Proposal of a Regulated Liability Network (RLN) Architecture to Support Settlement of Tokenized Assets, Liabilities and Transactions Using Tokenized Deposits and Wholesale CBDC (Real Digital)

Davi Castelo Branco Dias da Cunha[1]
Diego da Silva Oliveira[2]
João Paulo Aragão Pereira[3]
Ricardo Araujo de Almeida[4]
Wesley Rodrigues da Silva[5]

Abstract

This article presents the applicability of the Regulated Liability Network (RLN) in the settlement of financial transactions obligations through exchange of tokenized assets, including Real Digital — Wholesale CBDC (Central Bank Digital Currency). The main themes described in this article are related to the layers that make up the proposed architecture for Real Digital in Brazil, from advanced security using confidential computing, post-quantum cryptography (PQC) for digital signature, multiparty computing, KYC (Know Your Customer), KYT (Know Your Transaction), data privacy, and also to propose an interoperability layer, fungibility between different assets and compatibility between infrastructures based on distributed ledger technology (DLT) technology. This architecture must be compatible with EVM (Ethereum Virtual Machine), based on the guidelines of the Brazilian Central Bank, for DvP (Delivery versus Payment), PvP (Payment versus Payment) transactions, and even interoperability with current payment systems, such as PIX (BCB's faster payment system) or payments initiation entities via the Open Finance infrastructure. In summary, we present a feasible architecture designed to support a multi-assets model and an account-based "regulated liabilities" capable of supporting a programmable layer, digital money in the form of tokenized deposits or wholesale CB- DCs (Central bank digital currencies), "off-chain/on-chain" flow control and "on-chain"

1 davicunha@microsoft.com. Sr. Financial Service Industry (FSI) specialist – Latam.
2 dioliveira@microsoft.com. Global Black Belt for Security – Latam.
3 jopereira@microsoft.com. Innovation and Technology Specialist for Financial Service Industry – Latam.
4 ricardo.almeida@microsoft.com. Technology Strategist for Financial Service Industry (FSI) – Brazil.
5 wesley.rodrigues@microsoft.com. Security Solution Architect focused on Financial Service Industry (FSI) – Brazil.

finality of settlement using CBDCs. This proposed architecture can be used in several use cases ranging from tokenization of receivables to real estate's token negotiation, using Microsoft cloud platform.

Palavras-chave: CBDC; *real digital*; RLN*; security; interoperability*.

Part I - Foundation

1 Introduction

Based on (RLN, 2023), Central Bank Digital Currency (CBDC) work is under way to digitize central bank liabilities to enable their use by a wider range of economic actors. The potential for CBDC to disintermediate regulated private players is well documented in the literature. However, policy makers are investigating CBDC's potential to address a range of policy objectives, including improvements in financial inclusion and cross-border payments.

A CBDC may not anonymize transactions as some cryptocurrencies do, as by being able to monitor the transactions carried out with the CBDC, Governments and Central Banks will be able to combat tax evasion, money-laundering, and illicit economic activities more efficiently. Accordingly, CBDCs must maintain respect for fiscal secrecy and citizen data protection, as well as be executed on scalable, resilient, auditable, transparent, and extremely secure platforms. In a global scale of adoption, CBDCs should also be able to facilitate cross-border transactions, such as: currency exchange, global trade, multilateral trade agreements, international tourism, and cross-border investments (BIS, 2021).

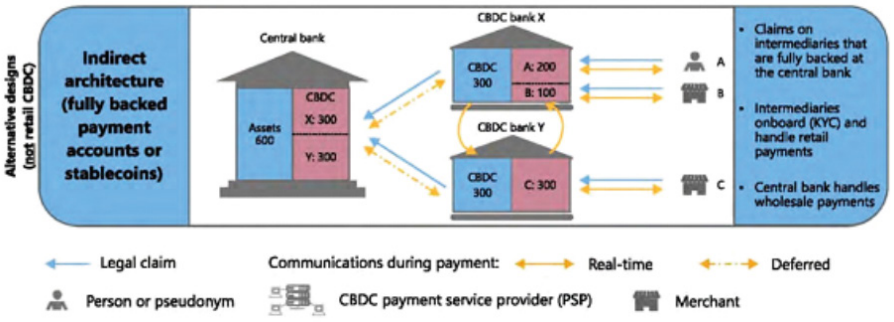
Wholesale CBDC refers to a digital currency that is issued by a central bank (BIS, 2018), in this case Brazilian Central Bank (BCB), and is exclusively designed for use by financial institutions (FIs), such as commercial banks and other financial intermediaries. Unlike traditional forms of money, such as cash and bank deposits, Brazilian wholesale CBDC (Real Digital) (CBDC, 2023) is a digital currency (e-currency) that is backed by BCB, which means that it is considered a risk-free asset. Real Digital can be used for settling financial transactions between financial institutions, as well as for facilitating the exchange of securities and other financial assets.

Real Digital is different from retail CBDC (BIS, 2021), which is a digital currency that is available for use by the general public (individuals or legal entities). Retail CBDC is designed to be used as a substitute for cash and traditional bank deposits, whereas Real Digital is used by FIs for interbank transactions and settlement purposes. In the case of retail e-currency, the tokenized real, to be issued based on the backing of deposits (assets), is a stablecoin based on the total reserve of assets, in the case of payment institutions, and a stablecoin based on the fractional reserve, in the case of banks.

The introduction of Real Digital is expected to improve the efficiency of financial market infrastructure, reduce transaction costs, and enhance the speed and security of financial transactions between FIs. It also provides to the BCB greater control over the monetary system and the ability to implement monetary policy more effectively. Figure 1 represents an indirect architecture similar to Real Digital ecosystem. Thus, CBDC is issued and redeemed only by BCB, but this is done indirectly to FIs. FIs, in turn, issue a claim to

consumers. FIs are required to fully back each claim with a CBDC holding at the BCB. In this case, BCB operates the wholesale payment system only.

Figure 1 – Alternative design for CBDC in 2 layers (BIS, 2021)



To accelerate the adoption of Real Digital, our foundational paradigm is an interoperable digital currency and digital assets ecosystem with CBDCs as its backbone. Digital currency interoperability is creating frictionless interoperability of different monies (e.g., CBDCs, tokenized loyalty points, tokenized deposits etc.), moving them efficiently using different rails (e.g., real-time gross settlement systems, permissioned distributed ledger technologies etc.) across different technology platforms. The transition towards digital currency interoperability is driven by innovations in three areas: CBDCs (RLN to support settlement of tokenized assets), embedded finance and banking as a service, and asset tokenization on DLT.

Embedded finance and Banking as a Service: Embedded finance is the presence of financial services such as lending or payment processing offered by non-financial providers in their business workflow. Current examples of embedded finance in a retail context include payment using credit card loyalty points, buy now pay later (BNPL) services, and point-of-service insurance. Banking as a service enables any business to extend financial products and services to their end consumers by partnering with licensed financial institutions. Additionally, with FSI customers developing their own loyalty ecosystem, the lanes between Retail and FSI have merged. In short, cross-company assets & identity exchange to offer financial services are becoming the norm. In order to meet this growing consumer demand, BaaS, and Embedded finance take a bilateral, API driven, approach.

Asset tokenization on Distributed Ledger Technology (DLT): While broadly, we are working to improve our customers' readiness in the digital asset landscape, digital currencies are a special asset class that require additional technology considerations. There has been a surge of adoption in stablecoins; a specific class of asset tokenization on both permissioned and permissionless DLT. Stablecoins can vary across different contexts. For example, financial institutions may offer a token denominated in the central bank currency and maintain its peg through assets held as bank deposits or short-term treasury bills. Retailers can peg their stablecoins by allowing for redemption to goods and services of an equivalent price in central bank money (e.g., a five dollars coffee may be five loyalty stablecoins).

Stablecoins on permissionless DLT (e.g., USDC on Ethereum) have already started to reduce cross-border payments costs, enable instant payouts to merchants of online

retailers, and are used extensively in the decentralized finance (DeFi) ecosystem. Stablecoins on permissioned DLT are gaining traction in the financial services industry (FSI). Fast and final inter-institution settlement, liquidity saving and heavily reduced reconciliation cost in intra-institution settlement, and retail conglomerate currencies are key emerging use cases in the market.

1.1 Objective

The main objective of this article is to demonstrate that it is possible to build a trusted asset fungibility network among participants (RLN – Regulated Liability Network), running on public cloud architecture, in order to support the settlement of tokenized assets, liabilities and transactions using tokenized deposits and Wholesale CBDC (Real Digital).

1.2 Expected contributions

Contribute to the Brazilian Central Bank as a technological support platform, by sharing this article, and also support the next test pilots and implementation of the RLN, in addition to the integration partitions of Brazilian financial institutions to the RLN.

