ADMAS UNIVERSITY SCHOOL OF POST GRADUATE STUDIES

DEPARTMENT OF COMPUTER SCIENCE - SECTION 2

OBJECT ORIENTED SYSTEM DESIGN

Cross-Border Money Transfer Using Blockchain

Requirements Analysis Document (RAD)

Project Members:

Name	ID No.
Seifu Birega	PGMGC/8062/20
Yordanos Woldu	PGMGC/8053/20
Mekonnen Ayalew	PGMGC/3118/19
Simeon Gebre Yohanes	PGMGC/8067/20
Habtamu Birhan Godana	PGMGC/8023/20

JANUARY 31, 2021

Table of Contents

1. Introduction

1.1. Overview

Blockchain is an electronic shared ledger for building an immutable historical record of transactions. The ledgers are concurrently stored in multiple computers that are part of the network to ensure a shared view of the same data. This eliminates extensive and complex reconciliation process banks put in place to ensure transaction consistency across systems involved in payment processing. Additionally, it helps in improving customer experience by getting them useful information – *exact timings*, *amounts*, *charges* and *fees* collected by each party in a fund transfer – quickly.

Currently, *data reconciliation* sits at the heart of most business models. However, because everyone maintains their own data, the process is affected by inefficiencies, such as the need for different parties to constantly message data back and forth between them to get things done. *Blockchain, by contrast, could enable a progression from today's multiple and sequential data reconciliation models to a much more efficient process in which reconciliation is an integral part of the transactional process.* (Accenture Consulting)

1.2. The Payment Industry

The payments industry is one of the major business areas of financial companies. Estimates show that the payments industry makes up ***34%*** of the global banking industry (Mckinsey, 2017).

Transferring money across international borders often involves sending money to people via money transfer operators and banks. Such transactions are known as remittances and are a large and growing business. For instance, expats send home more than $600 billion during 2016 (World Bank Group, 2015). The global payments industry continues to grow, with transaction volumes and account balances showing healthy developments. This positive scenario lays the groundwork for technological disruption which can change the dynamics between Fintechs and financial institutions (McKinsey, 2017). The trend of digitalization of services and processes is pushing financial companies to rethink their business models and strategies. [1]

1.3. The Blockchain Technology

Blockchain is attracting attention in the Fintech industry because of its potential to revolutionize operations, financials and business models (Deloitte, 2016). In a report, Deloitte states that blockchain ‘’is a technology that could transform the very infrastructure of financial services. It offers a chance to reimagine the industry, rebuilding financial processes into something simpler, more efficient and often altogether new. Blockchain also challenges many of the assumptions underlying today’s business models’’ (Deloitte, 2016). In just three years, blockchain has more than 2,500 patent filings and over $1.4 billion in investments. More than 24 countries are investing in it, 50 corporations have joined consortia around it, and 90 banks are discussing its potential. It is predicted that 80 percent of banks are initiating blockchain projects (Deloitte, 2016b). [1]

1.4. How a Blockchain works

The concept of the blockchain here is explained by explaining how Bitcoin works since it is intrinsically linked to the Bitcoin. However, the blockchain technology is applicable to any digital asset transaction exchanged online; in our case digital money transfer from Payer/Sender to Payee/ Receiver.

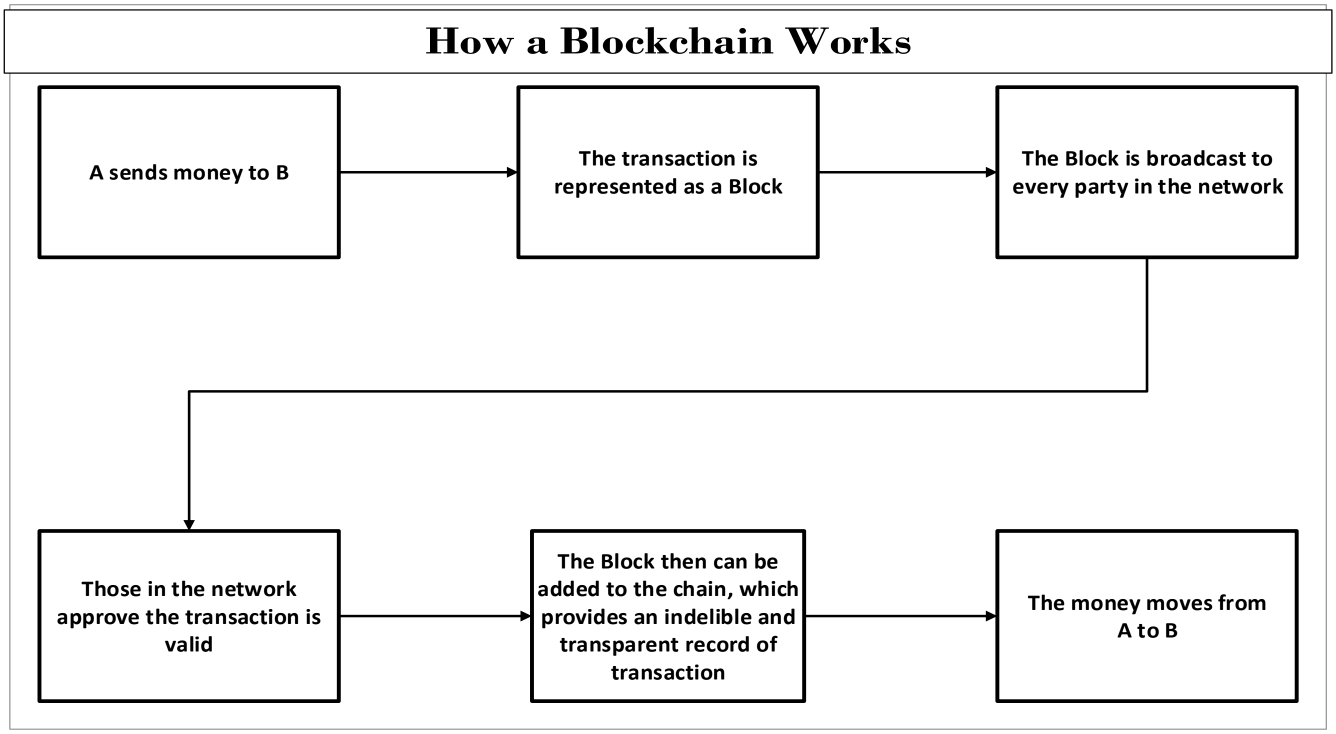
How a Blockchain Works
A sends money to B
The transaction is represented as a Block
The Block is broadcast to every party in the network
Those in the network approve the transaction is valid
The Block then can be added to the chain, which provides an indelible and transparent record of transaction
The money moves from A to B

