


People's Democratic Republic of Algeria

Ministry of High Education and Scientific Research

University of Akli Mohand Oulhadj Bouira

Faculty of Science and Applied Science

Computer Science department

Master 2 Thesis

In Computer science

Speciality: GSI

Theme

E-Payment System Based On Blockchain Tecknology

Supervisor by :

- DJELLABI Brahim

Realised by:

- ABBAS fateh
- LARACHI sofiane

2020/2021

Thanks

First of all, we thank God Almighty for giving us the courage and patience to accomplish this humble work. We would like to express our sincere gratitude to all those who directly or indirectly contributed to the completion of this thesis. A special and sincere thanks to our parents for their efforts. We especially thank our promoter **Mr. DJELLABI Brahim** who supervised his wise advice, support and great courage during the development of this work as well as the members of the committee supervising the evaluation of this project, and we also thank our friends who supported us during this thesis.

Dedication

I dedicate this humble work after I thank God for all the blessings, to my mother and father who encouraged me and gave me all the support and who guided me in this life to achieve success, and to all my close friends who supported me in the university environment, not forgetting the road friend **Abbas Fateh**, I thank all my family members for being Support me, thank you very much.

Larachi Sofiane.

Dedication

I dedicate this humble work after I thank God for all the blessings, to my mother and father who encouraged me and gave me all the support and who guided me in this life to achieve success, and to all my close friends who supported me in the university environment, not forgetting the road friend **Larachi Sofiane**, I thank all my family members for being Support me, thank you very much.

Abbas Fateh.

Contents

List of Figures

List of Tables

List of abbreviations

EPS	Electronic Payment System
ATM	Automated Teller Machine
EBS	Extranet Banking Services
MP	Mobile Banking
EFT	Electronic Funds Transfer
NEFT	National Electronic Fund Transfer
RTGS	Real Time Gross Settlement
IPMS	Immediate Mobile Payment Service
ACH	Automated Clearing House
IBAN	International Bank Account Number
ATI	Algeria Telecom Interbancaire
P2P	Peer To Peer
POW	Proof Of Work
POS	Proof of Stake
BFT	Byzantine Fault Tolerance
CFT	Consensus Fault Tolerance
POA	Proof Of Activity
POB	Proof Of Burn

General introduction

General Introductiont:

The year witnessed the development of payment systems as people used to barter among themselves without an intermediary, and these transactions were not accurate, as gold, silver and other metals were used until the emergence of money that derives its strength from the law, and with the development of technology, electronic payment emerged, which is the transfer of monetary value from Motivation to the recipient through certain mechanisms.

Every year, electronic payment systems develop into a new stage, due to the rapid growth of electronic commerce in the past decade, electronic payment has become very important, and electronic payment systems must provide people with the necessary infrastructure to facilitate payments. EPS today has become an integral part of increasing trade and business, but the problem remains one of trust, you have to put your money in a bank and you have to trust it.

But with this development in the field of electronic payment, it contains many problems, so we will develop an application related to Blockchain technology and try to solve some of these problems based on the study of the electronic payment system based on Blockchain technology and Hyperleger fabric platform, and the goal of our work is to eliminate centralization And the third party and give the user security and transparency in the transfer of his money.

Expected objectives:

We will try to create an application for the blockchain-based electronic payment system:
- No third party interference in transactions between users..
- Transparency of all transactions and can be viewed at any time.
-A decentralized application that uses blockchain technology at the end.
-Achieving security and making anyone feel safe when transferring and receiving their money.

Organization of the report:

Our report is organized in 3 chapters:

First chapter(Electronic payment system):

In this chapter we'll bring a general idea about this subject:
-Some definitions(payment and electronic payment).
- history of payment system.
-Types of electronic payment.
-Electronic Banking.
- E-Payment in Algeria
- Limitations of electronic payment systems.

Chapter 2: Alternative to centralized system:

In this chapter, we will discuss solving the problems mentioned in Chapter One, and we have introduced Blockchain as a solution:
-Centralized Systems
-Decentralized systems.
-Distributed system
-Peer-to-peer network
- BlockChain technology

-Some applications of blockchain

Chapter 3: Implementation and realization

In this chapter , we chose to work on the Hyperlager Fabric platform and create a blockchain-based application :

-The goal of the application.

-Realization.

- Hyperledger Fabric.

-System design.

-Application Scenario.

-Architecture of the application.

-application tes

Chapter 1

Electronic payment system

1.1 Introduction:

In this chapter and as an introduction to our research, we reviewed the concept of the electronic payment system and the methods used in electronic payment and compared it to the old payment system. We also talked about the services provided by banks in the field of electronic payment, then we talked about electronic payment in Algeria, and at the conclusion of this chapter we touched on the problems of the electronic payment system that cause embarrassment and a great obstacle to financial flow, most notably that this system is a central system that depends on a single authority.

1.2 Payment systems : historical evolution

The world witnessed a development in payment operations, as people used to deal with the exchange of goods among themselves, and this is called barter without any intermediary intervention, but due to the difficulty and inaccuracy of these transactions, as well as the limitations of this system, compulsory paper money appeared that derives its strength from the law, and with the developments that are not Advances in information technology, electronic payment methods have emerged, which represent an image of traditional payment methods that exist in various forms that correspond to the nature of transactions.[1]

1.3 Definition of payment and payment system

Payment is the transfer of monetary value. Thus, a payment is a transfer of money from the payer towards the beneficiary as a result of the payer benefiting from a good or service. The payment system consists of a set of banking tools and procedures and money transfer systems between banks that guarantee the circulation of funds and in this sense the payment system consists of three main processes

* **Payment Instruments:** The means by which the payer grants a bank authorization to transfer funds
* **Processing (clearing houses):** which includes payment instructions that are exchanged between the concerned banks (and accounts)
* **Settlement method :** for the payer's bank to compensate the payee's bank.[2]

1.3.1 Subscribers to the payment system

The propulsion system consists of the parts shown in **Figure 1.1**

Banks : Banks are a mandatory intermediary between users and payment systems because they hold a license to receive deposits and make payments that are subject to regulations

Settlement agent : The settlement agent manages the settlement accounts of the direct members and transfers the amounts between them to achieve the final status (a third party that assists in the conclusion of a deal between the buyer and seller).

Central bank: Central banks generally act as a settlement agent; However, central banks primarily aim to promote the smooth functioning of payment systems and protect the financial system..

Money market : Money market is an essential component of payment systems although it is not a part of it entirely. An efficient and liquid daily market is also essential for the smooth operation of the payment system as it enables commercial banks to finance.[2]

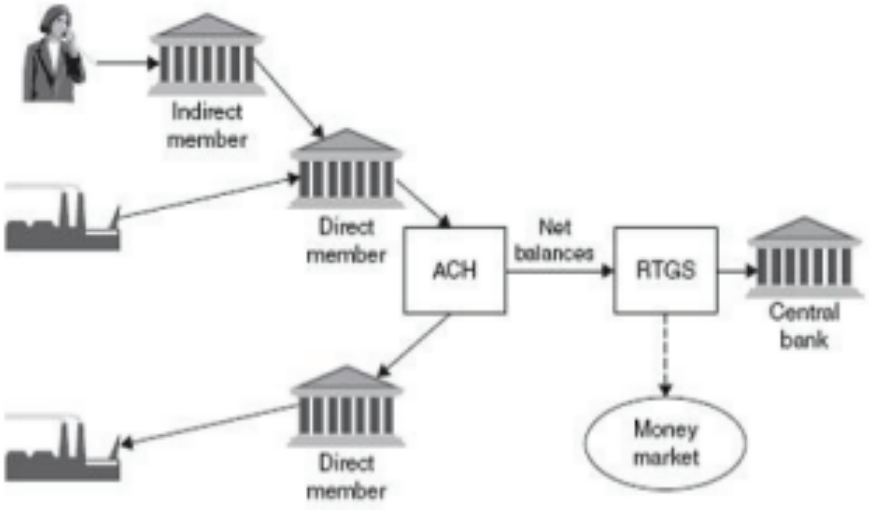

Figure 1.1: Payment chain between subscribers [2]

1.3.2 Payment instruments:an overview

Through **figure 1.2** shown below, payment is made in two ways: in cash or cash alternatives.

Types of money: Cash, Scriptural money, E-money

- **Cach:** Banknotes or Coins.
- **Scriptural money:** deposits with central banks or Sight deps with commercial banks.
- **E-money:** Network money or Card base money
- **Money substitutes:** Cheque, Bill of exchange, Credit card.

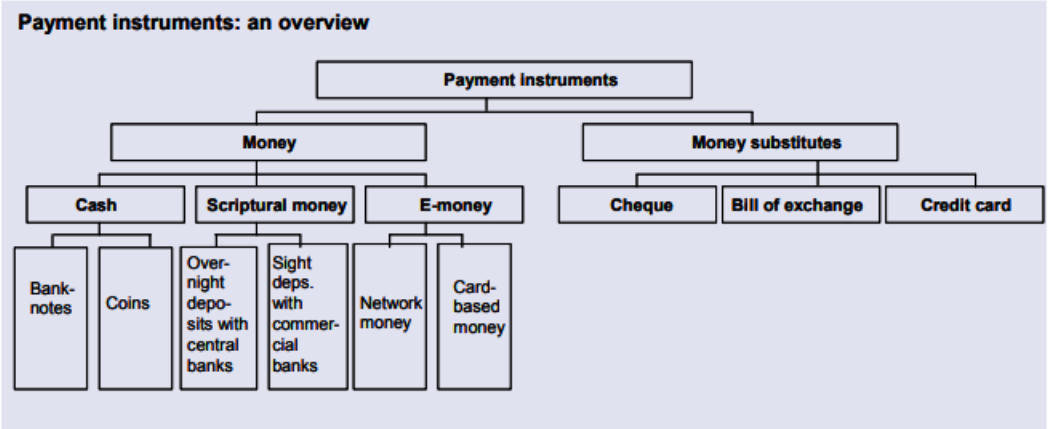

Figure 1.2: Various payment methods [3]

1.4 E-Payment System

1.4.1 Definition of electronic payments

Definition

The use of technology in modern banking services that we know as electronic payment systems makes banking performance more complete, and various activities can be carried out quickly and accurately while affecting productivity, Electronic payments are one of the payment mechanisms that use electronic means that do not include cash, or in other words, electronic transfer is the transfer of the value paid from the payer to the recipient through an electronic payment mechanism [4].

1.4.2 Types of electronic payment

With the increasing complexities of e-commerce transactions, many different electronic payment systems have emerged in the past few years," Murthy" (2002) explained six types of electronic payment systems: PC banking, credit cards, checks Electronic, Partial Payment, Smart Cards, Electronic Cash

"Whinston" (1996) also identified three types of electronic payment systems: electronic payment systems based on digital tokens, electronic payment systems based on smart card, and electronic payment systems based on credit.

According to the above classifications, electronic payment system can be broadly divided into four general types ("Anderson", 1998)

* Credit card payment system
* Electronic check system
* Electronic cash system
* Smart card-based electronic payment system [5]

Online credit card payment system

This type aims to extend the functionality of existing credit cards to be used as payment tools for online shopping. This payment system has been widely accepted by consumers and merchants all over the world and can be said to be the most popular payment method especially in the retail markets.
This payment system also has many advantages that were not available through traditional payment methods, the most important of which are: privacy, integrity, compatibility, good transaction efficiency, acceptability, convenience, mobility, low financial risk, and anonymity. Online credit card payments are also considered by consumers and sellers as a potential, time-tested alternative. But this payment system has raised many problems for consumers and merchants. Online credit card payment also seeks to address many of the limitations of online business credit card payments including non-authentication, refusal of fees, and credit card fraud. [5]

The basic process of the online credit card payment system: It is a very simple process, if consumers want to purchase a product or service they simply send their credit card details to the respective service provider and the credit card institution will handle the payments. **Figure 1.3** shows the credit card payment method

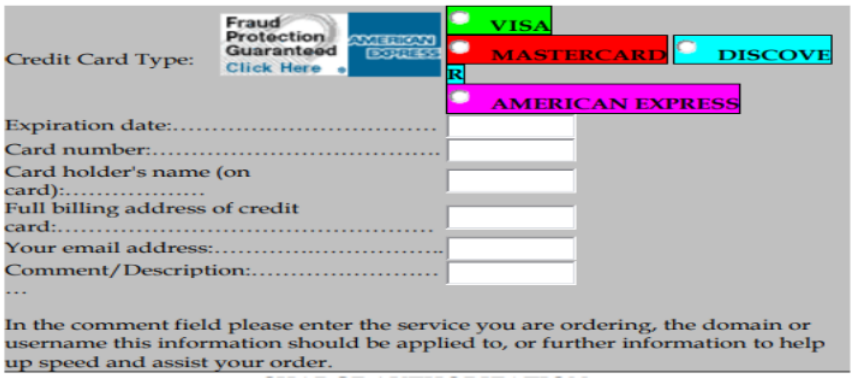

Figure 1.3: Credit Card Payment Form [5]

Electronic Cheque Payment System

Electronic checks are equivalent to paper checks, the funds are transferred over a computer network at the time of the transaction. The portable electronic check book is a combination of secure hardware and specialized software and interacts with the issuing bank's financial management and transaction processing software[5].

Payment process using electronic checks: The payer writes electronic checks on a computer, signs them in an encrypted manner, and emails them over the Internet. The payer also signs them using the secure device, and includes a Certificate of Authenticity signed by the issuing bank. The beneficiary receives the electronic check, verifies the signature of the payer on the electronic check, certifies it and writes down the deposit slip and signs it. The certified check is then emailed to the payee's bank for deposit. Payee bank staff checks the signatures of the payer and payee, credits the deposit, then scans the certified electronic check and clears it by sending it to the payer's bank. The payer's bank verifies the signature of the payer again and the amount in the electronic check is debited from the payer's account [5]

Electronic Cash Payment System

Electronic cash (e-cash) Electronic money is an electronic or digital form of storing and exchanging value with limited convertibility to other forms of value that require intermediaries for transfer. Electronic money offers features such as monetary value, storage, non-refundability and security. All these characteristics make it a more attractive online payment system. In addition, this payment system offers many advantages such as

strength, privacy, good acceptance, low transaction cost, convenience and good anonymity. But this payment system also has many limitations such as poor movement, poor transaction efficiency and high financial risk, as only people are responsible for loss or theft

Structure of electronic cash: The structure of electronic cash can be defined as a series of bits representing certain values such as reference number and digital signature, which can be used for security purposes to prevent fraud and criminal use (Wright, 2002). But the structure suggested by Wright (2002) needs some extension to make electronic money more secure. Therefore, the current model adds a digital watermark to the structure of electronic cash to further protect it from illegal copying and counterfeiting activities [5], and the model has modified the reference number structure to support traceability as shown in this **figure 1.4**

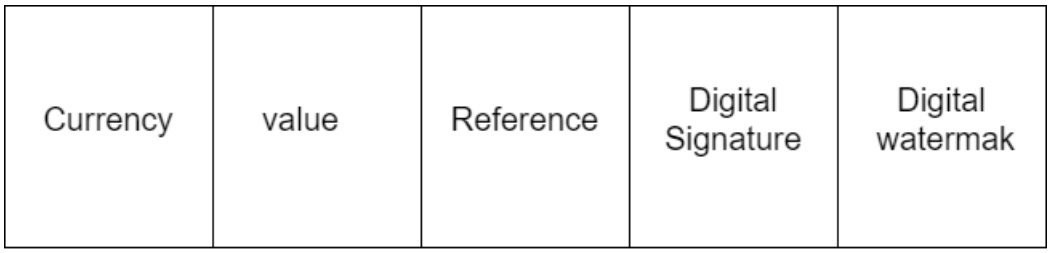

Figure 1.4: E-Cash Structure [5]

Smart Cards based Electronic Payment System

Smart cards are essentially credit card-sized plastic cards with memory chips and in some cases with microprocessors built into them to act as storage devices for much larger information than credit cards with the ability to process internal transactions. The figure Figure1.5 shows the structure of the smart card

Figure 1.5: Smart Card Image [5]

This card spread mostly in Europe and Asian countries. Due to its great flexibility, it has been used for a wide variety of functions such as highway toll payments, prepaid phone cards, and stored value debit cards. However, with the recent emergence of e-commerce, these devices are increasingly seen as a share that has a much greater level of security than credit cards.[5]

1.4.3 Cryptocurrencies

Cryptocurrencies are virtual digital currencies as well as a digital asset designed to serve as a medium of exchange in which records of ownership of individual currencies are stored in a ledger located in the form of a database using strong encryption to secure transaction records. There is no currency in physical form (such as paper money) and it is not usually issued by a central authority. Cryptocurrencies typically use decentralized control rather than central digital currency and central bank systems.[6]
Examples of cryptocurrencies: Bitcoin, Ethereum.

