Stellar

Whitepaper

STELLAR FOR CBDCs

Introduction

COINS TO CODE

EASE & STABILITY

In an oft-cited statistic, a growing number of central banks around the world are exploring the possibility of central bank digital currencies ("CBDCs").[1] *And the COVID pandemic has only accelerated the situation, with lawmakers and regulators even more willing to consider new technologies that could improve the lives of their citizens. Whether focused on increased competition in financial services*[2]*, greater ease of distributing social benefit payments*[3]*, or bringing safety and security to the unbanked*[4]*, central banks are imagining the promise and possibility of CBDCs.*

At the same time, central banks are rightfully focused on the risks. Those overseeing a country's financial system have a legitimate interest in the safety of their money and payments. Implementing changes requires examining the economic and political implications of any change, as well as the technology used to implement it. Advancements in technology often drive change, and central banks have long had to consider technology when ensuring the safety of their monetary systems. Originally, safety meant focusing on physical currency (coins and paper notes) to protect their value and to guarantee they were available and forgery-resistant. With the advent of digital technology, protecting money and payments meant controlling the infrastructure on which it was built by controlling the relevant databases and messaging systems.

***The Stellar Development Foundation** is a non-profit organization that supports the development and growth of Stellar, an open-source network that connects the world's financial infrastructure. Founded in 2014, the Foundation helps maintain Stellar's codebase, supports the developer, fintech, and business communities building on the network, and serves as an independent industry voice to regulators and institutions. The Foundation seeks to create equitable access to the global financial system, using the Stellar network to unlock the world's economic potential through blockchain technology.*

1 Bank of International Settlements, Impending arrival - a sequel to the survey on central bank digital currency, pg 3, available at https://www.bis.org/publ/bppdf/bispap107.pdf. 2 Bank of Canada, The Positive Case for a CBDC, pg 6-9, available at https://www.bankofcanada.ca/wp-content/uploads/2021/07/sdp2021-11.pdf. 3 European Union Blockchain Observatory and Forum, Central Bank Digital Currencies and a Euro for the Future,pg 72, available at https://www.eublockchainforum.eu/sites/default/files/reports/CBDC%20Report%20Final.pdf. 4 European Central Bank, Report on a digital euro, pg 10, available at https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

Introduction

And now, with blockchain technology a new paradigm in electronic money has developed: An asset can be kept safe and secure even if issued on common infrastructure. In essence, this shift is what this paper discusses. The idea that central banks can let go of the historical notion that "having control" of the infrastructure is necessary to warrant the safety of the assets. With the rise of computers and modern telecommunications, money entered the digital realm, extending its reach and expanding beyond the physical. Before blockchain technology, providers of digital money faced a trade-off between control and interoperability.

An issuer could host a closed ledger on its own servers and maintain complete control of the asset, but the ledger would only manage a single currency and was not interoperable. Foreign exchange, trade, or off-ledger transactions could be implemented only by trusted third-parties, limiting access to markets and hindering innovation. Conversely, an issuer could partner with others to maintain a joint ledger to intrinsically support transactions across assets. Unfortunately, the integrity of the joint ledger could be undermined by compromised participants regardless of the security of any given asset issuer.

Today, public blockchains promise the best of both worlds: cross-asset interoperability and security against bad actors. Most public blockchains achieve security for the assets through "mining" (the process of creating new cryptocurrency and distributing it to blockchain participants as a reward for hardening transaction security). Mining precipitated the remarkable advent of novel, counterparty-free assets such as Bitcoin and Ethereum. These cryptocurrencies have gained significant financial value while permitting secure transactions across mutually distrustful, even anonymous parties, all the while having no clear issuer of the asset that needs to be trusted. But cryptocurrencies such as these can only do so much to influence and better the lives of individuals. Currencies issued by sovereign states remain important financial instruments, and issuing them on a blockchain has positive implications for the global monetary system.

Stellar was built precisely with this use case in mind: allow trusted issuers to create digital representations of their assets. Stellar is uniquely suited to CBDCs precisely because it capitalizes on the trust inherent in asset issuers. Though a public blockchain, Stellar does not support mining. Rather, it bases security on two assumptions:

- ➔ First, each issuer wants to ensure the security of its own asset, and therefore can be trusted to provide the canonical truth about that asset.
- ➔ Second, issuers have a strong desire to interoperate with the rest of the world, and hence will not "cheat" or unilaterally deviate from the rules if doing so would cut them off from the world. Governance power stems from the value of assets in the ledger and participants' desire to remain in sync with the parties who issue and redeem those assets.

The interoperability, security, and safety of these assets can be ensured, even without any single entity having control of the underlying infrastructure – in fact, it is because there is no single source of control that the system maintains the necessary protections.

This paper is an introduction to the Stellar network, and how it can be used for CBDCs. The first section walks through the features of Stellar most relevant to asset issuance, and therefore to central banks considering CBDCs. The following section describes a hypothetical implementation of a CBDC on Stellar, highlighting how the key features would benefit a central bank.

Finally, the Appendix dives into Stellar's novel consensus algorithm in more detail, for readers who want a more in-depth understanding of how Stellar's design creates the features and characteristics beneficial to central banks.

II. Why Stellar?

COMPLIANCE MEETS INTEROPERABILITY

A GOOD FIT

Stellar is an open-source, decentralized blockchain network that was designed with asset issuance in mind. It offers the interoperability and flexibility of permissionless ledger while possessing built-in capabilities to ensure security, certainty, and control - as with a centralized or permissioned ledger. That combination makes it particularly well-suited for issuance of CBDCs.

We will investigate four specific features of Stellar in order to understand why they're important for any entity considering issuing a CBDC.

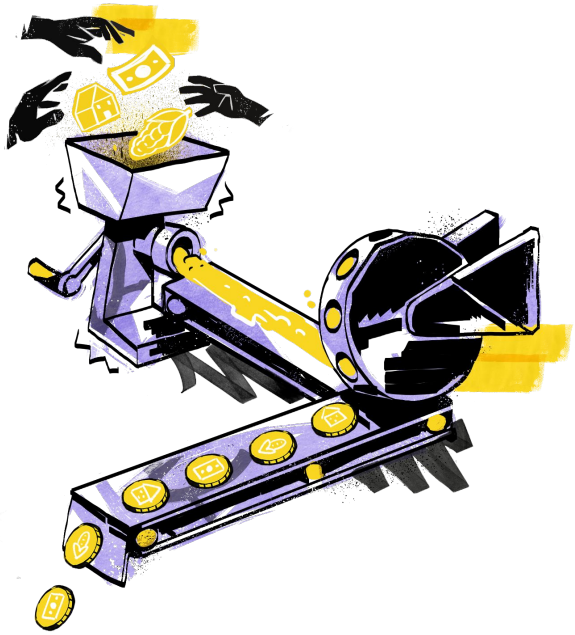
They are:

Secure Asset Issuance

Transaction Finality

Enhanced Compliance Capability

Automatic Interoperability



THE FUNDAMENTALS

SECURE ASSET ISSUANCE

Fundamentally, Stellar is a system for tracking ownership, and, as banks and accountants have for centuries, it uses a ledger to do so. That ledger lists accounts and the asset balances those accounts hold. To modify the ledger, account holders sign and submit transactions to network nodes, which are connected computers that ratify changes to the ledger's state. Primarily, users move part of their account balance to someone else's account. In other words, they make payments. That's what Stellar was designed for: payments.