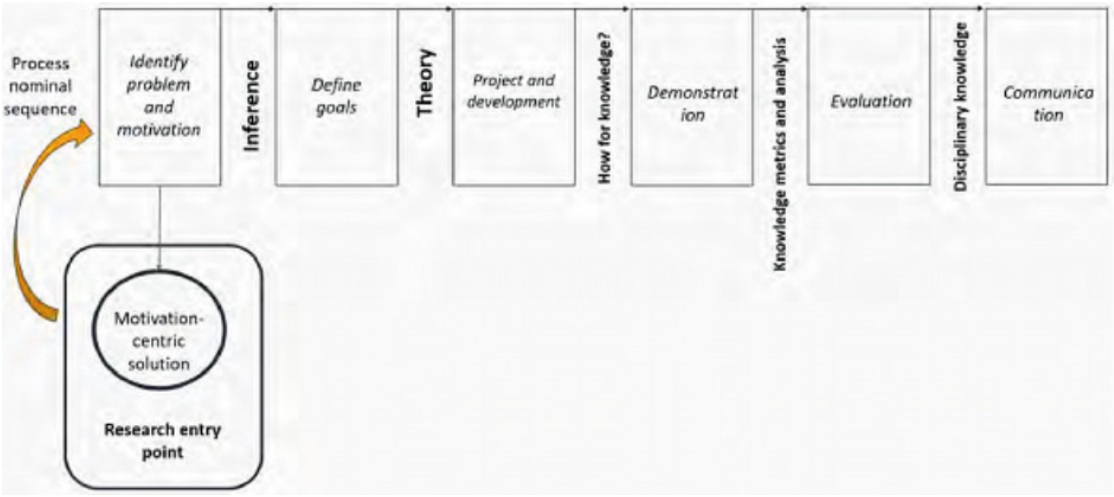
1.3 Document structure

The document is organized into three parts: Foundations, Proposal and Conclusion. In the first part, we have more four Chapters: Chapter 1 with the demands and goals, Chapter 2 describes the research method. Chapter 3 describes the basic concepts for a good understanding of the text. Chapter 4 discusses the implementations and pilots around the world related to CBDC and the present research. In the second part, we have one Chapter: Chapter 5 describes the proposal for this research and approach adopted. Finally, Chapter 6 presents use cases, conclusions and future works that may derive from this article.

2 Method

The method adopted to support the making of this article is the Design Science Research Methodology (DSRM) (Peffers *et al.*, 2007) in its nominal sequence. This method includes six steps: (1) problem identification and motivation; (2) definition of the objectives of a solution; (3) design and development; (4) demonstration; (5) evaluation; and (6) communication, as we can see in Figure 2. The method allows the search to start at any of steps (1), (2), (3) or (4), and therefore the nominal sequence of the process may not be followed. For this research, the solution sought is centered on motivation and, therefore, its first nominal activity was number one, based on BCB´s requirements.

Figure 2 – Nominal sequence of Design Science Research Methodology (DSRM)



2.1 Applying DSRM to this work

This section describes the applicability of DSRM to the construction of the Real Digital ecosystem based on RLN and Wholesale CBDC, from demand confirmation to communication.

2.1.1 Demand confirmation

Discussions and initiatives on the possible issuance of a currency by the BCB began in August 2020, which led to the creation of the Real Digital guidelines in May 2021. Since then, the BC has closely followed the growing trend of the use of financial transactions in DLT ecosystems in the Brazilian economy. Dialogue with the private sector and academia, especially through the LIFT Challenge, allowed for a detailed analysis of potential Real Digital emission models. As a result, in February 2023, the BC revised and published the Real Digital guidelines (BCB, 2023).

2.1.2 Definition of goals

Fundamental objectives for Real Digital are (BCB, 2023):

- **Multi-assets:** Use of a platform based on the DLT, in which predetermined assets of different natures (multi-asset) can be registered, as well as transactions between them.
- **Assets:** Deposits from Bank Reserve accounts, Settlement Accounts and the Single Account of the National Treasury; demand bank deposits; IP payment accounts; and Federal Public Securities (TFPs). The criteria for accessing Bank Reserves or Settlement accounts will be maintained, in accordance with current legal and regulatory discipline.
- **Transactions:** Issuance, redemption and transfer of the aforementioned assets, as well as financial flows arising from trading events. Transactions will include conditional and simultaneous settlement between the registered assets, in order to guarantee

Delivery against Payment (DvP), up to the end customer level (atomic settlement). Asset registries and transactions should allow for fragmentation, respecting the proximate pricing system, in order to maximize one of the potential benefits of DLT technology.

- **Programmable money:** Layers for registering assets, for settling their transfers and for protocols, as well as the smart contracts necessary for executing the proposed transactions.

2.1.3 Design

The Motivation-Centered Solution was triggered by a real demand, and can be treated with the development of an architecture, which allows the validation of hypothesis that serve as a basis for the solution design.

The definition of the model started with the architectural design of Real Digital. Real Digital ecosystem is composed five layers: **1** - Settlement; **2** - Interoperability; **3** - Protocol and Asset; **4** - Business Services; **5** - Presentation.

2.1.4 Demonstration

This activity consists of defining and sharing the standard architecture, based on Confidential Consortium Framework (CCF) (CCF, 2023), to support the interoperability layer in the Real Digital ecosystem.

2.1.5 Evaluation

The evaluation of the applicability of the RLN for Real Digital can be carried out later, via a pilot with the BCB, in order to implement the architecture proposed in this article. Metrics such as performance (TPS), applicability of PQC algorithms, interoperability between two or more DLT platforms, token fungibility can be used to qualify the proposed architecture.

2.1.6 Communication

Part of the work carried out by Microsoft will be published in 04/2023, by the BCB, through the pilot carried out in conjunction with Visa do Brazil — for Lift Challenge (Lift, 2023), where a solution for financing small and medium companies based on a decentralized finance (DeFi) protocol that could give this segment a viable way to access external financing sources. In addition, interoperability was built with PIX, for NFT mint payment related to agricultural commodity receivables, anti-fraud and anti-money laundering (AML) solution, digital onboarding with proof of life and use of decentralized digital identity, besides data privacy at all points in the network.

However, the idea of this work is to expand the previous MVP to an RLN network compatible with Real Digital with DvP, PvP, in order to be published and demonstrated in 05/2023 (workshop).

3 Theoretical Foundation

In this Chapter, we are going to cover the main topics about Blockchain, DLT (Distributed Ledger Technology), DvP (Delivery versus Payment), PvP (Payment versus Payment), Cross-border payments, RLN (Regulated Liability Network) and securities topics.

3.1 Blockchain x DLT

According to studies from Natarajan (2017), DLT and blockchain are two related but distinct concepts. DLT is a broader term that refers to any technology that allows multiple parties to have a synchronized, distributed and shared database, where transactions are recorded and validated through a decentralized network of nodes.

Blockchain is a type of DLT that uses cryptographic techniques to create a chain of blocks that store transaction data. Each block contains a cryptographic hash of the previous block, which creates a tamper-evident record of all transactions that have occurred on the network. The difference between blockchain and DLT is that blockchain is considered to be a form of DLT while not being the only form. With blockchain, you are still dealing with what amounts to a database. Blockchain technology is used in many applications, such as cryptocurrencies, supply chain management, and voting systems.

DLTs encompasses blockchain, but it can be implemented in many different ways, such as through a blockchain, a directed acyclic graph (DAG), or a hashgraph.

3.2 DvP, PvP and cross-border payments

DvP, PvP, and cross-border payments are all different types of financial transactions that occur between parties, with its specific characteristics.

DvP is a settlement mechanism used in financial markets, particularly in securities transactions, where the delivery of securities is done simultaneously with the payment of cash. In a DvP transaction, the seller of securities receives payment from the buyer, and the buyer receives the securities from the seller, all in one transaction. DvP reduces settlement risk, as it ensures that securities are not released until payment has been received, and payment is not made until securities have been received (RLN, 2023). In securities markets, expedited DvP settlement may be possible as digital assets proliferate and securities might be represented directly with the RLN.

PvP is a settlement mechanism used in foreign exchange transactions, where the payment of one currency is done simultaneously with the payment of another currency. In a PvP transaction, the two parties involved exchange currencies at an agreed exchange rate, and the payment is made in both currencies simultaneously. PvP reduces settlement risk, as it ensures that both parties receive their payments at the same time, eliminating the risk of one party defaulting on the transaction (RLN, 2023).

PvP is particularly important in the foreign exchange market, where high volumes of currency transactions occur every day, and the value of currencies can fluctuate rapidly. By using PvP, traders can minimize their risk and avoid potential losses due to currency price movements or counterparty defaults (RLN, 2023). RLN could settle obligations in multiple currencies on a PVP basis through atomic settlement arrangements. In FX Markets:

Expedited Payment PVP settlement may be possible through an RLN incorporating multiple central banks on the network.

Cross-border payments: Cross-border payments refer to any financial transaction that may involve the movement of money across different countries and regions, and it usually involves a currency exchange. Cross-border payments can be made between businesses, governments, and individuals and can be made for a variety of reasons, such as trade, remittances, or investment.

Cross-border payments can be sent through various channels, including wire transfers, online payment platforms, international money orders, and mobile money services. The process of cross-border payments can involve multiple intermediaries, such as banks, payment processors, and currency exchange providers. They also can be subject to various regulatory requirements, such as anti-money laundering and counter-terrorism financing laws and can involve additional fees and longer processing times compared to domestic payments. The fees charged for cross-border payments can include currency exchange fees, transfer fees, and intermediary bank fees (Shabsigh; Khiaonarong; Leinonen, 2020).

A recent paper from the European Central Bank (ECB) endorses that the interconnectivity of payment systems and CBDC could point toward the holy grail of cross-border payments. The RLN concept suggests a new global settlement service that could support both domestic and international use-cases, accelerating the adoption of cross-border payments in remittances scenarios (Bank, 2020).

3.3 CBDC: Wholesale x Retail

Wholesale CBDC is a type of CBDC that would be used to facilitate payments between banks, financial institutions and other entities that have accounts at the Central Bank itself. Wholesale CBDC is typically used in large value and high-frequency transactions, such as foreign exchange transactions, securities settlement, interbank transactions and large corporate payments. Wholesale CBDC is not generally available to the public and is limited to a select group of financial institutions. Retail CBDC is a type CBDC used for retail payments, for example between individuals, consumers and businesses, and akin to digital bank notes. Retail CBDC would be similar to physical cash, but in a digital representation format (BIS, 2023).

It would be accessible to the general public and could be used for a wide range of transactions, such as buying goods and services, paying bills, and sending money to friends and family. The main difference between retail and wholesale CBDCs are their target users and the proposed use cases. While Wholesale CBDC is intended for high-value transactions and can be used only by a select group of financial institutions, retail CBDC is intended for small, everyday transactions between individuals and businesses and accessible to the general public.

