DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
UNIVERSITY OF MOHAMED BOUDIAF - M'SILA

FACULTY OF MATHEMATICS
AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

A Dissertation in Fulfillment
For the Requirements of the Degree of Master in Computer

DOMAINE: Mathematics and Informatics

FILIERE: Informatics

OPTION: Information Systems and Software Engineering

By: Neguez Djamel

Entitled

Tracking Sensitive Products Using Blockchain Technology

Presented publicly to the jury:

Dr. Mouhoub Nasserddine	**University of M'sila**	**President**
Dr. Moussaoui Adel	**University of M'sila**	**Supervised**
Dr. AMRAOUI Noureddine	**University of M'sila**	**Examiner**

Acknowledgements

All praise belongs to ALLAH alone, and blessings and peace be upon the final Prophet.
I am grateful to my family, Especially my parents for their encouragement, prayers, motivations, and tired of us in our career. special thanks to my aunt it's my teacher since i was young , May God bless them , and all my friends in college and out of college who helped me through this period of my life.
Many thanks to my supervisor **Dr. Adel Moussaoui** for his advices and support.

Neguez Djamel

Thanks to you all.

Contents

List of Figures

Abstract

تعاني إدارة سلسلة التوريد التقليدية من مجموعة نقائص منها عدم الشفافية و كونها غير قابلة للتتبع و إنعدام الإتصال و التنسيق بين الأطراف المعنية و إرتفاع السرقة و المنتجات المغشوشة من أغذية أو أدوية مما يضر الدولة أو الشركة و حتى الفرد في المجتمع ، و لم تستطع برامج التسيير القديمة حل هذه المشاكل و هذا لتحكم العنصر البشري في ذلك . إستعمال تكنولجيا البلوكشين لإدارة سلسة توريد المنتجات الحساسة أحدثت ثورة في هذا المجال و ألغى إستعمال البرامج التقليدية ، و هذا لشفافيته و إمكانية التتبع و عدم تدخل العامل البشري في عملياته و عقوده ، مما يلبي متطلبات العملاء بشكل أفضل ويمكن أن تكون أداة أساسية للشركات لاكتساب ميزة تنافسية مستدامة...

Abstract

the management of the traditional supply chain suffers from a set of shortcomings, including lack of transparency and being untraceable, lack of communication and coordination between the concerned parties, high theft and adulterated products of food or medicine, which harm the state or the company and even the individual in society. The ancient solution to these problems and this is to control the human element in that. The use of blockchain technology to manage the supply chain of sensitive products revolutionized this field and eliminated the use of traditional software, due to its transparency, traceability and non-interference of the human factor in its operations and contracts, which better meets customer requirements and can be an essential tool for companies to gain a competitive advantage. sustainable...

General Introduction

The process of controlling the flow of products and services from the point of origin to the point of consumption is known as traditional supply chain management. Multiple parties, including suppliers, manufacturers, distributors, retailers, and customers, must coordinate their actions. The conventional supply chain is an ancient idea that has changed and advanced with time as technology and the environment around it have done. The success and competitiveness of organizations have become dependent on effective supply chain management that is compatible with the ever-changing environment and technology. Even after trying to digitize it and create programs (ERP) to run it, it still suffers from many problems and challenges . these include limited visibility, inefficient inventory management, poor supplier collaboration, complex logistics and transportation, quality control issues, data integration and system compatibility, as well as demand volatility and supply chain disruptions.

Blockchain replaces traditional transactions and management software by offering many benefits when applied to supply chain management. Transparency and traceability features allow a comprehensive view of the entire supply chain, enabling stakeholders to track the origin and movement of products. The security provided by the blockchain, through its decentralized and tamper-resistant nature, helps prevent fraud and counterfeiting. By automating processes and eliminating middlemen, we improve efficiency and reduce costs. Moreover, blockchain enhances trust and collaboration among supply chain participants, fostering stronger relationships and streamlining interactions.

We design and develop supplychain system using blockchain on ethereum network by writing smart contract on truffle freamwork and use api to facilitate communication between webapp and smart contract and using another database (Mongo db) for more flexibility and controle in authentication and authorization because we faced the problem of many parties and roles in this system and develop interface for user interaction .

This thesis is organized as follow :

- We start with chapter one and explain deeply blockchain technology and how it works , what problems does this technology solve, and here use case and how did Satoshi reach it and what techniques did he collect in order to bring this innovation to us We explained a lot of assistive technologies or based on this technology and vague terminology that needs to be explained down to the frameworks that are the latest to reach it.
- The second chapter we discuss about our domain which is supply chain of sensitive products and we choose pharmaceuticals products supply chain to dissect it and put it under the microscope , and study its problems and weakness globally and locally .
- The last chapter we implement this project and make it real , I explained the tools and how to use them to make decentralized applications .

Neguez Djamel

1

Chapter One

After economic problems , the blockchain technology emerged from the economic center through the invention of cryptocurrencie, dealing with them and trading them,In This Chapter we will discuss this technology high level in cryptography and security

1.1 Blockchain Definition

Chain of blocks, the simple definition of blockchain is a series of blocks has relation with hash used to store data and can transmit it , or it's peer-to-peer, distributed, immutable, decentralized and public ledger and to bring the concept closer we say it's like database that facilitates the process of recording transactions and tracking assets in a business network.

The first use case of this technology is the digital currency called bitcoin. and shared the white paper of bitcoin whith title "Bitcoin: A Peer-to-Peer Electronic Cash System in 2008 by the name of Satoshi Nakamoto. [15]

1.2 Blockchain Technology

Technical definition, Blockchain is a peer-to-peer, distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updatable only via consensus or agreement among peers.

Layman's definition: Blockchain is an ever-growing, secure, shared recordkeeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update.

From these technical definitions of the blockchain it consists of more than one technology which is:

- **Peer-to-peer :** Created when two or more nodes are connected and share resources without central controller in the network.
- **Distributed ledger :** Is a ledger recording the transaction and their details in multiple places at the same time, this ledger is spread across the network among all peers in the network and each node has the same data in the ledger. [57]
- **Cryptographically secure :** Using cryptography security services that make this ledger secure against tampering and misuse. non-repudiation, data integrity, and data origin authentication are some of these services.
- **Append-only :** This means data add only to the blockchain, and impossible to change or update this data, it can be considered practically immutable, which means block immutable.
- **Updatable via consensus :** Updatable only via consensus, and this is the power of decentralization. no central authority validates the update in the distributed ledger, any modification to the blockchain is subject to strict criteria established by the protocol, and it can only be added to the blockchain after the agreement has been reached among the majority of participating peers and nodes.

1.3 History of Blockchain technology

In 2008, Satoshi Nakamoto published a white paper introducing the concepts behind bitcoin and blockchain, Its practical implementation then occurred on Jan. 3, 2009, the first bitcoin block mined by Nakamoto and validating the blockchain concept. The block contained 50 bitcoins and was known as the Genesis block (the block with index 0), Satochi use Many technologies and collect them, Each of them has a role either directly or indirectly, accumulation of computer science and networks We can view this in chronological order

- 1960s – Invention of computer networks
- 1969 – Development of ARPANET
- 1970s – Early work on secure network communication including public key cryptography
- 1970s – Cryptographic hash functions
- 1973 – Extension of ARPANET to other geographic locations
- 1974 – First internet service provider - Telenet
- 1976 – Diffie–Hellman work on securely exchanging cryptographic keys
- 1978 – Invention of public key cryptography
- 1979 – Invention of Merkle Trees (hashes in a tree structure) by Ralph C. Merkle
- 1980s – Development of TCP/IP
- 1980 – Protocols for public key cryptosystems, Ralph C. Merkle
- 1982 – Blind signatures proposed by David Chaum
- 1982 – The Byzantine Generals Problem
- 1985 – Work on elliptic curve cryptography by Neal Koblitz and Victor Miller
- 1991 – Haber and Stornetta work on tamper proofing document timestamps. This can be considered the earliest idea of a chain of blocks or hash chains
- 1992 – Cynthia Dwork and Moni Naor publish Pricing via Processing or Combatting Junk Mail. This is considered the first use of Proof of Work (PoW)
- 1993 – Haber, Bayer, and Stornetta upgraded the tamper-proofing of document timestamps system with Merkle trees
- 1995 – David Chaum's Digicash system (an anonymous electronic cash system) started to be used in some banks

- 1998 – Bit Gold, a mechanism for decentralized digital currency, invented by Nick Szabo. It used hash chaining and Byzantine Quorums
- 1999 – Emergence of a file-sharing application mainly used for music sharing, Napster, which is a P2P network, but was centralized with the use of indexing servers
- 1999 – Development of a secure timestamping service for the Belgian project TIMESEC
- 2000 – Gnutella file-sharing network, which introduced decentralization
- 2001 – Emergence of BitTorrent and Distributed Hash Tables (DHTs)
- 2002 – Hashcash by Adam Back
- 2004 – Development of B-Money by Wei Dei using Hashcash
- 2004 – Hal Finney, the invention of the reusable PoW system
- 2005 – Prevention of Sybil attacks by using computation puzzles, due to James Aspnes et al
- 2009 – Bitcoin (first blockchain)
- 2013, Vitalik Buterin is a programmer and co-founder of the Bitcoin magazine stated and as one of the first contributors to Bitcoin codebase.