Stellar payments are not limited to assets hardwired into the ledger. In fact, the system was created to allow users to issue their own assets, which they do with a simple transaction, and to enable them to use those assets to make payments. Any Stellar account can issue an asset, and any account can hold a balance in an asset issued by another account. Unlike assets on many other blockchains, Stellar assets are a fundamental, built-in network feature, not the result of a smart contract, and issuing them doesn't require complicated coding that introduces the possibility of exploits and errors. It's as simple as adding an entry to a ledger.

Stellar accounts are secured using public-key cryptography, which means that on the ledger, each account is represented by a string of letters and numbers. But the system does not prize or rely on anonymity or pseudonymity. Quite the opposite. Organizations issue assets that represent real-world financial instruments, and to gain the trust of potential asset holders and other counterparties they link their accounts to verifiable information about themselves, their assets, and their Stellar integration. When users hold an asset on Stellar, they know who issued it, what it represents, and the terms and conditions of its redemption. Those terms are defined and made public by the asset issuer.

As we'll see below, the nodes that keep the Stellar ledger, many of which are run by asset issuers, also link to verifiable identifying information, so network users can see which entities are entrusted with the safety and security of the network. That's very different from other public blockchains such as Bitcoin and Ethereum, where nodes are anonymous and the individuals and organizations responsible for the integrity of the network are unknown. See the Appendix for more detail on how nodes configure themselves to create a secure, consistent network.

ENHANCED COMPLIANCE CAPABILITY

Issuers have a number of choices about how to configure an asset on the Stellar network. By default, a Stellar asset can be held by any account on the network, and for many issuers that setting is sufficient. Regulated financial institutions that issue fiat-backed stablecoins, for instance, often use standard Stellar compliance protocols to collect user information and perform appropriate Know Your Customer (KYC)/Customer Due Diligence (CDD) checks before moving value onto or off of the network. In many cases that's enough to comply with local laws and regulations.

However, certain use cases, including CBDCs, may require issuers to exert greater control over access to their assets. To accommodate those use cases, Stellar offers three settings that can be activated with simple account flags: authorization required, authorization revocable, and clawback enabled.

When authorization required is enabled, an issuer must approve an account before it can hold or transact with their asset. Issuers can perform necessary checks before granting that approval, and thereby ensure that only known entities or customers who have passed KYC or other compliance checks can transact with their asset. Authorization revocable, which is usually used in conjunction with authorization required, enables an issuer to disallow an approved account from transacting with their asset should the status of that account change. Finally, clawback enabled allows the issuer to reclaim any portion of their asset's balance from a user's account. For example, if a central bank wishes to reverse a transaction due to fraud, they can if their CBDC is set to clawback enabled.

Issuers can activate one, two, or all three of these settings prior to issuing an asset, and can deploy them to fine-tune access to their asset. The menu of options allows an issuer to dial in control based on their needs.

ENHANCED COMPLIANCE CAPABILITY

The ability to control access to assets has an important consequence: it makes it possible to take advantage of a public ledger to issue digital currencies without forfeiting compliance capabilities. However, for issuers of real-world currencies such as CBDCs to consider that possibility, they also need to be certain that when transactions are applied to the ledger, they can't be rolled back or overwritten. They need transaction finality.

The ability to control access to assets has an important consequence: it makes it possible to take advantage of a public ledger to issue digital currencies without forfeiting compliance capabilities. However, for issuers of real-world currencies such as CBDCs to consider that possibility, they also need to be certain that when transactions are applied to the ledger, they can't be rolled back or overwritten. They need transaction finality.

Because Stellar was purpose-built for real-world asset issuance,the engine that drives the network, the Stellar Consensus Protocol ("SCP"), was designed with that need in mind. The mechanics of SCP are covered in detail in the Appendix, but here is a high-level overview of how it powers the network:

Stellar is a public blockchain network, which means its ledger is copied and kept in sync on computers all over the world, run by independent individuals and organizations. Those computers, known as validators, run software that implements SCP to pool, ratify, and apply transactions to update the ledger.

Like all blockchain consensus protocols, the point of SCP is to make sure that validators always add the same set of transactions to the ledger history at each step.

Roughly every five seconds, Stellar validators follow SCP to step through a specific process to update the state of the ledger. First, they accept signed transactions from Stellar users that do things like issue assets and make payments. Then, they communicate with one another to share those transactions, and group them into a transaction set for verification. Then, they vote on that transaction set. If a quorum of validators agree that it looks right, the transaction set is accepted and it's appended to the system's history. Since each ledger contains a cryptographic hash of the previous ledger, it is easy to tell if past transactions have been altered in any way, and so each time a ledger closes, the integrity of all previous data is, in effect, confirmed by the whole network.

As you may be able to tell by reading that description, SCP is similar to other blockchain consensus protocols in many ways. However, unlike Proof-of-Work and Proof-of-Stake protocols, SCP, as referenced above, relies on validators run by known organizations with verified identities, not anonymous nodes. Those validators don't compete to add transaction sets to the ledger. Rather, each designates a subset of other validators to programmatically consult when evaluating a transaction set, and votes to accept it if and when that subset signs off. Once a validator accepts, its decision is final, and the transaction set it ratifies can't be overwritten. The same is not true of other protocols, which often branch temporarily, then default to the longest chain. This temporary branching means that some other networks must wait for multiple "confirmations" before being sure a transaction won't be reversed, which can take upwards of 10 minutes. On Stellar, transactions are final after a single confirmation, which takes around five seconds.

When an organization issues an asset on the network, they designate a specific validator to enforce transaction finality, and that validator serves as the source of truth for the state of the ledger. Often, issuers run (and designate) their own validator so that they have control over the subset of validators it consults when ratifying transaction sets, and running a validator is something any issuer of a CBDC would likely do. So long as no one compromises an issuer's validators (and the underlying digital signatures and cryptographic hashes remain secure), the issuer knows exactly which transactions have occurred and avoids the risk of losses from blockchain history reorganization.