3.4 Multi-assets supported by Regulated Liability Network (RLN)

One of the interesting features of DLT is that it can express any arbitrary asset on a common, programmable infrastructure, such as a DLT and blockchain. The RLN thesis relies on the potential of shared ledger technology and provides the ability to incorporate multiple currencies into the system by including multiple central banks and regulated financial institutions from various locations. The network would use blockchain

technology to facilitate these transactions in a secure, transparent, and compliant manner, while also providing participants with access to real-time market data, analytics, and other tools to help them make informed investment decisions.

The specific assets that are supported in an RLN can vary depending on the network's design and the regulations governing the jurisdictions where the network operates. For example, a RLN might support a range of financial assets that are subject to regulation such as securities, derivatives, bonds, stocks, futures contracts, and several other financial assets that are typically traded on traditional financial exchanges. Also, the RLN provides the ability to represent the liabilities of additional participant types within the network—that is, regulated non-bank institutions including e-money providers and, soon regulated stablecoin issuers.

3.5 Atomic transactions

At the most primitive form of programmability, atomic transactions enable liabilities to transfer to and from a downstream layer. In its simplest form, such an atomic transaction could even be achieved through a custodial transfer into a wallet (or an account) with support for metadata. i.e., consider a scenario where a commercial bank wants to offer an 'escrow' payment service, where four directors of a private limited would all have to pay (1 peso) to meet an outflow. The funds flowing to the beneficiary should only begin when all the four directors have paid.

The commercial bank could be allowed to create an automated temporary wallet with Real Digital system by including metadata to transfer (4 pesos) to beneficiary's wallet upon adequate funds (CBDCs) being received. If adequate funds are not made available within the stipulated time, the funds should be sent back to the issuing wallets respectively. After setting up the wallet, not even the commercial bank can access the funds in the wallet. With such a provision, each director may transfer their (1 peso) to the same wallet address (set up by the commercial bank), and upon reaching (4 pesos) threshold, the automated transfer is conducted. This ensures that either all the directors pay, and the transaction is completed, or all fund flows are reversed (atomic).

3.5.1 Hashed Time Clock Contracts (HTLC)

HTLC is a solution that furthers the atomic transaction concept. HTLC can enable escrow capabilities with different asset categories. Let's say Maria and João want to exchange securities for CBDCs on the system. Maria would lock her CBDC into a HTLC with a hash of her secret HA ="hash"(SA) targeting the transfer to João's wallet. João would observe HA and lock his tokenized securities into another HTLC with Maria's hash HA targeting the transfer to Maria's wallet. Maria would need to submit her SA to unlock value targeted to her wallet by João. In doing so, Maria would reveal SA to everyone including João. João would then simply unlock the value targeted to his wallet since Maria had revealed her secret. Naturally, Maria's contract is locked in for a longer duration (usually measured in block height also known as hashed time) than João's contract. If the HTLC is not invoked for the prespecified duration, the value returns to the original wallet. In a more realistic case, Maria and João could be two financial intermediaries who essentially use the Real Digital system to exchange tokens without counter party risks. Unlike the previous example, where till the atomic settlement happens based on a criterion, through HTLC,

BCB can enable a broader range of swap operations involving multiple asset categories. Note that HTLC can also be used to create asset swap across multiple layers.

3.6 Role of RLN in tokenized deposits (financial institution coin)

Tokenized deposit in RLN is a Regulated Liability issued by a commercial bank. It is not a stablecoin, because it is not collateralized. It is a different form factor for recording a deposit liability. Each bank creating its own "coin" in isolation may not lead to an efficient market structure. An interoperable network of tokenized deposits might be preferred. In an RLN system, a tokenized deposit can potentially be used to facilitate fast and secure retail transactions between participating individuals and small businesses. A tokenized deposit can also potentially provide increased financial inclusion by providing access to digital payments and financial services to individuals and small businesses that may not have access to traditional banking services, through new channels such as digital payments wallets. A tokenized deposit can potentially play an important role in an RLN system by providing a new form of digital currency that can facilitate fast, secure, and efficient retail transactions, improve financial inclusion, and enhance overall liquidity and stability in the network.

3.7 RLN settlement procedure

The RLN scheme may offer potential for a new global settlement infrastructure based on regulated issuers and instruments. RLN would deliver continuous settlement and finality of settlement across multiple asset types. The settlement stage involves the transfer of funds from the participant's account to the counterparty's account. This transfer is done using the RLN's digital currency, which is typically a stablecoin that is pegged to a fiat currency, or a CBDC (central bank digital currency) issued by Central Banks (RLN, 2023).

Below the main settlement procedures applied to a PvP (Payment versus Payments) scenario between two users in two different Banks, called Bank A and Bank B (R3, 2023):

1. All participants, such as Bank A and Bank B, represent their liabilities on a distributed shared ledger (virtual ledger) as a fungible digital assets token (or tokenized deposit) that can be exchanged at par for a settlement asset (or a wholesale CBDC).

2. A Bank debits a payor's account in Bank A virtual ledger respective to the amount of the payment.

3. A Bank A exchanges Bank A liability token for a settlement asset (wholesale CBDC) in the amount of the payment.

4. A Bank A transfers the settlement asset to Bank B. At the same time, Bank A reserves decrease by the respective payment amount.

5. Bank B exchanges the settlement asset in the amount of the payment for a Bank B liability token (or tokenized deposit).

6. Bank B then credits payee's account in the Bank B virtual ledger in the respective amount of the payment.

The suggested Regulated Liability Network (RLN) is intended to provide on-chain, 24*7, programmable, final settlement in sovereign currencies, consisting of the liabilities of both public and private regulated financial institutions (RLN, 2023).

3.8 Security in RLN

This section explains the main topics linked with security applied to Real Digital.

3.8.1 Multiparty Computing (MPC)

Multiparty computing or privacy-preserving computation allows parties in a business relationship to share data, do computations, and arrive at a mutual result without divulging their private data. Azure services can help you build a multiparty computing solution. The solution can include cloud-based and on-premises resources (Microsoft, 2023b). Multiparty computing has the following attributes: 1) More than one company or organization is involved; 2) The parties are independent. 3) The parties don't trust one another with all their data; 4) All parties access a common computing and data storage platform; 5) Some processes must be private for some of the parties involved.

Multiparty computing includes different technologies that enable parties to transact securely over a network. One option is distributed ledgers. Blockchain is an example. Blockchain is a data ledger that can be shared between independent parties where all parties trust the data on the ledger. Transactions are collected in blocks with each block linking to the previous block. Some distributed ledgers don't use blocks. Each transaction can be linked to the previous transaction on the ledger.

Another possibility for multiparty computing uses hardware protected memory on the CPU itself. These regions, called secure enclaves, are cryptographically protected. This approach means that even a privileged administrator having full access to the server can't look at the process or the data inside those secure enclaves. Since secure enclaves have the capability to remotely attest themselves to other enclaves, you can design a multiple organization network where the system runs from the enclaves. This approach is called the trusted execution environment (TEE), based on Intel or AMD processors.

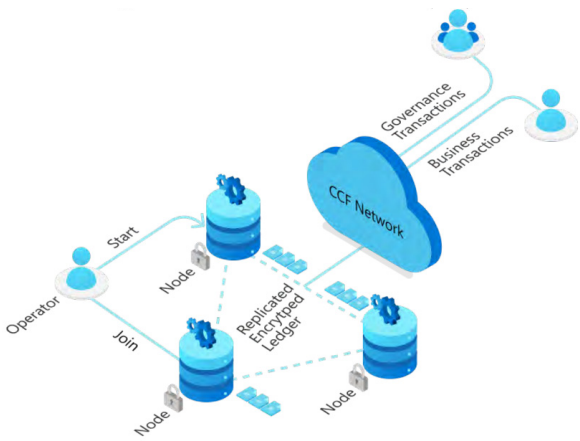
3.8.2 Confidential Computing and Confidential Consortium Framework (CCF)

Confidential Consortium Framework (CCF) (CCF, 2023) is an open-source framework for building highly available stateful services that provide programmable privacy protection and programmable governance, represented in Figure 3. CCF is built on TEEs. This positions CCF as a hardware encryption-based privacy enhancing technology. TEE is a secure enclave within a main processor. It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity, Data integrity — prevents unauthorized entities from altering data when any entity outside the TEE processes data, Code integrity — the code in the TEE cannot be replaced or modified by unauthorized entities. Unauthorized entities may include the computer owner (where TEE is itself running). These integrity conditions imply that even if BCB chooses to run a CBDC infrastructure on the public cloud, Microsoft as the cloud operator, cannot view the unencrypted data or alter the code in any form, unless authorized to do so. Furthermore, CCF unbundles governance from operation, enabling BCB to take a multi-cloud approach.

CCF's programmable privacy protection guarantees that only parties permitted by the BCB can view sensitive information as part of application operations. As an example, if BCB program a privacy rule to only allow the issuer and acquirer of Real Digital to see the identity and transaction details, CCF would ensure that such a privacy constraint is met. Using this privacy guarantee, operators (by default) will not be privileged to view transaction content (includes both identity of actors and transaction amounts), BCB can thus reduce a single point of failure by enabling multiple entities to operate Real Digital nodes without compromising on privacy. These entities may include banks, cloud providers, and the on-premises infrastructure of BCB itself (say within Clearing Corporation of Brazil).

The throughput of the system would depend on the connectivity between these entities. By provisioning an appropriate backbone network, these entities may be geographically separated to further enhance resilience during localized natural calamities. Finally, CCF supports both an account-based model and token-based model; owing to the design, it is a mere technicality in a CCF based system. We focus the narrative on token-based models to improve readability while noting that a corresponding account-based model exists for most of our designs outlined. In the DLT or non-DLT debate, CCF is a differ entiated alternative that provides the better of both worlds.

