
CROSS-BORDER
PAYMENTS WITH
BLOCKCHAIN
IDB | LAB
LACCHAIN
10 YEARS
CITI
INNOVATION
LABS
ioBUILDERS

Irene Arias Hofman
Chief Executive Officer, Innovation Lab (IDB Lab) of the Inter-American Development Bank

---

Cross-border payments are a critical element of our work as international development organizations. There are many applications focused on inclusion, such as official development assistance (ODA) and international remittances. These cash flow mechanisms are extraordinarily important for the economies of Latin American and the Caribbean, and most importantly, for ODA's final beneficiaries and international remittance recipient families.

This proof of concept enabled actual cross-border payments using tokenized money and blockchain technology between the Headquarters of the Inter-American Development Bank in Washington, DC, and individuals in the Dominican Republic. It demonstrated that cross-border payments using blockchain can be not only feasible, but faster, more traceable, and less manual, which can lead to significant fee reductions.

I would like to stress out the market potential of these results and the transformative impact they can bring to the functioning of cross-border payment markets. We are only at the beginning of a disruptive change, but it is already possible to visualize how people's lives can improve by having ODA tokens transferred in a matter of seconds and being end-to-end traceable, as well as faster and less taxed international remittances. With this preamble, I am honored to break the bottle on the bow of this ship, looking forward to the many borders it is poised to cross.

Francisco Ramón Ruiz García
Treasurer, Inter-American Development Bank

The Treasury Department of the IDB has been analyzing for several years the potential of decentralized technologies and tokenized assets, by conducting research and engaging in proofs of concept. As we acknowledge the potential of these technologies, we are also aware of the current limitations in terms of robustness of the technical components and compliance with regulatory frameworks.

This proof of concept on cross-border payments, motivated by the possibility of improving the traceability and reducing fees and times in disbursement operations, demonstrated that blockchain technology, tokenized money, and the LACChain blockchain network has real potential for this use case, and also allowed to identify some challenges and opportunities for these developments to keep evolving towards productive scenarios.

We will keep exploring and testing blockchain and other emerging technologies that prove to have value in the enhancement of financial procedures, including enterprise processes and operations and projects in the Latin American and the Caribbean region. We believe that technology is a tool that can always be useful when utilized correctly, which requires research and experimentation.

Nuria Simo Vila
Chief Information Officer and General Manager, Department of Information Technology (ITE) of the Inter-American Development Bank

---

At the IT Department of the IDB, we have been following closely the different proofs of concepts and pilots that several financial institutions across the globe have carried out using blockchain technology. Over the past years, we have analyzed different networks and solutions that aim to improve the way domestic transactions, international payments, and settlements work today. Last year, taking advantage of the LACChain blockchain infrastructure that has been enabled as a public good for Latin America and the Caribbean under the leadership of the IDB, we decided to design and build a solution in-house.

The possibility of leveraging our internal expertise in blockchain and partnering with Citi Bank to explore the benefits in terms of traceability, times and fees related to the thousands of cross-border payments that the IDB makes every year seemed very attractive to us. In the process we have learned a lot, contributed to build internal knowledge, raised awareness, and positioned our specialists at the forefront of the understanding of the state of the art of the technology. We will keep embracing the use of emerging technologies to improve the Bank's operation.

CROSS-BORDER PAYMENTS WITH BLOCKCHAIN

R. Gutiérrez (Project Leader) [1], M. Allende (Technical Leader) [1, 2, 3],
A. Leal (Project Manager) [1, 2, 3], A. Pareja (Lead Architect) [1, 2, 3], A. Pardo [1,2,3],
M. Da Silva [1], P. Marciszewski [4], O. Opeyemi [4], D. Whiting [4], M. Murphy [4],
D. López [1, 2, 3], S. Cerón [1, 2, 3], S. Murcia [1], R. Monteverde [1], R. Cessa [1], F. Munhoso [1],
M. Menéndez [1, 3], J.J. Ferrer [1], E. Gomez [5], C. Lopez [5], I. Saiz [5], F. París [5]

[1] IDB - Inter-American Development Bank, 1300 New York Ave, Washington DC, U.S.
[2] IDB Lab – Innovation Lab of the IDB, 1300 New York Ave, Washington DC, U.S.
[3] LACChain – Global Alliance for the Development of the Blockchain Ecosystem in LAC.
[4] Citi Bank - 388 Greenwich St, New York, U.S.
[5] ioBuilders - 28223 Pozuelo de Alarcón, Madrid, Spain.

This paper describes the proof-of-concept (PoC) developed by the Inter-American Development Bank, the IDB Lab, LACChain, the Citi Bank Innovations Labs, and ioBuilders to demonstrate cross-border payments between entities in different countries that involve currency exchange, using digital money represented by tokens -tokenized money- in the LACChain Besu Blockchain Network. For this PoC, Citi Bank played the role of the bank holding the funds; the IDB's headquarters in the U.S. played the role of the sender of tokenized dollars; an individual in Dominican Republic played the role of recipient of tokenized Dominican pesos; LACChain provided the blockchain infrastructure and developed the back end, the smart contracts and the integrations; and ioBuilders provided technical advice and developed the front end.

1. MOTIVATION AND CONTEXT

The IDB sends several thousands of transactions a year from the headquarters (HQ) in Washington DC the Latin American and the Caribbean Region, to fund projects through grants and loans, fund the country offices (COFs), and make payments to local service providers. These transactions usually involve the IDB's Agent Bank, an intermediary Bank that facilitates the currency exchange, and the Beneficiary's Bank. This leads to high transaction fees, reducible times, and improvable traceability.

The goal of this PoC was to demonstrate that it is possible to use blockchain technology to accomplish these cross-border payments while reducing costs and times as well as increasing traceability of the transactions, intermediaries, and fees. To this purpose, in the first phase of the PoC that we are presenting in this paper we created an IDB bank account with Citi Bank, owned by the IDB HQ. The bank account of the IDB HQ was pre-funded with dollars, with the intention of tokenizing and transferring them using the LACChain Blockchain Besu Network. The electronic transaction would go from an IDB HQ blockchain account -linked to its bank account with Citi Bank- to an individual's blockchain account -linked to a Bank Account in Dominican Republic-.

The LACChain Besu Network used for this PoC is the largest public-permissioned blockchain network in Latin America and the Caribbean. LACChain is the Global Alliance for the Development of the blockchain ecosystem in Latin America and the Caribbean, led by the Innovation Lab of the Inter-American Development Bank (IDB Lab) [1]. LACChain has enabled a regional infrastructure aimed to become a quantum-safe blockchain network of networks consisting of three layers: a public-permissioned blockhain ledger, a digital identity layer, and a tokenized money layer.

This PoC represents one more successful milestone in the road to enabling digital money based on blockchain, after several pilots carried out by central Banks and large financial institutions such as Jasper [2] (Canada), Ubin [3] (Singapur), Khokha [4] (South Africa), RTGS RP [5] (England), Stella [6] (Japan and Europe), LBChain [7] (Lithuania), the Central Bank of Brazil [8] (Brazil), Inthanon [9] (Thailand), and E-Krona [10] (Sweden), some of them involving cross-border transactions.

It is a reality that blockchain-based tokens provide a revolutionary way of representing and recording value and ownership on blockchain networks and have the potential to transform business models and services by enabling the development of decentralized applications for B2B, B2C, and C2C use cases. On April 2019, the Enterprise Ethereum Alliance (EEA) announced the formation of the blockchain-neutral Token Taxonomy Initiative to address the need to universally define tokens to better understand how their use and implementation can occur interchangeably across all token-enabled blockchain platforms. [11]

2. SCOPE

Blockchain technology enables the tokenization of assets by using smart contracts to define the features, rules, and permissions over those digital assets, called tokens. In the case of digital money, there are different types of tokens of interest. According to the popular taxonomy presented by the International Monetary Fund (IMF) in 2019 [12], money can be classified according to the type, the value, the backstop, and the technology utilized. From the IMF money tree, depicted in Figure 1, there can be distinguished five types of money: b-money, e-money, I-money, central bank money, and cryptocurrency. In this paper, the IMF also introduces the concept of synthetic central bank digital currencies (sCBDCs). Blockchain is in general behind all the "Decentralized" and "(De)Centralized" types, serving as the required ledger to provide that decentralization.

According to this classification, in this PoC we worked with b-money. Specifically, we created two stable coins pegged to the US Dollar and to the Dominican Peso, respectively. These tokens were always backed-up by fiat money in bank accounts that is guaranteed by Citi Bank as the Bank Agent and the financial institution providing the liquidity of b-money on the blockchain. This development has been based on a Ethereum Request for Comments (ERCs) that defines a set of rules required to implement tokens for the Ethereum ecosystem: the ERC-2020. The ERC-2020, a set of extensions of the ERC-20, known as the E-Money Token Standard, is "a proposed standard for e-money, bank and central bank money issued tokens, with extended functionalities such as holds, clearance, detailed compliance, funding,

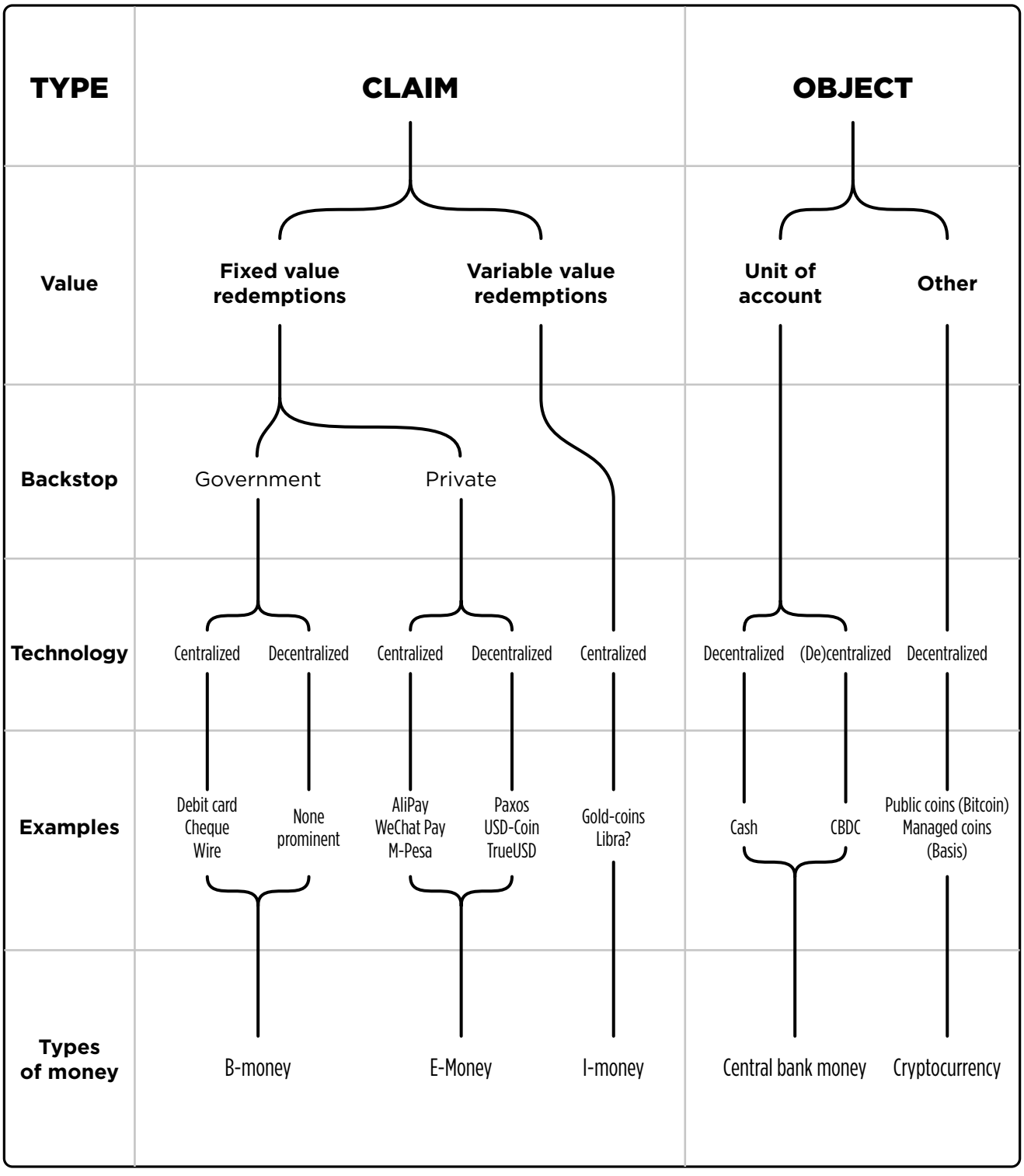


Figure 1. Types of money according to the IMF.

and payout"[1]. The E-Money Token is "working with global institutions, such as the International Telecommunications Union (ITU) and the Enterprise Ethereum Alliance (EEA) to become the standard for the use of real financial money on blockchain" [13] and has been recognized in the Technical Report elaborated by the ITU's DLT Focus Group on August 2019 [14].

The LACChain Besu Network utilized is a public-permissioned network[2] developed and maintained by the LACChain Alliance. This network builds on the Hyperledger Besu software [15], which is "an Ethereum client designed to be enterprise-friendly for both public and private permissioned network use cases". This network incorporates the LACChain tecno-legal framework and is already being used by governments, academic entities, large corporations, and start-ups, among others, that are using it for free for different use cases including academic credentials, exchange of information between custom administrations, notarization of documents, and procurement processes. This network was chosen for being the biggest public-permissioned network in Latin-America and the Caribbean, with no transaction fees, and supported by technical team that has been assuring its reliability since August 2019, when the network was launched.

3. RESULTS

For this POC, we integrated the architecture of smart contracts deployed in the LACChain Blockchain Network with the Citi WorldLink Payment Services through APIs. All the transactions sent in the timeline of a month from the IDB HQ bank account to the account in Dominican Republic were accomplished successfully. As we will cover in detail in Section 5.3, the main functionalities of the PoC were: Whitelist Account[3], Tokenize Money, Fetch FX Rate[4], Generate Transfer, Approve Transfer, and Execute Transfer. The time to execute each of the functionalities in the PoC was conditioned to the LACChain Blockchain and the WorldLink times, and was approximately of the following order:

- whitelist account takes an approximate of 10 seconds.
- tokenize money in a whitelisted account takes approximately 10 seconds.
- fetch FX Rate for a given currency combination takes an approximate of 2 seconds.
- generate transfer takes approximately 15 seconds.
- transfer approval takes an approximate of 8 seconds.
- execute transfer for ACH operations takes from 15 minutes to 1 hour.