Fig 1: How a blockchain works

Bitcoin uses cryptographic proof instead of the trust in the third party for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature. Each transaction is sent to the "public key" of the receiver digitally signed using the "private key" of the sender. In order to send money, owner of the cryptocurrency needs to prove the ownership of the "private key". The entity receiving the digital currency verifies the digital signature –thus ownership of corresponding "private key" -- on the transaction using the "public key" of the sender.

Each transaction is broadcast to every node in the Bitcoin network and is then recorded in a public ledger after verification. Every single transaction needs to be verified for validity before it is recorded in the public ledger. Verifying node needs to ensure two things before recording any transaction:

1. Sender/Payer owns the cryptocurrency—digital signature verification on the transaction.

2. Sender/ Payer has sufficient cryptocurrency in his/her account: checking every transaction against sender's account ("public key") in the ledger to make sure that he/she has sufficient balance in his/her account.

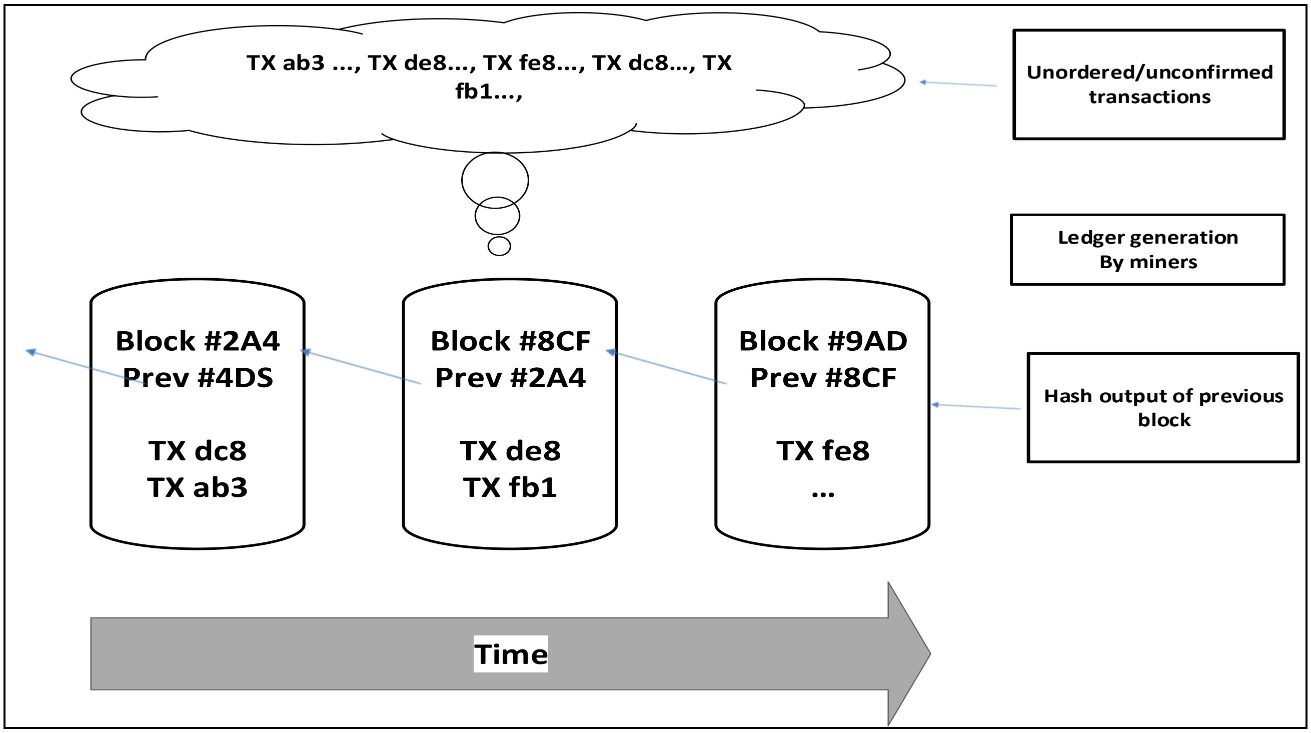
TX ab3 ..., TX de8..., TX fe8..., TX dc8..., TX fb1...,
Unordered/unconfirmed transactions
Ledger generation By miners
Block #2A4
Prev #4DS
TX dc8
TX ab3
Block #8CF
Prev #2A4
TX de8
TX fb1
Block #9AD
Prev #8CF
TX fe8
...
Hash output of previous block
Time

