Fortanix®

WHITEPAPER

TOKEN VAULT NETWORK

FORTANIX, INC.

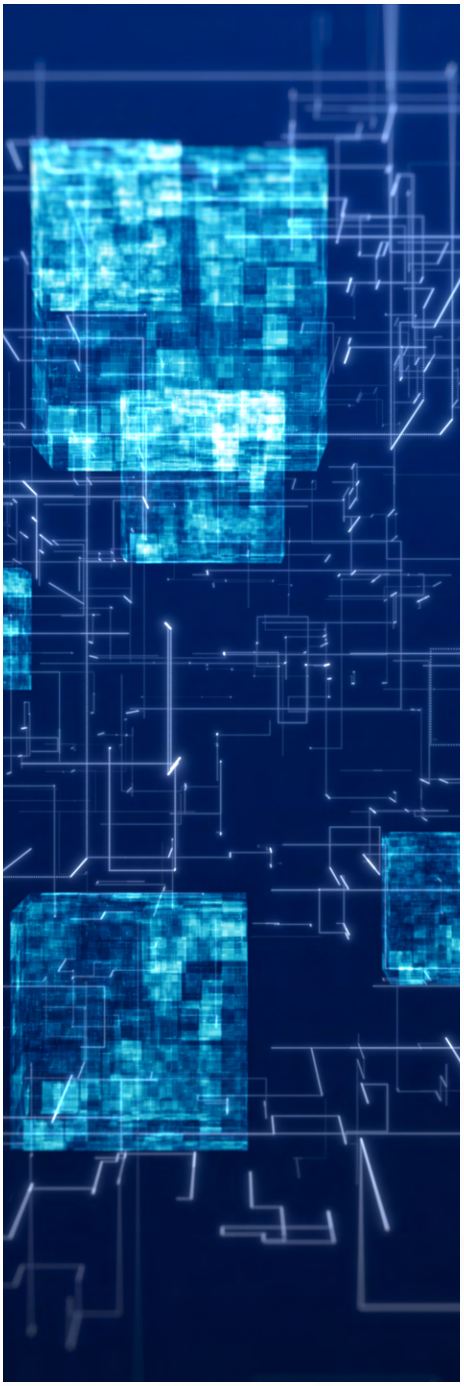
Pralhad Deshpande, Ph.D.

Anand Kashyap, Ph.D.

TABLE OF CONTENTS

Abstract

Tokens represent electronic value that can be transferred between custodians efficiently. We present a new token transfer technology that does not rely on distributed consensus for token transfers. Using our technology, tokens can be transferred point-to-point between banks while respecting the confidentiality and compliance requirements that banks must adhere to. We present several use cases that are enabled using our technology.



Introduction

The correspondent banking model has been in use for several centuries. The SWIFT network for global financial messaging is 50 years old. Yet, the fastest way to make a global payment today is with a tokenized stablecoin issued on a programmatic blockchain. It is fair to believe that the tokens model has certain efficiencies that the accounts model does not have.

Towards the latter part of 2015, the price of Bitcoin (Nakamoto, 2008) was hovering around the USD 500 mark, and Ethereum (Buterin, 2014) had just been launched. Several innovation arms of Banks and Central Banks started noticing the activity in the crypto-economics domain and set up innovation agendas for organized exploration. Looking back, two vastly different innovation agendas could have been set at that time.

Blockchain-focused agenda

Explore the use of blockchain to decentralize banking functions traditionally executed by centralized entities.

Token-focused agenda

Acknowledge that the tokens model is more efficient compared to the accounts model and explore how the tokens model could be adapted to the banking context.

Over the years, the blockchain-focused agenda has received significantly more focus and attention compared to the token-focused agenda. Innovation labs have explored topics such as decentralized netting of payments, decentralized atomic swaps of assets, and decentralized interbank messaging.

In this whitepaper, we are interested in exploring the less explored topic: how can we adapt the significantly more efficient tokens model in the banking context? In 2015, the tokens ecosystem was not fully developed, and even if one could see that tokens were efficient, it was unclear whether tokens had any positive social utility. Today we see a rich tokens ecosystem with many token issuers on programmatic blockchains. With a 25-fold increase in market capitalization over the course of the COVID-19 pandemic (The Stablecoin Index, 2023), stablecoins have become a mainstay of the gig economy. We believe that the tokens model has proven itself not only from the efficiency perspective but also from the positive social impact and utility perspective. Now is the right time to ask whether the tokens model could drive efficiencies in the banking world.