STELLAR AND SUSTAINABILITY

Because SCP relies on voting rather than a computational race, Stellar doesn't consume massive amounts of energy the way many other blockchains do.

According to a study conducted by Libraries, a single transaction on Stellar consumes approximately 0.22Wh, which is about 1 ten-millionth of the energy usage of Bitcoin, and similar to what the Visa network consumes.[5] In a world besieged by an ongoing climate crisis, that fact is likely important to anyone considering issuing an asset on a blockchain network, including central banks.

AUTOMATIC INTEROPERABILITY

By offering asset authorization capabilities and transaction finality, Stellar makes it possible for issuers to do something remarkable: they can take advantage of a tried-and-true public blockchain to issue and distribute assets without losing control over those assets or relying on unknown entities to validate transactions.

Issuing assets on a public network like Stellar comes with key advantages, including:

Transparency: a visible ledger allows anyone to monitor data and verify its correctness. Network users can track accounts, balances, and transactions without trusting the black box of third-party accounting.

Predictability: the protocol network participants use to update ledger data is open source, and anyone can audit the code to understand how it works and ensure that is sound.

Accuracy: that data is verified by independent entities, who validate any changes to it. No one can manipulate the data to their liking.

Redundancy: because the data is copied across a host of servers, there is no single point of failure. The system can sustain and recover from the breakdown or corruption of an organization's servers.

Security: because of that redundancy, malicious actors can't cheat the system by targeting a single entity. An entire network of validators prevents a local hack from impacting the ledger data.

But there's another, bigger advantage to issuing assets on a public network: automatic interoperability.

In addition to hosting assets issued by entities all over the world, Stellar natively supports markets between asset pairs. In a single transaction, a user can route a payment through those markets, which means they can both send and convert currency. It's a feature designed to make cross-border payments easy, efficient, and cheap.

Today, Stellar hosts a variety of stablecoins, which are fiat-backed digital assets issued by regulated financial institutions, and the issuers of those assets, along with companies that build network interfaces, wallets, and other applications, leverage that feature to offer innovative solutions to real-world problems created by fractured payment systems. For instance, rather than hopscotching cross-border payments through correspondent banks, companies use Stellar to power direct remittances from Europe to Africa. They provide their customers a cheaper, faster alternative to the status quo, and that's good for business and good for the world.

This feature becomes even more powerful if central banks issue CBDCs on Stellar. National currencies on a common ledger that automatically interoperate could facilitate secure, transparent, frictionless global commerce. Developers and entrepreneurs that build consumer- and business-facing products and services on the network could tailor their offerings to CBDCs and do even more to offer financial access and connect disparate markets.

The thriving ecosystem of businesses that create compliance solutions, provide liquidity, offer network services, and handle money transfer could work together with central banks and regulators to ensure the common infrastructure both serves business needs and protects consumers.

By encouraging participation, open networks like Stellar foster competition and spur innovation. They engage a wide variety of interests, draw on different perspectives to identify problems and develop solutions, and benefit from a diversity of creative ideas. Right now, as central banks consider CBDCs, they have a chance to build a new system designed from the beginning to facilitate those connections. If CBDCs are issued on open networks, they can inspire a better world, and avoid the problems that exist today due to siloed and disjointed payment systems.