All previous attempts to create anonymous and decentralized digital currency were successful to some extent, but they could not solve the problem of preventing like double spending and byzantine problem state machine replication) SMR problem) in a completely trustless or permissionless environment.

1.4 Blockchain Structure

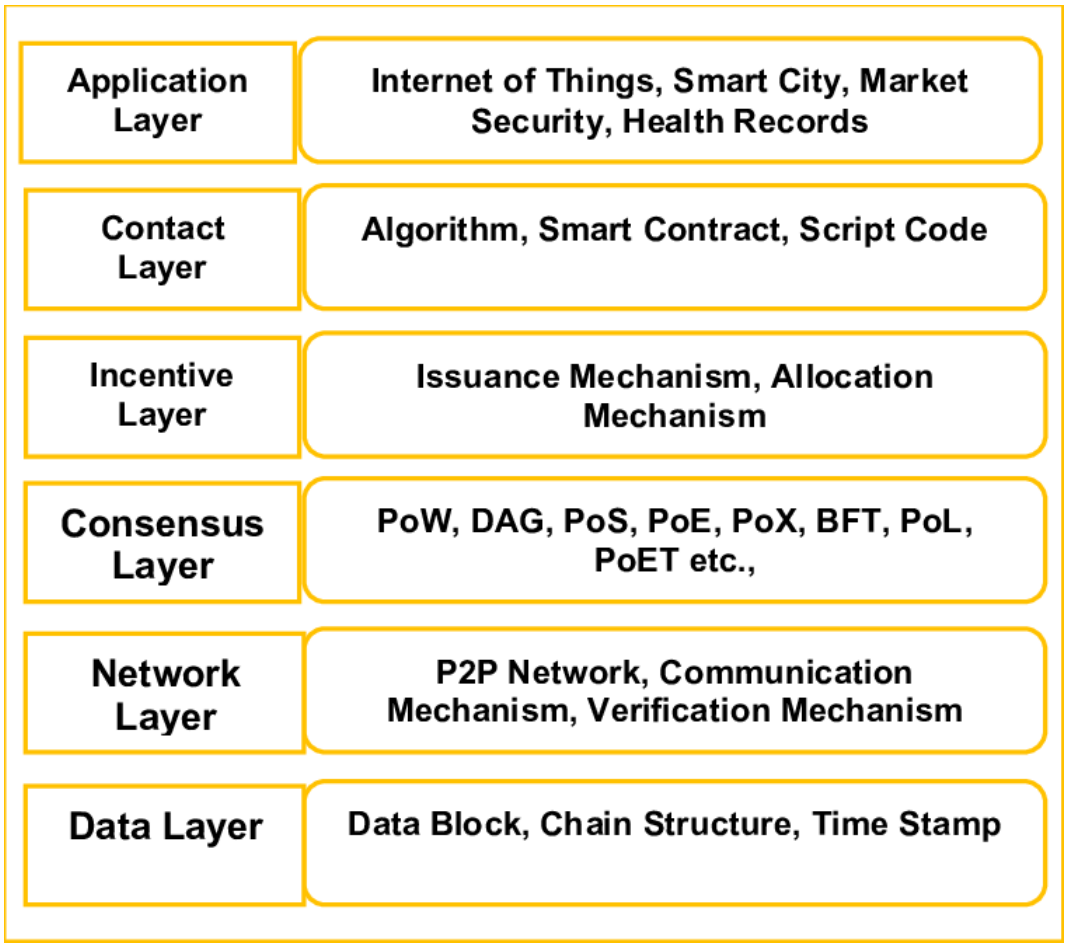


Figure 1.1: Blockchain structure

1.4.1 Transaction

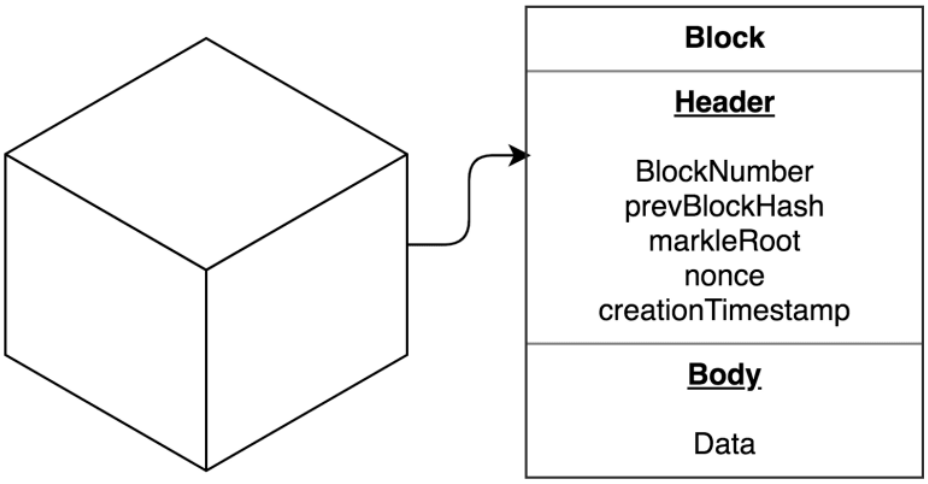
In general, a transaction is a sequence of operations performed on a database or other system that must be executed atomically, meaning that all of the operations must either succeed or fail as a single unit. In blockchain ,transactions are signed messages originated by an externally owned account,and transfer value from one address to another.that is broadcast to the network and collected into blocks. There are two main models for recording transactions on a blockchain: the UTXO (Unspent Transaction Output) model used in bitcoin and the account model used in Ethereum . every transaction has one-or-more inputs and one-or-more outputs. [41]

1.4.2 The Blocks

Blocks are the basic containers of information in a blockchain, they consisting of a block header and a content or data or transaction in her body. block header comprised of six

fields: Version, Previous Block Hash, Merkle Root, the difficulty, timestamp, and nonce.

Figure 1.2: The blocks of blockchain



- **Version :** A version number to track software/protocol upgrades.
- **Previous block hash :** It's a 32-bytes field that contains a 256-bits hash (created by SHA-256 cryptographic hashing) of the previous block. This helps to create a linear chain of blocks.
- **The difficulty :** refers to the effort required to mine a block. Proof of Work blockchains implement certain rules that cause this to rise or fall depending on the amount of hashing power on the network.
- **Merkle Root :** A hash of the root of the merkle tree of this block's transactions.
- **Timestamp :** Is a time of the creation of the block and time of records a transactions, its size 4 bytes.
- **None :** A counter used for the proof-of-work algorithm, has 4 bytes.