As we uncover the topic of tokens for banks, we notice that the prevailing token transfer technology, blockchain, is unsuitable for this environment. Blockchain relies on distributed consensus for token transfers, and distributed consensus involves over-replication of transaction data. However, banks operate in a regulatory environment where over-replication of data is prohibited. Therefore, for regulatory reasons, banks cannot use blockchain as a token transfer technology. The main contribution of this whitepaper is to introduce a new token transfer technology that respects the confidentiality, compliance, and reporting requirements that banks must adhere to. We present several use cases which are enabled by interbank tokens.

Why is The Accounts Model Inefficient?

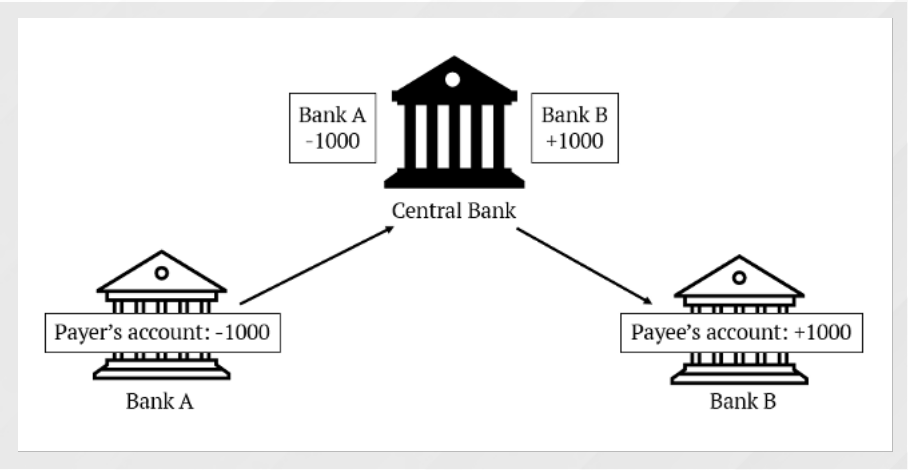


Figure 1: A simple schematic describing the flow of assets from one bank to another.

The traditional world of banks and large financial institutions is used to the accounts model. A financial institution issues assets, and these are maintained in the accounts held by its customers. The issuing entity is also the transaction processing entity. Assets issued by an institution can be easily transferred from one customer account to another, provided both accounts are held with the same institution. It is not possible to transfer an asset from an account in one institution to an account in another institution. For example, suppose you have an SGD denominated bank account with Bank A, what you have is Bank A's promise of SGD to you. As illustrated in Figure 1, moving value from a Bank A account to a Bank B account is only possible because both banks maintain SGD accounts with the Central Bank.

The accounts model is inefficient because:

A single custodian holds all assets. Transacting parties need to have accounts with custodians to transact with assets.

When assets are exchanged or a basket of assets held by several custodians is moved, the speed at which different assets are transferred is different. Some assets may change hands in real-time, some with a delay of T+1, T+2, or T+3. This results in an elongated clearing phase and introduces settlement risk in the system.

Interbank communication relies on structured messaging. Some messages may be received but not acted upon. Some messages may be acted upon multiple times. Consequently, the accounts model heavily relies on reconciliation frameworks to ensure the integrity of transaction processing.

On the other hand, as we shall see in the following section, the tokens model is far more efficient.

Why is The Accounts Model Inefficient?

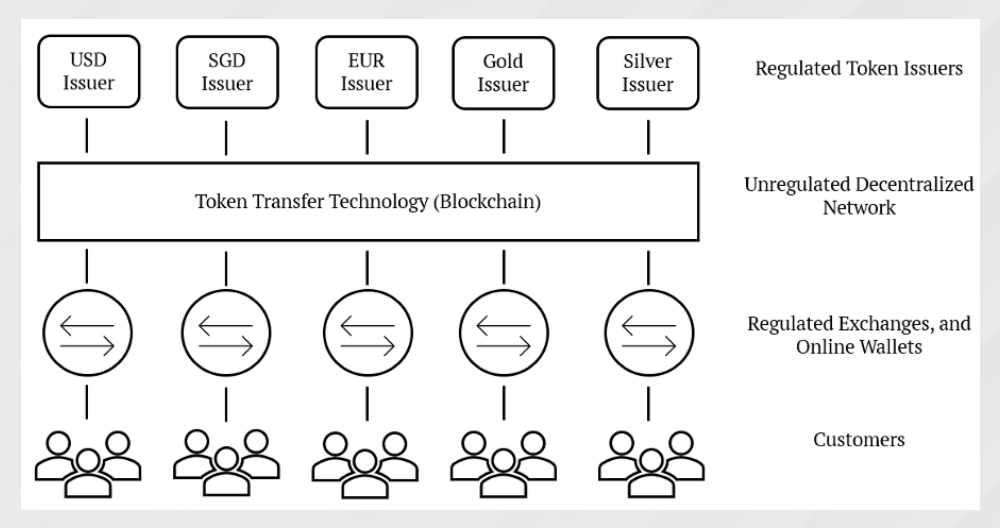


Figure 2: Four layers of the public blockchain ecosystem.