Fig 2: Generation of Blockchain from unordered transactions

The Bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called ***Blockchain***. The transactions in one block are considered to have happened at the same time. *These blocks are linked to each-other (like a chain) in a proper linear, chronological order with every block containing the hash of the previous block*. There still remains one problem. Any node in the network can collect unconfirmed transactions and create a block and then broadcasts it to rest of the network as a suggestion as to which block should be the next one in the blockchain.

How does the network decide which block should be next in the blockchain?

There can be multiple blocks created by different nodes at the same time. One can't rely on the order since blocks can arrive at different orders at different points in the network.

Bitcoin solves this problem by introducing a mathematical puzzle: each block will be accepted in the blockchain provided it contains an answer to a very special mathematical problem. This is also known as ***"proof of work"—***node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle. For instance, a node can be required to find a "nonce" which when hashed with transactions and hash of previous block produces a hash with certain number of leading zeros. The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash.

This mathematical puzzle is not trivial to solve and the complexity of the problem can be adjusted so that *on average it takes ten minutes* for a node in the Bitcoin network to make a right guess and generate a block. There is very small probability that more than one block will be generated in the system at a given time. First node, to solve the problem, broadcasts the block to rest of the network. Occasionally, however, more than one block will be solved at the same time, leading to several possible branches. However, the math of solving is very complicated and hence the blockchain quickly stabilizes, meaning that every node is in agreement about the ordering of blocks a few back from the end of the chain. The nodes donating their computing resources to solve the puzzle and generate block are called ***"miner" nodes"*** and are financially awarded for their efforts.

2. Current System

2.1. Overview

Currently, the infrastructure of global payments moves money from payment system to payment system through a series of internal book transfers across financial institutions. Most international transactions are executed through the *Society for Worldwide Interbank Financial Telecommunications (SWIFT)* network, a *cooperative society founded by seven international banks* which operate a global network *to facilitate the messaging of financial transfers.* Using this messaging system, banks can exchange data for funds transactions between financial institutions. SWIFT provides a network that allows over 10,000 financial institutions in 212 different countries to send and receive information about financial transactions to each other (Source: Transferwise, 2018). [1]

