STANDARD KEPLER

RESEARCH

FOUNDATION

Central Bank Digital Currencies

TECHNOLOGY REPORT | 18 MARCH 2019 (V1.00)

1. INTRODUCTION

We have previously identified Central Bank Digital Currencies (CBDC) as one of the more promising potential applications of Distributed Ledger Technology (DLT). As is made evident in Figure 1, a number of CBDC projects have been launched for purposes of evaluating the suitability of blockchain in future payment systems.

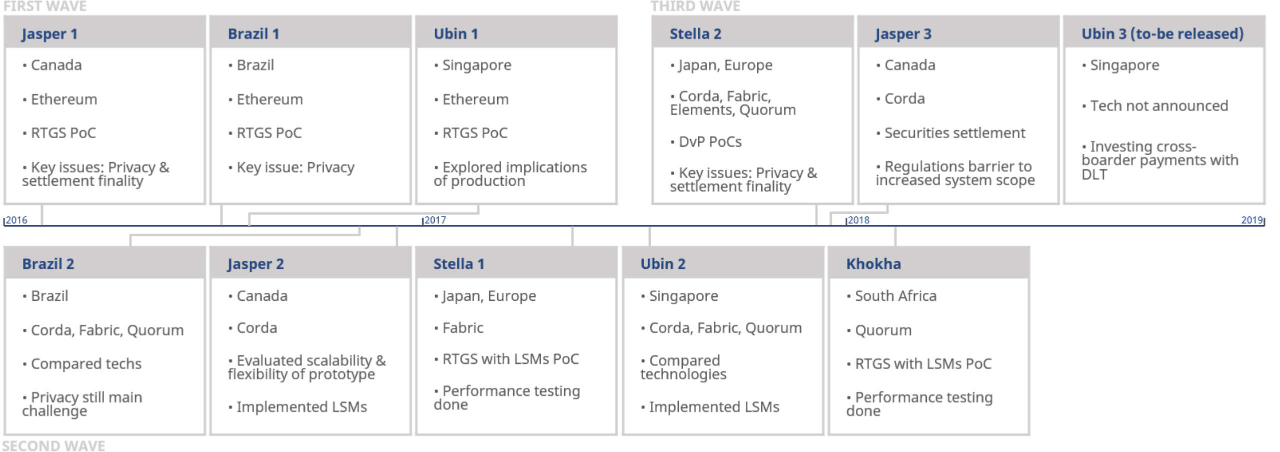
Financial market infrastructures (FMIs) are critically important institutions responsible for providing clearing, settlement and the recording of financial transactions. FMIs are trusted third parties between financial institutions, using centralized ledgers to record and track transactions. FMI operators display significant interest in technology that may increase the efficiency of FMIs, and three key waves of exploratory CBDC DLT projects have been launched to date.

A number of benefits are typically hypothesised for such future payment systems. It is speculated that financial sector back-office costs can be reduced via increased settlement automation. Further advantages are expected with regards to reliability and traceability of information, as well as shorter settlement times. However, CBDC DLT projects to date indicate that the technology is currently lacking the maturity to achieve these improvements.

Tobias Mathiasen
HEAD OF RESEARCH
Tobias@standardkepler.com

Johnny AuYeung
CHIEF TECHNOLOGY OFFICER
Johnny@standardkepler.com

Figure 1: Timeline of Key CBDC DLT Projects to Date



Due to their critical importance to financial stability, FMIs balance a number of significant risks. These include governance and legal risks, credit and liquidity risks, settlement risk, and operational risk. Appropriate transparency and privacy for system participants must also be achieved while maintaining the benefits of DLT technology. This results in a series of trade-offs, significantly so between system privacy, resilience, and scalability. Existing CBDC projects indicate that Corda achieves privacy and scalability at the cost of resilience, Hyperledger Fabric achieves privacy at the cost of resilience and privacy, and Quorum's zero-knowledge proofs achieve privacy at the cost of scalability.

CBDC DLT projects should be studied closely, as they bring us closer to identifying the core value proposition of DLT. We will make efforts to update this foundational report as further developments occur in the space of Central Bank Digital Currencies.

"We are not planning to create a central bank-issued digital currency. But we want to understand better the implications of a central bank issuing a digital currency."

- Bank of England

2. RETAIL PAYMENT SYSTEMS

2.1 WHAT IS MONEY?

The term crypto-currencies implies similarities with established currencies issued by central banks. This in turn leads to the question of whether crypto-currencies should be regarded as money. The world's oldest central bank (the Swedish Riksbank) is keen to stress that "theories of money and how to create a functioning monetary system can be understood on the basis of concrete problems that society has attempted to resolve throughout history". There are different definitions of money in existence, with modern definitions having developed to solve many of the pain-points involved in previous systems of barter exchange.

Metallism ties money to the value of an underlying good. These goods have often been metals, hence the name. A core idea of Metallism is that the limited supply of metals, and the increasing cost of excavating more, act as natural inflation limits. Bitcoin has found inspiration in Metallism, incorporating similar but digital limits to the total Bitcoin supply. Chartalism is another theory for how to define money. According to Chartalism, the value of money is derived from its status as legal tender issued by a national state. Chartalism thus places an indirect responsibility with the state for maintaining a functioning monetary system.

