bitt

The Importance of Interoperability in CBDCs

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

bittglobal ✉ info@bitt.com www.bitt.com

The Importance of Interoperability in CBDC's

The latter part of 2022 marked some major milestones in the development of CBDCs. In September 2022 the U.S. Department of Treasury published their reports on Digital Assets with extensive commentary on a potential digital USD, and in November the Federal Reserve Bank of New York announced a digital dollar pilot, collaborating with a set of major banks and payments companies. This comes as a welcome evolution in CBDC development across the globe, as many monetary authorities have been waiting for the American authorities to reveal their CBDC roadmap and disclose further information regarding their approach to CBDC. While the official publications do not commit the Fed to a digital dollar, they could signal the digital way ahead for the world's pre-eminent reserve currency. With high expectations set by many in the international financial community over the past few years, CBDC functionality is coming under increased scrutiny, and for good reason. One element that consistently emerges as critical is interoperability of CBDC systems – both with respect to cross currency integrations, and integrations with legacy financial networks and service providers.

While many questions remain unanswered, and many design choices are yet to be made, Treasury has identified some key elements to be addressed. The Department of Treasury report *The Future of Money and Payments* identifies eight policy objectives for a digital USD:

1. *A possible digital dollar must provide benefits and mitigate risks for consumers, investors, and businesses*
2. *Promote economic growth and financial stability and mitigate systemic risk*
3. *Improve payment systems*
4. *Ensure the global financial system has transparency, connectivity, and platform and architecture interoperability or transferability, as appropriate*
5. *Advance financial inclusion and equity.*
6. *Protect national security*
7. *Provide ability to exercise human rights*
8. *Align with democratic and environmental values, including privacy protections.*

While it's relatively straightforward to lay out the list of policy objectives, it's much more complex to design a CBDC architecture that achieves them – not least because some of these objectives are at times operating at cross-purposes. Interoperable CBDC platforms are essential to create digital currency systems that can implement Treasury's policy objectives of promoting economic growth, sustaining financial stability, and mitigating risks for consumers, investors, and businesses. Focusing on interoperability will allow central banks to better adapt to the multi-network future, allow central banks to integrate with a variety of tools as they emerge, and allow for increased network effects which will push forward increased acceptance of new internet native payment rails. The future of not just payments, but the greater web3 space will depend on interoperability as users continue to build valuable use cases on different platforms.

The release from treasury was informative and provided further context for the Federal Reserve's release earlier this year, however, it poses more questions than it does answers. Perhaps one of the benefits of this latest release is it brings further attention to the critical challenges faced by those of us developing CBDC systems. These systems need to have ultra-high availability and security with rigorous privacy preservation functionality, while delivering the extensive functionality required by monetary authorities of today, and the future. Central banks around the world are all working through similar design and policy challenges in their own CBDCs, not least of which being the choice behind the underlying transaction network. Many arguments could be made for issuing on a private permissioned network or an open permissionless network, however does a monetary authority need to choose one network on which to issue their currency? Who is to say that legal tender can only exist on one network, especially considering the fact that central bank money exists today in multiple forms. With such significant decisions still being debated in boardrooms, think tanks, and technology labs around the world, the case for interoperability in CBDC toolsets only becomes stronger.

Interoperability Creates Network Effects

While the general public may not recognize it, when they make a credit card payment, send a Venmo transaction, pull cash out from a convenience store ATM, or send money overseas to a relative, they are leveraging numerous underlying integrated payment systems that interoperate to ultimately deliver the funds from the sender to the intended recipient. As we lay the rails for the financial system of the future, we have the ability to assess the strengths and weaknesses, pros and cons, and integrative capabilities of the existing financial system to inform how the shift towards internet native payment networks will enable new use cases, bring about efficiencies, lower costs, and decrease fraud and abuse. CBDC use and integration should be designed and implemented with this ease of use for the end user in mind; where interoperability is inherent in the system, while creating more security, decreasing costs, and fostering increased privacy to all financial transactions than currently offered by the legacy financial system.

