UNIVERSIDADE DO PORTO • FACULDADE DE ENGENHARIA

Blockchain Technologies Applied to Interbank Transactions

João Carlos Ribeiro Duarte

July 2019

Scientific Supervision by

Filipe Figueiredo Correia, Assistant Professor
Department of Informatics Engineering

Master in Informatics and Computing Engineering

Contact Information:

João Carlos Ribeiro Duarte
Faculdade de Engenharia da Universidade do Porto
Departamento de Engenharia Informática

Rua Dr. Roberto Frias, s/n
4200-465 Porto
Portugal

Tel.: +351 22 508 1400
Fax.: +351 22 508 1440
Email: up201303834@fe.up.pt
URL: https://joaocarduarte.github.io/

. . . to my family and friends

This page was intentionally left blank.

Abstract

Nowadays, interbank transactions are costly and can take several days to be completed. The need of intermediary financial institutions and the need for a system of nostro accounts to sustain transactions between banks, makes all this process costly, not only for the customers but also for the banks themselves.

Projects as *RippleNet*, *IBM Blockchain World Wire* and even *SWIFT gpi* try to create solutions based on blockchain technologies to address the main problems that interbank transactions currently face. However, they are heavily controlled by central entities which need to exist in order for their projects to operate. This goes against one of the blockchain main principles: decentralization.

This work proposes a decentralized solution based on blockchain technologies that tries to address three main problems with the current way of processing interbank transactions: transaction time, transaction cost and the need for nostro accounts.

The solution consists of a private cryptocurrency/fiat exchange for each bank that works autonomously and has its main functionality quasi-instant money transfer to other banks. This is done without the need for the customer to be aware that cryptocurrencies are being used, neither that market orders are being placed. This functionality is only possible due to the trading volume on each exchange.

The *stellar blockchain* was used to create a prototype of the proposed approach. Stellar's native cryptocurrency, *XLM*, can be traded for fiat money on the exchange.

The validation process took into consideration the stated problems with the current way of processing interbank transactions, being the developed solution compared to the existing solutions mentioned previously.

Despite the difficult comparison due to the lack of specific data from the contending solutions, the prototype presented competitive results considering the time and cost of a transaction. There is no need for nostro accounts in order to the solution to work, however, in case of low trading volume on the platform, the bank would have to invest funds to populate the exchange with market orders. This investment is comparable to the investment made into nostro accounts on other existing solutions.

Resumo

Atualmente, as transações interbancárias são dispendiosas e podem levar vários dias para serem concluídas. A necessidade de instituições financeiras intermediárias e a necessidade de um sistema de contas nostro para sustentar transações entre bancos, torna todo esse processo caro, não só para os clientes, mas também para os próprios bancos.

Projetos como *RippleNet*, *IBM Blockchain World Wire* e até mesmo *SWIFT gpi* tentam criar soluções baseadas em tecnologias da blockchain para abordar os principais problemas que as transações interbancárias enfrentam atualmente. No entanto, estes projetos são fortemente controlados por entidades centrais que precisam de existir para que seus projetos funcionem. Isso vai contra um dos principais princípios do blockchain: a descentralização.

Este trabalho propõe uma solução descentralizada baseada em tecnologias da blockchain que tenta resolver os três principais problemas com a forma atual de processar transações interbancárias: tempo de transação, custo de transação e necessidade de contas nostro.

A solução consiste numa exchange privada de criptomoedas/fiat para cada banco que trabalha de forma autónoma e tem como funcionalidade principal a transferência de dinheiro quase instantânea para outros bancos. Isso é feito sem a necessidade de o cliente ter noção de que estão a ser usadas criptomoedas, nem que estão a ser feitas ordens de mercado. Essa funcionalidade só é possível devido ao volume de trocas em cada exchange.

A *stellar blockchain* foi usada para criar um protótipo da abordagem proposta. A criptomoeda nativa da stellar, *XLM*, pode ser trocada por dinheiro fiat na exchange.

O processo de validação teve em consideração os problemas com a forma atual de processar as transações interbancárias, sendo a solução desenvolvida comparada às soluções existentes mencionadas anteriormente.

Apesar da difícil comparação devido à falta de dados específicos das soluções concorrentes, o protótipo apresentou resultados competitivos considerando o tempo e

o custo de transação. Não há necessidade de contas nostro para que a solução funcione, no entanto, em caso de um baixo volume trocas na plataforma, o banco teria que investir fundos para popular a exchange com ordens de mercado. Esse investimento é comparável ao investimento feito em contas nostro noutras soluções existentes.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Nowadays, interbank transactions are made through financial institutions which use, not only, an outdated unidirectional messaging protocol to communicate the transactions information between them, but also, a costly and complicated fund transaction system.

With the emergence of blockchain technologies, some projects were created with the promise to revolutionize the current way that interbank transactions are processed [1]. This caught the eye of financial institutions and companies that provide solutions for banking area.

EbankIT is an Omnichannel banking software company that creates products focused on delivering the most widely adopted banking solutions to its customers [2]. Following the trend, EbankIT considers that blockchain technologies are the way to improve and modernize the current interbank transactions process and an opportunity to extend the array of products that already offers.

1.1 The need for evolution

Interbank transactions may have to cross long routes through sequences of financial institutions correspondence. In the case of the cross-border transaction or even cross-currency transaction, the sequence of intermediaries can be further and more fees can be applied [3].

EbankIT has interest in using blockchain technologies to improve the way that interbank transactions are made, not only, to provide the better solutions to their customers, but manly, to add a blockchain based solution to their array of products, which is almost a requirement for a software development company in the banking

field nowadays.

The need of improvement of interbank transactions and ebankIT desire to introduce a blockchain technologies based solution to their array of products raises a problem that can be summarized in the following sentence: *How blockchain technologies can be applied to improve interbank transactions?*

1.2 Current issues

As previously said, current interbank transactions are supported by correspondent banking arrangements that allows the sender bank transact funds to the receiver bank through a sequence of intermediaries if the sender and the receiver banks don't have a direct correspondence, in other words, if the two banks don't have an agreement between them to allow direct transaction of funds. For this to be possible, financial institutions need to keep huge sums of funds in accounts inside all banks with which they have correspondence. According to Ripple, over than 27 trillion dollars are kept inside these accounts all around the world [4].

The need for intermediaries leads to bigger transactions times and more costly fees. An interbank transaction can take more than 3 days to be processed, depending on the number of intermediaries required for that transfer [5]. The same goes for fees cost, with more intermediaries more transfer rates will be added together. In the case of cross-currency transactions, expensively fixed exchanges rates are also applied.

Current interbank transactions are dependent on a costly and time-consuming system which is heavily controlled by a central entity and constantly needs to rely on intermediaries.

1.3 Contributions and Goals

As the outcome of the present thesis, it is expected to achieve an extensive study through literature and technology review, the design of a solution and a prototype of that solution.

Initially, an extensive search through literature will be done to gather information about the background of interbank transactions and blockchain technology in order to list existing issues on the current way of transferring between banks and to delimit the possible aspects where blockchain technologies can be applied.

Then, different existing interbank transactions solutions with and without blockchain technologies will be analyzed. This technology review will grant information and data about the way existing solutions approach the transaction of money between banks.

To finish, with the acquired information through literature and technology review, a solution applying blockchain technologies will be designed to improve the current way interbank transactions are made. A prototype of the designed solution will then be developed.

The main goals of the expected solution contemplate the following topics:

- Decrease interbank transaction time;
- Decrease interbank transaction cost;
- Remove the need for intermediaries;

1.4 Document Structure

The present dissertation is structured into 7 chapters.

Chapter 1 is a brief introduction to the topics addressed in this document. This chapter is composed of a simple explanation of the context, a quick problem definition and the motivation for that existing problem and, finally, the presentation of the proposed objectives and expected contributions.

Chapter 2 is divided into two parts. The first one explains how the current interbank transactions are processed. The second part introduces the blockchain and some related concepts.

Chapter 3 presents existing solutions and their approaches to the defined problem. At the end of this chapter, some cryptocurrencies related to those existing projects are analyzed and explained.

Chapter 4 exposes a more complete picture of the problem, introduces the central hypothesis this document defends and explains the methodology used throughout the rest of the work.

Chapter 5 presents a possible solution having into account the problems and concerns defined in Chapter 4.

Chapter 6 summarizes the design and implementation process of the solution defined in Chapter 5.

Chapter 7 compares the produced solution with the existing solutions analyzed in Chapter 3, having into account the problems and concerns defined in Chapter 4. At the end of the chapter are given some conclusions and suggested possible future works.

Chapter 2

Finance and Blockchain technologies

As mentioned in the previous chapter, interbank transactions currently face some issues that can have a solution in blockchain technologies.

To better understand this process and these technologies, the present chapter is divided into two parts. The first part explains the current way that interbank transactions are processed, addressing the messaging system used, the correspondent banking arrangements and the global payments. The second part aims to introduce blockchain technologies and to synthesize some related concepts.

2.1 Interbank Transactions

Nowadays, transactions between banks are sustained by the SWIFT messaging system, which establishes communication paths, and correspondent banking arrangements, that allow funds settlement.

2.1.1 SWIFT messaging system

Currently, the majority of the communications between banks are supported by the SWIFT messaging system [6].

Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a cooperative undertaking controlled by its members, banks and other financial institutions, that provides secure messaging services and interface software for payment systems [7].

SWIFT messaging services went live in 1977 to replace an older technology called Telex that was used by banks to communicate instructions related to cross-border transfers. SWIFT offered higher speeds of messaging, lower costs, increased volumes

and more secure transactions in comparison to Telex. When the estimated cost for sending a letter of credit by Telex was on average 13USD, a SWIFT message would only cost 50 cents [8].

Since then, the SWIFT messaging system represents the primary communications channel for banking area, being used by more than 11,000 financial institutions all around the world. SWIFT is committed to the confidentiality, integrity, and availability of its messaging services [9].

In order to use SWIFT, all members need to pay a one-time joining fee, annual charges, and messaging fees [8].

2.1.2 Correspondent Banking Arrangements

When a customer wants to make a transaction between two different banks, the money is transferred from one institution to the other through correspondent banking arrangements. If these two banks don't have a direct correspondence will be required the use of intermediaries [7].

Two banks need to maintain a system of nostro/vostro accounts in order for a transaction to occur between them. Nostro refers to "our account of our money on your books" and vostro refers to "your account of your money on our books" [10].

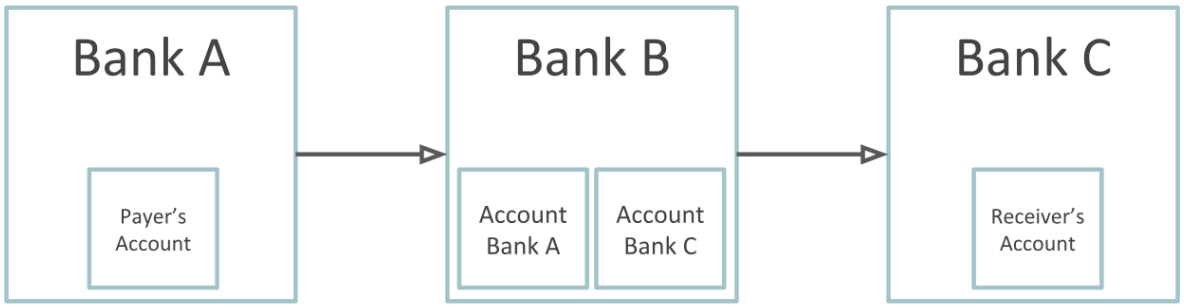

Figure 2.1: Example of correspondent banking system.

Figure 2.1 illustrate the settlement of one payment from Bank A to Bank C via a correspondent banking chain. Since Bank A and Bank C do not hold Nostro accounts with each other, they need to use an intermediary: Bank B, which holds Nostro accounts for both Bank A and Bank C. The transaction is processed in the following steps:

1. Debiting of payer's account in Bank A;
2. Payments message from Bank A to Bank B;

3. Debiting of Bank A's account in Bank B;
4. Crediting of Bank C's account in Bank B;
5. Payment Message from Bank B to Bank C;
6. Crediting of receiver's account in Bank C.

Generally, there could be more intermediaries involved in all this process. All banks in this correspondent banking chain will need to have funds available in their nostro accounts in order to execute the payment.

2.1.3 Global Transfers

Cross-border transactions face many hurdles and delays because of country-specific regulations, currency differences (cross-currency transactions) and the need for more intermediaries [3].

Nowadays, most international transactions occur in a very similar way to transactions between banks from the same country, using SWIFT messaging service and correspondent banking arrangements [11].

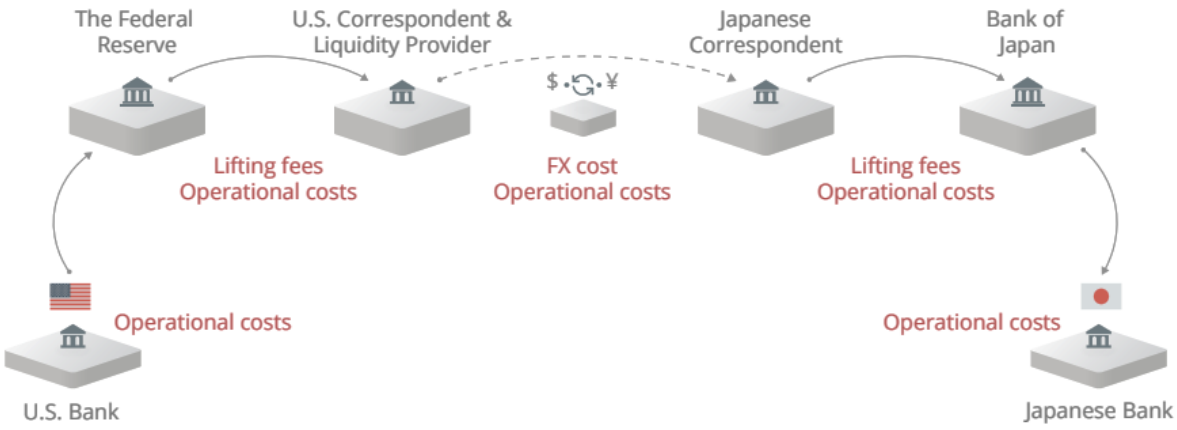

Figure 2.2: Cross-currency transactions. Adapted from [5].