Functionalism, the dominant modern interpretation of money, builds further on Chartalism. According to Functionalism, money must fulfil three criteria of functionality in order to be considered money. Money must function as 1) a means of payment, 2) a unit of account, and 3) a store of value. Means of payment means that money can realistically be used to pay a seller in return for goods, so as to avoid having to repay the seller using goods or services. To function as a means of payment means that money must function as a recognized measurement of value for different goods and services in the economy. Finally, to work as a store of value money should provide price stability, and peoples' decision to spend or not spend money should not be influenced by volatility in the value of money. See Figure 2 on the next page for more details on the expected functionality of modern money.

Central banks are typically responsible for ensuring that money can fulfil these three core functions. An example is found in the inflation targets often set by central banks, with the goal of maintaining the storage of value functionality of money. It is the opinion of several central banks that crypto-currencies should not be considered money, and most crypto-currencies are neither tied to the value of a tradeable good nor are they issued by national states. Crypto-currencies further struggle to fulfil some of the criteria associated to Functionalism, for instance: it must be easy to ascertain the value of money, money must be widely accepted in payments, and money must be durable and exhibit price stability.

"As mentioned above, there are several different theories of money, and crypto-assets probably cannot be classified as money in any of them.

They are not tied to any good with a market value and they are not issued by a national state. With regard to the third theory, what I have called functionalism, the answer depends on to what degree a crypto-asset can fulfil the three functions required.

One main objection that can be raised against crypto-assets, and particularly Bitcoin, is that they are actually not primarily used as a means of payment.

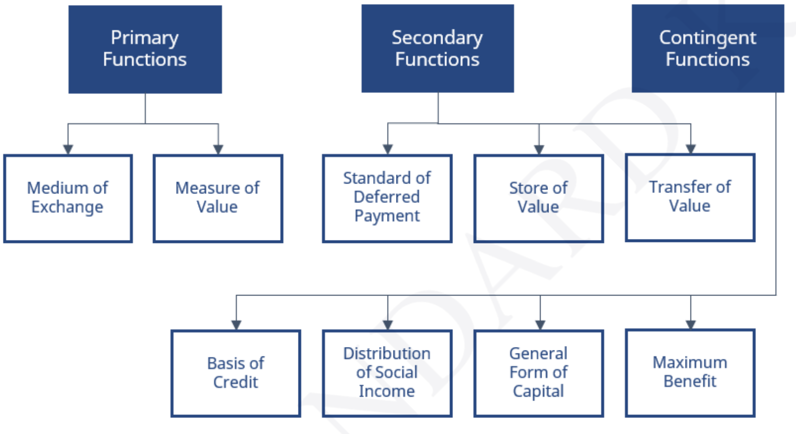
Instead, interest in owning Bitcoins has been linked to their development in value. Most users have thus chosen to use Bitcoin not as money, but as an asset."

- Economic Commentaries, No. 5, The Swedish Central Bank

This is not to say that cryptocurrencies cannot be issued by national states (some have been) or that they cannot be tied to the value of physical goods (some have been). But in order for crypto to see mass adoption as retail payment tools they must fulfil the criteria of Functionalism, and the path towards achieving price stability, sufficient price transparency, and wide recognition of crypto among buyers and sellers is long and difficult. It is made more difficult by the fact that the primary interest in crypto-currencies has been for speculative purposes, not for purposes of conducting transactions. It is further unlikely that central banks would recognize money (crypto-currencies) over which central banks lack the central authority to make monetary decisions (e.g. adjusting supply).

Central Bank Digital Currencies (CBDC), for the purposes of establishing retail payment systems, enter the picture as noteworthy alternatives to the likes of Bitcoin and Bitcoin Cash. Proposed retail CBDCs would not only have the potential to fulfil the criteria of Functionalism, but are also poised to solve some further issues that exist in modern economies, including an over-reliance on private providers and owners of retail payment infrastructure.