1.4.2.1 The genesis block

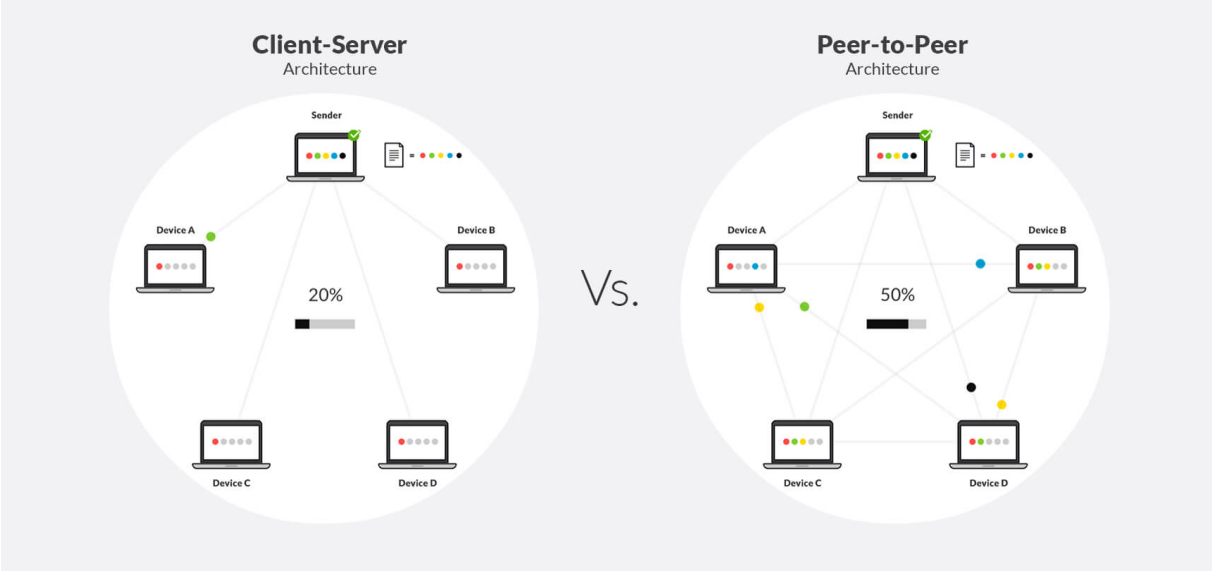
it's the single block with no precedent block , The first block in every blockchain is called the genesis block.

1.4.3 Network layer

Is the part of the Internet communications process where these connections occur, manages addressing and routing of packets between different physical routers blockchain based on

Peer-to-Peer Network Architecture, P2P network connects computer systems to each other, over a local network or the internet, without a central server.

Figure 1.3: Network layer of blockchain



1.4.4 Consensus operation

It is essential to make sure that the network members agree on the ledger's state, or the order and uniqueness of the records. Consensus algorithms are used to do this, and they use various techniques to make sure that the correct order and uniqueness of transactions have been determined and approved by sufficient users to be added to the ledger. Blockchain-Technology-Primer.pdf (iabtechlab.com)

The process of mining cryptocurrencies is another name for the consensus process. The mechanisms designed to ensure the accuracy and consistency of information stored by all nodes in a distributed ledger. there is many consensus mechanisms like POW for bitcoin network , and POS for Ethereum Network , Proof of Burn ,Proof of Activity , and there is no perfect consensus mechanism and only optimal solutions exist for specific scenarios , The consensus mechanisms of blockchain aims to eliminate mainly two known problems with digital currency

- Remove the problem of double spend
- Eliminate Byzantine Generals problem

we will explain what it is this problemes and how blockchain in bitcoin or in other networks solve this problems.

1.4.4.1 Proof of Work (POW)

Proof of Work (PoW) is a widely used consensus algorithm in blockchain-based systems such as Bitcoin. Its primary function is to validate transactions and add new blocks to the blockchain ledger. In a PoW system, miners or nodes are required to solve a complex mathematical puzzle to confirm a transaction and include it in the blockchain. The miner who successfully solves the puzzle first is rewarded with a certain amount of cryptocurrency. . . .

Figure 1.4: Proof of work (POW) image

1.4.4.2 Proof of stake (POS)

Proof of stake is consensus mechanism for blockchain networks, processing transactions and creating new blocks in a blockchain, The PoW algorithm is energy intensive, fee-wise, and limited in scalability. they follows a pseudo-random selection process to select validators from a group of nodes. The system uses a combination of factors, including storage time, randomness, and node wealth.

Figure 1.5: Proof of work (POW) image

1.4.4.3 Proof of Authority (PoA)

Is a consensus algorithm used in blockchain systems. It is a modified version of the Proof of Stake (PoS) algorithm which means that block validators are not staking coins but their own reputation instead. based on their reputation or identity selected as trustworthy entities, a set of pre-selected validators are given the authority to validate transactions and create new blocks.

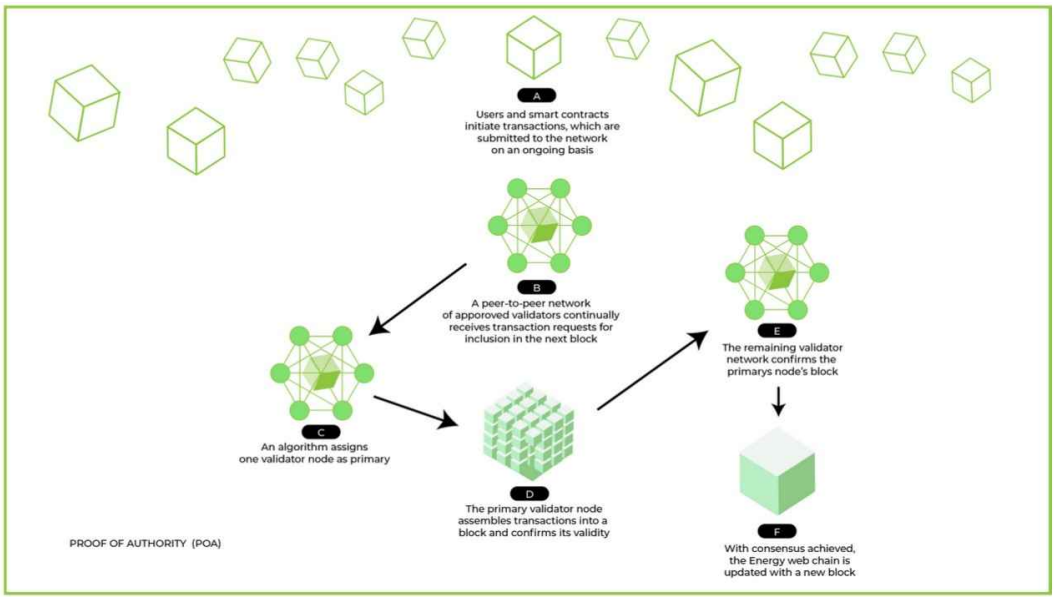


Figure 1.6: Proof of authority (PoA) image

1.5 The Incentive Layer

The incentive layer in blockchain systems aims to motivate nodes to engage in security verification. The overall security of a blockchain relies on the active participation of multiple nodes. For instance, in Bitcoin, the security is derived from the substantial computational power contributed by numerous nodes involved in the proof-of-work process, which prevents attackers from surpassing the collective computational strength. Node verification typically consumes computing resources and electricity. To encourage node involvement, blockchains typically reward participants with virtual currency. the second role of this layer is the distribution of rewards that are earned by nodes in the network for the work they do to reach consensus. Whether this layer is implemented or not depends on the consensus mechanism in use.[54] Prominent examples of cryptocurrencies generated through this mechanism include Bitcoin, Litecoin, and Ether.

Figure 1.7: Incentive Layer role

1.6 Smart Contract

In the 1990s, Nick Szabo published an article titled Formalizing and Securing Relationships on Public Networks that introduced the concept of smart contracts. "A smart contract is an electronic transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs." [37]