As can be seen in Figure 2.2, in addition to transfer fees, exchange fees are also applied in a cross-currency transaction.

2.2 Blockchain

The blockchain is a decentralized and distributed ledger that keeps continuous updated digital records.

Unlike traditional databases that are maintained by a central entity, a distributed ledger has a network of nodes with replicated and synchronized databases, visible to anyone within the network. This type of network can be private, with restricted membership, or public, accessible to anyone.

2.2.1 The birth of blockchain and how it works

Blockchain was introduced with bitcoin in 2008 as a solution to the double-spending problem [12][13][14]. Double-spending is when two or more transactions simultaneously claim the same output [15]. In other words, when a user submits multiple transactions spending the available balance multiple times.

A blockchain database contains two types of records: transactions and blocks.

Transactions are batched into timestamped blocks. Each block is identified by a cryptographic hash. In addition to carrying a list of transactions, each block also references the hash of the previous block. As can be seen in Figure 2.3, this results in a link between the blocks, creating a chain of blocks [16].

The first block of a blockchain, also known as Genesis, is the only block which doesn't refer to the hash of the previous block since it has no parent [13].

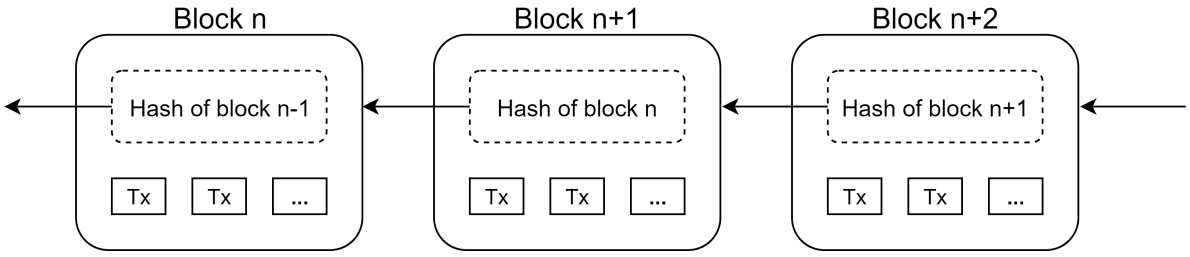

Figure 2.3: Representation of a chain of blocks. Adapted from [12] and [13].

A blockchain network is composed of a set of clients, called nodes. Each one of these nodes holds a copy of the blockchain, forming a peer-to-peer network.

The process to add transactions to the blockchain go through the following steps:

1. Users use a pair of private and public keys to sign their transactions.
2. Those transactions are broadcasted by their respective source node to its nearby peers.
3. The neighboring nodes validate the transactions and then repeat the previous step until the transactions are spread across the network.

4. After being validated by the network, the transactions are ordered and listed into a timestamped candidate block which is broadcasted back to the network, in a process called mining.

5. The network of nodes verifies if the block contains valid transactions and if refers to the correct previous block

6. If everything is right, the block is added to the blockchain and the transactions are applied.

To decide if an incoming transaction is valid or not, certain rules, that each transaction should conform to, are programmed into all blockchain clients. Based on this set of rules a client will then decide if the transaction should be relayed to the network or not.

2.2.2 Achieving Consensus

Any blockchain network needs a distributed consensus mechanism to achieve consensus in the network and to maintain a unique chronological chain.

Without a consensus mechanism, the blockchain would end up with forks of the chain every time nodes didn't agree on the transactions or their listed order on a certain mined block.

Given the type of the blockchain network, the type of distributed consensus mechanism used varies.

In the bitcoin blockchain, the entire network verifies the transactions. If the majority of the nodes agrees on the transactions they are listed on the blockchain. However, this raises a problem: the possibility of Sybil attack [17]. A single entity could set up multiple identities to get multiple votes and thus influences the network by constituting the majority.

To prevent Sybil Attacks, bitcoin uses proof of work protocol that makes the ability to verify the transactions depending on the computing power and not on the number of identities. To verify the transactions, nodes need to solve a cryptographic puzzle, which aims to artificially increase the computational cost. Bitcoin uses the SHA-256 [18] hash function as the cryptographic puzzle, but there are other hashing algorithms used in other blockchains, such as scrypt [19] in Litecoin [20].

In private blockchains, there is no need for costly consensus protocols, since all participant identities are white-listed. The consensus mechanisms used in this type of blockchains aim to provide solutions only to the Byzantine Generals Problems [21].

2.2.3 Private or public blockchains

Blockchains networks can be categorized into two types: public and private [22][23].

Public blockchains (permissionless ledger) are open-source networks without any restriction of access and use.

Private blockchains (permissioned ledger) refer to networks that require the authorization of participant to access the blockchain. Unlike public blockchains, these networks are usually developed and used by companies or group of companies inside their own private commercial environment.

2.2.4 Cryptocurrencies

As mentioned in Section 2.2.1, the birth of blockchain technology is directly related to cryptocurrencies, since blockchain was introduced with bitcoin in 2008 and followed by many more cryptocurrencies projects using this technology.

Cryptocurrencies are transferable digital assets secured by blockchain networks. Cryptocurrencies can represent any type of value, in other words, they can represent money, access to services or even the ownership of property [24].

There are a variety of cryptocurrencies with different purposes and use cases: privacy coins, supply chain-oriented coins, transaction-oriented coins, stable coins, and many others.

Both transaction oriented coins and stable coins are further discussed in this document since these two groups of coins are heavily related to the transaction of funds and the value of those funds.

Transaction oriented coins are cryptocurrencies that were created to offer faster transactions, a higher number of transaction per second and lower fees. On the other hand, stable coins are cryptocurrencies that try to suppress the price volatility of those coins which is already a well know controversial characteristic of cryptocurrencies.

2.2.5 Cryptocurrency trading platforms

Cryptocurrency trading platforms are exchanges that allow users to trade a cryptocurrency for another or even trade fiat money for cryptocurrencies.

It is possible to delineate two groups of cryptocurrency trading platforms. The first group of platforms is more simple and user-friendly, that allow users with less experience to buy/sell and trade cryptocurrencies, bound to higher fees. In contrast,

the second group of platforms has smaller fees and more trading options, but they are complex and aimed for more experienced users.

As an example of the first group, we have Coinbase, the world's largest Bitcoin broker, and of the second group, we have Binance, the largest cryptocurrency exchange by trade volume on CoinMarketCap [25].

Coinbase is a digital currency exchange that allows not only currencies trade but also the ability to buy and sell cryptocurrencies throughout bank transfers. It has a simple and easy to use interface and a more restrict variety of cryptocurrencies to choose from.

Trades are made instantly and after having the desired cryptocurrency in the platform, users are free to withdraw their cryptocurrencies to external cryptocurrency wallets or any other cryptocurrency exchange.

Binance, in contrast to the previous platform, is more complex to use and trades can take more time, however, it has a bigger range of cryptocurrencies and more markets to trade on.

To start to use the exchange, users need to transfer cryptocurrencies to the addresses given by the platform. After having cryptocurrencies in their balances, users can start trading, creating buy/sell orders on specific currency pairs markets.

Chapter 3

Existing Interbank Transactions Solutions and Cryptocurrencies for Fintech

After understanding the current way interbank transactions are made and the main concepts around blockchain technologies, is now time to analyze and compare the existing modern solutions for interbank transactions and to go over some cryptocurrencies that can be used in fintech area or even in a solution to the previously mentioned issues.

3.1 Modern Interbank Transactions Solutions

Since the first mentions of blockchain technologies until the present day some solutions were designed and developed based on these technologies aimed to improve current way interbank transactions are made.

RippleNet and IBM Blockchain World Wire emerge as the fruit of the development in this area using blockchain technologies.

As a response to the new technologies and competitor solutions, SWIFT launch their Global Payments Innovation Initiative(gpi) to deliver an up to date solution to interbank transactions.

3.1.1 SWIFT gpi

Swift gpi uses the current Swift messaging and correspondent banking system, adding to this old core a set of rules to commit banks to behave more reasonably

in cross-border payments. These rules form a new service level agreement (SLA) rulebook that aims to provide the opportunity for enhanced business practices and smart collaboration between participating banks [26].

Three sub-products were created to strengthen the new changes: an end-to-end payments tracking system (gpi Tracker), a data monitor of banks adherence to the SLA rules (gpi Observer) and a complete list of all gpi members and their details (gpi Directory).

DLT Proof Of Concept

Recently, SWIFT completed a blockchain proof of concept (PoC) to address nostro account reconciliation issues [27]. However, the use of this distributed ledger technology would maintain the need for nostro accounts. The difference from the current reality is that Swift private blockchain would track nostro accounts balances and improve the reconciliation effort banks face today.

For this PoC, the underlying technology selected was Hyperledger Fabric [28]. The reason for this open-source blockchain framework implementation being chosen was following main features/characteristics: being a private permissioned ledger, supporting selective data distribution and providing a smart contract platform [29].

Before initializing the DLT PoC, Swift identified 8 key requirements that DLTs need to accomplish to be widely adopted in the financial industry [30]:

- Strong governance - Clearly defined roles and responsibilities of the various parties as well as operating rules.
- Data Controls - Controlled data access and availability.
- Compliance with regulatory requirements.
- Standardization - Guaranteed straight-through processing, interoperability, and backward compatibility.
- Identity framework - The ability to identify parties involved to ensure accountability.
- Security and cyber defense.
- Reliability - Readiness to support mission-critical financial services.
- Scalability - Readiness to scale to support services which process hundreds or thousands of transactions per second.

The PoC only meet 6 of these 8 requirements, leaving aside compliance with regulatory requirements and security. Swift believes the technology is too new to undergo a security assessment and the regulatory developments remain in their infancy [29].

3.1.2 RippleNet

Ripple was launched in 2012 with the ambition to revolutionize the global banking industry. To achieve that goal, RippleNet was created [31].

RippleNet is a global payment system that enables a global network for financial institutions where payments can be sent and received via ripple technology.

RippleNet offers its customers two main products, namely xCurrent and xRapid.

xCurrent

xCurrent is a settlement solution for banks with the goal of improvement of cross-border transactions. xCurrent has a bidirectional messaging system to coordinate information exchange between the banks. It uses Interledger Protocol (ILP) to coordinate founds movement between institutions to settle the payment [32]. It is designed to fit within the bank's infrastructure, requiring minimal integration.

xCurrent allows the settlement of payments using intermediaries and this settlement is still made through the use of nostro accounts.

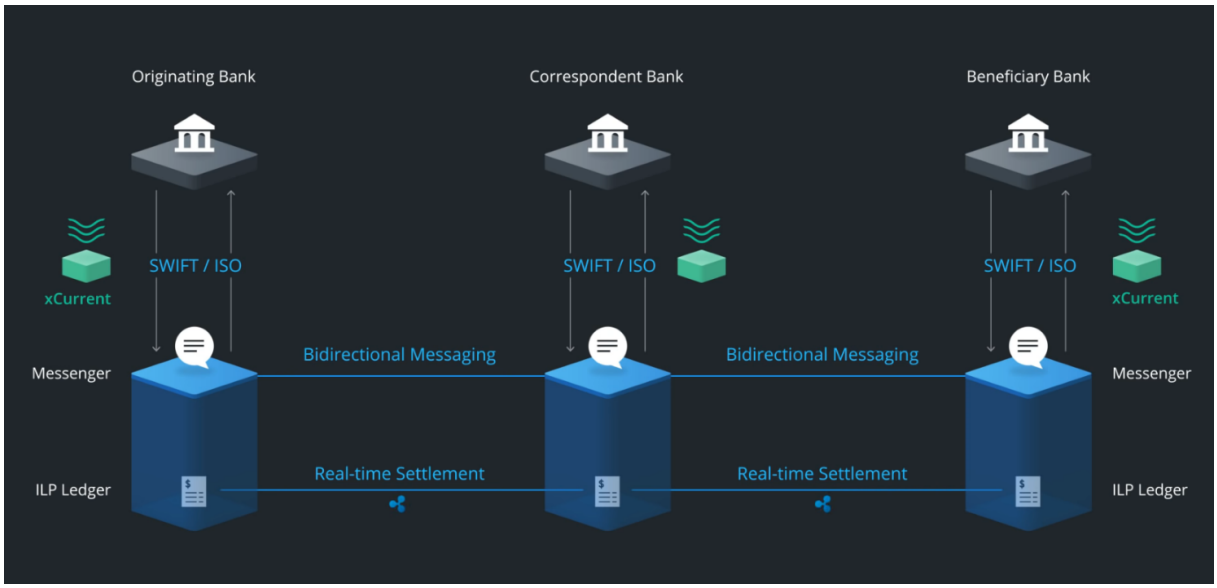

Figure 3.1: XCurrent Overview. From [33].

xCurrent parses existing message formats on a translation layer to collect the necessary information to initiate the payment. Then communicates with the sender and receiver banks to obtain their payment processing fees and total cost. After this process, a transaction information validation takes places even before funds move.[34]

Next, funds flow are coordinated across the private ILP Ledgers of the institution involved. xCurrent coordinates a hold of the funds on all ledgers until they create cryptographic signatures confirming that the funds are ready to transaction.