Figure 2: Expected Functions of Money

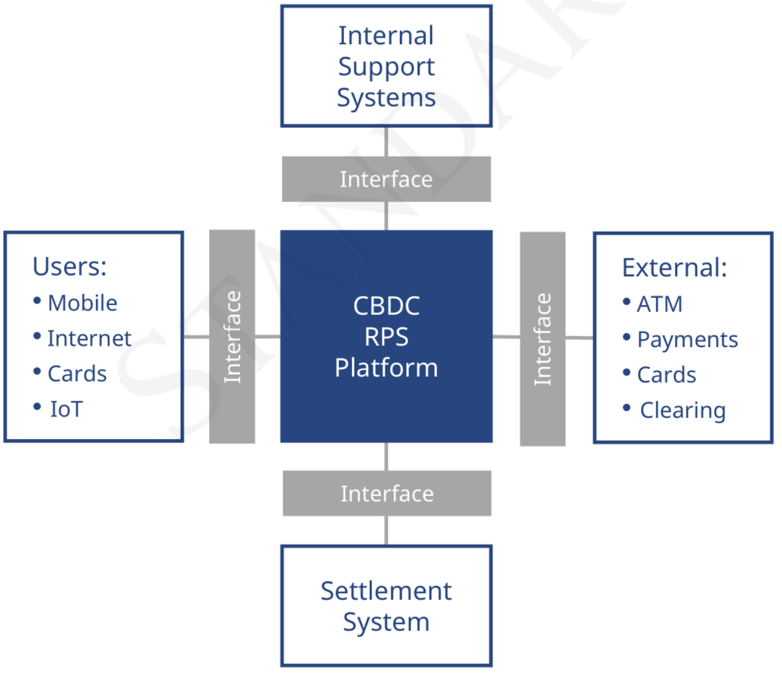


2.2 RETAIL PAYMENT SYSTEMS AND DLT

CBDC driven Retail Payment Systems (RPS) have been proposed as solutions to a number of problems. Some of these problems are related to the costs of using cash, and some are related to a lack of cash. Note that CBDC RPS can be designed without DLT, and DLT is just one possible underlying database infrastructure for such systems.

In scenario A, some countries have considered CBDC RPS as a way to reduce the usage of cash. The goal being to reduce the financial and environmental costs associated with handling cash, as well as the black economies which are facilitated by cash. In scenario B, countries such as Sweden have in recent years seen drastic reductions in cash usage. Cash currently constitutes just over 1% of GDP in Sweden, compared to the European average of 10% of GDP (see Figure 3). Half of Swedish retailers further expect they will stop accepting cash by 2025 at the latest. Central banks fear that such reductions in cash usage and cash supply can lead to difficulties for the public to gain access to central bank risk-free money and increased consolidation in the financial infrastructure among private digital retail payment systems. This in turn could lead to a more inefficient and vulnerable payment market, with decreased trust in the monetary payment system.

Figure 4: Overview of an Example CBDC RPS Platform



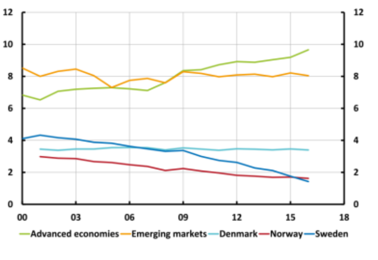
"The Riksbank has a statutory task to promote a safe and efficient payment system, and has for 350 years supplied the general public with money.

Increased digitalisation means, however, that the use of cash is declining. Developments in the field are rapid and within a few years, if the current trend continues, we will find ourselves in a situation where cash is no longer generally accepted as a means of payment.

New technology has brought to a head the matter of the Riksbank's responsibility towards the general public. The Riksbank can either choose not to react to developments on the payments market and pass responsibility for means of payment to the private sector, or choose to continue supplying a means of payment to the general public in a new digital form."

- The Swedish Central Bank (Riksbank)

Figure 3: Cash as Percentage of GDP



Graph Source: The Swedish Central Bank, E-krona project 1

CBDC RPS are conceived as a solution to the above two scenarios. A "digital dollar" platform could allow the public to hold digital dollars issued and guaranteed by the central bank. The platform would interface with users (via internet, card, IoT, etc.), settlement systems, internal support systems, and external systems such as ATM companies and payment service providers (see Figure 4). The costs associated with such digital dollars would likely be small in comparison to the handling costs of physical dollars, and digital dollars could provide central banks with traceability to limit black markets. Digital dollars would also provide the public with a guaranteed RPS that (unlike most existing RPS) is not run by private actors.

There are two primary approaches towards designing a CBDC RPS. It may be account-based (held in an account with the central bank) or value-based (stored in an app or on a card). Both require an underlying register that keeps track of transactions and ownership, meaning that usage is traceable. DLT has been considers as a possible choice, but "from a purely technical point of view, [the Swedish Central Bank] can see nothing at this point in time that would prevent an e-krona solution built around a central register."

Expect CBDC RPS to attract more attention in the future, although primarily in niche markets where cash usage is low (most countries still see significant cash usage, a notable example being the USA), or where there are significant black markets in existence. There are still important decisions to make in the design of an RPS: Should the digital dollar carry interest? Should it be account- or value-based? A digital dollar could make bank runs easier. Is such ease desirable or not? Strong demand for digital dollars (especially interest-bearing dollars) could also drain commercial banks, leading to a reduced ability to issue credit. These decisions would result in a new set of potential risks to the financial system that have to be carefully evaluated. For now, a value-based non-interest bearing dollar seems to be the most likely proof-of-concept candidate. To quote a Deutsche Bank report from 2018, "a compelling reason for consumers to switch voluntarily to crypto euros is hard to see – at least for the time being."

Figure 5: Comparison of Value- and Account-based CBDC RPS

Possible Properties	Value-based	Account-based
Instant payments	Yes	Yes
Underlying register	Yes	Yes
Legal form	E-money (prepaid value)	Deposit (account balance)
Interest	No, not as a rule	Yes
Anonymous payments	Yes (below EUR 250)	No
Traceability	Yes (but not if, for instance, a prepaid card changes owner person-to-person)	Yes
Offline Payments	Yes	Yes

"In the areas of payments and savings, digital cash would compete against bank deposits, physical cash and private cryptocurrencies to win over consumers.

Unless its use was strongly pushed by regulation, digital cash would need to convince users by offering better and more convenient payment solutions than other payment systems. In particular, it would need to match current low fee levels and high safety standards for regulated consumer payments.