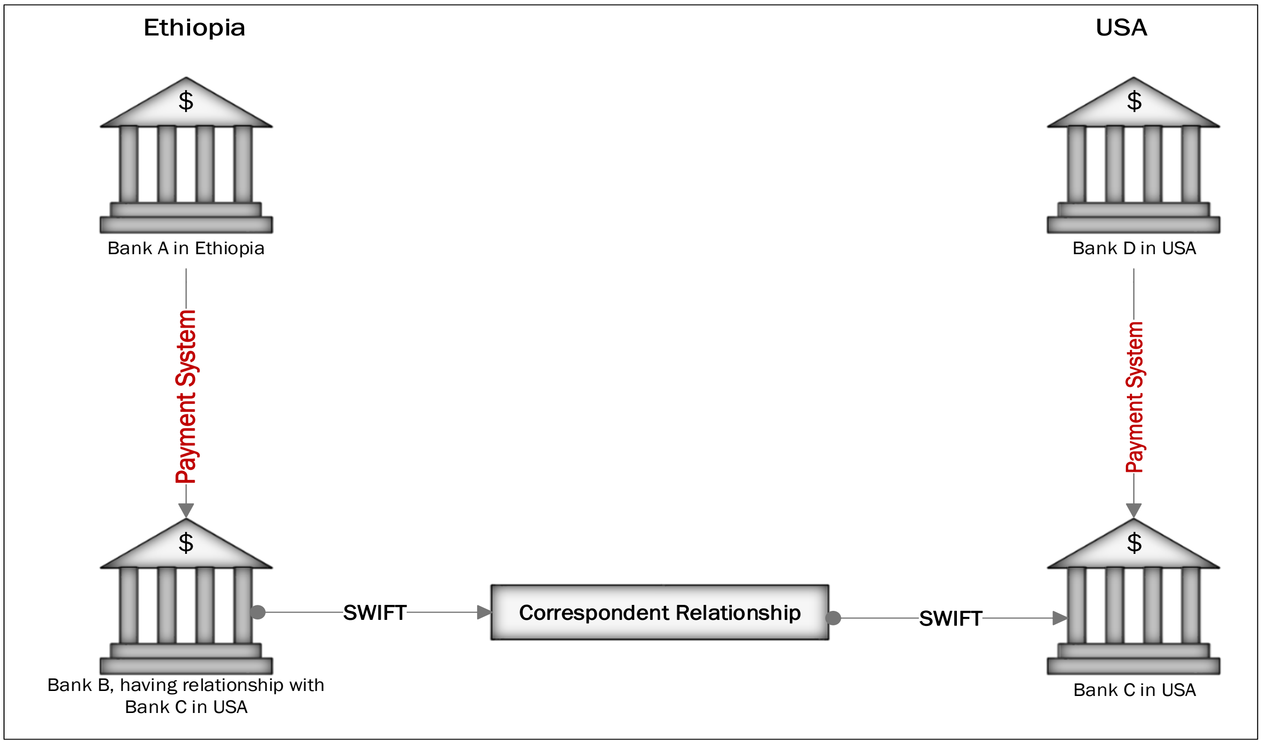

Fig 3: The traditional cross-border payment system (Bank A to Bank D)-USD Account

SWIFT does not actually send money; it just sends messages between the banks. As a result, other systems requiring more human intervention must be used to transfer the actual funds and this makes SWIFT transfers slow and costly because of the complex nature of these transactions.

Subsequently, in order to conduct international payments, a bank has to pre-fund a bank account or establish a line of credit with a correspondent bank. The correspondent bank provides the liquidity for these international payments in local currency accounts overseas, either itself or through partnerships.

2.2. Limitations of the traditional cross-border payment system

As the demand for cross-border payments is increasing, the traditional cross-border payment system is cost prohibitive and inefficient. The traditional cross-border payment system has four issues

1. **Access**

   For financial institutions, it is too expensive to fund positions around the world to service cross-border transactions. Instead, they rely on multiple correspondent banks to provide access to global currency corridors.

2. **Certainty**

   Sets of intermediaries' route payments and relay messages independent of funds settlement. With several potential points of failure and limited transaction visibility, the system results in frequent errors, unpredictable processing times, and uncertainty in the delivery of funds.

3. **Speed**

   Global payments can take up to seven days of processing time, depending on the currency corridor. The more parties involved, the longer transactions take to settle, especially across different time zones.

4. **Cost**

   Currently, banks absorb significant costs in order to service global payments, such as payment processing, treasury operations, foreign exchange, liquidity and compliance.

3. Proposed System – Blockchain Based Cross-Border Money Transfer

3.1. Overview

As one of the major use cases in the financial sector, the main hypothesis is that the ***Global Cross-Border Money Transfer System*** using Blockchain technology establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic, open and scalable digital economy from a centralized one.