1.4.4 The difference between electronic payment and traditional payment

Online payment is based on an open platform while legacy payment runs in a relatively closed system, cash payment requires the buyer to withdraw from his bank account, transfer cash to seller, and seller deposit payments into his account, which is a cumbersome process unlike electronic payment system in which the transfer of Electronic money [7]

PARTICULARS	TRADITIONAL PAYMENT	E-PAYMENT
Usage	Use Traditional Medium to communicate	Use advance technology to communicate
Circulation	Traditional payment is realized through physical circulation such as cash circulation, bill transfer and bank exchange.	E-payment introduces digital circulation to realize information transmission, so all means of e-payment are digitalized
Requirement	Uses traditional medium to communicate between parties	Requirement network and otherrelated software to work
Intervention	Needs human intervention to settle these processes	Uses advance technology to handle all the transaction process that requires money engagement such as money transfe

Table 1.1: The difference between electronic payment and traditional payment[7]

1.5 Electronic Banking

1.5.1 Definition

Commercial or electronic banking can be defined as the use of advanced communication networks to transfer funds in the banking system

Electronic banking includes electronic products and services in developing markets, including phone banks, credit cards, ATMs, direct deposits, electronic bill payments, rechargeable cards (smart cards) and products whose value is stored on the Internet.

In general, electronic banking refers to providing employees with facilities in order to improve their pace and efficiency in providing banking services in the branch, in addition to transactions between branches and between banks around the world, and providing hardware and software facilities to customers through which they can carry out the required banking operations at any time of the day .(24 hours) through secure and reliable communication channels. In other words[8]

1.5.2 The different forms of the electronic banking system

Automated teller machines (ATM)

ATM : An electronic terminal that allows customers to access banking services at almost any time. To withdraw cash, deposit or transfer funds between accounts, the consumer needs an ATM card and a personal identification number (PIN). [9]

Point of Sale (POS)

POS : This system allows consumers to pay for their retail purchases with a check card, which is a new name for the debit card. This card looks like a credit card, but with a big difference. The purchase funds are immediately transferred from the debit card holder's account to the store's account . [9]

Online / Extranet Banking Services

EBS : it is an electronic banking system that depends on web technology, whereby customers of the bank can conduct their commercial transactions with the bank through their personal computers. (The customer visits the electronic page of his bank and registers in it depending on the card that you get from The same bank can then do what the customer wants, for example, he can pay his bills, view his account, or transfer money from his account to another account ... etc.) [9]

Mobile Banking

Mobile banking : is the service provided by the bank to its customers to conduct financial transactions through mobile devices such as smartphones or tablets. It can be used at any time. This is usually done through banking apps. The customer can pay bills, transfer funds, inquire about the balance and check the mini-statement.[10]

Types of mobile payment

* **Mobile Payment (MP) :**It is in-store payment by consumers using applications installed on their devices such as mobile phones, from a technical point of view, applications installed on consumer devices must be connected to the retailer's point of sale (POS system) to make payments.[11]

* **A QR code :**

  It is a two-dimensional code that can be scanned and has a function similar to the traditional barcode that can be found in many products. A QR code is more efficient as it can store more information and is more flexible in terms of storage.

  The exchange of money value from cash to digital payment has evolved at full speed lately, especially using mobile phones for payment purposes. Mobile payments using QR code technology are among the most popular in the mobile payment market.[11]

1.5.3 Electronic funds transfer (EFT)

Definition OF EFT

EFT : Electronic Funds Transfer is a system that helps an individual to pay anywhere and anytime to another individual. The electronic transfer system is used on behalf of checks and money orders to transfer funds between bank accounts located in the different centers. The two most common technologies used in EFT are NEFT and RTGS.[12]

The different types of money transfer methods

* **National Electronic Fund Transfer :** National Electronic Funds Transfer (NEFT): It is a payment system that facilitates the transfer of funds from one person to another. Hereby, individuals and corporations can transfer funds electronically from any bank branch to any corporation, sole proprietorship or corporation that has an account with any other bank branch in the country participating in the Program.[13]

* **Real Time Gross Settlement(RTGS) :** It is the fastest possible money transfer system through the banking channel, where settlements are done in real time without any waiting time. "Real time" means that the transaction is not subject to any waiting lines, and is settled once it has been processed. "Group settlement" means that the money transfer settlement instructions occur individually or on an individual basis without netting another transaction, "Settlement" means that once the Transactions are processed, they are final and irrevocable. RTGS is primarily designed for high-value transactions [13]

  RTGS FUNCTIONING: Figure 5 illustrates the functional architecture of RTGS :

- Bi bank submits a payment order to RTGS.
- The order is executedor queued.
- The payment is transferred to the recipient's Bj bank accoun
- RTGS informs the recipient's bank about the transfer

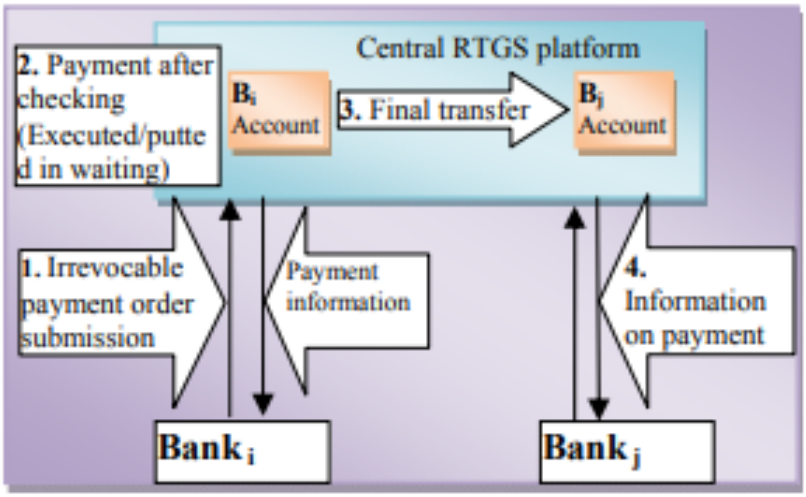

Figure 1.6: RTGS system architecture [16]

IMPS-Immediate payment service :IMPS is a mobile payment service where customers use mobile phones as a means of transferring money. IMPS is an easy and instant way to transfer funds instantly from one account to another, within the same bank or accounts across other banks. [13]

Automated Clearing House (ACH) : ACH is a system that is implemented for retail payments and entire interbank transfers in huge volumes automatically. Transactions in this system are settled in batches at a specified time (usually at 24 hours). Member banks can issue direct credit or direct debit transactions by sending a batch file containing various transaction orders to the corresponding bank. In this system, the debit or credit accounts of customers are transferred on the basis of the International Bank Account Number (IBAN) [13]

1.5.4 Advantages of E-Banking

- Electronic banking provides its customers with more convenience than can be obtained from traditional banks: this means that the customer does not care about

the timing or hours of the bank's work.

- Electronic banking services reduce the workload of banks and enable banks to improve services for customers, reduce the number of workers in banks so that traditional banking work requires a number of workers to meet the customer's requests, unlike electronic banking work, where electronic banking services help banks reduce operating costs because they do not need to Human operators to keep banking services working, all this can be done through electronic media

- Online banking is environmentally friendly, electronic transfers require no paper, reduce vehicle traffic and are virtually pollution-free. It also eliminates the need for office buildings and equipment. [14]

1.5.5 Disadvantages of E-Banking

- Understanding the use of online banking can be difficult for beginners (lower academic level). Although there are some sites that give a demo on how to access online accounts.

- The customer may not be able to access the online banking services if he has no or slow internet connection

- TTransaction security is a big issue, your account information may be hacked by unauthorized people online.

- Another problem that customers may encounter is that it is sometimes difficult for them to notice whether their transactions have been successful or not. This may be due to a slow connection, or the bank server is down. [14]

1.6 E-Payment in Algeria

1.6.1 The use of electronic payment systems in the Algerian banking system

In light of the development of the banking system around the world, Algeria found itself obligated to modernize its banking system. Algeria began implementing the modern-

ization of payment methods starting in 2005 by launching the bank card payment and withdrawal project. Algeria has implemented several projects, including the following:

Instant gross settlement system

On May 15, 2006, the Bank of Algeria, in cooperation with the Ministry of Finance, introduced the system, also known as the immediate payment system for large amounts, which is a system for interbank payment orders using bank or postal transfers for large amounts.[15]

Electronic Payment Clearing System

The electronic clearing system in Algeria is known as ATI (Algeria Telecom Interbancaire), the system came into force on May 15, 2006, allowing the exchange of all payment methods associated with public payments (cheques, commercial papers and card operations).[15]

Establishment and operation of automated cash network and automatic relations between commercial banks

The This national project is compatible with the international automated cash systems. The most important networks and companies operating ATMs in Algeria is SATIM.

* **Interbank ATM**: The Algerian Company for Banks and Electronic Banking Services (SATIM) is among the companies that mainly guarantee the development and operation of the BIBNIC system based on the use of the financial and banking information network and the allocation of bank cards in Algeria.
  In order to manage the interbank ATM network, the banks (BDL, CNEP, CPA, CNMA, ALBARAKA, BADR, BEA) established SATIM in 1995. [15]

* **Operation of the card system in the Algerian banking system**

  - **Card concept:** A bank card is an interbank CIB card, containing a microchip that provides all stages of financial payments. Since the cards were issued, three private banks have been registered: Societe GeneraleAlgeria, BNP Paribas, and Arab Bank AGB to BNP[15]

- **Types of cards used in the ATM system**

  The card inter-bank CIB: It is a card to pay and withdraw at the same time. This card is used by many banks and other financial institutions through its multiple bank code.

  Gold card: It is also provided to customers according to the criteria set by the bank and this card provides additional functions for withdrawal and payment that are more important than the first.[15]

1.7 Limitations of electronic payment systems

There are several disadvantages in electronic payment that we can identify through the following points:

1.7.1 Limitations of electronic payment systems: in general

- When a customer's card is stolen, anyone can exploit it.
- The emergence of electronic piracy, which is one of the most dangerous types of electronic theft, through which systems for electronic payment and account theft are breached.
- It is not possible to benefit from the electronic payment system and its means in the absence of the Internet or electronic devices.
- Anyone who knows the secret encryption key can create digital signatures
- The name of the buyer can be associated with each payment, eliminating the anonymity of cash.

1.7.2 Double spending

This is a potential error in the context of digital money management, which is the ability to spend digital money repeatedly, as shown in Figure 1.7 that one person sends an amount to two different people at the same time and does not have enough money

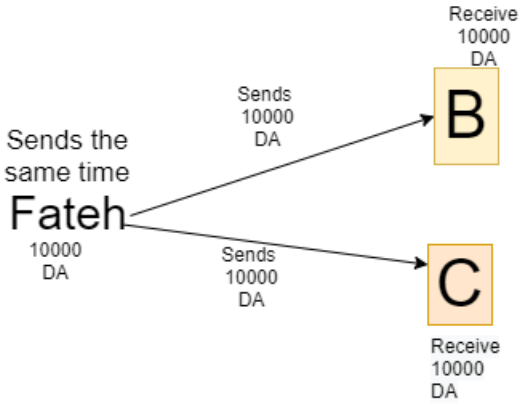

Figure 1.7: double spending

1.7.3 Central: the central bank

- The bank is the one that controls all transactions and your money, and you have to trust it, but if the bank is not guaranteed, then your money is not guaranteed.
- The Central Bank is responsible for all transfers in the event of a problem within the Central Bank (malfunction), which results in a malfunction and delay in collecting financial transactions.The **figure 1.8** shows the location and role of the central bank in financial transactions

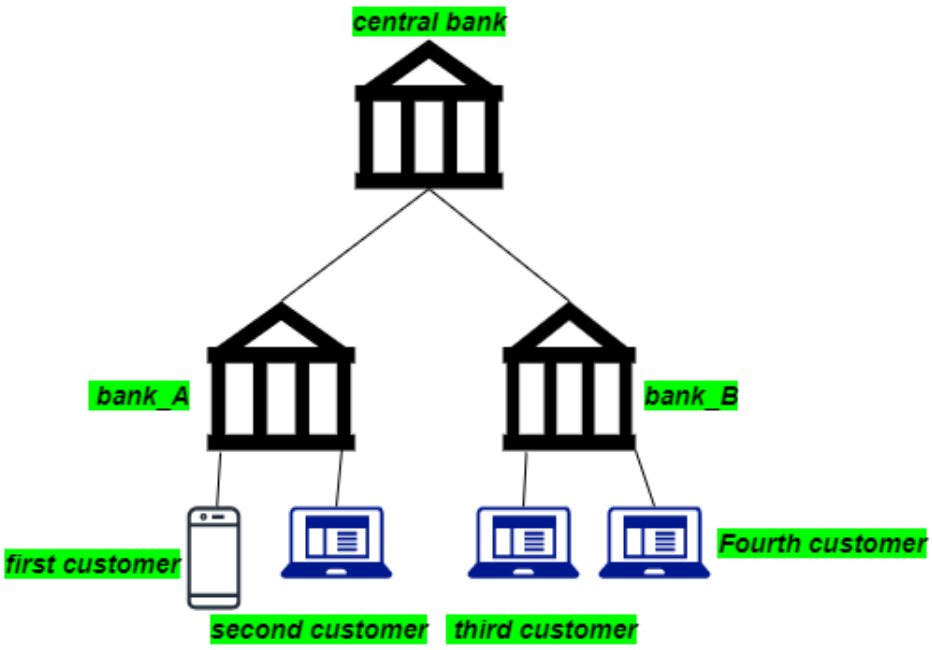

Figure 1.8: The central bank's mediation in financial transactions

1.8 Conclusion

this chapter, we mentioned the most important details about the importance of electronic payment, its types and the extent of its use, and compared it to traditional payment. We also talked about the most important and best electronic services that banks provide to their customers, and in the end we raised several problems about the electronic payment system, the most important of which is the single authority (the central bank), and to address this we use the blockchain technology that we will talk about in the second chapter.

Chapter 2

Decentralization, Distributed systems P2P Network And Blockchain Technology

2.1 Introduction

In the previous chapter, we talked about electronic payment and the problems it suffers from, and the main problem is centralization and dependence on third parties, and we saw that blockchain technology solves many problems related to electronic payment. In this chapter, we will learn about blockchain technology, and we will also explain the various centralized, decentralized, distributed and peer-to-peer systems.

2.2 Centralized Systems

Centralization is the traditional IT systems (server-client) where there is a single authority that controls the system, and is solely responsible for all operations on the system. All users of the central system rely on a single source of service. The majority of online service providers including Google, Amazon, eBay, Apple App Store and others use this traditional model to provide services. [18]

From this we can say that it is centralization that takes all the power within their reach, and no other entity can play a role in decision-making, if the center ceases to function, the whole system ceases to function.

The **Figure 2.1** represents an example of a centralized system where we see that allclients are connected to one server

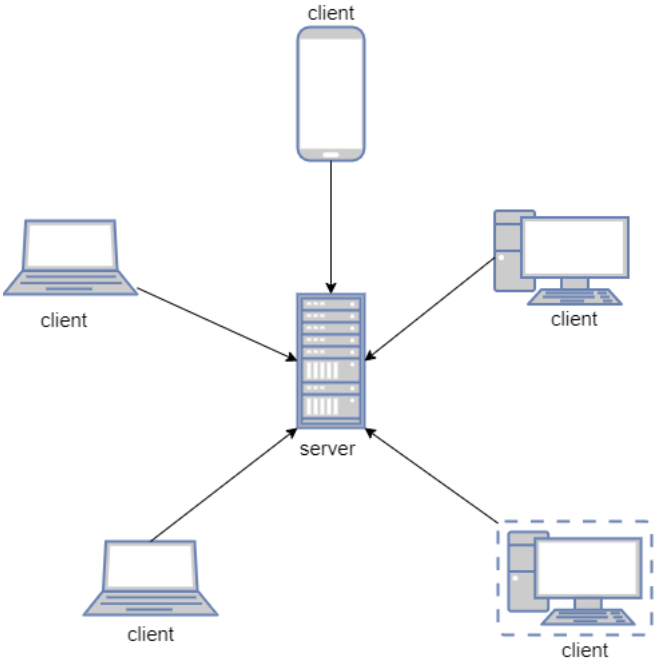

Figure 2.1: Centralized Systems

2.2.1 Advantages of centralization

- Consistent and efficient,
- Reasonable prices,
- Requires less infrastructure support.

2.2.2 Disadvantages of of centralization

- Users need to give up control of their data,
- Single point of failure,
- Limited scalability and bandwidth.