Additionally, the platform allows at all times for all the stakeholders to track the status of the payment as shown in figures 2 to 8 and described in detail in Section 5.3. In order to evaluate the reduction of costs**,** it would be necessary to know the business models developed by the financial institutions for these new types of blockchain-based money and transactions, in this case Citi Bank. No financial institution in the world has yet come up with a proposal of a business model for blockchain-based b-money or e-money liquidity.

Figures 2 to 8 present the user interfaces of different PoC functionalities. For a detailed description of each of the functionalities see Section 5.3.

1. The E-Money Token is a proposal spawn from the cooperative work of ioBuilders (https://io.builders/) and Adhara (https://adhara.io/).
2. According to ISO TC 307 WG5, blockchain networks can be classified into permissioned public, permissioned private, and permissionless public. Permissioned public networks are characterized by being open, transparent, decentralized, and with no transaction fees. At the same time, every participant is identified so both privacy and compliance with regulation can be enabled. Examples of these networks are Alastria in Spain, led by an association of over 500 members; EBSI in Europe led by the European Union; and LACChain in Latin America and the Caribbean, led by the Laboratory of Innovation of the Inter-American Development (IDB Lab).
3. Whitelisting is necessary to guarantee compliance with KYC and AML processes. By whitelisting a blockchain account, Citi is verifying that the entity behind it is a customer they have well identified in their systems and that the bank account the entity wants to link to the blockchain account belongs to the entity.
4. In order to fetch the FX rate, it was necessary to call the Citi WordLink Payment Services via API. As described in Section 4.2, one of the areas of improvement consists in feeding a smart contract with the FX rates in real time, so there is no need to leave to blockchain to fetch the FX rate for each cross-border transaction.

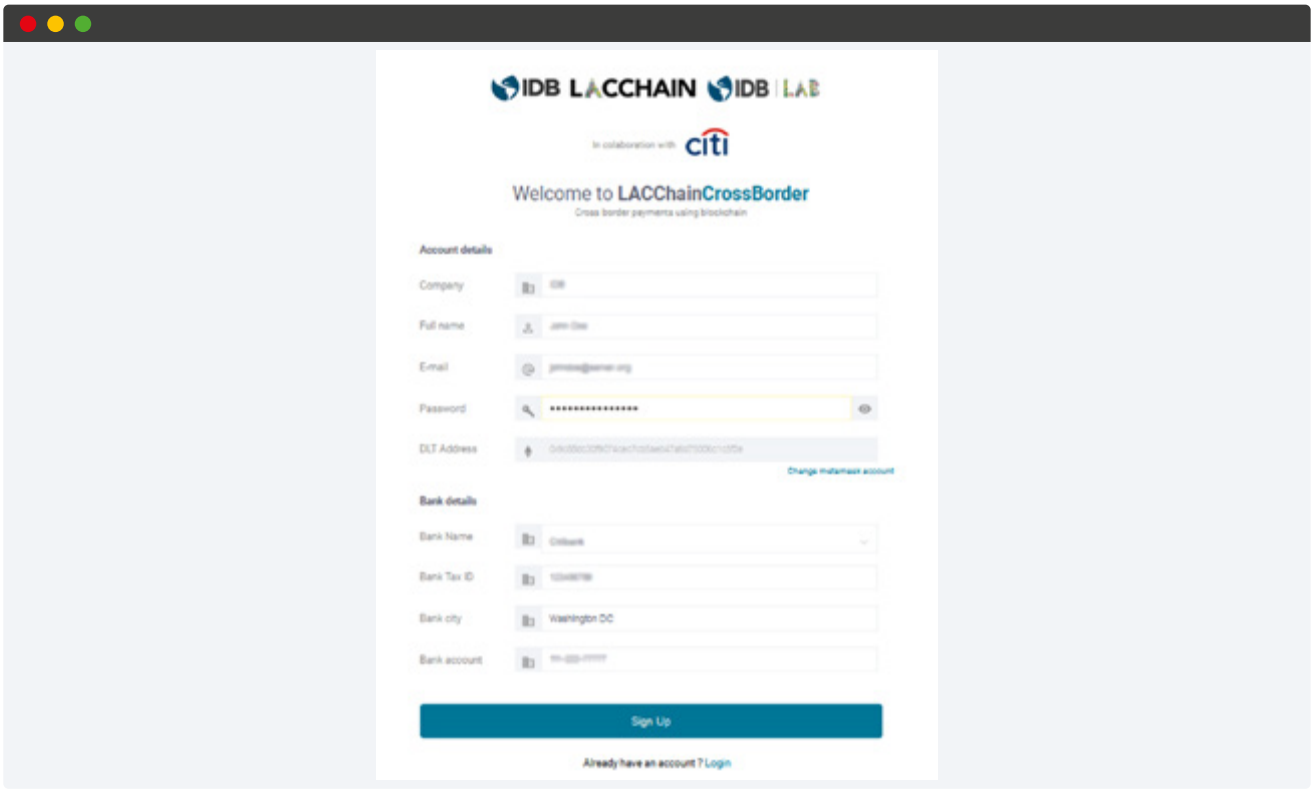


Figure 2. Sign-up user interface.

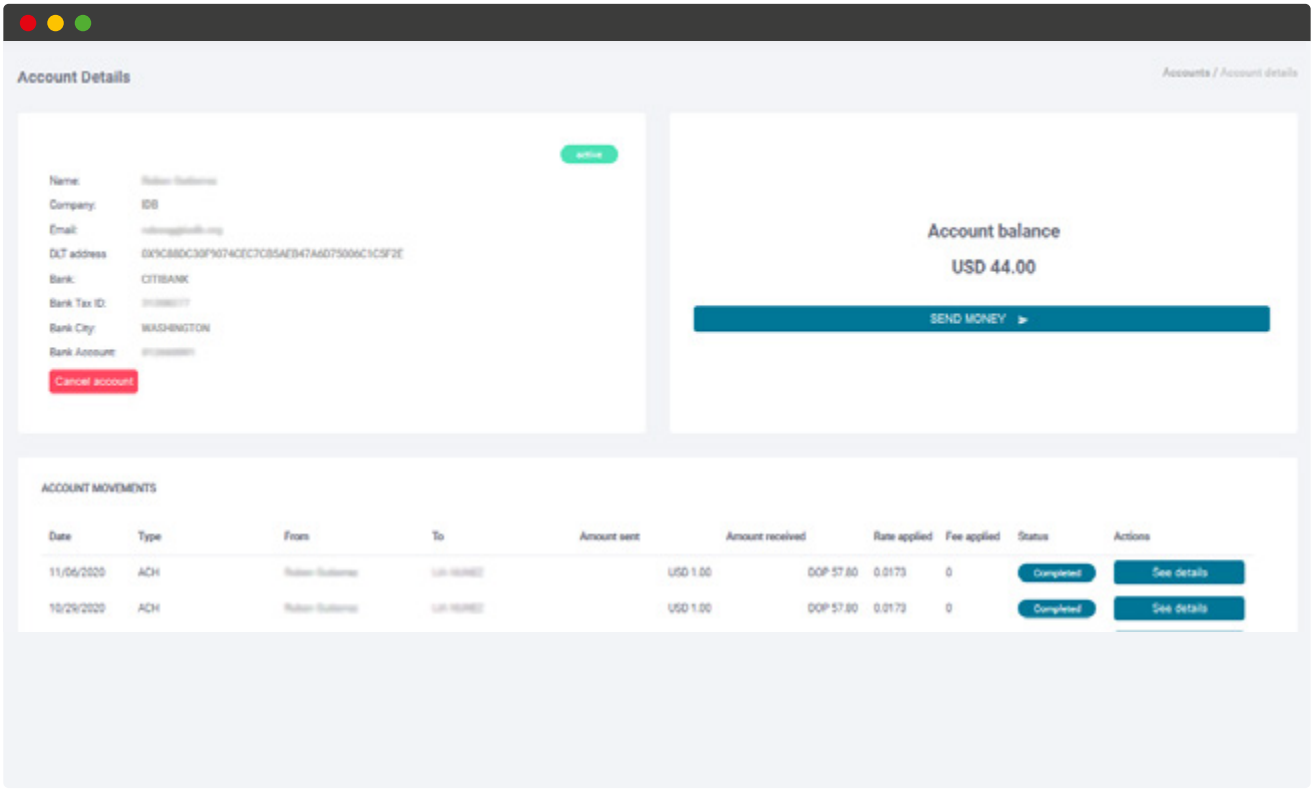


Figure 3. Account view user interface.

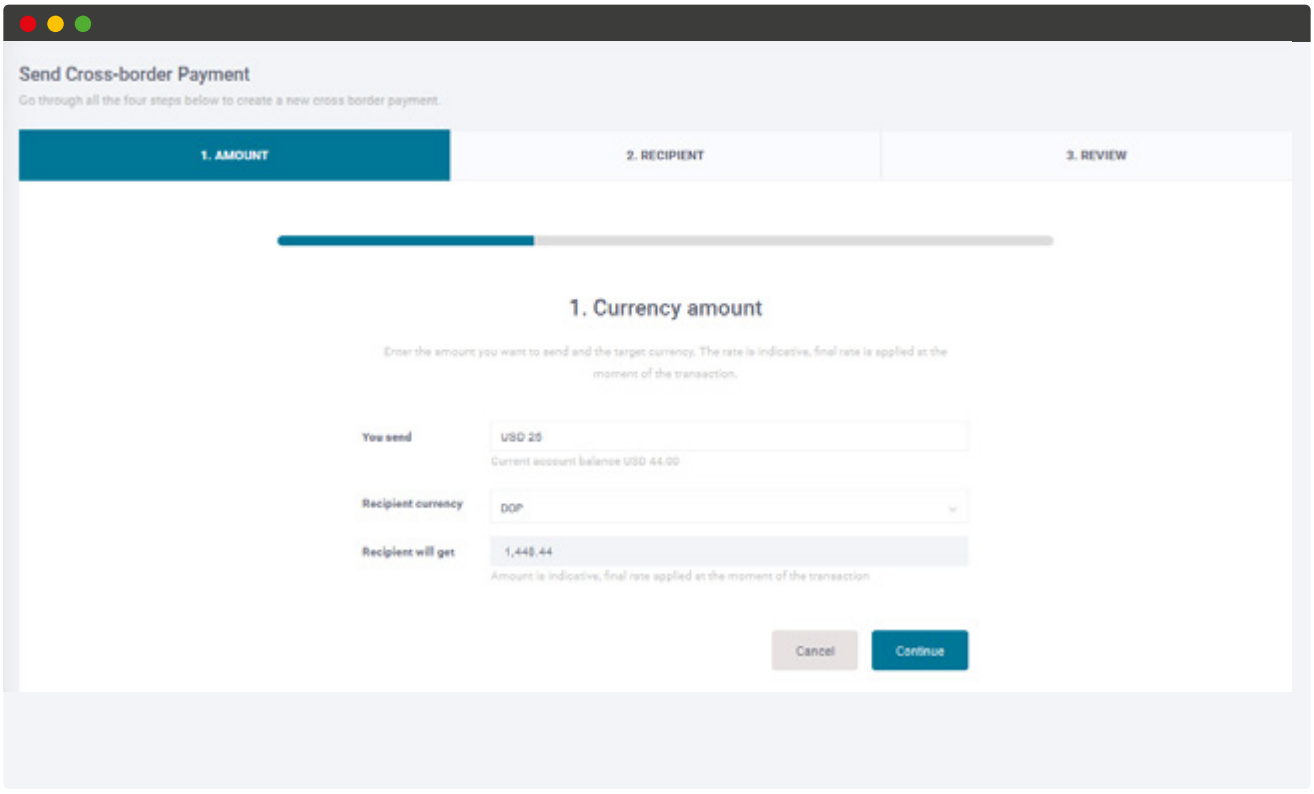


Figure 4. Cross-border payment step 1.

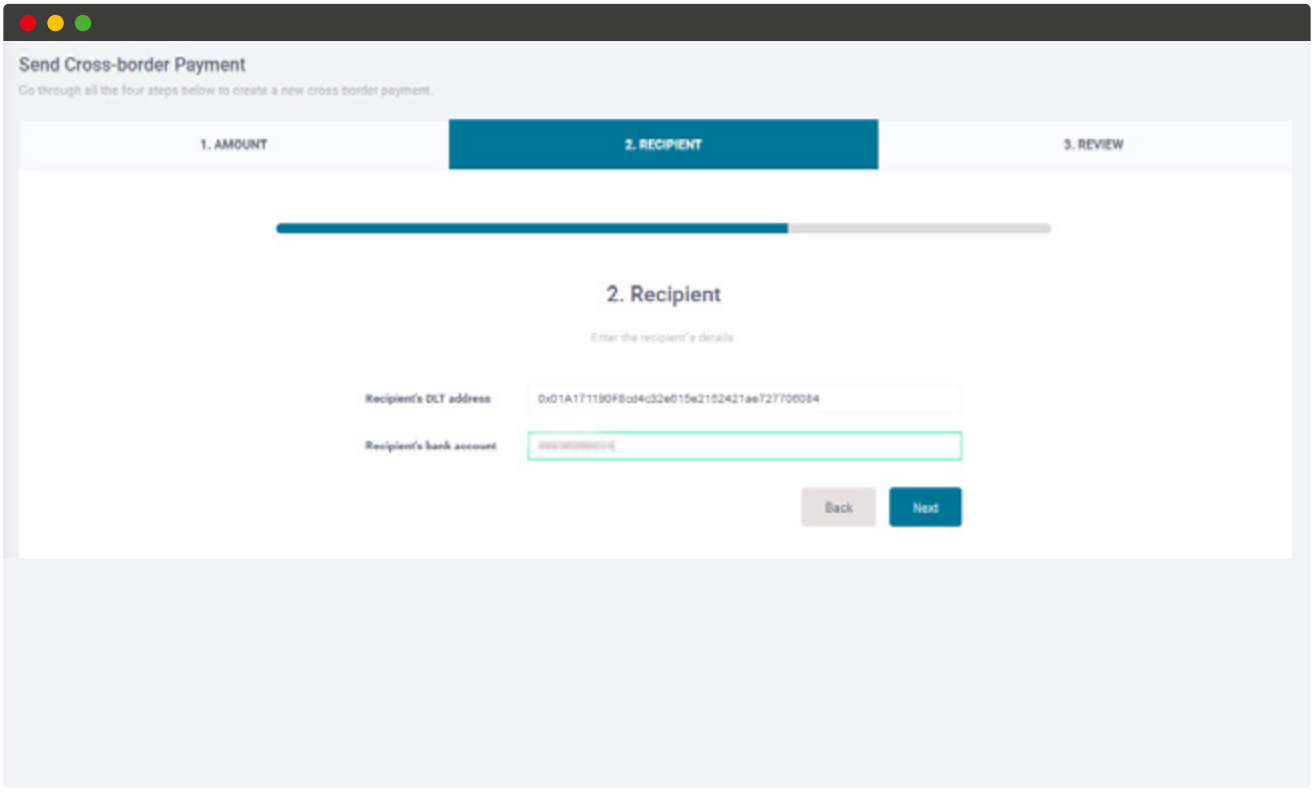


Figure 5. Cross-border payment step 2.