In an environment of high trust in public institutions, consumers would probably not be concerned if digital cash offered little data privacy."

- Deutsche Bank Research

3. WHOLESALE PAYMENT SYSTEMS

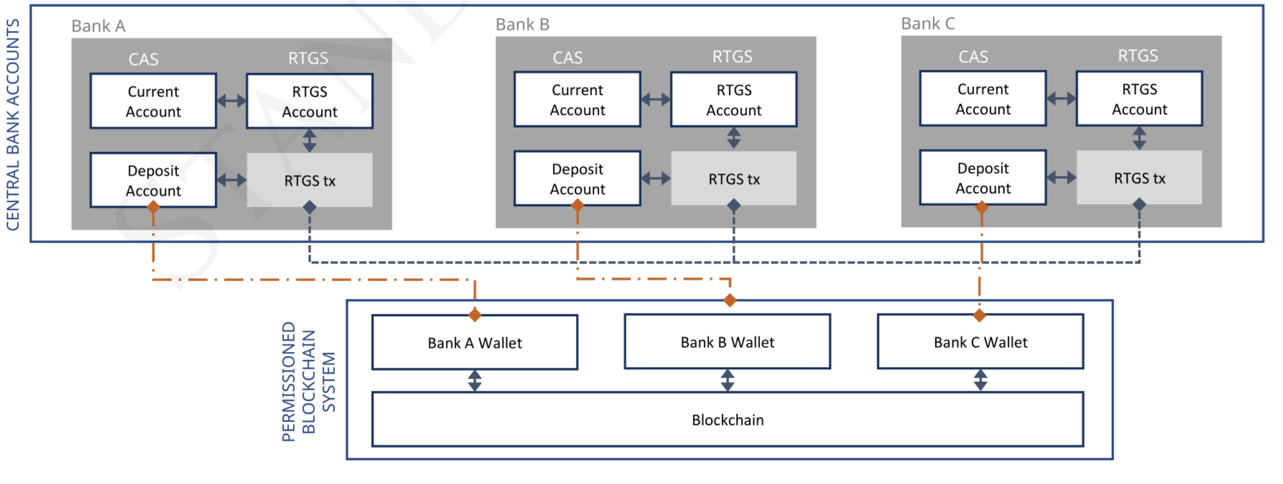
3.1 WHOLESALE PAYMENT SYSTEMS AND DLT

CBDC Wholesale Payment Systems (WPS) have seen wider and more rapid prototyping than CBDC Retail Payment Systems (RTS). This likely due to the more significant cost savings that may be possible via CBDC WPS. Furthermore, the interests of private financial institutions and central banks are generally aligned in the development of CBDC WPS, while CBDC RTS are viewed as possible competitors to existing RTS operated by private financial institutions.

A wholesale payment system "deals with inter-bank, inter-country large value, large volume real-time payments and related clearing and settlement systems governed by central banks integrating various globally accepted standards." A CBDC WPS considers how digital currencies can be utilized to improve the efficiency of WPS. A simplified example implementation of a WPS is proposed in Project Ubin, and is outlined in Figure 6

In this proposed system, banks hold a special deposit account with the central bank. A bank can deposit funds into this deposit account from the bank's RTGS account. The balance of this deposit is mirrored in a digital currency wallet on the permissioned blockchain system. Moving funds into the deposit account thus creates digital currency (in this case Deposit Receipts) in the wallet, and withdrawals from the Deposit Account burns Deposit Receipts in the wallet. Banks, with Deposit Accounts, can then transfer Deposits Receipts between bank wallets on the blockchain.

Figure 6: Example CBDC WPS as Proposed by Project Ubin



Such a system can be designed around DLT, and the specifics of the system depends on the digital ledger technology chosen. The options most commonly considered are R3's Corda, Hyperledger's Fabric, and JP Morgan's Quorum, which are introduced in 3.2, 3.3, and 3.4.

Several WPS proof-of-concepts have been developed to date. The concepts tested in these projects using these systems have generally proven that DLT is able to execute transactions at a rate matching existing RTGS volumes and with finality, albeit often at the cost of limited privacy or system resilience. Further development would be needed to achieve more efficient trade-offs between these aspects. One must also note that a full-fledged CBDC WPS ought to include liquidity management and credit extension functionality. Concepts for both of these functions exist, but are considered beyond the scope of this introduction on the CBDC topic.

As more actors in financial markets consider introducing DLT based systems, the complexity of interoperability and the potential for new business models both increase.

"As such, a single payment message or file transfer between direct participants in a central clearing and settlement arrangement has the potential to be captured in the internal record-keeping systems of multiple financial institutions.

Given the sheer volume of activity that flows through these systems — e.g., amounting to tens of thousands of payment messages and batch-file entries per day in Canada — erroneous and duplicate entries can and do occur, sometimes escalating into costly disputes between participating financial institutions.

Such errors and disputes typically require manual or semi-automat- ed resolution by the affected institutions."

- Project Jasper

3.2 R3'S CORDA

Corda argues that the essence of blockchain is "ensuring that data held by different actors is, and remains, consistent as operations are applied to update that data, and that this forms the foundation on which reliable transactions are built." This view allows Corda to pursue the advantages of DLT without utilizing a blockchain.