Interoperability enables network effects and provides all users with options for participating in connected financial ecosystems - options that can be useful in times of distress, but also for expanding business activity and accessing more and more counterparties to transact with. Interoperability also creates a greater opportunity for central banks to facilitate innovation and competition, to promote inclusion, and provide opportunity for all economic stakeholders. However, it demands that monetary authorities have modern and comprehensive toolsets through which to manage the digital version of their national currency - on at least one new network, if not multiple networks. This includes all elements of managing the digital currency lifecycle, the most crucial of which is the monetary authority’s ability to confirm that only authentically minted digital currency is circulating. Central banks also recognize the possibility to improve the precision through which they implement, monitor, and adjust monetary policy in real time; a robust CBDC platform should include such functionality while preserving end-user privacy; being flexible enough to evolve and adapt to future financial and monetary conditions.

Bitt’s CBDC platform enables smooth integration with financial intermediaries and decentralized finance (DeFi) asset markets, with proven network security and carefully designed privacy protections. Providing a platform on which financial intermediaries can integrate and compete to drive down the cost of payments, integrate with new digital currency networks, and provide technically provable security and privacy guarantees to all users are drivers for CBDC solution providers like Bitt. Central banks require reliable tools that enable them to continue to achieve their mandate in a rapidly evolving global financial ecosystem. These tools should be interoperable with the most advanced and performant transaction networks, including private permissioned networks such as Hyperledger, Corda, and MIT’s OpenCBDC-tx, as well as public networks such as Bitcoin, Ethereum, and Stellar.

Central banks have been experimenting with several transaction networks for their CBDC offering, including:

Hyperledger Fabric	*Ethereum*	*Corda*	*Quorum*	*OpenCBDC-tx*	*Stellar*	*Unknown*
European Central Bank Monetary Authority of Singapore Bank of Japan Saudi Arabian Monetary Authority Central Bank of the United Arab Emirates Banque De France Eastern Caribbean Central Bank	Reserve Bank of Australia Bank of Canada Hong Kong Monetary Authority Bank of Thailand New York Federal Reserve Norges Bank	Bank of Canada Monetary Authority of Singapore Bank of Thailand Banque De France Hong Kong Monetary Authority Swiss National Bank Reserve Bank of Australia Riksbank of Sweden Bank for International Settlements Innovation Hub Bank Negara Central Bank of the United Arab South African Reserve Bank Peoples Bank of China National Bank of Kazakhstan	Monetary Authority of Singapore South African Reserve Bank Bank of Canada Banque De France Swiss National Bank Negara Bank for International Settlements Innovation Hub Bank of Thailand Peoples Bank of China Central Bank of the United Arab Emirates Hong Kong Monetary Authority Reserve Bank of Australia	Federal Reserve Bank of Boston Bank of England Bank of Canada	National Bank of Ukraine	Peoples Bank of China Central Bank of the Bahamas Bank of Jamaica

While the above list is not exhaustive, it provides insight into which networks central banks are considering in their research. Each transaction network comes with its own unique structure and capabilities, including:

- UTXO or account-based structure
- Hosting structure ie. Node types and server requirements, private, permissioned, open, etc;
- Developer and community support
- Availability and depth of supporting documentation
- Compatible software languages and libraries
- Transaction throughput and scalability metrics, such as latency, blocksize, etc.
- Validation process and consensus mechanisms, such as proof of stake
- Governance structure
- Security considerations such as the cryptographic algorithm used and transparency behind its composition/functionality.

Other practical considerations include the use of the network in other projects, which enables monetary authorities to collaborate in a deeper way and to share experience and lessons learned. Similarly, a given monetary authority may have previous bias based on their exposure to a particular network, or the experience and inclinations of their IT department.

Ultimately, central banks will decide on a number of networks with which to test and pilot their CBDC, but must be ready to integrate with one another's networks as cross-currency and multi-currency functionality is built out. As such, it is worthy to explore the different pros and cons to the multiple transaction networks currently utilized by central banks around the world and how the different characteristics affect CBDC systems.