2.3 Decentralized systems

Decentralization is an administrative organization that is considered one of the most important principles of majority rule upon which democracy is based, and it is the opposite of the concept of centralization, which is the process of distributing jobs, powers, people or things away from a central location or authority. [26]
Decentralized benefits are increased efficiency, faster decision-making, better motivation, and reduced burden on top management.
In a decentralized system, there is no central entity to receive or respond to requests.
A decentralized architecture is more tolerant of failure, because when one central node fails, the other can continue to provide data to users.

2.3.1 Decentralization methods

There are two ways to achieve decentralization:

Decentralization through disintermediation

This way is to Disintermediation:*"Blockchain removes a central authority from the network, and thus transactions are decentralized. These transactions are verified and processed dependently on each node on the network. do you want or need This non-mediation? Given the application's use case, are there any major shortcomings of having a gatekeeper?"* Good reasons to prefer a blockchain-based database might include lower costs, faster workflows, automatic adjustments, or regulatory impacts. [27]

Decentralization through competition

In the method involving competition, different service providers compete with each other in order to be selected for the provision of services by the system. This paradigm does not achieve complete decentralization. However, to a certain degree, it ensures that an intermediary or service provider is not monopolizing the service. In the context of blockchain technology, a system can be envisioned in which smart contracts can choose an external data provider from a large number of providers based on their reputation,previous score, reviews, and quality of service. [29]

2.4 Distributed system

A distributed system is a set of autonomous computing elements that appear to its users as one coherent system. This concept indicates two distinct features of distributed systems : The first is that a distributed system is a set of computing elements each able to act independently of one another. The computing component can be either a node,a hardware device or a software process. The second feature is that users (whether they are people or apps) believe that they are dealing with a single system. This means that independent nodes need to cooperate in one way or another. How this collaboration is established is at the heart of distributed systems development. Note that we do not make any assumptions about the type of contract. In principle, even within a single system, it can range from high-performance mainframe computers to small devices in sensor networks. Likewise, we do not make any assumptions regarding the manner in which the nodes are interconnected.[17]

2.5 Peer-to-peer network

Basic definition of peer to peer. Which means there is no central console in the network, and all participants talk to each other directly. This feature allows data to be exchanged directly between peers without the intervention of a third party. [22]

A peer-to-peer system (often referred to by the acronym "P2P") is a network exchange model where each entity is a client and a server, as opposed to the client-server model. The terms peer, node, and user are generally used to designate the entities that make up such a system. A peer-to-peer system can be partially centralized or completely decentralized. It can be used, among other things, for file sharing, distributed computing, or communication. [24]

P2P can be defined in computer science. A peer-to-peer network consists of a group of devices that collectively store and share files. Each participant acts as an individual node. Each point is usually equal nodes, and in fintech, a peer-to-peer exchange of cryptocurrencies or digital assets over a distributed network. The P2P platform allows buyers and sellers to execute trades without the need for intermediaries. [23]

2.5.1 Peer-to-peer work

In a P2P network, users are responsible for maintaining a distributed network. As it is a peer-to-peer network, it does not require central authority or administrator. This means that each node needs to act as a client and server for the other nodes on the server. Each contract has a copy of the file. By doing this, each node acts as a server and needs to either download files from the other nodes or upload them to the other nodes. [25] This way of working is what sets it apart from any traditional client server setup. In a client server setup, there will always be a central server from which the client downloads files. [24] Nodes use hard drives to store shared files. When it comes to software, they use applications that can be used to share data or assist other devices in processing queries to find or download files. In any circumstance, peers need to act as the source for any given file.[24]

As we can see **Figure 2.2** The difference between a peer-to-peer network and a client-server network, where each peer in a peer-to-peer network can deal with another peer,and in a client-server network, all clients are connected to one server

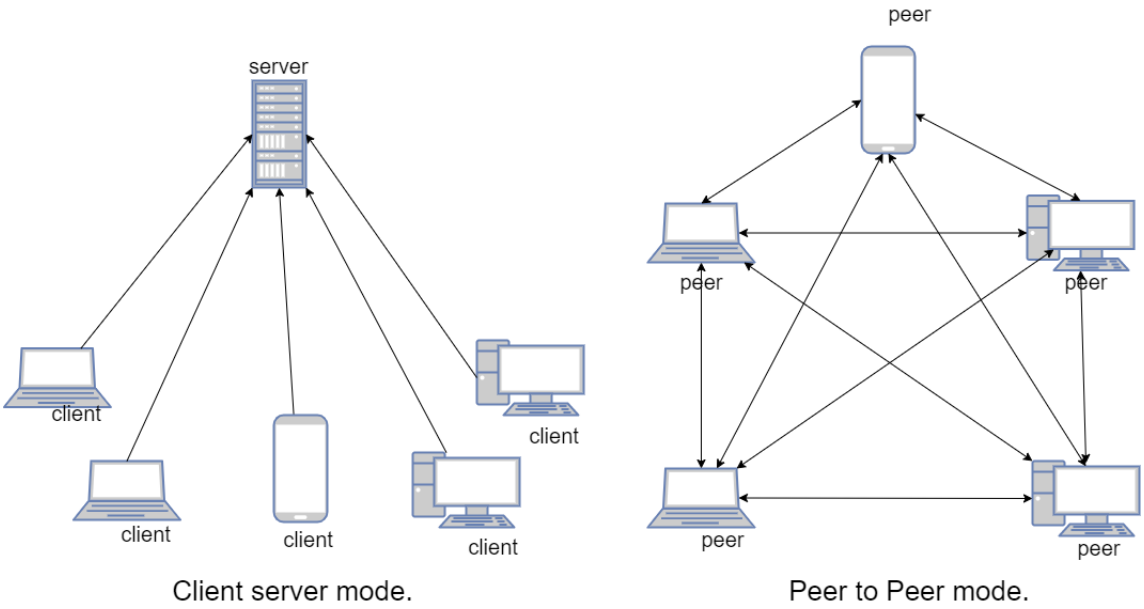

Figure 2.2: Client server vs P2P mode

2.6 The distributed ledger

The distributed ledger at the heart of the blockchain network is the distributed ledger that records all the transactions that take place on the network. The blockchain ledger is often described as decentralized because it is replicated across multiple network participants, each of whom collaborates on maintenance work. Distributed ledger is a broad term that describes shared databases ; Thus, technically all blockchains fall under the umbrella of shared databases or distributed ledgers. Although all blockchains are primarily distributed ledgers, all distributed ledgers are not necessarily the blockchain, and the primary difference between distributed ledger and blockchain is that the distributed ledger does not necessarily consist of blocks of transactions to maintain the growth of the ledger. Instead, the ledger is a special type of shared database that is made up of blocks of transactions. [29] As a summary, we can say the ledger is a list of all transactions executed in blochchain. The ledger is saved in the blockchain.

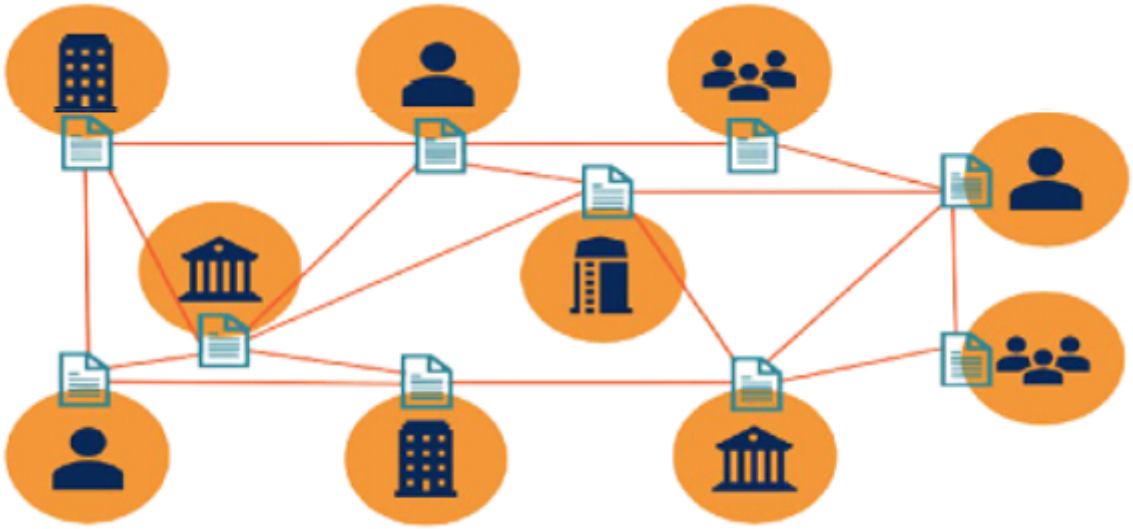

Figure 2.3: distributed ledger

2.7 BlockChain technology

Blockchain technology was originally considered just a term for organizing and sharing data.But now, blockchain technology has become the talk of the world, which is popularized by cryptocurrencies, and the most popular currency of Bitcoin.

2.7.1 History of blockchain

Stuart Haber and W. Scott Sternetta came up with the first idea of what many people know as a blockchain, in 1991. Their first work involved working on a chain of cryptographically secured blocks where no one could tamper with the timestamps of documents. In 1992, they updated their system to merge Merkle trees which improved efficiency and thus enabled more documents to be combined into a single block. However, in 2008, the history of Blockchain began to gain significance, thanks to the work of one person or group by the name of "Satoshi Nakamoto". The invention of the blockchain is attributed to a person or group of people under a name called "Satoshi Nakamoto", and this identity is considered anonymous. There are few people know his identity. [19] "Satoshi Nakamoto" also developed Bitcoin, authored Bitcoin White Paper, and created and published the original Bitcoin reference app. Blockchain works with a distributed database, which is more transparent and secure than the central databases that currently dominate the market. [20]

2.7.2 Definition of blockchain

A blockchain is a data structure that makes it possible to create a digital ledger of data and share it among a network of independent parties, and there are many different types of blockchain. [17]

Blockchain works with a distributed database, which is more transparent and secure than the central databases that currently dominate the market. Blockchain technology is faster and less expensive than traditional methods, for example if we want to transfer money from one country to another, it takes a week or more. But thanks to Blockchain technology we can use a phone or a computer, and we can transfer our money safely, easily and in a short time.

Blockchain is technologies that enable parties that do not have special trust in each other to exchange any type of digital data on a peer-to-peer basis with or without a number of third parties or intermediaries.
Examples of data include money, insurance policies, contracts, land titles, medical records, birth and marriage certificates, purchase and sale of goods and services, or any other type

of transaction or asset that can be translated into digital form. [21]

2.7.3 Type of Blockchain

Blockchain consists of different types: public and private blockchains and consortiums, and each of the above types works in different consensus ways, which we will discuss later.

Public blockchains

A large distributed networks that are run through a nativetoken such as Bitcoin and ethereum.In this kind of blockchain anyone canjoin the network, write and read.The data in a public blockchain are secured as itimpossible to modify once they have been validated on the blockchain.Everyone can check the transaction and verify it, and can also participate the process of getting consensus. [52]

The **figure 2.4** shows the public blockchain so that anyone can enter and deal with others without any permission

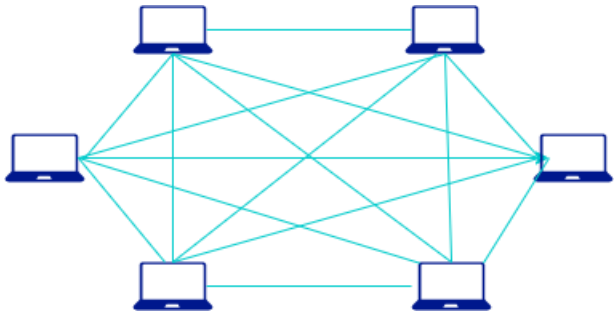

Figure 2.4: Public blockchains

Private blockchain

Permissions to read and write data on the blockchain are controlled by a single, "very reliable" organization with blockchain authority. In other words, the contract will be restricted.[53]

The **Figure 2.5** represents a private blockchain so that it can only be accessed with permission

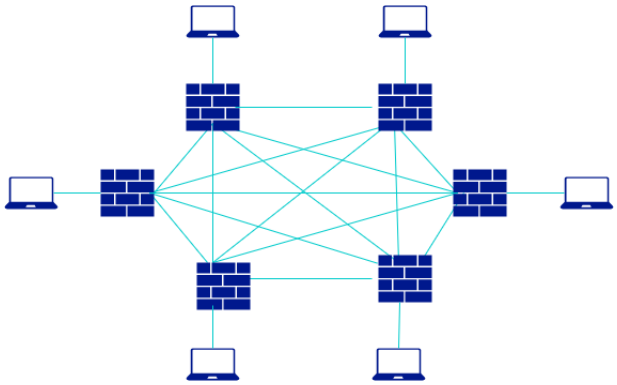

Figure 2.5: Private blockchain

Consortium blockchains

Consortium means the node that had authority can be choose in advance, usually has partnerships like business to business, the data in blockchain can be open or private, can be seen as Partly Decentralized. Like Hyperledger and R3CEV are both consortium blockchains.[53]

The **Figure 2.6** represents the Blockchain federation, from the image we see that there are nodes that can enter without permission and there is also a node that needs permission to enter the network

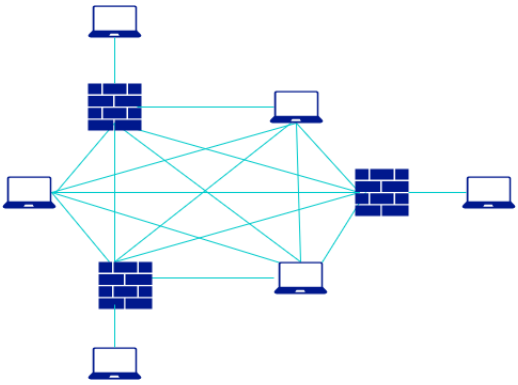

Figure 2.6: Consortium blockchains

Private blockchain VS Public blockchain

We have classified Blockchain systems into two categories : public and private. In the public blockchain, any node can participate in a peer-to-peer network, as the blockchain is completely decentralized. A node can leave the network if it so desires without any consent from the other nodes in the network. Bitcoin example.As for the private blockchain, the nodes need private access or permission without which they cannot obtain authentication from the network. Hyperledger is among the most popular private blockchains that only allow authorized members to join the network after authentication. [56]

2.7.4 Network

It's network composed of nodes . Each node contains a complete record of all transactions, these nodes have different locations all over the world.

2.7.5 The structure of blockchain

Blockchain comprises of blocks that contain lists of transactions that have been generated in the network. Transaction can be any information about the exchange of any type of data.

A block has a header and a body, Body of the block contains information regarding transactions. Header contains information that binds the block with other previous blocks, such as the hash of previous block and other information. [28]

Mainly in the block, it contains main data, a hash of past block, hash of current block, timestamp, and other data.

Every transaction is processed through encryption and after that it collects all transaction history and it stores it as blocks of data.