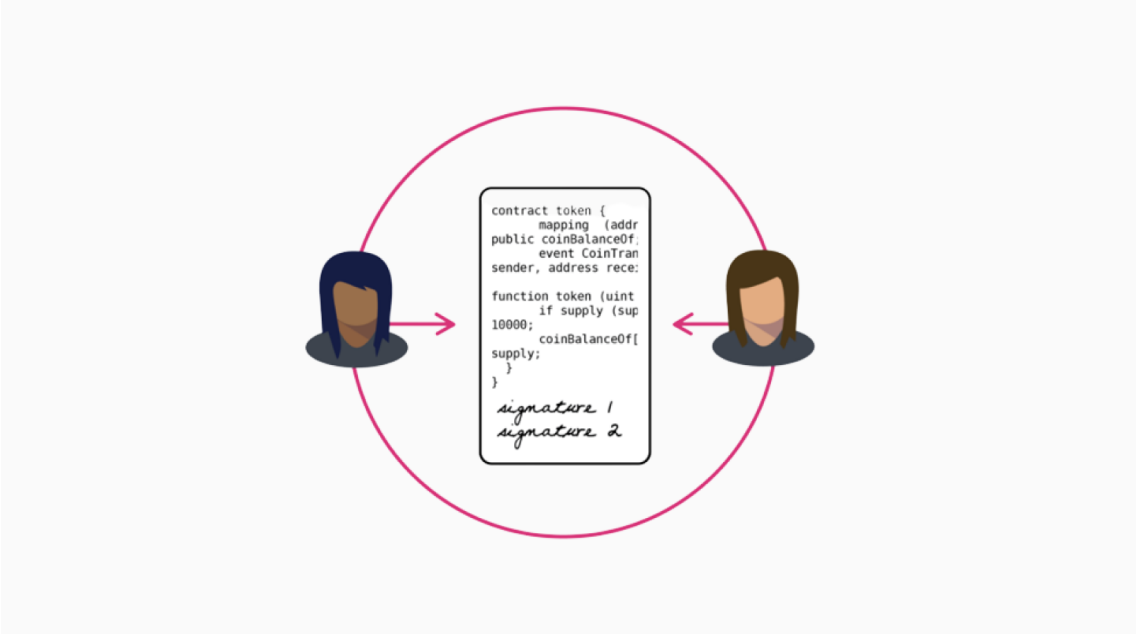


Figure 1.8: smart contract

The general definition of smart contracts digitizes agreements by turning the terms of an agreement into computer code that automatically executes when the contract terms are met.[29] when the necessary conditions are met, a smart contract's preprogrammed actions are automatically carried out. Additionally, the process is transparent since a copy of the contract is held by other blockchain nodes as well. Bitcoin script is the first use of smart contract based blockchain ,bitcoin script is a straightforward programming language that enables cryptographic and hash operations, along with conditionals. However, it lacks the capability to perform looping or recursion, making it non-Turing-complete. Despite its simplicity, it allows for essential functionalities within the Bitcoin network.Bitcoin Script is currently utilized by developers to generate multisignature Bitcoin addresses, time-locked transactions, and advanced protocols such as payment channels and cross-chain atomic trades. However, programming with Bitcoin Script can be challenging, making it difficult to create addresses and transactions. Ivy aims to simplify the process by providing an easier way to write and implement these programs, enhancing accessibility and usability in this domain. [1] and there is also many other types of smart contract in other blockchain network like ethereum , smart contracts in ethereum are typically written in a high-level language, such as Solidity. But in order to run, they must be compiled to the low-level bytecode that runs in the EVM. Once compiled, they are deployed on the Ethereum platform using a special contract creation transaction [16].

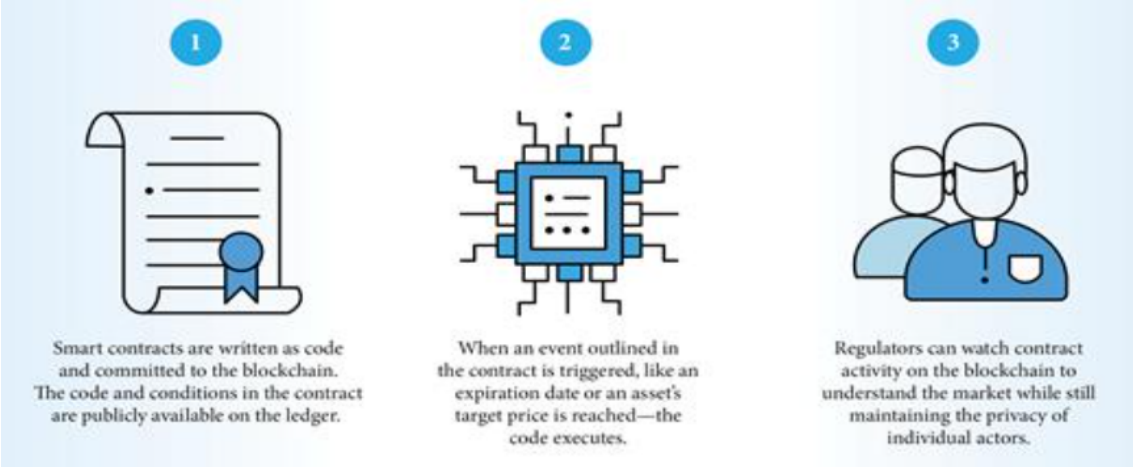


Figure 1.9: smart contract description

1.6.1 Smart Contract Functionality

Smart contract is the same with normal contract and here condition but writing with code and if-else condition,that runs on the blockchain and executed by all consensus nodes :

the first step is determine the terms of the contract , after that they are translated into programming code, this code describe the possible scenarios of a future transaction with here conditions .

Figure 1.10: Trasform condition of contract to code in smart contract

the second step is store this smart contract in block of blockchain like data , and deploy it on the blockchain network for all the nodes in the network , the code of this smart contract is runnings when event fired , it's executed in all nodes in blockchain network , if smart contract is deployed you can't change on it .

In ethereum network we will using solidity language to write a smart contract Unlike Bitcoin Scripting Language, solidity is a turing complete language , in ethereum network

for every transaction or run/execution of smart contract we will pay a Gas, It is basically used by the miner to perform calculations on your behalf [39].

1.6.2 Solidity Language

Solidity is an object-oriented, curly-bracket high-level language for implementing smart contracts. that run on the Ethereum Virtual Machine. Smart contracts are programs that are executed inside a peer-to-peer network where nobody has special authority over the execution [49].

Figure 1.11: Solidity Logo

1.6.3 Smart Contract Features

A smart contract is a self-executing program that runs within a blockchain and automates the actions required in an agreement or contract. It operates based on a set of predefined rules that constitute the terms of the agreement between two or more parties [18]. There are many additions and personal contracts in the social and economic life of the individual and society :

1. **Automatically Executable :** Once the coded conditions are satisfied, the smart contract automatically performs the designated actions, ensuring a seamless and efficient process. It does not require any manual intervention or third-party involvement for its execution.

2. **Immutable :** smart contracts cannot be changed when they are deployed , it can only be removed as long as the functionality is implemented previously.

3. **Deterministic :** The final outcome will not vary, no matter who executes the smart contract .If the result differs between nodes, then a consensus cannot be reached, and a whole paradigm of distributed consensus on the blockchain can fail.

4. **Secure :** the smart contracts are tamper-proof , blockchain usually provides these security guarantees , even if the encryption is broken, the hacker will still need to change every block that follows the one that was changed. and its very difficult .

5. **Unstoppable :** This means that nothing stops the smart contract until unfavorable conditions

1.7 Mining Process

The goal of using blockchain technology is to offer a decentralized option for storing information. by removing the data from a centralized system, it becomes more secure and is not vulnerable to physical failures at a single location, which strengthens its reliability. Mining is the mechanism that can validate transactions and add new blocks in blockchain with consensus algorithms , If and when they find new blocks by resolving the PoW, the miners rewards come in two different forms,new coins created with each new block, and transaction fees from all the transactions included in the block , To earn this reward, the miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm . A miner or node is the CPU that attempts to solve a challenging arithmetic problem in order to find a new block [17].

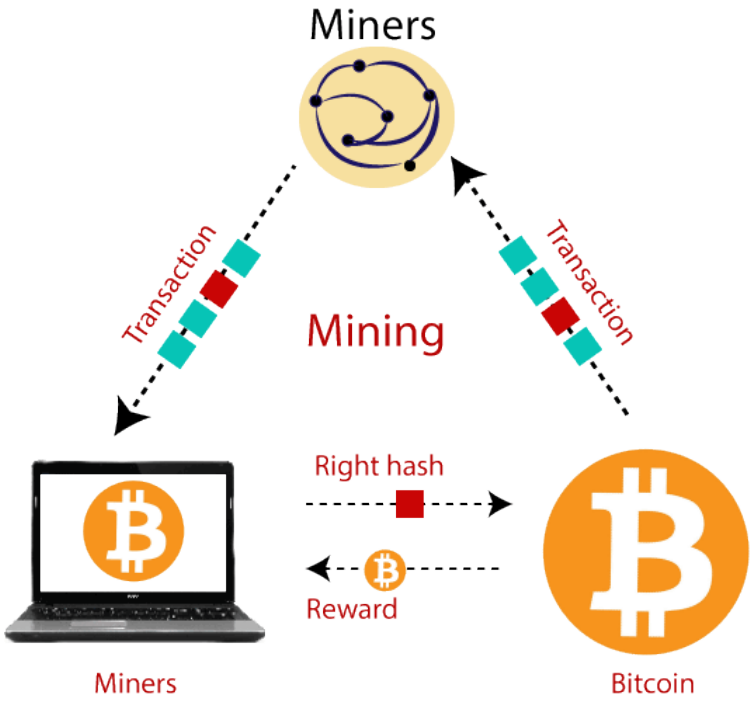


Figure 1.12: Miner How It work

1.8 How does Blockchain Work ?

blockchain technologie recorded the information pertaining to the transaction on a digital ledger called block, each block linked with the previous block with hash ,one block containing a number of transactions , This technology provides a decentralized and unchanging data

storage system that can be used in a network of users. It can act as a shared ledger that records all transactions. when block added to the chain is given an exact timestamp [27].