As shown in Figure 2, the public blockchain ecosystem can be mapped to four layers – (i) token issuers, (ii) blockchain, (iii) regulated exchanges and online wallets, (iv) customers.

The tokens model has several efficiencies:

- Any token issuer can issue tokens on the token transfer layer.
- Any crypto exchange or online wallet may plug into the token transfer layer to hold and globally transfer assets in real-time on behalf of their customers.
- Exchanges and online wallets need not have a direct relationship with any token issuer.
- The speeds at which tokens can be transferred are the same for all tokens. This significantly differs from the accounts-based model, where different assets tend to settle at different speeds.
- Token transfers can happen 24x7x365 in real-time at low costs.
- Reconciliation frameworks are not required in the tokens model.

The tokens model is efficient because of the separation of concerns. Token issuers are not burdened with transaction processing and customer onboarding. Vastly different sets of entities handle transaction processing and customer onboarding.

Why Don't Banks Use The Prevailing Tokens Model?

If the tokens model is so efficient, why don't banks use it? While the tokens model can bring in several efficiencies, the prevailing token transfer technology, public blockchain, has several shortcomings.

Public blockchains are unsuitable for banks for the following reasons:

All transactions are recorded publicly. Even though the transactions are between pseudonymous addresses, several works have shown that it is possible to map these addresses to real-world identities. Banks report to their regulators, not the public at large.

A blockchain is a shared resource with limited throughput. Blockchain users compete for this shared resource. Transactions that result in higher fees collected for the miners/ validators are chosen to be included in the blockchain. Others are discarded.

Proof-of-Work blockchains do not provide explicit acknowledgements of having processed transactions. Blocks added to the blockchain may be discarded later by miners causing confusion.

Proof-of-Stake blockchains are often highly centralized, with most of the voting power controlled by a handful of entities. Banks would be extremely uncomfortable letting a handful of pseudonymous entities process their transactions.

For various reasons, the prevailing token transfer technology, public blockchains, is unsuitable for banks. The efficiencies that the tokens model delivers are indeed worth aspiring for, but we need a new token transfer technology that is suitable for banks. Are Permissioned Blockchain and Distributed Ledger Technology (DLT) suitable token transfer technologies?

Why Don’t Permissioned Interbank Blockchains Support Tokens?

Between 2016 and 2020, the Monetary Authority of Singapore (MAS) ran Project Ubin (Project Ubin, 2016), a collaborative project with the industry to explore the use of Permissioned Blockchain and DLT for clearing and settlement of payments and securities. Partior (Partior, 2023) is the blockchain platform for payments clearing and settlement that grew from Project Ubin. But Partior does not use the tokens model. It relies on the traditional accounts model instead. Despite the tokens model being so much more efficient than the accounts model, why don’t interbank blockchains such as Partior use it?

The tokens model requires distributed consensus on double-spend prevention. This model requires that transaction data be replicated across a vast number of banks. Unfortunately, banks must adhere to strong confidentiality and compliance requirements. Only the parties involved in the transaction should be aware of it. Transaction data cannot be over-replicated for regulatory reasons. Consequently, banks cannot implement distributed consensus on double-spend prevention and hence cannot implement the tokens model.

Interbank Token Vault Network

While the tokens model is extremely efficient, there is a need to develop a new token transfer technology that is suitable for banks. Based on the discussion thus far, we can put together a concise list of requirements that a new token transfer technology must satisfy:

Confidentiality

Only the two banks involved in transferring tokens must be aware of the transaction.

Scalability

The token transfer technology should be scalable. There should be no upper limit on the throughput of the network.

Token Receipts

Every received token should be acknowledged with a receipt.

Auditability

Each bank should be able to produce a tamper-proof trace of their transactions for reporting purposes. One should be able to import the trace into well-known auditing tools.