The blocks are then linked with the cryptog-raphy and protected from modification or forgery.Then the whole process creates a stable and immutable record of the transactions that occurred over the network. In addition, these log blocks are copied to every computer

participating in the network, so that everyone can access them. Meaning we can create a shared reality across untrusted entities. [29]

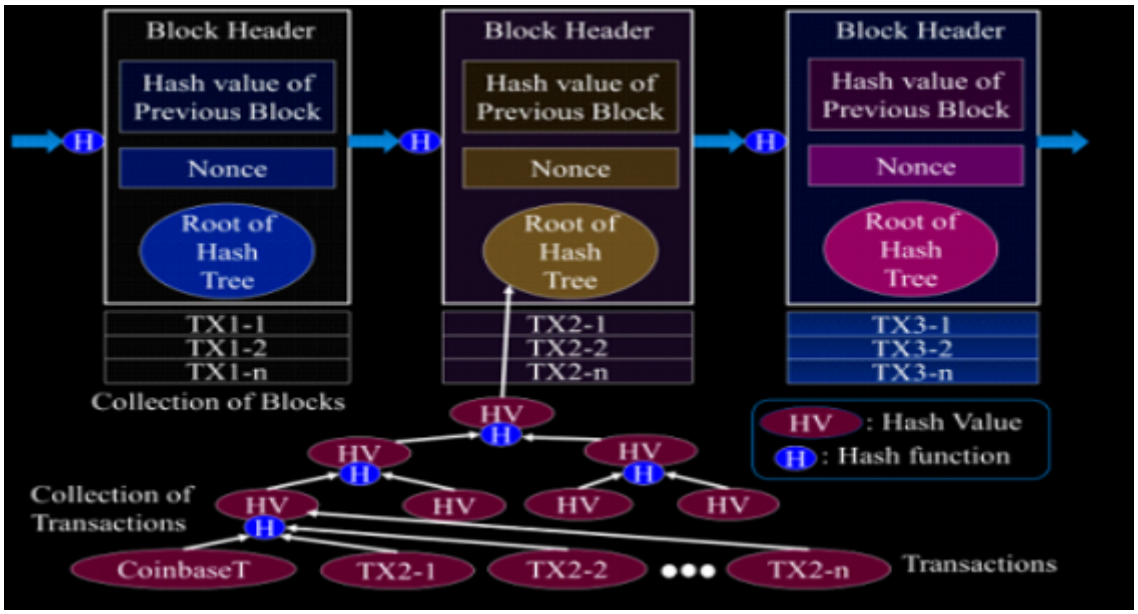

Figure 2.7: The structure of blockchain [29]

2.7.6 Core components of the blockchain system

The basic components of a blockchain system are. Node,Block,Chain,Consensus,Transaction As shown in the figure, the components of the exponential in the blockchain, we will explain them in detail

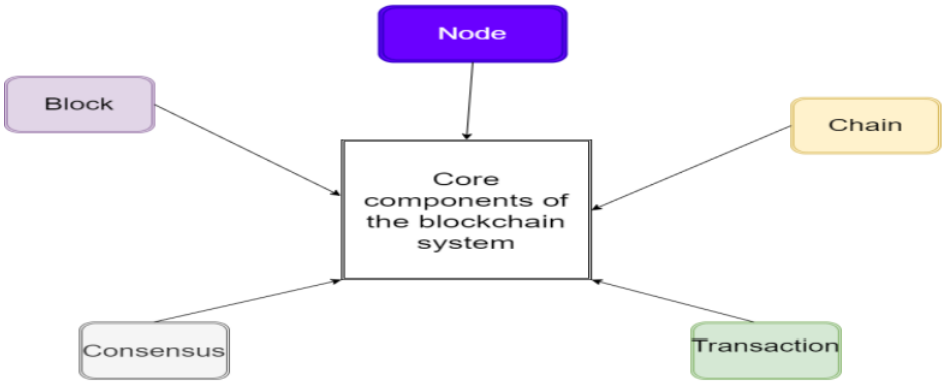

Figure 2.8: components of the blockchain

2.7.7 node

A node is a computing device which is part of the distributed network. Generally,each node has a copy of the blockchain and thus of the ledger, can have varying roles to issue, verify, receive, inform, etc. For all intents and purposes, a node can be a V, If two nodes participate in one transaction, it is called a node to a node (N2N) .[32]

A.Roles of nodes Nodes can be divided into consensus nodes and non-consensus nodes according to the different functions in permission chain. Consensus nodes participate in consensus process, generate blocks and broadcast blocks to non-consensus nodes.[33]

2.7.8 Block

Contains a list of transaction recorded into a ledger over a given period.The size, period, and triggering event blocks is different for every blockchain

A block consists of the block header and the block body as shown :

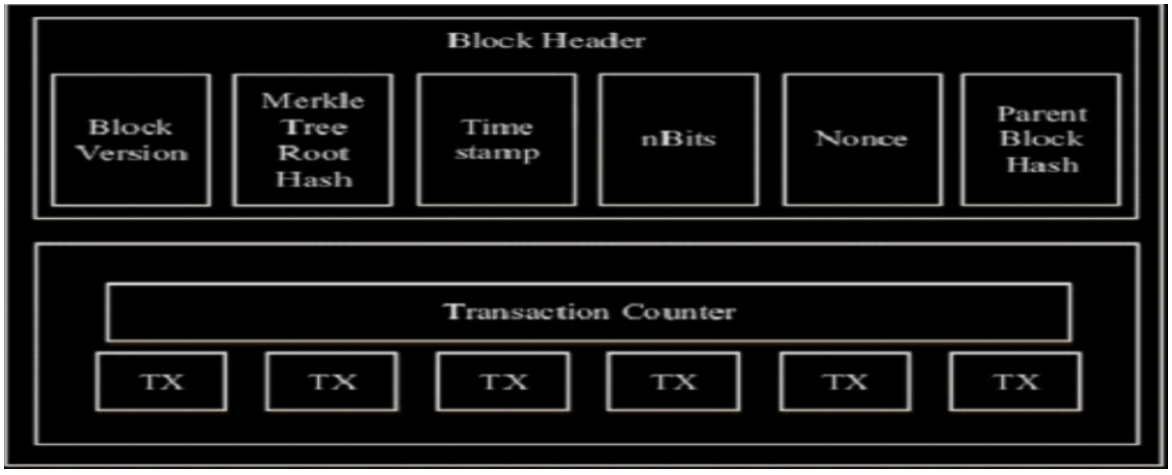

Figure 2.9: The structure of block [34]

- **Block header:**

  Block header stores the metadata about the block and body which stores all the information about the block. Metadata comprises of version of Block, MerkleTree Root Hash, Time Stamp, n Bits, Nonce, and Parent Block hash. Block Version indicates the validation rules to be followed in the network. MerkleTree Hash stores the hash value of all transactions in a block.

- **block body:**

  The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction.

2.7.9 Chain

The blocks are linked together by each block containing the hash summary of the header of the previous block, thus forming the blockchain. If a previously published mass is altered, it will have a different hash.This, in turn, will cause all subsequent blocks to also have different hashes since it includes the hash of the previous block. This makes it possible to easily detect and reject modified blocks.[38]

Represents Figure 2.9 Generic Chain of Blocks

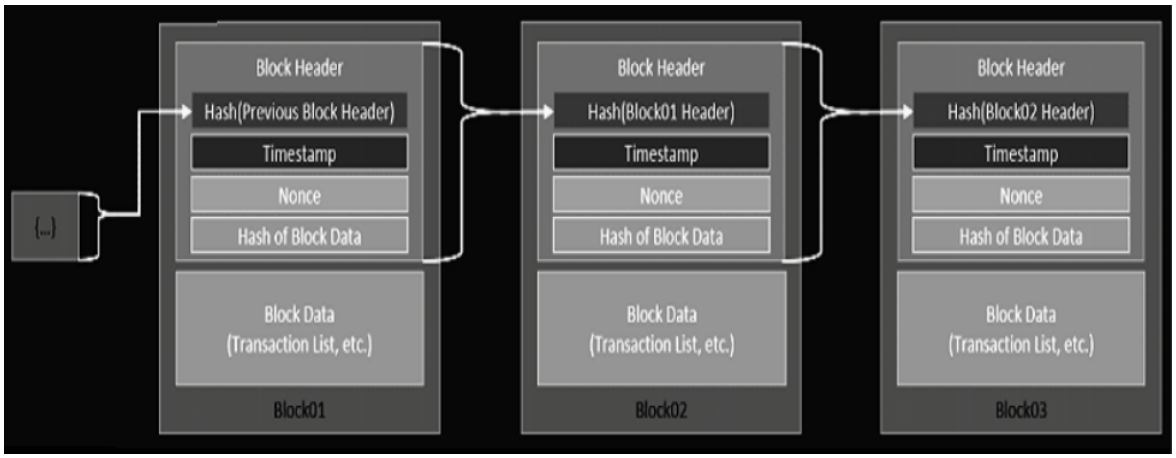

Figure 2.10: Generic Chain of Blocks[38]

2.7.10 Transactions

Transactions in the blockchain are data structures that store value transfer data between different addresses. In the case of cryptocurrencies, the value transferred through transactions is the amount of currency that the sender sends to the recipient. All transactions are publicly available and can be viewed using what is called a block explorer. BlockExplorer is already decrypting network transaction logs into a human-readable one.[39]

Verify the transaction

These rules include :

—The transaction must be correct ;

—The inputs or outputs of the transaction must not be empty or both ;

—The inputs or outputs of the transaction must not be empty or both ;

—The transaction must not already exist in one of the main blockchain blocks ;

—The sum of the output values must not exceed the sum of the input values ;

—If a person creates a block with an invalid transaction, that is, it violates one of the protocol rules, then the block also becomes invalid and therefore other participants in the chain network that contain such a block will not accept it.[39]

2.7.11 Consensus methods

Blockchain technology allows participants to read or update on the shared ledger (blockchain) as its state is collectively maintained by the network in a decentralized manner to maintain the state of the blockchain, often using a consensus mechanism that ensures integrity and consistency, and ensures an unambiguous common arrangement of transactions and blocks. In other words, consensus protocols preserve the sanctity of the data recorded on the blockchain and provide the building blocks that allow the blockchain platform to function properly in normal as well as hostile circumstances. [21]

The blockchain expects to have a large number of anonymous and untrusted participants because any node can join the network, and this requires consensus mechanisms to take into account the inherent slag.For example, Bitcoin solves this problem by designingand setting up a consensus protocol where all nodes are bound to prove that they are You spent a certain amount of energy. This protocol is known as Proof of Work (PoW).

Various technologies are used by different unauthorized blockchain platforms (for example, Bitcoin uses Proof of Work while Ethereum Metropolis uses a variant of Proof-of Stake).

In the authorized blockchain, the nodes are semi-trusted with only the participating members being the registered and authenticated members. The number of nodes is ex-

pected to be small, allowing one to use consensus mechanisms other than the program of work. Many aspects of current research in the field of Byzantine Fault Tolerance (BFT) in Distributed Systems are also applicable in the context of reaching consensus in licensed blockchains. Thus, current blockchain platforms (for xample, Hyperledger) have utilized a well-known Byzantine Practical Error Tolerance (PBFT) algorithm.[30]

The methods of consensus are divided into authorized and unauthorized methods, as shown in the **figure2.10**

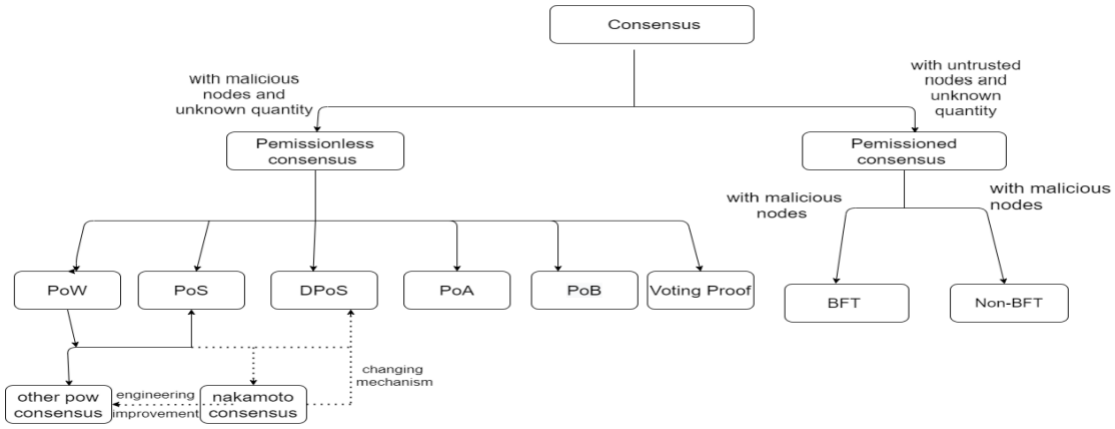

Figure 2.11: Consensus protocols in blockchain systems

Proof-of-Work (PoW)

As an aspect of scalability, the distributed validation system allows for the provision of validation checking for a large number of nodes while adding resilience against Sybil attacks. In the context of a blockchain, a valid blockchain proposal from a node should encapsulate the evidence that they worked for some cost. The Proof of Work system uses a puzzle-solving process to express membership choice. So that if a node wants to participate in proposing a block in consensus, it must find a solution before knowing which other blocks have been proposed for that specific index.

Membership Optimization accepts any number of nodes as long as it offers a correct solution To produce a valid block with proof of work,the miner sends it repeatedly and sequentially the selected nonce value along with the hash of the previous block, hash of the transaction root, and other metadata to the hash function. The resulting output is then compared against the threshold of difficulty to determine its validity. The difficulty

threshold, which is blockchain dependent, is directly proportional to the number of hashes expected to make to find a valid solution, plus it acts as a delay between offers. [47]
The **figure 2.12** shows Proof-of-Work method

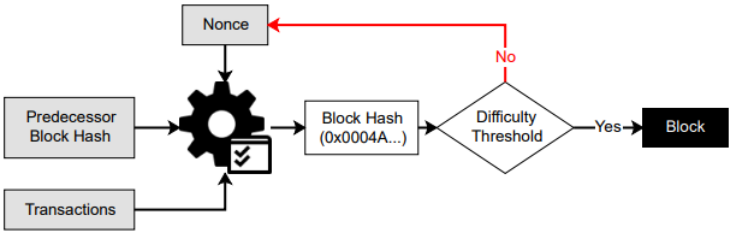

Figure 2.12: Proof-of-Work flow [47]

Proof-of-Stake (PoS)

The concept of blockchain proof of stake was first proposed in a Bitcoin community forum in 2011 to provide faster and more specific confirmation of transactions through a virtual mining mechanism. The idea of Proof-Stake is that consensus participants are asked to deposit something of value at stake, and that deposit can be withdrawn if the node is found to be working incorrectly. Not only does virtual mining provide a green blockchain system, by saving total energy consumption when compared to PoW, but it also improves productivity dramatically as blocks can attach and adhere to the chain faster. The Proof of Stake concept provides flexibility to be implemented in a number of ways. Each execution calculates the user quota differently and imposes different triggering mechanisms to reinforce the node behavior.[31]

The primary motive behind Proof-of -Stake is to reduce the energy waste that results from the Proof-of-Work block production process.
The primary meaning is a node that proves valid by pooling the assets, replacing the hash to solve the crypto puzzle with a stake-based choice, while preserving the unlicensed nature of the blockchain. The share is taken from their current balance, locked up or deposited by the shareholder. The voting power of a node can be set in proportion to the quota it issued. [47]

The **figure 2.12** shows Proof-of-Work method

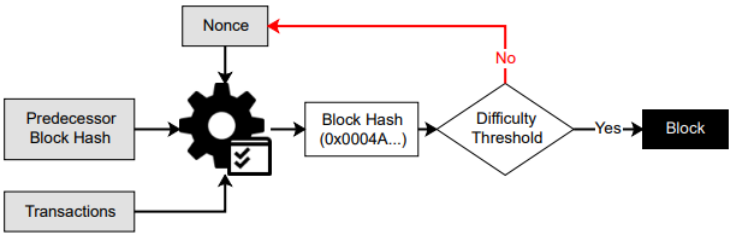

Figure 2.13: Proof-of-Stake flow [47]

Delegated Proof-of-Stake (DPoS)

In order to further speed up the transaction and solve the security issue that an offline node at the POS can also accumulate in the lifetime of the coin, Daniel Larimer proposed DPoS in April 2014 , which is currently the consensus mechanism for BitShares platforms And Crypti . In DPoS, in the system there are two roles which are witness and delegate, both of which have multiple members.[54]

Candidates for these two roles are selected by stakeholders with an approval voting process according to their number of quotas. Stakeholders with stakes above 51% can vote for N Witnesses and Delegates. Witnesses are only involved in creating the block and generate transaction fee revenue that has nothing to do with the transaction accounts in which they participate.

The DPoS node is divided into commissioners and witnesses, which have different rights respectively.delegates are responsible for voting and witnesses only need to be their followers. This is the crucial difference between PoS and DPoS. [55]

Proof of Activity (PoA)

software is a hybrid approach that is introduced to overcome some of the issues in PoS and PoW. In this method, mining starts with PoW and at some point PoS switches. Currently, "Decred" is the only currency that uses a different type of Proof of Activity[50]

Proof of Burn (PoB)

In this method, aspiring auditors increase their stake in the system by sending their coins to an unrecoverable location. The auditors are chosen at random, but those with a greater stake in the system have a high likelihood of being selected. Over time, the stake acquired diminishes and the contract has to burn more coins to increase its stake. The only coin that uses a proof firing mechanism is the Slender coin. At this point we cannot determine the most effective method. Each method has its advantages and disadvantages.[21]

Voting Proof

A High-Performance Consensus Algorithm Based on Voting Mechanism and Blockchain Consortium The blocks are checked using the voting mechanism. Four roles are identified in the Federation Network model. These are the delegates, filter personal servers, personal servers, and regular users. The algorithm showed the best performance suggested in terms of power consumption. From this, we conclude that a proof of vote (POV) algorithm is effective from (PoW).[42]

Byzantine fault tolerance (BFT)

Byzantine Fault Tolerance (BFT) is a property of a system capable of withstanding the type of failure derived from the dilemma of the Byzantine generals problem. This means that the BFT system is able to continue functioning even if some nodes fail or act maliciously. There are several possible solutions to the problem of the Byzantine generals, which means that there are several ways to build the BFT system.[50]

Consensus protocols for fault tolerance (CFT)

CFT model there is a quorum of N / 2 + 1 nodes which must agree on a certain value, so as long as you have N / 2 + 1 nodes available, which means that you have a quorum you will be able to reach an agreement , since the majority agree on this. And NO it cannot guarantee anything in the presence of malicious actors.[51]

The difference between CFT & BFT

The main difference is in the assumptions and the threat / failure model, CFT can support up to N / 2 + 1 system failures, without any warranty on the adversary nodes. BFT

provides guarantees to stand up and achieve consensus properly in the presence of N / 3 failures of any kind, including Byzantine. You can think of it as a two-phase commit versus a three-phase commit.