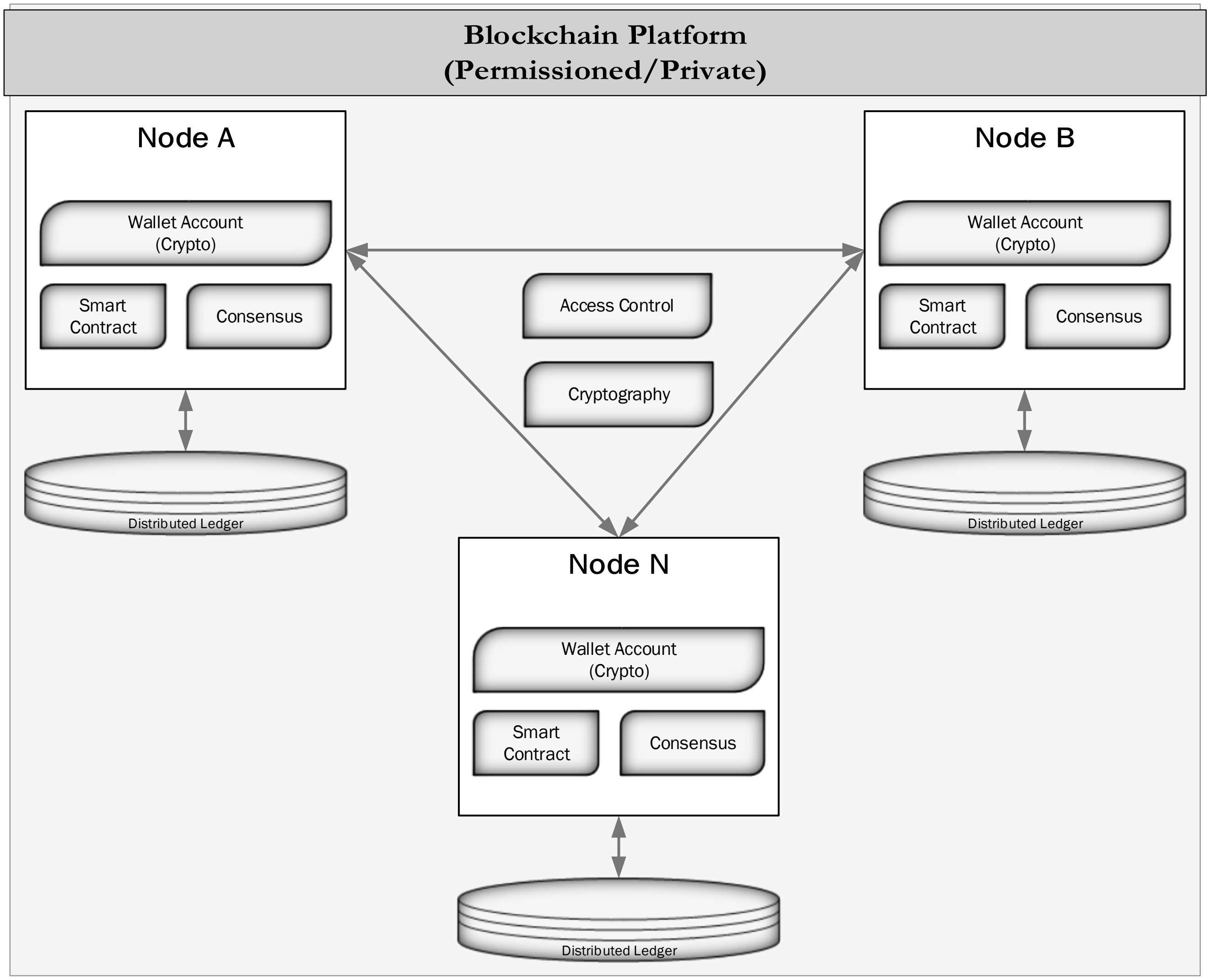

Fig 4: A Permissioned Blockchain Platform-Proposed

3.2. The Blockchain Technology

The blockchain is a private / public, trusted and shared ledger, based on a ***peer-to-peer network*** as shown in ***Fig 4***. above; meaning no one controls it, instead it is maintained by thousands of participants, making it a shared ledger. Since the blockchain is available to all the participants, it is a public ledger. The information that is recorded on the blockchain cannot be manipulated without going unnoticed, making it a trusted ledger. These elements allow information transfer on the blockchain without any intermediaries. Consequently, the role played by financial institutions as trusted third party mitigating the risk of a transaction is being questioned. Blockchain and its benefits are interesting for the payments industry, as it promises to facilitate fast, secure, low-cost international payment processing services through the use of encrypted distributed ledgers that enable trusted verification of transactions in real time without needing intermediaries.

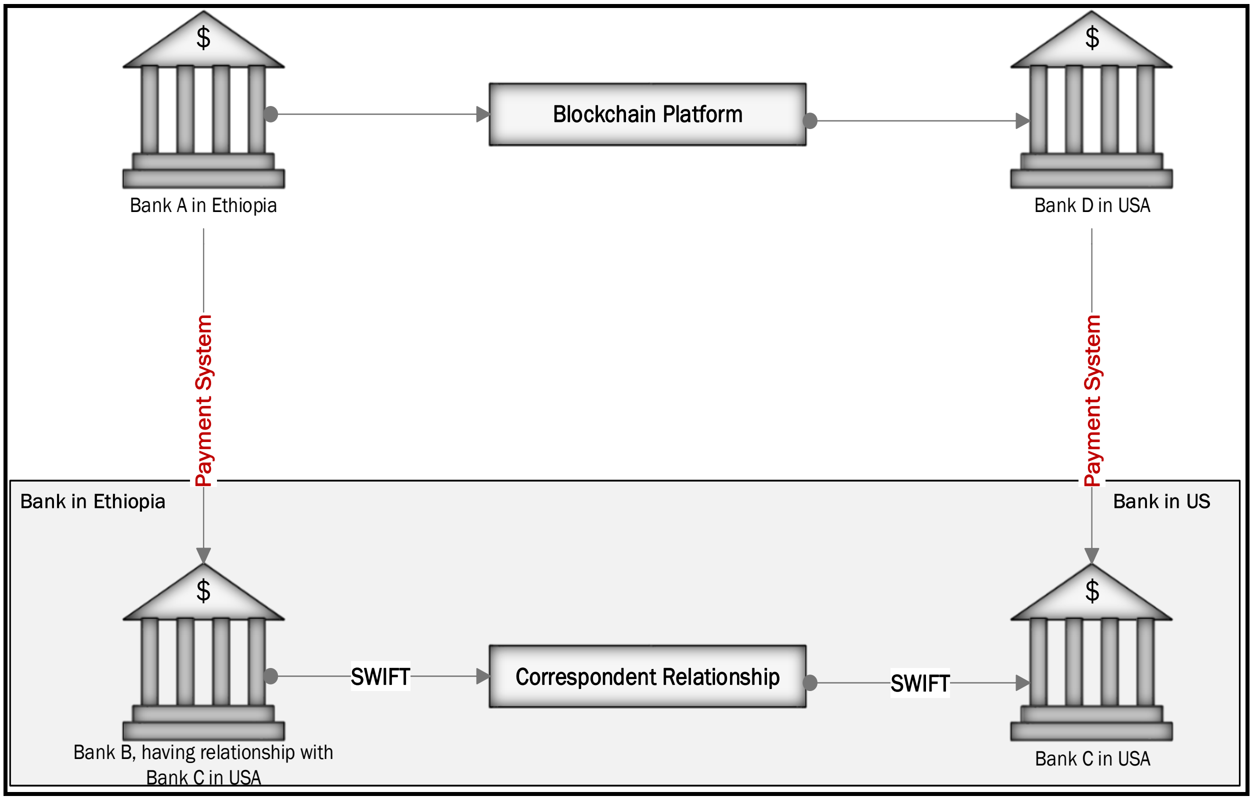

Fig 5: Money transfer from Bank A to Bank D eliminating the intermediaries as shown in the shaded part

3.3. Advantages of the proposed payment system

The transactions in blockchain are *cryptographically signed to prevent tampering, making it a secured and trusted platform*. Additionally, an *auditable trail of all the transactions is maintained in the ledger*. *These features remove the necessity of a trusted middle man or intermediary banks financial institutions rely on for global payments.* The use of intermediary adds to the cost and causes a delay in payment processing. Blockchain avoids delays and expensive payments made for the intermediaries as shown in figure 3 above.