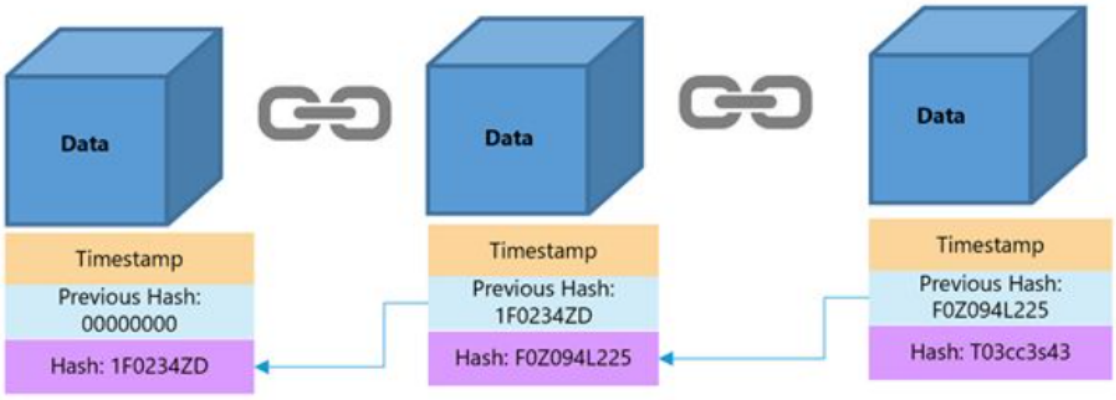


Figure 1.13: Blockchain Structure

there is two type of nodes , the first type is the miners that create new blocks and mint cryptocurrency (coins), the second type is the signers who validate and digitally sign the transactions. to make decision of which node will append the next block to the blockchain in every network This decision is made using a consensus mechanism. the steps transactions and creates and adds blocks to grow the blockchain :

1. **Transaction is initiated :** In a blockchain system, a node initiates a transaction by creating and digitally signing it using its private key. Transactions can represent different actions within the blockchain network, with the most common being the transfer of value between users. The transaction data structure typically includes information such as the transfer logic, rules, source and destination addresses, and validation details. Transactions can involve cryptocurrency transfers or the execution of smart contracts, enabling various desired operations. Ultimately, a transaction takes place between two or more parties involved in the blockchain network.

2. **Transaction is validated and broadcast :** Once a transaction is created, it is shared with other peers in the network through data-dissemination protocols like the Gossip protocol. These peers validate the transaction based on predetermined criteria for its validity. Before the transaction is broadcasted, it undergoes a verification process to ensure that it meets the necessary requirements to be considered valid by validators or miners .

3. **Find new block :** After the transaction is validated by miners in the blockchain network, it becomes part of a block, and the mining process commences. Referred to as "finding a new block," this process involves miners racing against each other. Their

objective is to successfully complete and add their created block to the blockchain by solving intricate mathematical puzzles.

4. **New block found :** The block is deemed "found" and finished after a miner completes a mathematical puzzle (or complies with the demands of the consensus process set out in a blockchain). The deal is now regarded as completed. As an incentive for their work and the resources they used in the mining process, cryptocurrency blockchains like Bitcoin often provide the miner who solves the mathematical problem a set amount of coins.

5. **Add new block to the blockchain:** Once a new block is created, it undergoes validation, and the transactions or smart contracts contained within it are executed. The block is then shared with other peers in the network, who also validate and execute its contents. At this point, the block becomes a permanent part of the blockchain or ledger. The subsequent block in the chain is cryptographically linked to this block through a hash pointer, establishing a secure connection between them.

1.9 Blockchain Variants

There are different types of Blockchain that are being used currently.

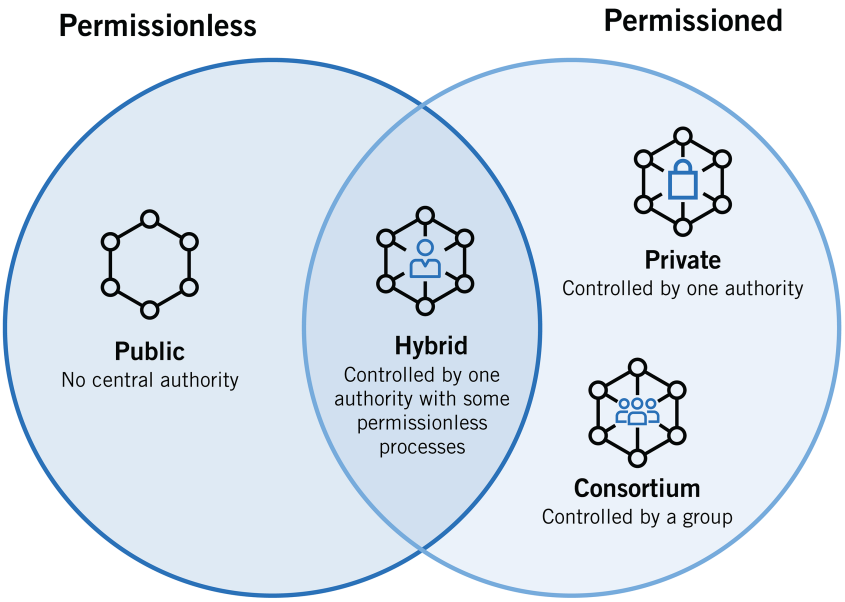


Figure 1.14: Blockchain Types

1.9.1 Public Blockchain

A public blockchain is completely decentralized,does not have a single entity that controls the network, anyone with an internet connection can join the network by create personal address and participate become a 'node' of the network and can reading, writing, or auditing within the Blockchain.from anywhere to input data and transactions and review them as long as they are connected to the network . examples of a public blockchains are Bitcoin and Ethereum blockchains . [59]

1.9.2 Private Blockchain

A private blockchain or managed blockchain , is a centralized system that uses distributed ledger technology because its blockchains controlled by a single organization the central authority in private blockchain determines who can be a node. The central authority also does not necessarily grant each node with equal rights to perform functions. Some examples of private blockchains are the business-to-business virtual currency exchange network Ripple and Hyperledger, an umbrella project of open-source blockchain applications [59]. Consortium and hybrid blockchains were created as a response to the disadvantages present in both public and private blockchains. Public blockchains usually

have extended validation periods for new data, while private blockchains are more susceptible to fraudulent activities and malicious entities

1.9.3 Consortium Blockchain

Consortium blockchains are governed by a group of organizations, making them permissioned blockchains, in contrast to private blockchains which are controlled by a single entity.[50] This decentralized approach provides consortium blockchains with higher levels of security compared to private blockchains.

1.9.4 Hybrid Blockchain

A Hybrid Blockchain a combination of both public blockchain and private blockchain. Simply put, a hybrid blockchain provides controlled access and freedom simultaneously. The members of the hybrid blockchain can decide which of the transaction should keep private and which should be made public. Even if the transaction is private, it can not be altered or modified by members. some examples of hybrid blockchain are XinFin is a Hybrid blockchain that uses Ethereum and Quorum blockchain solutions. [32]

1.10 The Blockchain Technology Cases

additional than for the purposes of digital currency, blockchain has a wide range of additional uses. Additionally, the inclusion of smart contracts in Ethereum paved the way for a wide range of blockchain-based financial applications.

- **Charity donate :** A cryptocurrency payment is a digital transaction in which a cryptocurrency, such as Bitcoin, Ethereum, or Litecoin, is used to buy products or services. Unlike typical payment methods like credit cards or bank transfers, cryptocurrency payments are decentralized, which means they are not processed by a centralized authority like a bank or government. [21]
- **Supply chain Management :** there is many obstacles in supply chain system and face numerous challenges in terms of transparency and efficiency. Throughout the whole supply chain, from production to distribution to final consumers, blockchain technology can offer real-time visibility and product tracking of commodities and products. As a result, there is more openness and trust among the various supply chain participants. [21]
- **Healthcare :** Blockchain technology has the potential to transform the healthcare industry by increasing healthcare data security, privacy, and efficiency.