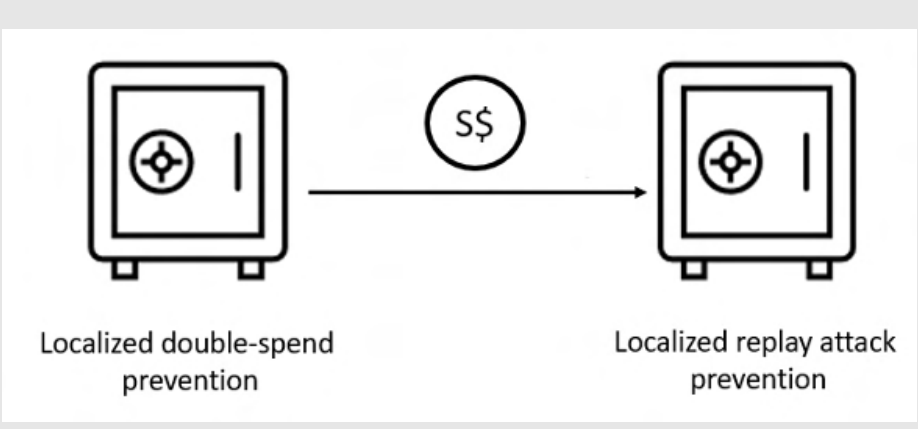


Figure 3: With two new primitives, interbank token transfers can be executed point-to-point between Token Vaults.

We introduce the concept of a Token Vault. As depicted in Figure 3, Token Vaults are merely custody solutions that implement two new primitives. The first primitive is localized double spend prevention. This primitive ensures that the same token is not spent more than once. The second primitive is localized replay attack prevention. This primitive ensures that the same token is not received more than once. Using these two primitives, it is possible to transfer both fungible and non-fungible tokens between Token Vaults in a point-to-point manner. Since the messaging between Token Vaults is point-to-point, the Token Vault Network (TVN) is highly scalable. In fact, the total network capacity increases with the addition of new Token Vaults.

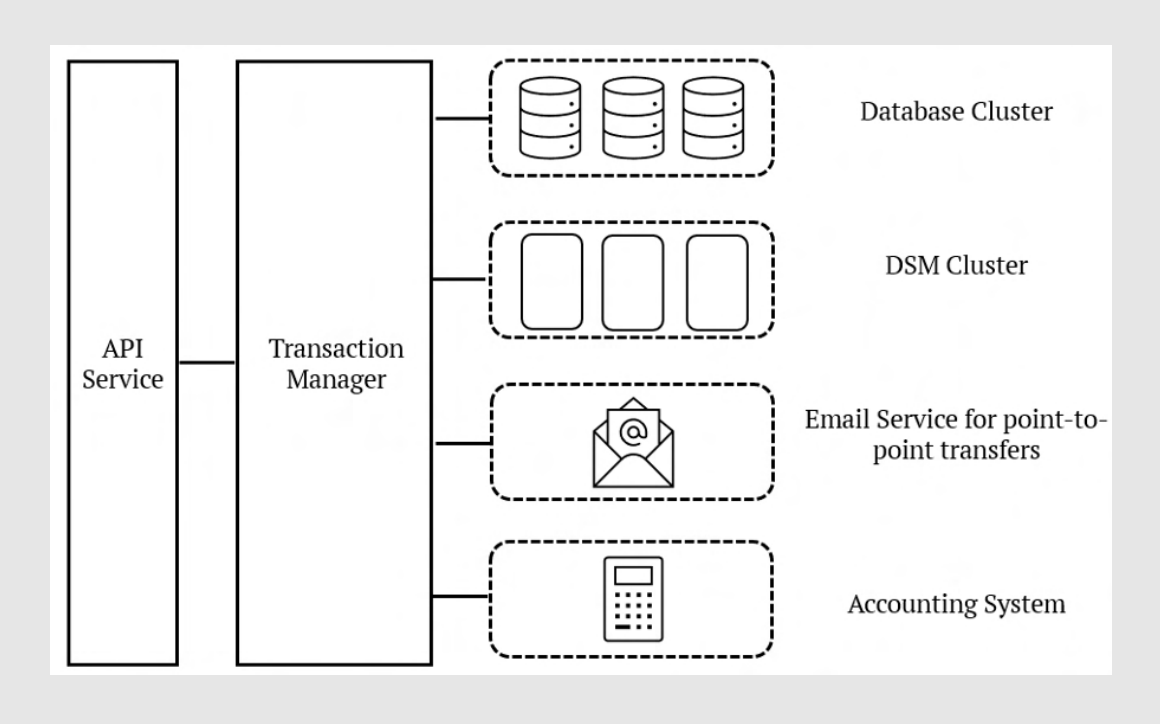


Figure 4: High-level architecture of a Token Vault.