Apart from the above advantages the following are also the potential advantages of blockchain technology [2]

Better resilience:

The decentralized nature of blockchain significantly reduces or even removes the risk of a single point of failure.

Better auditability:

As all transactions are recorded in the blockchain, auditing can be decentralized and performed by anyone holding a copy of the master ledger, significantly increasing transparency. While transparency is anoption in centralized systems, as the data could be published by the maintainer, a blockchain ensures that data must be public.

Better security:

Because transaction ordering may be performed by a majority of parties, it is less prone to fraud and collusion, thus increasing security.

Reduced legal requirements:

As validation is built-in by design, blockchain systems may prove far more efficient in terms of governance. The time, human and financial resources employed by a large number of institutions (banks, regulators, law enforcement, courts) to mediate disputes can be reduced, leading to lower legal and oversight costs related to financial transactions.

Notice: Limitations of the traditional cross-border money transfer like ***Access***, ***Certainty***, ***Speed***, and ***Cost*** will be resolved by the proposed ***Cross-Border Money Transfer using Blockchain*** technology which were discussed in ***section 2.2*** above.

3.4. Functional Requirements

As specified in the proposed system section of this document the following are the requirements of the system

- The system will transfer money in a cross-border location in a peer-to-peer manner, this includes
    - Sender/Payer opens his Wallet Cryptographic Account
    - Scan / Copy the receiver's / payee's address

- Enters the transfer amount and the fee to the system
- Transfer / Sends the amount to the Payee
- *The system mines the data, calculates the hash*
- The transaction is propagated and validated by the network
- The wallet signs the transaction using the Senders private key
- The nodes verify the result and propagate the *block / transaction*
- Confirmation message will be displayed to the payee and the payer

3.5. Non-Functional Requirements

Since the project duration is very short (***February 1, 2021 to March 13, 2021***) and the Blockchain technology is in its infant stages the non-functional requirements like ***latency***, ***integrity***, ***cost***, ***confidentiality*** and ***throughput*** issues are not considered as part of this project.

3.6. Limitations of the proposed system

As the Blockchain technology is in its infant stage and the project duration is very short (*February 1, 2021 to March 13, 2021*), further developments and detail research in this area are crucial, to make the project as effective and feasible as possible. The following are the limitations of the proposed system

- The system is proposed to work in a permissioned / private Blockchain platform
- *Smart contract* and *Consensus agreements* are not part of this proposal
- Non-functional requirements are not considered as part of the RAD.
- Modeling, designing, and implementation of the system can be challenging using the existing software engineering processes and tools.
- Our knowledge to *data mining*, *data warehouse*, *cryptography* and *big data* is limited, it is therefore we will research more in the area after we take a course related to the above concepts or develop our knowledge in the above areas by ourselves.
- The System modeling section needs time to model the system; we decided to work with and research the blockchain Cross-Border money transfer with less than a week from the list of options – Smart Shopping using IoT, Blockchain and IoT.