2.7.12 Hashing

A cryptographic hash function is a mathematical transformation that can be used to map data of arbitrary size to data of fixed size.[20]
A hash function has some very important attributes :
— Its input can be any string of any size ;
— It produces a fixed size output. 256-bit output size ;
— It has to be efficiently computable - Given any string of data, you can figure out what the output will be in a reasonable length of time.and it is deterministic so the same message always results in the same hash.[56]

2.7.13 Cryptographic Properties of a Hash Function

1- Map variable-length (x) input to constant-length output(y). Hash : 0,1*-¿0,1

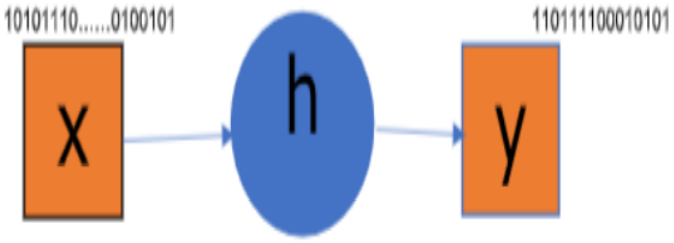

Figure 2.14: – variable-length (x) input to constant-length output(y).[37]

2- Finding the preset for a specific output is not easy

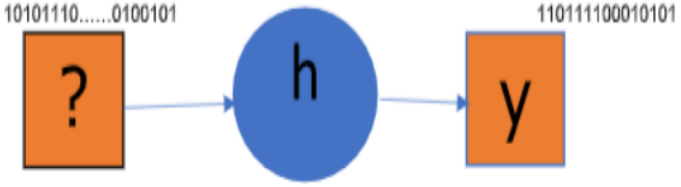

Figure 2.15: Difficulty finding image presets for exit .[37]

3- Finding a twin bumping into a particular entrance is not easy

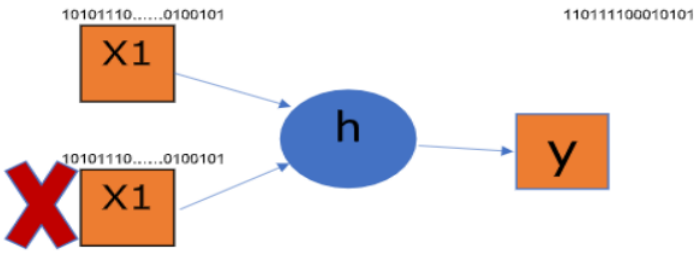

Figure 2.16: Difficulty finding a twin bumping into a particular entrance.[37]

4-Minor input mismatch to major output-mismatch

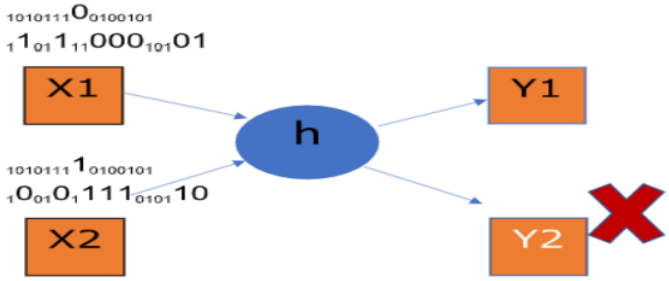

Figure 2.17: Minor input mismatch to major output-mismatch.[37]

2.7.14 Puzzle friendliness

Puzzle friendliness. A hash function H is said to be puzzle-friendly if for every possible n-bit output value y, if k is chosen from a distribution with high min-entropy, then it is infeasible to find x such that H(k ‖ x) =y in time significantly less than .[36]

Exemple

Merkle-Damgard transform SHA-256

SHA-256

One of the most popular common encoder functions is the basic fixed-length anti-collision segmentation function of the compression function. They are mathematical operations performed on digital data, the number 256 in the function name indicates the number of bits, while the SHA indicates the secure hash algorithm.[35]

Data :"fateh abbas"

Hash : 978c9dd0bbd671b83f2dc54544681912ba0505f8563141e47b2fe6443c78fb4b SHA256

2.7.15 Cryptographic Nonce

A cryptographic nonce is an arbitrary number that is only used once. A cryptographic nonce can be combined with data to produce different hash digests per nonce : hash (data + nonce) = digest Only changing the nonce value provides a mechanism for obtaining different digest values while keeping the same data.[38]

2.7.16 Merkletrees

Another useful data structure that we can build using hash pointers is a binary tree. A binary tree with hash pointers is known as a Merkletree, after its inventor Ralph Merkle. Suppose we have a number of blocks containing data. These blocks comprise the leaves of our tree. We group these data blocks into pairs of two, and then for each pair, we build a data structure that has two hash pointers, one to each of these blocks. These data structures make the next level up of the tree. We in turn group these into groups of two, and for each pair, create a new data structure that contains the hash of each. We continue doing this until we reach a single block, the root of the tree.[36]

The **figure 2.19** illustrates: In a Merkle tree, data blocks are grouped in pairs and the hash of each of these blocks is stored in a parent node. The parent nodes are in turn grouped in pairs and their hashes stored one level up the tree. This continues all the way up the tree until we reach the root node

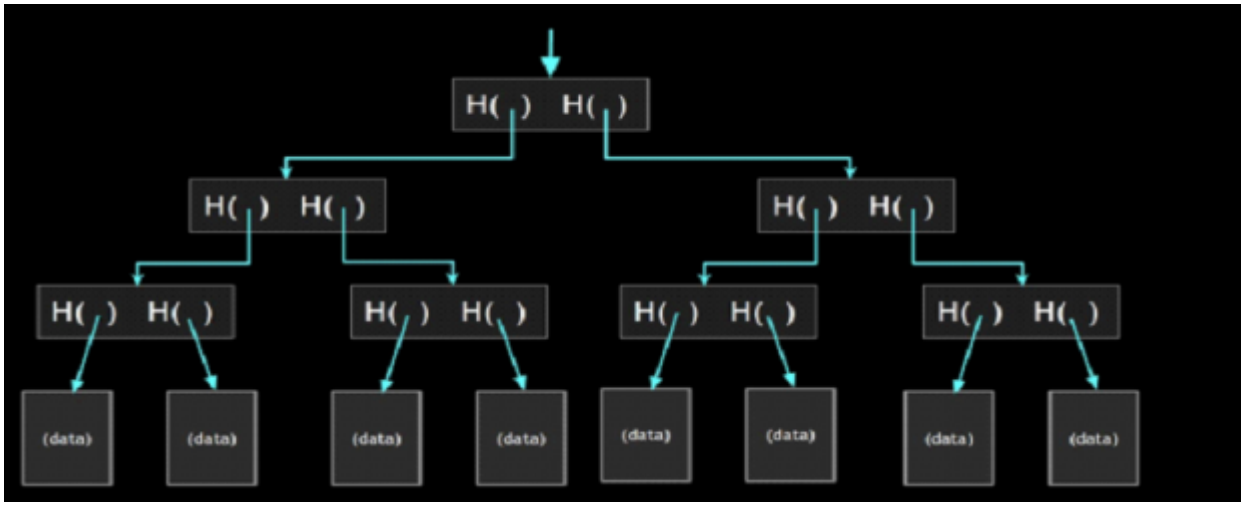

Figure 2.18: Merkle tree[36]

2.8 Blockchain features

- **Secure:** It is really impossible for anyone to tamper with transactions or ledger records present in the blockchain, which makes it more secure, so it is seen as a reliable source of information.[43]
- **Automated operations:** Operations are fully automated through software. Private companies are not needed to handle operations, which is why there is no mediation required to carry out the transactions, and trust is assured, so people can carry out their own transactions.[43]
- **Distributed:** Blockchain works in a distributed mode, in which records are stored in all nodes in the network. If one node goes down, it doesn't impact any other nodes or any other records, because they are globally distributed across all the nodes.[43]
- **Flexible:** Blockchain is programmable, using basic programming concepts and programming semantics, which makes blockchain very flexible.[43]

2.9 blockchain platform

The blockchain contains several public and private platforms, and there are criteria for choosing these platforms and also according to the requirements of your application

2.9.1 Selection criteria for the Blockchain platform

One of the most important factors:
Network type: the public or private network depends on the application
Activity: The active development of the platform also plays a role.
Price: this is the most important decision-making factor
Programming languages: The programming languages used to write the code on the platform have an important role in the choice.
Popularity: popularity is one of the main selection factors [20]

2.9.2 Hyperledger

Hyperledger, a Linux Foundation project, is an open source community to help advance technology and thought leadership. It is considered an "umbrella" for developer communities building open source blockchain and related technologies. Hyperledger was announced and formally named in December 2015 by 17 companies in a collaborative effort created to advance blockchain technology for cross-industry use in business. Now with over 130 members across the world, it is the fastest growing project in Linux Foundation history.[41] The modular architecture allows you to adjust things like the blockchain's Consensus mechanism, as well as manage storage, set services for identities, set permissions for the identities you set, and create smart contracts (in Hyperledger Fabric, smart contracts are called chaincode). In terms of programming languages, Hyperledger's chaincode is written in Go (Golang) ; however, you can utilize JavaScript with the Hyperledger Composer tool. Chaincode de can then be used to implement and automate the business logic. [40]

2.9.3 Ethereum

Ethereum is currently the most widely used smart contract development and design platform, and Ethereum introduces the concept of accounts. There are two types of accounts : 1-Externally Owned Accounts (EOAs) 2-Contract accounts. The difference is that the first is controlled by private keys without binding a symbol to them, while the second is controlled by their own node code along with the associated code. Ethereum supports the Solidity programming language. Ethereum offers faster processing and private transactions within an approved group of participants within the network.[46]

2.9.4 Bitcoin

Bitcoin is the first well-known blockchain network based on cryptocurrency. It follows PoW consensus algorithm. This is a single-chain architecture and C11is used for programming. [44] Initial application of blockchain technology is the original public ledger of bitcoin, which has later inspired other implementations called altchains. with blockchain as its core technology - even aims ambitiously to become a future legislative entity. The idea of the bitcoin system is that the entire earlier transaction history is verified by solving

a cryptographic computation. This "work" – or computation time is extremely difficult to fake. This method is called "proof-of-work" (PoW). In a process called mining, blocks are created in about 10 minutes each, after which the solvers of the computation challenges are rewarded currency. Users of the system use the bitcoin protocol to send and receive payments to "wallets", which are anonymous . Bitcoin protocol verifies each transaction. Bitcoin protocol development is an open source project supported by the Bitcoin Foundation, and the development efforts are supported by a global community of developers and entrepreneurs [57]

2.9.5 Other platforms

Corda

is an open source platform that implements a distributed ledger consisting of a mutual distrust contract that records the status of deals and commitments between entities, which can be institutions or individuals. Unlike Ethereum, Corda smart contracts are currently limited to applying financial logic, and all non-financial applications are out of scope. One of the key features of Corda is pluggable consensus within the same network.[44]

HydraChain

Such as Ethereum,Expands the platform by adding support for creating ledgers. It can reuse all the tools on the Ethereum platform. The primary difference is that HydraChain does not use Proof of Work for consensus, but rather relies on a registered and accountable group of auditors, who propose and validate the order of transactions.[44]

IOTA

is a distributed ledger technology developed by the IOTA Foundation to enable fee-free transactions. Python is used in this IOTA. [44]

Chain Core

a platform dedicated to issuing and transferring financial assets.[45]

Azure platform

developed by Microsoft offering blockchain as a service. It provides services and capabilities for creating and deploying blockchain applications.[28]

AChain

enables the creation of smart contracts and issuance of tokens, and provides a platform for developing decentralized application systems. [48]

EOSIO

it is an open source platform used to develop private and public blockchain networks. This platform provides better authentication, database, asynchronous communication, and scalability. [48]

2.10 Smart Contract

Smart contracts are at the core of blockchain technology. These are programs written in Turing-complete programming languages and are capable of self-verifying and selfexecuting agreements that can function autonomously or without any external intervention. A smart contract is a piece of code that is stored in the blockchain, is triggered by the blockchain transactions, and which then reads or writes data from/to that blockchain's database.[49]

2.10.1 chaincode

Smart contracts in Hyperledger(chaincode) Smart contracts in Hyperledger In Hyperledger calledchaincode,It is conveniently written in Go, node.js, and Java and runs in a se-cure Docker container. Unlike other smart contract platforms that must offer yourcontract to a public network to enforce it, the serial token is isolated from the pro-public blockchain peer process. This allows you to keep your business logic private.Another feature that distinguishes chain token from many other platforms is thateach pincode contract is isolated. Other organizations that use Hyperledger cannotaccess your master code directly unless permitted.[57]

2.11 Blockchain applications

Companies have become dependent on Blockchain technology in different applications, because Blockchain provides good requirements:

2.11.1 patient records

Blockchain provides an opportunity for health care service interoperability as it provides a shared ledger of clinical records, all health care service providers have access to a decentralized ledger.
Although the user interfaces may be unique, this ensures that the central ledger is the same for all suppliers. The problem that occurs is related to the current state of health records across vendors that contain large amounts of similar data under different identifiers that may not be connected. [21]

2.11.2 Voting

Accusations of vote fraud have occurred as recently as the recent presidential elections in the United States. Given the use of a PC system that sometimes costs a large number of dollars, scammers are finding more and more creative opportunities to manipulate them.

Smart contracts are a direct and affordable answer to this problem. They can be used to approve a voter's identity and record their vote. Once the voting has stopped, this data can be used to start a process. Since the blocks inside the blockchain cannot be changed.[21]

2.12 Conclusion

During this chapter, we talked about decentralized networks, distributed systems, and peer-to-peer network that were the basis for creating blockchain technology. We have also delved into blockchain technology by studying the ledger, the structure of the blockchain, its basic components, types, public and private consensus methods, and talked about the different blockchain platforms.

Chapter 3

Implementation and realization

3.1 Introduction

In the first chapter we talked about electronic payment and the problems suffered by the most prominent central and we presented blockchain as a solution, and we chose to work on the platform hyperleger fabric to develop the application and father to deal between banks and in this chapter we will present a Implementation and realization

3.2 The goal of the application:

The goal of our application is to allow users to exchange money among themselves, whether they belong to one bank or two different banks, and this is done with all security and transparency.

In the old banking system, the users' transactions are controlled by the bank and can be tampered with, but in our application, no one can change the transactions, because there is no central authority controlling the system.

Also in the old banking system to transfer money from one bank to another, it takes a long time and the transaction fees are high, but in our app, the transactions happen in moments and the transaction fees are low. Transactions are recorded in the ledger and every user has a copy of it, and when a user sends money to a user, it will surely arrive because it is recorded in the ledger.

3.3 Realization

To implement and build the system we chose the Hyperlager fabric platform, due to all the advantages it provides, in particular security, our choice of blockchain technology, and the goal is to solve the problems that we have covered in the first chapter.

3.4 Hyperledger Fabric

Hyperledger Fabric (contributed by IBM) This is a permission Hyperledger Fabric provides a framework for developing block- chain solutions with a modular architecture, pluggable implemen- tations, and container technology. While leveraging open-source best practices, Hyperledger Fabric enables confidentiality, scal- ability, and security in business environments.