When all ledgers involved generate those signatures, all funds are released at the same time, ensuring no settlement risk. In the end, xCurrent provides a confirmation message to the institutions.

xRapid

After the integration of xCurrent, institutions will have the option of using xRapid. xRapid is made to eliminate the need for nostro accounts, using ripple's digital currency XRP that offer on-demand liquidity, with improved speed and lower costs [33]. This is a core feature for cross-border transactions, especially in emerging markets where the trading volume is low and the cost of currency exchange is high.

3.1.3 IBM Blockchain World Wire

IBM Blockchain World Wire is a global payment solution presented by International Business Machines (IBM) in collaboration with Stellar Organization. The solution is intended to reduce the settlement time and lower the cost of completing global payments, helping financial institutions address the process of cross-border transactions [35].

This solution uses Hyperledger to drive the payment messaging and clearing component [36].

Digital currencies are used on the stellar network facilitating the exchange to allow for near real-time settlement [37]. At the moment of the writing of this document, both stellar's native asset, XLM, and a stable coin backed by U.S. dollar, USDS, are supported by World Wire network. Other stable coins backed by other fiat currencies like Euro, Indonesian Rupiah, Philippine Peso, Korean Won and Brazilian Real are currently waiting for approval to being added to the network [38].

As can be seen in Figure 3.2, two financial institutions that want to realize transactions between them agree to use a digital asset to work as a bridge between the fiat currencies the institutions use. The sender institution, connected to World Wire's

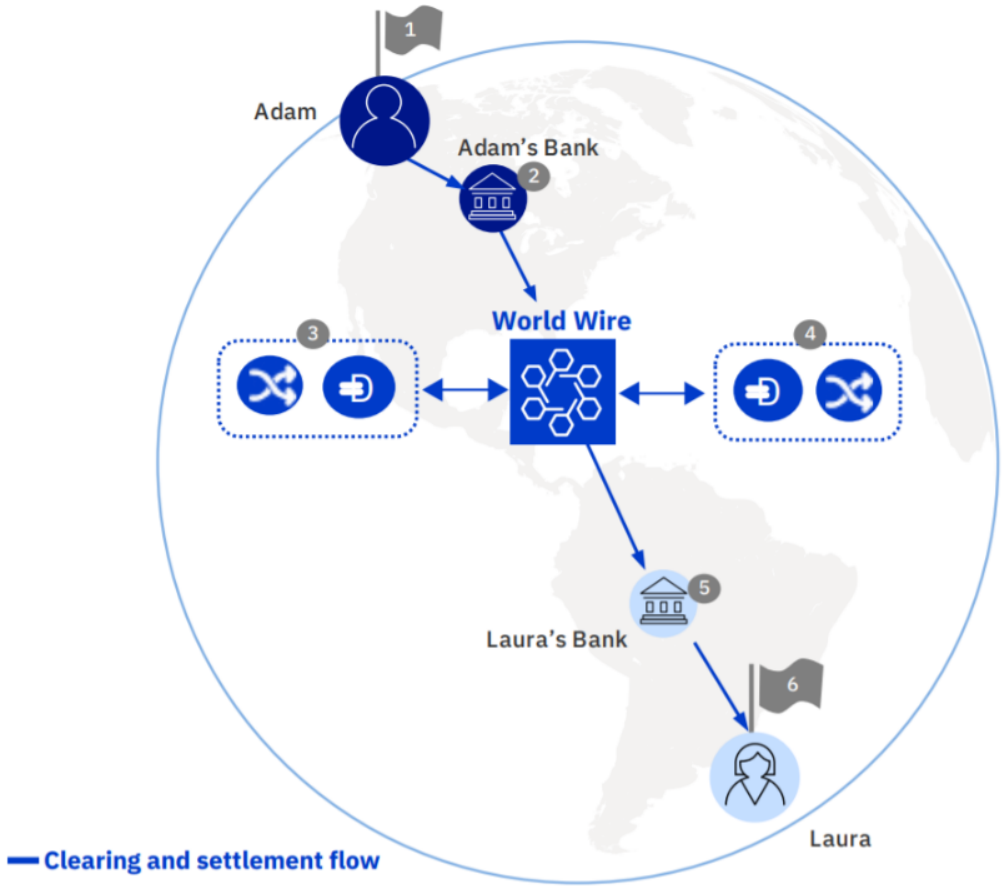

Figure 3.2: World Wire Overview. From [39]

APIs, converts their fiat currency into the chosen digital asset. Simultaneously, World Wide converts the digital asset into the fiat currency used by the receiver institution, completing the transaction. The transaction details are recorded onto a blockchain for clearing purposes [39].

3.1.4 Overview of existing interbank transactions solutions

In comparison with the current way interbank transactions are made, all the three solutions presented until this section affirm to have improved in terms of transaction time and cost.

Ripple claims that using their solution payments reach their destination in seconds instead of days. Also claims that reduce the transaction cost, without giving any quantitative data, and lowers the operation cost for the institutions by 50% [33][32].

On the other hand, SWIFT gpi states that 50% of the transactions processed are

credited in less than 30 minutes and almost 100% within 24 hours [40]. Also claims that reduce payment costs [41].

World Wide also promises transactions processed in seconds and lower transactions costs.

Both SWIFT gpi and RippleNet need intermediaries to work. SWIFT gpi still depends on correspondent bank arrangements to settle the funds and intermediary exchanges to convert currencies in case of a cross-currency transaction. RippleNet also uses external exchanges to find the best convert ratio for the fiat and cryptocurrency used in the transaction.

The need for nostro accounts is eliminated in both RippleNet and World Wire, but it is maintained in SWIFT gpi because of the use of correspondent banking arrangements.

Table 3.1 resumes the main characteristics about these solutions.

Table 3.1: Comparison of the modern interbank transactions solutions.

	SWIFT gpi	**Ripplenet**	**World Wire**
Transaction Time	30 min - 24 h	Seconds	Seconds
Transaction Cost	Reduce	Reduce	Reduce
Need for intermediaries	Yes	Yes	No
Need for nostro accounts	Yes	No	No
Centralized Control	Yes	Yes	Yes

3.2 Cryptocurrencies

After analyzing the existing solutions to interbank transactions based on blockchain, it can be noticed there is a common aspect to both RippleNet and World Wire: the use of cryptocurrencies.

The cryptocurrencies used or planned to be used on those projects can be distinguished into two categories: transaction-oriented coins and stable coins.

3.2.1 Transaction Oriented Coins

Both XRP, used on RippleNet, and XLM, used on World Wire, are transaction-oriented coins, in other words, cryptocurrencies that gather a set of characteristics to allow faster and less costly transactions.

The main characteristics of this category of cryptocurrencies are the following:

- High transaction speed.

- Low transaction fee.
- Great number of transactions per second.

As was said before, XRP and XLM are great examples of transaction-oriented coins, but these two aren't the only ones that try to satisfy the characteristics enumerated above.

Table 3.2 presents the main characteristics of XRP and XLM. Should be considered that the world of cryptocurrencies is constantly changing and evolving and the data reunited in Table 3.2 should not be accurate over time.

Table 3.2: XRP and XLM comparison.

	XRP	**XLM**
Transaction Speed	3 - 5 sec.	2 - 5 sec.
Transaction Base Fee	0.00001 XRP	0.00001 XLM
Current max. TPS	1500 TPS	1000 TPS
Scalable max. TPS	50000 TPS	10000 TPS
Current Market Cap	20 billion USD	3 billion USD
Current Circulating Supply	43 billion	19 billion

XRP and XLM are respectively the native currencies of ripple and stellar blockchain.

Ripple and stellar blockchains are very similar, even being the stellar creator one of the initial developers of ripple. However, they have different goals and different ways of addressing decentralization.

Ripple blockchain has a controversial decentralization since all the validator nodes of the network are maintained by the Ripple company.

3.2.2 Stable Coins

As mentioned in Section 3.1.3, *World Wire* is trying to implement the use of stable coins.

Cryptocurrencies are generally associated with wide fluctuations of their prices in comparison to fiat currencies. These volatile prices have proven dissuasive to users who want to use cryptocurrencies as a unit of value or storage of value [42].

Stable coins are an attempt to solve the problem of the wide price volatility.

Three different types of stable coins can be delimited: *Fiat or Commodity-Backed*, *Cryptocurrency-Backed* and *Seigniorage Shares Style*.

Fiat or Commodity-Backed

This type of stable coins are coins that are fully backed by fiat money or commodities. Commodities are goods or services that their instances are treated by the market as equivalent, for example, precious metals.

These coins are backed 1:1 by real assets in real reserves, in other words, 1 USD of stable coin is equivalent to 1 USD of fiat money that is stored in a real bank account.

This type of stable coins is dependent on central entities since these entities are responsible for maintaining and ensure the fiat/commodities reserves that back the value of their stable coins.

Cryptocurrency-Backed

Cryptocurrency-backed stable coins are coins backed by other cryptocurrencies. Typically, more than one cryptocurrency backs this type of stable coin to decrease volatility.

However, these stable coins are still much volatile than other assets as fiat money or commodities.

Seigniorage Shares Style

In contrast to the two previous types, Seigniorage shares style stable coins are not back by any asset.

This stabilization system of the value of a coin suggests the use of two types of coin: a coin that acts like money and a coin that acts as a share. For a moment, we'll just call these *coins* and *shares*. The goal is to stabilize the price of *coin*. In case of a increase in price, the supply of *coin* increases by distributing more *coins* to the *share* holders and destroying the correspondent *shares*. In case of a decrease in price, the supply of *coin* decreases by distributing *shares* to the *coin* holders and destroying the correspondent *coins* [43].

However, the complexity associated with this method and the early-days of projects trying to implement this system has affected the adoption by the community until the moment of writing of this dissertation.

Chapter 4

Problem Statement

The current way interbank transactions are made uses SWIFT messaging system and correspondent banking arrangements. In order to work, there is a need for intermediaries to transfer or convert the funds and nostro accounts to facilitate the settlement of those funds.

4.1 Problem

The main objective of the present dissertation is the improvement of the current way interbank transactions are made. To allow this improvement, there are three considered main problems that need to be addressed:

- **Transaction time** The time needed to a transaction occurs between two accounts on different banks is directly related to the need for financial intermediaries and their settlement processes.

  If the two banks involved in the transaction don't have a direct correspondence, one or more intermediaries will be used to facilitate the transfer. Each intermediary adds a portion of time to the transaction between the sending and the receiving bank.

  In the case of a cross-currency transaction, the transaction time will be even higher.

- **Transaction costs** As transaction time, the transaction cost is also related to the need for intermediaries.

  When there is the need for intermediaries, each intermediary applies a fee to transaction making it more and more costly.

- **Funds in nostro accounts** When we are talking about correspondent banks, we are referring to banks that hold nostro accounts with each other.

  A bank needs to provide a great number of funds to fill its nostro accounts on correspondent banks. These funds are only used to allow direct transactions and facilitate the settlement.

4.2 Hypothesis

Blockchain is a possible solution to improve or resolve the main problems mentioned in Section 4.1. That said, the main hypothesis this Dissertation defends is:

"A blockchain based solution that is fully decentralized is a better solution to interbank transactions than the existing solutions"

The previous sentence involves some subjective terms that can lead to possible misinterpretation. For this reason, the intended meanings of these terms are explained below.

What is understood by *blockchain based solution*?

A *blockchain based solution* is a solution to interbank transactions which main functionalities are supported by and/or use blockchain technologies.

What is understood by *fully decentralized*?

The solution shouldn't be dependent on any central entity, in order to be always usable even if the distributor entity ceases to exist.

What is understood by *better solution*?

A *better solution* is a solution with lower processing time, lower transacting costs and without the need of nostro accounts, in other words, a solution that addresses the problems mentioned at Section 4.1 in a better way than the rest of the existing solutions.

What is understood by *existing solutions*?

The *existing solutions* to interbank transactions are, not only, the current way of transacting money between banks approached in 2.1, but also, the modern solutions mentioned at Section 3.1: *RippleNet*, *SWIFT gpi* and *IBM Blockchain World Wire*.

4.3 Methodology

After exposing the main problems that the current dissertation addresses and the hypothesis that it defends, it is now time to explain the methodology used to solve the problems and to prove the hypothesis.

Firstly, there is a need for finding a solution to interbank transactions that can solve the problems mentioned in Section 4.1 and still being fully decentralized. This first step will consist of designing a solution that tries to address the liabilities of the available alternatives and certain blockchain technologies that can be used.

The viability of the designed approach is shown through a prototype that can be used to support the validation of the approach.

Lastly, the validation process consists of comparing the achieved solution to all existing solutions analyzed previously in order to prove the main hypothesis of the current document.

4.4 Approach Overview

It is expected the solution produced be a fully decentralized platform for each bank without the need of being dependent on any other entity or external service.

The different platforms in different banks should only communicate through transactions in a proper blockchain, eliminating the need for any centralized communication system.

This decentralized solution should present lower transaction times and lower transaction cost than any other mentioned existing solution and should eliminate the need for the use of nostro accounts.

It is crucial that the clients of the banks don't need to directly work with any blockchain technology neither have more education about this area than a regular bank client. Additionally, it is also important that this platform represents a low investment solution for the bank, in order to have a good adoption in the banking area.

Chapter 5

Interbank transaction solution based on a cryptocurrency exchange platform

It is now time to find a solution that addresses the problems listed in Section 4.1: transaction time, transaction cost and need for nostro accounts. This solution should agree with the concerns mentioned in Section 4.4 and it should be capable of proving the main hypothesis of the current document.

