a protocol called Inter-Blockchain Communication Protocol (IBC) will be used to connect blockchains built with Tendermint with one another. IBC will allow heterogeneous chains to exchange value, particularly tokens, which makes them interoperable.

Learn more at bisontrails.co/tendermint

this as long as the third-party infrastructure providers are provided with access to the network. Otherwise the central bank can do it for their permissioned users. For fully open, decentralized networks, participation infrastructure is more broadly available due to open source code, existing infrastructure providers, and client team support.

> "Invariably innovation will trend towards currencies that interoperate with other currencies, financial systems, and the emerging global, decentralized digital asset landscape. In such a case, a CBDC's level of decentralization or interoperability will be a key value proposition of the asset."
>
> — JOE LALLOUZ, BISON TRAILS CEO

For some countries, the network effects of a more decentralized financial ecosystem offer significant value. For example, the Ukranian e-Hryvnia proof-of-concept pilot found that using a decentralized blockchain network would be more effective than a centralized network, citing the advantages of having trust distributed across the network with any party capable of checking the validity of a transaction. As Bitcoin has made clear, a higher level of decentralization provides valuable benefits to a cryptocurrency, like trustlessness, permissionless access, and distributed security—and would so for a CBDC.

The technology used to build CBDCs must be ready to integrate with the economy of tomorrow, including bridging the gap between existing financial institutions and the growing economy of blockchain and DeFi applications. As FinTech and DeFi businesses proliferate, a broader variety of financial products are created and offered to organizations far beyond the financial world. Successful CBDC infrastructure will be highly composable, inviting innovation from all comers. Bridges and APIs built by outside organizations and developers will align function

and decentralization, in turn further distributing agency throughout society through financial inclusion.

Decentralized, cryptographic features can increase the security and resiliency of digital currency systems while building equitability and privacy into the core of the finance system. Moreover, smart contracts via blockchain can automate a central bank's execution of terms and agreements, thereby drastically increasing labor efficiency and productivity.

So far, retail payment networks have trended towards permissioned, private iterations of public blockchains. Wholesale payment models have been more conducive to blockchain-based solutions like Quorum, Fabric, and Corda, with a more decentralized node structure between participating institutions. All three protocols have borne out the viability of DLT serving as the core of CBDC infrastructure; no technology, however, has proven singularly effective or ready for deployment. The shortcomings of the technology fall inside the scalability trilemma, or the balancing of speed, security, and decentralization.

Ethereum-based enterprise blockchain Quorum excels in transaction privacy, distributed security, censorship resistance, and network resiliency, but its intrinsic decentralization means it lags behind in transactional capacity due to the broader consensus required for validation. Corda is not a blockchain, and is thus not beholden to a meaningful standard of decentralization. This freedom facilitates higher transaction capacity, but its requirement of a notary node results in a single-point-of-failure vulnerability that could be catastrophic to an economy if exposed.

Despite the issues with these private blockchain solutions, it is clear that most CBDCs, especially in the first phase of official release, will not be built on a public blockchain network. CBDCs have a number of specific needs that make public chains a less than ideal fit for full scale deployment. These requirements include scalability, regulatory compliance, censorship stopgaps, and security.

When addressing the scalability trilemma, governments and CBDCs will almost always sacrifice decentralization in favor of speed and security. The

transactional throughput requirements of a national-level currency are immense, and decentralized public blockchains trend slower than centralized systems. Government entities will likely desire censorship control over network activity and participation and, as such, may favor proprietary solutions. Further, many public blockchains' native cryptocurrencies remain in a state of regulatory confusion, causing problems for a government relying on their blockchain tech to be a CBDC network.

However, blockchain networks that feature private-public chain interoperability are increasingly being used as prototypes in the second wave of CBDC development. This model could create a balanced solution to the scalability trilemma while it creates opportunities for third-party innovation to connect the private chain to the wider blockchain ecosystem.

The Marshall Islands provides one example of how the benefits of a decentralized blockchain infrastructure can be adjusted for the permissioned needs of a CBDC. The Marshall Islands SOV will operate on a private, permissioned version of Algorand, but will remain interoperable with the public Algorand blockchain and other private chains as needed. Algorand's 'Co-Chain' function intends to offer the benefits of an open, public, decentralized network, including a functional and inclusive staking mechanism that can be isolated from the wider public chain. This segmentation is particularly important in order to provide the network oversight required for regulatory and security purposes.