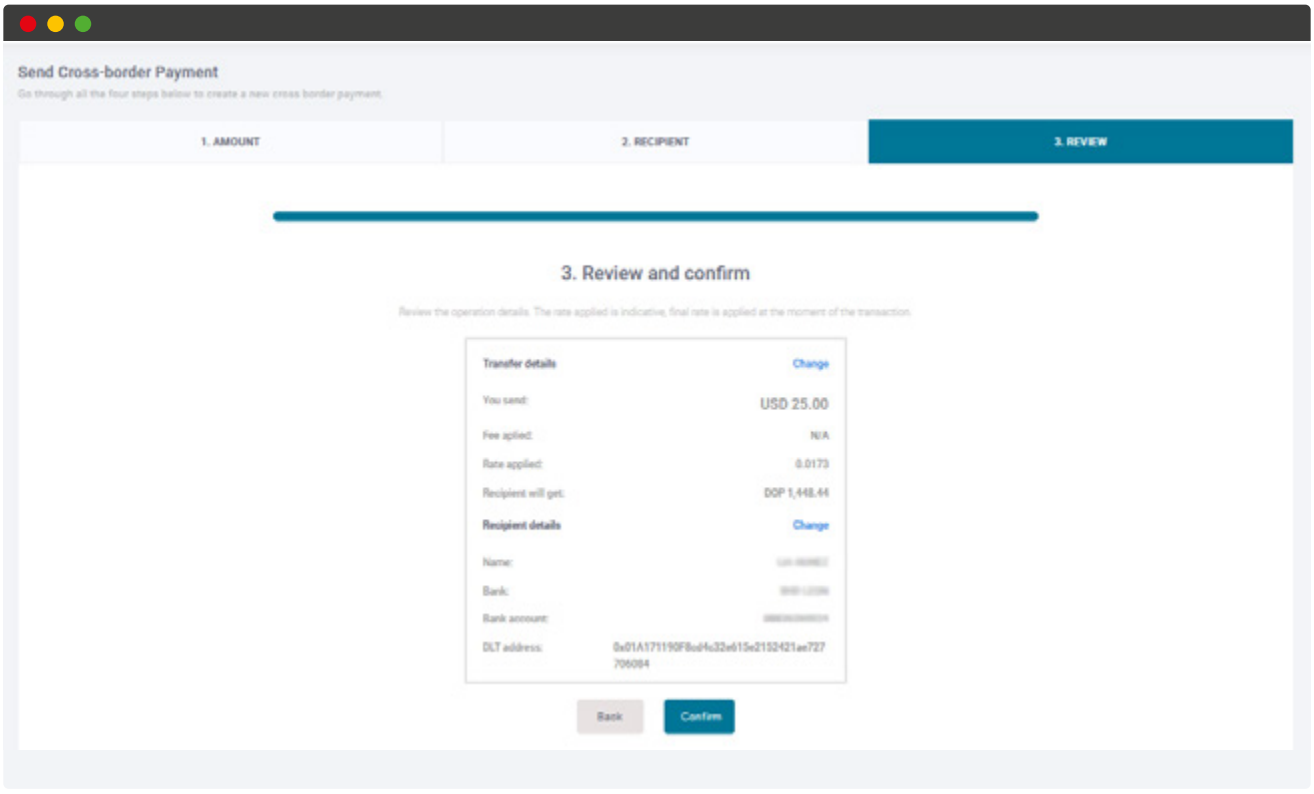


Figure 6. Cross-border payment step 3.

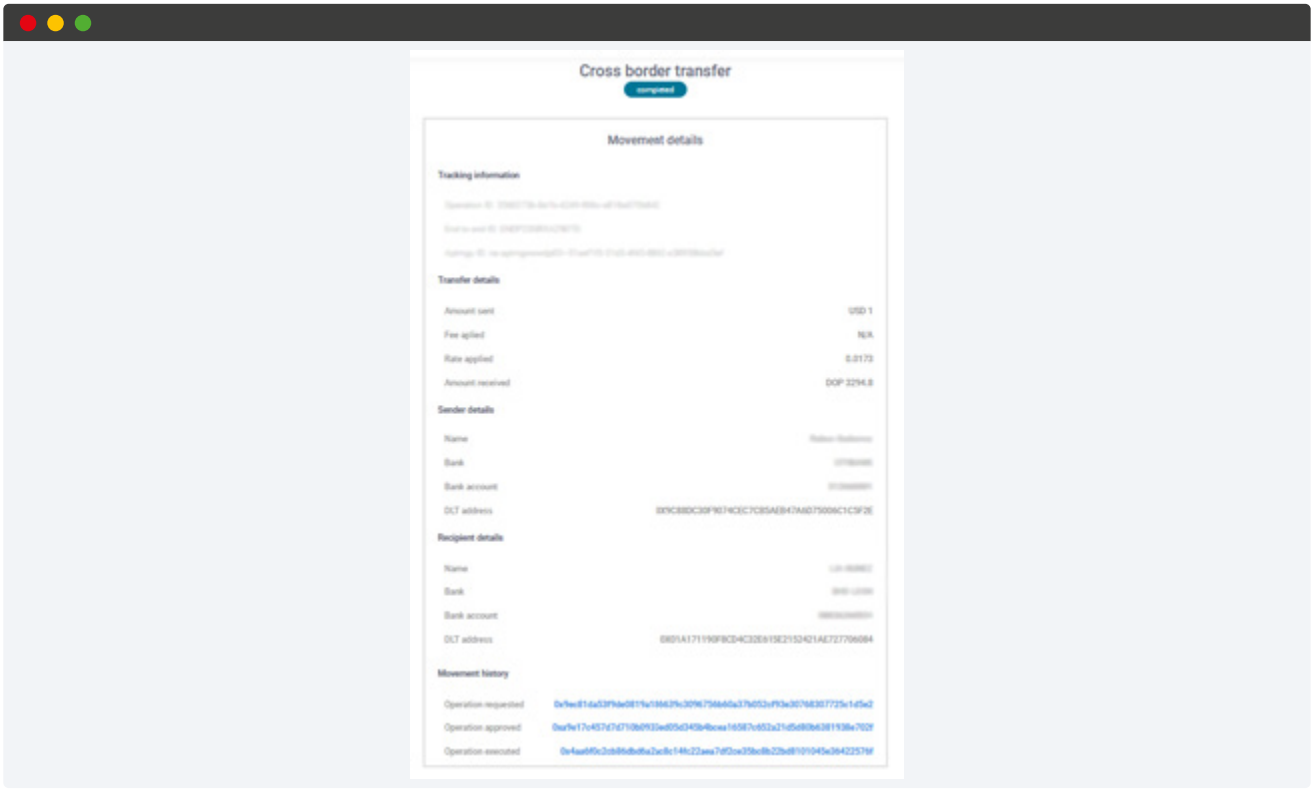


Figure 7. Account movements.

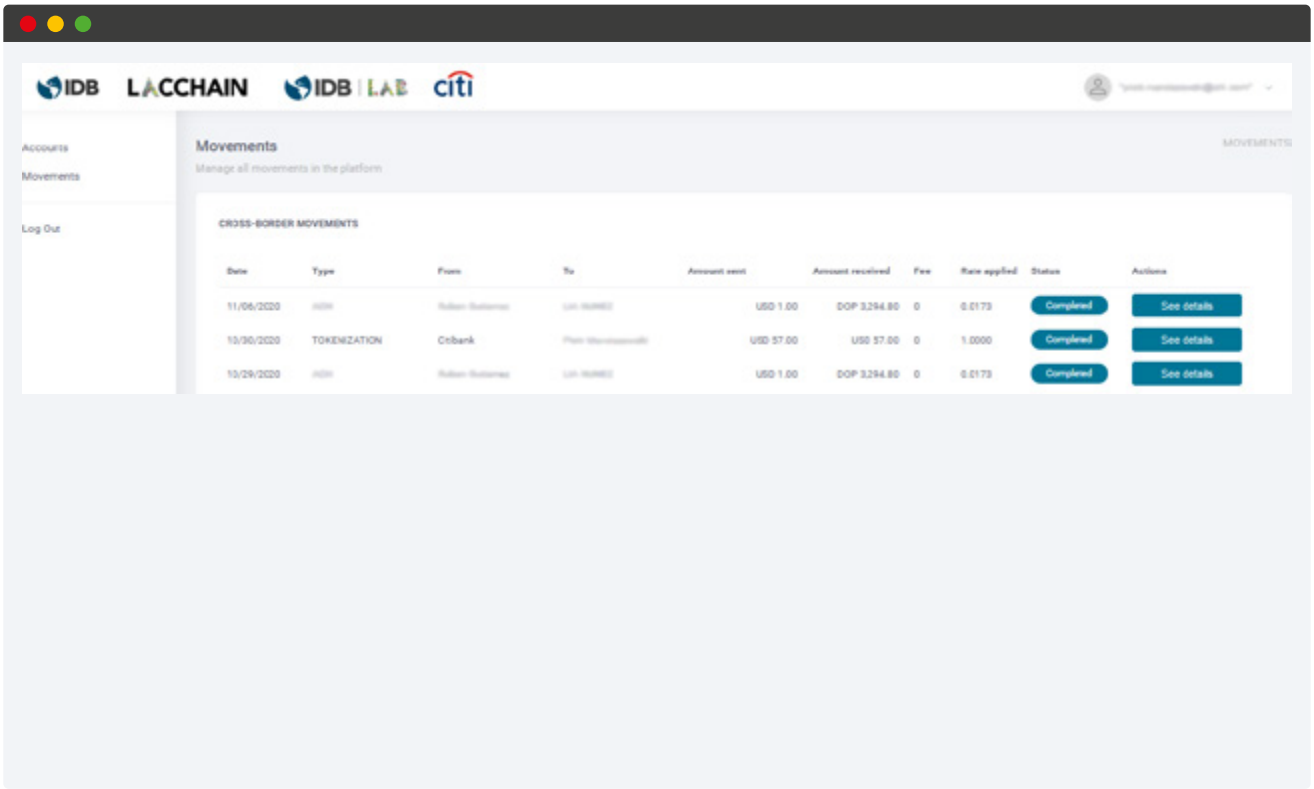


Figure 8. Movement details.

4. CHALLENGES AND OPPORTUNITIES

In this PoC we have identified several limitations, challenges, and opportunities for cross-border payments using money tokenized by financial institutions in blockchain networks. In this section we present an overview of some of the most relevant challenges and opportunities that are independent from the type of network used (i.e., permissioned public, permissioned private, or permissionless public). In those cases where the statement applies only to a specific type of networks, we have tried to point it out. We have classified the challenges and opportunities into three categories: the challenges and next steps for blockchain networks, the challenges and next steps for financial institutions, and the challenges and next steps for end-user adoption.

Challenges and opportunities for blockchain networks

Privacy and correlations: one of the main challenges when using blockchain networks as the public ledgers for the exchange of digital assets, and particularly tokenized money, is that transactions are immutably recorded and completely exposed to anyone with access to the public network. Blockchain not only does not guarantee privacy by default, but presents very relevant challenges to erase potential correlations[5] and personal identifiable information

5. By correlations we mean independent information or data that can be related. For instance, a transaction between subject A and B in the context X and a transaction between A and C in the context Y for which subject A uses the same blockchain account and the transactions are recorded in a public and immutable ledger.

from transactions made in different contexts by the same blockchain account. Therefore, if the identity behind a pseudonymous account is discovered in one context, the entire transaction history of that identity is revealed because of the public character of the blockchain. One potential solution is the use of mixers. Mixers allow to erase the traceability of blockchain transactions in a way that it is not possible to link the sender with the recipient.

Blockchain-based identities: today, digital identity is far from ideal. In general, there are not suitable ways to identify individuals electronically with the maximum level of assurance, which is necessary to provide digital services with all the guarantees. Blockchain networks are not exempt from this. With the aim of overcoming this, a set of standards and tools coming up under the scheme Self-Sovereign Identity (SSI), such as the Decentralized Identifiers (DIDs) [16] and the Verifiable Credentials (VCs) [17] from the W3C are intended not only to improve the interoperability, ownership, pseudonymity, portability, recovery, scalability, and security of the digital identification and authentication of individuals, but to also match real identities with blockchain accounts in a trustable, reliable, and essential way to guarantee compliance with KYC and AML processes when dealing with tokenized money -and other digital assets- living in blockchain networks.[6]

Key management: key management is one of the biggest challenges when dealing with blockchain tokens of any kind. For large institutions it is easier to use key vaults or HSMs to store the private keys and leverage their corporate solutions for the identification of employees, allowing each individual to use their private keys indirectly when generating blockchain transactions from friendly interfaces. For individuals, it is not straightforward. Digital wallets are the personal and private repositories proposed in the SSI model for this purpose, but there is still some work to be done around developing good mechanisms for things such as authorization to access the wallets, authorization to use digital tokens, authorization to use the digital identity to access digital services, and recovery of private keys and credentials in case a digital wallet is lost or compromised.