3.4.1 History

Hyperledger Fabric is an application within the blockchain framework developed by Digital Asset, IBM and now Linux under the hyperledger project. Fabric was added to the incubating hyperledger project in early 2016 and a year later, it became the first project to enter an "active" status. On July 11, 2017, the hyperledger technical steering committee announced the first production-ready distributed ledger token base, Hyperledger Fabric V1.0.[58]

3.4.2 Definition

Hyperledger Fabric is an open source, licensed, enterprise-grade distributed ledger technology (DLT) platform designed for use in enterprise contexts, which provides some key differentiation capabilities over other popular distributed ledger systems or blockchain platforms. Fabric is the first distributed ledger platform to support smart contracts that were authored in general-purpose programming languages such as Java, Go, and Node.js, rather than Domain-Specific Languages (DSL). This means that most organizations already have the skill set needed to develop smart contracts, and no additional training is needed to learn a new language or DSL. One of the most important differentiating factors in the platform is the support for pluggable consensus protocols that enable the platform

to be more effectively customized to fit use cases and trust models, eg when deployed within a single organization, or operated by a trusted authority, a complete fault-tolerant Byzantine consensus can be considered Unnecessary and excessive burden on performance and productivity. In such cases, a fault-tolerant consensus protocol (CFT) can be used, while in the case of a multilateral decentralized use, the Byzantine Consensus Protocol (BFT) can be used.[59]

3.4.3 Key Concepts of Hyperledger Fabric

Figure 3.1 shows the important components of Hyperledger fabrics that we list as follows

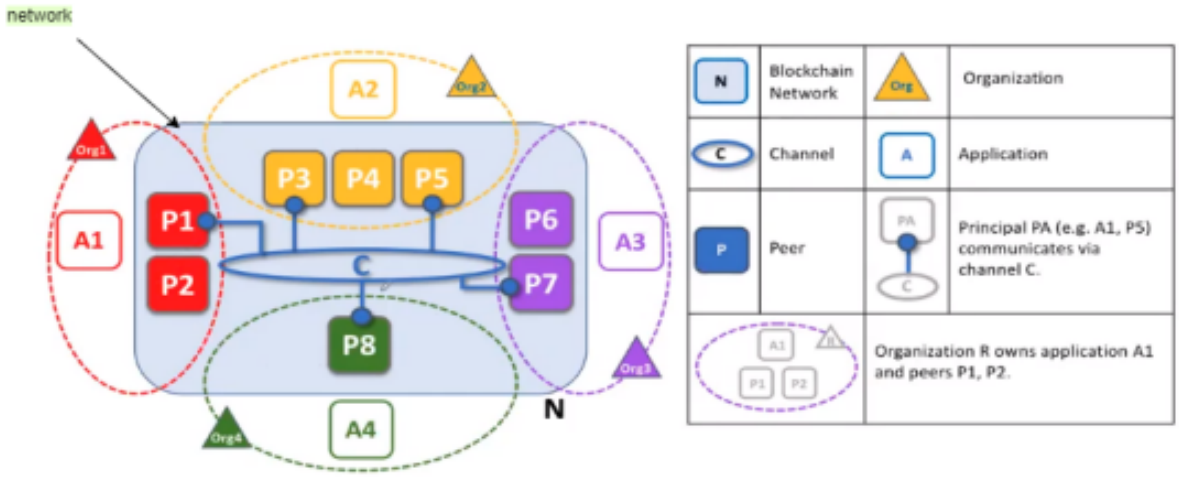

Figure 3.1: Structure of Fabric

Smart contractor Chaincode

A smart contract, or "Chaincode" called Hyperledger Fabric, is a logic or method that defines business rules, represented by an application and called by a client application outside the blockchain network in order to manage access and modification to a set of key-value pairs in a "global state" Ledger. It is installed on the peer nodes and began to work on the channels[60]

Channels

Hyperledger Fabric implements channels, which are essentially separate ledgers. The data on a channel is only visible to the members of that channels, but not to other peers in the system. This solution provides some measure of privacy (from non-member peers), but it still requires that all members of a channel trust each other with all the data on this channel. To create a new channel, the client SDK calls configuration system chaincode and references properties such as anchor peers, and members (organizations). This request creates a genesis block for the channel ledger, which stores configuration information about the channel policies, members and anchor peers. When adding a new member to an existing channel, either this genesis block, or if applicable, a more recent reconfiguration block, is shared with the new member.[61]

Organisation

Organizations are entities that own peers (e.g peer0org1,per1org1). By adding a Membership Service Provider (MSP) to a network, an organization is joined to that network With an MSP and a valid identity issued by organizations, network members can verify each other's signatures (for example, via transactions).[60]

Membership Service Provider(MSP)

The MSP maintains the identities of all nodes in the system (clients and peers) and is responsible for issuing the node credentials used for authentication and authorization. Because Fabric is authorized, all interactions between nodes occur through authenticated messages, usually with digital signatures. The Membership Service consists of a component in each node, which can authenticate transactions, verify the integrity of transactions, sign and verify authentications, and authenticate blockchain operations. The membership service provider allows Hyperledger Fabric participants to have some trust between one another. The MSP defines the relationships between the participants and gives them different access rights. Only nodes registered via MSP can connect to Hyperledger Fabric. MSP provides platform security definition.[63]

Peer

A network entity that maintains a ledger and runs string code containers in order to perform read/write operations to the ledger. It is owned and maintained by members, contains ledgers and may have strings attached in order to carry out offers from customers.[60]

Types of peers

— **Committing peer (Committer)** : all peers in a channel are committing peers who will verify all transactions submitted before committing to and updating the ledger.[94]

— **Endorsing peer (Endorser) :** peer on which a chaincode was installed. It has the ability to execute and reply to the proposal attached to that chaincode. It is not mandatory that all peers in a channel are endorsing peers.[60]

Ledger

A ledger is a key concept in Hyperledger Fabric ; it stores important factual information about business objects ; both the current value of the attributes of the objects, and the history of transactions that resulted in these current values.[21]

Orderer

Transactions in Bitcoin and Ethereum are arranged and grouped into blocks which means that every node can participate in consensus. These systems rely on probabilistic consensus algorithms that ultimately ensure the consistency of the ledger to a high degree of probability, but are still vulnerable to disparate ledgers (also known as Ledger "fork"), in which different participants in the network have a different view of the order of transactions accepted.Hyperledger Fabric works differently. It is characterized by a node called an "Orderer" (also known as an "order node") that arranges these transactions, which together with other order nodes constitute an ordering service. Since Fabric's design is based on deterministic consensus algorithms, any peer-validated block is guaranteed to be final and valid. Ledgers cannot fork in the way they do in many other distributed and unauthorized blockchain networks.[63]

3.5 Tools and developing environments

3.5.1 Software development environment

Docker:

Docker is a virtual machine, but unlike virtual machines that create a completely separate operating system, Docker allows applications to use the Linux kernel on the same machine they are installed on, and by taking advantage of this feature, it can make applications ready to ship to other machines running the same Linux operating system With somewhat different configurations.

GIT:

Git is a software for tracking changes in any set of files, usually used-for coordinating work among programmers collaboratively developing sourcecode during software development. Its goals include speed, data integrity, andsupport for distributed, non-linear workflows .

Apache CouchDB:

Apache CouchDB is an open source, document-oriented NoSQL database implemented in Erlang. CouchDB uses multiple formats and protocols to store, transfer, and manipulate its data. It uses JSON to store data, JavaScript as a query language with MapReduce, and HTTP for the API.

Visual Studio:

Visual Studio Code is an integrated development environment (IDE), created by Microsoft for Windows, macOS, and Linux. It is a source code editor that can work with multiple programming languages such as Java, JavaScript, Go, Node.js, Python and C++.

3.5.2 Developing languages

Node js:

Node.js is an open source, cross-platform JavaScript runtime environment that implements JavaScript code outside of a web browser. Node.js allows developers to use JavaScript to write command line tools and for server-side scripting.

Go:

Go is a statically typed, compiled programming language designed at Google by Robert Griesemer, Rob Pike, and Ken Thompson. Go is syntactically similar to C, but with memory safety, garbage collection, structural typing, and CSP-style concurrency.

HTML:

HTML Markup Language: It is a markup language used to create and design web pages and websites, and this language is considered one of the oldest and most widely used languages in web page design

CSS:

CSS: is a formatting language for web pages concerned with the appearance and design of websites, it is specifically designed to separate formatting from the content of the written document and this applies to the colors, fonts, images and backgrounds used in the pages, complete. Flexibility and comfort. This technology takes care of the overall appearance of web pages, including colors, images.

JavaScript:

JavaScript: is a formatting language for web pages concerned with the appearance and design of websites, it is specifically designed to separate formatting from the content of the written document and this applies to the colors, fonts, images and backgrounds used in the pages, complete.

Flexibility and comfort. This technology takes care of the overall appearance of web pages, including colors, images.

3.6 Hardware configuration

During this current project, all work was done on a laptop with the following technical characteristics. During this current project, all work was done on a laptop with the following technical characteristics.

Materials	**Laptop**
CPU	Intel Core i5-3360 M @ 2.80 GHz
RAM	12 GO
OS	Windows 10 Pro x64
GPU	Intel(R) HD Graphics 4000
STORAGE	HDD 298 GO

Table 3.1: Hardware Environment.

3.7 System design

As shown in **Figure 3.2**, the network contains many parties with different roles and functions

enrollAdmin: is the process in which certificates are created and granted to the identity user. This username and password are given outside the domain, and they use the name and password as part of the Fabric-ca-client call to the CA. Then the public and private keys are generated.

RegisterUser :is done by the CA administrator. The identity is assigned a username and password, along with the attributes (would the identity be an admin or a node, for example?). This registration places the username and password, along with other relevant information about the identity, into the CA's database.

QueryNetworkThe query is a string code call that reads the current state of the ledger but does not write to the ledger. A serial code function may query specific keys in a

ledger, or it may query a set of keys in a ledger.

blockValidator Creates transactions ,Executes and validates transactions with other validating nodes on the network ,Maintains a local copy of ledger ,Participates in consensus and updates ledger

invokeNetwork:Network connection: The app is connected to a network blockchain

queryNetwork:Inquire and apply all instructions on the network

application:Connect and implement all previous classes.

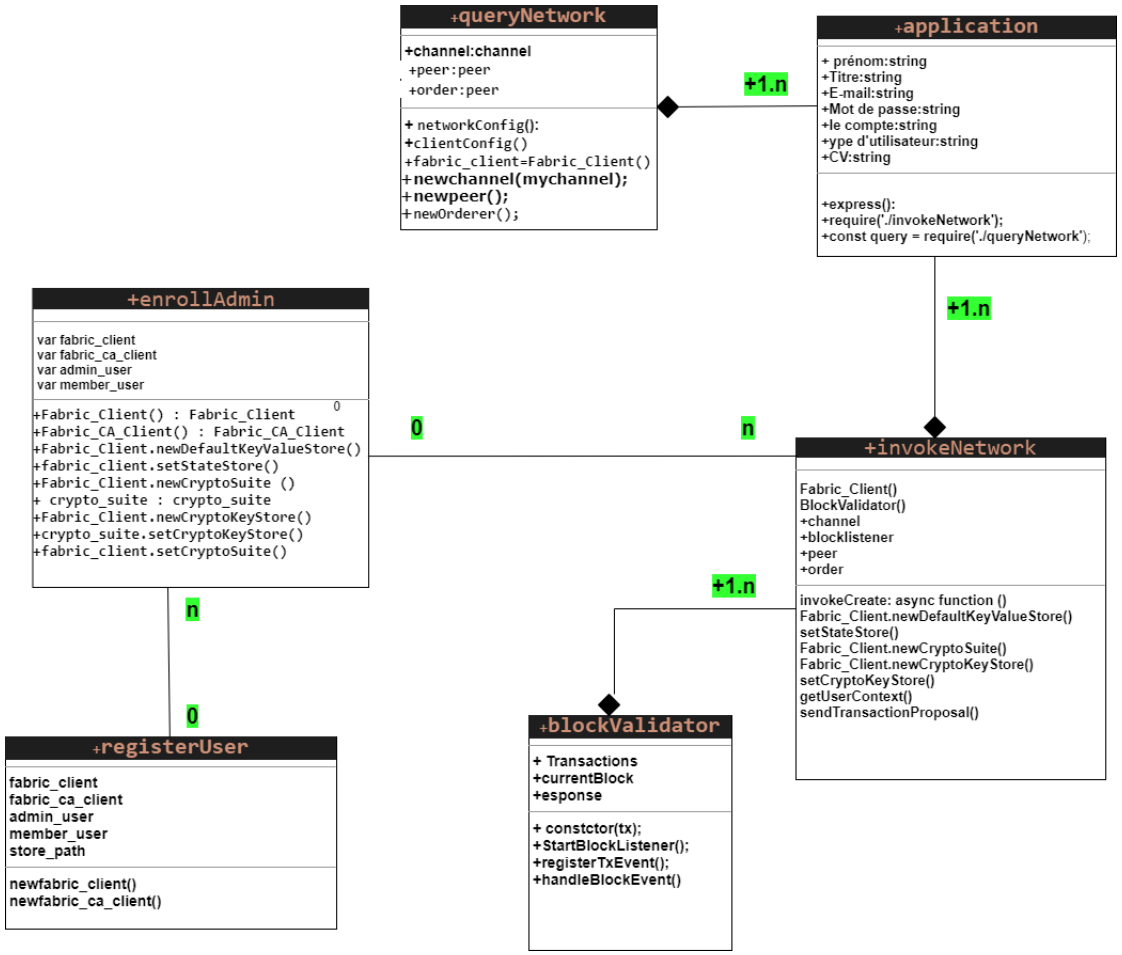

Figure 3.2: Class diagram of e-payment

3.8 Application Scenario

We have developed our application to consist of several organizations. Every organization we consider a bank, every bank can deal with another bank by sending transactions so that we have a customer in Bank A who wants to send it to another customer in Bank B. The transfer is done through the platform with a simple transaction without an intermediary

or third party and the transactions are recorded in the ledger after The approval of the two banks.

3.9 Architecture of the application

In this architecture **Figure 3.3**, we proposed four banks belonging to the same network called **'Network'**, connected in a channel called **'chennel'** Each bank has multiple users P1, P2, .., P10, for each user a ledger containing the basic information of the user and all the transactions he has made, whether he is the one who sent the money or received it from another user.

As for the **orderer** system, it organizes and arranges transactions in terms of their validity and validity

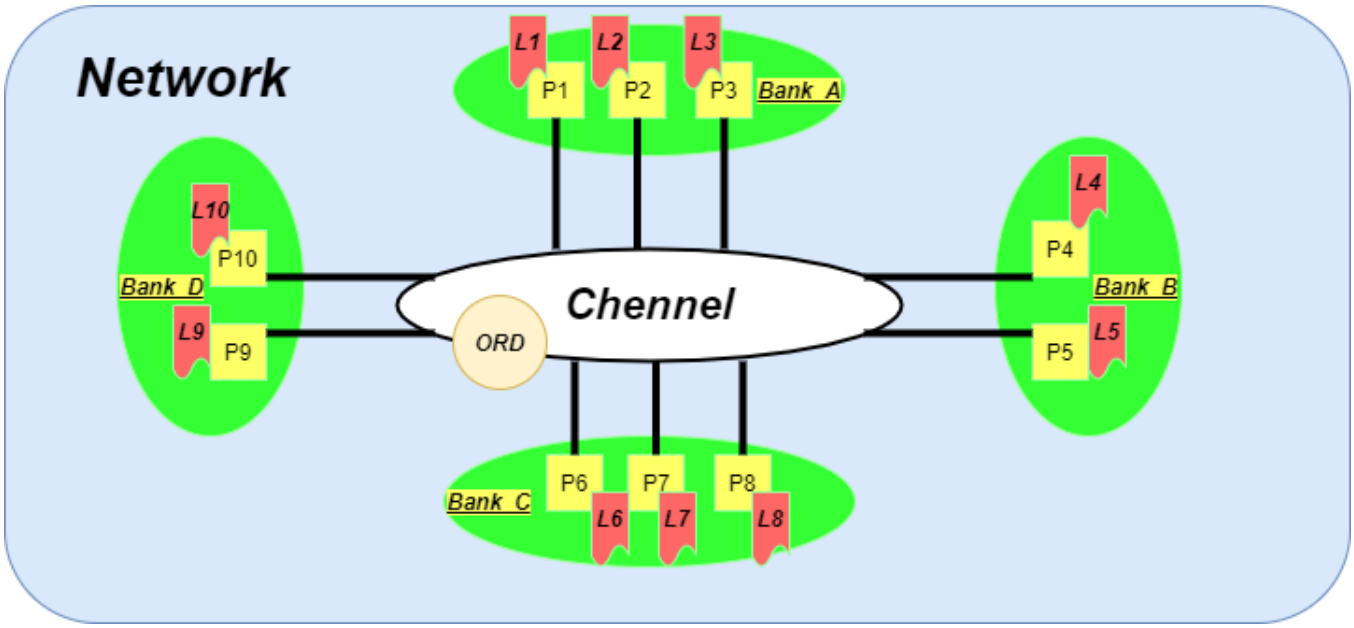

Figure 3.3: Architecture of the application

3.10 application test

3.10.1 cypto-config.yaml file.

cypto-config.yaml is the file that contains all the details about the bank network, the request, the peer nodes, the organization (ORG1, ORG2) and helps us create the cipher materials required for the corporate network using the cipher command.