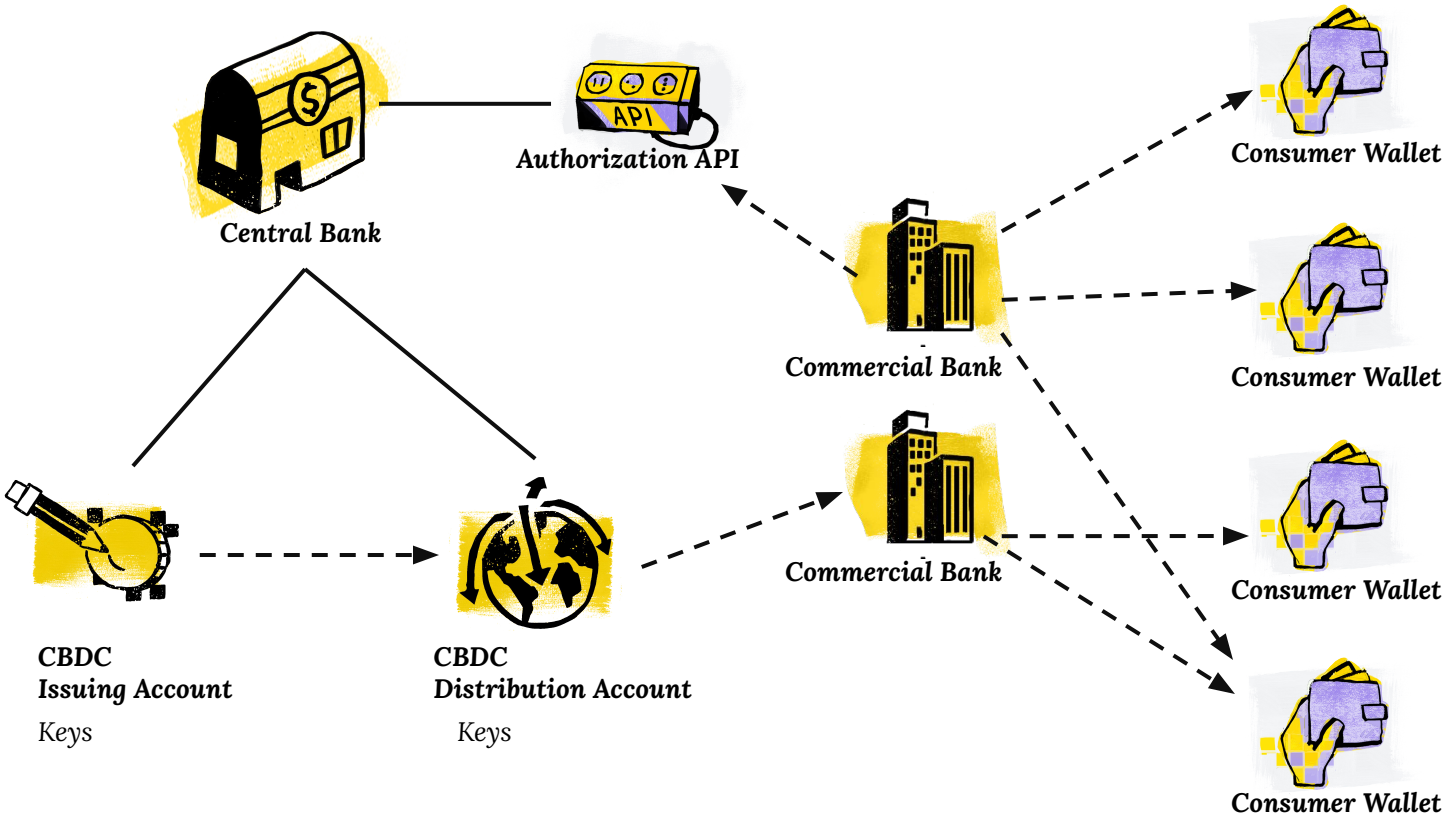
INTEROPERABILITY WITH TRADITIONAL FINANCIAL RAILS AND OTHER BLOCKCHAINS

As discussed under Secure Asset Issuance, Stellar was designed with the idea that regulated financial institutions would issue assets on it. Another way of putting this is that Stellar was designed from the start to interoperate with the traditional financial system. Its core features, APIs, and tooling were all built to be easy for banks and other traditional financial actors to hook into and interact with their systems. This is exactly what "interoperability" is. This interoperability extends to other blockchain networks as well. While Stellar is tailor-made for CBDCs, some central banks may choose to issue assets on other blockchain networks instead. The same things that allow Stellar to work with financial institutions make it easy for Stellar assets to interact with assets on other networks. Companies throughout the Stellar ecosystem are already building bridges to other blockchains that allow transactions to straddle ledgers, thereby opening up the possibilities for generalized functionality.

BEYOND THE FEATURES

Section II laid out many of the general features of Stellar that are beneficial for the issuance of a CBDC. This section provides a sample implementation of a CBDC on Stellar, to highlight how some of those features could work in practice. Different institutions will have different needs, of course, so this is meant to be an example only. The exact design and configuration of any CBDC will require additional technical, policy, and operational research. But this section gives the reader a sense of what is possible on Stellar.

The below diagram shows the key components of the design, each of which will be discussed in detail. This design assumes a so-called "two-tier system," in which the central bank mints the digital currency and distributes it to financial institutions, who then distribute it to end users. Many other designs could be implemented on Stellar as well.



A sample CBDC implementation on Stellar. This is a 2-tier model, for which many central banks have expressed a preference. A 1-tier model, in which the central bank distributes CBDC directly to consumers, could be implemented on Stellar as well.

CENTRAL BANK ACCOUNT SETUP, MINTING, AND DISTRIBUTION

In order to issue a CBDC on Stellar, the central bank would need to create two Stellar accounts, which we will call the Issuing Account and the Distribution Account. The Issuing Account is the source account whenever new tokens are minted. To mint tokens, the Issuing Account initiates a payment to the Distribution Account, which creates the tokens.6 Once minted, the CBDC would sit in the Distribution Account. From there, the central bank can transfer as needed to the commercial banks acting as "tier 2."

KYC/CDD AND DISTRIBUTION TO END USERS

By taking advantage of the authorization required feature on Stellar, central banks would be able to restrict their assets to being held only in accounts they have explicitly authorized. Much like with the creation of a bank account today, the central bank would need to make sure KYC/CDD checks had been conducted before authorizing an end user's Stellar account to receive the CBDC. In the existing system, banks, financial institutions, fintechs, and others (call them "Verifiers") that interact directly with users shoulder this responsibility, rather than the central banks. It would be no different with a CBDC. Verifiers could take care of all appropriate KYC/CDD screening, to make sure that no token of a CBDC would ever be held in an account that had not been fully vetted.

The exact process for doing this would differ slightly for custodial wallets and self-hosted wallets. Custodial wallets are wallets in which the wallet operator has control over the Stellar account holding the digital assets. In most cases, this means the wallet operator maintains a single Stellar account, which it uses as an omnibus account for all its users (much as a traditional wallet app might do with an omnibus bank account). Just like with financial institutions and other regulated entities today, these wallets would handle KYC/CDD checks of their users. The central bank would only need to authorize the wallet operator's omnibus Stellar account.

Self-hosted wallets are wallets in which each individual user manages their own private keys, and therefore the wallet provider does not have control of the underlying Stellar account for each user. In this case, the wallet provider is not "in the flow of funds," and is merely providing technology that helps the user interact with the Stellar network.

In the case of self-hosted wallets, there would have to be a more automated process for authorizing Stellar accounts because there would be no wallet operator to be responsible for KYC/ CDD. To address these issues, the central bank could set up a relatively simple process for Verifiers to perform this function that takes advantage of existing protocols currently employed by issuers of fiat-backed Stellar assets to conduct KYC/CDD. The basic steps would be as follows:

6 Every Stellar account is secured with cryptographic keys, which must sign any transaction moving assets out of that account. Accounts can be setup with any number of signing keys, and require any threshold number of keys for transactions. In this example, the Issuing Account is secured by three keys, and 2 out of the 3 are needed to sign transactions. Central banks are already experienced with managing sensitive electronic credentials and physical access to key hardware, so management of the keys for these Stellar accounts would not be fundamentally different from responsibilities they have today.

1. Individual proves to the Verifier that they control a particular account by sending a test transaction.
2. Verifier programmatically collect KYC/CDD information.
3. Verifier performs KYC/CDD checks on the individual.
4. Verifier sends a request to the API maintained by the central bank asking for the account to be authorized.
5. The central bank API authorizes the account.

Under this system, the central bank does not need to manually screen every account.[7]