5.1 Seeking a solution

As was seen before there are already solutions created or being created that use blockchain technologies to present new alternatives to process interbank transactions. However, the solutions analyzed in the previous chapters have controversial decentralization.

The current way of transacting money between banks approached in Section 2.1 and some of the solutions mentioned at Section 3.1 use third-party entities to make transactions possible. This use of third-party services is also directly associated with centralization.

Not only the current way of transacting money between banks but also RippleNet and Swift gpi maintain the need for third-party financial institutions. Additionally to this, a big part of validator nodes from RippleNet blockchain is controlled by Ripple company, making this blockchain controversially centralized. Lastly, IBM's World Wire is based around a central exchange that all banks would use to transact money and without this central service the solution wouldn't work.

Therefore, the current dissertation considers that there is a need for a solution

that addresses the problems described at Section 4.1 respecting the main principle of blockchain: decentralization.

To reach this goal, the proposed solution shouldn't be dependent on any central entity neither any third-party institution or service.

5.2 Solution

Having into account Sections 4.4 and 5.1 a idea of a solution was created to address the problems listed in Sections 4.1:

Each bank institution has one private digital exchange where only the bank's clients can trade fiat currency for cryptocurrency, or vice-versa.

The reason for the integration of the exchange on the project is to allow users to trade their fiat money for cryptocurrency, which can be sent to other users of other bank institution which has also adopted the proposed solution. The value is transacted through a blockchain and can be traded by the user on the other end in their bank's own exchange.

The exchange platform is divided into 2 views: one more complex and the other more user-friendly.

The more complex view is oriented for users who want to trade their currencies manually and to have the option to deposit/withdraw cryptocurrency, in other words, users interested by the trading features of the platform.

The more user-friendly view is for users that just want to transfer their fiat currency without the need of directly interacting with the trading markets or cryptocurrencies.

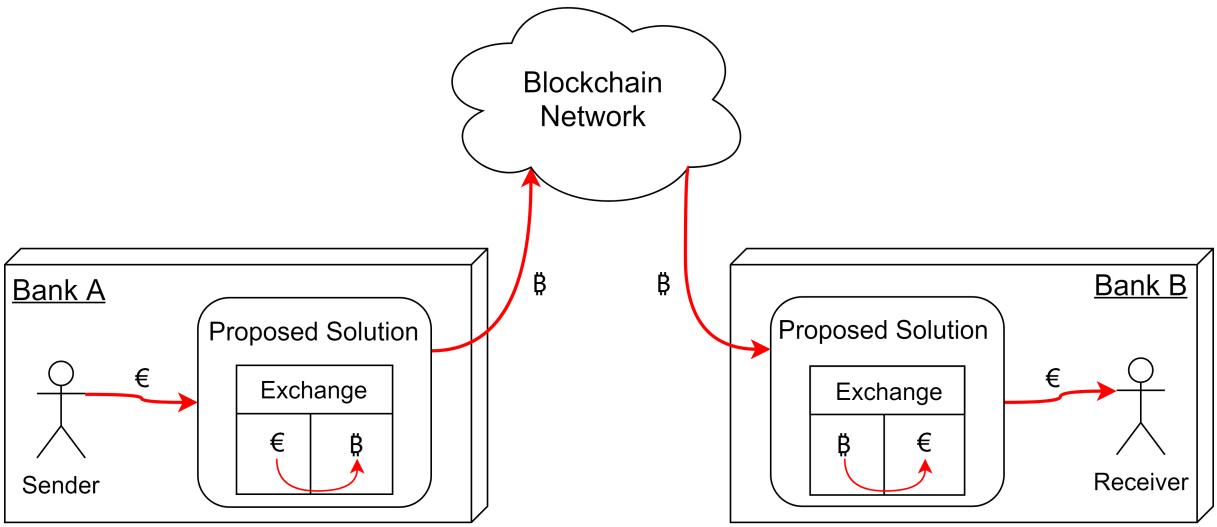

Figure 5.1: Representation of the solution being proposed.

As can be seen in Figure 5.1 there isn't fiat money being transacted between banks, only transactions of cryptocurrency through the blockchain. Each bank only needs to assure the trade of cryptocurrency and fiat currency between its own customers was done properly.

5.3 Functional Aspects

The main focus of the presented solution is the money transfer between accounts of different banks without the need for client involvement in the trading market.

However, the currencies exchange aspect is the base of the solution and it is what allows the money transfer functionality to work.

5.3.1 Interbank money transfer aspect

Users should be able to use the platform only as a money transfer platform if they want.

Sending money using the platform should be simple and straightforward: the user just needs to select the amount of fiat currency and the address of the destination account and confirm the transaction.

The process of sending money from a bank account to another account on another bank follows the onward sequence:

1. The sending user defines the sending amount and the destination and confirms the transaction;
2. The sending platform automatically converts the fiat currency to cryptocurrency, using its own trading market;
3. The funds are transacted as cryptocurrency via blockchain;
4. The receiving platform automatically converts the cryptocurrency into fiat currency, using its own trading market;
5. The destination user is credited with the received fiat money.

5.3.2 Currencies exchange aspect

The fiat/cryptocurrency exchange aspect can be considered as the heart of this approach since this aspect feeds the market with market orders that are essential to the money transfer functionality.

Create Market Orders

Users should also be able to trade fiat money for cryptocurrency and vice-versa if they want, having in their account a balance of fiat money and also a balance of cryptocurrency.

The trades between users will always happen inside the bank. The bank just needs to assign the correct amount of currency to each user after a trade. The total amount of fiat reserves of a certain bank is never affected since there is no fiat money being transferred from or to other banks.

Deposit and Withdraw of Cryptocurrency

Users should be able to deposit and withdraw cryptocurrency to and from the platform. With this option, it is expected the bank never needs to invest and insert cryptocurrency into the system, letting their own clients do that.

5.4 Choosing the Cryptocurrency

The user using the solution should have the perception of fast and economic transactions made via a trustworthy platform and components.

Being one of the main components of this solution, the chosen cryptocurrency should have the following characteristics.

- Fast transaction speed
- Low fee
- Credibility

The credibility of a cryptocurrency is a key factor for users to trust the cryptocurrency as a bridge to transact their money. The team behind the cryptocurrency blockchain, the cryptocurrency blockchain project goals and the trade volume worldwide are attributes that should be considered in order to recognize a cryptocurrency as credible or not.

We must also not forget that the chosen cryptocurrency project should follow the main principles of a blockchain. Wouldn't be correct to use a blockchain with controversial decentralization if one of the goals of the purposed solution is to achieve full decentralization as mentioned in Section 4.2. With this requirement, the possibility of using stable coins based on fiat money or commodities in the proposed approach is discarded.

The idea of the proposed approach is to solve the problems mentioned in the previous section, namely, reducing transaction time, reducing transaction cost and eliminating the need for nostro accounts. The chosen cryptocurrency should be a transaction-oriented coin to present lower transactions times and costs. This would help the approach to address both the transaction time and transaction cost problems found in the current way of processing interbank transactions. Any other type of cryptocurrency could be used in the development of the approach, however, the results achieved may not be significant or even worst in terms of time and cost.

5.5 Cold-start and low trading volume problems

Money transfers made using the solution are maintained by the trading volume of the exchange platforms of the sender and receiver banks. The trading volume of the exchange platform is fed by the market orders made by its own users.

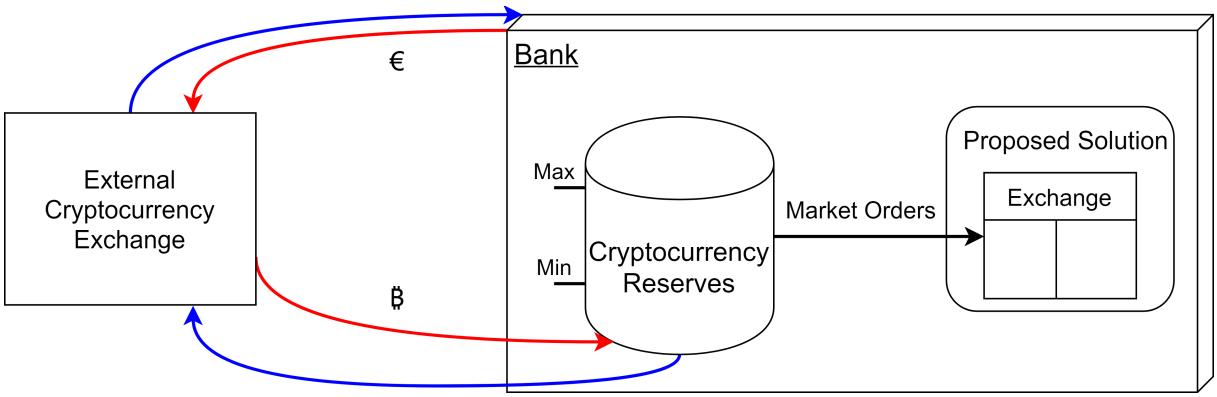

Figure 5.2: Representation of the cold-start and low trading volume solution.

In small banks or in early times of the solution adoption, the small trading volume could represent a problem to the solution's functionality of money transfer. Without sufficient amount of listed market orders on at least one of the two exchange platforms involved in a transaction, the process can't be completed as fast as might be expected.

EbankIT suggested adding to the project a solution to address the mentioned cold-start and trading volume problems. That solution consists of a reserve of cryp-

tocurrency maintained by the bank in order to fill their trading market with market orders.

The solution for the cold-start and low trading volume problems is represented in Figure 5.2.

The cryptocurrency reserve has a maximum and minimum limit number of cryptocurrency that the bank considers to be sufficient to meet its exchange platform requirements. The bank uses external cryptocurrency platforms to buy cryptocurrency when bank's cryptocurrency reserve reaches their minimum limit or to sell if the reserve exceeds their maximum limit.

Chapter 6

Design and Implementation

Following the approach introduced in the last chapter to address the defined problems, it is now time to present the design and implementation details of the solution prototype made along with the current dissertation.

6.1 Design

Stellar blockchain and its native currency were the blockchain and cryptocurrency chosen to be used in the prototype. This decision was made since the stellar blockchain is a network aim for the fintech area, already being used in *IBM Blockchain World Wire*, as it was seen in Section 3.1.3. It has great characteristics like fast transaction speed, low transaction fee and high TPS, as can be seen in Table 3.2. In contrast to ripple blockchain, stellar blockchain is a fully decentralized network.

More specifically, the stellar public test network was used during the development and testing of the proposed approach in order to avoid real monetary investment.

6.1.1 Architectural Design

Figure 6.1 tries to represent a more high-level component diagram with the main components needed for the proposed approach to work.

In the diagram, *Main Solution* refers to the private cryptocurrency/fiat exchange for each bank that works autonomously and has its main functionality instant money transfer to other banks, presented in Section 5.2. At the same time, *Crypto-Tank Solution* refers to the solution proposed by EbankIT to address the cold-start and low trading volume problems, mentioned in Section 5.5.

Both main and crypto-tank solutions are connected to the same MySQL database. This database is responsible for storage and availability of information related to accounts, market and transactions. It also works as a bridge between the main solution and the crypto-tank solution: the crypto-tank solution creates new market orders in the database that will feed the money transfer functionality of the main solution; on the other hand, the main solution will consume those market orders or create new ones.

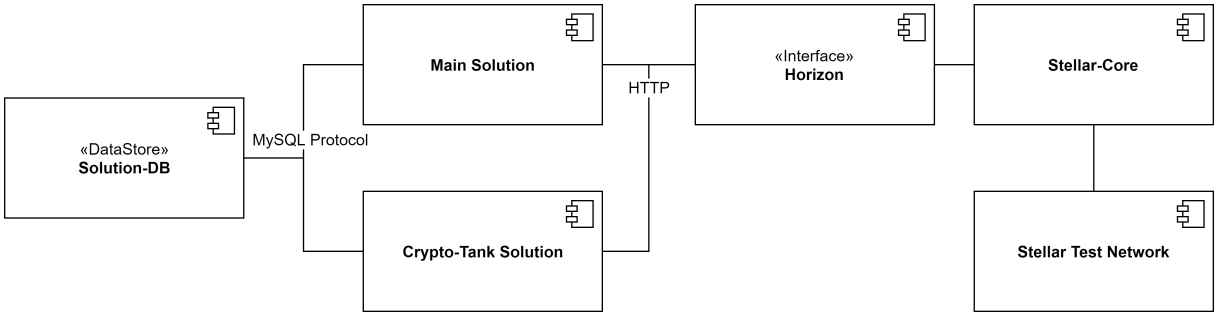

Figure 6.1: High level component diagram.

Horizon is an API server that acts as an interface between applications and stellar-core, allowing a straightforward way to submit transactions [44].

Stellar-core works as a node of the stellar network, validating and agreeing with other stellar-core instances on the status of every transaction through the *Stellar Consensus Protocol* [45][46].

In this prototype, we used public instances of horizon and stellar-core maintained by *Stellar Development Foundation*, but it is possible to host our own horizon and stellar-core instances. A final solution should use its own instances of these components, in order to not depend on a third party, have more control over who to trust and to help make the public stellar network more reliable and robust for others.

The stellar test network is maintained by *Stellar Development Foundation* and aimed to help developers producing applications and doing smaller tests. This network is backed by only 3 stellar-core validators [47].

Main Solution Architectural Design

The *Main Solution* mentioned in Figure 6.1 is a web application developed in NodeJS and it is the heart of the proposed approach. Therefore, it is essential a more in-depth overview of the architectural design of the *Main Solution*.

As can be seen in Figure 6.2, the *Main Solution* is structured into 6 modules that reunite all the functions needed for the platform to work.