Transaction troughput and fees: when dealing with blockchain networks, transaction throughput and fees can become strong limitations. The number of transactions a blockchain network can process per second is and will always be limited, because of the time required to process them and reach consensus, and the block size. Similarly, incentive mechanisms in certain types of networks -in general permissionless- require to pay a fee for each transaction.[7] Shardings and second layer solutions for transaction processing such as state channels and rollups are interesting alternatives under development to guarantee scalability. Permissioned public networks with no transaction fees and incentives based in fixed memberships seem suitable to guarantee affordable costs.

Optimal models for the distribution of resources: in permissionless networks with crypto incentives and transaction fees, the use of the network is easily regulated. The more you want to use it, the more you have to pay. In permissioned networks where there are not transaction fees is necessary to develop mechanisms to guarantee the availability of the network in an equitable way to all the participants, and avoid DOS attacks. A potential solution consists in enabling a gas distribution model consisting of distributing gas to the nodes dynamically based on how stressed the network is at every time and how much is node is using it. Gas can be distributed based on memberships with a fixed price.

Specific-purpose settlement networks: this PoC was a single-banking effort, involving only Citi Bank as an intermediary. Real cross-border situations will generally involve two, including the sender's Bank and the recipient's Bank,

6. LACChain has recently published a book on SSI addressing this and other topics, and is releasing the LACChain ID Stack, a set of free tools to enable scalable SSI on the LACChain networks. [18]

7. In the first weeks of the year 2021 the average transaction fee in the Ethereum mainnet has been of around $10, reaching a maximum of over $24. The volatility and unpredictability of transaction fees in permissionless networks such as Ethereum or Bitcoin make them very unsuitable for use cases that involve high transaction throughputs.

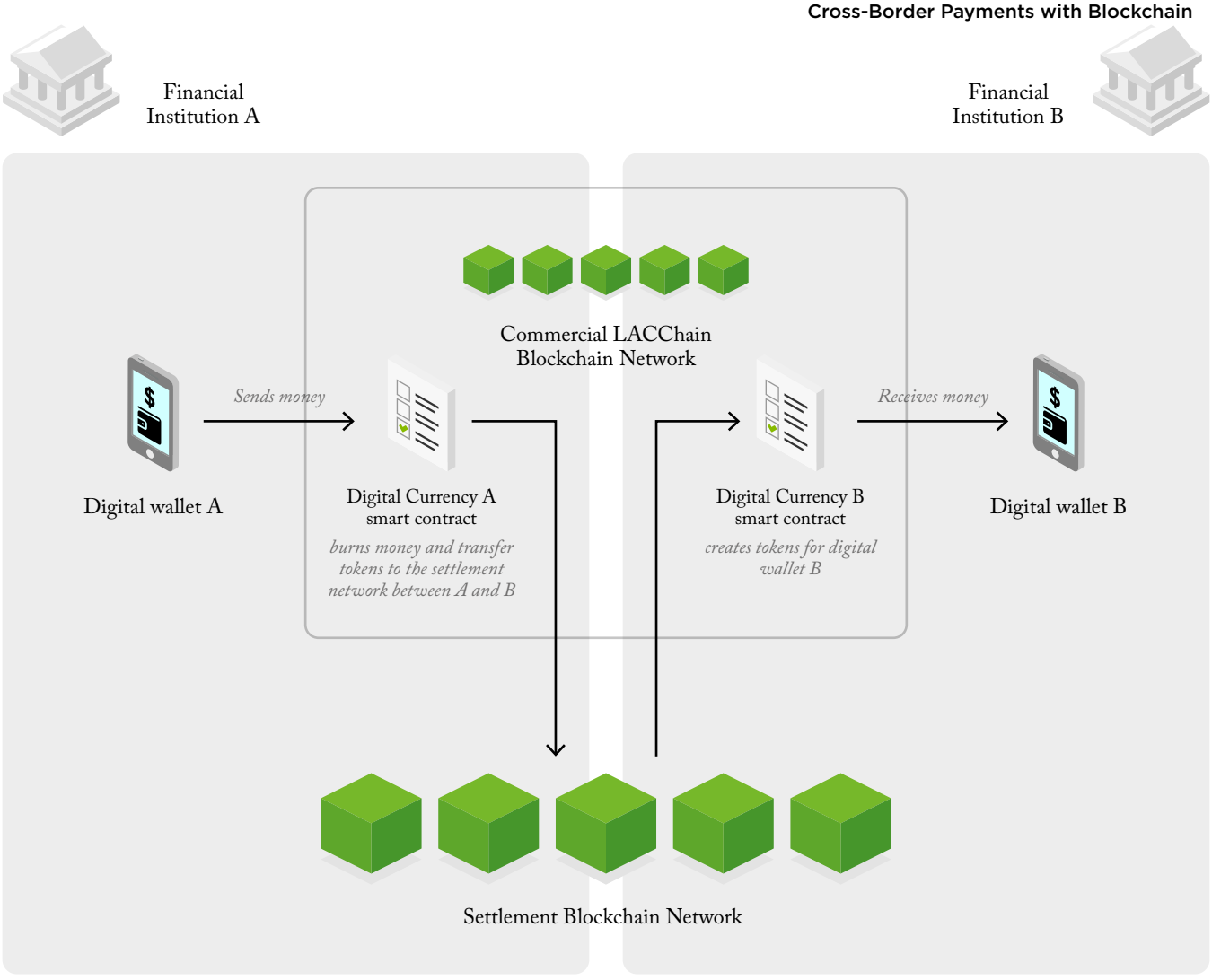


Figure 9. Interoperability between multi-purpose commercial blockchain networks and specific-purpose settlement networks.

or more. These two financial institutions will typically have their own smart contracts for the tokenization of money integrated with the core financial systems. Therefore, when the sender sends digital money minted by one financial institution and the recipient aims to cash out with a different financial institution, settlement is required. We understand that multi-purpose networks that enable payments using tokenized money are not suitable for settlements, as settlement networks require specific regulatory frameworks and governance models. Thus, we think that it might be necessary to develop clearing mechanisms that could also leverage blockchain networks that can be interoperable with commercial blockchain. For instance, two financial entities could provide tokenized money for their customers in a commercial blockchain network and settle payments in another specific-purpose blockchain network, as shown in Figure 9, where their blockchain accounts are backed up by bank accounts in a common institution, such as a Central Bank.[27] Smart contracts can be leveraged for the automation of clearings.

Legal frameworks and regulatory policies: the money used in this PoC shall be understood as b-money represented in the form of blockchain-based tokens. When providing services in different jurisdictions, it is essential

27. FNALITY International has built by 15 major financial institutions to the purpose of creating blockchain networks for settlement that are backed by RTGS, eliminating counterpart risk.

that both blockchain infrastructure and the issuance and exchange of e-money comply with all the regulations of the countries of operation.

Quantum safeness: with the advent of quantum computers, all the current algorithms used for signature and encryption over the internet are no longer secure, including RSA, elliptic curves (ECC), and discrete logarithms (DLL). NSA [19] and NIST [20], among others, have strongly advised against their use since 2016 . Blockchain technology not only uses the internet but relies strongly on ECC for the signature and verification of transactions. The possibility of "hack today, crack tomorrow" urges to move towards quantum-safe cryptography[30] now. Otherwise if, for instance, a financial institution issues $100 million in a blockchain network under a specific public key or set or public keys, when someone develops a robust quantum computer they could reverse the financial institution's public keys and use the private keys to impersonate it. Therefore, they could issue or burn tokenized money. It get worse when, in some cases, the impersonation might not leave trace or might not be associated to a quantum computer.

Challenges and next steps for financial institutions

KYC and AML of blockchain-based identities: as we mentioned in the previous section, in regulated environments of blockchain-based tokenized money it is necessary for financial institutions to be able to link the blockchain identities of their customers with their real identities. In the SSI approach, where individuals can generate their own identifiers, these individuals need to prove to the financial institution that they are behind a specific identifier so KYC and AML processes can be accomplished. The identity behind an identifier can still remain unknown for other entities, and individuals will even have different types of identifiers for interacting with different services and institutions. Financial institutions should develop the mechanisms to accomplish these identity proofing processes -to guarantee KYC and AML policies- in this new blockchain environment in an automatized, efficient, and reliable way, and then ensure that only whitelisted accounts can receive and send tokens. The latest can be achieved by introducing permissioning in the smart contracts, in a way that only blockhain accounts that have been previously whitelisted by the financial institution can send or received money. This is compatible with the mixers proposed in the previous section to avoid undesirable public traceability between sender and recipient.

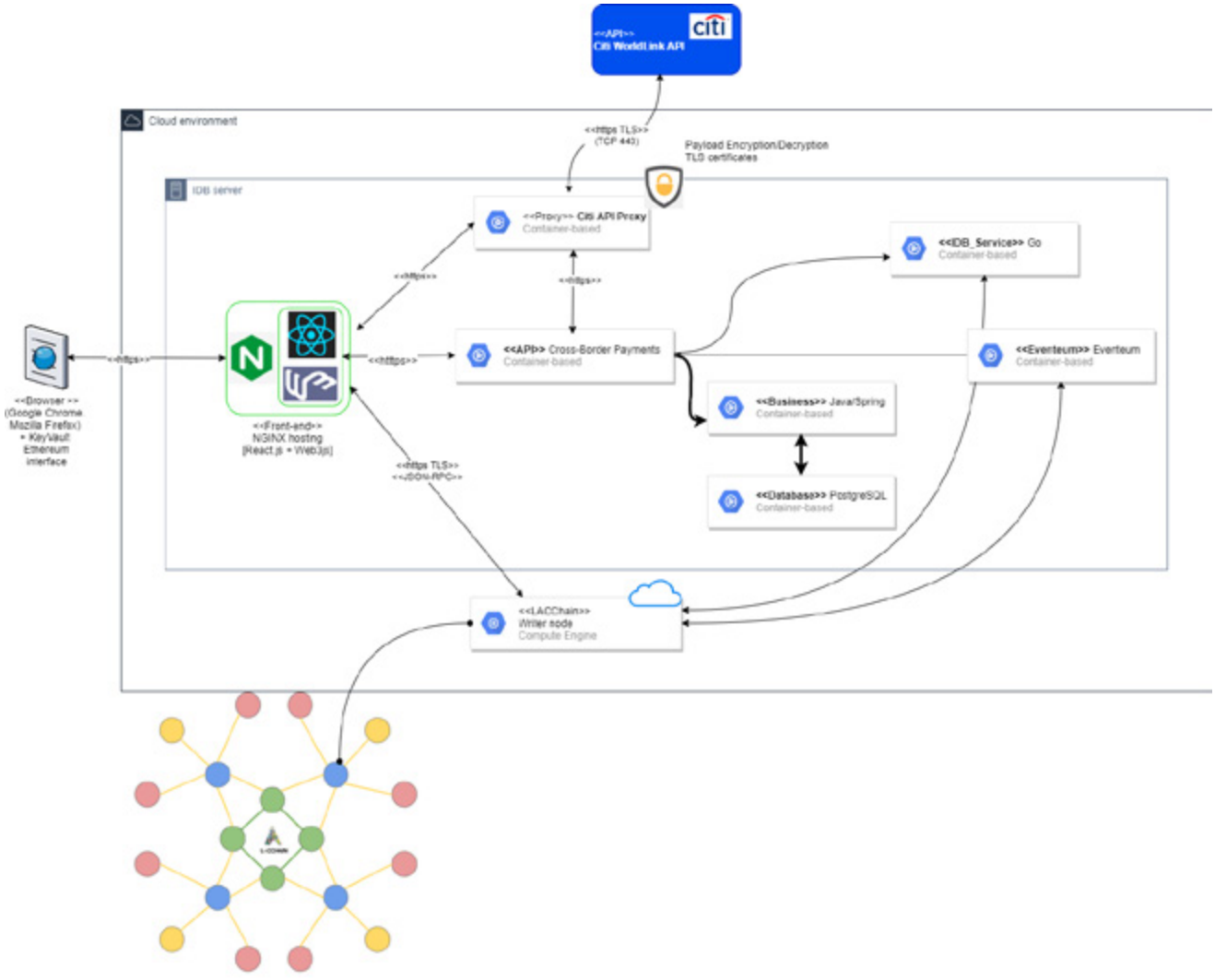
Integration with core financial systems: the processes of whitelisting, blacklisting, tokenizing, detokenizing, providing liquidity for foreign exchanges, and enabling settlements, among others, require an integration between the current back offices of the financial institutions and the blockchain networks where the tokenized e-money lives. This will allow, for example, the automation of a request by an individual to tokenize a certain amount of the money available in their checking account, that would imply holding that money from the account and minting it in the individuals' blockchain account to be now managed from a digital wallet. This will also allow the transactionability of that money between that individual and entities in real time and with no intermediaries.

FXs on the fly / on-chain FX rates: in order to increase efficiency in the automation of blockchain transactions, in those cases where a foreign exchange is involved, it is very convenient to bring the FX rates to the blockchain by storing them in smart contracts. Otherwise, for each foreign transaction it would be necessary to call an external service to request the FX rate, as it was the case in this pilot, which also limits the transparency. In order to bring the FX to on-chain smart contracts, financial institutions would need to develop and enable oracles.

Development of new business models: today, in the context of electronic payments, financial institutions play an essential role in the identification of individuals, the accomplishment of KYC and AML processes, the intermediation of the payments between parties, and the provision of e-money managed today mainly with credit and debit cards, among others. The advent of blockchain networks, tokenized money, and cryptocurrencies might disrupt how some of these tasks are accomplished in the

30. In a book published in 2019 we present the impact of quantum technologies in different industries as well as in cyber security, blockchain, and AI [21]

Figure 10. Cross-Border Payments Architecture.



future, and other roles for financial institutions might also emerge. For instance, peer-to-peer payments may erase intermediaries, blockchain networks may reduce counterpart risk and provide high efficiency for clearings and settlements, and tokenized money can be conditioned with smart contracts. This is at the same time a challenge and an opportunity for financial institutions.