- **Governance :** Blockchain technology can be used to bring more democratization, fairness, and security to the governance of various sectors. As a potential solution to eliminate voting fraud and the need for trust during elections or constitutional processes, blockchain-based systems can offer a transparent and immutable way of tracking voting results. Moreover, blockchain can also be used to combat corruption, enhance data integrity, and improve traceability in various scenarios, including tax collection and financial aid distributions. [21]

- **Internet of Things (IoT) :** The combination of blockchain technology and the Internet of Things (IoT) has the potential to completely transform how gadgets communicate and share data. IoT devices may share data in a more efficient, transparent, and secure manner by leveraging the safe and decentralized features of blockchain. Blockchain can be used to trace the flow of items in the supply chain, automate the execution of smart contracts between devices, securely and transparently share data, enable peer-to-peer energy trading, and manage the ownership and whereabouts of assets, to name a few applications. Overall, the combination of blockchain and IoT has the potential to open up new avenues for secure, decentralized, and automated communication and data exchange between devices, potentially altering how we engage with technology in our daily lives.

- **Payment solutions and dApps :** A cryptocurrency payment is a digital transaction in which a cryptocurrency, such as Bitcoin, Ethereum, or Litecoin, is used to buy products or services. Unlike typical payment methods like credit cards or bank transfers, cryptocurrency payments are decentralized, which means they are not processed by a centralized authority like a bank or government.

1.11 Cryptocurrency

Cryptocurrencies are digital or virtual currencies underpinned by cryptographic systems to secure online payments without the use of third-party intermediaries. Cryptocurrencies using a decentralized system based on blockchain to record transactions and issue new units. generally not issued by any central authority are generated through a mining process [31] . The growth of the digital currency market and the large number of its transactions forced us to study it , The total crypto market volume over the last 24 hours is 47.44B$, which makes a 78.32% increase. The total volume in DeFi is currently 3.79B $, 7.99% of the total crypto market 24-hour volume. The volume of all stable coins is now 42.88B$, which is 90.38% of the total crypto market 24-hour volume [24].Cryptocurrency Prices, Charts And Market Capitalizations — CoinMarketCap There are many cryptocurrencies being created and used for specific purposes like bitcoin , ethereum , litecoin , ripple , xrp . . .

Figure 1.15: Crypto Projects

1.11.1 Cryptocurrency Evaluation

Cryptocurrency evaluation refers to the process of assessing and determining the value of digital currencies such as Bitcoin, Ethereum, or other cryptocurrencies. Evaluating cryptocurrencies involves analyzing various factors and metrics to understand their potential value, market trends, and investment prospects.

1.11.1.1 The First Cryptocurrency

The first appearance of Cryptocurrency in eCash developed by DigiCash company created by David Chaum's in 1990 , the idea of using cryptography is to secure and verify transactions goes back several decades , ecash it is not considered only an attempt to work on crypto but there are many attempts such as :

- **E-Gold :** Douglass Jackson, Barry Downey, and Reid Jackson developed the electronic gold system (E-Gold) in 1996. An early instance of a digital currency backed by actual gold housed in vaults throughout the world is E-Gold. All transactions in the E-Gold system were processed through a single central server run by the E-Gold corporation because it was a centralized system. On the E-Gold website, users could register for accounts and use those accounts to send money to other users all over the world. [45]
- **Bit Gold :** Bit Gold was never fully implemented it is considered to be an important precursor to modern digital currencies like Bitcoin . Nick Szabo suggested Bit Gold, a decentralized digital money with gold backing, in 1998. To verify transactions and stop fraud, the system employed a peer-to-peer network and a proof-of-work mechanism. The system was entirely backed by gold since each transaction involved computer labor

equivalent to the quantity of gold moved. The objective was to make Bit Gold more valuable and reliable than other digital currencies by creating a "digital scarcity" as a result of the computational labor necessary for each transaction. Despite its incomplete implementation, Bit Gold is regarded as a crucial forerunner to contemporary digital currencies like Bitcoin.[45]

- **B-Money :**

  B-money is a "anonymous, distributed electronic cash system" that was suggested in 1998 by developer Wei Dai. Dai proposed two distinct protocols, one of which needed an unjammable and synchronous broadcast channel. B-money was never successful in the end and had several differences from Bitcoin. However, it was also an effort at a private, secure, and anonymous electronic payment system.[45]

- **Hashcash :**

  Hashcash, a digital currency created in the middle of the 1990s and used before bitcoin, was among the most popular. Hashcash was created to stop DDoS assaults and reduce email spam, among other things. [33]

  All these digital currencies were forgotten after the appearance of Bitcoin , bitcoin resolved two fundamental mathematical problems :

  - **Double spending problem**
  - **Buzantian problem**

1.12 Cryptocurrency Problems

1.12.1 Double spending problem

When it comes to digital cash, ensuring that specific units can't be duplicated is of paramount importance. The entire system would be undermined if Alice could receive 10 units, copy-and-paste them 10 times, and find herself in possession of 100 units. Similarly, such a scheme can't work if she can send the same 10 units to both Bob and Carol simultaneously. So, for digital money to function, there must be mechanisms in place to prevent this behavior. Bitcoin is carefully designed to prevent double-spending attacks, at least when the protocol is used as expected. That is, if individuals wait for transactions to be confirmed in a block, there is no easy way for the sender to undo it. To do so, they would need to "reverse" the blockchain, which requires an unrealistic amount of hashing power. [19]

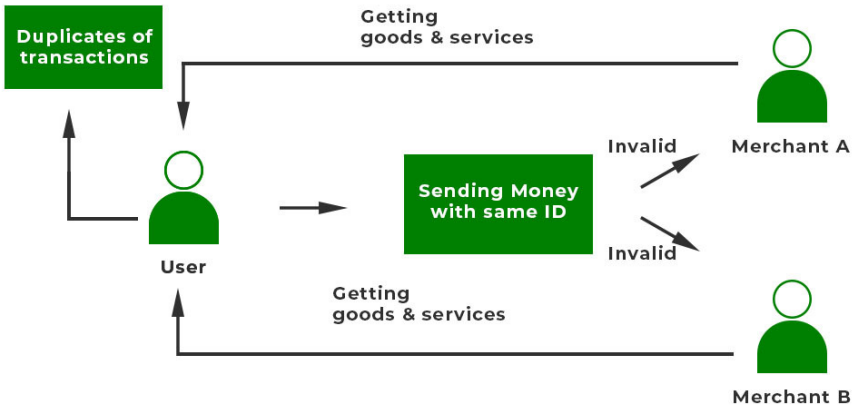


Figure 1.16: Double spending problem

1.12.2 Byzantine Problem

The Byzantine Generals' Problem, conceptualized in 1982, is a logical challenge that demonstrates communication difficulties among a group of Byzantine generals attempting to agree on their next action. The scenario assumes that each general commands an army positioned at various locations surrounding the target city. The generals must reach a consensus on either attacking or retreating, with the specific decision being less important than achieving unanimous agreement for coordinated execution. [9]

In the context of blockchains, the Byzantine Generals' Problem can be likened to network nodes, where each general represents a node. In this scenario, the nodes must achieve consensus on the system's present state. In simpler terms, the majority of participants within a decentralized network must agree and take the same action to prevent a total breakdown.

Byzantine fault tolerance (BFT) system is able to continue operating even if some of the nodes fail or act maliciously. there are different approaches for a blockchain to achieve Byzantine fault tolerance and this leads us to the so-called consensus algorithms . [20]

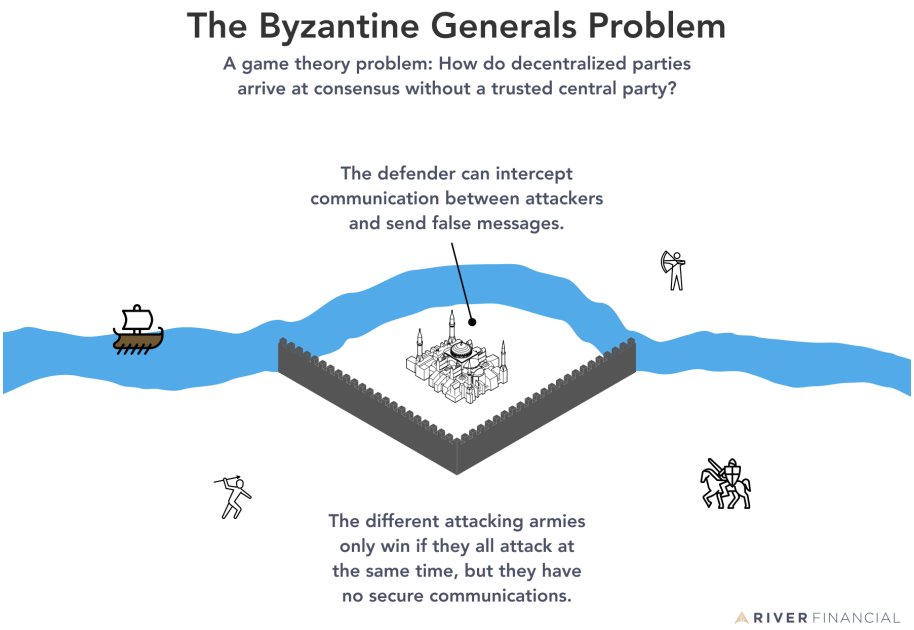


Figure 1.17: Byzantine Generals Problem

1.13 Blockchain Frameworks :

Blockchain frameworks are software platforms or architectures that provide a foundation for building and deploying blockchain applications. These frameworks offer developers a set of tools, protocols, and libraries that simplify the development process and enable the creation of decentralized applications (DApps) on top of a blockchain network.