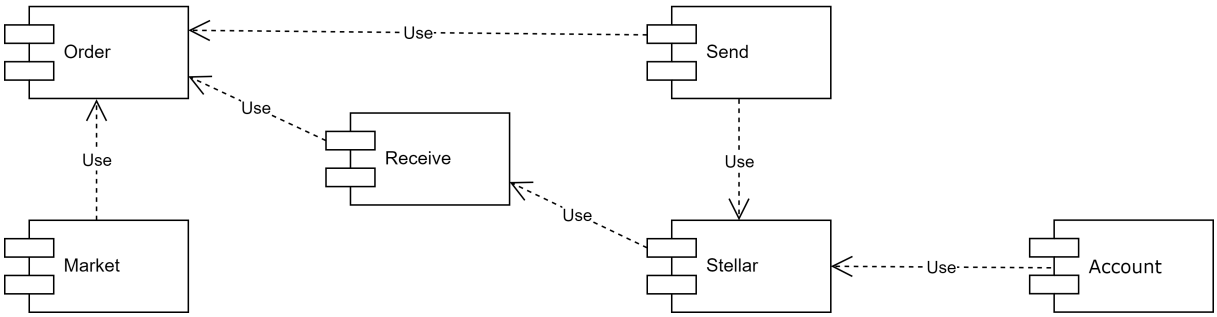

Figure 6.2: Low level component diagram.

- *Account* has the base functions related to the user page.
- *Market* has the base functions related to the market page.
- *Order* has the more advance functions related to market orders and to the process of automatically resolve them.
- *Stellar* is the module that communicates with the horizon instance from 6.1 and handles the deposit and withdraw of cryptocurrency.
- *Send* and *Receive* are the modules responsible for the main functions used in the money transfer functionality.

All of the mentioned modules communicate with the MySQL database through queries.

6.1.2 Data Model Design

The MySQL database used in the prototype is structured into 6 tables that store information about the user, market orders and transactions through the stellar network.

Account table stores both fiat and cryptocurrencies balances of the respective user.

Buy order and sell order tables associates an existing user to a market order, buying or selling a certain amount of XLM for a certain price in EUR.

As can be seen in Figure 6.3, stellar transactions table stores the information needed for a stellar transaction (destination, amount of XLM and a memo) and the state of the transaction processing inside the platform. Stellar transactions table records all sending transactions that are being processed.

Stellar cursor table stores an identifier token of the last processed receiving transaction allowing the solution to know what receiving transactions were already processed and the ones that still need to be processed.

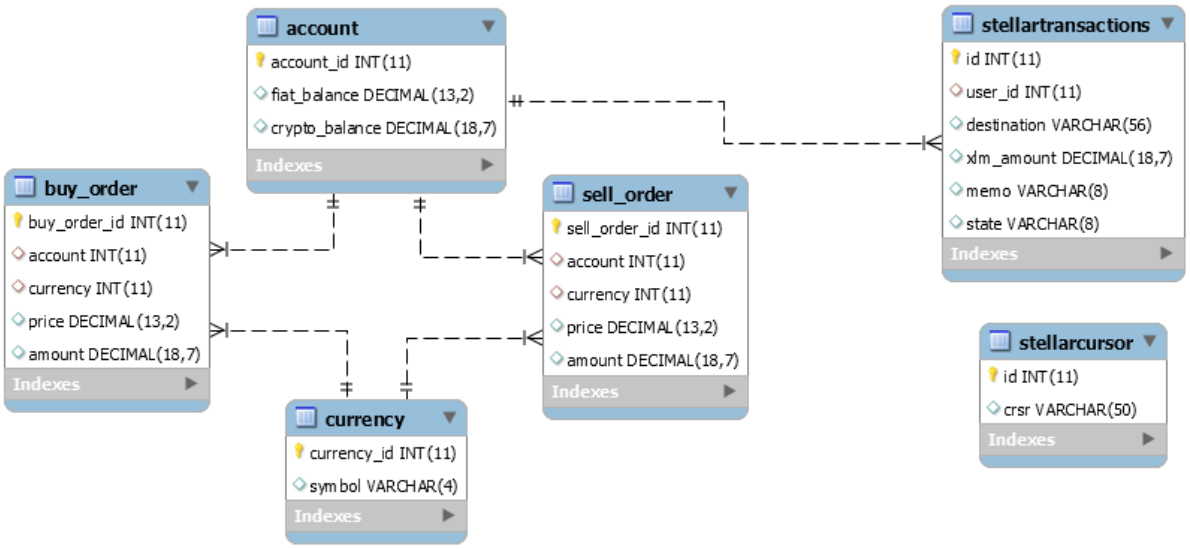

Figure 6.3: Data model diagram.

6.2 Features Walkthrough

The features of the solution prototype can be divided into 3 stages: exchange related, stellar integration and transacting between exchanges.

6.2.1 Exchange Related

This platform has 2 user interface views in this stage: "Market" and "Account".

In the Market page, there are two separate tables for listing all buy and sell orders in the trading market. In addition, there are two forms that allow users to interact manually with the trading market placing buy and sell orders, as can be seen in Figure 6.4.

Both market orders tables are composed of 4 columns:

- **Price** (in EUR) users want to buy/sell each XLM.
- **Amount** of XLM users want to buy/sell at that price.
- **Total** value (in EUR) of all XLM users want to buy/sell at that price.
- **Sum** of all total values until that line, from top to bottom.

In the Account page, there are two tables for the market orders made by the corresponding user. User's balances of both currencies are also displayed on this page, as can be seen in Figure 6.5.

Figure 6.4: Market Page.

There are "Cancel" buttons on each line of the market orders tables, allowing users to cancel their own market orders at the chosen price.

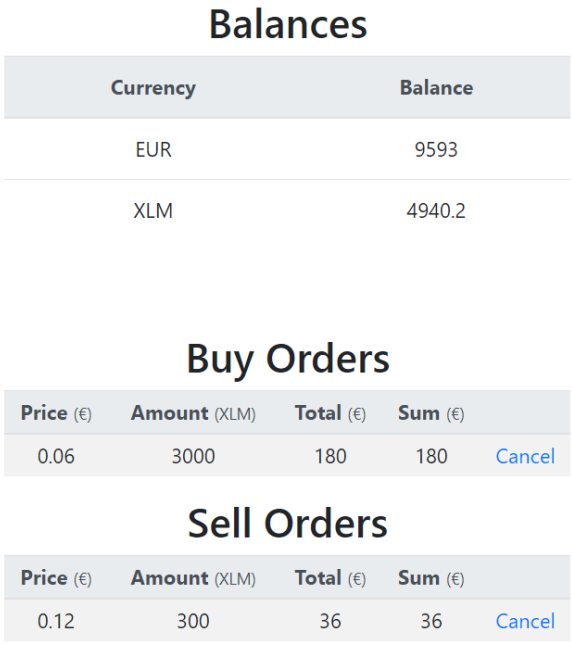

Figure 6.5: User balances and market orders in Account page.

6.2.2 Stellar Integration

Stellar integration was possible due to Stellar JavaScript library which allowed the platform to communicate with stellar testnet. This made deposits and withdraws of cryptocurrency possible on the platform.

In the Account page, there is the deposit information and a withdraw form as can be seen in Figure 6.6.

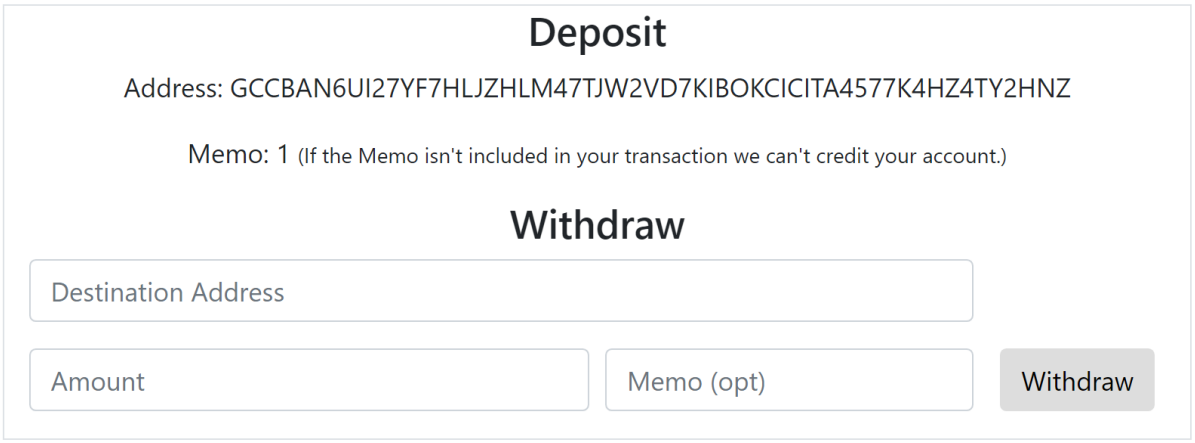

Figure 6.6: Deposit information and Withdraw form in the Account page.

There is only one deposit address for the exchange, meaning that users' XLM balances are jointly saved in the same "crypto-wallet".

An indicator of an account should be added to the transaction as a "memo" in order to platform to assign the received XLM to the right client in the platform's database.

6.2.3 Transacting between exchanges

One more user interface view is introduced in this section: "Send".

In the Send page, there is a simple form with 3 fields, as presented in Figure 6.7. This form needs to be filled by the user in order to the money transfer to occur.

The user needs to write the amount of money that wants to transfer, followed by the address and the memo of the receiver. After pressing the "Send" button, the specified funds are converted into cryptocurrency, sent through Stellar blockchain, and, finally, converted again to fiat money at the private exchange of the receiver's bank.

The memo defined by the sending user is modified by the sending platform prior to the transaction, adding a token before the rest of the memo. The receiving platform by identifying the token can distinguish a transaction from another bank from a simple cryptocurrency deposit. This allows the receiving platform to automatically convert the received cryptocurrency into fiat money and assign it to the respective client.

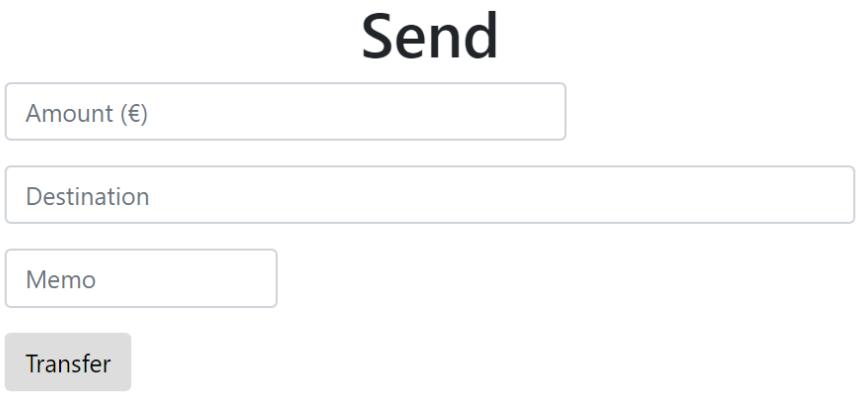

Figure 6.7: Send page.

6.3 Project Details

As was already mentioned, the prototype of the solution was developed using NodeJS and Express and the database was made in MySQL. The Javascript library Stellar SDK made possible the integration of XLM cryptocurrency and the connection with stellar test network.

Development history

The implementation of the prototype started in early November 2018, being mainly developed between November 2018 and February 2019 as presented in Figure 6.8.

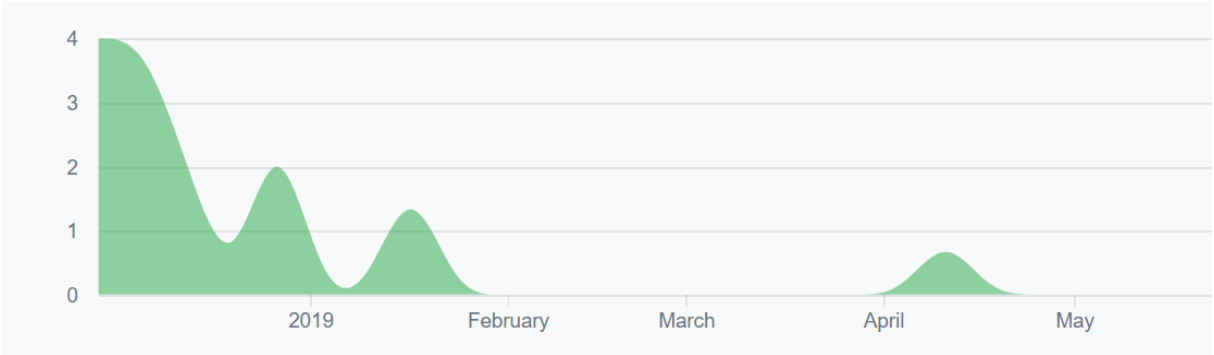

Figure 6.8: Number of commits on the project over time.

Availability

The prototype and other developed support tools are available in open-source. The source code of the developed prototype, the instructions to set up the development

environment and the link for some developed support tools can be found in the following address: https://github.com/joaocarduarte/diss-exchange.

6.4 Future Work

With the end of the design and implementation, it can be delimited some features that can be added to the prototype and some features that could be improved.

Federation protocol

The stellar federation protocol can map a custom email-like address to more information about a user. This protocol could be used in the prototype by resolving an email-like address such as "IBAN@domain.com" into a stellar public address and a memo.

With this addition, a client from a bank could use the IBAN of another client on another bank to make a transaction, instead of the pair of stellar public address and memo that is currently being used.

