otc*Digital

Central Bank Digital Currency

Towards A Composable Standards-Based Implementation

Vipin Bharathan
Mani Pillai

November 2020

Abstract

otcDigital introduces a unique standards-based approach to the implementation of a Central Bank Digital Currency (CBDC) in this paper.

The paper starts with a brief background of the work done by otcDigital on a suite of products targeting a digital marketplace to demonstrate competence and familiarity with the solution space.

The paper explores the purposes of central banks and links these purposes to the rationale for CBDC and subsequent requirements. The sources are public statements, speeches, papers from central banks, expert commentaries, publications from advocacy groups, and conversations with central bankers and other experts. No specific central bank is in focus.

The proposed solutions reference several standards, the Token Taxonomy Framework (TTF) for tokens, and the International Swaps and Derivatives Association (ISDA) Common Domain Model (CDM) for contracts.

The proposal's basic pattern is a contract network linked to a token network, bridging the gap between business contracts and the corresponding exchange of value. This pattern, along with some other standards-based components in different configurations, can help realize different CBDC scenarios.

Parts of these components have already been created under open source in Hyperledger Labs through the Hyperledger Capital Markets Special Interest Group (CMSIG). Some other components are implemented as extensions of a commercial product. From these building blocks, different CBDC use cases are constructed. This dual network can be implemented in platforms other than DLTs. When specific DLTs are used, they are for illustration or implementation.

The solution is meant to be transferable to alternate platforms with similar properties. These concepts were refined by building working software and demonstrating the functions to several central bankers and software service providers. Lastly, the paper summarizes unanswered questions and extensions necessary for production deployments.

Introduction

otcDigital

otcDigital and its affiliates created and continue to maintain an institutional OTC trading platform that covers cash equities to OTC (Over-The-Counter) derivatives for over 15 years. otcDigital put this commercial offering into production at major investment banks and financial services firms. The product is continuously hardened over years of use in critical financial infrastructure and over many asset cycles.

Over the past 3 years, otcDigital has incorporated various digital technologies — DLTs, blockchains, and multi-party computation (MPC) — to bring privacy, confidentiality and security to a regulated digital asset marketplace, extending and upgrading its original offering. otcDigital is also building the core infrastructure and platform with digital standards including the Common Domain Model (CDM) and Token Taxonomy Framework (TTF) to address digital assets covering CBDC, Stablecoins, Security Token Offerings (STO), and more. Integration with parts of the traditional asset trading platform also continues, offering an amalgam of the enterprise-focused infrastructure with digital asset cash, derivatives trading, and clearing and settlement. Next-generation security is integrated into core functions in the form of MPC. It is in this process, the Company identified the need for a CBDC and have been exploring implementing the same technologies, standards and frameworks for CBDC. otcDigital is a member of ISDA CDM Working Group, Hyperledger Capital Markets Special Interest Group, Wall Street Blockchain Alliance (WSBA), and Digital Currency Global Initiative (DCGI).

The Rest Of The Paper

The first section explores the concept of central bank digital currency. From the purposes and functions of a central bank, the rationale for a CBDC is developed. The paper then highlights broad scenarios in which central banks and general payment systems operate. These payment systems are wholesale CBDCs, retail CBDCs, and cross border systems. This paper also discusses models proposed, suggested, or built by researchers. Readers who are familiar with CBDC concepts may skip to the section titled, “CBDC Implementation.”

The CBDC implementation section describes the proposed implementation. It starts with a description of the specific standards used in the implementation. A dual network is proffered as

the basic building block. This building block, along with other components, is used to construct implementation architectures for three scenarios. These scenarios are a wholesale CBDC, a retail CBDC, and cross border applications of both. Lastly, the paper addresses challenges and themes connected to production deployment and operation of CBDC.

Central Bank Money

Why Central Banks?

The primary role of a central bank is to ensure the effective operation of a nation's economy in the public interest. Central banks do this by creating stability in the money supply to promote maximum employment, regulating banks individually as well as on a systemic level, and fostering payment and settlement system safety. Most central banks are sheltered from political interference so that they can take independent action to fulfill their mission.[1]

The three functions of money: a unit of account or numeraire, a store of value, and a medium of exchange; can be best supported by a stable currency sheltered from volatility. These features are in the service of current or future payments. The tension between two of the functions, money as a store of value and a medium of exchange, is controlled through monetary policy.

This paper takes the necessity of central banks for granted. Evolution over many years has brought us to the current system. A monetary system controlled by a monetary authority is better than exclusive private money systems that existed before. The creation of a CBDC provides the central bank with more tools to stabilize the economy for the good of its citizens.

Money Supply

The money supply in any modern economy consists of narrow money and broad money. Narrow money is referred to as base money, or M0. Narrow money is money in reserve accounts at the central government plus vault cash and cash in circulation. Narrow money is the safest form of money, since it is the liability of a central bank. Reserve accounts are digital, cash is not. In a rapidly digitizing world, cash is being used less frequently. The global pandemic has not helped the case for cash.[2]

Broad money is available widely, consisting of money in commercial bank accounts plus cash in circulation. Circulating cash is part of both M0 and M1. Broad money is where the majority of money supply of any country is created and held through loans from commercial banks and

[1] "The Fed - What does it mean that the Federal Reserve is "independent within the government"" 1 Mar. 2017, https://www.federalreserve.gov/faqs/about_12799.htm. Accessed 29 Aug. 2020.

[2] "Covid-19, cash, and the future of payments - BIS Bulletin" 3 Apr. 2020, https://www.bis.org/publ/bisbull03.pdf. Accessed 28 Aug. 2020.

deposits from the account holders. These components are digital as well. The proportion of broad money to narrow money is about 4:1 or 5:1, even during the pandemic. This ratio applies when circulating cash is only counted in narrow money.

Broad money may be divided into various groups based on maturity. These groups include money that is immediately callable by the depositors, in demand deposits, and money that is locked up in longer term deposits and loans. The main function of banks is to serve as maturity transformation machines, taking in short duration deposits and giving out longer duration loans. This maturity difference introduces the possibility of bank runs through withdrawal from demand deposits or shorter term accounts. The protection to commercial bank money for reasonable amounts is extended using deposit insurance. This makes a proportion of broad money behave like narrow money. Insurance schemes suppress and even eliminate the incidence of bank runs.

When the economy goes through a crisis, liquidity dries up in the market as banks refuse to lend and create money. Central banks step in as Lenders Of Last Resort (LOLR) to inject liquidity into the market during times of crisis. They also provide additional liquidity by cutting reserve requirements. These actions stabilize the money supply and hence the economy.

The major function of money is to enable payments. Smooth and resilient payment systems are necessary for economic stability. If the payor and the payee are individuals and enterprises with no central bank accounts, the only medium they can directly rely on for safe payment is cash. As cash is a way to transfer a direct claim to the central bank. Otherwise, entities have to use payment service providers whose rails terminate in banks with reserve accounts.

Banks with reserve accounts use a Real Time Gross Settlement Service (RTGS) usually run by a central bank. RTGS results in finality with no-recourse settlement using reserve accounts. This is very similar to the finality attained with cash for retail payments. Although they are achieved using fundamentally different mechanisms, the use of narrow money, the safest form of money, is their distinguishing feature.

Rationale for CBDC

There are many digital forms of money available to the public today for store of value and for payments, including regular bank deposits accessed through banking apps or debit cards. Another form includes credit cards or closed systems such as AliPay, WhatsAppPay, and Paypal. Big banks, financial markets utilities, and others who have accounts at the central bank have

access to their reserves, which are also digital. Why do we need one more form of digital money? Researchers have answered this question comprehensively.[3][4][5] Some prominent reasons are listed below.

One purpose of a CBDC is to provide **a method of rapid digital payment with central bank money**, fitting modern methods of commerce, which is increasingly online. There is no comparable form of digital money available to the public.

Network effects increase the value of the network exponentially for existing participants with increased adoption. Network effects have resulted in consolidation of payment networks by creating a barrier to entry for newer entrants, even those with better technology. The resulting consolidation of payment networks creates monopoly power, which means higher cost per transaction especially for smaller merchants. The concentration of the payment function in a few enterprises increases systemic risk. CBDC can provide an alternate retail or wholesale payment system. This is independent of any private system whose failure could impact citizens. **A CBDC run by a central bank provides a public payment alternative** in times of stress and crisis as well as provides competition to curb monopolies.

The migration of most of the citizens to private money, including stablecoins or other forms of money, may cause the central bank to lose control of monetary policy. **The provision of CBDC by the central bank allows transmission of monetary policy through one more channel**. The central bank can break through the zero lower bound of cash to stimulate the economy. The central bank can curb inflation through positive interest rates.

Commerce has grown due to the globalization of supply chains. Remittances from abroad keep many economies afloat. These are some of the reasons for growth in cross border payments. Cross border payments include wholesale, large value payments, and smaller retail payments. Cross border payments today use a system of correspondent banks and many messages, leading to delays and costs. **Cross border payments can be simplified using CBDC**.