Challenges and next steps for end-user adoption

Digital wallets: as mentioned before, digital wallets can be used for the management of digital assets and credentials. Digital wallets are personal and private repositories, such as a mobile app, that have the potential to allow individuals to have ownership over their digital persona. Key recovery mechanisms, secure authentication, better user experience, and clear business models are required for digital wallets to be adopted worldwide.

Usability: in order for blockchain-based cross-border payments to be worth it, there must be an ecosystem were digital tokens are accepted as a payment method. If sender and recipient order tokenization and detokenization, respectively, for each transaction, then times will not be shorter, and fees will not be lower. This ecosystem is something that needs champions in different industries and from all type of entities, from governments to start-ups. LACChain is working in several countries from Latin America and the Caribbean to develop these ecosystems.

5. TECHNICAL DEVELOPMENT

Architecture of the PoC

The architecture of the PoC was designed and implemented in three layers: front-end, API and back-end, as illustrated in figure 10 and described below:

- the front-end layer allows user interaction via a web interface that requires user authentication using a key vault. Front-end components include a React.js UI that integrates the Ethereum web3.js collection of libraries enabling interaction with the LACChain network as illustrated in the use cases sequence diagrams.
- the API layer consists of two endpoints, one endpoint exposes the business logic for users, roles and accounts, the other endpoint exposes container-based *Citi-API-Proxy* that provides transparent access to Citi's WorldLink API.

The back-end layer comprises:

- container-based Java/Spring Boot business logic application *ManagementService* uses a container-based PostgreSQL database to manage users, roles, and account information.
- container-based Go application *IDB_Service* interacts with the Cross-Border Payments' smart contracts for operations (Execute transfer, Dollars to exchange, Dollars to pesos, Pesos to recipient).
- container-based Eventeum application listens to the smart contract's events using geth and JSON-RPC. In the LACChain network topology [22], writer nodes are the only nodes allowed to broadcast transactions to the network.

Smart Contracts

The smart contracts designed and developed for this PoC are based on the Open Zeppelin library.[23] The smart contracts containing the logic of the PoC are the following:

- Cross-Border Payment smart contract handles the cross-border operations (Execute transfer, Dollars to exchange, Dollars to pesos, Pesos to recipient) on the LACChain network: https://github.com/ccamaleon5/CrossBoarderPayment/blob/master/contracts/CrossBoarderPayment.sol
- eMoney Token smart contract extends the ERC20 token contract and the role-based permissioning scheme allowing the burn money and mint token functionalities, as well as the eMoney transaction states (executeHold, releaseHold, balanceOnHold) based on the ERC2020 token standard: https://github.com/ccamaleon5/CrossBoarderPayment/blob/master/contracts/eMoneyToken/EmoneyToken.sol

The utility smart contracts developed for the PoC are:

- String Util: https://github.com/lacchain/cross-border-management/tree/master/contracts/libraries
- Holder Operator Role: https://github.com/ccamaleon5/CrossBoarderPayment/blob/master/contracts/permissions/HolderOperatorRole.sol

Use Cases

As presented in Figure 11, there are 11 different use cases in the PoC that are described in this section. These use cases relate to the IDB HQ and recipient users, and the Citi Admin user, as the financial institution accomplishing KYC/AML and tokenizing the money. The functionalities accomplished by the Citi Admin user were included in the PoC for demonstration purposes, as these functionalities would most likely be done with a combination of an API balance check and a smart contract to automate the steps outlined below in a production release of the Cross-border payments application.

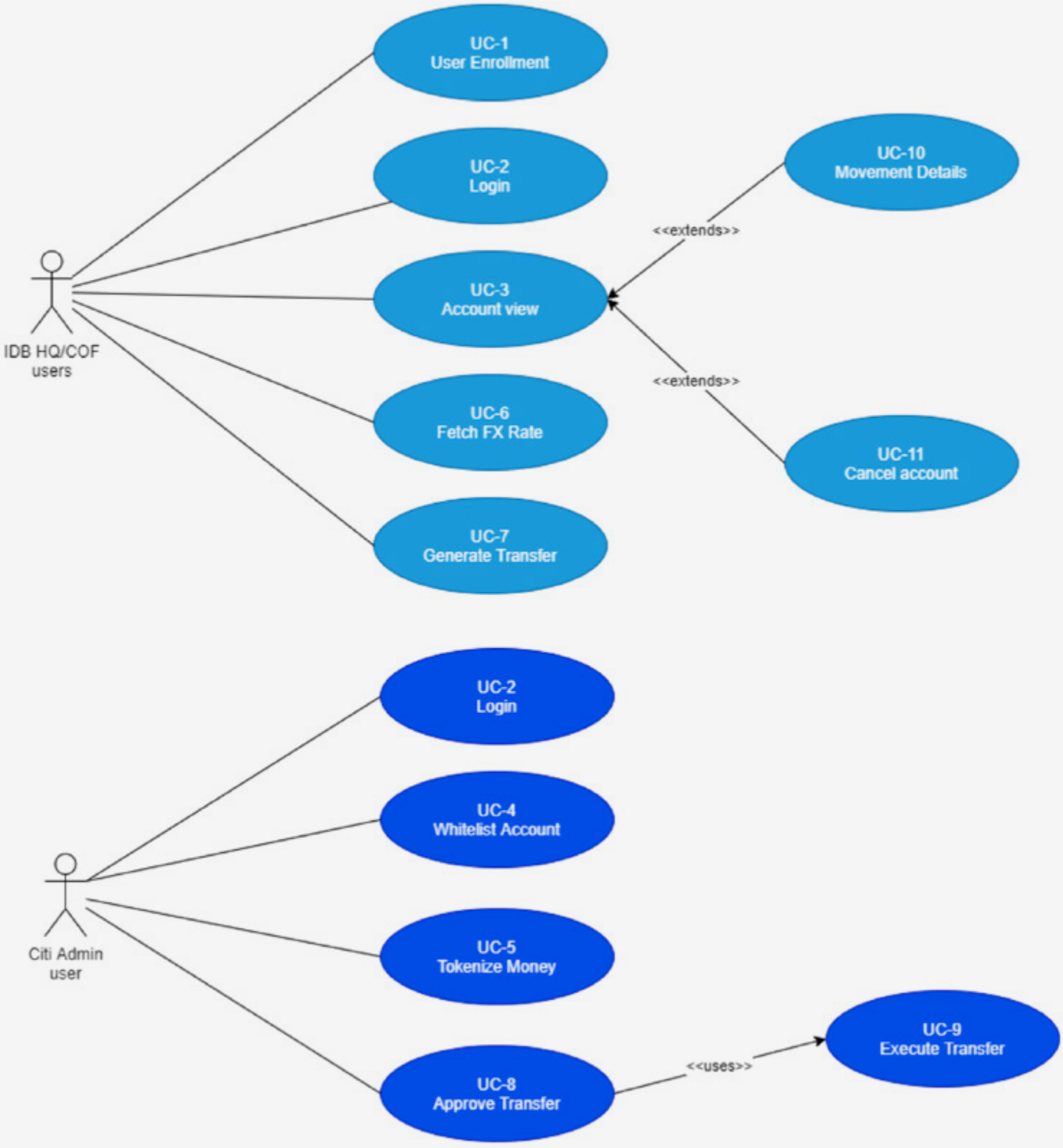


Figure 11. Use cases diagram.

Use case #1

USER ENROLLMENT (SIGN-UP)

ID	UC-1
Name	User enrollment
Description	Functionality that allows users to enroll in the application.
Actor(s)	IDB HQ / Recipient users
Pre-conditions	IDB HQ / Recipient users have a key vault installed with the LACChain network configured and connected.
Main course	**1.** User has access to the enrollment user (sign-up) web interface. **2.** User fills the enrollment form with the following fields: **Account details** **a.** Company Name **b.** Full Name **c.** E-mail **d.** Password **e.** DLT Address (Key vault account address) **Bank details** **f.** Bank Name [1. Citi 2. Other banks] **g.** Bank's Tax ID **h.** Bank City **i.** Bank account number (Account number to which funds will be deposited/withdrawn) **3.** User clicks the **Sign-Up** button. **4.** The application attempts to enroll user.
Alternate courses	AC-1: If IDB HQ / Recipient or Citi Bank user does not have the key vault interface installed, the message "Please make sure you are connected with your key vault with the LACChain network." is displayed and the **Install Key Vault** button is available; user can click on the button to install the key vault interface. AC-2: If the key vault interface is not connected, the message "Please make sure you are connected with the key vault with the LACChain network." is displayed and the **Connect to Key Vault** button is available in the user interface; user can click on the button to open the key vault login user interface. After logging in the key vault, the user interface displays a Connect Request view with the message "CrossBorderPayments would like to connect to your account" and the Connect/Cancel buttons are available; user may click on the Connect button and connect with the LACChain network. AC-3: If user is enrolled the message "The user already exists" is displayed.
Post-Conditions	IDB HQ / Recipient users enrolled in the application.

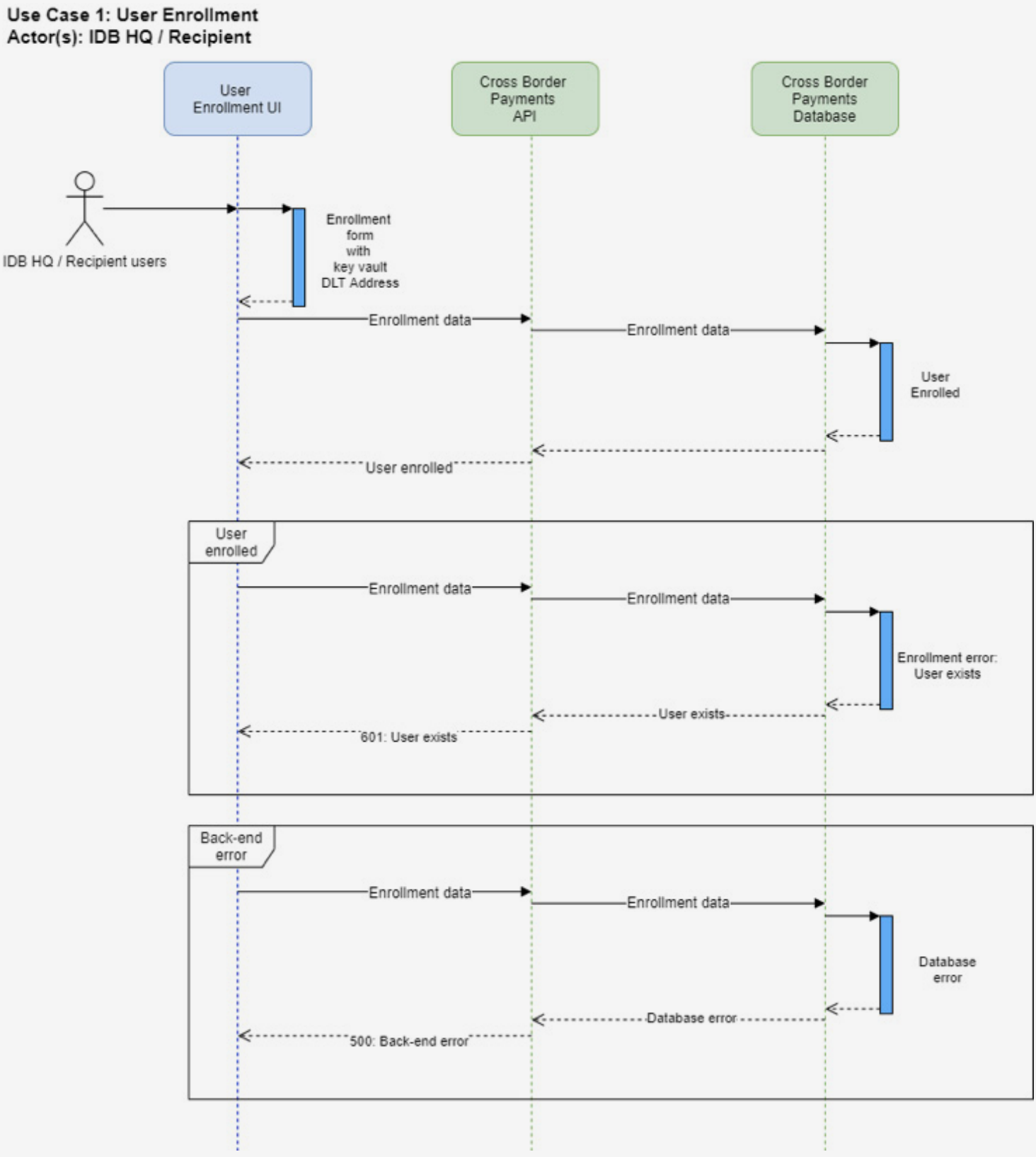


Figure 12. User enrollment sequence diagram.

Use case #2

USER LOGIN (SIGN-IN)

ID	UC-2
Name	User login
Description	Functionality that allows users to log in the application.
Actor(s)	• IDB HQ / Recipient User • Citi Admin User
Pre-conditions	**1.** IDB HQ / Recipient user enrolled in the system. **2.** IDB HQ / Recipient users have the key vault installed with the LACChain network configured and connected.
Main course	**1.** User has access to the sign-in user interface. **2.** User enters DLT Address. **3.** User enters e-mail and password. **4.** User clicks the **Sign in** button. **5.** User has access to the Account view user interface.
Alternate courses	AC-1 and AC-2 same as UC-1. AC-3: If any of the user credentials (e-mail, password or DLT address) is invalid, the message "Invalid email, password or DLT address" is displayed.
Post-Conditions	IDB HQ / Recipient and Citi Admin users logged in the application.