1.13.1 Bitcoin

Bitcoin is a decentralized digital currency and the first cryptocurrency to gain widespread recognition and adoption. It was created in 2009 by an anonymous individual or group of individuals using the pseudonym Satoshi Nakamoto. Bitcoin operates on a peer-to-peer network called the blockchain, which records all transactions made with the currency [17].

1.13.1.1 Bitcoin Transaction

A transaction within a network signifies that the current owner of a certain value of Bitcoin has granted permission for that value to be transferred to a new owner. This transfer enables the new owner to utilize the Bitcoin by initiating another transaction, thereby authorizing its transfer to yet another owner. This cycle of ownership continues in a sequential manner, forming a chain of transactions.the valid transaction must be signed by the sender using their private key , Bitcoin does not have accounts. Instead, pieces of Bitcoin of arbitrary size are all associated with an address, which is controlled by the owner of that bitcoin. These pieces of Bitcoin are called Unspent Transaction Outputs (UTXOs).

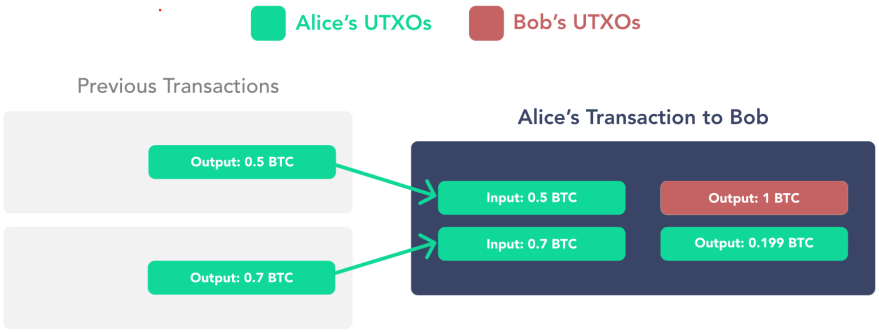


Figure 1.18: UTXO In Transaction

Transactions in a UTXO-based blockchain consist of inputs and outputs. Inputs refer to the UTXOs being spent, while outputs outstanding unspent "coins." A transaction consumes one or more existing UTXOs as inputs and generates new UTXOs as outputs, which are then added to the UTXO set. This process maintains the conservation of value within the system. [8]

1.13.1.2 Cryptographie and Hashage in Bitcoin

Cryptography and hashing it is the cornerstone of this technique and used many times . Bitcoin use SHA-256 hashing algorithm and asymmetric cryptography

- **SHA-256 hashing algorithm :** is a cryptographic hashing algorithm utilized to ensure the integrity of messages, files, and data. It belongs to the SHA-2 family of hash functions and employs a 256-bit key to transform a given piece of data into a fixed-length, unrecognizable data string. This resulting hash value, consisting of a combination of random characters and numbers, is also 256 bits in length [58].
- **Asymmetric Cryptography :** is a process that uses a pair of related keys private key public key to encrypt and decrypt a message and protect it from unauthorized access or use . public key is for everyone and can encrypts data, private key must be kept secret is used to decrypts data .

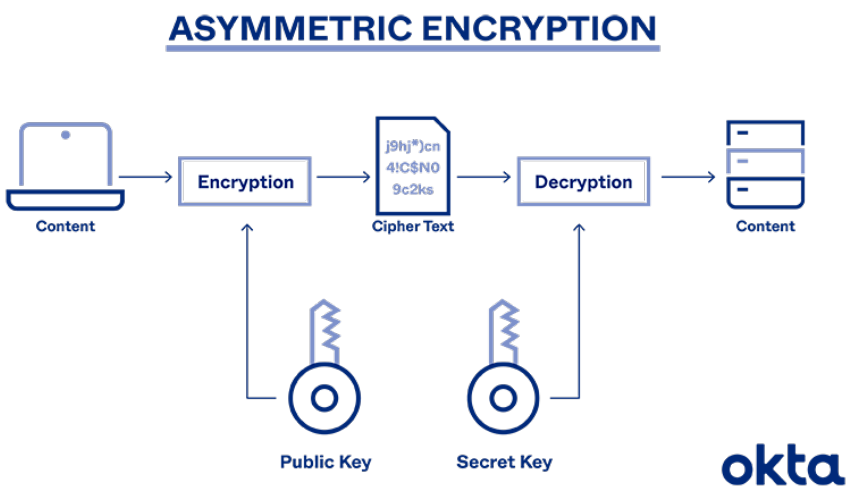


Figure 1.19: Asymmetric Cryptography

1.13.1.3 Bitcoin Addresses

A bitcoin address is a distinct alphanumeric identifier used for receiving bitcoin to your wallet. it's like : `1LMcKyPmwebfygoeZP8E9jAMS2BcgH3Yip`

we have two types of address Pay-to-PubkeyHash and Pay-to-ScriptHash , public key is not the same with bitcoin address , to generate it we see Figure 1.20

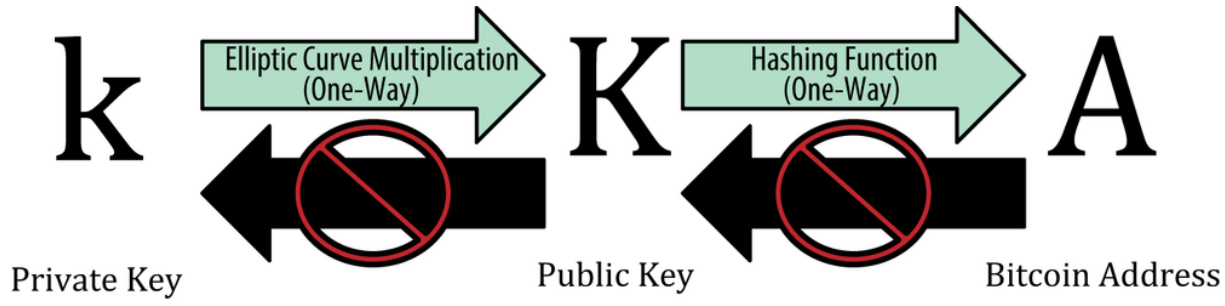


Figure 1.20: Private key, public key, and bitcoin address

- **Private Key :** A private key is simply a number, picked at random and is used to create signatures that are required to spend bitcoins by proving ownership of funds used in a transaction.[17].
- **Public Key :** The public key is calculated from the private key using a mathematical function known as "elliptic curve multiplication" , it is a cryptographic code that is used to encrypt messages and verify digital signatures. A public key is visible to anyone and can be shared with others to receive cryptocurrency payments. [56]
- **Bitcoin Address :** A bitcoin address is a string of digits and characters that can be shared with anyone who wants to send you money. The bitcoin address is derived

from the public key by hashing function . Starting with the public key K, we compute the SHA256 hash and then compute the RIPEMD160 hash of the result:

```
A = RIPEMD160(SHA256(K))
```

1.13.1.4 Merkle Trees

Merkle Trees is data structure used for serve to encode blockchain data more efficiently and securely. Merkle Trees are binary trees containing cryptographic hashes [17].