CBDC is meant to exist alongside all other forms of fiat for the short to medium term. Payments using CBDC will exist alongside all other existing payment rails. Innovation in CBDC and

---

[3] "Comparing Means of Payment: What Role for a Central Bank ...." 13 Aug. 2020, https://www.federalreserve.gov/econres/notes/feds-notes/comparing-means-of-payment-what-role-for-a-central-bank-digital-currency-20200813.htm. Accessed 30 Aug. 2020.

[4] "Economic Review 2, 2020 - Riksbanken." Accessed August 28, 2020. https://www.riksbank.se/globalassets/media/rapporter/pov/engelska/2020/economic-review-2-2020.pdf.

[5] "Tiered CBDC and the financial system - European Central Bank." Accessed August 28, 2020. https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf.

payment systems will happen if the right technology is chosen. Dynamic interest rate setting and other smart features require programmable money.

Types Of CBDC & Their Desired Features

Figure 1 depicts three intersecting sets. The three sets are central bank issued, digital, and widely available. Central bank issued currencies, the most stable and safe digital currencies, are addressed in this paper. As seen in the diagram, the two types of CBDC are wholesale CBDCs available only to reserve account holders and retail CBDCs that are available to all.

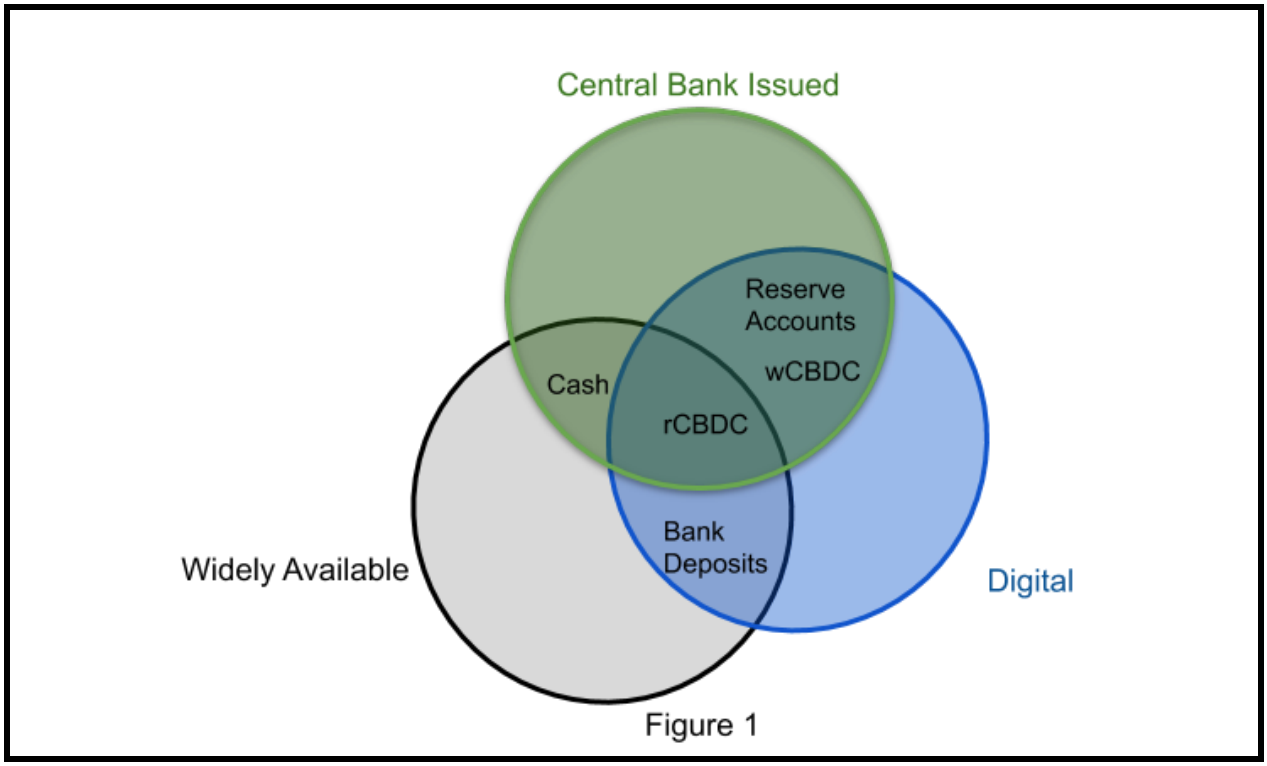

Figure 1

Wholesale CBDC (wCBDC)

Wholesale CBDC serves wholesale transactions. Wholesale transactions are high-value transactions conducted between banks, large financial institutions, and large corporations. Annual global figures for inter-bank wholesale transaction flow is $5000 trillion in 2 billion transactions. The average transaction amount is $2.5 million. Annual commercial wholesale

transactions are another $650 trillion through 250 billion transactions. In contrast, retail annual transaction flow is about $35 trillion a year in 2 trillion transactions.[6]

Wholesale transactions flow through Real Time Gross Settlement Systems (RTGS), which are normally operated by the central banks against the reserve accounts of banks. Wholesale CBDCs issued by the central bank can circulate among big banks, allowing instant clearing to happen without direct central bank involvement or a round trip to the central bank reserves. This creates a more decentralized peer-to-peer ecosystem among banks and institutions with central bank reserve accounts. Since central banks already service these accounts, no new setup is needed. Recent RTGS modernisation programs plan to expand this circle to include payment service providers and larger fintechs.

For their monetary policy operations, central banks engage in many activities. One of the most important ones is to act as the LOLR through the provision of intra-day liquidity to back up Liquidity Saving Mechanisms (LSM) through continuous or even intra-day RTGS. Central banks act to provide short term financing in the Repo market. Central banks provide a backstop for sliding asset prices through special programs for asset purchases ranging from sovereign debt and mortgages to corporate debts. Another activity is the provision of emergency liquidity swaps in conjunction with central banks of other countries. These programs installed during crisis periods are difficult to taper easily without proper transparency.

Today, most of the programs are enacted through the mechanism of central bank reserve accounts. Converting these reserve accounts into wCBDC operations can help decentralize the programs and provide more transparency into the efficacy and compliance of the special programs. CBDC driven decentralized facilities will prevent abuse, profiteering, and paradoxically, more automated control. The availability of programmability, provenance, and auditability in CBDC makes this possible.

DvP, DvD, PvP, TvT, T*vT*

These acronyms expand to delivery versus payment (DvP), delivery versus delivery (DvD), payment versus payment (PvP), token vs token (TvT), and token(s) versus token(s) (T*vT*). All of them refer to mechanisms set up to reduce settlement risk. Settlement risk is magnified when using RTGS, which implements a non-recourse final settlement of the payment leg. Usually, this is the practice of two parties in a contract exchanging assets simultaneously so that one of them,

[6] (2020, April 9). III. Central banks and payments in the digital era - Bank for International Settlements Retrieved August 9, 2020, from https://www.bis.org/publ/arpdf/ar2020e3.pdf

having honored their side of the contract, is not exposed to the risk that the other does not. The two legs of the contract need to be atomic or indivisible. Either both fail, or both succeed. In traditional settings, this is usually done through the mechanism of a central counterparty, often using a pre-funded net settlement facility. In a CBDC, automation of atomicity occurs through smart contracts in addition to some programmatic escrowing mechanisms.

Retail CBDC (rCBDC)

Different sources list rCBDC properties derived from rCBDC's payment rationale and its parallel to cash. These properties exist on a spectrum. Table 1 below lists the properties and the multiple ways in which different settings of these properties can be viewed from completely analogous to cash to the converse of cash.

Retail CBDC serves retail transactions. As noted above, these are low-value transactions, but there are numerous transactions among many accounts. Retail customers do not have central bank accounts today. The two-tier model refers to the provision of core infrastructure by central banks, which allows commercial and private players to build retail-facing user interfaces and controls on top. This creates room for private innovation to thrive. The two-tier model is preferred by experts.

There is a school of thought that advocates public direct access to central bank accounts.[7] Arguments for direct accounts at the central bank include financial inclusion and rapid payments of benefits during times of crisis. The proponents of direct accounts have a point, since years of lip service from the private sector has not provided such access to financially excluded players. This option is presented as one of the architectural models. There is nothing preventing the coexistence of the following models: a direct central bank account structure for outgoing benefit payments and a rCBDC core infrastructure providing a substrate for private players to build upon.

Retail CBDC is often meant to emulate cash. As a bearer instrument, cash can be private and anonymous, with an interest rate of zero, and can be exchanged in disconnected settings. A CBDC denotes a direct claim to the central bank. Therefore, a CBDC is most like cash. Since cash is a component of narrow money, a CBDC assumes a similar role and can be used for final settlement. Like cash, a CBDC should be usable in a disconnected context.