Hyperledger Fabric

Hyperledger Fabric is a private, permissioned blockchain in which participation is restricted to users with the requisite certificate authorization from the governing authority to integrate with the transaction network. Participation in the network is restricted to authorized intermediaries such as licensed financial entities ie. banks and payments service providers and is managed by the monetary authority -- a common trait for all permissioned ledgers.

Within Hyperledger Fabric, the governing authority (AKA the Issuing Central Bank) provides permissions to other nodes that enable the processing of specific types of transactions. Access control can be configured directly on specific nodes, channels or even consortium levels. Hyperledger allows for multiple transactions to be executed simultaneously, enhancing performance and scalability. Settlement and executions within Hyperledger follow the KAFKA and the RAFT algorithms to arrive at consensus. Hyperledger utilizes chaincode within its business logic that can be written in standard programming languages like Java and Go, making product development and support more straightforward for the monetary authority and firms integrating with the network.

Hyperledger allows for both UTXO-based structures and account-based structures. While the account-based model was tested to perform up to 1500 TPS, the UTXO-based model should achieve over 3500 TPS. Hyperledger provides unique utility in the hosting structure since a variety of node types can be deployed, including transaction proposer, transaction endorser, transaction order, and transaction and state validator.

Corda

Corda, like Hyperledger Fabric, is a private, permissioned transaction network: integration is restricted to users with the proper authorization from the monetary authority.

Unlike Hyperledger, Corda utilizes a file-based configuration to access nodes and grant them permissions. Within Corda, data is shared on a need-to-know basis instead of global broadcasts, allowing for greater control of privacy but with some sacrifice on performance. Corda's consensus algorithm utilizes notary nodes within the blockchain that validate transactions as they are entered into the system and add blocks to the greater chain. Corda utilizes Ricardian Contracts coded within Java or Kotlin languages, giving central banks a certain amount of flexibility in product development and integration with other systems.

Corda only utilizes UTXO based models in order to process transactions; each transaction consumes a set of existing states to produce a set of new states. Corda's TPS within its newest production version has been clocked between 600 TPS and 2500 TPS depending on whether issue or issue plus repeated pay is being measured. Upgrades from previous versions (from Corda 1 to the planned Corda 5), are primarily focused on increasing performance, security, and usability for developers utilizing the platform.

Quorum

Quorum, like Corda and Hyperledger Fabric, is also a private, permissioned transaction network, based on the Ethereum blockchain.

Quorum is structured through organizations, sub-organizations, and accounts. Organizations consist of nodes and accounts with permissions and functionality determined by the monetary authority. Sub-organizations consist of accounts and roles dictated by the needs of the monetary authority and/or financial intermediaries. Accounts are synonymous with wallets, and are effectively public- private keypairs that enable transactions on the underlying network. Quorum uses an internal protocol called the QuorumChain to reach consensus as transactions enter the blockchain. The system utilizes a voting process that confirms transactions using majority results from voting, coupled with BFT and RAFT algorithms. Quorum, in comparison to Hyperledger and Corda, is written in Solidity, complicating possible product development due to its relatively lesser use in comparison to Java or Go. However, developers can benefit from the wide -array of open source EVM compatible software used in the many popular DeFi applications to date.

Quorum primarily uses an account based structure which enables as a result of its integration with Zether protocols, a cryptographic protocol set that allows Quorum to complete transactions in an anonymized way. Transactions with this protocol anonymize not only how much is being sent, but also who is sending the transaction using zero knowledge proofs.(ZKP’s). Transactions per second vary depending on the use case and architecture, with TPS ranging from the several hundred to several thousand range depending on the project. Quorum updates primarily come from Consensys, with upgrades increasing performance.

OpenCBDC

OpenCBDC-tx was created by MIT and the Federal Reserve Bank of Boston as a testing ground for a possible CBDC system. OpenCBDC-tx was designed as a modular transaction processing system and implemented within two architectures to allow support for a variety of models for intermediaries and data storage; the only difference between designs is that one architecture keeps a record of transactions in the order they were processed (atomizer structure) while the other does not (two-phase commit structure). OpenCBDC-tx uses a UTXO model in which users interact with a central transaction processor by means of digital wallets storing private cryptographic keys. It divides validation logic into two parts, a front-end validator that verifies signatures and amounts, and a back-end validator that ensures against double-spend. Wallets create cryptographic signatures to authorize payments and funds are transacted to public key addresses.