fig. 1 Custodial Wallet

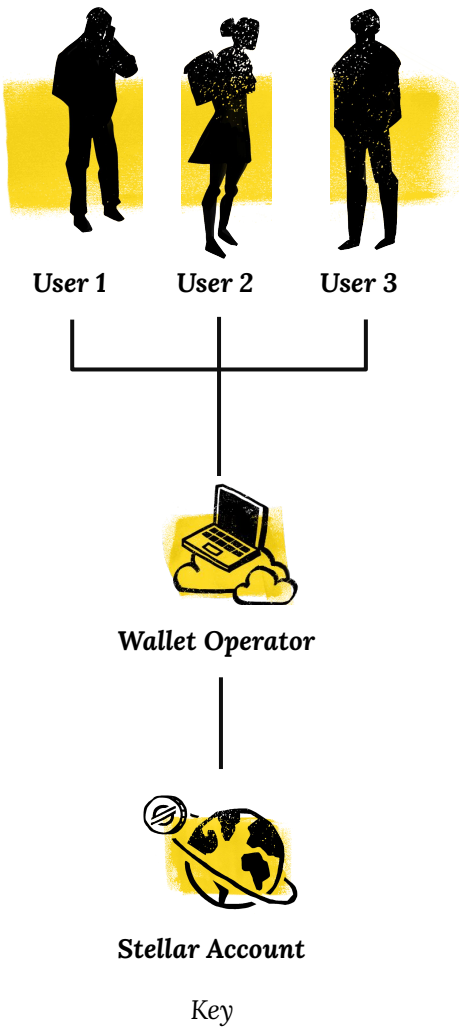
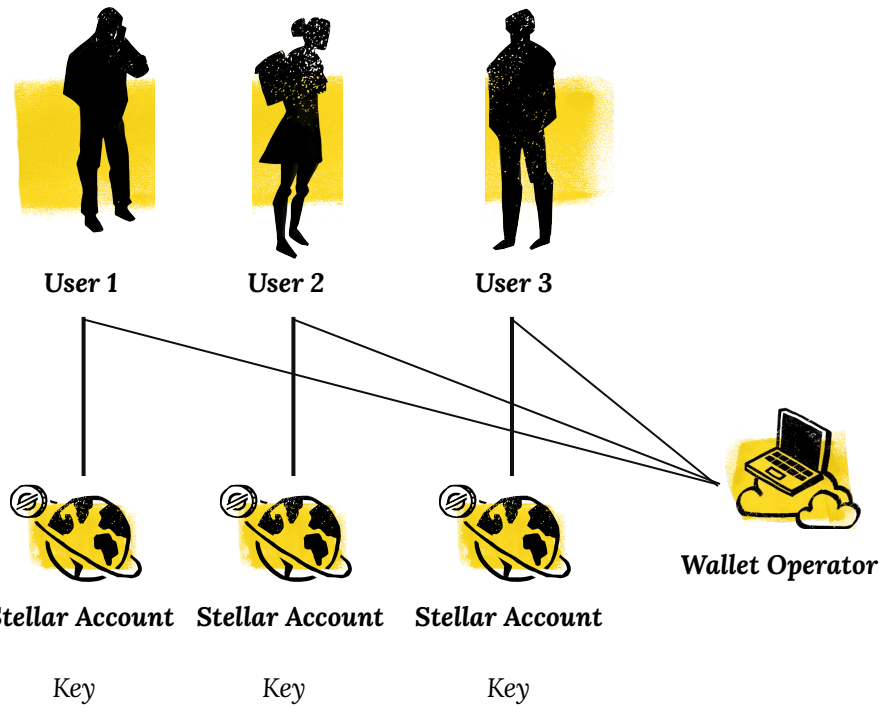


fig. 2 Self-Hosted Wallet



In a custodial wallet, the wallet operator manages the Stellar account and keys directly. In a self-hosted wallet, each User has its own Stellar account, and manages their own key.

STELLAR-HOSTED WALLETS AND FINANCIAL INCLUSION

Self-hosted wallets are the closest thing to holding cash in one's pocket, but in digital form, because the user has complete control over the assets. For this reason self-hosted wallets could be a useful tool in furthering financial inclusion. Although users would have to learn some new behavior, such as managing a private key, the basic usage could be analogized to using cash.

In the case of the unbanked. Central banks could use Verifiers other than traditional financial institutions to screen these users for purposes of authorizing their Stellar accounts to hold the CBDC. Post offices could be an interesting option, given their geographic reach and individuals' familiarity with them. Simple processes could be designed where an individual can go to a post office, show required identification, and then scan a QR code in order to load the test transaction needed to verify control of their account. In this way, the entire authorization process could be done in minutes, and the user could start enjoying the simplicity of cash with the reach and security benefits of electronic money.

BURNING

In the current system, commercial banks periodically send fiat currency back to the central bank, to be exchanged for increased reserves. In the CBDC context, they would do this by transferring the CBDC back to the Distribution Account. The central bank could retire CBDC entirely by transferring it from the Distribution Account back to the Issuing Account. Sending the CBDC to the Issuing Account burns those tokens, and they will no longer appear on the ledger.

CENTRAL BANK VALIDATOR

In addition to the account setup described above, the central bank can contribute to the overall resilience and security of the network by running Stellar validators. Validators are the nodes of the network that run the Stellar code to keep a copy of the ledger and process transactions. By running validators, the central bank can treat the ledger maintained by its validators as the definitive source of truth for balances of its CBDC. As explained in more detail in the Appendix, validators on Stellar choose which other validators to trust for the purpose of maintaining the ledger. This means that as a validator is processing transactions and about to update its ledger, it checks with the validators it trusts to make sure they agree with the proposed changes. In this way, validators on Stellar know exactly what organizations they are relying on to keep the ledger safe and consistent, rather than relying on anonymous actors.

The central bank would choose other reputable institutions, such as its own regulated institutions or other countries' central banks, as its trusted validators.

7 The Stelar network already has certain network protocols for these steps, including Stellar Web Authentication for individuals to prove control of an account (Step 1), and the Stellar KYC API for collecting KYC/CDD information (Step 2). Central banks could utilize these standards, or define their own.

This setup achieves two main results. First, it promotes resilience because even if the central bank's validators were to go down for some reason, their CBDC could continue to be transacted because these other validators would continue processing transactions. Second, it promotes safety; attacking the CBDC would mean compromising the validators of some number of these other entities, which would be very difficult given their sophistication and scale.

This is unlike other networks, where amassing enough computation power or total capital can allow an attacker to compromise the system.

STELLAR AND PROGRAMMABILITY

Many central banks researching CBDCs are focused on their "programmability" as one of the key benefits, and therefore believe the underlying technology must have "smart contracts" (the ability to write arbitrary programs that execute on the network). Stellar does not have smart contracts of this type, but in most cases, they are unnecessary for the programmability of CBDCs, and introduce security risks.

The important aspect of programmability is that it is easy for entities to write software that interacts with CBDCs – not that the execution of that software be decentralized. Current payment and banking systems were designed in ways that made it hard for private actors to do this, which is what has prompted Open Banking initiatives around the world. Because Stellar is an open network, it would not suffer from these same issues.

Furthermore, much of the "programmability" envisioned bycentral banks could be accomplished with the built-in features of Stellar, which include multi-signature accounts and batched transactions, without introducing the risks of bugs and security flaws in arbitrary smart contracts. For example, a common use case raised is ensuring social benefit payments are only spent on certain items (e.g., food, rent, health care). This could be solved quite easily on Stellar by issuing a separate asset for these payments (which would be legal tender, like a general CBDC), and making accounts go through an approval process before being authorized to hold it (using the authorization required feature of Stellar). In this way, a central bank could be certain that those funds are not being used to pay for excluded items.

IV. Conclusion

THE WORK BEGINS

This paper has walked through the ways in which Stellar is uniquely suited for the issuance of CBDCs and laid out a sample implementation. Any actual implementation will require detailed work from policymakers, economists, and technologists. As with the development of the internet, blockchain technology will have its greatest impact on our world if the public sector and private actors work together to imagine its possibilities. We look forward to the part Stellar can play in this journey.