[7] (2018, June 4). Central Banking for All: A Public Option for Bank Accounts. Retrieved August 9, 2020, from https://greatdemocracyinitiative.org/wp-content/uploads/2018/06/FedAccountsGDI.pdf

The curse of cash is that it can be used to easily circumvent controls meant to prevent money laundering and financing terrorism. rCBDC designs try to cure this weakness of cash by establishing privacy and anonymity for small transactions while creating KYC/AML provisions for larger CBDC transactions using programmability. The other downside of cash is that it is physical and bulky in large amounts; this is easily avoided in a digital form.

Like cash, rCBDC has the desirable property of allowing users to transact without a bank account. Cash also works in disconnected settings where there is no internet connectivity or any electricity. Most of the ordinary users will use rCBDC through user devices. User devices include mobile phones of all form factors: tablets, laptops, desktops, smart cards, and universal access devices (UADs). The application running on a user device is a digital wallet. UADs are used by people with limited mobility or other disabilities and should be considered in the design of digital wallets. If a fully disconnected user wallet is used for small transactions, then an eventual reconciliation to common and shared infrastructure is needed.

To recap, rCBDC does not need to be completely analogous to cash; however, widespread acceptability and adoption requires rCBDC to emulate cash. As mentioned, Table 1 presents the various properties and choices for implementation. As long as there is programmability of the underlying core infrastructure as well as digital wallets and a clean separation, the chosen properties can be implemented. This paper mostly addresses core infrastructure.

Uniformity of money

One view is that rCBDC should be fully convertible at par to and from all other forms of money, including bank deposits. In another view, this frictionless and unlimited convertibility should be constrained, especially to avoid bank runs and other unforeseen monetary policy convulsions. The programmability of digital tokens can be used to dynamically set limits of conversion and conversion rates based on observed behaviors and changing laws. These controls should be available even in the first iterations of a production deployment of CBDC.

Full convertibility may not be possible, since the potential demand for CBDC can cover the whole of M2, which is about 400-500% of M0. Some amount of this asymmetry can be overcome with liquidity provision from the central bank. With cash, this level of demand is not even a distant possibility because of the physical nature of cash and the narrow in-person setting in which cash can be used. The demand for CBDC in the wild will definitely fluctuate. Obviously, this has significance for fungibility across types of fiat money. Today, there is full fungibility

across the various representations of fiat. Deposits, cash, and other forms of fiat are fully fungible.

Table 1. CBDC Properties

Property	Analogue to Cash	Hybrid	Converse of cash
Account needed?	Only for ramp*	Only for ramp	Mandatory
Privacy	Always	Risk-Based**	Never
KYC/AML	Txn>$10,000		Always
Interest	0%	0% for < $1000	Spread to FedFunds rate
Disconnected	Always	For small amts < $10,000	Never
Convertibility	Full	Limited: excess for legitimate purpose	Hard Limit
Recoverability	None	Not for low amounts	Always
Expiry	Not applicable	Settable property	Needs to be renewed periodically

* Only for ramp: A bank account is needed to get the asset and to deposit the asset.

** Risk Based: privacy is available only for smaller transactions, for larger transactions KYC/AML and other forms of regulations operate. Even then limited privacy could operate, with only regulators being privy to the KYC/AML conformance. For law enforcement, proper legal procedures have to be followed including warrants and other judicial controls.

Cross Border Payments

Current cross border payments processes and supporting infrastructure involve multiple parties that include originating banks, correspondent banks, central banks, and other utilities such as SWIFT and CLS. The stringent regulatory requirements on KYC and AML impose significant

manual checks at these intermediaries, slowing the entire process and leading to a multi-day settlement cycle.

CBDC Models

Several models have been proposed for CBDC. For wCBDC, there is a great chance that direct central bank accounts prevail, since that is the current practice for reserve accounts. There is very little opposition to this idea. For rCBDC, most experts prefer the two-tier approach. The two-tier approach preserves the relationship that people have to commercial banks, allowing for direct claims to the central bank.

There is a variant on the two-tier model called a synthetic CBDC (sCBDC), which is not a true CBDC since the claims to the central bank are indirect. Synthetic CBDC follows the narrow bank approach using full reserve banking for backing CBDC.[8] sCBDC is like a stablecoin, except the central bank is directly in charge of the reserves. This also means the central bank has to be able to control the supply of sCBDC that can be issued by the commercial bank.

The other debate is whether the basic model for a CBDC should be account-based or token-based. Since the basic meanings of these terms are under debate, the solutions addressed below are broad enough to accommodate the various interpretations.

In limited use cases, digital and physical meet in smart cards. Physical control of digital assets can be demonstrated using a smart card. In this case, the public witness has to record the reservation or escrow of the amount. However, for the CBDC to be fully fungible and to enter back into the system, a shared ledger has to be updated.

In all the models below, the central bank issues the CBDC. The holders of CBDC have a direct claim on the central bank.

Central Bank Accounts

The central bank issues CBDCs. Users are on-boarded and managed by the central bank. CBDC is issued and transferred to a user in exchange for other forms of fiat. This user then transfers to other on-boarded users.

The wCBDC use case can be fully covered by this model, since central banks already manage these accounts. In the retail case, the sheer number of user accounts to be on-boarded and

[8] "Financial Innovation and Deregulation in Perspective." James Tobin, 1985 https://www.imes.boj.or.jp/research/papers/english/me3-2-3.pdf. Accessed 21 Aug. 2020.

managed is the main challenge. These numbers are far from the comfort zone of most central banks, except when the population and the users are under a few million and the currency is not widely used outside the borders. In some countries, legislative barriers prevent central banks from opening user accounts.

Another use case is payment of direct benefits through central bank accounts, either intermediated by other relevant arms of the government like the treasury department or directly administered. Commercial banks are very wary of this model for rCBDC, since this can break their relationship with retail users. The vast majority of the money supply is generated by commercial banks through loans, so any effect on the loan process or to the continued viability and health of commercial banks due to direct central bank accounts has to be studied carefully.

Two-Tier Model

The two-tier model only applies to rCBDC. The central bank issues CBDCs. Retail users are not on-boarded through the central bank but rather through the commercial banks that have retail competency and have established relationships with many users. Commercial banks distribute rCBDC to the on-boarded users. Once the user has the rCBDC, they can use it to conduct retail transactions. The users have a direct claim on the central bank, meaning that retail users can freely use rCBDC without the involvement of commercial banks. For people with no bank accounts, a limited form of on-boarding can be performed through a certified wallet provider. Options for receiving and spending for all wallet holders would be limited by the KYC/AML/CFT regulations.

CBDC Implementation

Current CBDC proof of concepts (POCs) are limited in scope with basic functions and focus on separating the solutions for retail and wholesale CBDCs. These POCs do not address complex scenarios such as periodic facilities, repo operations, or central bank swap lines. The security of CBDC implementation is barely addressed. Most CBDCs are built on a single platform and rely on or work around the limitations of the chosen DLT, blockchain, or central ledger. Standards of token representation or business rules are not considered. Requirements are driven by a single organization or central bank.

This section is the core of the paper. A novel standards and basic building blocks-based approach is proposed. The basic building block can be used in multiple wCBDC and rCBDC settings. The solution also proposes robust security. What follows is a discussion of the chosen standards that leads to the proposal for a dual network. The contracts and business rules are on one network, and the digital token is on another network. The two networks are bound together for a single purpose: the controlled issuance, transfer, and management of CBDC. The token network has been implemented using TTF and its expression in Ethereum. The contract network has been implemented using ISDA CDM on Corda. The contract network and its linkage to the CBDC token network are used to illustrate the issuance part of any CBDC, a rCBDC or wCBDC. The cross border use case is demonstrated using the basic building block of a dual network.

Why Standards?

Early prototypes and test versions of CBDC tend to be focused on a particular DLT or blockchain to leverage the ledger's proprietary, non-standard features. The next-generation CBDC solution is likely a standards-based implementation that enables interoperability and portability. Standards prevent vendor and protocol lock-in by increasing portability. This prevents dependency on any single ledger or smart contract language. Layering of the technical stack with well-defined and loosely-coupled standards for interaction using APIs allows the independent development of the different layers of the stack. This also enables the adoption of the best in class solution for each layer of the stack. Different central banks will adopt different technical stacks and operating models for implementing CBDCs. For cross border payments and other

applications where two or more CBDC technical and business stacks have to interoperate, standards are especially important.

Properly developed standards incorporate multiple points of view. In the current environment, central players often dictate the requirements and implementation and force adoption, which leads to variations in standards. In a decentralized digital environment, peer to peer interactions need a precise and unambiguous specification of standards.

CBDC standards need to be domain-specific. The proposals presented here rely on existing or emerging domain-specific standards. The domains for CBDC fall into two categories: financial contracts and digital modeling of money as value. These two domains have to interact. The Common Domain Model (CDM) for financial contracts and Token Taxonomy Framework (TTF) address these two domains.