Incentive mechanisms

Aside from the scalability trilemma, a further benefit of operating a permissioned CBDC network is the reduced need to build incentive mechanisms into the network's design. Open, fully decentralized ledgers use mechanisms such as mining or validation rewards to ensure validation is done securely and the network remains active at all times. Permissioned networks use other motivators to keep the ledger running, such as the potential earnings of offering retail services to end users.

As Shermin Voshmgir, director of the Research Institute for Cryptoeconomics at the Vienna University of Economics, explains in her writings on token economics, "Only permissionless ledgers (public Blockchains like Bitcoin or Ethereum) need some sort of incentive mechanism to guarantee that block validators do their job according to the predefined rules. In permissioned (federated/consortium/private) distributed ledger systems, validators and block-creators may be doing their job for different reasons: i.e., if they are contractually obligated to do so. In permissioned environments, validators can only be members of the club and are manually and centrally controlled."[14]

While having permissioned users maintains decentralization without requiring openness—removing the associated incentive mechanisms and security concerns of full decentralization—only having validators participate because of contractual obligations has its own challenges.

Bridging the gaps in the technological knowledge of permissioned members joined together for mainly economic reasons can be an arduous task in the development of a permissioned DLT. Central banks working with indirect distribution partners as validators for permissioned decentralized networks should be prepared to offer support for teams at varying experience levels; central banks may need to partner with experienced infrastructure providers in order to create a system all parties can use within the desired timeline.

ALGORAND

Algorand is an open-source pure proof of stake protocol with open participation and transaction finality. It is built on Byzantine consensus, and the network identifies its proof of stake consensus model as 'pure' as the protocol neither allows for delegation, or selecting a validator in the active set to represent one's stake, nor bonding, or locking one's assets into the protocol in order to gain validation rights. The protocol's co-chain architecture allows for permissioned blockchains to be built on top of their permissionless network, interoperating with the Algorand main chain to transact with other co-chains and inheriting all updates to the protocol while operating in a permissioned fashion.

14 Voshmgir, S., 2019. Cryptographic Tokens - Introduction. [online] BlockchainHub. Available at: <https://blockchainhub.net/tokens/> [Accessed 21 December 2020].

Diem, a permissioned network that aims to function similarly to a CBDC, provides a clear example of the challenges that come with bridging the gaps in understanding amongst permissioned participants. As Bison Trails product manager Jaron Parnala reflected on Diem's premainnet development, "Experience with blockchain technology varied broadly across the Association members. Some members are native blockchain-industry companies with a deep level of understanding and familiarity with the field, whereas, for others, Diem is their first foray into the world of blockchain technology. For the latter group, participating in premainnet was like diving into the deep end. The varying levels of industry experience, paired with the speed of development, added another layer of complexity to group collaboration... Though the process moved rapidly, the Diem Core team provided excellent templates for running a validator in AWS, GCP, or Azure. This helped to provide us with the building blocks we needed to develop our infrastructure in the midst of fast-paced development and a rapidly changing software."

Compute and storage considerations

On more centralized CBDC networks, the cost of compute and storage capacity required for the long-term maintenance of the network can be very high for a central bank as they are entirely responsible for running the network. As most blockchain infrastructure is now cloud-based, centralized networks will likely need to consider who hosts their network, the associated variable costs, and how they can ensure failover for the network during a regional outage. Those central banks that prefer greater centralization, and thus local security, have the option of hardware-based storage and computing. This option has additional associated expenses such as energy costs, cooling systems, and even the hard infrastructure of storage, floor, and rack space.

A centralized network may need to account for all of the variable power consumption required to handle peaks in computation across the network, as opposed to how a decentralized network shares cryptographic computation amongst validators or miners. The integration of cryptographic innovations can help with the scalability of transactional computation, such as by enabling

SNARKS for validation. SNARKS are designed for privacy, allowing systems to verify that information is true without needing to display that information. This design means the system no longer needs to explicitly verify certain elements of each transaction on a singular basis; instead, one SNARK can prove as an attestation for all signatures on a block. This reduces the need for calculations for the blockchain's verification, increasing the scalability of transaction computation.

Security and privacy

The primary concern for every single CBDC project is security, a subject that is complex at present and riddled with unknowns in the future. Invariably, any active CBDC will be a target of malicious actors and hackers; there is no room for error. A hacked national currency is one of the worst conceivable outcomes for any government looking into CBDCs.