4. System Models using UML

4.1. Use Case Diagram

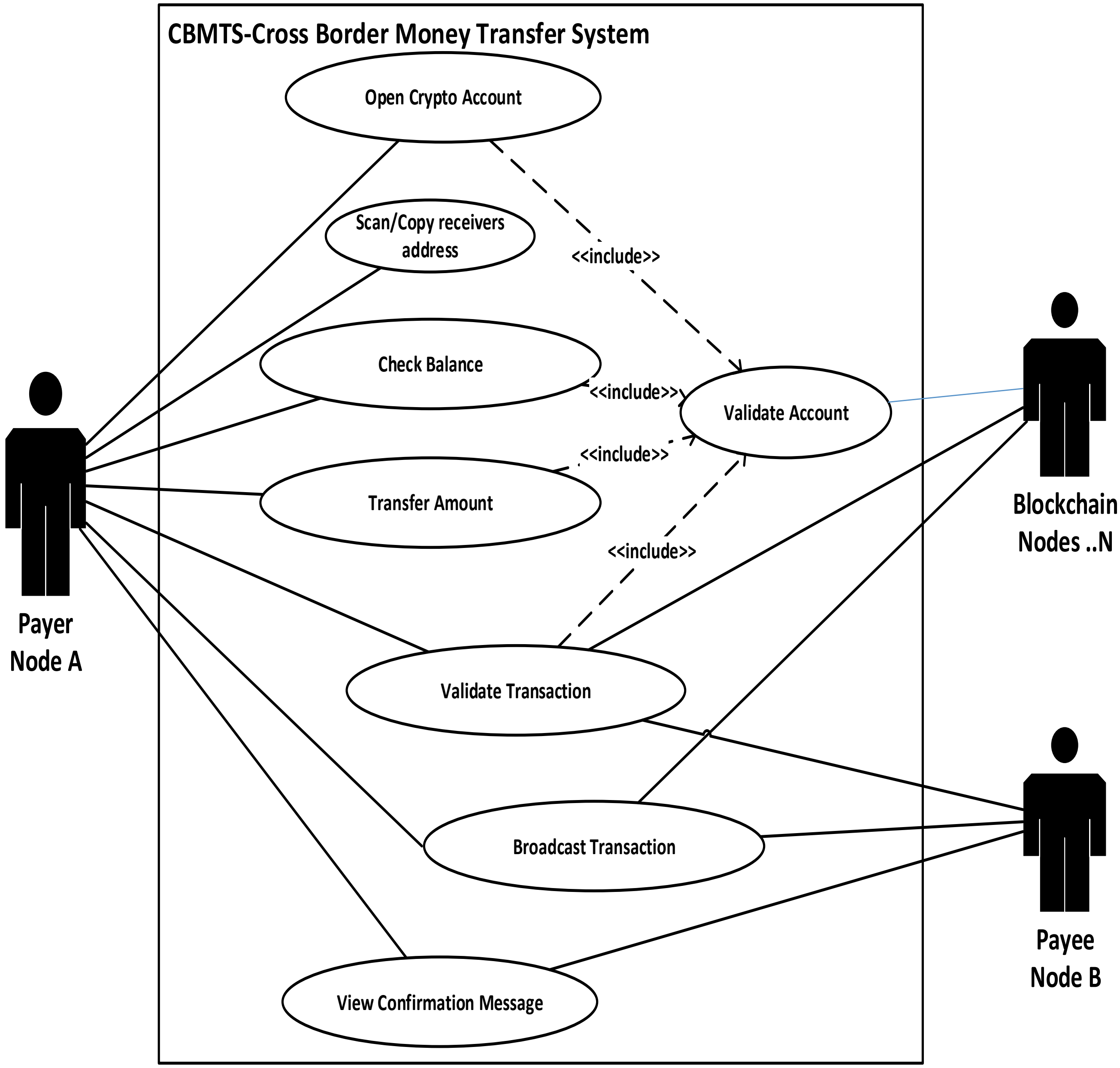

Fig 6: Use Case Diagram

4.2. Class Diagram

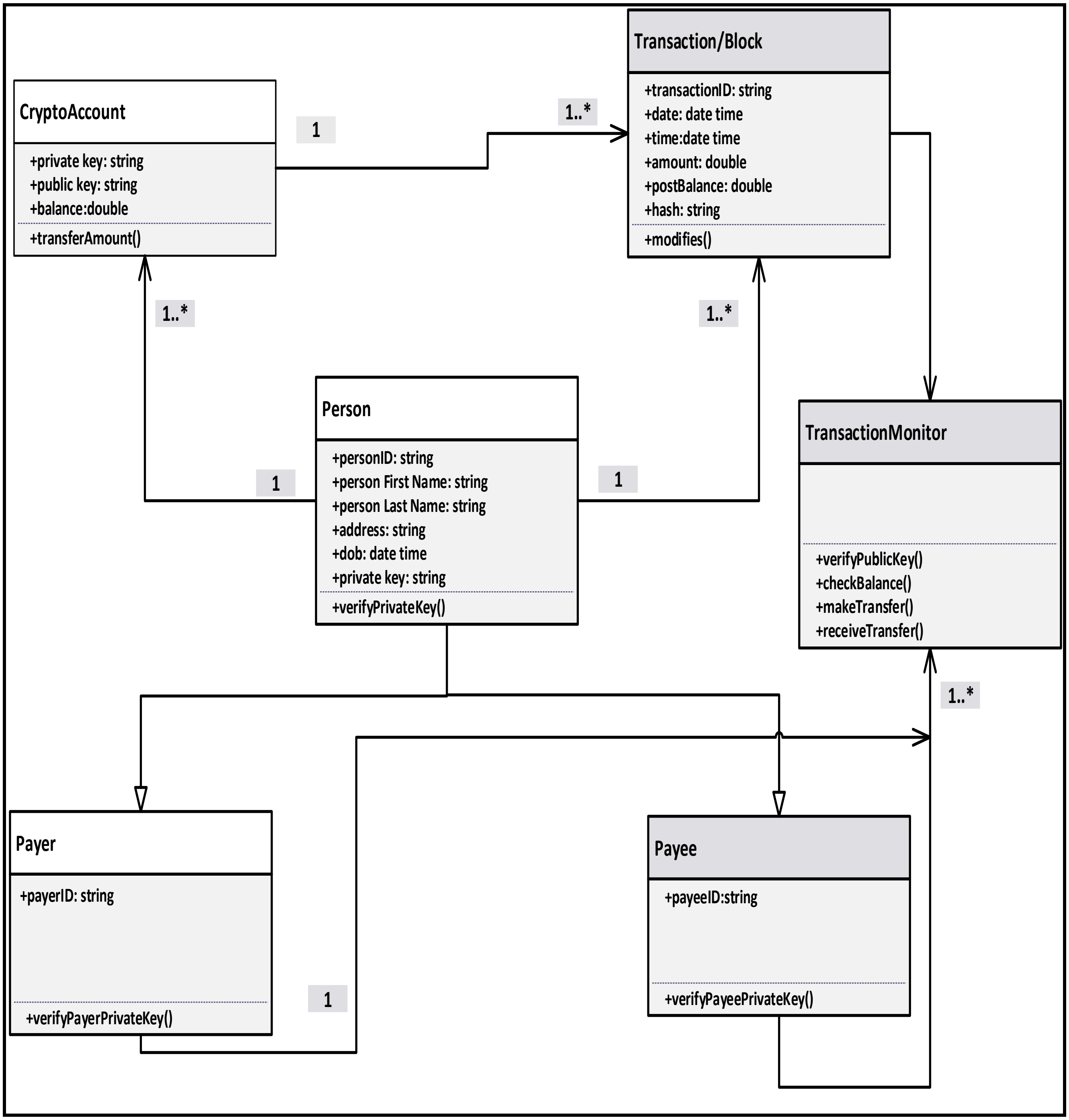

Fig 7: Class Diagram

5. Glossary

Cross-border money transfers – are transactions where the payee and the transaction recipient are based in separate countries. The transactions can be between individuals, companies or banking institutions who are looking to transfer funds across territories.

SWIFT - Society for Worldwide Interbank Financial Telecommunications.

Blocks – a collection of data containing multiple transactions over a given period of time on the blockchain network.

Chain – the cryptographic link which keeps blocks together using a 'hash' function.

Blockchain – a blockchain is a secure, global, immutable public ledger that records every transaction, chronologically, on the network.

DLT: Distributed Ledger Technology is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, or institutions. Unlike with a distributed database, there is no central administrator.

Permissionless blockchain: anyone may join the network and read from the state stored, and write to the blockchain.

Public permissioned blockchain: a limited set of participants may write to the blockchain. Anyone may join the network and read the state.

Private permissioned blockchain: a limited set of participants may join the network, and write a new state. Only this set can read the state

Peer-to-peer Network – every node of the network is a client as well as server, holding identical copies of the application state

Cryptography – use of public key cryptography and cryptographies hash functions: essential for transparency and privacy.

Bitcoin – a Peer to Peer Electronic Cash System that would enable people to send it directly without it going in a financial institution. Blockchain is the technology that runs Bitcoin.

Coin: a cryptocurrency 'coin' is seen as a means of payment. The purpose of a coin is to act like money – to allow transactions of products and services to occur.

Nonce: is an abbreviation for "number only used once," which is a number added to a hashed—or encrypted—block in a blockchain that, when rehashed, meets the difficulty level restrictions. The nonce is the number that blockchain miners are solving for.

Decentralized: a system where no individual has ownership of the system and there is no central point of control. In the case of decentralized blockchains, the system is spread over the entire network of users. This makes it almost impossible to hack, tamper with or destroy.

Cryptocurrencies – the digital currencies that are secured using cryptography and built using blockchain technology.