Standards For CBDC

Given below are details of the standards used in the construction of the dual network. These standards are still being forged in the open, reference implementations and tools are also available in open source. The standards are still works in progress, but certain principles and core ideas have been recognized.

Standards Development Organizations (SDOs) are meeting and working to break ground on CBDC and digital currencies in general. As long as SDOs consider openness, overall provenance, and stable interfaces, they will converge on standards that look similar to CDM and TTF. Standards are not abstract, so they need reference implementations, test suites, common sense metrics, legal and regulatory backing, and independent certification to build consensus, trust, and adoption. Open source availability also allows independent verification of the standards.

Common Domain Model (CDM)

To implement robust solutions covering digital-shared data, services and a value exchange framework need new standards. Standards such as FIX, FpML, ISO 20022 are all designed to address current practices in capital markets. While each standard addresses specific markets and trading practices effectively, they do not have a shared vision of the front-to-back trade flow. This fragmentation and associated reconciliations result in huge operational costs for the industry.

Existing standards are momentary; they standardize communication between parties at each event. Fidelity and provenance are lost as these messages are processed piecemeal by the various platforms inside each party. Independent multi-party storage and lack of cryptographic integrity and trusted provenance adds to tracking, reconciliation, conflict resolution and reporting challenges.

ISDA has recognized the huge cost structures in post trade services and has developed a digital representation of trade data and business events: ISDA CDM. CDM started out as a swaps and derivatives data and process standard. With recent additions to digital security definitions and security life cycle, CDM is in a unique position to address the digital representation for the entirety of capital markets ranging from cash to security finance to derivatives.

CDM is a lifetime data standard, tracking a contract from inception to expiration. Economic events during the lifetime are also tracked and linked to the originating contract. Digital signatures on immutable hashes and provenance through hash links, secure the integrity and track the unfolding of the contract over time. otcDigital is working with the CDM Working Group to implement issuance and settlement business events in CDM, which would complete all the functions required for CBDC. CDM is available in machine-readable and machine-executable formats, making it ideal to interact with newer technologies like cloud, AI, and distributed ledger. These properties make it ideal for regulatory oversight in a timely and efficient manner.

CDM has standards for serialization resulting in uniform persistent storage. Porting from one platform to another is simpler with such a data format as the CDM contract with its linkages and digital signatures resembles a blockchain in itself.

Given below in Figure 2 are simplified CDM life cycle events for CBDC such as mint, transfer, and burn states. The steps in the life cycle are marked with descriptions and events that drive the process forward. Sometimes an event causes effects on a separate network, like issuing or transferring CBDC tokens on a token network. The lineage, depicted as a series of backward arrows, link the start of the life cycle to the end of the life cycle. All payment-related tokens have a linkage to the original CDM contracts. Each CDM payment-related contract event binds to the resulting token network transactions. These linkages create a two-way bridge between the contract network and the token network. The two-way bridge irrevocably links the contractual reason and the activity in the token network.

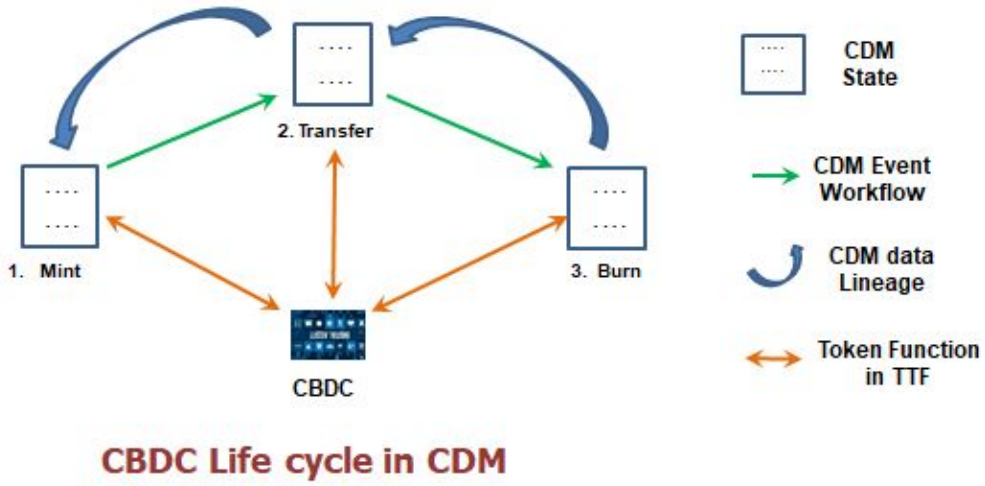

Figure 2

Token Taxonomy Framework (TTF)

Here, the word token means a digital artifact, reflecting value that is programmable to automate behaviors and attributes. In this sense, any CBDC is a token. Tokens implemented in specific blockchain platforms have exploded in recent years. Most have been implemented in platform-specific standards, such as the ERC-20 token standard in Ethereum. The TTF was started as a way to collaborate using a meta-language to describe tokens using a simple formula in a platform-independent way. TTF has tooling to generate interfaces, documentation, and code from the formula. The actual implementation can be on any platform as long as the interfaces are created and accessible. Many token formulae and associated artifacts have been created, and more are currently being worked on.

Initially incubated under the Enterprise Ethereum Alliance (EEA), the TTF has migrated to the InterWork Alliance (IWA). One of the main motives of the move was to demonstrate the platform independence of TTF. TTF is the linchpin of the IWA. IWA has ambitions to create a meta-language and an ecosystem for contracts and analysis layered on top of the token definition standard. IWA members include Microsoft, Accenture, SDX (The Swiss Digital Exchange), Nasdaq, DTCC, ING, R3, Digital Assets, Chainlink, NEO, DLA Piper, UBS, and other representatives from the old and new economies. The collaborators in the mix are software developers, line of business executives, and regulators.

TTF defines a token as composable, assembled from a base behavior, overlaid with multiple other behaviors and properties. The token definition produces a series of artifacts, progressing from a formula to other artifacts including business requirements, analogies and documentation. From the formula, a set of interfaces and control messages can be generated to interact with the token. A set of visually friendly modeling tools is under development. These tools automatically generate all the artifacts discussed before. The power of the TTF is demonstrated with an example: a CBDC called eThaler developed under Hyperledger Capital Markets Special Interest Group (SIG). eThaler artifacts are available in open source in Hyperledger labs.[9] These artifacts include all the resources generated by TTF tooling. eThaler was implemented as an ERC 1155 token in enterprise Ethereum. The code is also available in the same location. Anyone can recreate the solution on their own using this code and deploying it on Consensys Quorum or any Ethereum variant.

eThaler was modeled with the following formula. Each letter in the formula is a behavior that translates to a set of interfaces to be implemented on a platform.

The eThaler formula is **tF{d,t,p,c,SC}**

Business Description: The base behavior is fractional fungible (**tF**). To be fractional, it has to be divisible (**d**). To be fungible it has to be transferable (**t**). These behaviors make eThaler similar to money. eThaler is pausable (**p**) for possible freezing of movement and all other operations because of market conditions. Supply control (**SC**) is a behavior set that ensures that a token can be minted (***m***) or burned (***b***) only by a permitted authority (***r***). SC is a behavior set that wraps m, b, and r behaviors. Compliant(c) behavior in eThaler assures that programmatic checks ensure transfer, burn or mint, operations are within regulations.

Business Example: eThaler enables the issuance of regulated electronic money by the central bank (mintable and burnable only by the central bank) and its practical usage in real financial applications.

This formula was used to automatically generate a series of artifacts, including a PDF file that details the interfaces, business analogies, and use cases that make up eThaler. The code that implements this token was created in a platform specific manner as detailed below.

[9] "hyperledger-labs/eThaler: Model a sample CBDC in ... - GitHub." https://github.com/hyperledger-labs/eThaler. Accessed 29 Aug. 2020.

ERC 20 & ERC 1155

The TTF behavior model had to use a specific platform for eThaler implementation. eThaler uses Consensys Quorum which is an Ethereum variant, specifically targeted for enterprises. ERC 20 and ERC 1155 are Ethereum specific standards. ERC 20 has wide adoption. Most of the tokens on the Ethereum mainnet are implemented using ERC 20. Defi tokens are also implemented in ERC 20.

ERC 1155 is an evolving multi-token standard. eThaler implementation used ERC 1155 with some extensions. There are several reasons for choosing ERC 1155. In ERC 1155, a single solidity smart contract can implement multiple tokens. A single eThaler smart contract implementation addresses multiple wCBDC implementations, each with slightly different characteristics. For example, in response to COVID-19, CBs announced several special purpose financings schemes with specific restrictions in a short period of time. The ERC 1155 contract could be used to implement such schemes and also can track the effectiveness of such programs.