From a security perspective, CBDC prototypes have favored permissioned DLT models that offer issuance control, granular participation controls, confidentiality control, dispute resolution oversight, and absolute governance of stakeholders. This preference for permissioned, closed systems could be a result of conservative thinking about security that presumes control and oversight results in greater security. Blockchain technology is a paradigm shift for this field, with byzantine fault tolerance providing security in decentralized networks. Maturing CBDC models can capitalize on this shift in thinking.

This preference for permissioned, closed systems could be a result of conservative thinking about security that presumes control and oversight results in greater security. Blockchain technology is a paradigm shift for this field.

The security of successful CBDC structures will be bolstered by decentralization and distributed node architecture. Striking the right balance between node distribution, consensus mechanisms, and node management is required for

a functional and secure CBDC. CBDCs built on private cul-de-sacs of next generation networks like Algorand and Tezos may find this balance best, with the ability to harness the security benefits of a distributed network while maintaining a degree of permissionality amenable to central bank institutions.

There are many components of CBDC distribution where security must be reinforced. The back-end must accommodate a secure, private, and resilient data storage system, a set of public-facing access points for connections to front-end components, and supporting and redundant components (firewalls, backups, etc.). The front-end must feature dedicated devices (online and potentially offline), software APIs for mobile and desktop, and a web interface. While factors like decentralization, privacy, and speed will define the success of CBDCs, security will define the sector's failures.

Centralized and direct-issuance CBDC networks are at particular risk due to their information 'honeypot'. With KYC completed by the central bank, and all user accounts stored within centralized payment solutions, a hacker could effectively gain access to the financial footprint for residents of an entire nation—opening the door for blackmail, extortion, identity theft, and the like.

With a centralized network one incident could impact the entire user-base of a CBDC forever, while in a decentralized or indirect model the multiple storage and security points means one attack may only affect a small portion of the populace—more similar to the risk of participating in the traditional financial system.

Additionally, critics of centralized CBDC networks point to the theoretical risk of a government having access to all end-users' financial history. Again, a decentralized or indirect model breaks access into multiple entry points, thus potentially lessening the ability of a government to weaponize financial information against dissidents and political enemies. However, this privacy relationship between state and end-user need not be adversarial or zero sum. If incentives are appropriately aligned, a balance between transparency and privacy exists—and blockchain technology, such as the integration of zero-knowledge proofs and other innovative trustless mechanisms, can navigate this reality to provide security for government issuers and privacy for citizens.

"The privacy mechanisms of a CBDC need to be built into the architecture from the beginning, or at least follow a short-term upgrade path. It will be a big hurdle to adoption for many CBDCs if there isn't a robust privacy mechanism built in from the ground up. Checks on authority are essential for many citizens to align behind CBDCs, and therein lays an opportunity to provide utility."

— AARON HENSHAW BISON TRAILS CTO

"So far, addressing the privacy models of CBDCs has taken a backseat while prototypes prove the use case for core blockchain technology," says Aaron Henshaw, Bison Trails co-founder and CTO. "While that has gone very well, the privacy mechanisms of a CBDC need to be built into the architecture from the beginning, or at least follow a short-term upgrade path. It will be a big hurdle to adoption for many CBDCs if there isn't a robust privacy mechanism built in from the ground up. Checks on authority are essential for many citizens to align behind CBDCs, and therein lays an opportunity to provide utility. This is just another way that blockchain technology can provide solutions. Zero-knowledge proofs or a similar tech that allows for automated, but conditional transparency, blind audits, and checked privileges could be an effective solution."

For example, private-key infrastructure and self-sovereign identity may allow users to access their funds and interact with financial institutions to use their services. Zero-knowledge proofs, wherein only limited transactional or account data is communicated across the network, can provide a functional solution for ensuring privacy while not sacrificing scalability, particularly when installed with mechanisms like secret-sharing or multi-signature accounts that allow for audits only in the case of a warrant.

Determining whether a CBDC network will operate in a centralized or decentralized manner is an essential component of the network's infrastructure, and requires consideration of a number of critical security concerns and elemental privacy functions. An in-depth consideration of the proper integration of existing blockchain innovations, and a thorough analysis of the final end-use cases, distribution model, and key stakeholder participation elements of the CBDC, can help structure an appropriate decision regarding the level of decentralization as well as the conjoining security of the network.

Public<>private partnerships

Given the variety of design and infrastructure considerations, CBDC development is a prime candidate for the use of public private partnerships. Existing blockchain protocols could fill an essential role in the successful implementation of CBDCs.