3.10.2 structure crypto-config.yaml

As shown in **Figure 3.4**, a file **crypto-config** consists of the following parts:

- Organization structure
- Number of peers in each organization
- User in every organization

```
1
2   OrdererOrgs:
3     # ---------------------------------------------------------------------------
4     # Orderer
5     # ---------------------------------------------------------------------------
6     - Name: Orderer
7       Domain: example.com
8       Specs:
9         - Hostname: orderer
10        - Hostname: orderer2
11        - Hostname: orderer3
12        - Hostname: orderer4
13        - Hostname: orderer5
14  PeerOrgs:
15    # ---------------------------------------------------------------------------
16    # Org1
17    # ---------------------------------------------------------------------------
18    - Name: Org1
19      Domain: org1.example.com
20      EnableNodeOUs: true
21
22      Template:
23        Count: 2
24
25      Users:
26        Count: 1
27    # ---------------------------------------------------------------------------
28    # Org2: See "Org1" for full specification
29    # ---------------------------------------------------------------------------
30    - Name: Org2
31      Domain: org2.example.com
32      EnableNodeOUs: true
33      Template:
34        Count: 2
35      Users:
36        Count: 1
37
```

Figure 3.4: Crypto-config.yaml file structure

3.10.3 Structure of configtx.yaml file

configtx.yaml file consist of

- organizations section
- orderers sectio
- applications section
- capabilities section
- profiles section

3.10.4 Organizations Section in configtx.yaml file

This section contains the details of the organization and that organization can be an organization or a peer organization. As shown in the **Figure 3.5** below, the first tag is "Organizations" and under that you can select any number of organizations according to the requirements.

Each organization has its own name, ID, and MSPDir. Here MSPDir is the location where that organization's encryption materials are stored.It also contains host and port details for the anchor peer as well.

```
Organizations:
    - &OrdererOrg
        Name: OrdererOrg
        ID: OrdererMSP
        MSPDir: crypto-config/ordererOrganizations/example.com/msp
        Policies:
            Readers:
                Type: Signature
                Rule: "OR('OrdererMSP.member')"
            Writers:
                Type: Signature
                Rule: "OR('OrdererMSP.member')"
            Admins:
                Type: Signature
                Rule: "OR('OrdererMSP.admin')"
    - &Org1

        Name: Org1MSP
        ID: Org1MSP

        MSPDir: crypto-config/peerOrganizations/org1.example.com/msp
        Policies:
            Readers:
                Type: Signature
                Rule: "OR('Org1MSP.admin', 'Org1MSP.peer', 'Org1MSP.client')"
            Writers:
                Type: Signature
                Rule: "OR('Org1MSP.admin', 'Org1MSP.client')"
            Admins:
                Type: Signature
                Rule: "OR('Org1MSP.admin')"
        AnchorPeers:
            - Host: peer0.org1.example.com
              Port: 7051
```

Figure 3.5: 0rganizations (ORG1) section structure

3.10.5 Orderer Section in configtx.yaml file

This section(**Figure 3.6**) contains details about the order. This helps the composition blocks to form well.

Order type: This can have a value such as "Solo" or "Kafka". It is used solo in du-ring development and kafka is used in production environment.

Addresses: This contains the host and port details of the request command.

BatchTimeout: Wait a while before creating a batch. The task of the command is to create a set of transactions so that this is the time to wait for it.

3.10.6 Application section in configtx.yaml file

Application is being referred in the genesis block. As shown in the **Figure 3.7** below organizations is list of orgs which are defined as participants.

```
Orderer: &OrdererDefaults
  OrdererType: solo
    Addresses:
        - orderer.example.com:7050
        BatchTimeout: 2s
BatchSize:
        MaxMessageCount: 10
        AbsoluteMaxBytes: 99 MB
        PreferredMaxBytes: 512 KB
        Kafka:
        Brokers:
            - 127.0.0.1:9092
    Organizations:

    Policies:
        Readers:
            Type: ImplicitMeta
            Rule: "ANY Readers"
        Writers:
            Type: ImplicitMeta
            Rule: "ANY Writers"
        Admins:
            Type: ImplicitMeta
            Rule: "MAJORITY Admins"
        BlockValidation:
            Type: ImplicitMeta
            Rule: "ANY Writers"
```

Figure 3.6: Orderers section

3.10.7 Capabilities

Fabric channels can be joined by orderer and peer nodes that are running different versions of Hyperledger Fabric. Channel capabilities allow organizations that are running different Fabric binaries to participate on the same channel by only enabling certain features. For example, organizations that are running Fabric v1.4 and organizations that are running Fabric v2.x can join the same channel as long as the channel capabilities levels are set to V1_4_X or below. None of the channel members will be able to use the features introduced in Fabric v2.0.

```
123 Application: &ApplicationDefaults
124     Organizations:
125     Policies:
126         Readers:
127             Type: ImplicitMeta
128             Rule: "ANY Readers"
129         Writers:
130             Type: ImplicitMeta
131             Rule: "ANY Writers"
132         Admins:
133             Type: ImplicitMeta
134             Rule: "MAJORITY Admins"
135
136     Capabilities:
137         <<: *ApplicationCapabilities
```

Figure 3.7: Application section in configtx.yaml

```
75  Capabilities:
76
77      Channel: &ChannelCapabilities
78          V1_3: true
79      Orderer: &OrdererCapabilities
80          V1_1: true
81      Application: &ApplicationCapabilities
82          V1_3: true
83          V1_2: false
84          V1_1: false
85
```

Figure 3.8: Capabilities

3.10.8 Profile section in configtx.yaml file

The last and important section in the configtx.yaml file is the profile section.

As shown in the **figure 3.9** it mainly consists of two parts, one is the configuration block details and the second is the channel details.
TwoOrgsOrdererGenesis refers to the configuration block and has requested details within that. It contains block capabilities, order details (organization and capabilities), and union details (peer organizations).
TwoOrgsChannel indicates the channel that helps to create the desired channel.

```
Profiles:

    TwoOrgsOrdererGenesis:
        <<: *ChannelDefaults
        Orderer:
            <<: *OrdererDefaults
            Organizations:
                - *OrdererOrg
            Capabilities:
                <<: *OrdererCapabilities
        Consortiums:
            SampleConsortium:
                Organizations:
                    - *Org1
                    - *Org2
    TwoOrgsChannel:
        Consortium: SampleConsortium
        <<: *ChannelDefaults
        Application:
            <<: *ApplicationDefaults
            Organizations:
                - *Org1
                - *Org2
            Capabilities:
                <<: *ApplicationCapabilities

```

Figure 3.9: Profile section

3.11 Run application

3.11.1 Network creation

Run these commands **../byfn.sh up -s couchdb**

We have created a file called beynf and its work is:

When the channel group configuration is updated, the relevant organizations - Org1, Org2, and OrdererOrg - need to sign it. Usually this task is carried out by individual enterprise administrators, but in BYFN it is he who signs the enterprises To run the file beynf we run the command **../byfn.sh up -s couchdb**

The **figure 3.10** shows the first step: This first step creates all the certificates and keys for our different network entities, the configuration block used to boot the request service, and a set of configuration parameters required to configure the channel. Then this will run all containers, then run a complete end-to-end application scenario as shown in **Figure 3.11**

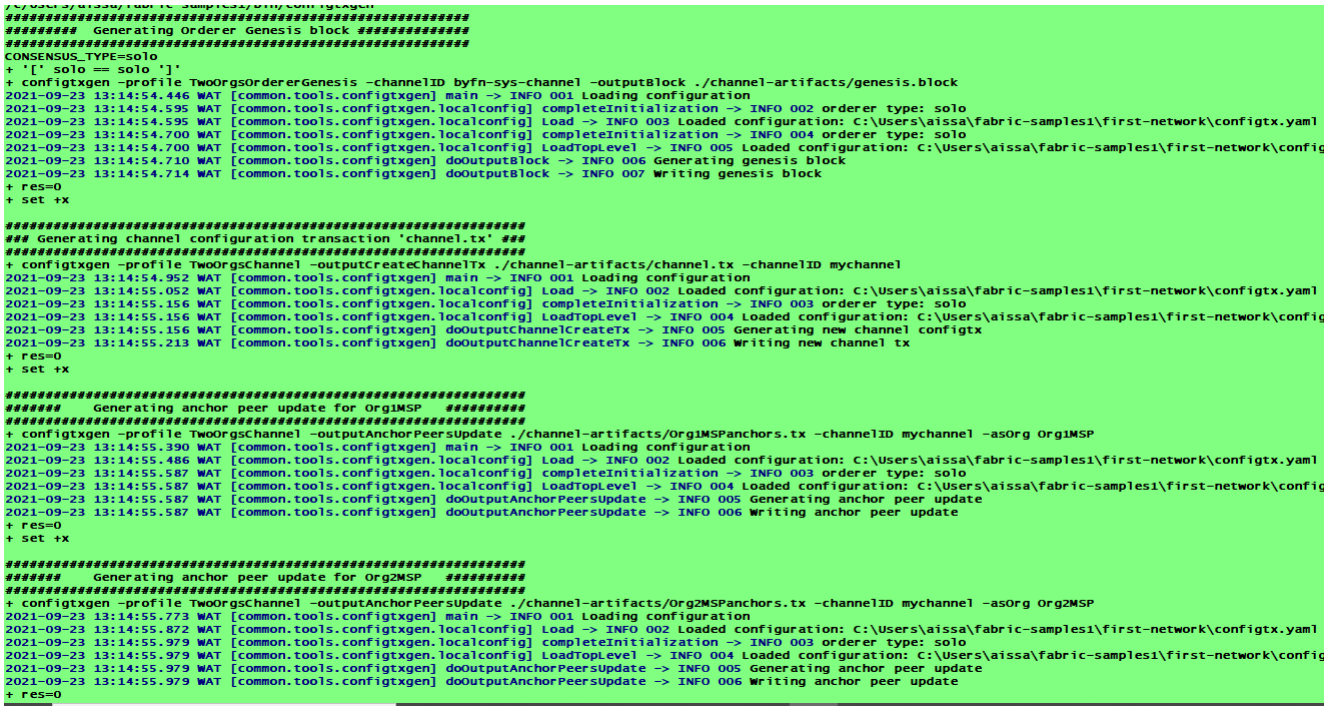

Figure 3.10: Generate all certificates, keys, and config block used

3.11.2 Connect the network with the WAP application

In this part, we will review the most important interfaces used in our application and wewill mention them as follows :

Index interface

This interface consists of logging in to three banks or subscribing to one of the banks

Figure 3.11: Run Containers and Building First Network

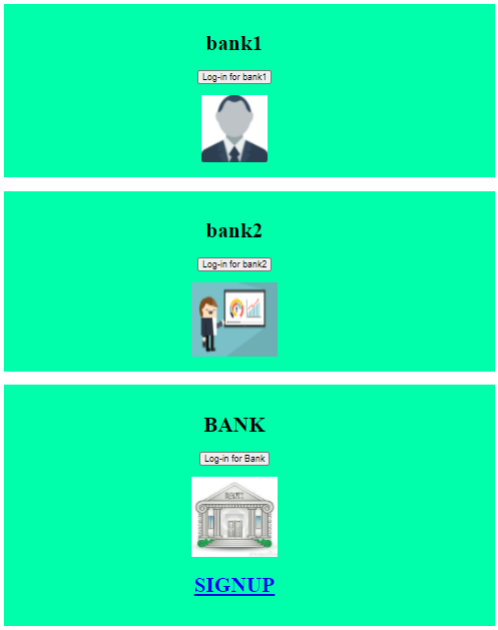

Figure 3.12: Index interface

Signup interface

We fill in the required information in the interface (name, address, etc.), then we choose the bank and after pressing the register button, you become a subscriber to a bank. **Figure 3.13** shows this

Login interface

After subscribing to a bank, you can enter by pressing the login button and view the balance or send or receive money with a user from the same bank or a user subscribed to another bank as shown in the **Figure 3.14**

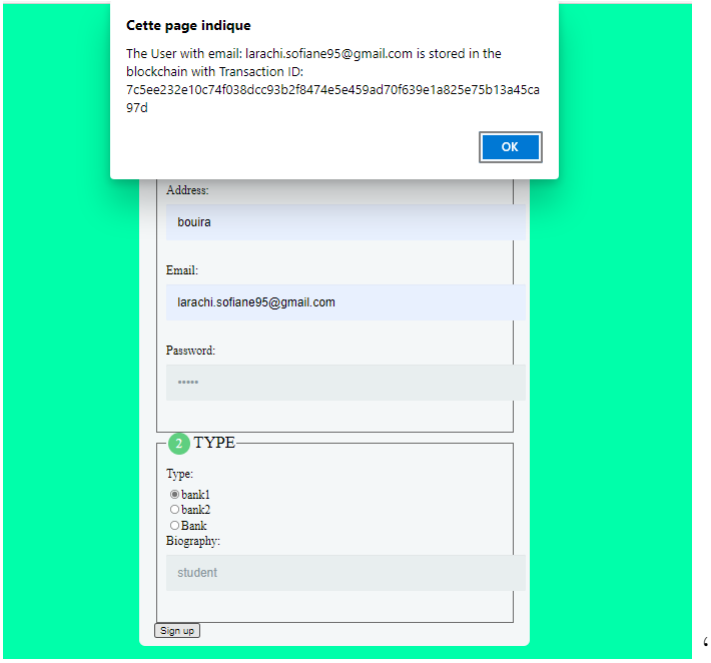

Figure 3.13: Signup interface

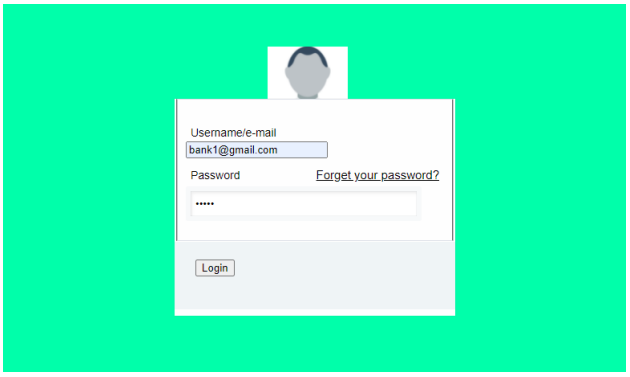

Figure 3.14: Login interface

User account interface

After logging in, the interface appears in **Figure 3.15**. If we want to send money, we press the add button. If we want to view the ledger (Transaction history), we press the button View.