Securing The Private Key

Most of the modern cryptographic methods for digital signatures and encryption use public key cryptography (PKC). PKC relies on a private key, public key pair. The private key, a secret that needs to be guarded against observation by attackers, is thus a unique vulnerability in the safekeeping of digital assets and securing the trust framework of contracts.

A payment transaction signed and submitted by a Financial Service Provider (FSP) to the digital payment network is irreversible.FSPs have to ensure that each and every signature is securely signed by their corresponding private key. A single fraudulent transaction submitted by either stealing or copying the private key undermines trust in the signing party and the whole network. The management and security of keys are not part of what is understood to be core infrastructure, but usually runs on user facing applications called digital wallets. Given how important that function is, standards-based approaches to robust key management and usage have to be addressed.

Digital wallets will likely run on a variety of user devices which have a multiplicity of form factors and capabilities. User devices include mobile phones, tablets, desktop computers, smart cards and universal access devices (UADs). Risk-based standards anchored on modern

cryptographic techniques are needed for secure interactions using digital wallets running on user devices to transfer money or sign contracts.

The detailed design of digital wallets is beyond the scope of this paper. However, as the security of the system hinges on the private key, the design of digital wallets are a significant part of any CBDC infrastructure. Central banks will likely have regulations around the function of digital wallets that secure CBDC as well as certification programs for it. Existing standards like FIPS 140 in the US could function in the global context.

Current forms of security of private keys in wallets include an exchange holding keys, browser wallets, paper-based cold wallets, multisig wallets, hardware wallets, Hardware Security Modules (HSMs), and Multi-Party Computation (MPC). The subject of digital wallet implementation is vast and requires a separate paper. MPC is addressed below, since it is the next-generation key management solution especially relevant to enterprises.

Multi-Party Computation

Multi-Party Computation (MPC), also known as Secure Multi-Party Computation (SMPC), is the next-generation cryptographic technique where parties (representing users within an organization) jointly compute and sign a transaction without sharing the private key in whole or in parts. A valid signature can only be computed from a rule-based quorum of signers in different roles from an authorized group of signers. This is called threshold cryptography, as a threshold of m signers from a larger number n is needed to create a valid signature. Unlike traditional custody cryptographic techniques, MPC ensures the privacy, security, and integrity of keys in signed transactions. Figure 3 outlines the MPC technique:

- The private key is mathematically computed and assigned to the signing parties without constructing the whole key in any location or function
- Each party signs the ledger transaction with its own part of the key and sends the partial signature to the MPC computation servers
- Once the threshold rule is fulfilled, the MPC servers mathematically compute the final signature which attests the transaction being sent to the ledger

The private key is never present as a whole anywhere; it cannot be stolen or observed by attackers. Secure MPC with m of n threshold signatures provide the utmost secure handling of private keys and signing mechanisms. Thus, the use of a robust MPC framework would

effectively provide cyber security and resiliency against malicious attacks. NIST labs recently launched a threshold cryptography standards initiative.[10]

Given that individual retail users may hold only a small amount of CBDC in their digital wallets, an MPC solution is not recommended for retail users. FSPs can provide many simpler and highly secure wallets to retail users. For disconnected and direct access, small amounts of CBDC may be managed through wallets on smart cards or other UADs.

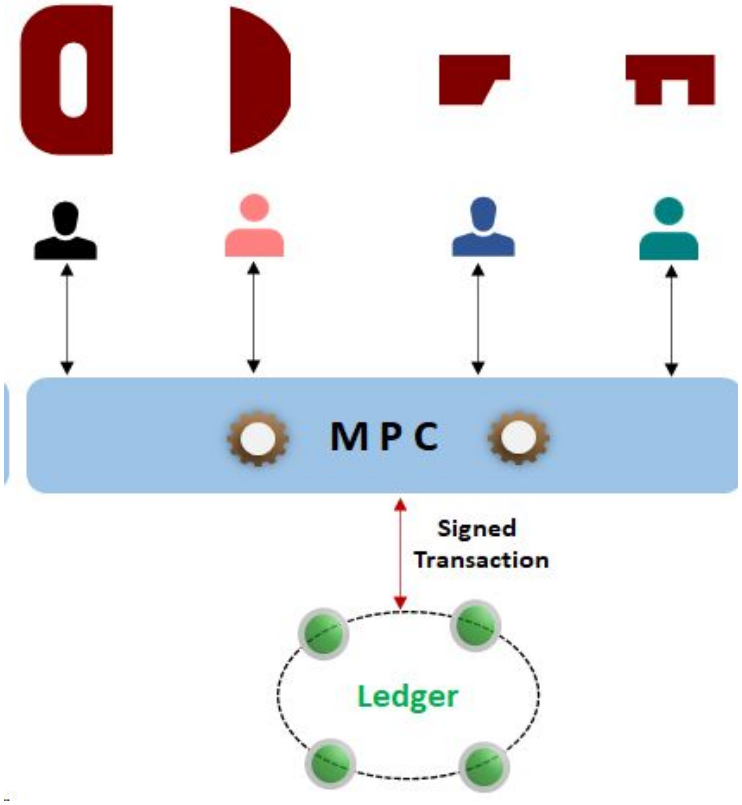

Figure 3

The Dual Network

A contract network and a token network linked together constitutes the dual network. The participants in the dual network are the Financial Service Providers (FSPs) and the Central Bank (CB). The term FSP is broad enough to encompass commercial banks, payment service providers (PSPs), central security depositories (CSDs), central counterparties (CCPs), and other types of financial service providers.

[10] "NISTIR 8214A, Roadmap - NIST Computer Security Resource ...." https://csrc.nist.gov/publications/detail/nistir/8214a/final. Accessed 23 Aug. 2020.

The contract network is privacy intensive and uses CDM to model the contract and business flow between the CB and a FSP. The CBDC token network needs to be more widely accessible for a fungible asset token flow.

The execution of each CBDC business event is controlled by smart contracts on both the contract network and the token network. Thus, the smart contract is distributed between functions controlling the CDM and in the appropriate token network. For example, a request from an FSP to issue more CBDC is first processed as a CDM business event and then, subject to all conditions being satisfied, the CB executes the transfer function in the token network.

In both networks, the network operator is the CB or a service provider under the control of the CB. Nodes in the network are run on invited participants' infrastructure. This creates a certain amount of resilience through decentralization. The use of the word "node" implies a multi-party system; ways of implementing a multi-party system includes blockchains or DLTs. Public access for rCBDC is through certified digital wallets.

The separation into business contracts and fungible tokens and running them in two networks have the advantage of increasing the transaction rate. This separation makes it possible to pick different platforms that fulfill different functional and non-functional requirements for contracts and tokens. Although depicted as two separate conceptual networks, the dual network can also be implemented in a single platform as long as the requirements and risks are well understood.

wCBDC

A wholesale network as a dual network is illustrated below in Figure 4. In the wholesale network, every participant (FSP) is registered by the CB and every FSP account, represented externally by a wallet, is approved by CB. A FSP will make a formal request to CB to issue CBDC against their reserve account. After validation and verification, the CB will make appropriate reserve adjustments and then issue CBDC into the FSP account. A FSP thereafter is free to transfer payments to another without the need for any CB operation. To redeem CBDC, a FSP would make a formal request which would be similar to issuance and the CB would reclaim CBDC from FSP's account and make appropriate adjustments to the reserve account.

Control functions govern all central CB interactions with FSPs on a peer to peer (P2P) basis. These functions are distributed over the asset and contract networks. The affected networks are listed where appropriate. The control functions include:

- FSP registration by CB (whitelisting the provider) - contract network
- FSP wallet registration by CB (whitelisting the wallet) - token network
- FSP Request for Issuance / redemption against CB reserves (or collateral) - contract network
- FSP to FSP direct transfer - Token network (maybe backed by a different contract network)
- Support for RTGS, prefunded and deferred netting amongst FSPs - see below
- Enables DvP by recording each transaction in CDM, tracking the delivery and final settlement of each leg (delivery or payment) - both networks
- Support for cross border payments (PvP) with CDM interoperability across CBs - both networks
- Support for Repo operations between CB and FSP using multi-tokens - both networks
- Other CB ad-hoc operations similar to COVID-19 responses - both networks

Real Time Gross Settlement System

While the transacting parties can keep their non-CBDC leg of the transaction private in another ledger or database, the CB can require proxy registration of that transaction for surveillance and AML purposes. So, if two parties agree to transfer wCBDC, they would still register their other leg in CB's contract network by reference.

Pre-funded Netting

While this operation is relatively risk-free compared to RTGS and deferred netting, the CB would be similarly interested in the other leg information for AML and surveillance.

Deferred Netting

In deferred netting, transactions are not immediately settled but are netted over a period of time, from a few minutes to a day. This can be done in a bilateral or in a multilateral way. Deferred netting is a liquidity saving mechanism. Liquidity needs can be reduced upto 100 fold through deferred netting compared to immediate settlement. For transparency, the information about the netted transactions in any other venue for settlement in wCBDC should be made available in the contract network.