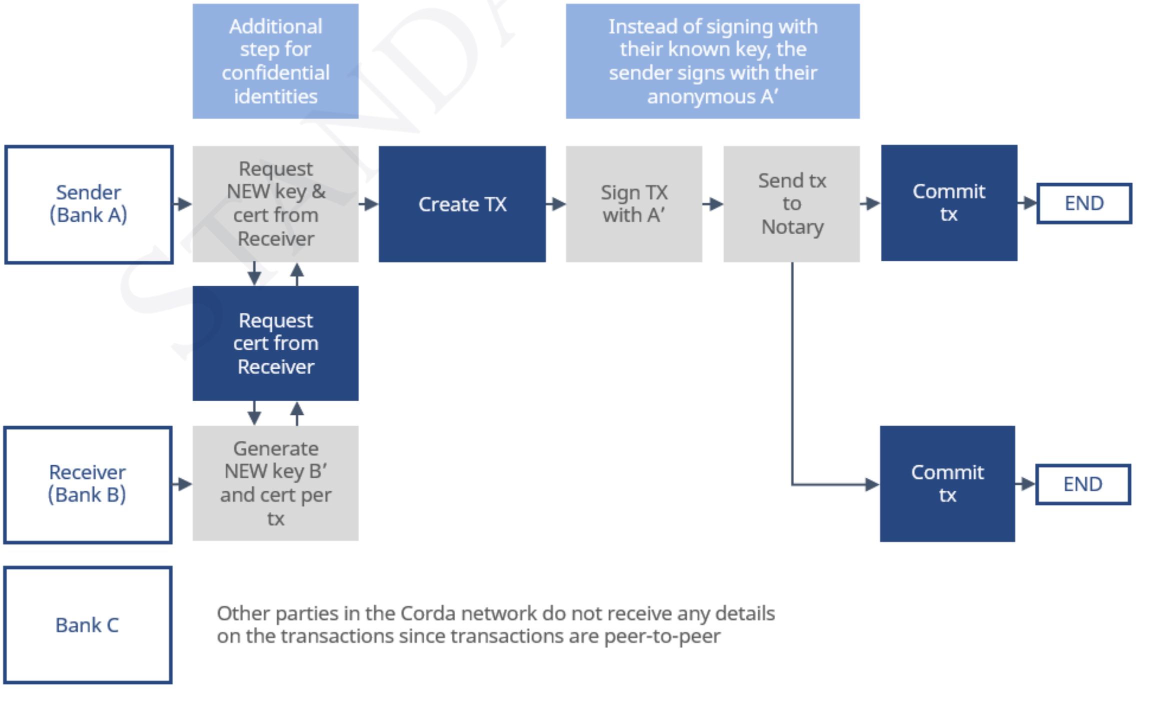
"[Corda] is heavily inspired by blockchain systems, but without the design choices that make traditional blockchains inappropriate for many financial transactions." Corda defines its ledger as a set of immutable state objects. This ledger acts as a reliable single source for the Corda platform, yet it does not make transactions nor entries on this ledger globally visible. Cryptographic hashes are instead utilized to identify parties and data and ensure that only parties that are part of a agreement can see relevant ledger details.

Corda seeks to achieve consensus among parties of an agreement on the state of that specific agreement as it evolves. This "per agreement" approach is in contrast to systems (e.g. Bitcoin) that seek to achieve consensus on the state of an entire ledger. Updates to the Corda ledger are applied using txs that consume existing state objects and create new state objects (there is no native cryptocurrency involved). The validity of a transaction can be checked independently by parties by running the contract code. However, a predetermined observer node is required to reach consensus over uniqueness. Importantly, this observer node only checks consumed input states, and does not need to see the full content of a transaction. There is no concept of mining in Corda.

"Banks were amongst the earliest adopters of information tech and, contrary to popular belief, they have done a good job in automating previously manual processes and in digitizing previously physical processes. However, there are significant opportunities to improve the cost and efficiency of the architectures that emerged."

- R3 Corda

Figure 7: Transaction Flow of Fund Transfers in R3 Corda



On Corda, state objects represent an agreement between parties. This agreement is governed by contract code that is linked to legal prose. Transactions in turn transition state objects through a lifecycle, and transaction protocols enable parties to coordinate actions without a central controller. Combined, these components are referred to as CorDapps, and need to be built by developers on the platform.

Corda is a timely reminder that a blockchain is only a way to implement a distributed ledger, but not all distributed ledgers necessarily employ blockchains. Hyperledger Fabric and Quorum are two other ways of building distributed ledgers. CBDC Project Ubin 2 interestingly compares all three, a comparison we will return to.

3.3 HYPERLEDGER'S FABRIC

Hyperledger Fabric is part of the Hyperledger family of projects hosted by the Linux Foundation. These projects have all been designed to be modular, with the intention of offering greater flexibility to customers and developers alike. In theory, this allows developers to experiment with different components without affecting the rest of the system, allowing for a Lego-like approach to building solutions for diverse problems from a fixed set of components. Fabric further runs distributed applications written in general-purpose programming languages, without depending on a native cryptocurrency.