Figure 4 shows a high-level architecture of a Token Vault. Fungible and non-fungible tokens are stored within the database cluster and transferred following the double spend prevention logic implemented within the highly secure Data Security Module (DSM) cluster. Token Vaults communicate with each other using encrypted email. When a token is received, it is validated for integrity and added to the database cluster while following the replay attack prevention logic implemented in the DSM cluster. DSM is an Enterprise Grade Confidential Computing platform developed by Fortanix. Several top banks, financial service providers, and government entities use this platform for various use cases. The platform is certified to the highest standards of security and compliance controls, including FIPS 140-2 L3, PCI-DSS, SOC 2, and SOC 3. Each received token is responded to with a receipt.

The Token Vault generates a tamper-evident trace of transactions for regulatory reporting. The trace can be imported into popular accounting systems easily. If required, the Token Vault can be enhanced to support online regulatory compliance. For example, we can configure the Token Vault to require approvals from a regulatory authority before a token is spent. Approvals may be enabled for every transaction or when certain transactional limits are breached.

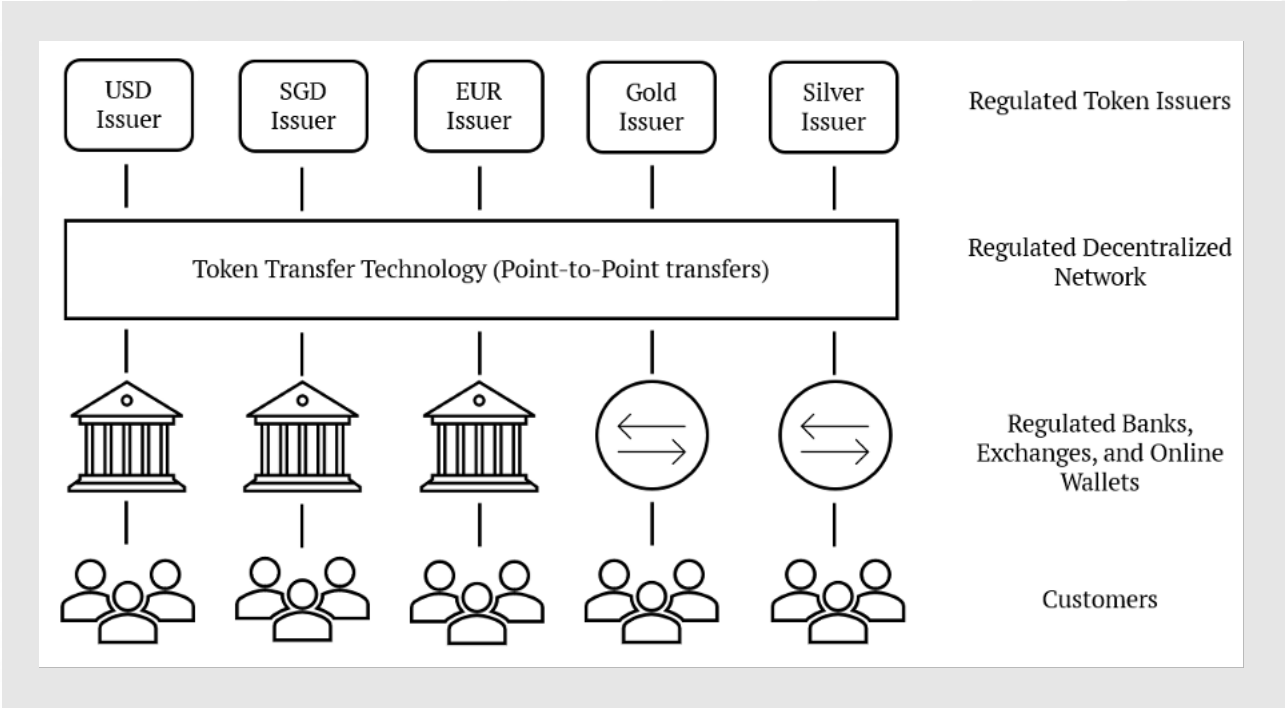


Figure 5: A regulated, decentralized TVN.

An interbank tokens ecosystem could look remarkably like the public blockchain ecosystem shown in Figure 2. But we must swap out the Blockchain layer with a layer allowing point-to-point token transfers. This could be a regulated, decentralized TVN, as shown in Figure 5.

Use Cases

The TVN unlocks several novel use cases. In this section, we capture the prominent ones.

Global Real-Time Payments With Stablecoins

Imagine a network of Token Vaults spread across various banks, payment service providers, and even online crypto-currency wallet providers and exchanges. Several stablecoin issuers could issue fiat-backed stablecoins directly on this network. Consumers could make instant global payments using such a network. The sub USD 200 global remittances market is woefully underserved. It is not cost effective to make small-valued payments across national boundaries. A TVN could support instant global real-time payments while charging a percentage of the transacted value instead of flat fees.