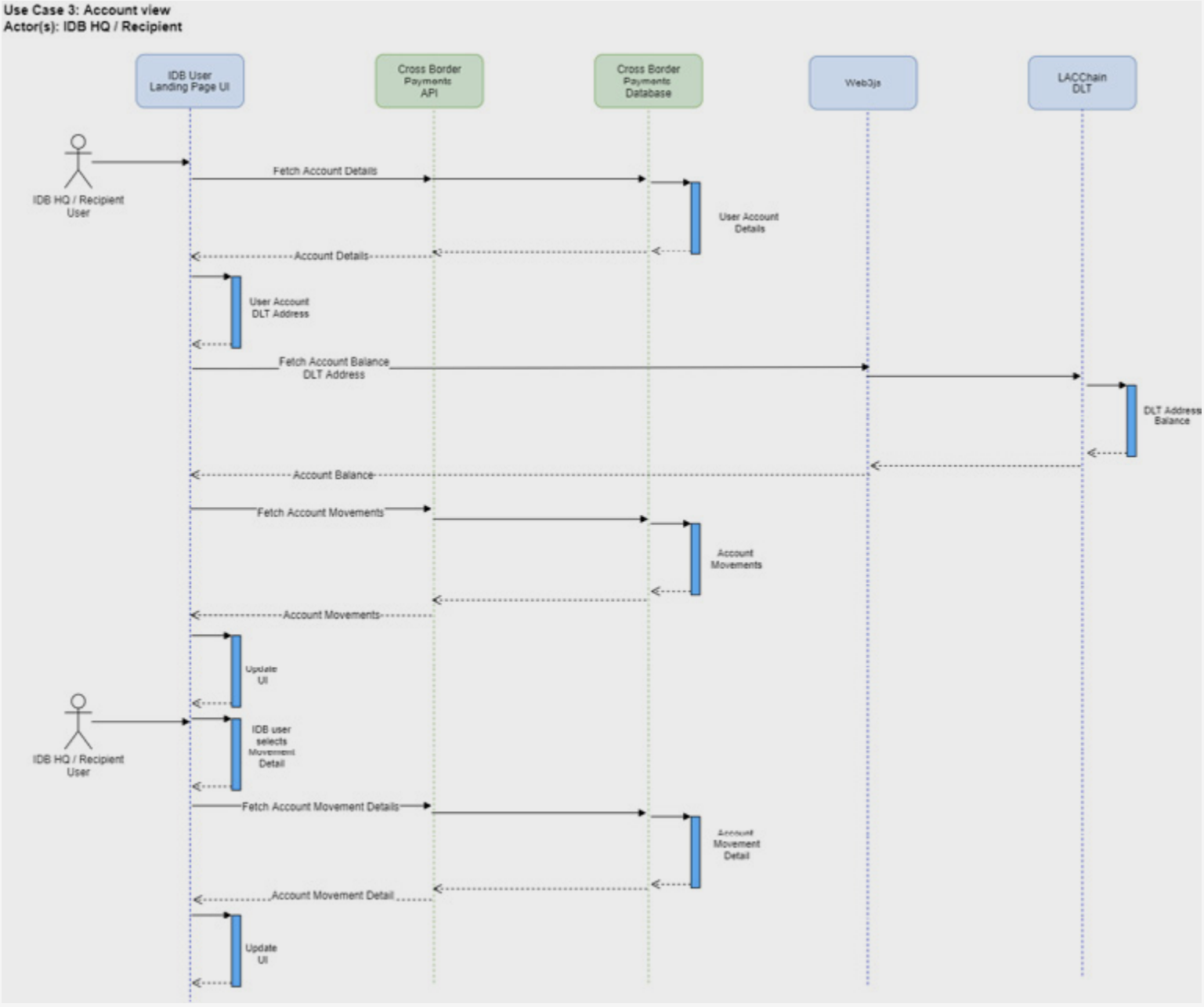
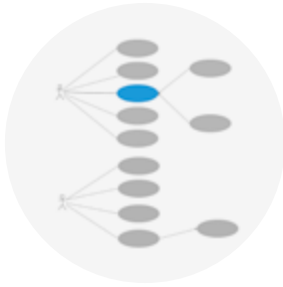


Figure 13. User login sequence diagram.



Use case #3

ACCOUNT VIEW

ID	UC-3
Name	Account view
Description	Functionality that enables users to view their account, account details and movements.
Actor(s)	IDB HQ / Recipient users
Pre-conditions	**1.** IDB user enrolled in the system. **2.** IDB users have the key vault installed with the LACChain network configured and connected.
Triggers	User login (UC-2)
Main course	**1.** The IDB HQ / Recipient users have access to the account view user interface. **2.** The account view provides Account details. **3.** The account view provides Account balance. **4.** The account view provides Account movements with **Date**, **Type**, **From**, **To**, **Amount sent**, **Amount received**, **Rate applied**, **Fee applied**, and **Status.** **5.** The account view provides a **Send Money** button that enables users to perform a cross-border payment. **6.** The account view provides a **Cancel account** button that enables users to de-whitelist the account. **7.** The account view provides a **Log out** button that enables users to log out the cross-border payments application.
Alternate courses	AC-1 and AC-2 same as UC-2.
Post-Conditions	Users visualize account details, account balance and account movements information.

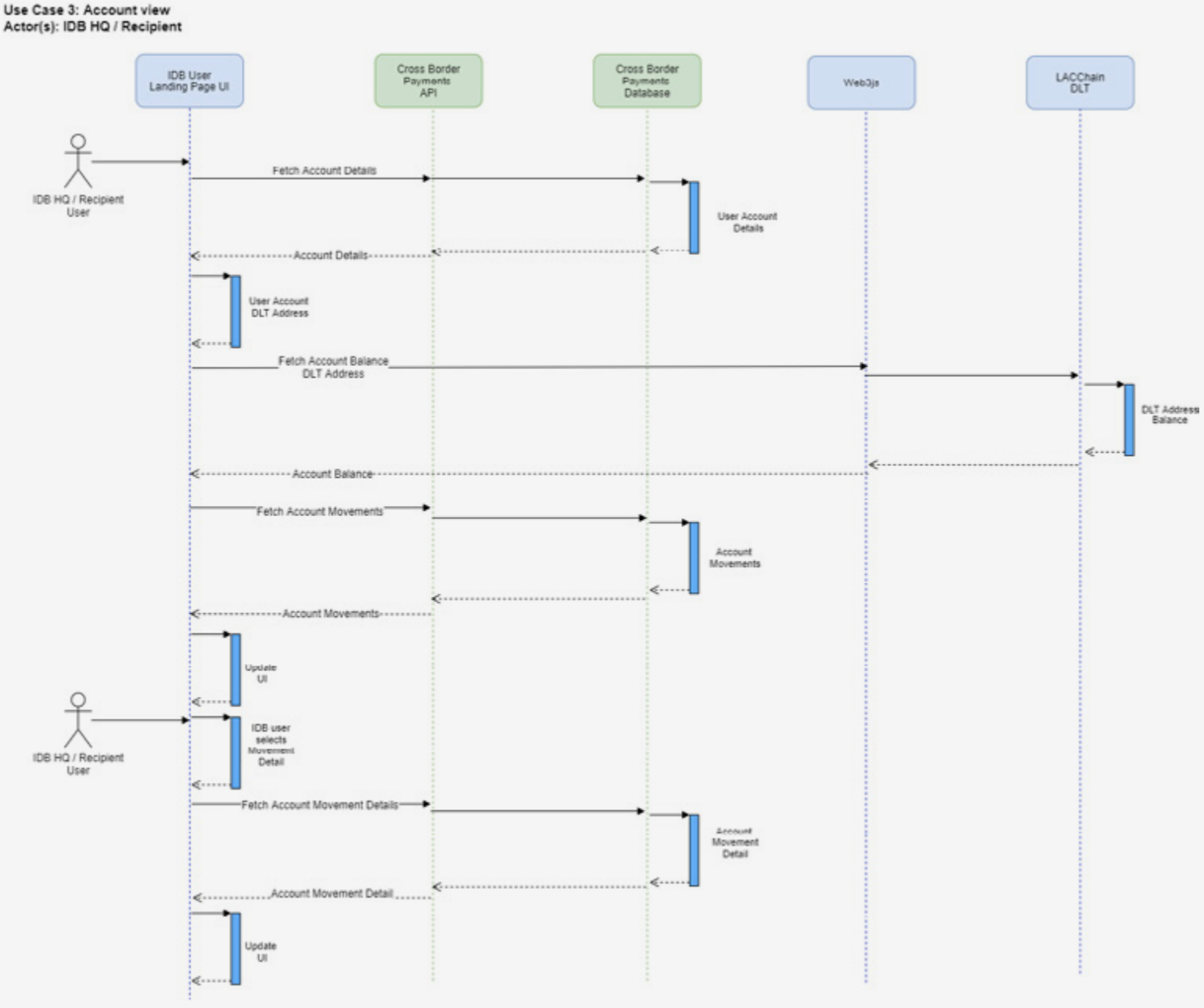
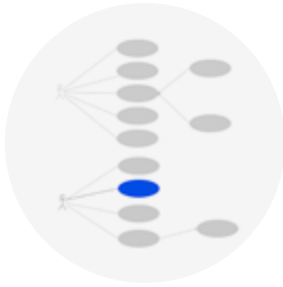


Figure 14. Account view sequence diagram.



Use case #4

WHITELIST ACCOUNT

ID	UC-4
Name	Whitelist Account
Description	Functionality that allows a Citi Admin user to whitelist an account in order to have and transfer tokens.
Actor(s)	Citi Admin user
Pre-conditions	**1.** IDB HQ, Recipient and Citi Bank DLT addresses created. **2.** Citi Admin user has the key vault installed with the LACChain network configured and connected.
Main course	**1.** Citi Admin user has access to the Accounts management user interface. **2.** Accounts management interface provides **Company**, **Name**, **Bank**, **Account Number**, **DLT address**, **Current balance**, and **Status** information for each user account. **3.** Citi admin user selects a non-active (pending) account waiting for whitelisting. **4.** Citi admin user clicks the **Whitelist account** button and is prompted to select a currency for the account. **5.** The whitelist account transaction is broadcasted to the LACChain network by IDB's writer node. **6.** The application listens the transaction consensus (LACChain network) and updates the back-end (API/Database) whitelisting the account. **7.** The Accounts management user interface is updated.
Alternate courses	AC-1 and AC-2 same as UC-1. AC-3: If a back-end error occurs the API returns HTTP code 500.
Post-Conditions	The user account (DLT Address) is whitelisted, in order to have and transfer tokens.

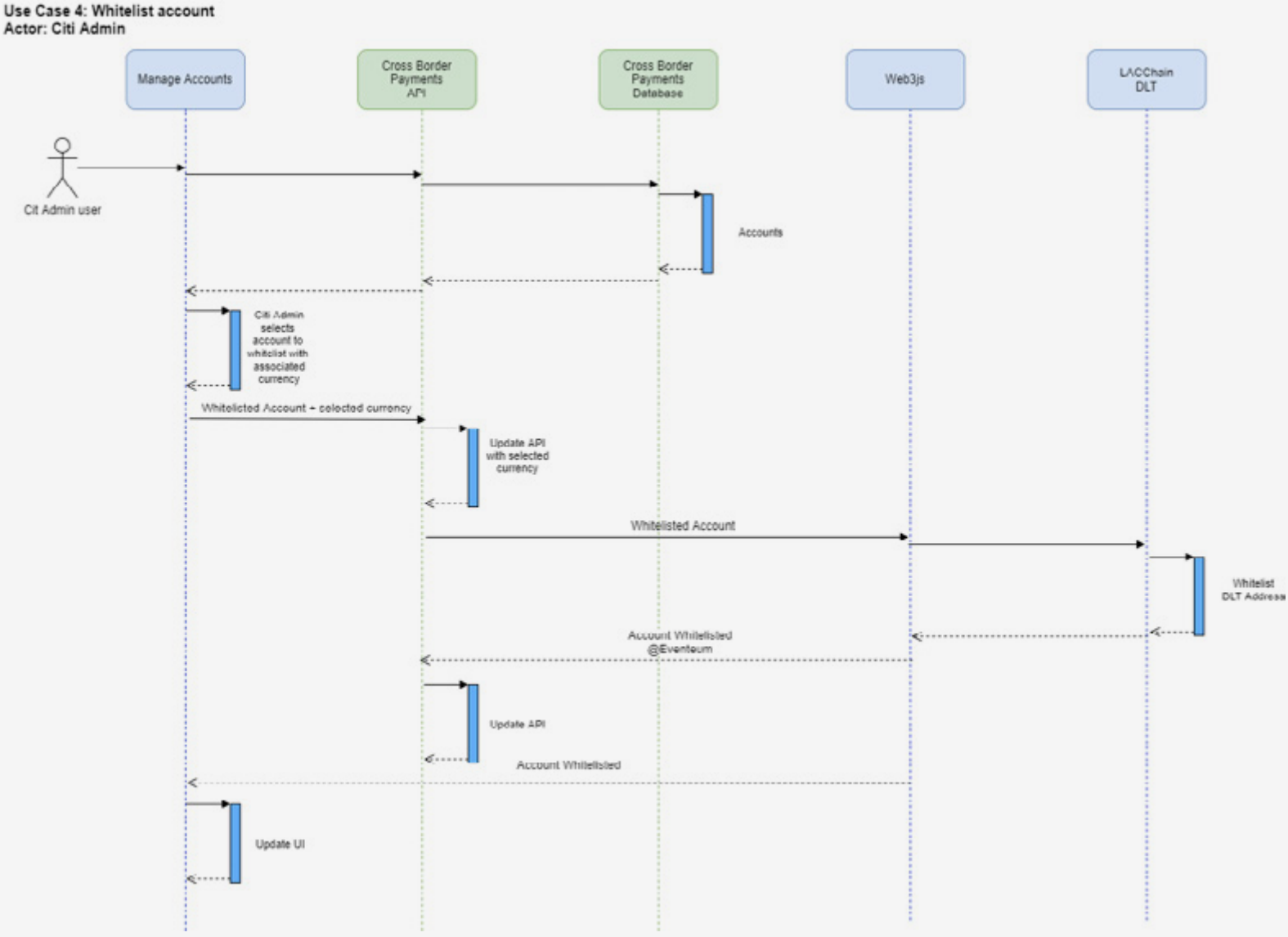
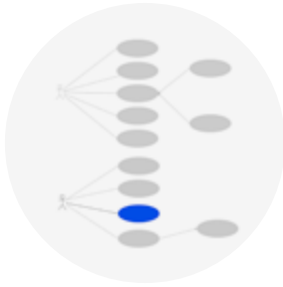


Figure 15. Whitelist account.