DApps: DApps are 'decentralized applications'. They are applications, like Bitcoin or Ethereum, that are built on a decentralized blockchain.

Hash: the result of applying an algorithmic function to data in order to convert them into a random string of numbers and letters. This acts as a digital fingerprint of that data, allowing it to be locked in place within the blockchain.

Digital Signature: a digital code generated by public key encryption that is attached to an electronically transmitted document to verify its contents and the sender's identity

Public Address: the cryptographic hash of a public key. They act as email addresses that can be published anywhere, unlike private keys.

Private Key: a string of data that allows you to access the tokens in a specific wallet. They act as passwords that are kept hidden from anyone but the owner of the address.

Proof of Work: a consensus distribution algorithm that requires an active role in mining data blocks, often consuming resources, such as electricity. The more 'work' you do or the more computational power you provide; the more coins you are rewarded with.

Node: a copy of the ledger operated by a participant of the blockchain.

Miners: validate new transactions and record them on the global ledger (blockchain). Compete to solve a difficult mathematical problem based on a cryptographic hash algorithm.

Smart Contract-are simple programs based on certain condition to transfer money.

Consensus: all nodes in the Blockchain create consensus, agree the validity of Blocks.

6. References

1. Blockchain technology and its effects on business models of global payment providers, Author: German Dolinski University of Twente
2. Blockchain Payment Systems, Elwood Research Series 09 December 2019
3. Blockchain Technology, Beyond Bitcoin, Michael Crosby, Google Nachiappan, Yahoo Pradhan Pattanayak, Yahoo Sanjeev Verma,
   Samsung Research America Vignesh Kalyanaraman, Fairchild Semiconductor
4. Blockchain for Global Payments, Oracle
5. Cross-Border Money Transfer Using Blockchain – Enabled by Big Data
6. Software Engineering Research for Blockchain Based Systems, Dr Mark Staples, Research Team Leader
7. Application Analysis on Blockchain Technology in Cross-border Payment
8. From Distributed Consensus Algorithm to the Blockchain Consensus Mechanism
9. Streamlining Cross Border Payment Processing with Blockchain, TATA Consultancy
10. Cryptography just for Beginners, tutorialspoint, simply easy learning
11. Virtual currency schemes, European Bank
12. Cryptographic Hash Functions, http://web.cse.ohio-state.edu/~lai.1/5351/6.Hash.pdf