The concept of channels is also at the core of Fabric. The system is built on a network of bilateral channels between participants, with each bilateral channel forming one ledger. By establishing such channels, data privacy can be maintained within the channel and away from other system participants. A third party, such as a monetary authority, can be included in the channel for purposes of transaction recording and monitoring. Multilateral channels can also be created, such as in the case of Singaporean project Ubin, where participating banks are linked by multilateral funding and netting channels. Such a funding channel allows participants to move funds between their individual channel-level accounts. Note that the number of bilateral channels, and thus system complexity, grows with each new system participant.

"Once you start sharing a database with others, many questions arise:

• Who do you trust to share your data?

• How can you tell that someone is who they say they are online?

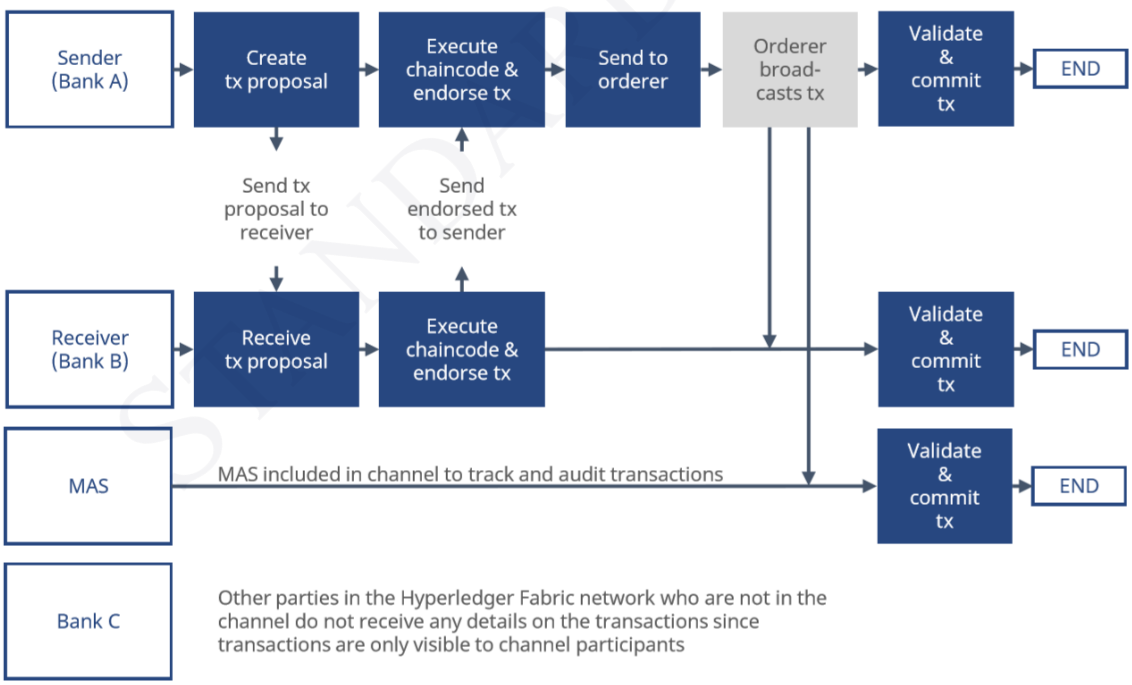
• What are they allowed to do to the database?

• What happens if both head office and the sales rep want to sell the same items?

• Who settles any conflicts or disputes?"

- Hyperledger Fabric

Figure 8: Transaction Flow of Fund Transfers in Hyperledger Fabric



Any blockchain that sees usage within financial market infrastructure must provide immediate finality, rendering consensus algorithms such as proof of work and proof of stake unviable. Fabric prevents double spending attacks via a system endorsements and an orderer. Participating nodes validate a transaction against the system endorsement policy (defined by the chaincode) to ensure the validity of the transaction and its signatures (see Figure 8). An orderer packages endorsed transactions into blocks, and broadcasts these blocks to the channel participants. These subsequently validate the transactions before they are committed to the ledger. It is also possible to include a consensus mechanism that allows for a multiple node ordering service.

Several proof of concept Central Bank Digital Currency (CBDC) systems have been built on Hyperledger Fabric, most notably so Singaporean Ubin 2 and Japanese-European Stella 1 & 2.