Figure 3 – Confidential Consortium Framework (CCF)



3.8.3 Post-Quantum Cryptography (PQC) and NIST

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce. NIST is responsible for developing and maintaining standards for a wide range of technologies, including cryptography. NIST is currently working on developing post-quantum cryptographic standards. In 2016 NIST published a call for papers aiming to improve FIPS-186-4 and other standards with post quantum resistance for public key processes (NIST, 2016). There are different approaches for post quantum algorithms, and these four have presented performance and feasibility: Lattice-based (finding multidimensional vectors for a given point), Code-based (decoding generic linear code), Hash-based (security of hash functions), and Multivariate (multivariate polynomials over a finite field). In 2022, NIST (NIST, 2022) selected four finalist algorithms:

- CRYSTALS-KYBER (Public-key Encryption and Key-establishment Algorithms)
- RYSTALS-Dilithium (Digital Signature Algorithms)
- FALCON (Digital Signature Algorithms)
- SPHINCS+ (Digital Signature Algorithms)

Central Bank Digital Currencies (CBDCs) are expected to be used by citizens for their daily transactions. Companies that deal with digital asset custody are responsible for securing large amounts of digital assets That value makes them a prime target for attackers, it important to ensure that the cryptographic algorithms used to secure these transactions are secure and resistant to quantum attacks to protect their clients' assets. Another concerning fact is that quantum computers are no longer theoretical machines. Companies like Microsoft, IBM, Intel and Google are already running working computers able to operate with hundreds to near a thousand qubits as stated by Gamrat and Bertels (2023).

3.8.4 Data Privacy and masking

Data privacy is an essential chapter of information security concerning collecting, using, and disclosing personal data. Data privacy has become a crucial issue in today's digital world, as personal data is frequently collected and used for various purposes, including marketing, research, and analysis. The rise of data breaches, cyberattacks, and identity theft has made data privacy an increasingly critical issue that individuals, businesses, and governments must address.

Data can be categorized into different types, including personal data, sensitive data, and non-personal data. Personal data is any information that can identify an individual, such as their name, address, or any government identification. Sensitive data is any information that is considered confidential or private, such as medical records, financial information, or legal documents. Non-personal data is any information that cannot be used to identify an individual, such as anonymous browsing data or aggregated statistics. In this case, the recommendation is to mask the data, essentially personal and sensitive data.

Masking is a technique that replaces accurate data with artificial or masked data. There are several masking techniques, including randomization, substitution, and encryption. Randomization involves replacing data with random values, making it difficult to link

the masked data to the original data. Substitution involves replacing data with similar but different values, such as replacing a name with a pseudonym. Encryption involves converting data into an encoded form that can only be decoded with a key. Masking techniques can be applied alone or in combination, depending on the type of data and the desired level of privacy.

Masked data can be stored using different architectures, including centralized and decentralized architectures. A centralized architecture is one where data is stored in a single location or server. This architecture can provide better control over data and easier management of security measures, such as firewalls and intrusion detection systems. However, it also creates a single point of failure, making it vulnerable to cyberattacks and data breaches.

On the other hand, a decentralized architecture distributes data across multiple servers or nodes, making it more difficult for cybercriminals to access or compromise. Decentralized architectures also provide better resilience against data loss, as data is replicated across multiple nodes. However, it can be more challenging to manage data security measures in a decentralized architecture, and it can also be more challenging to enforce privacy policies and regulations.

Masking is essential for protecting personal and sensitive data by replacing accurate data with artificial or masked data. It can be applied to all types of data and used in combination with other techniques, such as de-identification with Microsoft Presidio (Microsoft, 2018), to provide a more comprehensive privacy protection approach. Different masking techniques, such as randomization, substitution, and encryption, can be used depending on the type of data and the desired level of privacy. Masked data can be stored using different architectures, including centralized and decentralized architectures, each with its benefits and drawbacks. Organizations must carefully consider their data privacy needs when selecting an architecture.

3.8.5 Decentralized digital identity

Our digital and physical lives are increasingly linked to the apps, services, and devices we use to access a rich set of experiences. This digital transformation allows us to interact with hundreds of companies and thousands of other users in ways that were previously unimaginable. But identity data has too often been exposed in security breaches. These breaches affect our social, professional, and financial lives. Every person has a right to an identity that they own and control, one that securely stores elements of their digital identity (Microsoft, 2023c) and preserves privacy.

Today we use our digital identity at work, at home, and across every app, service, and device we use. It's made up of everything we say, do, and experience in our lives, purchasing tickets for an event, checking into a hotel, or even ordering lunch. Currently, our identity and all our digital interactions are owned and controlled by other parties, in some cases, even without our knowledge. Every day citizens grant apps and devices access to their data. A great deal of effort would be required for them to keep track of who has access to which pieces of information. On the enterprise front, collaboration with consumers and partners requires high-touch orchestration to securely exchange data in a way that maintains privacy and security for all involved.

Standards-based Decentralized Identity (DiD) system can unlock a new set of experiences that give users and organizations greater control over their data—and deliver a higher

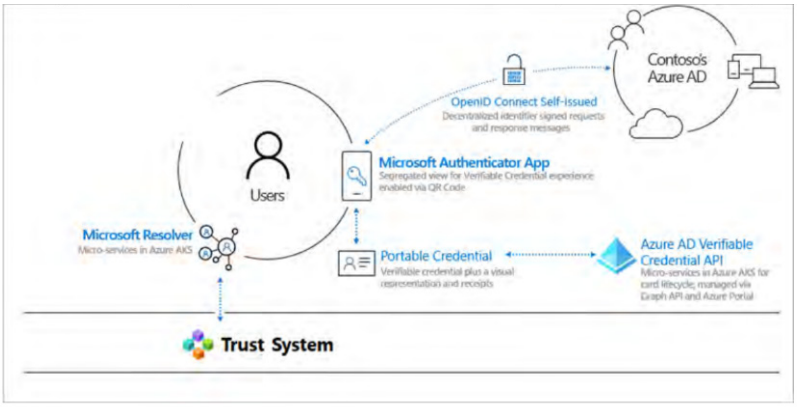
degree of trust and security for apps, devices, and service providers. This kind of approach is essential to build a robust and secure CBDC for any country. DIDs are user-generated, self-owned, globally unique identifiers rooted in decentralized systems like ION (identity overlay network) or web (Microsoft, 2023d). They possess unique characteristics, like greater assurance of immutability, censorship resistance, and tamper evasiveness. These attributes are critical for any ID system intended to provide self- ownership and user control.

A verifiable credential solution uses decentralized credentials (DIDs) to cryptographically sign as proof that a relying party (verifier) is attesting to information proving they are the owners of a verifiable credential (W3C, 2022). In short, verifiable credentials are data objects consisting of claims made by the issuer attesting to information about a subject. These claims are identified by schema and include the DID issuer and subject. The issuer's DID creates a digital signature as proof that they attest to this information. In the case of Real Digital, a DID could be the government or even the banks, the main point is that the BCB would have to trust in those DIDs and different DIDs inside the CBDC ecosystem must to trust each other.

3.8.5.1 How Decentralized Identity works

For a secure CBDC, we need a new form of identity. We need an identity that brings together technologies and standards to deliver key identity attributes like self-ownership and censorship resistance. These capabilities are difficult to achieve using existing systems. To deliver on these promises is necessary a technical foundation made up of seven key innovations. One key innovation is identifiers that are owned by the user, a user agent to manage keys associated with such identifiers, and encrypted, user-controlled datastores. Figure 4 represents a decentralized system for identity:

Figure 4 – Example of Verifiable Credential environment (Microsoft, 2023a)



1. **W3C Decentralized Identifiers (DIDs):** IDs users create, own, and control independently of any organization or government. DIDs are globally unique identifiers linked to Decentralized Public Key Infrastructure (DPKI) metadata composed of JSON documents that contain public key material, authentication descriptors, and service endpoints.

2. **Trust System:** In order to be able to resolve DID documents, DIDs are typically recorded on an underlying network of some kind that represents a trust system. Microsoft currently supports two trust systems, which are: A) **ION** (**Identity Overlay Network**) — it is a layer 2 open, permissionless network based on the purely deterministic Sidetree protocol, which requires no special tokens, trusted validators, or other consensus mechanisms; the linear progression of Bitcoin's time chain is all that's required for its operation. We have open-sourced an npm package to make working with the ION network easy to integrate into your apps and services. Libraries include creating a new DID, generating keys and anchoring your DID on the Bitcoin blockchain; B) **DID:Web** — it is a permission-based model that allows trust using a web domain's existing reputation.

3. **DID User Agent/Wallet:** Microsoft Authenticator App. Enables real people to use decentralized identities and Verifiable Credentials. Authenticator creates DIDs, facilitates issuance and presentation requests for verifiable credentials and manages the backup of your DID's seed through an encrypted wallet file.

4. **Microsoft Resolver:** an API that looks up and resolves DIDs using the did:web or the did:ion methods and returns the DID Document Object (DDO). The DDO includes DPKI metadata associated with the DID such as public keys and service endpoints.