The design was created with three key themes: the decoupling of transaction validation from execution, the creation of a transaction protocol that provides self-custody and programmability, and finally a system design that efficiently executes these transactions. OpenCBDC-tx currently uses C++.

OpenCBDC-tx claims a throughput of 1.7 million transactions per second with the two phase commit structure, and 170,000 TPS with the atomizer structure, with latency totaling less than half a second per transaction. Development of OpenCBDC-tx is still ongoing, with planned Phase 2 research by the Boston Federal Reserve and MIT into new functionality capacity and alternative technical designs. Planned research topics and upgrades include cryptographic designs for privacy, auditability, security from attacks, programmability, and offline payments among many other use cases.

Stellar

Stellar is an open-source, decentralized blockchain network designed with digital asset issuance in mind. It is considered to be a “hybrid “ blockchain, with the flexibility of a permissionless ledger while possessing capabilities similar to permissioned blockchains via authorization requirements, revocable authorizations , and clawback, enhancing security and control from the issuing authority. Stellar, unlike other blockchains, does not use smart contracts to transfer assets since assets within Stellar are fundamental. Any Stellar account can issue its own assets and transfer them to other Stellar accounts, which is then entered into the ledger.

Nodes on Stellar link to verifiable identifying information so users can see at all times which entities are trusted within the network. Stellar also allows for automatic interoperability by offering native support for different markets with different asset pairs; this means a user could route a transaction with two different currencies automatically via separate markets in a cheap, safe, verifiable manner even if they are in differing currencies.. Stellar currently allows for programmability via the integration of smart contract API’s from external sources or native hosted builds from the user building on Stellar, with plans to release native smart contract capacity in the near future. .

Stellar’s consensus protocol functions via a voting mechanism in which verified nodes from reputable sources (in a CBDC deployment this could be the central bank, government regulators, and large financial entities), validate transactions as they enter the ledger. Nodes are protected and made redundant/replaced via a multi-phase process to ensure reliability and speed within the network. Stellar is programmed utilizing C++, Java, and Go, making at accessible to a broad community of software engineers.

Stellar utilizes an account based structure within its architecture; it is capable of processing over 1,000 transactions per second. Version updates have primarily focused on stability improvements to better voting consensus, increased performance focusing on load management, and features like smart contracts, offline payments, and privacy.

Ethereum

The most heavily trafficked decentralized blockchain network is Ethereum, having gained significant market share of the entire cryptocurrency asset class enabling thousands of tokens to circulate using the ERC20 smart contract standard, among others. Ethereum recently switched to a proof of stake consensus mechanism whereby stakers are rewarded for processing validating transactions that are consistent with the rules of the network (no double spend), and are punished for attempting to write non-compliant transactions to the network (via “slashing”, when the stake is forfeited).

Written in Solidity, Ethereum utilizes Ethereum Virtual Machines, which has gained significant momentum as a protocol for developers worldwide. Ethereum can be considered a “pay for compute” network that enables anyone to issue and distribute assets to EVM compatible wallets. While Ethereum at the layer 1 level (eg. ERC-20 token) is impractical for CBDC given gas costs and lack of monetary authority controls, so-called layer 2 protocols are emerging that provide substantial throughput and scalability gains alongside federated controls and other functions.

The majority of the defi ecosystem utilizes the Ethereum network for advanced financial use cases (eg. Curve, Aave, and more), which have driven unique value propositions to users seeking complex financial products without traditional intermediaries.

Each of these transaction networks offer unique characteristics especially with respect to their applicability to CBDCs. In addition to the initial list of considerations, technical parameters such as block size (for blockchain-based networks) and the ability to implement a UTXO system could significantly impact scalability. Technologies such as transaction channels and zero knowledge proofs could provide users with the privacy they require. Companies like Bitt will continue to evaluate such technologies as we research and develop solutions that address the requirements of the next generation of internet native rails.