For example, in indirect models of issuance, existing blockchain protocols could serve as the payment rails for CBDCs, with retail institutions leveraging solutions built on existing protocols to enable user participation and to validate transactions. Within this model the central bank would need to maintain the issuance and control mechanisms of the digital currency, such as developing and maintaining smart contracts built to integrate with each protocol's network.

However, protocol teams could then take on the responsibility for consensus, further R&D opportunities, and the development of interchain bridge mechanisms. The expertise of existing blockchain infrastructure companies could also be leveraged to implement and support the existing protocol structures, such that central banks don't have to build from scratch.

Similarly, in direct models of issuance, existing protocols and their code bases have the potential to serve as the base from which to build an entirely new CBDC network—again allowing existing private participation partners to use their protocol experience to help the CBDC network grow and succeed. Partnerships with

private protocols have the potential to ensure digital interoperability even in direct systems, as well as to drive the utilization of open source software, standards, and libraries for significantly more efficient development of CBDCs and supporting networks.

A second-wave of countries building out CBDC prototypes have opted to work with public blockchain platforms for just this reason. When France's Societe Generale-Forge announced plans to use Tezos in developing a Euro-pegged stablecoin for France's national bank (Banque de France), it mentioned Tezos' on-chain governance, proof of stake consensus model, and formally verified smart contracts as contributing factors to the decision to partner.

Visa also recently announced that the company now settles payments in the USDC stablecoin, based in the Ethereum network, as part of the payment giant's long-term goal of moving towards settling payments using CBDCs[15]. Though launched in a limited capacity with a crypto-native partner, Visa cited a primary driver for the decision as giving "the next generation of crypto native issuers the option to directly settle with Visa in a digital currency over a public blockchain," stating that "it's really an extension of what we do every day, securely facilitating payments in all different currencies all across the world."[16] This represents yet another movement within the space reflecting the consumer drive for interoperability within the digital payments system, leveraging public/private partnerships to expand options for retail users and institutions alike by adopting existing blockchain technology.

If every CBDC were to be built from scratch, without partnerships or the integration of existing ecosystem knowledge, we could face a new financial ecosystem riddled with competing standards and reduced efficiency. All CBDC networks, no matter the design, will need to exchange currencies and interact with each other's financial systems. Having every country develop different proprietary solutions to the same problem, rather than using existing knowledge and public

15 Khatri, Y. (March 26 2021). Visa now settles payments in USDC stablecoin on Ethereum blockchain. Retrieved 6 April 2021, from https://www.theblockcrypto.com/post/99639/visa-now-settles-payments-in-usdc-stablecoin-ethereum

16 Khatri, Y. (March 26 2021). Visa now settles payments in USDC stablecoin on Ethereum blockchain. Retrieved 6 April 2021, from https://www.theblockcrypto.com/post/99639/visa-now-settles-payments-in-usdc-stablecoin-ethereum

private partnerships, could lead to a series of implementations using the same basic technologies but different functionalities. Difficulties may ensue when attempting to integrate with one another and private, often cross-border, financial solutions.

> "National currencies and cryptocurrencies, digital assets and financial instruments, becoming truly global, programmable, and accessible, will meaningfully change the lives of billions of people. It will also come with huge opportunities around the world for the technologies best positioned to connect the dots and salve pain points—ideally before they emerge."
>
> — AARON HENSHAW, BISON TRAILS CTO

While many benefits to permissioned CBDC chains exist, there is also great potential for a CBDC issued by a central bank but accessible on all available digital ledgers. Currently, stablecoins such as USDC issued by Coinbase and Circle, or Tether issued by Bitfinex, allow digital currency holders to use fiat holdings across protocols and diverse use cases. A central bank issued stablecoin, available across protocols and used on private central bank-controlled payment networks and public blockchain networks, could still be governed by smart contracts developed and maintained by the issuing central bank. Such a setup could induce wide adoption of digital currencies, rather than remaining siloed in their own national implementation.

"Even as we get closer to the reality of digital assets becoming a primary format of money in the world, it doesn't become a zero sum game to see which tech becomes the omni-blockchain that rules them all," says Bison Trails co-founder and CTO Aaron Henshaw. "We've already seen the blockchain industry trend

towards network interoperability and composability. It's not about having one tool for every job, it's about having the right tool for a specific job and having those tools be able to work together and stack. Those tools, many of which will need to be built themselves, will come from the blockchain industry. National currencies and cryptocurrencies, digital assets and financial instruments, becoming truly global, programmable, and accessible, will meaningfully change the lives of billions of people. It will also come with huge opportunities around the world for the technologies best positioned to connect the dots and salve pain points—ideally before they emerge."