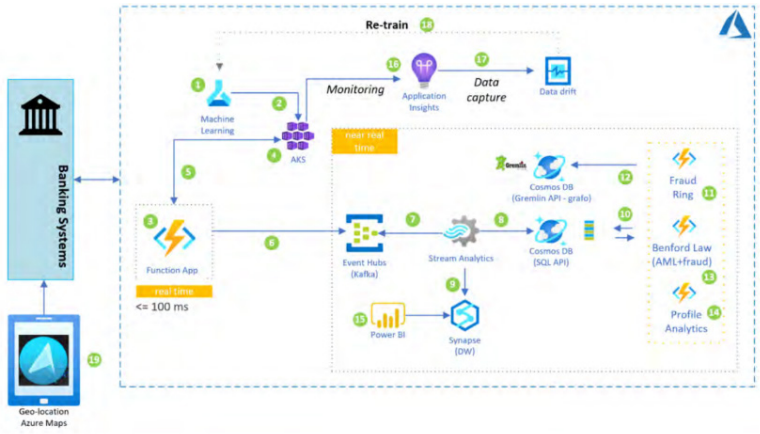
5. **Enter Verified ID Service:** an issuance and verification service in Azure and a REST API for W3C Verifiable Credentials that are signed with the did:web or the did:ion method. They enable identity owners to generate, present, and verify claims. This forms the basis of trust between users of the systems.

By adopting Decentralized Identifiers (DIDs) in CBDCs ecosystems, the Central Bank will be able to work with financial institutions to perform peer-to-peer verifications during financial transactions. When one institution initiates a transaction, the receiving institution or company can ensure that the customer who initiated the transaction is who they claim to be without using sensitive data from personal e-wallets. This approach goes beyond helping to strength mechanisms to protect customers data, identity, and assets, but also strength the combat against frauds, money-laundering and other financial crimes, and this approach will also facilitate the full potential of the Open Finance integrated with the CBDCs ecosystems while keeping customer with the control of their data.

3.8.6 Anti-fraud and anti-money laundering for digital assets such as real digital

The architecture represented in Figure 5 is part of an off-chain anti-fraud and AML engine for digital assets, like Real Digital or others such as receivables tokenized. It was based on four different scores of the same payload, used in the Lift Challenge (BCB, 2022) for the delivered project: our work proposed a solution for financing small and medium companies based on a decentralized finance (DeFi) protocol that could give this segment a viable way to access external financing sources. The payload for testing was composed for 15 fields: 1) source wallet; 2) destination wallet; 3) value of transaction; 4) gas fee; 5) timestamp; 6) type of transaction; 7) latitude x longitude; 8) source country; 9) destination country; 10) source of taxonomy of user (end or legal entity); 11) destination of taxonomy of user (end or legal entity); 12) initial score from onboarding digital (e-KYC); 13) mac address of mobile phone; 14) country match; 15) age of account. The characteristic of this engine is continuous learning based on Reinforcement Learning (Microsoft, 2022b), and is explained in the following sequence:

Figure 5 – Reference architecture for anti-fraud/AML related to digital assets (Microsoft, 2022a)



1. Training a supervised model (e.g., Random Forest or XGBoost). If the BCB or FI does not have data labels, clustering algorithms (unsupervised) can be used.

2. Implementation of trained model.

3. Serverless service receives a request from other modules, such as Analytics, Inbound/Outbound, or banking systems.

4. Call of the trained model to generate score, running on containers, to calculate the fraud probability.

5. The model returns to fraud prediction in a time less than or equal to 100ms.

6. Serverless service returns an output to start the analysis process, and posts the payload and score prediction.

7. Service consumes the event.

8. The event is processed and the result is sent to database (SQL API).

9. The event is processed and the result is sent to data warehouse, for further analysis.

10. Change Feeds in database triggers serverless service to run the rules and generate 3 more different scores.

11. Serverless service is used to assemble the fraud ring, based on transaction and other information about value, digital wallets, such as the status of each individual in relation to credits, for example.

12. The data is persisted in graph mode in database (Gremlin API).

13. A Python code for Benford Law (USP-IME, 2022) evaluates the value of each transaction, in relation to the first and second digits. Results are uploaded and stored in database.

14. Serverless service Analytics concentrates different information and creates a purchase and usage profile, crosses it with geolocation, social networks and receives, via API, if the user used proof of life in the authorization and authentication process.

15. Interactive visualization of reports and dashboards, near real-time.

16. Requests to APIs are monitored.

17. Data from new requests are collected in order to detect Data Drift.

18. If the drift exceeds a threshold, the model's automatic retrain is activated.

19. Optionally, the financial institution could want to add the location in each transaction and pass to Profile Analytics algorithm.

3.9 Offline CBDC

There are two categories of offline CBDC solutions (1) non-respendable and (2) respendable. **Non-respendable**, as the name suggests, allows for an issuer to transfer CBDCs in an offline manner to an acquirer who would in turn need to connect to the Real Digital system to spend it. In a respendable architecture, the acquirer could in turn spend offline their funds after receiving it. While both scenarios must prevent double spending, non-respendable only needs to support a single offline spending while respendable needs to support multiple offline spending. In a non-respendable scenario, the acquiring device would simply procure the authorization of spending using a HSM (hardware security module).

Respendable scenarios require two mutually authenticatable cards that perform a similar operation. Although tamper-proof hardware is used for offline CBDCs, to reduce risks, a commercial bank or e-money service provider may be involved as an intermediary to offer offline CBDC functionalities. To the extent possible, in the upper two-layers of the Real Digital system may be recommended to issue offline CBDCs in a custodial manner i.e., offline CBDCs are held in wallet addresses of intermediaries. First, this limits the impact on the online CBDC ledger as all offline CBDCs are recorded as being held by the corresponding intermediaries. Transfers in and out of these offline systems happen online. Secondly, it enables innovation in the offline transaction processing space by allowing for the intermediaries to create their own secure transaction capabilities. This aligns incentives (e.g., preventing double spending is aligned with the business objective of offline CBDC issuer).

3.10 Open Finance interoperability

CBDC is a relatively new concept, and its implementation is still being explored by central banks around the world. Open Finance, on the other hand, refers to the use of open APIs, sharing of banking customer data and transactions and decentralized financial technologies to create a financial services ecosystem truly interoperable. Open finance and CBDC interoperability can potentially create a new financial ecosystem that is more inclusive, efficient, and innovative.

Open finance platforms could integrate CBDC as a form of payment or settlement, allowing users to hold and transact in CBDC alongside other digital assets. This

would enable users to take advantage of the benefits of CBDC, such as fast and secure transactions, while also benefiting from the flexibility and innovation of open finance platforms.

Payment initiators are entities that initiate payments on behalf of users in the financial system. In open finance, payment initiators can be an authorized entity that has access to payment APIs from third-party financial institutions, with given a customer's consent, can initiate payments on behalf of their customers. These could include fintech companies, payment processors, and other financial intermediaries. With the introduction of CBDC and tokenized deposits, payment initiators would be able to initiate and receive payments in digital token, which could potentially provide numerous benefits over traditional payment methods. For example, CBDC payments could be settled in real-time, 24/7, which could significantly improve the speed and efficiency of payments. Additionally, CBDC-style payments could be more secure than traditional payment methods, as they are backed by the central bank and are immune to issues such as counterfeiting, double-spending or even market liquidity risks.

Open finance platforms could enable decentralized exchanges for CBDC, allowing users to trade CBDC with other digital assets or traditional currencies in a peer-to-peer manner. This would provide a more efficient and cost-effective way for users to access CBDC and could potentially increase liquidity for CBDC.

The interoperability between CBDC and open finance can also provide additional benefits. Here are some possible scenarios:

Cross-border payments: With the interoperability of CBDC and open finance, it will be possible to make cross-border payments instantly and at a lower cost than traditional methods. This could be a game-changer for international trade and could increase financial inclusion. Integration with BCB PIX payments system, could potentially accelerate use of PIX for Cross-borders transactions (PIX International).

Programmable money: CBDC could be programmed to automatically execute smart contracts, enabling a wide range of automated financial services. This would enable businesses to streamline operations, launch innovation, increase efficiency, while reducing transaction costs.

Decentralized Finance (DeFi): With the interoperability of CBDC and open finance, it would be possible to create DeFi platforms that integrate with the traditional financial system. This could make DeFi more accessible to mainstream users and could bring more liquidity into the DeFi ecosystem.

However, interoperability between CBDC and open finance could pose some challenges as well. Some of the challenges include the need for standardization, data privacy and security concerns, and changes to regulatory compliance. Central banks, financial institutions and ecosystem will need to work together to develop a framework that ensures the seamless interoperability of CBDC and open finance while addressing these challenges.

3.11 Real Time Payments (PIX) interoperability

PIX (BCB, 2023a) is a real-time payment system developed by the Brazilian central bank that enables instant payments 24/7. PIX uses a centralized platform to enable fast and

secure payments between individuals and businesses, and it has gained widespread adoption in Brazil since its launch in 2020. CBDC, on the other hand, as a digital form of fiat currency issued and backed by a central bank.

Real-time payments systems like PIX (Instant payments) in Brazil and CBDC can be interoperable, potentially providing numerous benefits to users and financial institutions, and even create a more efficient and convenient payment ecosystem. CBDC can also improve instant payments, because it is backed by the central bank, it can provide increased trust, security and reliability compared to other forms of digital payments.

However, to achieve interoperability between PIX and CBDC, will require collaboration between regulators (central banks), banks, regulated fintechs and payment intermediaries to develop a common framework that ensures the secure and efficient exchange of payments. It will be necessary to establish common standards and protocols that enable the seamless exchange of payments between the two systems. Additionally, regulatory compliance and standardization will be necessary to ensure the customer's security and reliability of payments and protect against issues such as money laundering and fraud scenarios.

3.12 ISO 20022

ISO 20022 (Microsoft, 2020) is a widely adopted standard for financial messaging that provides a common language for exchanging financial information between different systems and institutions. It is a structured data model that defines a standardized set of message formats, data elements, and business processes for financial transactions. Additionally, ISO 20022 supports rich data sets, which can include information beyond the basic payment details such as transaction purpose, invoice information, and remittance details. This additional information can help to enhance the accuracy and speed of transaction processing and can enable the automation of additional business processes.