Stablecoins

In comparison to public CBDC developments, existing private sector versions of national currency (stable coins), exist primarily on open permissionless networks. Circle’s USDC is currently issued and circulating on Ethereum, Algorand, Solana, Stellar, Tron, Hedera, Avalanche, Flow, and Polygon; while Bitfinex’s Tether (USDT) is issued and circulating on Algorand, Ethereum, EOS, Liquid Network, Omni, Tron, Bitcoin Cash’s Standard Ledger Protocol, and Solana.

The issuance of digital USD on open permissionless networks is primarily driven by market demand from cryptocurrency and defi users in a variety of trading, lending and other financial activities. Retail payments use cases have yet to be addressed at scale by stablecoins on permissionless networks, save for Strike’s efforts in El Salvador and beyond. Strike is building stablecoin payments tools on the Lightning Network, a layer two relay network built on top of the bitcoin protocol. Strike is working towards being the Bitcoin L2 remittance processor of choice, and is in good company with Lightning Labs and Lightspark, who are both building on the Lightning Network with a great deal of support. While the private stable coin issuers are mainly building to address immediate user demand in web3 realms, issuing on networks that host the majority of crypto trading, lending, and other defi or web3 use cases, monetary authorities are seeking platforms and solutions that can provide the functionality and assurances they require to safely and securely achieve their mandate in the financial system of the future.

The Monetary Authority’s Mandate

Historically, a monetary authority’s core mandate is implementing monetary policy to optimize growth with price stability. With central banks entering further into the provision of public financial infrastructure – in the form of CBDCs - for governments, enterprises and retail users alike, they will be adding a number of responsibilities to their existing mandate, including CBDC platform security, availability, and instant payments. In order to accomplish this augmented mandate, central banks must level up on the technology front – which is currently happening in the form of public private partnerships, increased IT hiring, and international collaboration through bodies such as the Bank for International Settlements, the World Bank, and the International Monetary Fund.

To drive at the heart of the decision around which transaction network a central bank chooses, one must consider the available toolset for integrating with, and managing the lifecycle of a digital currency issued on the networks in question. In web3 and crypto ecosystems, firms consider the amount of pre-existing open-source software and tooling they can utilize, the size and depth of the community, and the amount of activity (tx volume, number of users, etc.) when choosing which network on which to build their offerings. Some of these considerations apply to a monetary authority’s decision as well, but with one key difference: the monetary authority will be playing a key administrator role for the asset they’re issuing as well as the underlying network. They will be the effective gatekeeper for all intermediaries seeking to integrate CBDC payments into their applications and offerings.

With all of these considerations in mind, it is difficult for central banks to decide on which transaction network is best suited for their CBDC. In fact, given the amount of competition at the transaction network layer with no clear winner in sight, it is most likely that the financial system of the future is a composite of multiple transaction networks interoperating with one another to process and settle transactions of all types. Therefore, In order to achieve their traditional mandate, as well as their new responsibilities in operating a CBDC network, monetary authorities require toolsets that are interoperable with multiple underlying transaction networks.

We at Bitt have created the DCMS Numa, which defines deployment parameters for any digital currency or stablecoin issued by the client monetary authority. The Numa allows for many monetary policy actions, integrations to any transaction network (including both blockchain and legacy networks), role-based permission settings for all stakeholders, configurable wallet types and tiers, along with the capacity to develop and implement both internal and external API's and SDKs for a wide array of use cases. We've seen the multi-network future and have constructed our DCMS.