Questions and comments on this paper can be directed to partnerships@stellar.org.

Diving Deeper

APPENDIX

Appendix

SCP DEEP DIVE

This appendix explains the Stellar Consensus Protocol ("SCP") in greater detail. Stellar gives asset issuers (like central banks) the certainty, safety, and control of a permissioned system, with the openness and interoperability of a permissionless network. This appendix seeks to explain how its design leads to these properties.

We start by discussing consensus protocols in general, including a brief explanation of the most common types used by blockchains (Proof-of-Work and Proof-of-Stake). Then we go through how SCP works, including an analogy to help build intuition. With that groundwork laid, we turn to a hypothetical CBDC issuance, to see how SCP benefits central banks in practice.[8]

Consensus Protocols in General

Every blockchain network (including Stellar) consists of multiple computers that store a copy of a ledger. The blockchain establishes rules for how those computers check transactions and update their ledgers. The "consensus protocol" for a blockchain refers to the system of rules the network uses to make sure all copies of the ledger match (i.e., keep consensus with each other). Probably the most widely known consensus protocols are Proof-of-Work, which is what the Bitcoin network uses, and Proof-of-Stake, which is what the Ethereum network is planning to switch to (it currently uses Proof-of-Work).

The key point to understand for our purposes is that in both of these systems, the nodes contributing to consensus are totally anonymous. An organization operating a node on those networks has no way of knowing what organizations or entities are doing the work that maintains the integrity of the overall ledger. As a result, these systems can be compromised if a malicious actor has enough resources. In the case of Proof-of-Work, an organization with 51% of the computation power on the network could manipulate the ledger. And similarly in the case of Proof-of-Stake, an organization with 51% of the total amount staked could manipulate the ledger.[9]

8 This Appendix seeks to explain the key aspects of SCP only, and is not meant to be a technical, exhaustive description of the protocol. For a formal treatment of SCP, see Mazières, David, The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus, available at www.stellar.org/papers/stellar-consensusprotocol (the "SCP Paper").

9 In most Proof-of-Stake systems, if an actor were to commit an attack of this kind they would lose the value they had staked. The logic goes that no attack would be worth the huge amount of staked value that would be lost in an attack. We do not think this argument holds up in the case of CBDCs, though, because the total value of the CBDC issued on the network could be orders of magnitude larger than the total value of the native network asset. Furthermore, attackers could have non-financial motivations for an attack, meaning it could still be worth doing even if they lose money.

Box 1. COMMON CONSENSUS MECHANISMS

In a Proof-of-Work system, nodes on the network compete to add new blocks of transactions by trying to solve a difficult computation problem first (and thereby getting a reward). As soon as they solve it, they broadcast their new block (and proof that they solved the hard problem) and other nodes add it to their history of the ledger. Everyone then starts working on a new block of transactions, and so on.

In a Proof-of-Stake system, each time a new block is considered a set of nodes is chosen randomly to review and certify it. The probability of a node being chosen is based on the amount of value the node has put at risk, or "staked." If a node tries to certify a fraudulent block, it forfeits some or all of its stake.

The Stellar Consensus Protocol

SCP works very differently from Proof-of-Work or Proof-of-Stake. The most important distinction is that nodes on Stellar are not anonymous. Instead of having no idea who is participating in the network, every organization that runs a node is expected to publish a special document (called a toml file) on a public web page controlled by that organization. For example, is the toml file for the nodes operated by the Stellar Development Foundation ("SDF"), which has been published on a page at the stellar.org domain (which is controlled by SDF). This file explicitly identifies specific Stellar nodes as SDF-operated. This transparency of the organizations running nodes on Stellar is key to understanding how a central bank could safely issue a CBDC on Stellar.[10]

Voting

Nodes on Stellar that participate in consensus are called validators and do so by voting on various statements about proposed changes to the ledger.[11] For example, about every 5 seconds they vote on whether to apply a set of new transactions to the ledger history. If that vote passes, those transactions become an official part of "the blockchain," and are used to update the balances on the ledger itself.

Because Stellar is an open network with nodes potentially joining or leaving over time, and because there are practical realities such as network latency and unexpected outages that can cause complications (as can happen with any network), voting isn't as simple as every node saying "yay" or "nay". Instead, nodes go through a multi-phase process to ensure the network cannot get stuck if different nodes vote for different ledger modifications.

Going through every detail of this process isn't necessary for our purposes, other than two key points.

10 It should be noted that even though SDF runs nodes on the Stellar network, SDF does not own, operate, or control the network.
11 There are actually three different types of nodes on Stellar. In this Appendix, we use "node" and "validator" interchangeably. More information on Stellar node types can be found at https://developers.stellar.org/docs/ run-core-node/#types-of-nodes.

First, when it's time to pick a new set of transactions to add, the network goes through two distinct phases, called nomination and balloting. Nomination means voting on statements of the form "This is a set of transactions we should consider applying." Once a statement like that is nominated (meaning a candidate set of transactions has been chosen), then balloting is the process of picking exactly one candidate transaction set to apply to the ledger.

Second, voting for a particular statement entails a node casting two types of vote on that statement: "accept x" and "confirm x." You can think of these in the following way:

- "Accept x" = "I am ready to vote for x, and won't vote for anything else"
- "Confirm x" = "I vote for x"

With this foundation, we can now see how SCP works.

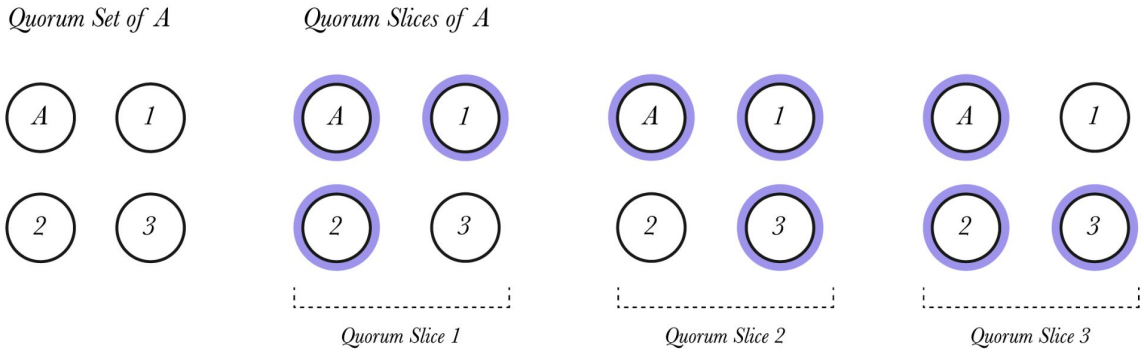
Quorums

The point of SCP is to make sure that nodes always add the same set of transactions to the ledger history. In this way, the complete ledger history and current ledger state maintained by any two nodes will be identical.