Represent EUR with more decimal places

Currently, the developed prototype only allows the user to specify up to 2 decimal places for the price in EUR in the creation of market orders, being the minimum variation of 0.01EUR. This variation corresponds to almost 10% of the current price of 1 XLM.

Adding more decimal places for the price of market orders could lead to fewer percentage variations between the consecutive lines of the market tables.

Chapter 7

Conclusions

After the development, the prototype went through a process of testing and comparison with the other existing solution from Section 3.1. The results were analyzed taking into account the points defined in Section 4.1 and the central hypothesis of the document presented in Section 4.2.

7.1 Validation Process

The prototype testing has in consideration the points defined in Section 4.1. The idea of the approach had already eliminated the need for nostro accounts, leaving only the transaction time and transaction cost to be tested.

As was said in Section 6.1.1, stellar testnet was used during the development, and end up being also used in the collection of performance data, even though *Stellar Development Foundation* states that the testnet isn't the proper network for load and stress testing [47].

Environment

The process of testing the prototype was made in a personal laptop with the Intel Core i7-6700HQ CPU, 16GB of RAM, and a strong internet connection of 200Mbit/s of download and 200Mbit/s of upload.

Two instances of the project were run using different configurations to represent two different banks. Two distinct databases for the banks were initiated and populated with the needed information and market orders. Although both platforms were running in the same computer, they only communicate through transactions in the stellar test network.

Procedure

The function that starts the process of money transfer was changed in order to create 100 distinct interbank transactions when the user pressed the "Send" button in the "Send" page of the platform. All the interbank transactions had the same fiat money amount, destination and memo. To confirm that were actually created 100 distinct interbank transactions, the information in both databases was compared, namely, it was assessed the final balances of both users and it was used an external stellar testnet block explorer to confirm that the 100 interbank transactions were actually made in 100 distinct blockchain transactions through the stellar test network.

Data collection

The exact time of the starting point of sending the 100 interbank transactions in the sending bank and the exact time of the completion of the last interbank transaction in the receiving bank were both recorded. Those records were made using JavaScript Date method, printing the hour, minutes, seconds and milliseconds of those moments. The sums of the sent and received fiat amount were also recorded.

This testing process was replicated 10 times in order to achieve more reliable data.

There is additional information to replicate the testing process in the "Read Me" file in the GitHub repository of the prototype. The GitHub repository link is provided in Section 6.3.

7.2 Results Analysis

The data obtained from the development and validation process was synthesized into Table 7.1 adding to the data from the contending solutions. The comparison between all the solution was made according to the main problems presented in Section 4.1: transaction time, transaction cost and need for nostro accounts.

Table 7.1: Comparison of the developed solution with the other existing solutions.

	SWIFT gpi	**Ripplenet**	**World Wire**	**Our Approach**
Transaction Time	30 min. - 24 h.	Seconds	Seconds	6 seconds
Transaction Cost	Reduced	Reduced	Reduced	0.000001EUR
Intermediaries	Yes	Yes	No	No
Nostro accounts	Yes	No	No	No
Centralized Control	Yes	Yes	Yes	No

7.2.1 Transaction time

The transaction time obtained by the developed solution was recorded in a performance test using the stellar testnet. The data from other solutions isn't also really specific, however, even using testnet, the developed solution achieved competitive results in terms of transaction time, as can be seen in the first line of Table 7.1.

The total time of the 100 interbank transactions was divided by 100 to achieve the time of one interbank transaction. The average time of one transaction at the end of the 10 iterations is 6.409 seconds, being the lowest value achieved 6.358 seconds and the highest 6.447 seconds.

7.2.2 Transaction cost

During the 10 iterations, each interbank transaction was sent with 1EUR. In the sending platform, this 1EUR was converted into 10XLM since the minimum existing sell order was selling each XLM for 0.10EUR. In the receiving platform, the higher buy order was buying each XLM for 0.09EUR. These converting differences lead to the client in the second bank only received 0.90EUR from each interbank transaction. If we consider all the interbank transactions in an iteration, it was sent 100EUR but only received 90EUR.

Taking into account the last paragraph, it can be noted that there is a risk that the market orders values could be different in each bank exchange. This can cause value variations between the sent and received money. The current document will not consider these variations as transaction cost since they can lead to a negative variation but also can lead to a possible positive variation, where the recipient account would receive more fiat money than it was sent.

With respect to the value presented in Table 7.1, the only common cost for the user is the transaction fee applied by Stellar blockchain that is currently 0.00001 XLM (currently close to 0.000001EUR).

The data provided by the other solutions isn't again conclusive in terms of transaction cost what leads to a not viable comparison. However, without considering the risk of the distinct market order values in the two banks involved in an interbank transaction, we can arguably consider the proposed approach as a low-cost option for interbank transactions.

7.2.3 Need of nostro accounts

The proposed approach doesn't use nostro accounts since the fiat money transfers only occur internally in each bank.

Nevertheless, with the addition of the cold-start and low trading volume solution, the investment the bank needs to do to fill its exchange with market orders can be compared to the investment current banks made into nostro accounts. Plus, with the addition of that solution, the bank would also be dependent of intermediaries, in this case, external cryptocurrency exchanges/brokers.

7.3 Contributions

Coming to an end of the current document, it is important to look at the work that was generated during the time allocated to this master dissertation:

- A well defined approach.
  - An explained approach that can be used by anyone to develop a solution for the problems from Section 4.1, using different ways of design and implementation.
- Summary of the design and implementation of a prototype.
  - Both the design and implementation of the prototype were documented, explaining its structure and features.
- Article
  - An article that summarizes the current document into less than 12 pages, Appendix A.

7.4 Future Work

Finally, it is now time to give a global overview of the proposed approach and suggest some improvements and future work:

- Both time and cost of a transaction using the developed solution present competitive results. Sending money through the solution, however, has a risk associated: the cryptocurrency could be trading at distinct prices in different bank exchanges,

which could impact the difference between the money sent and received. It would be interesting if future works attempt to minimize the risk, maintaining the decentralization of the solution and small time and cost of the transactions.

As a possible solution to minimize this risk the sending platform could register the sent fiat value into the memo of the stellar transaction, in order to the receiving platform to know the exact fiat money the receiving account should receive. The difference between the sent and received fiat money could be absorbed by the receiving bank. This money difference that the receiving bank would absorb could represent a loss sometimes, but also could represent profit other times.

- The developed prototype in the current document was, like expect, a decentralized solution to interbank transactions without the need for nostro accounts neither intermediaries. However, with the addition of the cold-start and low trading volume solution, the proposed approach is affected in terms of the need for nostro accounts and intermediaries, as mentioned in Section 7.2.3. With this in mind, there is a concern about the possibility of solutions for these and other real-world integration problems could affect the validation of the main solution decentralization, the need of investments similar to the investment banks currently make into nostro accounts and the possible need for intermediaries.

  It would be interesting if future works actually test the proposed approach in a real-world banks environment in order to better delineate how solutions for real-world problems could affect and change the originally proposed approach.

- As mentioned several times throughout this document, the stellar test network was used instead of the stellar main network to avoid real investment during the development and testing of the prototype. Also, since the data reunited from the contending solutions was not specific enough, there wasn't a strong need for a better performing network than the stellar testnet to get performing data to the comparison.

  With more dissemination of specified information to the public about the contending solutions, it would be essential for future works to use the stellar main network to get more realistic performance data.

Appendix A

Article

Blockchain Technologies Applied to Interbank Transactions

João Duarte[1[0000−0002−0611−8371]] and Filipe Figueiredo Correia[1,2[0000−0002−6653−1598]]

[1]Faculty of Engineering, University of Porto, Porto, Portugal
[2]INESC TEC, FEUP Campus, Porto, Portugal
{up201303834, filipe.correia}@fe.up.pt

Abstract. Nowadays, interbank transactions are costly and can take several days to complete. The need of intermediary financial institutions and for a system of nostro accounts makes the process costly for both the banks and their customers.
Projects such as *RippleNet*, *IBM Blockchain World Wire* and even *SWIFT gpi* use blockchain technologies to address the main issues of interbank transactions. However, these projects are controlled by central entities, going against one of the blockchain main principles: decentralization.
This work proposes a decentralized solution that addresses the three problems of interbank transactions: transaction time, transaction cost and the need for nostro accounts. The solution consists of a private cryptocurrency/fiat exchange for each bank that works autonomously and supports quasi-instant money transfer to other banks. This is done without the need for the customer to be aware that cryptocurrencies are being used, neither that market orders are being placed. This functionality is only possible due to the trading volume on each exchange.
The Stellar blockchain was used to create a prototype of the proposed approach. The prototype presented competitive results when compared to existing solutions in terms of time and cost of a transaction and the need for nostro accounts. However, the solution can suffer from cold-start or low trading volume problems which can only be addressed with the investment of funds, which will be, to some extent, similar to the investment made into nostro accounts.

Keywords: Interbank transactions · Blockchain technologies · Decentralization.

1 Introduction

Nowadays, interbank transactions are made through financial institutions that use, not only, an outdated unidirectional messaging protocol to communicate the transactions information between them, but also, a costly and complicated fund transaction system.

With the emergence of blockchain technologies, some projects were created with the promise to revolutionize the current way that interbank transactions are processed [9].

1.1 Current interbank transactions issues

Current interbank transactions are supported by correspondent banking arrangements that allows the sender bank transact funds to the receiver bank through a sequence of intermediaries if the sender and the receiver banks don't have a direct correspondence, in other words, if the two banks don't have an agreement between them that allows direct transaction of funds. For this to be possible, financial institutions need to keep huge sums of funds in accounts inside all banks with which they have correspondence. According to Ripple, over than 27 trillion dollars are kept inside these accounts all around the world [7].

The need for intermediaries leads to bigger transactions times and more costly fees. An interbank transaction can take more than 3 days to be processed, depending on the number of intermediaries required for that transfer [15]. The same goes for fees cost, with more intermediaries more transfer rates will be added together. In the case of cross-currency transactions, expensively fixed exchanges rates are also applied.

1.2 Goals

Blockchain is a recent technology that is still in an exploratory state in terms of usage and applicability in different areas.

Idealizing the correct usage of blockchain technologies in an interbank transactions solution has the potential to solve some of the current issues.

The present work describes all the process involved in the creation of a possible better interbank transaction solution in comparison to the currently existing solutions. To accomplish that, there was made an extensive study through literature and technology review, followed by the design and implementation of a prototype and, in the end, an analysis of the results.

2 How are current interbank transactions made?

Nowadays, transactions between banks are sustained by the SWIFT messaging system, which establishes communication paths, and correspondent banking arrangements, that allow funds settlement.

2.1 SWIFT Messaging System

Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a cooperative undertaking controlled by its members, banks and other financial institutions, that provides secure messaging services and interface software for payment systems [12].

The SWIFT messaging system represents the primary communications channel for banking area, being used by more than 11,000 financial institutions all around the world. SWIFT is committed to the confidentiality, integrity, and availability of its messaging services [23].

2.2 Correspondent Banking Arrangements

The funds from transactions are transferred from one bank to the another through correspondent banking arrangements. If those two institutions don't have a direct correspondence will be required the use of intermediaries [12].

Two banks need to maintain a system of nostro/vostro accounts in order for a transaction to occur between them. Nostro refers to "our account of our money on your books" and vostro refers to "your account of your money on our books" [21].

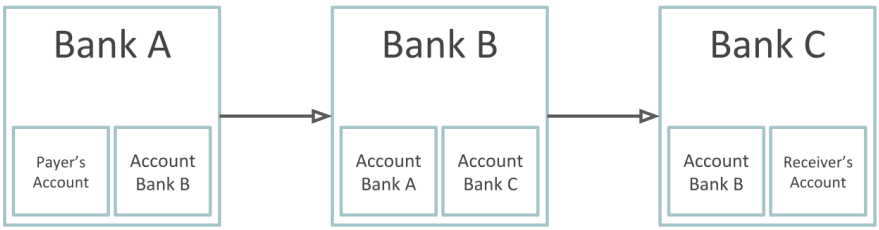

Fig. 1. Example of correspondent banking system.

Figure 1 illustrate the settlement of one payment from Bank A to Bank C via a correspondent banking chain, since Bank A and Bank C do not hold nostro accounts with each other. The transaction is processed in the following steps:

1. Debiting of payer's account in Bank A;
2. Crediting of Bank B's account in Bank A;
3. Payments message from Bank A to Bank B;
4. Debiting of Bank A's account in Bank B;
5. Crediting of Bank C's account in Bank B;
6. Payment Message from Bank B to Bank C;
7. Debiting of Banks B's account in Bank C;
8. Crediting of receiver's account in Bank C.

Generally, there could be more intermediaries involved in this process. All banks in this correspondent banking chain will need to have funds available in their nostro accounts in order to execute the payment.

2.3 Global Transfers

Cross-border transactions face many hurdles and delays because of country-specific regulations, currency differences (cross-currency transactions) and the need for more intermediaries [18]. In addition to transfer fees, exchange fees are also applied in a cross-currency transaction.

Nowadays, most international transactions occur in a very similar way to transactions between banks from the same country, using SWIFT messaging service and correspondent banking arrangements [14].

3 What is blockchain?

The blockchain is a decentralized and distributed ledger that keeps continuous updated digital records. It is maintained by a network of nodes with replicated and synchronized databases, visible to anyone within the network. A blockchain can be private, with restricted membership, or public, accessible to anyone.

3.1 The birth of blockchain and how it works

Blockchain was introduced with Bitcoin in 2008 as a solution to the double-spending problem [13][4]. Double-spending is when two or more transactions simultaneously claim the same output [5], in other words, when a user submits multiple transactions spending the available balance multiple times.

A blockchain network is composed of a set of clients, called nodes. Each one of these nodes holds a copy of the blockchain, forming a peer-to-peer network.