OTC Markets

The TVN could enable OTC markets for several types of tokens. Tokenized gold and other commodities could easily be traded on this network. Likewise, tokenized real estate and tokenized securities could be traded as well. Using fungible tokens, it is easy to fractionalize assets. One can envision a trader buying 100 tonnes of a tokenized commodity and then immediately selling 1 tonne of it to a willing buyer.

Global Wallets for Banks

Banks with subsidiaries in several countries often attempt to move value among the subsidiaries at a speed faster than SWIFT and traditional correspondent banking. The concept of a multi-currency global wallet is becoming popular. Such wallets support same day or next day value transfers. All multinational banks have the desire to facilitate faster cross-border payments. In a novel pilot, National Australia Bank (NAB) issued a stablecoin on Ethereum and used it to support cross-border payments between subsidiaries. The payments were settled in minutes but the public nature of Ethereum is a concern. Do banks want to expose intrabank flows to their competitors? An intrabank TVN could facilitate instant value movements between various subsidiaries. The same infrastructure could support several types of tokens, including tokenized gold and other commodities. Of course, the intrabank value flows would remain confidential to the subsidiaries involved and their regulators.

Atomic Swaps

Financial transactions are almost never unidirectional. Financial institutions are interested in either (i) Payment-versus-Payment (PvP) transactions which involve swapping one currency for another, or (ii) Delivery-versus-Payment (DvP) transactions which involve swapping securities for currencies, or (iii) Delivery-versus-Delivery (DvD) transactions which involve swapping one security for another. It is important that the two parties involved receive their assets simultaneously. In programmatic blockchains, it is possible to deploy smart contracts that implement the logic for atomic swaps. But as we have discussed extensively in this whitepaper, blockchains are unsuitable for banks because of their public nature. A pair of Token Vaults can exchange both fungible and non-fungible tokens atomically without involving any intermediary or blockchain.