Use case #5

TOKENIZE MONEY

ID	UC-5
Name	Tokenize Money
Description	Functionality that allows credit IDB account with tokenized money.
Actor(s)	Citi Admin user
Pre-conditions	**1.** IDB HQ, Recipient and Citi Bank DLT addresses created. **2.** The account where money will be tokenized is whitelisted. **3.** Citi Bank verifies that IDB's fiat money has been deposited in omnibus account.
Main course	**1.** Citi Admin user has access to the Account management user interface. **2.** Citi Admin selects a whitelisted account and has access to account details. **3.** Citi Admin user clicks on the **Tokenize Money** button and is prompted to enter the amount to tokenize. **4.** Citi Admin user inputs amount and clicks on the **Tokenize** button. **5.** The transaction is broadcasted to the LACChain network by IDB's writer node. **6.** The Digital Dollar smart contract containing the logic calls the CrossBorderPayment Logic smart contract and verifies that IDB's account is whitelisted. **7.** The IDB account address is credited with Tokenized Money (digital dollars). **8.** The Digital Dollar smart contract generates an event indicating the amount is credited. **9.** The application listens the transaction consensus (LACChain network) and updates the back-end (API/Database) with the account movement. **10.** The account balance is updated in the user interface.
Alternate courses	AC-1 and AC-2 same as UC-1. AC-3: If a back-end error occurs the API returns HTTP code 500.
Post-Conditions	IDB account is credited with tokenized money.

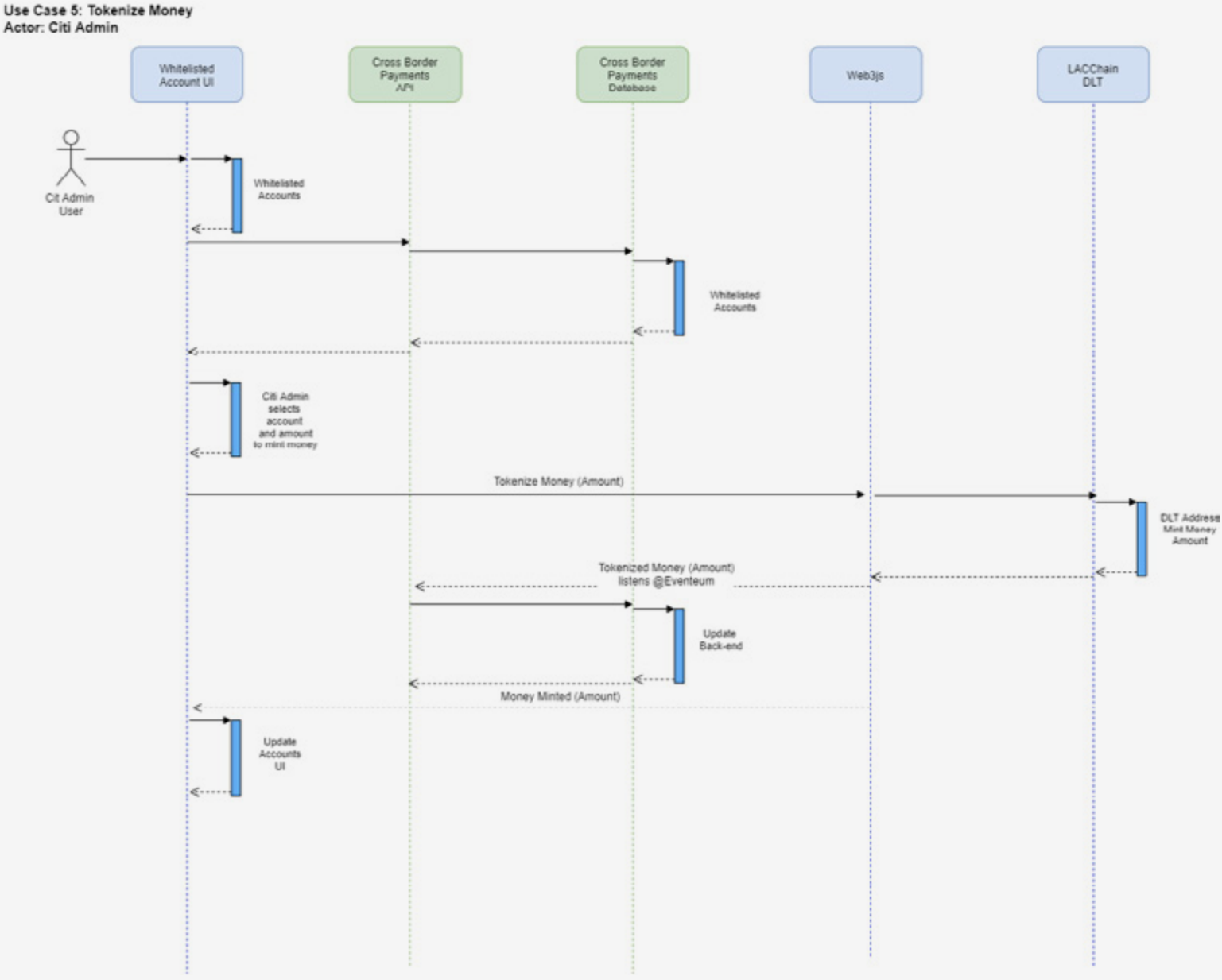


Figure 16. Tokenize money sequence diagram.

Use case #6

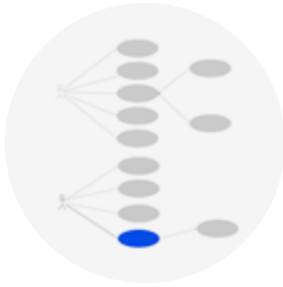
FETCH FX RATE

ID	UC-6
Name	Fetch FX Rate
Description	Functionality that allows IDB HQ users to fetch and provide the FX Rate for the given currency combination.
Actor(s)	IDB HQ user
Main course	**1.** IDB user has access to the fetch FX Rate user interface. **2.** IDB user inputs Amount and Currency. **3.** User interface requests Fetch FX Rate Inquiry via Citi WorldLink API and updates the user interface. **4.** IDB user obtains FX rate information.
Alternate courses	AC-1: User clicks on the Cancel button and the fetch FX Rate operation is cancelled, returning to the previous user interface.
Post-Conditions	IDB user obtains FX Rate information.

Use case #7

GENERATE TRANSFER

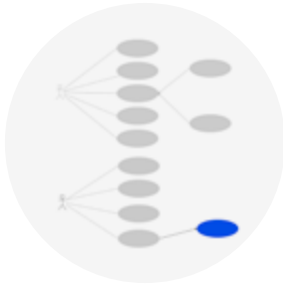
ID	UC-7
Name	Generate Transfer
Description	Functionality that allows IDB HQ users to generate a transfer order to the Recipient.
Actor(s)	IDB HQ user
Pre-conditions	**1.** IDB HQ user enrolled and logged in the system. **2.** IDB HQ user must be logged in with the key vault interface with the LACChain network configured.
Main course	**1.** IDB HQ user has access to account details user interface. **2.** IDB HQ user clicks the **Send Money** button. **3.** IDB HQ user inputs the amount to transfer, Citi WorldLink API is queried to obtain FX Rate (UC-6), and indicative amount the recipient will receive is displayed in the user interface. **4.** IDB HQ user enters recipient details to generate a transfer order: **a.** Recipient DLT address **b.** Recipient Bank account number **5.** After entering recipient details, the application validates that recipient DLT address corresponds with the registered recipient bank account number and displays validation results. **6.** Citi WorldLink API is queried to fetch FX Rate (UC-6) for payment initiation. **7.** The transfer is broadcasted as a transaction to the LACChain network by the writer node. **8.** The smart contract containing the cross-border payment logic checks the whitelist contract and verifies that IDB account is whitelisted to send digital dollars and the IDB recipient account is whitelisted to receive digital pesos. **9.** The digital dollars are held in the IADB HQ blockchain address until the FX information is collected. **10.** The Transfer Order is placed in OnHold state waiting for approval.
Alternate courses	Same as UC-4.
Post-Conditions	IDB HQ user generated a Transfer Order. The Transfer Order is in OnHold state.



Use case #8

APPROVE TRANSFER

ID	UC-8
Name	Approve Transfer
Description	Functionality that enables Citi Admin user to approve the transfer order.
Actor(s)	Citi Admin user
Pre-conditions	A transfer order is in OnHold state.
Main course	**1.** Citi Admin user has access to the Movements management user interface. **2.** Citi Admin user selects a movement with Requested status. **3.** Citi Admin user has access to Movement status and clicks **Approve transfer** button. **4.** The approval is broadcasted to LACChain via IDB's writer node. **5.** The transfer order changes state to Approved and an event is generated. **6.** The movement management user interface is updated, and the movement is displayed with Approved status.
Alternate courses	Same as UC-4.
Post-Conditions	The Transfer Order changes state to Approved and an event is generated.
Comments	• This use case is included for demonstration purposes in the POC. • This use case could include a Transfer amount limit for manual approval.



Use case #9

EXECUTE TRANSFER

ID	UC-9
Name	Execute Transfer
Description	Functionality that executes the transfer.
Actor(s)	Cross-Border Payments application
Pre-conditions	A transfer order is in Approved state.
Triggers	Approve Transfer (UC-8)
Main course	**1.** Citi's WorldLink API is invoked to create a payment initiation. **2.** The transfer order changes state to Executed. **3.** The Executed event is generated, and the transfer is executed. **4.** The transaction is broadcasted to the LACChain network. **5.** The Transfer Order changes state to Executed. **6.** The smart contract burns the digital dollars, generates a fee in digital dollars that goes to Citi's account address. **7.** The smart contract mints the digital pesos for IDB's account address.
Post-Conditions	Recipient verifies his blockchain address has been credited.

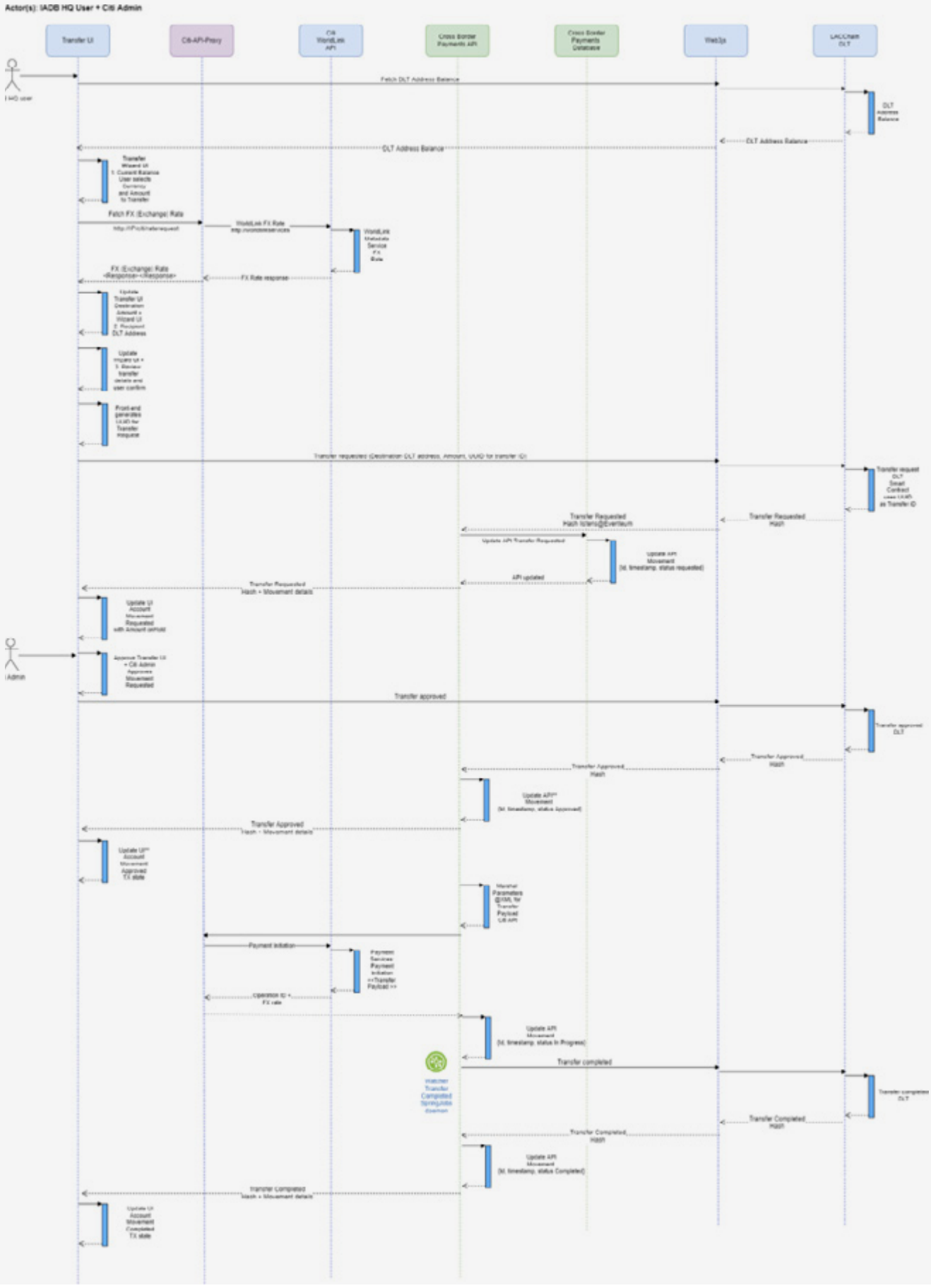


Figure 17. Fetch FX Rate, Generate Transfer, Approve Transfer, and Execute Transfer.

Use case #10

MOVEMENT DETAILS

ID	UC-10
Name	Movement Details
Description	Functionality that allows an IDB user to view movement details.
Actor(s)	IDB HQ / Recipient users
Pre-conditions	**1.** IDB user enrolled and logged in the system. **2.** IDB user must be logged in with the key vault interface with the LACChain network configured.
Main course	**1.** IDB user has access to the account view user interface. **2.** The account view provides Account Movements and the user clicks the **See details** button. **3.** IDB user has access to the Movement details user interface. **4.** The Movement details view provides **Status**, **Tracking information**, **Transfer details**, **Sender details**, **Recipient details**, and **Movement history**. **5.** IDB user clicks the X button to exit the Movement details user interface and return to the account view. **6.** The account view provides Account balance.
Post-Conditions	IDB HQ / Recipient users visualize Movement details.