There are two types of records in a blockchain database: transactions and blocks. Transactions are batched into timestamped blocks. Each block is identified by a cryptographic hash. In addition to carrying a list of transactions, each block also references the hash of the previous block. This results in a link between the blocks, creating a chain of blocks [3]. The process to add transactions to the blockchain go through the following steps:

1. Users use a pair of private and public keys to sign their transactions.
2. Those transactions are broadcasted by their respective source node to its nearby peers.
3. The neighboring nodes validate the transactions and then repeat the previous step until the transactions are spread across the network.
4. After being validated by the network, the transactions are ordered and listed into a timestamped candidate block which is broadcasted back to the network, in a process called mining.
5. The network of nodes verify if the block contains valid transactions and if refers to the correct previous block
6. If everything is right, the block is added to the blockchain and the transactions are applied.

To decide if an incoming transaction is valid or not, certain rules, that each transaction should conform to, are programmed into all blockchain clients. Based on this set of rules each client will then decide if the transaction should be relayed to the network or not.

3.2 Cryptocurrencies

The birth of blockchain is directly related to cryptocurrencies since blockchain was introduced with Bitcoin in 2008 and followed by many more cryptocurrencies projects using this technology [6].

Cryptocurrencies are transferable digital assets secured by blockchain networks. They can represent any type of value, in other words, they can represent money, access to services or even the ownership of property [25].

There are a variety of cryptocurrencies with different purposes and use cases: privacy coins, supply chain-oriented coins, transaction-oriented coins, stable coins, and many others.

Transaction oriented coins are cryptocurrencies that were created to offer faster transactions, a higher number of transaction per second and lower fees.

4 Modern Interbank Transactions Solutions

Since the first mentions of blockchain technologies until the present day some solutions were designed and developed based on these technologies aimed to improve current way interbank transactions are made.

RippleNet And IBM Blockchain World Wire emerge as the fruit of the development in this area using blockchain technologies.

As a response to the new technologies and competitor solutions, SWIFT launch their Global Payments Innovation Initiative in other to deliver an up to date solution to interbank transactions.

4.1 SWIFT gpi

SWIFT gpi uses the current SWIFT messaging and correspondent banking system, adding to this old core a set of rules to commit banks to behave more reasonably in cross-border payments. These rules form a new service level agreement (SLA) rulebook that aims to provide the opportunity for enhanced business practices and smart collaboration between participating banks [2].

DLT Proof Of Concept Recently, SWIFT completed a blockchain proof of concept (PoC) to address Nostro account reconciliation issues [8]. However, the use of this distributed ledger technology would maintain the need for nostro accounts. The difference from the current reality is that SWIFT private blockchain would track nostro accounts balances and improve the reconciliation effort banks face today.

The PoC was completed without meeting all the requirements defined. SWIFT believes the technology is too new to undergo a security assessment and the regulatory developments remain in their infancy [24].

4.2 RippleNet

RippleNet is a global payment system that enables a network for financial institutions where payments can be sent and received via Ripple technology [19].

RippleNet offers its customers two main products, namely xCurrent and xRapid.

xCurrent xCurrent is a settlement solution for banks with the goal of improvement of cross-border transactions. xCurrent has a bidirectional messaging system to coordinate information exchange between the banks. It uses Interledger Protocol (ILP) to coordinate founds movement between institutions to settle the payment [16]. It is designed to fit within the bank's infrastructure, requiring minimal integration.

xCurrent allows the settlement of payments without intermediaries, but this settlement is still made through the use of nostro accounts.

xRapid After the integration of xCurrent, institutions will have the option of using xRapid. xRapid is made to eliminate the need for nostro accounts, using Ripple's digital currency XRP that offer on-demand liquidity, with improved speed and lower costs [17]. This is a core feature for cross-border transactions, especially in emerging markets where the trading volume is low and the cost of currency exchange is high.

4.3 IBM Blockchain World Wire

IBM Blockchain World Wire is a global payment solution presented by International Business Machines (IBM) in collaboration with Stellar Organization. The solution is intended to reduce the settlement time and lower the cost of completing global payments, helping financial institutions address the process of cross-border transactions [11].

This solution uses Hyperledger to drive the payment messaging and clearing component and digital currencies to facilitate the exchange, allowing for near real-time settlement [1][20].

Two financial institutions that want to make transactions between themselves agree to use a digital asset to work as a bridge between the fiat currencies the institutions use. The sender institution, connected to World Wire's APIs, converts their fiat currency into the chosen digital asset. Simultaneously, World Wide converts the digital asset into the fiat currency used by the receiver institution, completing the transaction. The transaction details are recorded onto a blockchain for clearing purposes [10].

4.4 Overview of the existing solutions

All of the previous solutions affirm to have better transaction times and lower transactions costs in comparison with the current way interbank transactions are made. However, as can be seen in the first two lines of Table 1, none of them provide specific information about these two aspects.

SWIFT gpi and RippleNet maintain the need for third-party financial institutions. Additionally to this, a big part of validator nodes from RippleNet blockchain are controlled by Ripple company, making this blockchain controversially centralized. Lastly, IBM's World Wire is based around a central exchange that all banks would use to transact money and without this central service the solution wouldn't work.

Table 1. Comparison of the modern interbank transactions solutions.

	SWIFT gpi	**Ripplenet**	**World Wire**
Transaction Time	30 min - 24 h	Seconds	Seconds
Transaction Cost	Reduce	Reduce	Reduce
Need for intermediaries	Yes	Yes	No
Need for Nostro accounts	Yes	No	No
Decentralized	No	No	No

5 Problems and Solution

As was mentioned initially, the current way interbank transactions are made presents some issues that need to be addressed. This work considers there are three main problems:

- **Processing Time** The time it takes for a transaction to be processed is directly related to the need for financial intermediaries.
  If two banks involved in the transaction don't have a direct correspondence, one or more intermediaries will be used to facilitate the transfer. Each intermediary adds a portion of time to the transaction between the sending and the receiving bank.
- **Transaction Costs** As processing time, transaction cost is also related to the need for intermediaries. Each intermediary applies a fee to transaction making it more and more costly.
- **Funds in nostro accounts** When we are talking about correspondent banks, we are referring to banks that hold Nostro accounts with each other. A bank needs to provide a great investment to fill its nostro accounts on correspondent banks.

5.1 Goal

In general, the existing solution analyzed in Section 4 try to address the defined problems, however, all of them fail in one main characteristic: decentralization. In other words, each of the analyzed solutions is controlled by a private company or are depended on a central entity.

Decentralization is one of the main aspects of blockchain and the current work considers that a proper solution for interbank transactions should inherit this aspect.

Therefore, this work defends that a blockchain based solution that is fully decentralized can address the defined problems in a better way than the rest of the existing solutions.

5.2 Solution

A solution was created after a rational process taking into account the conditionals and goals imposed by this work.

The solution consists of a cryptocurrency/fiat exchange where the main functionality is instant money transfer from a bank to another.

The exchange platform is divided into 2 views: one more complex and the other more user-friendly.

The more complex view is oriented for users who want to trade their currencies manually and to have the option to deposit/withdraw cryptocurrency, in other words, users that want to be directly involved with cryptocurrencies and have interest in the trading features of the platform.

This interaction with the platform is the heart of the solution since the market orders created by these users will sustain the instant money transfer functionality.

The instant money transfer functionality is present in the more user-friendly view. This view is for users that just want to transfer their fiat currency without the need for directly interacting with the trading markets or cryptocurrencies.

The sender platform automatically converts the fiat money into cryptocurrency money using the existing exchange market orders, and then sends the money through the blockchain network to the receiver bank. The receiver bank converts the received cryptocurrency money into fiat money using its own exchange market orders and, lastly, assigns the resulting fiat money to the recipient user.

Cold-start and low trading volume problems Early in the creation of this concept were considered two main flaws: a cold-start problem for banks that just started to use the solution and a trading volume problem for small banks.

Both situations can be summed up as low number or even nonexistent market orders on the bank exchange due to the small adoption of the solution by the bank users or due to a small client base of a bank.

Without sufficient amount of listed market orders on at least one of the two exchange platforms involved in a transaction, the process can't be completed as fast as might be expected.

To address this obstacle was suggested a solution that consists of a reserve of cryptocurrency maintained by the bank in order to fill their trading market with market orders when needed.

The cryptocurrency reserve has a maximum limit and minimum limit of cryptocurrency that the bank considers to be sufficient to meet their exchange platform requirements. The bank uses external cryptocurrency exchange platforms to buy cryptocurrencies when bank's reserve reaches their minimum limit or to sell if the reserve exceeds their maximum limit.

6 Design and Implementation

The Stellar blockchain and its native cryptocurrency XLM were used in the creation of the solution prototype providing a network for fast and low-cost transactions. Stellar's testnet was used to avoid being spent real money during the development and test of the platform.

The prototype was developed with NodeJS and MySQL.

The features of the solution prototype can be divided into 4 groups: exchange development, stellar integration, transacting between exchanges, and lastly, addressing cold-start and trading volume problems.

Exchange development Firstly, a simple cryptocurrency exchange was developed. This platform has 2 user interface views: "Market" and "Account". In the Market page, there are two separate tables for listing all buy and sell orders in the trading market. In the Account page, there are two tables for the buy and sell orders made by the corresponding user.

Stellar integration With the use of Stellar SDK it was possible to make deposits and withdraws of cryptocurrency. In the Account page, there was added deposit information and a withdraw form.

Transacting between exchanges One more user interface view was introduced in this step: "Send". In the Send page, there is a form with 3 fields that needs to be filled by the user in order to use the instant money transfer functionality.

Addressing cold-start and trading volume problems A separated project was created to interact with external cryptocurrency exchanges and to fill the main project exchange with market orders.

7 Results and Conclusions

After the development the solution went through a process of testing and comparison to the other existing solution from Section 4. The data obtained was synthesised into Table 2.

Table 2. Comparison of the developed solution with the other existing solutions.

	SWIFT gpi	**Ripplenet**	**World Wire**	**Solution**
Transaction Time	30 min - 24 h	Seconds	Seconds	7 seconds
Transaction Cost	Reduced	Reduced	Reduced	0.000001$
Intermediaries	Yes	Yes	No	No
Nostro accounts	Yes	No	No	No
Decentralized	No	No	No	Yes

Transaction time The transaction time obtained by the developed solution was recorded in a performance test using the Stellar testnet. As was said in Section 6, Stellar testnet was used during the development and end up being also used in the collection of performance data. Stellar states that testnet isn't the proper network for load and stress testing [22]. The data from other solutions isn't really specific, however, even using testnet, the developed solution achieved competitive results in terms of transaction time.

Transaction cost With respect to transaction cost, the only common cost for the user is the transaction fee applied by Stellar blockchain that is currently 0.00001 XLM (currently close to 0.000001$).

Additionally, it should be considered that there is a risk that the market orders values could be different in each exchange. This can cause value variations between the sent and received money. This work doesn't consider these variations as transaction cost since they can lead to a negative variation but also can lead to a possible positive variation, where the recipient account would receive more fiat money than it was sent.

Need for intermediaries There is no need for intermediaries in the developed solution. However, with the implementation of the solution for cold-start and low trading volume problems would be used external cryptocurrency exchanges to fill bank's cryptocurrency reserves.

Nostro accounts The solution doesn't use nostro accounts as the fiat money transfers only occur internally. Nevertheless, the investment needed for the cold-start and low trading volume solution can be compared to the investment current banks made into nostro accounts.

Decentralization The blockchain used and the developed solution are both decentralized. This decentralization can be called into question when the cold-start and low trading volume solution is applied since banks cryptocurrency reserves would be dependent on the interaction with external cryptocurrency exchanges. The number of external exchanges being used could be increased in order to decrease the dependency on each external exchange, yet the base solution without addressing cold-start and low trading volume problems would always be more decentralized.

7.1 Conclusions

Both time and cost of a transaction using the developed solution present competitive results. Sending money through the solution, however, has a risk associated: the cryptocurrency could be trading at distinct prices in different bank exchanges, which could impact the difference between the money sent and received. It would be interesting if future works attempt to minimize the risk,

maintaining the decentralization of the solution and small time and cost of the transactions.

In terms of the need for nostro accounts and the decentralization of the solution, both were debatably affected by the addition of the cold-start and low trading volume solution. With this in mind, there is a concern about the possibility of solutions for these and other real-world integration problems could affect the validation of the main solution decentralization and the need of investments similar to the investment banks currently make in nostro accounts.