In all three scenarios, standardized cross chain information is required to notify the CB contract network about pending payments.

wCBDC

The first illustration of the dual network pattern is in Figure 4.

Prerequisites: FSP is registered by CB

wCBDC Issuance Workflow:

1. FSP requests CB for CBDC issuance
2. CB verifies and makes adjustments to reserves
3. CB issues tokens to FSP
4. CB sends transaction confirmation details to FSP
5. FSP confirms from the token network that tokens are issued
6. CDM issuance contract is completed

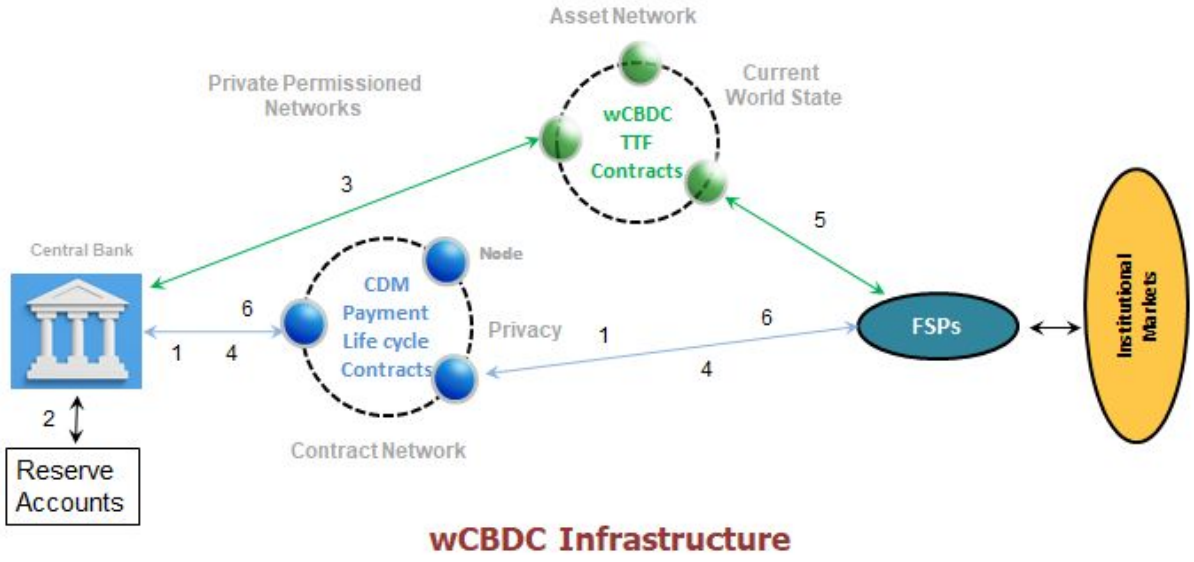

Figure 4

rCBDC

The retail network is similar to the wholesale network, the CB registers each FSP and issues rCBDC against the corresponding reserve account. FSPs register fully authenticated retail

accounts and move money into these accounts without the need for any CB operation. Such retail accounts are managed by the FSP. rCBDC can be held in the institutional wallets for transfer to the retail wallets.

Restricted retail wallets with pseudonymous identities can be made available to anyone, not just KYC account holders. Both types of identities are provisioned on the token network such that peer to peer rCBDC transactions are possible. Restricted wallets have to operate within the boundaries of non-KYC regulations. Thus all retail customers have a direct claim to the CB. FSPs and other wallet providers can provide highly secure, innovative and user friendly wallets to retail users. If the CBs are authorized to provide accounts to retail customers, the network rules are easily adjustable to accommodate that. It is up to each individual country's laws and regulations to draw the functional line between the CB and FSPs.

rCBDC Issuance

Figure 5. adds to the pattern introduced in Figure 4. The contract and token dual network pattern in wCBDC is used in the rCBDC infrastructure to support the workflows between the CB and FSPs. The issuance workflow in wCBDC network still holds. To complete the rCBDC network functions, the following workflows are added:

- FSP registration of retail users devices and wallets in rCBDC network
- Ability to directly transfer between user devices subject to retail limits set by CB

Prerequisites: Retail users are registered in rCBDC by FSPs

1. Retail user requests FSP for rCBDC transfer to their personal wallet
2. FSP transfers tokens to the retail user's registered wallet in the rCBDC token network
3. FSP decrements the user's deposit account or credit line
4. Retail users can freely transfer rCBDC to settle payments or obligations using their digital wallets without the need for any coordination either from the CB or the FSP.

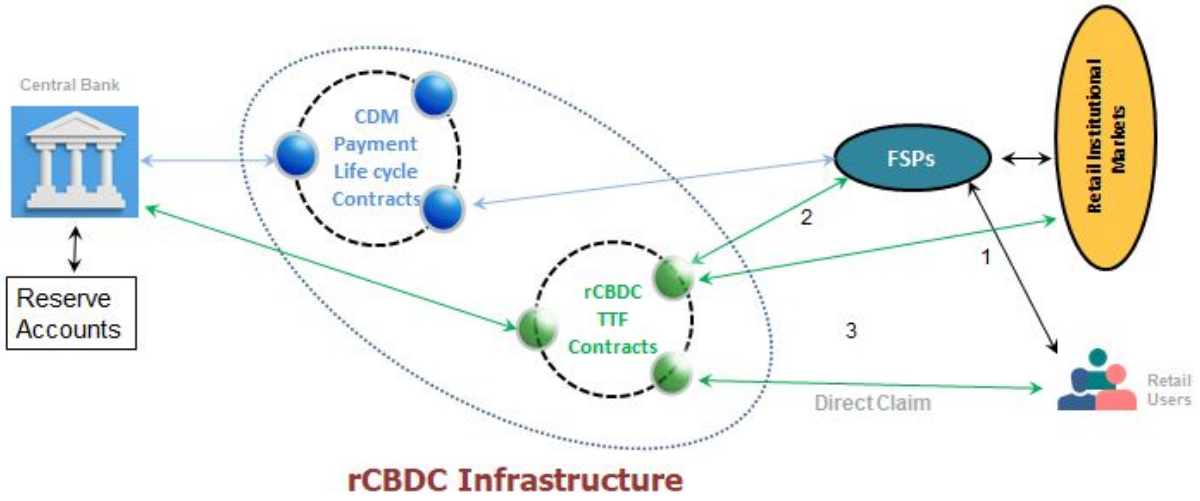

Figure 5

Anonymous wallets

Anonymous wallets are needed for users who do not have bank accounts and have to be able to transact without a KYC. Anonymous wallets can also serve users who wish to keep some of their transactions private. The Financial Action Task Force (FATF) guidelines along with national regulations control the total amount and rates of such transactions.

1. Steps have to be taken so that a user does not create multiple anonymous wallets to circumvent the limits set by appropriate laws and regulations.
2. Retail user anonymously downloads a personal wallet app from a CB approved site
3. Digital wallet registers an anonymous identity without KYC on the token network.
4. Anonymous retail user gets rCBDC payment from a user who has rCBDC in their wallet.
5. Anonymous retail users can freely transfer rCBDC to settle payments or obligations using their digital wallets without the need for any coordination either from the CB or the FSP.
6. Any anonymous user can use rCBDC to convert to cash using a service provider much like a check cashing service or by exhausting rCBDC for payments.
7. Both the above transfers are subject to limits set by the CB for anonymous transfers and holdings.

Retail users do not participate in the CDM contract network. If they need to refer to other contract networks because they are small or medium businesses or even wealthy individuals, the linkage can be inserted in the transaction in the token network using the wallet.

Integrated CBDC Infrastructure

For operational efficiency, FSPs can request for transfer of CBDC between the wholesale and retail networks. To facilitate such optional intra-CBDC network transfers, rCBDC and wCBDC infrastructures can be merged as shown in Figure 6. The main feature is that the CDM payment lifecycle contracts are now shared between the two networks rCBDC and wCBDC. The next step for such an integration would be to house both the wCBDC and rCBDC token contracts in one network. Obviously, the number of accounts, the participants in operating the nodes, and the demands on the system in terms of the number of transactions per second are different for different currencies. All of these have to be taken into account when making such decisions. For nations with smaller populations and a currency used by few, the merging of these networks makes sense.