Central Bank Digital Currency

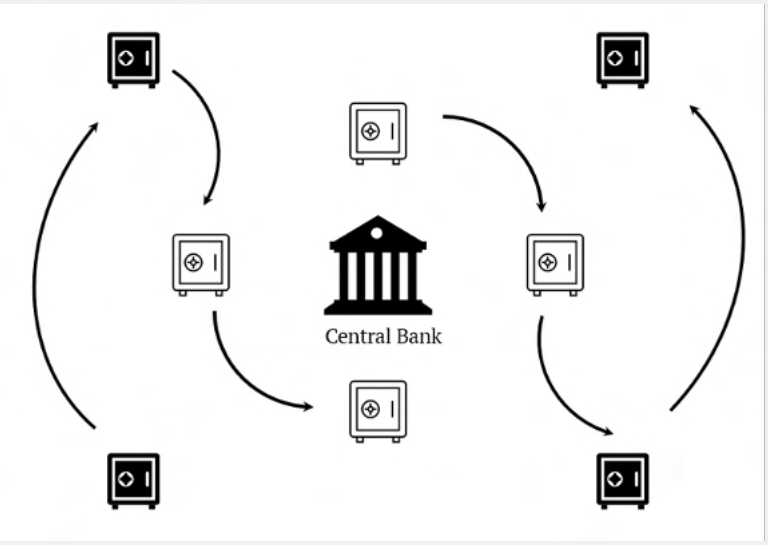
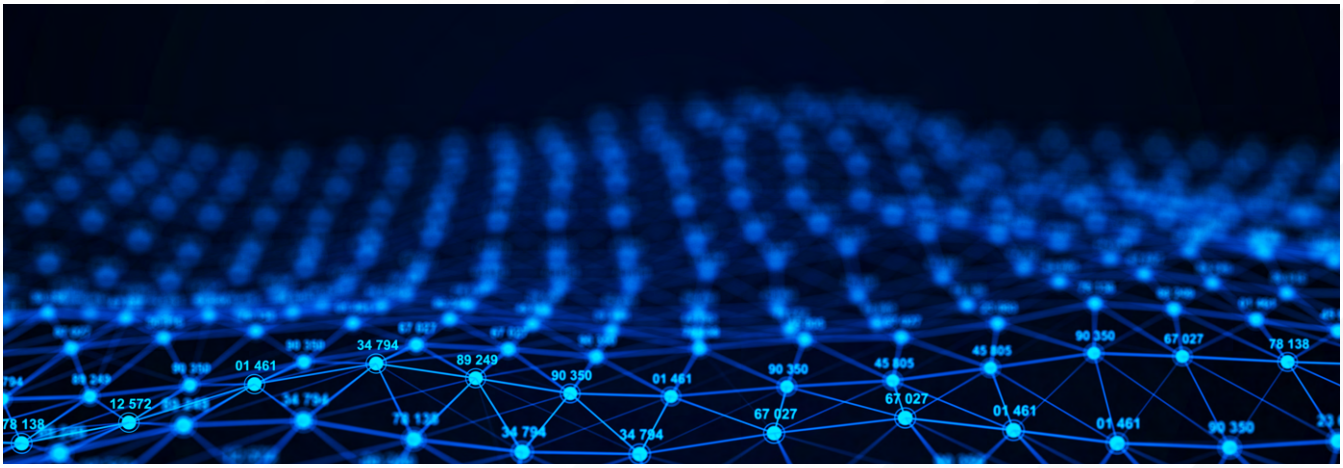
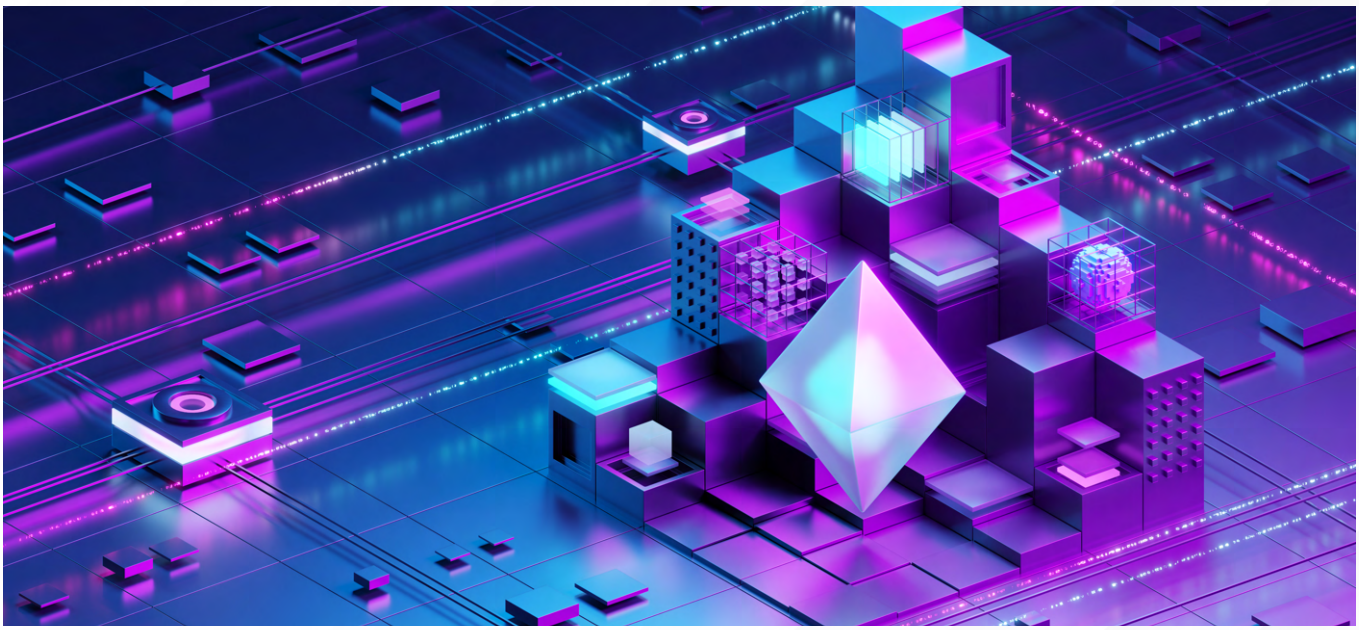


Figure 6: A TVN deployed across various banks to support CBDC.

The main benefit of Central Bank Digital Currency (CBDC) is an instant, risk-free settlement in Central Bank money. Surprisingly, it is hard to find a practical architectural model that delivers instant risk-free settlements for retail CBDC payments. A report from BIS (Auer & Böhme , 2020) proposes three models for CBDC. The Direct Model, where the Central Bank manages all aspects of the CBDC system, including user onboarding is impractical. The Indirect Model and the Hybrid Model only offer deferred settlements. Can another model deliver instant, risk-free settlements with CBDC? As depicted in Figure 6, imagine a TVN deployed across various banks. CBDC could easily flow through this network. Settlements are instant and risk-free. As depicted in Figure 6, imagine a TVN deployed across various banks. CBDC could easily flow through this network. Settlements are instant and risk-free.