Use case #11

CANCEL ACCOUNT

ID	UC-11
Name	Cancel Account
Description	Functionality that allows an IDB user to Cancel (inactive) its account.
Actor(s)	IDB HQ / Recipient users
Pre-conditions	**1.** IDB HQ, Recipient and Citi Bank Metamask addresses created. **2.** Citi Admin user has the key vault installed with the LACChain network configured and connected.
Main course	**1.** IDB user has access to the Account details user interface. **2.** IDB user clicks on **Cancel account** button. **3.** The smart contract de-whitelists the user account. **4.** The unwhitelist account transaction is broadcasted to the LACChain network by IDB's writer node. **5.** The application listens the transaction consensus (LACChain network) and updates the back-end (API/Database) whitelisting the account. **6.** The Accounts management user interface is updated. **7.** The Account details user interface is updated, and the account is displayed as inactive. **8.** The account is unable to tokenize, send or receive money.
Alternate courses	AC-1 and AC-2 same as UC-1. AC-3: If a back-end error occurs the API returns HTTP code 500.
Post-Conditions	The user account (DLT Address) is inactive, unable to tokenize, send or receive tokenized money.

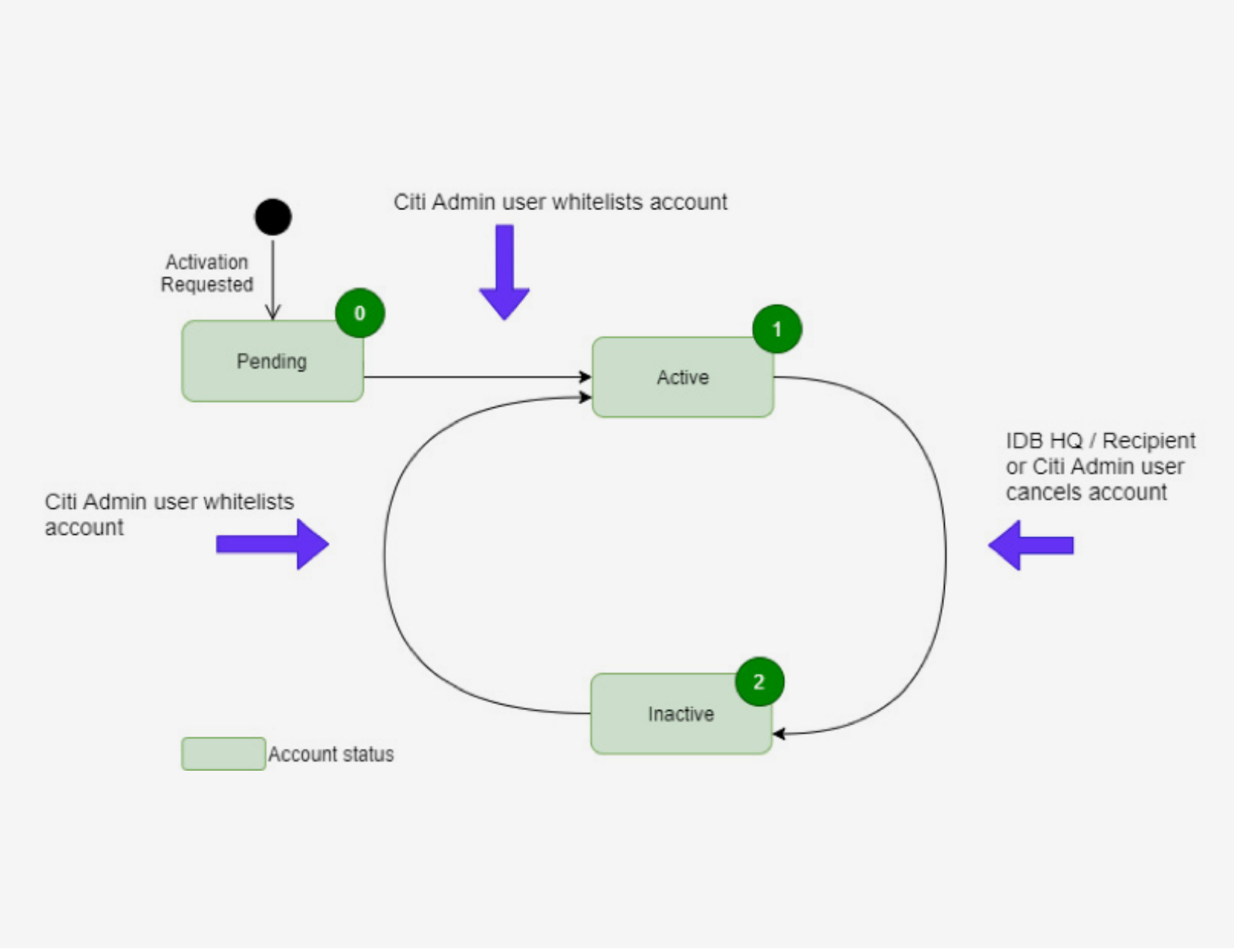


Figure 18. User account status diagram.

Account statuses

Account state 0 (Pending) represents when an end user signs-up in the Cross-Border payments application and requires account whitelisting. Once a Citi Admin has whitelisted the account, its status changes to 1 (Active) and has access to all PoC functionalities, in Active status the end user or the Citi Admin may cancel the account changing its status to 2 (Inactive) and unable to tokenize, send or receive money. A Citi Admin can whitelist the account changing its status to 1 (Active) and continue to access the functionalities. Figure 18 illustrates the account statuses.

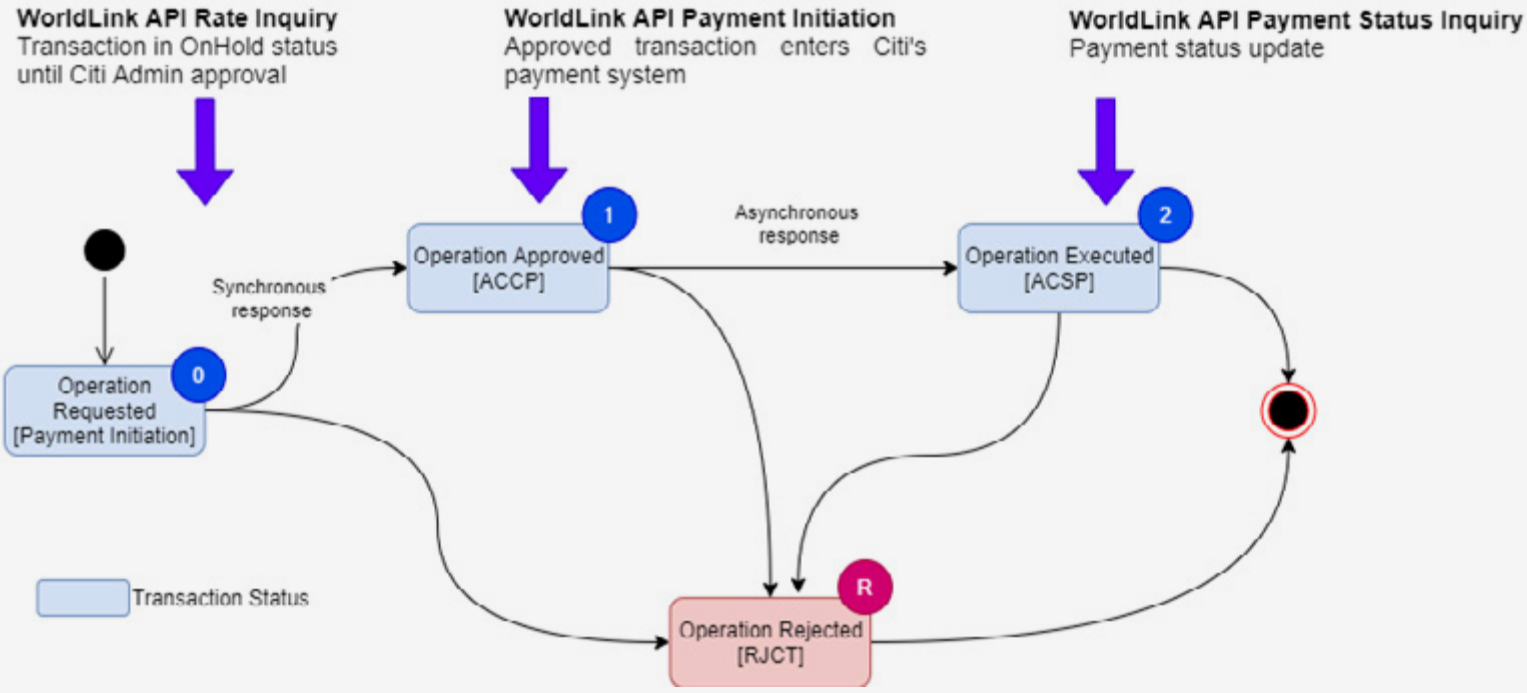


Figure 19. Transaction status diagram.

Transaction statuses

After executing the API Rate inquiry call, the transaction status 0 represents the operation request (known as Payment Initiation in the payment system), transaction is in OnHold state requiring transfer approval. Once approved, transaction status changes to state 1 entering the payment system with a synchronous response (payment system status is ACCP). Once the transfer is executed in the payment system, the transaction changes to status 2 (payment system status is ACSP and funds are disbursed to recipient account) and the operation is completed in the Cross-Border payments application. Figure 19 depicts the transaction statuses.

6. CONCLUSIONS

In this PoC we demonstrated that cross-border payments using blockhain -particularly the LACChain Blockchain Besu Network- in combination with the Citi WorldLinkPayment System are faster and more traceable, and can also be cheaper, than solutions using current technology. We believe that decentralized registries of information, peer-to-peer solutions, emerging digital and crypto financial assets, and digital wallets have the potential to bring substantial changes to the financial system and the work of international development organizations. Faster, traceable, cheaper cross-border payments can bring a transformative impact to markets and industries. They have the potential to improve the terms of development financing through grants and loans to the countries, as well as enabling more efficient remittance corridors across the LAC region, among other use cases. There are, however, many challenges yet to be faced in order for these new elements to be used worldwide and for blockchain-based cross-border payments to be chosen as the first option by a majority of large financial institutions.

We have identified some relevant limitations and opportunities and classified them into the areas of blockchain networks, financial institutions, and end-user adoption. We understand that blockchain networks need to continue to improve on the consolidation of robust blockchain-based identities, secure and user-friendly key management, assurance of the transaction scalability (fees and throughput), optimal models for the distribution of resources, interoperability between multi-purpose blockchain networks and specific-purpose settlement networks, legal frameworks and regulatory policies, and quantum safeness. With regard to financial institutions, we consider that it could be interesting to address KYC and AML of blockchain-based identities, integrations with core financial systems, FXs on the fly, and the development of new business models around the technology. Last but not least, with respect to the end-user adoption, the consolidation of digital wallets and the raise of an ecosystem of digital services that incorporates e-money and b-money tokens would be necessary for blockchain-based cross-border payments to become mainstream.

REFERENCES

[1] https://www.lacchain.net/

[2] Cross-Border Interbank Payments and Settlements. (2018). Project Jasper. Retrieved from https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/

[3] Enabling Broad Ecosystem Opportunities. (2019). Project Ubin Phase 5. Retrieved from https://www.mas.gov.sg/schemes-and-initiatives/project-ubin

[4] Pushing the Limits of Interbank Payment Settlement with Blockchain. (2019). Project Kokha. Retrieved from https://consensys.net/blockchain-use-cases/finance/project-khokha/

[5] Supporting DLT Settlement Models. (2019). RTGS Renewal Programme. Retrieved from https://www.ledgerinsights.com/bank-of-england-blockchain-dlt/

[6] Balancing Confidentiality and Auditability in a Distributed Ledger Environment. (2020). Project STELLA. Retrieved from https://www.boj.or.jp/en/announcements/release_2020/rel200212a.htm/

[7] https://www.lb.lt/en/lbchain

[8] Distributed Ledger Technical Research in Central Bank of Brazil. (2017), Banco Central do Brasil. Retrieved from https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf

[9] Project Inthanon and the Project DLT Scripless Bond. (2019). ADBI Institute. Retrieved from https://www.adb.org/sites/default/files/publication/535851/adbi-wp1030.pdf

[10] Second Special Issue of the e-Krona. (2020). Sveriges Riskbank. Retrieved from https://www.riksbank.se/globalassets/media/rapporter/pov/engelska/2020/economic-review-2-2020.pdf

[11] https://entethalliance.org/enterprise-ethereum-alliance-launches-blockchain-neutral-token-taxonomy-initiative-to-accelerate-a-token-powered-blockchain-future/

[12] T. Adrian and T. Mancini. (2019). The rise of digital money. International Monetary Fund. Retrieved from https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097

[13] https://emoneytokenstandard.org/

[14] Distributed ledger technology use cases. (2019). ITU-T FG DLT. Retrieved from https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf

[15] https://www.hyperledger.org/use/besu

[16] Decentralized Identifiers v1.0. (2021). World Economic Forum. Retrieved from https://www.w3.org/TR/did-core/

[17] Verifiable Credentials v1.1. (2019), World Economic Forum. Retrieved from https://www.w3.org/TR/vc-data-model/

[18] LACCHAIN DI PAPER SSI

[19] CNSA Suite and Quantum Computing FAQ. (2016). NSA. Retrieved from https://apps.nsa.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm

[20] Report on Post-Quantum Cryptography. (2016). NISTIR 8105. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[21] PAPER QUANTUM Retrieve from https://publications.iadb.org/en/quantum-technologies-digital-transformation-social-impact-and-cross-sector-disruption.

[22] https://github.com/lacchain/besu-network/blob/master/TOPOLOGY_AND_ARCHITECTURE.md

[23] https://github.com/OpenZeppelin/openzeppelin-contracts


IDB | LAB
LACCHAIN
10 YEARS
CITI INNOVATION LABS
ioBUILDERS