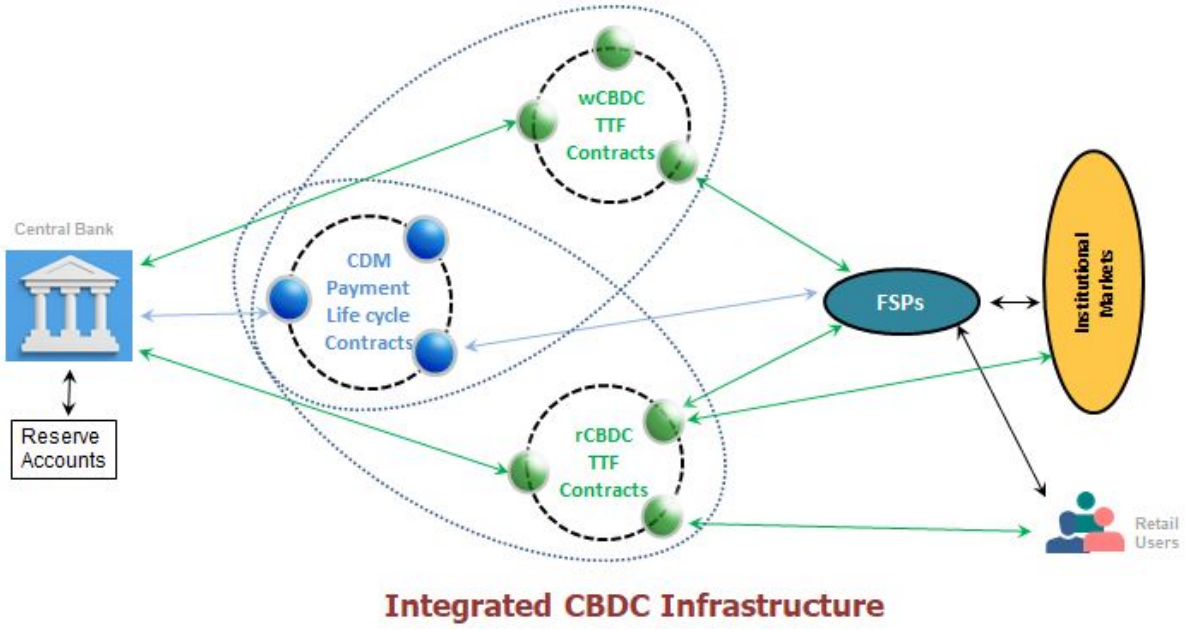

Figure 6

Central Bank Liquidity Swaps

These swaps operate between countries' central banks to ensure that funding in the appropriate currency is available across borders. The counterparties and participants in these arrangements are central banks of the currencies involved. These are temporary facilities established during times of crisis.[11] The more generic and common use case of cross border payments is addressed next to show how the structures set up for a specialized case can be further augmented and used in that context.

A currency swap between CBs is modeled using the standardized CDM cross currency swap. This process is similar to the wholesale CBDC workflow but with two legs. Each leg would require CBs to transfer appropriate CBDC at the trade date and swap maturity date.

Following the design pattern, the wCBDC token network and the CDM Contract Network are combined into a single logical wCBDC network. This is depicted in the following Inter-CB cross currency infrastructure diagram below.

CB Cross Currency Swap Workflow:

Prerequisites: CBs are registered in each other's network

1. CB2 requests CBDC1 from CB1 with a CDM cross currency swap proposal for CBDC2
2. CB1 verifies the request against its currency accounts and reserves
3. CB1 approves the currency swap
4. Asset transfer phase
    a. CB2 issues CBDC2 to CB1
    b. CB1 issues CBDC1 to CB2
5. Asset transfer verification phase by both CBs: 5a & 5b

The first leg of cross currency swap is executed as in the CDM contract. At the maturity of the swap, both parties transfer and verify tokens to complete the entire swap life cycle.

[11] "Central bank liquidity swaps - Federal Reserve Board." 15 Apr. 2020, https://www.federalreserve.gov/monetarypolicy/bst_liquidityswaps.htm. Accessed 27 Aug. 2020.

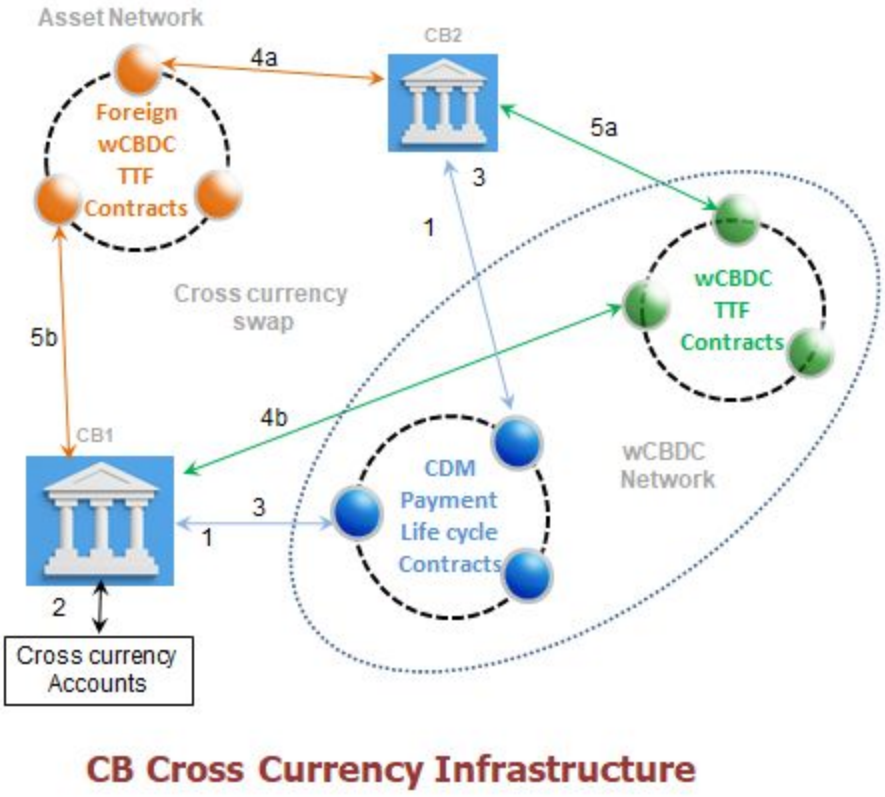

Figure 7

Cross Border Payments Using CBDC

Cross border payments involve different currencies and hence different central banks. Sometimes the payments go through a more commonly used currency such as USD or other global currencies. Given below is a proposal for cross border payment using the dual network as a building block.

Expanding on the above themes, the CBDC design pattern can then be applied to cross border transactions by cross registering CBs and FSPs against each other. The cross border transactions can be categorized broadly into 3 areas:

1. CB to CB cross currency swaps (this was addressed above)
2. CB to local FSP cross currency swaps (these swaps are executed within a national boundary)
3. Cross border FSP transactions

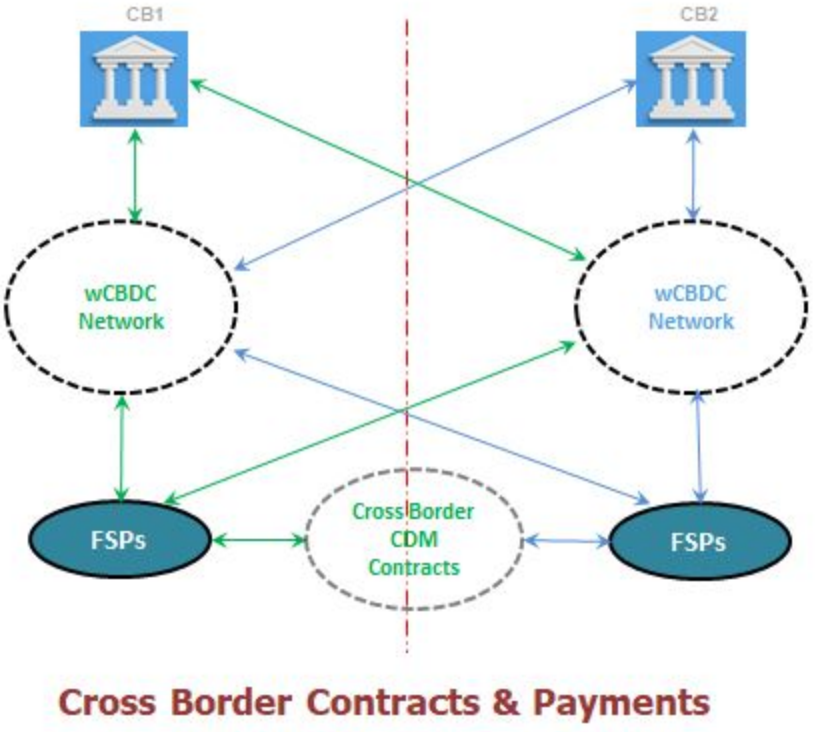

Figure 8

Preparing To Deploy & Operate A CBDC

Central banks need to consider many factors for the production deployment, continued support, and operation readiness of CBDCs. The analysis below is not meant to be comprehensive; however, it is a glimpse into the complexity and scale of the effort needed. A production CBDC will be a large-scale technical project. Processes and practices for such a project must follow established procedures and invent some new ones. In addition, the socioeconomic, political, legal, regulatory, and security challenges are unprecedented, but not insurmountable with proper planning, preparation, global standards, and the right team.