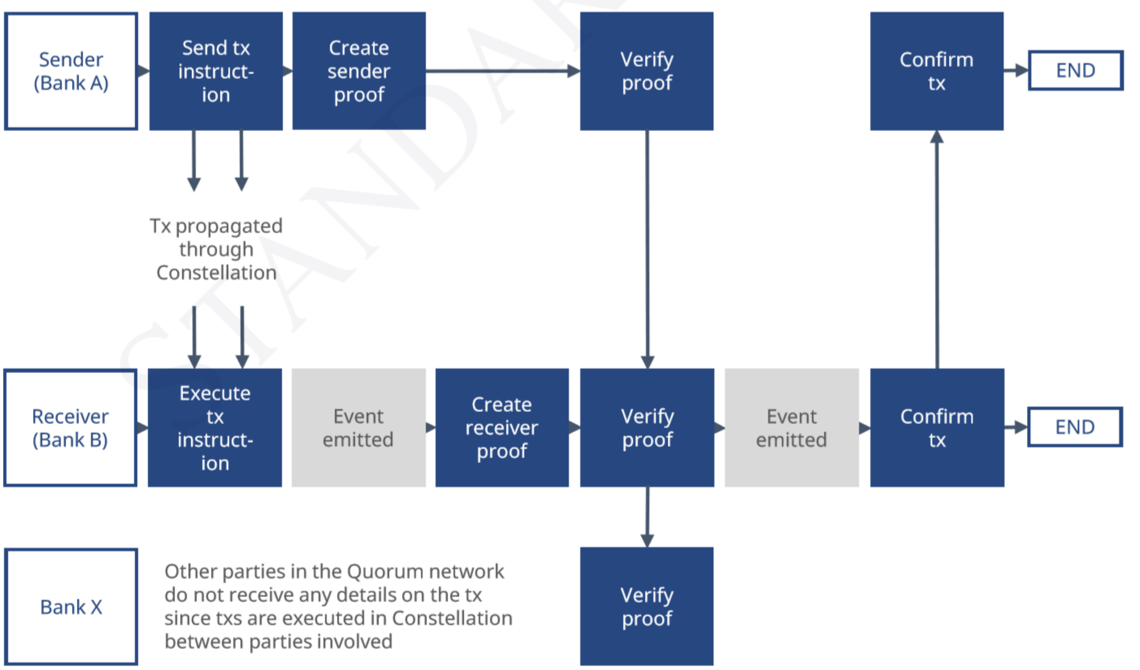
3.4 JP MORGAN'S QUORUM

Achieving appropriate levels of privacy is a core requirement in enterprise blockchain. How a blockchain achieves this is a question with many possible answers, ranging from the relative simplicity of bilateral channels to the use of data heavy zero knowledge proof transactions. JP Morgan's Quorum sets out to build on the work already done by Ethereum, and to turn Ethereum into an "enterprise-ready distributed ledger and smart contract platform".

All nodes in a Quorum network run the same set of components. However, these components differ somewhat from Ethereum. Foremost is the introduction of private state trees. The Quorum blockchain (just like Ethereum) saves information in the form of states, and transactions modify states on the blockchain. Quorum nodes have a public and individual private state trees, with the public state tree storing vanilla Ethereum transactions and hashes of encrypted private smart contract changes.

A Zero Knowledge Security Layer (ZSL) developed by the team behind Zcash is another core component of Quorum. ZSL enables the transfer of assets on the network without revealing the sender, receiver, nor the quantity of the asset. Hashed values of the initial balance, transaction amount, and final balance are submitted by the sender and receiver to a proof generator off-chain. They are subsequently submitted to the Quorum chain for verification by other nodes on the network, following which the transaction is confirmed and balances are updated.

Figure 9: Transaction Flow of Fund Transfers in JP Morgan's Quorum



Quorum thus requires both private and public smart contract transactions. The private contracts enable private transactions between two parties, while public transactions are used to distribute ZSL proofs for verification on the Quorum network. The transaction flow under Quorum is visualized in Figure 9, and narrated most succinctly by the Ubin Phase 2 whitepaper itself: “A payment instruction for fund transfer is initiated from the sender’s dApp. The dApp invokes the private contract to generate a private transaction. The sender’s dApp then invokes a public transaction which will be executed by all nodes on the Quorum network. The public transaction is created with the hash of payment instruction amounts which will be used as inputs to generate and verify proofs. Hashing is done to maintain data privacy since public transactions are propagated to all nodes in the network.”

Transaction finality is another characteristic that is of crucial importance in enterprise settings. Financial institutions are typically unable to handle probabilistic finality, and the probabilistic nature of finality under Ethereum’s Proof-of-Work is thus unsuitable for enterprise applications. Quorum introduces alternative ways of achieving consensus, the one having been evaluated by Singapore’s Monetary Authority for wholesale settlement purposes being “Raft”. Raft has been used for many years in software such as Kubernetes. It relies on the concept of a single leader, who proposes blocks that others validate. This means there is no forking, and as such there is transaction finality. Raft also enables the setting of block times that are significantly faster than is possible under Ethereum.

Having thus far introduced R3’s Corda, Hyperledger’s Fabric, and JP Morgan’s Quorum, we will next briefly compare all three according to their suitability in supporting wholesale payment systems.

3.4 COMPARING CORDA, FABRIC, AND QUORUM

Several CBDC proof-of-concept and prototype projects have been conducted to date (see part 1). These projects have generally been spearheaded by a central bank, yet in collaboration with financial institutions (who use existing financial market infrastructure) and developers of enterprise level Distributed Ledger Technology. The following is a brief comparison between the three most prominent contenders (Corda, Fabric, Quorum), largely based on the findings of previous CBDC projects.