Legal Framework

The tokens model will likely require a legal framework to go with it. The legal framework needs to define the rights and obligations of token holders and token issuers. For example, when a token is redeemed, the token issuer must be obligated to transfer the ownership of the underlying asset to the redeemer.

Summary

Every new way of doing electronic value transfer has the potential of very significantly impacting how the world works. Consider the amazing technical work that went into getting the design and implementation of a replicated database right. It unlocked digital banking. Consider the Nakamoto consensus algorithm and the impact that it is having on the world right now. It has unlocked a whole new way of doing electronic value transfers and invited a generation of technologists and enthusiasts to the conversation of what it means to have fast global electronic value transfer systems. Or you may want to consider the impact of secure Integrated Circuits on stored value cards and mobile phones and how they are silently enabling a revolution in one-tap payments.

In this whitepaper, we highlighted how the tokens model is significantly more efficient compared to the accounts model. We also discussed why the prevailing token transfer technology is unsuitable for banks. Given that banks operate in an environment where confidentiality and compliance requirements must be adhered to, a new token transfer technology is required. A Token Vault is a custody solution that implements the primitives of localized double-spend prevention and localized replay attack prevention. Tokens can be transferred in a point-to-point manner within a TVN. The TVN unlocks several use cases, including global real-time payments with stablecoins, OTC markets for tokenized commodities, real estate and securities, asset financing, and CBDC.

References

Auer, R., & Böhme , R. (2020). The technology of retail central bank digital currency. BIS.

Buterin, V. (2014). Ethereum Whitepaper. Retrieved from https://ethereum.org/en/whitepaper/

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review.

Partior. (2023). Retrieved from https://www.partior.com/

Project Ubin. (2016). Retrieved from https://www.mas.gov.sg/schemes-and-initiatives/project-ubin

The Stablecoin Index. (2023). Retrieved from https://stablecoinindex.com/

About the Authors

Pralhad Deshpande earned his Ph.D. in Computer Science from Stony Brook University in 2012. Since then, he has worked with IBM Research as a researcher, launched his own startup, and now drives Fortanix's efforts in the Web3 and digital assets domain. With over 20 patents filed and granted, Pralhad is an accomplished innovator. Pralhad's first book is titled, "Securing Web3 Infrastructure."

Anand Kashyap is the CEO and co-founder at Fortanix. Anand has previously worked at Symantec and VMware as a researcher and an engineer in the areas of security and networking. He has presented at Financial Cryptography and BlackHat conferences and has filed over 25 patents. Anand holds a Ph.D. from Stony Brook University and a Bachelor of Technology from IIT Kanpur, both in Computer Science.

About Fortanix

Fortanix is a Silicon Valley based late-stage startup with Series C financing. It is the leader in Enterprise Grade Confidential Computing. Enterprises worldwide, especially in industries like healthcare, fintech, financial services, government, and retail, trust Fortanix for data security and privacy. Fortanix investors include Goldman Sachs Asset Management, GiantLeap Capital, Foundation Capital, Intel Capital, Neotribe Ventures, and In-Q-Tel.

For more information, visit www.fortanix.com

Glossary of Terms

Bitcoin: The world's first cryptocurrency.

Correspondent Banking: A financial institution that provides services to another one—usually in another country.

DLT: Distributed Ledger Technology. A technology inspired by public blockchains.

DSM: Data Security Manager. An enterprise grade confidential computing platform developed by Fortanix, Inc.

Ethereum: The first blockchain with smart contracts functionality.

FIPS 140-2: The Federal Information Processing Standard Publication 140-2, is a U.S. government computer security standard used to approve cryptographic modules.

Localized double spend prevention: This primitive ensures that the same token is not spent more than once.

Localized replay attack prevention: This primitive ensures that the same token is not receive more than once.

MAS: Monetary Authority of Singapore. The Central Bank of Singapore.

OTC: Over the counter.

PCI-DSS: an information security standard used to handle credit cards from major card brands.

Proof-of-Stake: A voting based consensus algorithm used in several blockchains including Ethereum

Proof-of-Work: The consensus algorithm used in Bitcoin.

Reconciliation: Reconciliation is the process of comparing transactions and resolving any discrepancies that may have been discovered.

SOC 2: A standard which specifies how organizations should manage customer data.

SOC 3: A public report of internal controls over security, availability, processing integrity, and confidentiality.

SWIFT: The Society for Worldwide Interbank Financial Telecommunication. It provides services related to the execution of financial transactions and payments between banks worldwide.

Token Vault Network: A network of token vaults.

Token Vault: A custody solution which implements the primitives of localized double spend prevention and localized replay attack prevention.

Token: A token is a digital bearer asset.