The key rule is this: a node cannot vote "confirm x" until it sees a quorum of other nodes vote "accept x." This rule obviously requires a definition of "quorum," which we will build up by going through three key definitions: quorum set, quorum slice, and (finally) quorum.

First, every node on Stellar defines an explicit set of other nodes that it trusts. Those nodes, along with the node itself, are called its quorum set. You can think of a node's quorum set as the set of nodes that it never wants to disagree with.

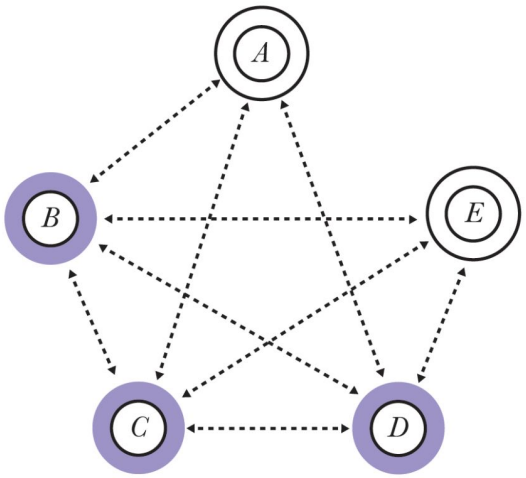
Second, every node also defines a threshold for how many of the other nodes in its quorum set must vote identically for a vote to succeed.12 That threshold results in a bunch of subsets of the quorum set, which are called quorum slices. For example, the below diagram shows that if a node has 3 other nodes in its quorum set, and a threshold of 2, it has 3 different quorum slices.



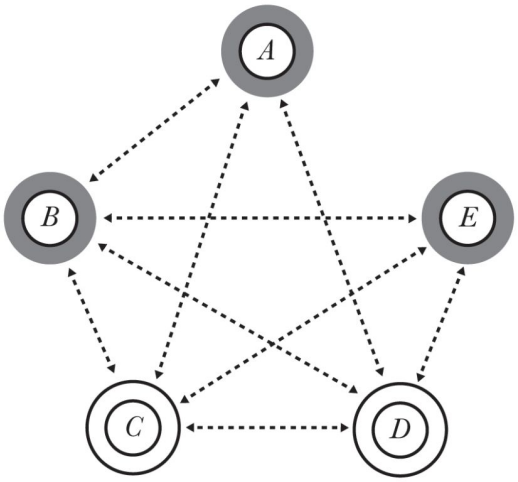
An example Quorum Set and the resulting Quorum Slices. If node A has three other nodes in its Quorum Set and requires at least 2 of them, A has 3 resulting Quorum Slices.

12 Requiring agreement of the entire quorum set to move forward wouldn't be practical, because if a single node in that set went down for any reason (such as routine maintenance or an unexpected outage), the node would be stuck. Allowing a subset makes the system resilient.

We can now finally define a quorum. A quorum is a set of nodes that includes at least one quorum slice for each of the nodes in it. Put another way, for each node V in a quorum, the quorum also contains at least one of V's quorum slices. In the diagram below, the arrows show what nodes are in a node's quorum set, and suppose all nodes require 2 other nodes for a quorum slice.



{B,C,D} is a quorum, because they each have at least two other nodes in their Quorum Set in it



{A,B,E} is NOT a quorum. Node B has a quorum slice, but nodes A and E do not.

Now we can understand the key rule stated before: a node cannot vote "confirm x" until it sees a quorum of other nodes vote "accept x." So when a node N is considering confirming a set of transactions to add to its ledger history, it waits until a set of nodes (including itself) that make up a quorum have voted to accept (i.e., are ready to confirm it themselves). Importantly, it's not enough for N to see that one of its quorum slices has accepted the set; N needs to see that an entire quorum (which by definition will include at least one of N's quorum slices) has accepted the set. Only then can N confirm the set of transactions and apply them to its ledger.

Math Test Analogy

To help make this rule make more sense, consider the following analogy. While not perfect, it should help you understand the intuition behind SCP's design.

Imagine you are in a large math class with a take-home test, and you are allowed to compare answers with other students before handing it in. Naturally, each student is going to have a set of other students that they trust to help with the test. I might trust Isaac, Leonard, and Emmy, while you might only trust Isaac, Ada, and Carl. Everyone has their own preferences.

Furthermore, each student will have a threshold for how many of their trusted friends they need to agree with in order to hand in the test. I might be comfortable handing in the test if at least 2 of my friends agree with my answers, but you might need 3.

When it's time to actually do the test, the best way to do it is to form study groups and have everyone in the group agree on the answers before submitting the tests. When picking a study group, I am naturally going to make sure that enough of my trusted friends are in the group so that I can feel confident in the answer we all decide on. But if I want to have confidence that the entire study group will actually hand in the answers we agree on, it's not enough for me to make sure I have enough friends in the group. I need to make sure that every other person in the study group also has enough of their friends in it. Suppose Alice is in the group, but doesn't have enough of her friends in it. Even if Alice tells everyone that she plans to hand in a particular set of answers, we can't know for sure that's what she'll ultimately hand in. After we're done, she might go meet with a study group that does have enough of her friends, and they could convince her to hand in different answers.

Relating this back to SCP terminology, each student is like a node, and their set of trusted friends is their quorum set. The subsets of friends that are enough to hand in a test are quorum slices. Finally, a correctly constructed study group is a quorum. This hypothetical math test is effectively how SCP works to keep ledgers in agreement with each other.

Quorum Intersection

We now know how each individual node makes decisions, but the natural question is how can we know that every node is going to end up with the same vote every time? The answer is that SCP is guaranteed to get total agreement as long as any two quorums intersect in at least one honest node (i.e., a node correctly following the rules of SCP). We call this property Quorum Intersection.[13]

Turning back to our math test analogy, imagine that based on everyone's friendships, there are only two study groups in the class, and that Alice is the only student in both study groups. If Alice is honest, the two study groups will have to hand in the same answers, because each study group will only hand in answers once everyone in the study group, including Alice, agrees on them. If Alice is honest, she can only commit to one set of answers.

Back in SCP terminology, if there is Quorum Intersection, then two different quorums confirming different statements would mean that the honest node in both of them had accepted two different statements. That is impossible, because once an honest node accepts a statement, it can never accept anything different (remember that you should think of "accept x" as "I am ready to vote for x, and won't vote for anything else").