CBDC can also benefit from using the ISO 20022 standard for its messaging and communication protocols. The use of ISO 20022 in CBDC systems can also help to ensure compatibility and interoperability between CBDC systems, eventually across different regions and jurisdiction, which is essential for creating a seamless and efficient payment ecosystem and enable the secure, fast and efficient exchange of payments. ISO 20022 could enable CBDC payments to be processed and settled quickly, potentially in real or near real time, and securely across different platforms and institutions.

However, achieving interoperability between CBDC systems using ISO 20022 will require strong collaboration between regulators, central banks, and payment institutions to develop a common framework that ensures the secure and efficient exchange of payments, adherence to regulatory compliance and standardization to ensure payments security, as well as, protection against money laundering and payments fraud.

4 State of the Art and Practice

This Chapter discusses Wholesale and Retail CBDC use cases as well as mCBDC (multi-CBDC) cases.

4.1 Countries using CBDC

Until March of 2023, there are eleven countries (CBDC-TRACKER, 2023) that have officially launched their CBDCs:

- **Bahamas:**
  - Launched the Sand Dollar (Bank of Bahamas, 2023) in October of 2020 becoming the first country in the world to officially launch a CBDC on a national scale.
  - Bahamas' case is based on retail, and they are using conventional centrally controlled databases and DLT as the underlying technology.
  - Their CBDC is directly claimed on Central Banking, but payments and real- time transactions are facilitated by financial intermediaries, including commercial banks.
  - As a next step, they are working to achieve interoperability between its various wallet providers.
  - The Bahama's motivations for the CBDC pilot include improving financial inclusion and strengthening security against money laundering or illicit economic activities.
- **Eastern Caribbean Central Bank:**
  - **Members:** Antigua and Barbuda, Anguilla, Dominica, Grenada, Montserrat, Saint Kitts and Nevis, Saint Lucia and Saint Vincent and the Grenadines.
  - They launched DCash (ECCB, 2021) in March 2021 for four of their eight members, the last of the eight countries to adopt DCash was Anguilla in April of 2022. With DCash, the Eastern Caribbean has become the first currency union central bank to issue digital cash.
  - Eastern Caribbean Central Bank case is based on retail, and they are using only DLT as the underlying technology to run DCash.
  - Their CBDC is directly claimed on Central Banking, but payments and real- time transactions are facilitated by financial intermediaries including commercial banks.
  - Financial inclusion is the primary goal of the Eastern Caribbean Currency Union. This is followed by enhancing anti-money laundering and combating the financing of terrorism measures and expanding banking across difficult terrains.
- **Jamaica:**
  - Launched the Jamaican Digital Exchange or JAM-DEX in February of 2022 and started the rollout in May of 2022.
  - Jamaica's case (Bank of Jamaica, 2020) is based on retail, and they are using only conventional centrally controlled databases as the underlying technology, at this moment they are not using DLT.

- Their CBDC is directly claimed on Central Banking, but payments and real- time transactions are facilitated by financial intermediaries including commercial banks.

- The primary motivation associated with developing the CBDC was to reduce the storage and handling costs of cash usage. JAM-DEX is expected to save about seven million US dollars per year, which Jamaica currently spends on replacing, storing, and handling cash.

- **Nigeria:**

  - Nigeria launched Africa's first digital currency, the eNaira in October 2021. A phased approach was adopted to the rollout. During the initial phase, only bank account holders could access eNaira. The next phase includes expansion to the unbanked, with unstructured supplementary service data and offline payments to be released in the medium term.

  - Nigeria's case is based on retail, and they are using only DLT as the underlying technology to run e-Naira (Bank of Nigeria, 2021).

  - The eNaira is expected to help Nigeria reach its target of increasing financial inclusion from 64 percent to 95 percent. It is projected that a well-managed eNaira could add twenty-nine billion dollars to the GDP (Gross Domestic Product) over the next ten years.

4.2 LACChain

LACChain (LACChain, 2023a) is a global alliance integrated by different actors in the blockchain environment and led by the Innovation Laboratory of the Inter-American Development Bank Group (IDB LAB) for the development of the blockchain ecosystem in Latin America and the Caribbean.

Looking at the problematic process related to traceability, regulatory and compliance of Cross Border Payments, LACChain in partnership with Citi Innovation Labs and ioBuilders have built a functional Proof of Concept for Cross Border Payments envisioning the time reduction of this kind of operation.

The solution consists in the tokenization of fiat money linked to different currencies between different countries for International Banks and CBDCs with the possibility of being programmed for transfer, conditional payments, or remittances. The fiat money can be tokenized by financial institutions assuring automation, transparency, traceability, and efficient reconciliation through the entire transaction lifecycle.

Some benefits (LACChain, 2023b): 1) Utilize e-money in the form of ERC20 tokens deployed by an authorized entity over a permissioned blockchain network; 2) Perform KYC and AML of accounts, before whitelisting, to send and receive e-money; 3) Integration with CitiBank's WorldLink API to perform rate exchange queries, payment execution and payment status queries.

With solutions like the one created by LACChain, cross-border financial operations would be much simpler, and the use of this concept by Central Banks for their respective CBDCs would make the cross-border trading and tourism much more robust and accessible for every person and organization across the world, besides removing the need to tokenize fiat money, since the CBDC would already be its digital representation.

4.3 Discussion

Like 31 other countries (Atlantic-Council, 2023), the pilot initiated by the BCB (BCB, 2023b) will cover wholesale market and the following financial products: deposits from the Bank Reserves, Settlement Accounts and Single Accounts of the National Treasury; bank demand deposits; payment accounts of payment institutions; and Federal Public Bonds. It is a good start to enable the tokenization of several different kinds of assets and its settlement through CBDC currency.

BCB is going to implement a multi-asset DLT since the beginning of their pilot to make it possible to add different kinds of financial products and assets, also thinking about topics that will enable PvP and DvP based on current regulation. It will be ready to be adapted to future regulation which will make it possible to fast attach new financial services linked to physical assets. In this way, it will be easier to transfer assets' owners of the products being negotiated as part of the transactions' flow, going beyond of the payment, transfers, and settlement transactions that are the main scope of the majority of CBDCs projects.

As per the different kinds of implementations of CBDCs by Central Banks around the world, it would be very important to have a coordinated global governance effort to make it easier for the central banks to build integrations in the future. Furthermore, enable the knowledge exchange between the countries more advanced in their CBDCs, mainly in security, resilience and reliability.

Part II - Proposal

5 Proposal

This chapter comprises a reference architecture for an multi-participants, multi-assets, and interoperable RLN.

5.1 Reference architecture for Real Digital in Brazil

In this section we propose an architecture for a Regulated Liabilities Network (RLN) implementation on a multi-node, multi-assets, multi-blockchain, and interoperable platform, as show in Figure 6. The initial proposal is that central banks issue a whole CBDC on a large-scale, private, permissioned, Ethereum-based (EVM) network in which central bank-appointed intermediaries act as nodes. These intermediaries would work together on a single platform in coordination with Central Bank as providers/holders of the currency (CBDC).

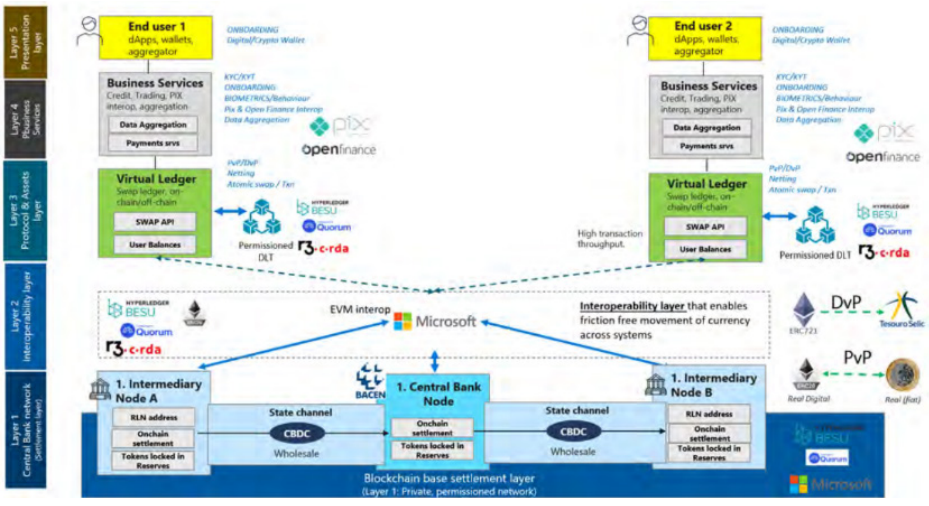
The initial RLN configuration would be comprised of Regulated entities (Banks, regulated payments institutions etc.) who would be responsible to issue, hold and trade multiple digital assets, based on consumer's deposits and applying common standards, as defined by RLN rules and policies. This configuration will allow for regulated entities to compete to offer innovative services to citizens and businesses.

RLN configuration is a multi-party system, with each participant (banks) holding their own partition (an independent blockchain layer) in order to provide a purpose-built and programmable system upon which to deliver decentralized blockchain applications using technologies such as Smart Contracts. This system solves the layers of complexity and interoperability that exist between multiple layers of DLT and blockchain technologies and provides an enterprise-grade and scalable platform.

Our functional architecture is divided into five different and complementary layers:

- **Layer 1: Central Bank network** (**Settlement**) – There is one base settlement layer on a permissioned DLT, managed and governed by the Central Banks, providing settlement finality, using wholesale CBDCs reserves (Consensys, 2020)

Figure 6 – Regulated Liability Network (RLN) and CBDC layers (modified by Consensys, 2020; Schär, 2021)



- **Layer 2: Interoperability** – It provides an orchestration layer over multiple DLT/blockchain ledgers, enabling interoperability between multiple decentralized application, multiple protocols and different regulated assets types, backed by different DLT standards, based on CCF (CCF, 2023).