Privacy: Corda only seeks to achieve consensus among parties of an agreement on the state of that specific agreement as it evolves, as opposed to seeking agreement on the state of a globally distributed ledger. Hyperledger Fabric offers the ability to set up shared channels (each one a ledger) between parties, with transaction within the channel being private to outside parties. It is worth noting that channel-level account balances can be viewed by channel participants. Regulators (e.g. a central bank) can be included in channels for compliance purposes. Quorum achieves privacy via public and individual private state trees, with the public state tree storing vanilla Ethereum transactions and hashes of encrypted private smart contract changes. Quorum thus offers and requires both private and public smart contract transactions. The private contracts enable private transactions between two parties, while public transactions are used to distribute zero knowledge proofs for verification on the Quorum network.

Scalability & Performance: Due to its design, Corda is not a proper blockchain. This not only alleviates privacy concerns, but also makes scaling significantly easier compared to traditional DLTs. The addition of a new participant only requires the installation of a new node to the existing network. In Fabric, [N x (N-1) / 2] + M channels are required to operate, with N = number of participating nodes, and M = number of multilateral channels. The network complexity rises with each new participant, and participants need to maintain and move funds between individual channel-level accounts for each channel. Quorum’s vastly improves upon the performance of Ethereum by virtue of being a permissioned network, yet there is further room for improvement with regards to the speed of running zero knowledge proofs.

Resiliency: While Corda can continue to operate should individual bank nodes go offline, the use of a single notary node (e.g. central bank) to achieve consensus over uniqueness is a potential point of weakness. This can be rectified with a notary node operated by multiple parties, although at the expense of added complexity. Fabric involves a blockchain, but an orderer is required to order transactions into blocks. The Ubin 2 prototype is built on a single orderer, which introduces a single point of failure. A multi-node ordering service could solve this issue. Propagating hashes of private transactions to the global ledger improves resilience in Quorum. This use of a central ledger ensures significant resilience, and under the tested Raft consensus method the consensus leader could be rotated with each transaction for added resilience. This may or may not be possible in the usage scenario of CBDC, and the consensus leader could thus constitute a point of weakness.

Finality: Of crucial importance to financial service providers. The use of a notary node ensures certain transaction finality in Corda, with a notary signature indicating that input states are thus far unspent. Fabric's ordered node orders a transaction into a block, and sends it out to channel participants for commitment to the shared channel ledger. The transaction is finalized upon commitment. The Raft consensus method tried alongside Quorum relies on a consensus leader to commit blocks to the chain after verification. Once a block has been committed, the chain cannot be reversed since there is no concept of mining involved, and finality is thus achieved.

Figure 10: A Brief Summary of Corda, Fabric, and Quorum

Aspect	Corda	Fabric	Quorum
Privacy	Consensus only on individual agreements, Not on whole ledger	Channels as data partitioning mechanism	Private state trees and zero knowledge proofs
Scalability & Performance	Not a proper blockchain, thus easier to scale	Number of channels required increases with each new participant	Vastly superior to Ethereum, but zero knowledge proofs possible bottleneck
Resiliency	Use of a single notary node (e.g. central bank) can be point of weakness	Use of single ordering node is possible point of weakness	Strength of a global distributed blockchain, yet Raft leader possible point of weakness
Finality	Achieved via notary node	Finality achieved within channels	Finality achieved by Raft consensus leader
Notable Prototypes	Jasper 2, Jasper 3, Ubin 2, Stella 2	Stella 1, Stella 2, Ubin 2	Ubin 2, Khokha, Stella 2, JPMorgan Coin

4. REFERENCES

Bank of Canada; Payments Canada; R3. 2017. *Project Jasper: Outline.*

Bank of Canada; Payments Canada; R3. 2017. *Project Jasper: A Canadian Experiment with DLT for Domestic Interbank Payments Settlement.*

Bank of Canada. 2018. *Project Jasper: Are distributed wholesale payment systems feasible yet?*

Bank of Canada; TMX Group; Payments Canada; Accenture; R3. 2018. *Jasper Phase 3: Securities settlement using DLT.*

Corda. 2018. *The Corda Platform: An Introduction.*

Deutsche Bank Research. 2018. *Why would we use crypto euros?*

European Central Bank. 2018. *Stella: BOJ/ECB joint research project on DLT.*

Hyperledger. 2018. *An Introduction to Hyperledger.*

JP Morgan. *Quorum Whitepaper.*

Monetary Authority of Singapore; Deloitte; Bank of America Merrill Lynch; BCS Information Systems; Credit Suisse; DBS Bank; HSBC; J.P Morgan; Mitsubishi UFJ Financial Group; OCBC Bank; R3; Singapore Exchange; UOB Bank. 2017. *Project Ubin; SGD on Distributed Ledger.*

Monetary Authority of Singapore; The Association of Banks in Singapore; Monetary Authority of Singapore. 2017. *Project Ubin Phase 2.*

Monetary Authority of Singapore; SGX; Anquan Capital; Deloitte; Nasdaq. 2018. *Project Ubin: Delivery versus Payment on DLT.*

South African Reserve Bank. 2018. *Project Khokha: Exploring the use of DLT for interbank payments settlement in South Africa.*

Sveriges Riksbank (Swedish Central Bank). 2017. *The Riksbank's e-krona project report 1.*

Sveriges Riksbank (Swedish Central Bank). 2018. *The Riksbank's e-krona project report 2.*

Sveriges Riksbank (Swedish Central Bank). 2018. *Economic commentaries: Are Bitcoin and other crypto-assets money?*

And more.