Finance experts, government agents, and politicians are increasingly aware of the benefits and pitfalls of public-private partnerships for CBDC. In a virtual hearing in June 2020, US Federal Reserve Chairman Jerome Powell said, "The private sector is not involved in creating the money supply, that's something the central bank does."[17] Similar sentiments are echoed in China, where a CBDC was developed internally within the People's Bank of China. Later, in March of 2021, Powell stated that CBDCs "need to coexist with cash and other types of money," and should "not only be flexible but also foster innovation,"[18] leading some sources to speculate that sentiments at the Fed may be moving towards interoperability with existing digital assets.

17 De, N., 2020. US Fed Chair Says Private Entities Should Not Help Design Central Bank Digital Currencies - Coindesk. [online] CoinDesk. Available at: <https://www.coindesk.com/us-fed-chair-says-private-entities-should-not-help-design-central-bank-digital-currencies> [Accessed 30 December 2020].

18 Steve, M. (2021). Fed Chair Jerome Powell: CBDC Needs to Coexist with Cash and Other Types of Money. Retrieved 19 March 2021, from https://www.coinspeaker.com/jerome-powell-cbdc-money/

TEZOS

Tezos is an open-source platform for assets and applications backed by a global community of validators, researchers, and builders. The protocol leverages proof of stake consensus, and its on-chain governance mechanism allows the protocol to evolve by upgrading itself; any Tezos stakeholder can vote on changes to the protocol to reach consensus on proposals, including amendments to the governance procedure itself. Tezo's smart contracts are formally verified, meaning that they are mathematically proven to be correct rather than relying on software testing to identify bugs. Due to this high level of smart contract verification, smart contract developers can have a high level of confidence in the bug-free nature of the contracts when developing and publishing applications.

Learn more at bisontrails.co/tezos

While creation of the money supply may be a function controlled by central banks, the tech that integrates with this new form of money and brings it to the public almost certainly needs to be built by blockchain and tech industry stakeholders. Building a public, universal digital currency infrastructure requires replacing an almost half-century standard and bringing it up to date with one of the newest and fastest emerging technologies in the world—one that is global, open-source, and collaborative. With limited time and the need for perfect execution, it could be an incredible lost opportunity for governments to eschew private-sector involvement.

Tommaso Mancini-Griffoli, a Deputy Division Chief at the IMF, argues that a public-private partnership to develop synthetic CBDCs will spur monetary innovation, stating that the private sector could "interface with clients and innovate," while the public sector could "regulate and provide trust." Armelius et al. of the Riksbank of Sweden agrees, saying that the government should provide the fundamental infrastructure, and the private sector will compete and foster innovation for customers. A public-private partnership in CBDC development can bring "the best of both worlds."

> "Every blockchain network in the world is driven by aligned incentives. There is a huge opportunity to align across the private and public sectors."
>
> — JOE LALLOUZ, BISON TRAILS CEO

Further, the notion of CBDC development eschewing private-sector involvement is already demonstrably void. Even the current landscape of CBDC prototype partners—IBM, ConsenSys, Ethereum, Tezos, Algorand—are built on private or open-source, non-governmental technology. This a sign that this public infrastructure will need to be built by coalitions of stakeholders to accommodate distributed systems, consensus mechanisms, security apparatuses, node management, payment rails, retail financial products, public-sector financial

instruments, novel monetary levers, interoperability mechanisms, and innovations that connect all the dots to compose the money systems of the future.

The optimal development of CBDCs comes down to more than the particular chains used or the details of the decentralized architecture. The most powerful value proposition of CBDCs is derived from the aligning incentives for all stakeholders: governments, central banks, financial institutions, the general public, and the blockchain industry.

“Every blockchain network in the world is driven by aligned incentives,” says Joe Lallouz. “There is a huge opportunity to align across the private and public sectors. What we should be asking now is how can the crypto and blockchain ecosystem illustrate to the public sector the value that this technology provides so strongly that they’re enthusiastic about adoption?”

In almost all cases, for a central bank to run the necessary infrastructure they will need a dedicated and experienced blockchain-native partner. An example of this can be found in the US government’s foray into CBDC development. An official CBDC proof-of-concept or other experimental implementation has not been announced. Instead, the government is openly collaborating with partners such as the Stanford Crypto Lab and the MIT Media Lab to explore the infrastructure options available for the design of a DLT network before making any official considerations of the economic side of CBDC development.