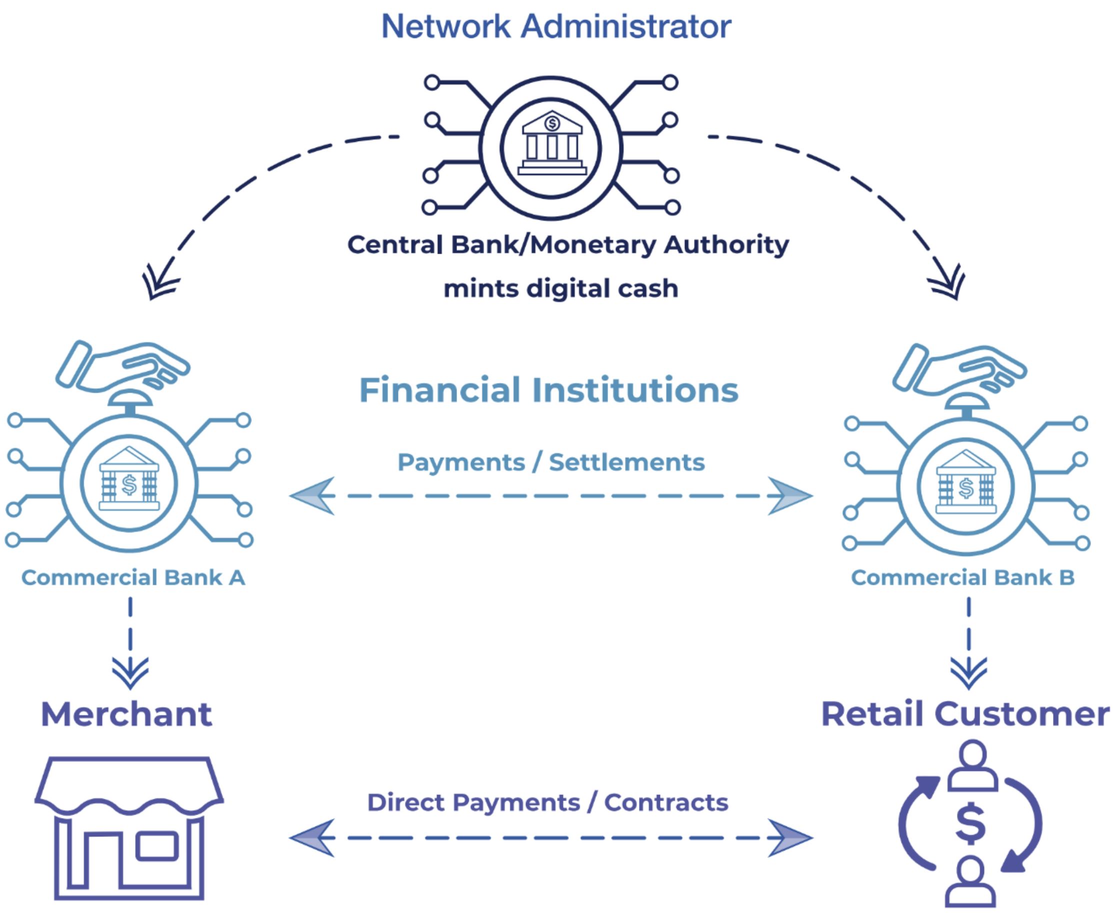
Interoperability is about more than just working with standard technologies and tech is only one part of building an interoperable system. Real-world testing is needed to determine if a CBDC solution is ready for wider adoption – by stakeholders of all types. The technology that is being developed to further CBDC solutions is advancing, however, it's only one piece of the puzzle. In order for CBDC systems to be considered interoperable, other parts need to be considered as well: governance and legal frameworks; standards development; and testing or piloting. We at Bitt are here for the journey, and continue to advance the capabilities of national digital currencies with our clients around the globe.

For more information about BItt and our DCMS offering, please contact simon@bitt.com

About Bitt

Enabling The Digitization of National Currencies

Bitt is a global financial technology company that provides digital currency solutions to central banks, financial institutions, and ecosystem participants worldwide. Bitt's Digital Currency Management System (DCMS) is the secure infrastructure that monetary authorities need to deploy CBDCs, and for financial institutions to integrate digital currencies into their financial service offerings. Bitt's DCMS has been deployed in 12 countries across Africa, Central America, Europe, and the Caribbean. Bitt is a portfolio company of Medici Ventures, L.P., a blockchain-focused fund. The general partner of that Enabling The Digitization About Bitt of National Currencies fund is an entity affiliated with Pelion Venture Partners.


Network Administrator
Central Bank/Monetary Authority
mints digital cash
Financial Institutions
Payments / Settlements
Commercial Bank A
Commercial Bank B
Merchant
Retail Customer
Direct Payments / Contracts