Quorum Intersection can fail in two main ways. If the intersection of two quorums consists of dishonest nodes, those quorums may confirm different values (because the dishonest nodes might send "accept x" to one quorum and "accept y" to the other, violating the rules of SCP). Second, if there are quorums that don't intersect at all, they can confirm different values. This would be like having two study groups with no overlap. Because nodes on Stellar publish their quorum sets and quorum slice configurations, it is easy to check that quorums intersect, and in what nodes.[14]

13 For a formal definition of Quorum Intersection and related theorems proving how it leads to consensus, see the SCP Paper.
14 Stellarbeat.io is a free tool for doing quorum analysis.

Furthermore, because nodes are not anonymous, issuers and users alike can understand how many nodes would need to be dishonest in order to cause issues. In the case of CBDCs, these nodes would be run by institutions like central banks and financial institutions.

It would be very difficult for multiple nodes like this to act dishonestly. In our view, this is much safer than comparable Proof-of-Work and Proof-of-Stake systems. Manipulating Stellar would require massive coordination among highly regulated, geographically dispersed entities, which would be much harder to accomplish than a single actor amassing a large amount of computational power or capital.

Consequences of SCP for Issuing a CBDC on Stellar

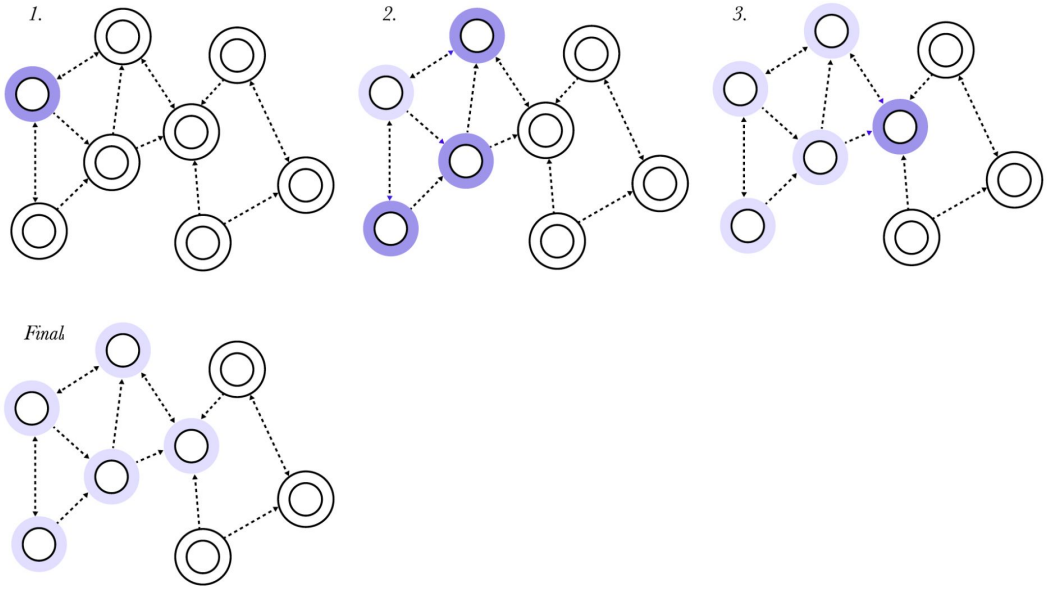
With this understanding of how SCP works, we can better appreciate how Stellar is uniquely suited for CBDCs. Suppose a central bank wanted to issue a CBDC on Stellar.

Choosing a Quorum Set - Giving the Issuer Confidence

To begin, the central bank sets up its own nodes, so that it can participate directly in ensuring the integrity of its CBDC and all transactions involving it. The central bank then chooses which other nodes to put in its quorum set. Presumably, it chooses only nodes operated by extremely trustworthy and responsible organizations and institutions. If other central banks have issued CBDCs, it probably wants to include those central banks' nodes in their quorum set as well. It can also include nodes from regulated financial institutions, such as banks or other financial institutions.

By choosing its quorum set, the central bank knows exactly which other nodes have the potential to influence its copy of the Stellar ledger, and which can have no impact whatsoever. In other words, the central bank does not have to rely on anonymous actors following a complex protocol to keep their asset safe; they can rely on known organizations and institutions.[15] Suppose there is a node that the central bank knows for certain is malicious and is doing everything it can to manipulate the ledger and interfere with transactions. The central bank can check very easily if that node has any chance of impacting the central bank's ledger by finding something called its transitive quorum set. Start with the central bank's quorum set. For every node in it, add that node's quorum set. Repeat this process until there aren't any more nodes to add. The resulting set contains all nodes that can directly or indirectly affect the central bank's ledger. If the malicious node is not in this set, the central bank does not have to worry about that node affecting the integrity of the ledger.

15 Because nodes aren't anonymous, the central bank can use whatever means it wants to verify that the nodes it adds to its quorum set are actually operated by the given institutions. For many Stellar participants, simply checking the toml file is enough assurance, because it is posted on an internet domain controlled by the organization. But institutions like central banks could go even further and require direct certifications and proof from trusted individuals at the organizations. It could also enter into legal contracts with these other organizations to ensure compliance with specific standards or requirements.



To find the transitive quorum set of a node, add its quorum set and then the quorum sets of those nodes, and so on until there are no new nodes to add.

Issuer Enforced Finality - Giving Users Confidence

The above shows how the central bank can be confident in the safety of its ledger and now we turn to how users of a given CBDC can be confident in their balances and transactions. As mentioned before, one of the risks with Proof-of-Work and Proof-of-Stake systems is that any transaction can potentially be reversed in the future. The likelihood goes down with time, but it's always there. Furthermore, at any given time there can be multiple branches of the ledger history, which might show a person as having two different balances of an asset. All of this obviously creates difficulties for someone trying to understand how many CBDC tokens are in their account.

The reader may, however, point out that a user of the CBDC could worry about the possibility that there are quorums with no intersection (like the math test example with non-intersecting study groups), and therefore two different nodes could have different histories. This is true, but it has a very simple solution. When a user wants to check their CBDC balance, they can simply check the ledger maintained by the central bank's node. At the end of the day, that is the balance that matters, because it's the source of truth for the central bank.

We refer to this concept as issuer-enforced finality. In the unlikely event that nodes have different histories, it's always clear which one is correct with respect to a given asset. And in fact, users don't have to go around checking a different node for each asset balance. If central banks choose quorum sets that overlap, then their nodes' ledgers will match. Central banks have a strong interest in making their quorum sets overlap heavily (for example by adding each other) to make the system more resilient, so this would almost certainly happen in practice.
Furthermore, they would pick organizations and institutions with a very low probability of being dishonest.

Stellar

THANK YOU!

stellar.org