Blockchain infrastructure partners, as experts on existing protocol structures and the workings of participatory validation, are in the best position to advise on building CBDC networks. Dedicated infrastructure companies bring the experience of contributing DLT network code base, running premmainet and dry-run mainnet tests, and supporting pilot programs. They can massively scale the public adoption of a CBDC by enabling the rapid integration of privately-developed applications, as they currently do with existing read/write node infrastructure offerings.

Blockchain, transfer value, and crypto networks are designed to make more efficient computing systems, transfer value systems, and seamless financial and

data systems. For governments and central banks, these are ideal technologies to address the many core needs of CBDCs. For the blockchain industry, the integration of blockchain and digital assets in the public sector will move the technology forward in ways that private innovation and an outsider economy cannot.

The emerging trajectory of CBDCs suggests that the private sector will not only be incorporated into the development process, it will drive the process. While CBDC technology has moved from theoretical to prototypical at a steady pace, the implementation phase will be marked by a significant increase in urgency, particularly after the launch of China's digital Yuan shows legislators what is at stake. With a mandate to produce expediently, private sector collaboration will answer the call.

	ACCESS	CONSENSUS	LEDGER	SMART CONTRACTS	INTEROPERABILITY	ADVANTAGE
ALGORAND	Open source	Pure proof of stake	Blockchain	Yes	Permissioned co-chain architecture with the Algorand ecosystem	Inclusive staking with isolation from public chain
CORDA	Permissioned	Validity consensus with a notary for finality	DLT	Yes, with increased confidentiality	Interoperability between consortia available. Option via Accenture for interoperability between Fabric-, Corda-, Quorum-, and Digital Asset-based protocols	High transaction capacity
FABRIC	Permissioned	Permissioned voting-based	Blockchain	Yes, containerized	Option via Accenture for interoperability between Fabric-, Corda-, Quorum-, and Digital Asset-based protocols	Noted for scalability, speed, and pluggable features
SUBSTRATE	Open source	Customizable, but must be stateful	Blockchain	Yes, pluggable module available	Interoperability with Polkadot ecosystem when security is shared	Noted for scalability, speed, and pluggable features
TENDERMINT	Open source	Proof of stake	Blockchain	Yes, pluggable module available	Permissioned IBC interoperability architecture with Cosmos ecosystem	Pluggable features
TEZOS	Open source	Proof of stake	Blockchain	Yes, formally verified	No built-in interoperability	Public network means full decentralization
QUORUM	Permissioned	Raft or IBFT with a notary node for finality	Blockchain	Yes, private or public	Option via Accenture for interoperability between Fabric-, Corda-, Quorum-, and Digital Asset-based protocols	High transaction privacy

IV. Conclusions

The design space surrounding CBDC development is enormous. Though intimidating in scope and complexity, the opportunities for making leaps in technological innovation are endless. Central banks and their development partners will need to be intentional with their design, infrastructure, and implementation. Startups, enterprises, and the wider blockchain industry will need to produce innovations that align incentives. Products and implementations that provide benefits for the state and the end-user, with proper considerations for security and scalability, will find the least resistance from all stakeholders.

The most successful national and international CBDC infrastructure will likely be built with public input and private sector know-how, calling on established industry experts and leading organizations to build the components of a larger system. Blockchain, digital asset, and distributed systems technologists who are furthest along will be the best situated to play a part in building this blockchain-as-a-public service. Partnerships with enterprises broadly, and infrastructure service providers specifically, have the potential to massively increase the speed of implementation and quality of the creation, maintenance, rollout, adoption, and, ultimately, success of these CBDC efforts.

While natural resources like oil and gas were the dominant market forces of the 20th century, technology is now the greatest driver of capital and innovation. Leadership in our global economy will be achieved through technology more than manufacturing or resources. FinTech, blockchain, and cryptocurrency are beginning to build a new global financial infrastructure with the potential to dominate the 21st century. To do so will require partnership between national governments, central banks, financial technology enterprises, and the novel factor of the upstart blockchain industry.

Nations will drive the CBDC market forward, focused on the inherent financial and economic improvements it will bring. But a fully realized digital asset ecosystem will only come about if it is effective and efficient for the individual, providing them with cheap, fast, and secure transactions, reducing red tape in international spending and the movement of money, and enabling exponentially more accessible financial products.