Any CBDC in production will be an important part of the national infrastructure of any country. One of the most important considerations for a production deployment of CBDC will be the security of the system. Researchers, practitioners, and others concentrate on requirements and simple implementations today. Any CBDC system has to withstand attacks from state and

non-state actors. A successful and well-publicized attack on the system can break trust in the system. Even rumors amplified through social media can diminish this trust.

Digital Identity & Wallets

Countries with existing robust identity systems will have an easier road to the construction of secure wallets. These countries usually have a comprehensive legal and regulatory system to support a national identity. Emerging decentralized digital identity and verifiable claims concepts are being standardized under the World Wide Web Consortium (W3C). These standards along with legal protections for customer data will make the design of digital wallets and digital lockers easier, even in countries such as the US with a patchwork and ad-hoc identity system.

Digital wallets are going to be an important part of any CBDC ecosystem. User experience design and a seamless experience across devices will be key to adoption. Central banks need to be involved in the design, approval, and certification of wallets that handle CDBDC. This is not part of the usual expertise of central banks, and they need to hire talent that can help them.

Interoperability

CBDC implementations have to be interoperable for smooth adoption and operation of CBDC. There are several types of interoperability to be considered: interoperability of the CBDC with existing systems run by FSPs and the ease of on-boarding new FSPs and their mutual interactions. This is called intra-CB interoperability. Cross-Border interoperability is interoperability between CBs and FSPs in cross border payments. CDM has the advantage of being convertible into standard messages. FINOS Alloy has built in templates and models that can be leveraged to convert from CDM to ISO20022. Alloy is slated to be open sourced in September 2020[12]. The CDM reference implementation has utilities to convert to FpML messages as well.

Intra-CB interoperability: Within a CB jurisdiction, interoperability between the CBDC and traditional payment networks can be achieved by adopting CDM or prevailing FIX, SWIFT, or ISO standards. In countries where there are no existing CB payment systems, adopting CDM as the common communication standards for all interfaces is highly recommended. Where there

[12] "Alloy Overview." https://www.finos.org/alloy. Accessed 29 Aug. 2020.

are existing or ongoing CB RTGS implementations, CDM along with the other standards listed above could be utilized.

Cross Border interoperability: Cross border payments (Figure 8) and Central Bank Liquidity Swaps (Figure 7) show how interoperability between the various CBDC implementations work. Similar to Intra-CB interoperability, the CDM digital standard would promote smoother implementations and foster further innovation in cross border transactions.

Ledger Name System (LNS)

Interoperability requires discoverability through a name system. A LNS implemented hierarchically through a universal registry system is one solution. In the short term, a simple whitelist can be implemented. The Domain Name System (DNS) of the internet is the nearest analogy. Drawing upon the experiences in building a robust and secure DNS should assist in the design, the processes and implementation of the LNS.

Scaling CBDCs

Current transaction data from around the world suggests huge numbers of retail accounts are needed to service rCBDC payments. In the US, this could be as high as 300 to 400 million accounts. In the eurozone, the numbers are in the area of 500 million. A larger number of accounts are handled in countries like India through the Aadhaar infrastructure, proving that such a huge number of users can be managed. Most governments have systems that handle retail accounts at scale, mostly for benefit payments and tax administration.

Transaction rates for rCBDC will ebb and flow with broader market needs and with the season. Peak Visa transaction rates of 35,000 transactions per second are cited as a goal for a robust rCBDC infrastructure. Large CBs should target to double or triple that rate to future proof the design.

DTCC and its partners tested selected enterprise blockchains and found that high transaction rates are sustainable for a period of time in the context of equity trading. They mentioned 100 million transactions a day at 6,300 transactions per second.[13]

[13] "DTCC Announces Study Results Demonstrating that DLT Can ...." 16 Oct. 2018, https://www.dtcc.com/news/2018/october/16/dtcc-unveils-groundbreaking-study-on-dlt. Accessed 30 Aug. 2020.

A related challenge is the total volume of stored transactions. As time goes on, an immutable ledger steadily accumulates transactions and eventually becomes too unwieldy to store or to synchronize. There are multiple proposals to prune transactions by substituting cryptographic proofs for transactions or blocks of transactions. Pruned transactions can be archived and need not be stored in all the replicas. Layer 2 schemes are touted as solutions to the scaling challenge of public blockchains. Such a system can be built for CBDC. Since the resulting solution introduces intermediaries into the claim on the central bank, it is beyond the scope of this paper.

Labs

Central banks can use existing labs or set up new labs to test the various proposals for CBDCs. The labs should use standardized terminology for metrics, a good start is the guidance published by the Hyperledger performance and scale working group.[14] The Digital Currency Global Initiative (DCGI), a collaboration between Stanford university and the UN with a membership of 190 countries and 170 private institutions, has an intention to create a lab to test CBDC proposals.

Cost Structure

Central banks need to analyze costs for operating CBDC at scale. Costs include recurring capital expenses and operating costs. Costs can be classified as creation of core infrastructure including platforms and smart contracts, network creation and operation, institutional and individual wallet creation and certification. By law, a central bank similar to the Federal Reserve System in the US has to operate in the black every year. When doing ROI calculations, central banks should include returns due to seigniorage and lowering system costs for printing and managing cash. Construction of infrastructure creates longer term and beneficial emergent effects that are not often quantifiable. A public private cost sharing of the networks is feasible because there is substantial benefit for the private sector in the new digital market structure.

Upgrades

In such a large ecosystem, it is practically impossible to guarantee that everyone in a network will be able to simultaneously upgrade to the latest version of the digital standards. While the

[14] "Hyperledger Blockchain Performance Metrics." https://www.hyperledger.org/wp-content/uploads/2018/10/HL_Whitepaper_Metrics_PDFVersion.pdf. Accessed 28 Aug. 2020.

core platform is expected to be upgraded in a controlled timeline, the on-ramp interfaces must be designed for present and future compatibility thus enabling the CBs and FSPs to implement their own upgrade timeframe. CDM and TTF will help portability across versions and across base platforms.

Financial Inclusion & CBDC

Financial inclusion is a hot topic among central bankers. There is a persistent percentage of the unbanked and underbanked even in developed economies. Some experts think that providing free direct central bank accounts will close this gap. The cost of creating a basic bank account will decrease through the provision of CBDC wallets at scale, increasing user enrollment. Instantaneous payments reduce the pressure on wage-earners who are dependent on timely employer payments for their other expenses. Benefit payments are easier with rCBDC, since it creates a digital rail for rapid payments. The availability of CBDC wallets on UADs as well as smart cards increase the accessibility of users to a rapid payment system. User friendly, easily accessible, and simple CBDC wallets are needed for people who are challenged by complex digital systems.

Circuit Breakers

Cyber attacks can quickly damage widely used critical digital infrastructure and hence affect the national economy. Economic and market crises can also have unintended consequences as demand can be rapidly transmitted through a frictionless payment system. Programmatic monitoring and automatic application of circuit breakers decrease the risk of systemic collapse due to such events. Circuit breakers are a common feature of today's equity markets. Lessons from such rapidly moving markets should be applied to the design of CBDC infrastructure.

To contact the authors

Vipin Bharathan: vipin@otc.digital or vip@dlt.nyc

Mani Pillai: mani@otc.digital or mani@swapshub.com

Glossary of Terms

AML	Anti-Money Laundering
API	Application Programming Interface
BC	Blockchain
CBDC	Central Bank Digital Currency
CCP	Central CounterParty
CDM	Common Domain Model
CFT	Combatting the Financing of Terrorism
CMSIG	Hyperledger Capital Markets Special Interest Group
CSD	Central Securities Depository
DCGI	Digital Currency Global Initiative
DLT	Distributed Ledger Technology
DTCC	Depository Trust & Clearing Corporation
DvP	Delivery vs Payment
ECB	European Central Bank
FATF	The Financial Action Task Force
FIX	Financial Information eXchange
FpML	Financial products Markup Language
FSP	Financial Services Provider
ISDA	International Swaps and Derivatives Association, Inc.
ISO	International Organization for Standardization
IWA	InterWork Alliance
KYC	Know Your Customer
LNS	Ledger Name System
LOLR	Lenders Of Last Resort
LSM	Liquidity Saving Mechanism

MPC	Multi-Party Computation
OTC	Over-The-Counter
PSP	Payment Service Provider
PvP	Payment vs Payment
rCBDC	Retail CBDC
RTGS	Real Time Gross Settlement
SDO	Standards Development Organization
SDX	Swiss Digital eXchange
SIG	Special Interest Group
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TTF	Token Taxonomy Framework
TvT	Token vs Token
T*vT*	Tokens vs Tokens
UAD	Universal Access Device
W3C	World Wide Web Consortium
wCBDC	Wholesale CBDC