- **Layer 3: Protocol and Assets** – Each intermediary and participant (Bank, regulated fintech etc.) operates its own Virtual Ledger or side chain, implemented with DLT/Blockchain technology, to provide a local ledger capable of controlling on-chain/off-chain operations, managing user balances, converting different assets types including tokenized deposits (a type of token).This layer also enables PvP (payments versus payments) and DvP (delivery versus payments) operations, as well as providing other functions to enable more scalable and autonomous operations for end-users of decentralized applications (also called dApps). The virtual ledger also ensures that systems remain consistent with standard policies and rules applicable to tokenized deposits and other regulated liabilities and assets. The virtual ledger shall provide easy integration, interoperability, and coexistence with banks' core banking systems through standard application programming interfaces (or APIs).

- **Layer 4: Business Services** – It is comprised of application-level services and functions to enable services in layer 1, such as Data aggregation services, KYC (know-your-customers), KYT (know-your-transactions), anti-fraud detection and services that provide interoperability and connectivity with current systems (such as BCB PIX).

- **Layer 5: Presentation** (**End Users**) – At the top we find many different end user interfaces, offered by banks, credit unions, regulated fintechs, aggregators and other providers, each in competition with each other, in control of customer relationship and with their own special functionalities, in order to provide the best possible end user experience via frictionless digital onboarding processes, and ability to manage tokenized deposits and other multiple types of assets, in different types of user wallets (Consensys, 2020).

5.2 Discussion

This chapter presents our reference architecture for the Brazilian Real Digital, in five layers, using the RLN network, feasible to be implemented in a scalable public cloud, such as Microsoft Azure (CCF, 2023). The architecture considers the provision of a digital wallet for the end user to carry out financial transactions, in **layer five** (retail side). A layer of application services, or **layer four** that offers, among others, customer identification services, authentication, anti-fraud/AML capabilities, besides integration with SFN (National Financial System) systems, such as PIX and Open Finance. In **layer three**, there is a dedicated distributed ledger structure for each network participant, responsible for managing user balances, applying policies and business rules, converting tokens and controlling financial transactions for the end user. At **layer two**, an interoperability model is proposed, which offers an interconnection layer between the BCB network and the individual network of participants (financial institutions). Lastly, **layer one** provides a base settlement layer, based on DLT technology (EVM and Hyperledger Besu client compatible) and managed by the BCB.

Part III - Conclusion

6 Use Cases, Conclusion and Future Work

This Chapter is to discuss use cases, final remarks and future work.

6.1 Use cases applied based on Real Digital

Real Digital has a wide range of use cases that can benefit different segments of society, from high-net-worth individuals to unbanked and informal businesses, showed in Figure 7. Here are some of the key use cases of Real Digital followed by each category.

- **Private Banking:** for high-net-worth individuals, Real Digital can offer increased privacy and security for cross-border payments. Transactions can be conducted seamlessly and with reduced friction, and Non-Fungible Tokens (NFTs) can be issued to represent high-value assets such as art, collectibles, and real estate, providing a new level of liquidity and flexibility to private banking.

- **Corporate Banking:** it can enable transparent and secure trade finance, reducing the risk of fraud and increasing efficiency. Payments and goods can be tracked along the supply chain, providing greater visibility and confidence to buyers and sellers. Moreover, Crowdfunding can be powered by Real Digital, enabling companies to raise funds in a decentralized and transparent manner.

- **Commercial Banking:** for Small and Medium-sized Businesses (SMBs) can benefit greatly from Real Digital. Cross-border payments can be facilitated through Real Digital, enabling SMBs to access international markets with greater ease and lower costs. Additionally, Real Digital can be used to track supply chain information, providing greater visibility and control over operations.

- **Retail Banking:** it can provide an accessible and secure way for individuals and households to manage their cross-border payments. Digital wallets can be created, providing a more convenient and cost-effective way to send and receive money internationally. Additionally, Know Your Customer (KYC) and Know Your Transaction (KYT) processes can be automated, reducing the cost and complexity of compliance.

- **Low-Income/Unbanked/Semi-Banked:** it can offer a more inclusive and equitable financial system for those at the lower end of the social pyramid 7. Cross-border remittances can be facilitated through Real Digital, providing a low-cost and secure way for people to send and receive money. Anti-fraud measures can be implemented, reducing the risk of scams and increasing trust in the financial system. Informal businesses can also benefit from Real Digital, providing them with access to formal financial services and reducing their dependence on cash.

- **Informal businesses:** it can support informal businesses by providing them with access to formal financial services, such as cross-border payments and digital wallets. This can help them grow their businesses and improve their financial stability.

- **Faster access to international markets:** it can offer faster and more efficient cross-border payments, enabling businesses and individuals to access international markets in a more cost-effective way.

- **Advanced Anti-Fraud Measures:** Real Digital can use advanced machine learning algorithms to detect patterns of fraud, such as detecting unusual transactions or identifying patterns of fraudulent activity. Real Digital can use blockchain technology to provide transparent and immutable transaction records, making it easier to track and investigate fraudulent activity.

- **KYC/KYT Measures:** Real Digital can require users to verify their identity through government-issued identification documents or biometric authentication. This process can use third-party services to conduct background checks on users and ensure they are not on any watchlists or have a history of fraudulent activity. Also, Real Digital can implement transaction monitoring tools to track the source of funds and ensure that they are not derived from illegal activities.

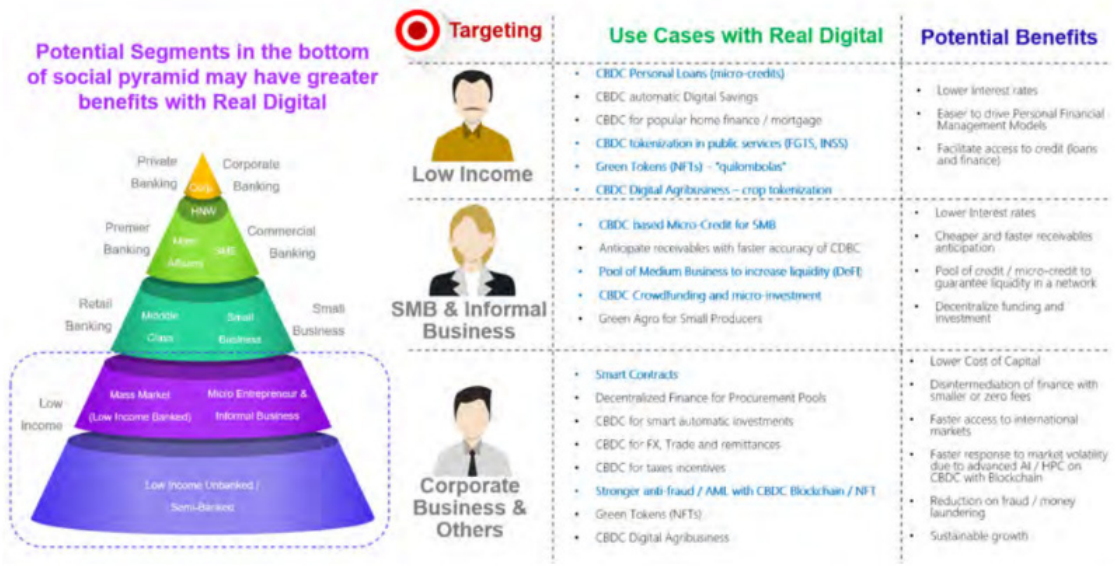
- **Enhanced Due Diligence (EDD):** This involves conducting a more in-depth investigation into customers and their activities when there is a higher risk of money laundering or fraud. This can include obtaining additional documentation and conducting site visits.

- **Compliance with Regulatory Requirements:** Real Digital can ensure compliance with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF)laws by implementing measures such as transaction monitoring, KYC/KYT measures, and reporting suspicious activity to regulatory authorities. Real Digital can work with regulatory authorities to ensure that the platform is up to date with any changes to regulations and to implement necessary measures to comply with new requirements.

All the use cases are connected directly with the Financial Action Task Force (FATF), which provides guidance on AML and CTF measures that can be implemented by financial institutions, including those working with virtual assets such as CBDC (FATF, 2019a). Also, the Financial Action Task Force (FATF) published guidance on risk management and compliance measures for banks working with virtual assets (FATF, 2019b).

Another relevant source is The Bank for International Settlements (BIS) which has published research on the use of blockchain technology for AML and CTF measures, including the use of transaction monitoring and machine learning algorithms (BIS, 2019).

Figure 7 – Use cases based on societal division of the Brazilian population



Real Digital is a platform that has the potential to revolutionize the financial industry, prroviding a more efficient, secure, and inclusive system for cross-border payments and financial services. By leveraging blockchain technology, Real Digital can offer faster and more cost-effective transactions, reducing the friction and costs associated with cross-border payments.

Furthermore, Real Digital can also address the challenges faced by different segments of society, from high-net-worth individuals to the unbanked. By offering new services such as NFTs, smart contracts, and crowdfunding, Real Digital can create a new paradigm of financial services that is more flexible and accessible to all.

In addition, Real Digital can also promote financial inclusion and reduce inequality. By offering services such as digital wallets and anti-fraud measures, Real Digital can provide a more secure and convenient way for low-income and unbanked individuals to access financial services. Furthermore, it can also support informal businesses, providing them with access to formal financial services and reducing their reliance on cash-based transactions.

Overall, Real Digital represents the future of cross-border payments and financial inclusion. Its potential to transform the financial industry is immense, and its benefits will be felt by all segments of society, from the high net worth to the unbanked. As we look towards a more connected and globalized world, Real Digital offers a solution that is not only efficient and secure but also inclusive and equitable.