User transaction intrface

The **Figure 3.16** shows the process of sending money. You choose the balance to be sent and click on Send

https://www.overleaf.com/project/61489ae9d459411d80845a91

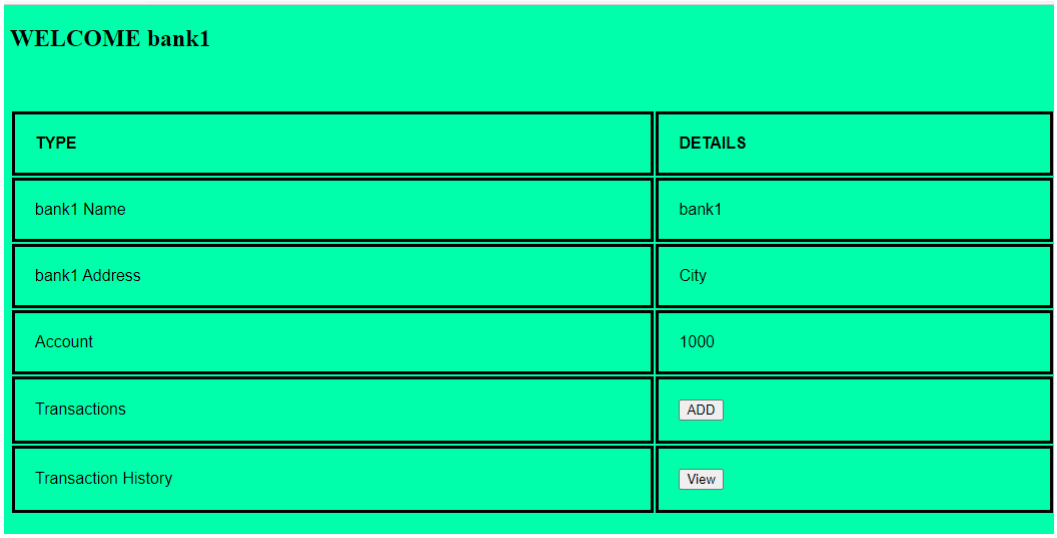

Figure 3.15: welcome to bank intrface

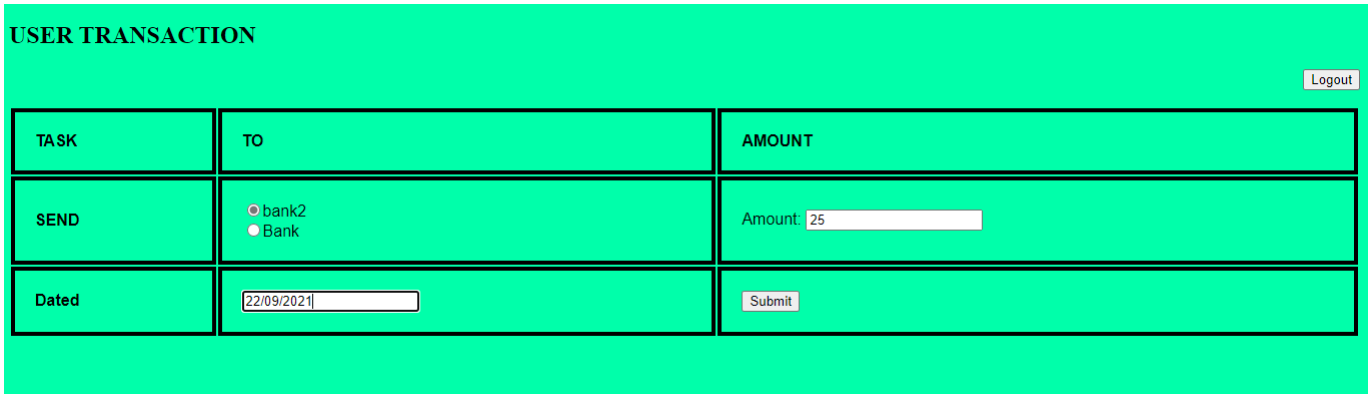

Figure 3.16: User transaction interface

transaction history

The user can view his transaction history all the time as shown in the **Figure 3.17**

Transaction History

Transaction ID	To	From	Amount	Dated
txnID_bank2_16323093742	bank	bank2	25	22/09/2021
txnID_bank_16323094191	bank2	bank	80	23/09/2021
txnID_bank2_16323094577	bank1	bank2	25	23/09/2021
txnID_bank1_16323096849	bank2	bank1	30	23/09/2021
txnID_bank_16323083427	bank1	bank	45	23/09/2021

Figure 3.17: double spending

3.12 Conclusion

Due to the development that the world has witnessed in the electronic payment system and the diversity of payment methods in the areas of collection, these systems have suffered from many problems such as the current central system and the emergence of blockchain technology that allows us to ease and transparent transactions, we have chosen Hyperlager Fabric platform to implement an interbank communication application that allows For everyone to transparently send their money from one bank to another, we chose the HyperLege platform because it does not require strong hardware support.

General conclusion

We have built a blockchain-based electronic payment system to address the shortcomings of central electronic payment systems, and the implemented system enables different banks to transact transparently and securely.
The proposed system is a compromise between the classic electronic payment system and the cryptocurrency-based system.

With the continuous development of blockchain technology and the diversity that this technology is witnessing, our goal is to create a decentralized solution that provides solutions to the problems of the electronic payment system and our application allows users to exchange money securely and transparently, as we have used blockchain technology, a technology that works without a central entity.

Fabric is a modular and scalable distributed operating system to run licensed blockchains. It introduces a new architecture that separates transaction execution from consensus and enables policy-based authentication that is reminiscent of middleware replicated databases. By its modularity, Fabric is well suited to various further improvements and investigations.

The HyperLege platform was chosen because it does not require strong hardware support, and Hyperlager did not solve the 51% problem where members joining the chain must be a trusted and secure CA Fabric CA that automatically generates the certificate or creates an account that Fabric Peer can have multiple peers, Where the ledger and the blockchain are stored, a single peer can join different channels of the fabric order service Provide sorting services Create block sort using Solo, and configure it to sort using Kafka

(Limited State Machine)

We had no luck in achieving a comprehensive application that works on all platforms (Linux and Windows), we will work to improve it as much as possible, for example payment with QR code, phone.

Bibliography

[1] Boel, P. (2019). Payment systems–history and challenges. Sveriges Riksbank Economic Review, 1, 51-66.

[2] Gogoski, R. (2012). Payment systems in economy-present end future tendencies. Procedia-Social and Behavioral Sciences, 44, 436-445.

[3] Heng, S. (2004). E-payments: modern complement to traditional payment systems. E-Conomics Working Paper, (44).

[4] Fatonah, S., Yulandari, A., Wibowo, F. W. (2018, December). A review of e-payment system in e-commerce. In Journal of Physics: Conference Series (Vol. 1140, No. 1, p. 012033). IOP Publishing.

[5]Sumanjeet, S. (2009). Emergence of payment systems in the age of electronic commerce: The state of art. Global Journal of International Business Research, 2(2).

[6]Moşteanu, N. R., Faccia, A. (2020). Digital Systems and New Challenges of Financial Management–FinTech, XBRL, Blockchain and Cryptocurrencies. Quality-Access to Success Journal, 21(174), 159-166.

[7]Agrawal, R. (2021). Block-2 E-Payment Systems.

[8]Khatib, A., Kafi, M., Mullick, N. H. Study of Effect of Electronic Banking Services on Increase of Resources in Mashhad Shahr Bank.

[9]Bultum, A. G. (2014). Factors affecting adoption of electronic banking system in Ethiopian banking industry. Journal of Management Information System and E-commerce, 1(1), 1-17.

[10]KAFLEY, G. S. (2018). Recent trends in electronic payment systems in india.

[11]KAFLEY, G. S. (2018). Recent trends in electronic payment systems in india.

[12] Mallick, S., Das, K. K. Banking in India: An Emperical Study on Innovative Trends by use of IT Products.

[13]Hasan, A., AtifAman, M., Ali, M. A. (2020). Cashless Economy in India: Challenges Ahead. Journal of Commerce, 8(1), 21-30.

[14]Magaji, B. M. (2020). A Legal Overview of Electronic Banking in Uganda.

[15]Ghanem, H., Cheriet, S. (2018). The role of El ectronic Payment Systems in the development of the Algerian Banking system.

[16]Badiâa, H., Mohamed, A. N., Samir, A., Karima, B. (2012). INTERBANK PAYMENT SYSTEM (RTGS) SIMULATION USING A MULTI-AGENT APPROACH.

[17]. Blockchain For Dummies®, 2nd Edition Published by: John Wiley Sons, Inc., 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com Copyright © 2019 by John Wiley Sons, Inc., Hoboken, New Jersey

[18]. Blockchain Revolution An imprint of Penguin Random House LLC 375 Hudson Street New York, New York 10014 Copyright © 2016 by Don Tapscott and Alex Tapscott

[19]. wiki/Satoshi$_N$*akamoto/en.wikipedia.org/wiki/Satoshi*$_N$*akamoto*[20].*BLOCKCHAINNOWAN*
$92 - 76 - 08977 - 3$,

[21]. I. Bashir, "Mastering Blockchain . 2nd ed", Paperback, Mar 2018, ISBN : 9781788839044

[22] Peer-to-Peer //academy.binance.com/ar/articles/peer-to-peer-networks-explained

[23].wiki Peer-to-Peer // fr.wikipedia.org/wiki/Pair-%C3%A0-pairAutres$_a$*pplications*

[24]. 101blockchains peer-to-peer/ /101blockchains.com/peer-to-peer-network

[25]. wiki/Centralisation/ /fr.wikipedia.org/wiki/Centralisation$_($*histoire*)

[26]. wiki/DecentralizationBlockchain$_t$*echnologyen.wikipedia.org/wiki/DecentralizationBlockchain*$_t$*e*
$13(pbk) : 978 - 1 - 4842 - 3080 - 0ISBN - 13(electronic) : 978 - 1 - 4842 - 3081 - 7$

[28]. Puri, V., Kumar, R., Van Le, C., Sharma, R., Priyadarshini, I. (2020). A vital role of blockchain technology toward Internet of vehicles. In Handbook of research on blockchain technology (pp. 407-416). Academic Press.

[29]. Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. IEEE Consumer Electronics Magazine, 7(4), 6-14.

[30]Luo, Y., Chen, Y., Chen, Q., Liang, Q. (2018, November). A new election algorithm for DPos consensus mechanism in blockchain. In 2018 7th International Conference on Digital Home (ICDH) (pp. 116-120). IEEE.

[31] Consensus Immutable agreement for the Internet of value

[32] Li, D., Peng, W., Deng, W., Gai, F. (2018, July). A blockchain-based authentication and security mechanism for IoT. In 2018 27th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-6). IEEE.

[33] Li, D., Peng, W., Deng, W., Gai, F. (2018, July). A blockchain-based authentication and security mechanism for IoT. In 2018 27th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-6). IEEE

on Consensus, Membership and Structure", Aug 2019, arXiv:1908.08316v1 [cs.DC]

[34]R. C. Merkle, "A digital signature based on a conventional encryption function," in Conference on the Theory and Application of Cryptographic Techniques. Springer, 1987, pp. 369–378.

[35]bytemaster and bitsharestalk.org, "Transactions as proof-of-stake the end of mining," 2013. [Online]. Available: https://bitsharestalk.org/index.php? topic=1138.msg13602msg13602A

[36] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.

[37]. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2019). Bitcoin and cryptocurrency technologies. Curso elaborado pela.

[38] Gupta, S. S. (2017). Blockchain. IBM Onlone (http://www. IBM. COM).

[39]. Yaga, D., Mell, P., Roby, N., Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

[40]. Oberstar, A. (2020). Tehnologija veriženja blokov v zdravstvu (Doctoral dissertation, Univerza v Ljubljani, Fakulteta za računalništvo in informatiko).

[41] Elrom, E. (2019). Hyperledger. In The Blockchain Developer (pp. 299-348). Apress, Berkeley, CA. [31]. Lin, I. C., Liao, T. C. (2017). A survey of blockchain security issues and challenges. IJ Network Security, 19(5), 653-659.

[42] Editor: Blockchainprep .BLOCKCHAIN FUNDAMENTALS TEXT BOOK Fundamentals of Blockchain Publisher: Blockchainprep UAE ISBN: 301.345.908

[43].Nehra, V., Sharma, A. K., Tripathi, R. K. (2020). Blockchain implementation for Internet of Things applications. In Handbook of Research on Blockchain Technology (pp. 113-132). Academic Press.

[44] .BAMBARA, Joseph J., ALLEN, Paul R., IYER, Kedar, et al. Blockchain: A practical guide to developing business, law, and technology solutions. McGraw Hill Professional, 2018.

[45]. Hyperledger Global Forum 2021 – Join us on June 8–10 and register today (https://events.linuxfoun
global-forum/) .

[46].Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266-2277.

[47] Natoli, Christopher, et al. "Deconstructing blockchains: A comprehensive survey on consensus, membership and structure." arXiv preprint arXiv:1908.08316 (2019).

[48] QuantumMechanic, "Bitcoin Forum - Proof of Stake instead of Proof of Work," 2011. [Online]. Available: https://bitcointalk.org/index.php?topic=27787.0

[49] Ethereum Wiki, "Problems," 2017. [Online]. Available: https://github.com/ethereum/wiki/wiki/P

[50] Wan, Shaohua, et al. "Recent advances in consensus protocols for blockchain: a survey." Wireless networks 26.8 (2020): 5579-5593.

[51] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in Proceedings of the 17th International Conference on Distributed Computing and Networking. ACM, 2016, p. 13.

[52] Lin, Iuon-Chang, and Tzu-Chun Liao. "A survey of blockchain security issues and challenges." IJ Network Security 19.5 (2017): 653-659.

[53] Peters, G. W., Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking beyond banks and money

[54](pp. 239-278). Springer, Cham. Kim, M., Kim, Y. (2019). Development of IoT device management system using blockchain DPoS consensus algorithm. Journal of IKEEE, 23(2), 508-516.

[55]Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., Qijun, C. (2017, October). A review on consensus algorithm of blockchain. In 2017

[56]IEEE international conference on systems, man, and cybernetics (SMC) (pp.Liu, X., Wang, Z., Jin, C., Li, F., Li, G. (2019). A blockchain-based medical data sharing and protection scheme. IEEE Access, 7, 118943-118953.2567-2572). IEEE.

[57]Foschini, L., Gavagna, A., Martuscelli, G., Montanari, R. (2020, June). Hyperledger Fabric Blockchain: Chaincode Performance Analysis. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[58]Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In Workshop on distributed cryptocurrencies and consensus ledgers (Vol. 310, No. 4).

[59] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

[60]Nguyen, T. S. L., Jourjon, G., Potop-Butucaru, M., Thai, K. L. (2019, April). Impact of network delays on Hyperledger Fabric. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 222-227). IEEE.

[61]Benhamouda, F., Halevi, S., Halevi, T. (2019). Supporting private data on hyperledger fabric with secure multiparty computation. IBM Journal of Research and Development, 63(2/3), 3-1.

[62] hyperledger-fabric : hyperledger-fabric.readthedocs.io

[63]Kwon, M., Yu, H. (2019, October). Performance improvement of ordering and endorsement phase in hyperledger fabric. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 428-432). IEEE.

ملخص

مع تطور التجارة الالكترونيه اصبح نظام الدفع الالكتروني ضروريا في الحياة اليوميه ولكن دائما مايتعرض لبعض المشاكل من بينها الاختراق فهو غير امن بشكل جيد ،حيث تقوم بعض البنوك بادارة جميع المعاملات باستخدام وحده مركزية قابله للفشل،مما يعرض اموال المستخدم للخطر،كما تحتوي هذه الوحدة المركزيه على العديد من نقاط الضعف فقط تعرضت بعض البنوك للاختراق وسرقة اموال المستخدمين،كل هذا ادى الى البحث عن بديل لامركزي يوفر سلامة ومنح المستخدمين السيطرة على معاملاتهم بكل حرية وامان.

يهدف مشروعنا الى تطوير برنامج دفع الكتروني يعتمد على تقنية البلوك تشين وهي تقنية لا تتطلب وحدة مركزية للادارة ،كما قمنا بتطوير برنامجنا على منصة البلوك تشين الخاصة Hyperleger Fabric فهي توفر لنا المتطلبات التي نحتاجها لتطوير تطبيقنا.

قمنا بانجاز تطبيق واب ،واجرينا سيناريو تجريبي على عدة بنوك افتراضية،وفي المستقبل سنحاول تطويره على مختلف منصات أنظمة التشغيل وربطها بمختلف طرق الدفع.

كلمات مفتاحية :

التجارة الاكترونية،الدفع الاكترونية،الاختراق،الامان ،مركزية ،لامركزية ،بلوكتشين.....

Abstract

With the development of electronic commerce, the electronic payment system has become necessary in daily life, but it is always exposed to some problems, including penetration, as it is not well secured, as some banks manage all transactions using a central unit that is subject to failure, which exposes the user's money to risk, and this central unit also contains On many weaknesses, only some banks were exposed to hacking and theft of users' money, all of this led to the search for a decentralized alternative that provides safety and gives users control over their transactions freely and securely

Our project aims to develop an electronic payment program based on blockchain technology, a technology that does not require a central unit for management, and we have also developed our program on a private blockchain platform hyperleger Fabric.
They provide us with the requirements we need to develop our application. We have completed a WAP application, and conducted a test scenario on several virtual banks,

and in the future we will try to develop it on various operating system platforms and link it to various payment methods.

Mots clé:E-commerce, electronic payment, hacking, security, centralization, decentralization, blockchain..... ...

Resume

Avec le développement du commerce électronique, le système de paiement électronique est devenu nécessaire dans la vie quotidienne, mais il est toujours exposé à certains problèmes, notamment de pénétration, car il n'est pas bien sécurisé, car certaines banques gèrent toutes les transactions à l'aide d'une unité centrale qui fait l'objet à l'échec, ce qui expose l'argent de l'utilisateur à des risques, et cette unité centrale contient également Sur de nombreuses faiblesses, seules certaines banques ont été exposées au piratage et au vol de l'argent des utilisateurs, tout cela a conduit à la recherche d'une alternative décentralisée qui offre sécurité et donne aux utilisateurs le contrôle de leurs transactions librement et en toute sécurité

Notre projet vise à développer un programme de paiement électronique basé sur la technologie blockchain, une technologie qui ne nécessite pas d'unité centrale pour la gestion, et nous avons également développé notre programme sur une plateforme blockchain privée hyperleger Fabric.
Ils nous fournissent les exigences dont nous avons besoin pour développer notre application.
Nous avons terminé une application WAP et mené un scénario de test sur plusieurs banques virtuelles, et à l'avenir, nous essaierons de la développer sur différentes plates-formes de système d'exploitation et de la relier à différentes méthodes de paiement.

Key words: E-commerce, paiement électronique, piratage, sécurité, centralisation, décentralisation, blockchain..... ...