References

1. Aitken, R.: IBM's Blockchain 'Cross-Border' Payments Initiative With Silicon Valley Firm To Drive Efficiencies (2017), https://www.forbes.com/sites/rogeraitken/2017/10/16/ibms-blockchain-cross-border-payments-initiative-with-silicon-valley-firm-to-drive-efficiencies/#3f200f5c7ef6
2. Blair, D.: Ripple vs SWIFT: Payment (r)evolution. Tech. rep. (2016), https://www.atc.asia/articles/170105/aca161124ripple.pdf
3. Carlozo, L.: What is blockchain? Journal of Accountancy **224**(1), 29 (2017)
4. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things (2016). https://doi.org/10.1109/ACCESS.2016.2566339, http://ieeexplore.ieee.org/document/7467408/
5. Decker, C., Wattenhofer, R.: Information propagation in the Bitcoin network. In: 13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings. pp. 1–10. IEEE (sep 2013). https://doi.org/10.1109/P2P.2013.6688704, http://ieeexplore.ieee.org/document/6688704/
6. Dziembowski, S., Stefan: Introduction to Cryptocurrencies. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15. pp. 1700–1701. ACM Press, New York, New York, USA (2015). https://doi.org/10.1145/2810103.2812704, http://dl.acm.org/citation.cfm?doid=2810103.2812704
7. Elison, M.: McKinsey: Corporates Need Faster Payments, Too — Ripple (2016), https://ripple.com/insights/mckinsey-corporates-need-faster-payments/
8. Elison, M.: SWIFT GPI Part 3: the Empire Strikes Back — Ripple (2017), https://ripple.com/insights/empire-strikes-back/
9. He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Saadi Sedik, T., Stetsenko, N., Verdugo Yepes, C.: Virtual Currencies and Beyond: Initial Considerations. Staff Discussion Notes **16**(3), 42 (2016). https://doi.org/10.5089/9781498363273.006, www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf
10. IBM: How IBM Blockchain World Wire revolutionizes cross-border payments - Flyer (2018), https://www.ibm.com/downloads/cas/YW3W2JPZ
11. IBM: IBM Blockchain World Wire Cross-Border Payments Solution — IBM (2018), https://www.ibm.com/blockchain/solutions/world-wire
12. Kokkola, T.: The Payment System - Payments, Securities and Derivatives, and the Role of the Eurosystem (2010), http://www.ecb.europa.eu http://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf

13. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.Org p. 9 (2008). https://doi.org/10.1007/s10838-008-9062-0, https://bitcoin.org/bitcoin.pdf
14. Park, Y.S.: The Inefficiencies of Cross-Border Payments: How Current Forces are Shaping the Future. Visa International Service Association p. 36 (2006), http://euro.ecom.cmu.edu/resources/elibrary/epay/crossborder.pdf
15. Ripple: The Cost-Cutting Case for Banks The ROI of Using Ripple and XRP for Global Interbank Settlements (2016), https://ripple.com/files/xrp_cost_model_paper.pdf
16. Ripple: A brief technical overview for financial institutions on RippleNet. Tech. rep., Ripple (2017), https://ripple.com/files/xcurrent_brochure.pdf
17. Ripple: One frictionless experience to send money globally. Tech. rep., Ripple (2017), https://ripple.com/files/ripplenet_brochure.pdf
18. Ripple: Liquidity Explained — Ripple (2018), https://ripple.com/insights/liquidity-explained/
19. Ripple: Solutions To Send Money Globally, Using Blockchain Technology (2018), https://ripple.com/solutions/
20. Roberts, J.: Blockchain Banking: IBM Launches Global Payment Platform — Fortune (2017), http://fortune.com/2017/10/16/ibm-blockchain-stellar/
21. de Roover, R.: The Medici Bank Financial and Commercial Operations. The Journal of Economic History **6**(2), 153–172 (nov 1946). https://doi.org/10.1017/S0022050700056916, http://www.journals.cambridge.org/abstract_S0022050700056916
22. Stellar: Testnet — Stellar Developers (2018), https://www.stellar.org/developers/guides/concepts/test-net.html
23. Swift: Discover SWIFT (2017), https://www.swift.com/about-us/discover-swift/messaging-standards
24. SWIFT: Can blockchain pave the way for real-time Nostro reconciliation and liquidity optimisation ? Tech. rep. (2018)
25. White, L.H.: The Market for Cryptocurrencies. SSRN Electronic Journal (dec 2014). https://doi.org/10.2139/ssrn.2538290, http://www.ssrn.com/abstract=2538290

Nomenclature

API	Application programming interface.
DLT	Distributed Ledger Technology.
FX	Foreign exchange rate.
gpi	Global Payments Innovation Initiative.
IBAN	International Bank Account Number.
IBM	International Business Machine.
ILP	Interledger Protocol.
KYC	Know your costumer.
PoC	Proof of Concept.
SWIFT	Society for Worldwide Interbank Financial Telecommunications.

References

[1] D. He, K. Habermeier, R. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakos-Saad, H. Oura, T. Saadi Sedik, N. Stetsenko, and C. Verdugo Yepes, "Virtual Currencies and Beyond: Initial Considerations," *Staff Discussion Notes*, vol. 16, no. 3, p. 42, 2016. [Online]. Available: www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf Cited on p. 1.

[2] EbankIT, "EBANKIT | Omnichannel Innovation." [Online]. Available: http://www.ebankit.com/ Cited on p. 1.

[3] Ripple, "Liquidity Explained," 2018. [Online]. Available: https://ripple.com/insights/liquidity-explained/ Cited on pp. 1 and 7.

[4] M. Elison, "McKinsey: Corporates Need Faster Payments, Too," 2016. [Online]. Available: https://ripple.com/insights/mckinsey-corporates-need-faster-payments/ Cited on p. 2.

[5] Ripple, "The Cost-Cutting Case for Banks The ROI of Using Ripple and XRP for Global Interbank Settlements," 2016. [Online]. Available: https://ripple.com/files/xrp_cost_model_paper.pdf Cited on pp. 2 and 7.

[6] S. Seth, "How the SWIFT System Works," 2017. [Online]. Available: https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp Cited on p. 5.

[7] T. Kokkola, *The Payment System - Payments, Securities and Derivatives, and the Role of the Eurosystem*, 2010. [Online]. Available: http://www.ecb.europa.eu/pub/pdf/other/paymentsystem201009en.pdf Cited on pp. 5 and 6.

[8] S. V. Scott and M. Zachariadis, "Origins and development of SWIFT, 1973–2009," *Business History*, vol. 54, no. 3, pp. 462–482, jun 2012. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/00076791.2011.638502 Cited on p. 6.

[9] Swift, "Discover SWIFT," p. 1, 2017. [Online]. Available: https://www.swift.com/about-us/discover-swift/messaging-standards Cited on p. 6.

[10] R. de Roover, "The Medici Bank Financial and Commercial Operations," *The Journal of Economic History*, vol. 6, no. 2, pp. 153–172, nov 1946. [Online]. Available: http://www.journals.cambridge.org/abstract_S0022050700056916 Cited on p. 6.

[11] Y. S. Park, "The Inefficiencies of Cross-Border Payments: How Current Forces are Shaping the Future," *Visa International Service Association*, p. 36, 2006. [Online]. Available: http://euro.ecom.cmu.edu/resources/elibrary/epay/crossborder.pdf Cited on p. 7.

[12] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin.Org*, p. 9, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf Cited on p. 8.

[13] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," pp. 2292–2303, 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7467408/ Cited on p. 8.

[14] S. Dziembowski and Stefan, "Introduction to Cryptocurrencies," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*. New York, New York, USA: ACM Press, 2015, pp. 1700–1701. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2810103.2812704 Cited on p. 8.

[15] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings*. IEEE, sep 2013, pp. 1–10. [Online]. Available: http://ieeexplore.ieee.org/document/6688704/ Cited on p. 8.

[16] L. Carlozo, "What is blockchain?" *Journal of Accountancy*, vol. 224, no. 1, p. 29, 2017. [Online]. Available: https://www.journalofaccountancy.com/issues/2017/jul/what-is-blockchain.html Cited on p. 8.

[17] J. R. Douceur, "The Sybil Attack." Springer, Berlin, Heidelberg, 2002, pp. 251–260. [Online]. Available: http://link.springer.com/10.1007/3-540-45748-8_24 Cited on p. 9.

[18] National Institute of Standards and Technology, "FIPS.180-4 Secure Hash Standard (SHS)," vol. 4, no. March 2012, 2015. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/180/2/archive/2002-08-01 Cited on p. 9.

[19] C. Percival, "The scrypt key derivation function and encryption utility," 2009. [Online]. Available: https://www.tarsnap.com/scrypt.html Cited on p. 9.

[20] Litecoin, "Litecoin - Open source P2P digital currency," 2013. [Online]. Available: https://litecoin.org/ Cited on p. 9.

[21] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, jul 1982. [Online]. Available: http://portal.acm.org/citation.cfm?doid=357172.357176 Cited on p. 9.

[22] R. Lai and D. Lee Kuo Chuen, "Blockchain-From Public to Private," in *Handbook of Blockchain, Digital Finance, and Inclusion*. Academic Press, jan 2017, vol. 2, pp. 145–177. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128122822000073 Cited on p. 10.

[23] M. J. Rennock, A. Cohn, and J. Butcher, "Blockchain Technology and Regulatory Investigations," *Practical Law The Journal*, p. 11, 2018. [Online]. Available: https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature-Blockchain.pdf Cited on p. 10.

[24] L. H. White, "The market for cryptocurrencies," *Cato Journal*, vol. 35, no. 2, pp. 383–402, 2015. [Online]. Available: https://object.cato.org/sites/cato.org/files/serials/files/cato-journal/2015/5/cj-v35n2-13.pdf Cited on p. 10.

[25] CoinMarketCap, "Cryptocurrency Exchange Rankings." [Online]. Available: https://coinmarketcap.com/rankings/exchanges/ Cited on p. 11.

[26] D. Blair, "Ripple vs SWIFT: Payment (r)evolution," Tech. Rep., 2016. [Online]. Available: https://www.atc.asia/articles/170105/aca161124ripple.pdf Cited on p. 14.

[27] M. Elison, "SWIFT GPI Part 3: the Empire Strikes Back," 2017. [Online]. Available: https://ripple.com/insights/empire-strikes-back/ Cited on p. 14.

[28] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. W. Cocco, and J. Yellick, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *CoRR*, vol. abs/1801.1, 2018. [Online]. Available: http://arxiv.org/abs/1801.10228 Cited on p. 14.

[29] SWIFT, "gpi real-time Nostro Proof of Concept," Tech. Rep., 2018. [Online]. Available: https://www.swift.com/resource/gpi-real-time-nostro-proof-concept Cited on pp. 14 and 15.

[30] SWIFT, Accenture, and W. F. of Exchanges, "SWIFT on distributed ledger technologies," *Position paper*, 2016. [Online]. Available: https://www.swift.com/insights/press-releases/swift-and-accenture-outline-path-to-distributed-ledger-technology-adoption-within-financial-services Cited on p. 14.

[31] Ripple, "Solutions To Send Money Globally, Using Blockchain Technology," 2018. [Online]. Available: https://ripple.com/solutions/ Cited on p. 15.

[32] ——, "xCurrent," Ripple, Tech. Rep., 2017. [Online]. Available: https://ripple.com/files/xcurrent_brochure.pdf Cited on pp. 15 and 17.

[33] ——, "RippleNet," Ripple, Tech. Rep., 2017. [Online]. Available: https://ripple.com/files/ripplenet_brochure.pdf Cited on pp. 15, 16, and 17.

[34] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," Tech. Rep., 2008. [Online]. Available: https://www.rfc-editor.org/info/rfc5246 Cited on p. 16.

[35] IBM, "IBM Blockchain World Wire," 2019. [Online]. Available: https://www.ibm.com/blockchain/solutions/world-wire Cited on p. 16.

[36] R. Aitken, "IBM's Blockchain 'Cross-Border' Payments Initiative With Silicon Valley Firm To Drive Efficiencies," 2017. [Online]. Available: https://www.forbes.com/sites/rogeraitken/2017/10/16/ibms-blockchain-cross-border-payments-initiative-with-silicon-valley-firm-to-drive-efficiencies/{#}3f200f5c7ef6 Cited on p. 16.

[37] J. Roberts, "IBM and Stellar Are Launching Blockchain Banking Across Multiple Countries," 2017. [Online]. Available: http://fortune.com/2017/10/16/ibm-blockchain-stellar/ Cited on p. 16.

[38] IBM, "IBM Blockchain World Wire, a New Global Payment Network, to Support Payments and Foreign Exchange in More Than 50 Countries - Mar 18, 2019," 2019. [Online]. Available: https://newsroom.ibm.com/2019-03-18-IBM-Blockchain-World-Wire-a-New-Global-Payment-Network-to-Support-Payments-and-Foreign-Exchange-in-More-Than-50-Countries Cited on p. 16.

[39] ——, *How IBM Blockchain World Wire revolutionizes cross-border payments - Flyer*, 2018. [Online]. Available: https://www.ibm.com/downloads/cas/YW3W2JPZ Cited on p. 17.

[40] SWIFT, "SWIFT gpi reduces cross-border payment times to minutes, even seconds," 2018. [Online]. Available: https://www.swift.com/news-events/press-releases/swift-gpi-reduces-cross-border-payment-times-to-minutes_even-seconds Cited on p. 18.

[41] ——, "SWIFT gpi for banks," 2018. [Online]. Available: https://www.swift.com/our-solutions/swift-gpi/swift-gpi-for-banks Cited on p. 18.

[42] U. W. Chohan, "Are Stable Coins Stable?" *SSRN Electronic Journal*, jan 2019. [Online]. Available: https://www.ssrn.com/abstract=3326823 Cited on p. 19.

[43] R. Sams, "A Note on Cryptocurrency Stabilisation: Seigniorage Shares," Tech. Rep., 2015. [Online]. Available: https://assets.ctfassets.net/sdlntm3tthp6/resource-asset-r390/5a940afb21681d19c0b3b76cf69259e1/58ebe9e2-1f28-4a8d-8ce1-26abef07aedf.pdf Cited on p. 20.

[44] Stellar.org, "Horizon," 2018. [Online]. Available: https://www.stellar.org/developers/horizon/reference/ Cited on p. 32.

[45] ——, "Stellar Network Overview," 2018. [Online]. Available: https://www.stellar.org/developers/guides/get-started/ Cited on p. 32.

[46] ——, "Stellar Consensus Protocol," 2018. [Online]. Available: https://www.stellar.org/developers/guides/concepts/scp.html Cited on p. 32.

[47] ——, "Testnet," 2018. [Online]. Available: https://www.stellar.org/developers/guides/concepts/test-net.html Cited on pp. 32 and 39.