6.2 Final remarks

This article proposes an applicable and modular architecture of a Regulated Liability Network (RLN), which could be applied in the Brazilian Real Digital's ecosystem. The main reasons are to provide a cost-efficient, scalable, multi-assets, and multi-blockchain platform (EVM compatibility), and also interoperable with current systems in National Financial System (SFN), such as BCB's PIX (fast payment system) and Open Finance.

The successful implementation has the potential to accelerate the delivery of benefits of Brazilian Real Digital platform while reducing risks and improving security. The proposed model is expected to also speed up adoption of Real Digital by regulated financial institutions, unlock more innovative financial services, promote market competition, with the potential to extend benefits for the Brazilian population. The proposed platform model, in the future, can accelerate implementation of new use cases such as more efficient cross- border payments across different countries and regions.

6.2.1 Main contributions of our approach

The main contributions of this work is defining a model that:

1. ensures interoperability between blockchain/DLT platforms;
2. ensures interoperability between current payment systems, such as PIX;
3. scalable environment, with flexible performance, in public cloud;
4. possibility of accelerating numerous use cases, related to DvP, PvP, cross-border payments, disintermediation, in addition to cash-less movement;
5. security, in hardware at all levels and points of the Real Digital ecosystem, also based on data privacy (in compliance with Law 13709).

6.3 Future work

Future work is related to the implementation of the proposed architecture, together with the Brazilian Central Bank, and all financial institutions involved in the new ecosystem.

References

ATLANTIC-COUNCIL. **Shaping the global future together**. 2023. Available in: https://www.atlanticcouncil.org/cbdctracker. Accessed in: 2023 Mar. 24.

BAHAMAS CENTRAL BANK. **Digital Bahamian Dollar**. 2023. Available in: https://www.sanddollar.bs. Accessed in: 2023 Mar. 24.

BANCO CENTRAL DO BRASIL – BCB. **Lift Challenge**: Real Digital dá início à execução dos projetos. 2022. Available in: https://www.bcb.gov.br/detalhenoticia/629/noticia. Accessed in: 2022 Out. 25.

BANCO CENTRAL DO BRASIL – BCB. **What is Pix?** 2023. Available in: https://www.bcb.gov.br/en/financialstability/pix_en. Accessed in: 2023 Feb. 9.

BANCO CENTRAL DO BRASIL – BCB. **BC divulga diretrizes do projeto-piloto do Real Digital**. 2023. Available in: https://www.bcb.gov.br/detalhenoticia/667/noticia. Accessed in: 2023 Mar. 15.

BANCO CENTRAL DO BRASIL – BCB. **BC divulga diretrizes do projeto-piloto do Real Digita**l. 2023. Available in: https://www.bcb.gov.br/detalhenoticia/17848/nota. Accessed in: 2023 Mar. 24.

BANCO CENTRAL DO BRASIL – BCB. **CBDC**. 2023. Available in: https://www.bcb.gov.br/estabilidadefinanceira/real_digital. Accessed in: 2023 Jan. 25.

EUROPEAN CENTRAL BANK. **Report on a digital euro**. Europe: European Central Bank, 2020. Available in: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf. Accessed in: 2023 Mar. 2.

BANK FOR INTERNATIONAL SETTLEMENTS – BIS. **Central Bank Digital Currencies**. 2018. Available in: https://www.bis.org/cpmi/publ/d174.pdf. Accessed in: 2023 Feb. 2.

BANK FOR INTERNATIONAL SETTLEMENTS – BIS. **Embedded supervision**: how to build regulation into decentralised finance. 2019. Available in: https://www.bis.org/publ/work811.htm. Accessed in: 2023 Mar. 20.

BANK FOR INTERNATIONAL SETTLEMENTS – BIS. **Central bank digital currency**: the quest for minimally invasive technology 2021. Available in: https://www.bis.org/publ/work948.pdf. Accessed in: 2022 May 18.

BANK FOR INTERNATIONAL SETTLEMENTS – BIS. **Central bank digital currencies**: foundational principles and core features 2023. Available in: https://www.bis.org/publ/othp33.pdf. Accessed in: 2023 Mar. 5.

BANK OF JAMAICA. **A Primer on BOJ's Central Bank Digital Currency**. 2020. Available in: https://boj.org.jm/a-primer-on-bojs-central-bank-digital-currency. Accessed in: 2023 Mar. 24.

BANK OF NIGERIA. **Currency eNaira**. 2021. Available in: https://www.cbn.gov.ng/Currency/eNaira.asp. Accessed in: 2023 Mar. 24.

CBDC-TRACKER. **Today's Central Bank Digital Currencies Status**. 2023. Available in: https://cbdctracker.org. Accessed in: 2023 Mar. 24.

CCF. 2023. Available in: https://microsoft.github.io/CCF/main/overview/what_is_ccf.html. Accessed in: 2023 Mar. 2.

CONSENSYS. **A complete suite of trusted products to build anything in web3**. 2020. Available in: https://pages.consensys.net/ central-banks-and-the-future-of-digital-money. Accessed in: 2023 Mar. 17.

ECCB. 2021.

FINANTIAL ACTION TASK FORCE – FATF. **Guidance RBA Virtual Assets**. 2019. Available in: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html. Accessed in: 2023 Mar. 24.

FINANTIAL ACTION TASK FORCE – FATF. **Virtual Assets and Virtual Asset Service Providers**. 2019. Available in: https://www.fatf-gafi.org/content/dam/fatf/documents/recommendations/RBA-VA-VASPs.pdf. Accessed in: 2023 Mar. 22.

GAMRAT, C.; BERTELS, K. The race towards operational quantum computers. **HiPEAC Vision 2023**, p. 110, 2023. Available in: https://news.harvard.edu/gazette/story/ 2021/07/harvard-led-physicists-create-256-qubit-programmable-quantum-simulator/. Accessed in: 2023 Mar. 23.

LACCHAIN. **LACChain**. 2023. Available in: https://www.lacchain.net/home?lang=en. Accessed in: 2023 Mar. 24.

LACCHAIN. **Características de LACChain**. 2023. Available in: https://www.lacchain.net/projects/Cross-border\%20payments?lang=en. Accessed in: 2023 Mar. 24.

LIFT. **Lift Challenge**. 2023. Available in: https://www.bcb.gov.br/site/liftchallenge/en. Accessed in: 2022 Nov. 11.

MICROSOFT. **Presidio**: Data Protection and De-identification SDK. 2018. Available in: https://microsoft.github.io/presidio/. Accessed in: 2023 Mar. 15.

MICROSOFT. **Harnessing the opportunity of ISO20022 for financial services organizations**. 2020. Available in: https://www.microsoft.com/en-us/industry/blog/financial-services/2020/12/14/ harnessing-the-opportunity-of-iso20022-for-financial-services-organizations/. Accessed in: 2023 Jan. 18.

MICROSOFT. **Azure Real-Time Fraude Detection**. 2022. Available in: https://github.com/microsoft/azure-realtime-fraud-detection. Accessed in: 2022 Dez. 19.

MICROSOFT. **Reinforcement learning**. 2022. Available in: https://news.microsoft.com/source/features/ai/ reinforcement-learning/. Accessed in: 2022 July 3.

MICROSOFT. **Azure active directory verifiable-credentials decentralized identifier overview**. 2023. Available in: https://learn.microsoft.com/en-us/azure/ active-directory/verifiable-credentials/decentralized-identifier-overview. Accessed in: 2023 Mar. 24.

MICROSOFT. **Azure architecture blockchain multiparty compute**. 2023. Available in: https://learn.microsoft.com/en-us/azure/architecture/guide/blockchain/multiparty-compute. Accessed in: 2023 Feb. 16.

MICROSOFT. **Azure active directory verifiable-credentials how to dnsbind**. 2023. Available in: https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/how-to-dnsbind. Accessed in: 2023 Mar. 24.

NATARAJAN, H.; KRAUSE, S.; GRADSTEIN, H. **Distributed ledger technology and blockchain**. Washington, DC, World Bank: 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. **Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms**. Gaithersburg: NIST, 2016. Available in: https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms. Accessed in: 2023 Mar. 23.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY – NIST. **Post-Quantum Cryptography - Selected Algorithms 2022**. Gaithersburg: NIST, 2022. Available in: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022. Accessed in: 2023 Mar. 23.

PEFFERS, K. et al. A design science research methodology for information systems research. **Journal of Management Information Systems**, Routledge, v. 24, n. 3, p. 45-77, 2007. Available in: https://doi.org/10.2753/MIS0742-1222240302. Accessed: 2023 Jan. 2.

R3. **The Regulated Liability Network on Cord**a. 2023. Available in: https://r3.com/blog/the-regulated-liability-network-on-corda/. Accessed in: 2023 Feb. 13.

RLN. **The Regulated Liability Network Whitepaper**. 2023. Available in: https://regulatedliabilitynetwork.org/wp-content/uploads/2022/11/The-Regulated-Liability-Network-Whitepaper.pdf. Accessed in: 2023 Feb. 13.

SCHäR, F. Decentralized finance: On blockchain and smart contract-based financial markets. **Federal Reserve Bank of St. Louis Review**, p. 153-174, 2021. Available in: https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets. Accessed in: 2023 Mar. 17.

SHABSIGH, M. G.; KHIAONARONG, M. T.; LEINONEN, M. H. **Distributed ledger technology experiments in payments and settlements**. [*S.l.*]: International Monetary Fund, 2020.

USP-IME. **Lei de Benford e aplicações**. 2022. Available in: https://www.ime.usp.br/~abe/lista/pdfr6aqDSXtbC.pdf. Accessed in: 2022 Sept. 30.

W3C. **Verificable Credentials Data Model v1.1**. 2022. Available in: https://www.w3.org/TR/vc-data-model/. Accessed in: 2023 Mar. 24.