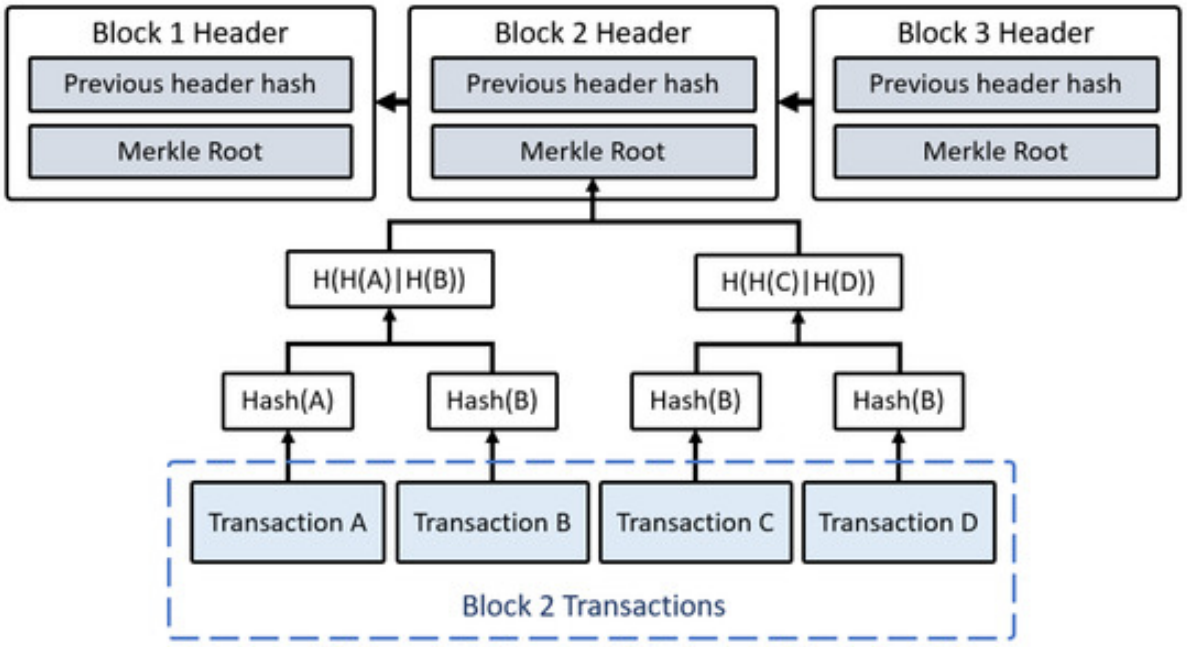


Figure 1.21: Private key, public key, and bitcoin address

Merkle trees are utilized in Bitcoin to create a compact representation, known as a digital fingerprint, of all the transactions within a block. This allows for efficient verification of whether a transaction is part of a specific block. The construction of a Merkle tree involves repeatedly hashing pairs of nodes until only one hash, called the merkle root, remains. In Bitcoin, the cryptographic hash algorithm SHA256 is applied twice (double-SHA256) to create the hashes used in the merkle tree [17].

1.13.1.5 Bitcoin Minning & Consensus

In Bitcoin, mining is the process of verifying and adding new transactions to the blockchain. Miners compete to solve a computational puzzle called proof-of-work, which involves finding a specific number (nonce) that, when combined with the block data, produces a hash value that meets certain criteria. The miner who solves the puzzle first is rewarded with newly created Bitcoins and transaction fees.

Consensus , where the longest valid chain is considered the correct version of the blockchain. Nodes independently validate incoming blocks, and forks are resolved by extending the chain with the most accumulated proof-of-work. Mining and consensus ensure the security, integrity, and decentralized operation of the Bitcoin network

1.13.2 Ethereum

Ethereum is a blockchain with a computer embedded in it. It is the foundation for building apps and organizations in a decentralized, permissionless, censorship-resistant way.[**?**] Vitalik develop ethereum from a more practical perspective, Ethereum is an open source, globally decentralized computing infrastructure that executes programs called smart contracts. It uses a blockchain to synchronize and store the system's state changes, along with a cryptocurrency called ether to meter and constrain execution resource costs [16] . The original goal of Ethereum was to create a general-purpose blockchain that could be customized for a number of applications. However, Ethereum's ambition swiftly grew to include a DApp development platform and organizations.[16] hold assets, transact, and communicate without being controlled by a central authority. Ethereum uses the Proof of Stake (PoS) consensus mechanism [3] .

1.13.2.1 Accounts in Ethereum

Account are basic units of ethereum protocol , there are two types of accounts in Ethereum: externally owned accounts and contract accounts. **externally owned accounts (EOA) :** are similar to Bitcoin private/public key pairs. In both models, the address and public key are associated to a private key via an Elliptic Curve Digital Signature. controlled by anyone with the private keys. **Contract Accounts :** is owned and controlled by a piece of code known as the smart contract instead of an entity. However, they still rely on EOA to deploy it and execute their functions.

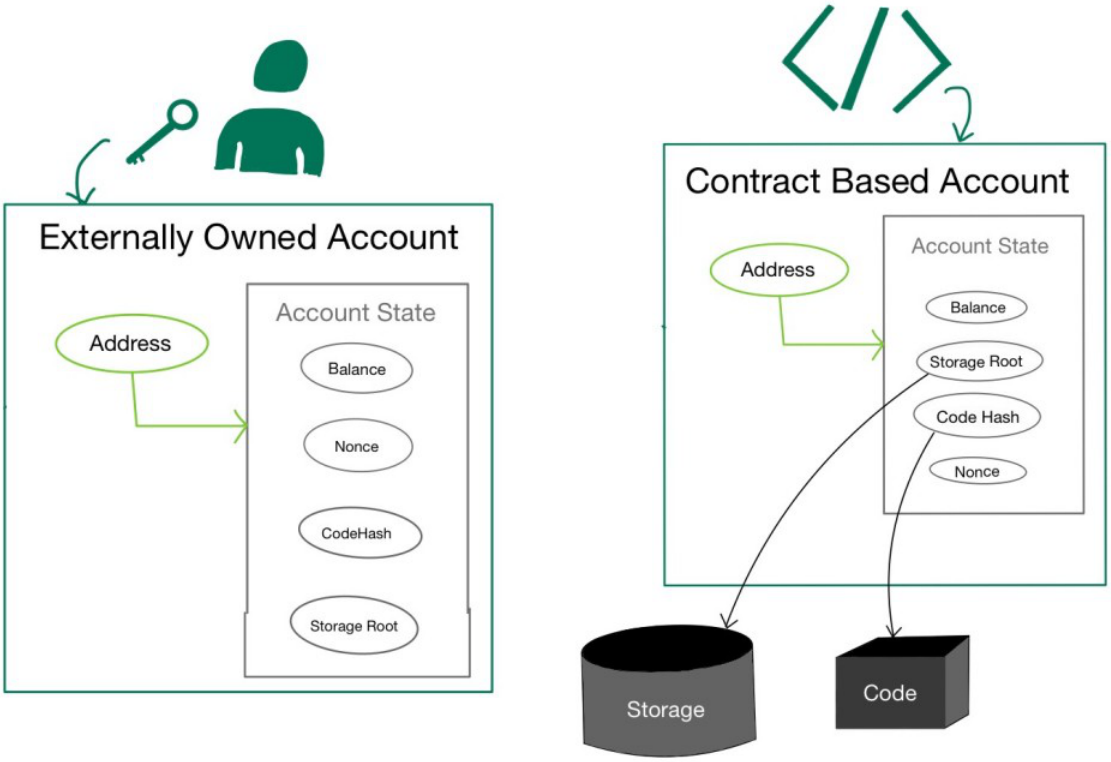


Figure 1.22: Ethereum Accounts

1.13.2.2 Ether in Ethereum

Ether is currency unit for ethereum network

1.13.2.3 Evm (Ethereum Virtual Machine)

The Ethereum Virtual Machine (EVM) is the computational engine responsible for managing the state of the Ethereum blockchain and enabling the execution of smart contracts. It is an integral part of the client software (such as Geth or Nethermind) required to operate an Ethereum node. Nodes in the Ethereum network store transaction data, which is processed by the EVM to update the shared ledger. The EVM is native to Ethereum nodes, as it is implemented within the client software to provide this essential functionality [28].

2

Chapter Two

In this Chapter we will discuss about supply chain management of sensitive products like drugs and tracking it from the manufacturer to the consumer

2.1 Introduction

Today, sensitive products supply chains are an essential part of the global economy. They play a vital role in the transportation of goods such as food, pharmaceuticals, and medical equipment. The effective management of sensitive products supply chains is essential to ensure the safety and quality of these goods, and to protect the health and well-being of consumers around the world. The pharmaceutical supply chain is a complex system that involves many stakeholders, from raw material suppliers to patients. It is essential to ensure that this chain is secure and efficient in order to deliver safe and effective medicines to those who need them.There are a number of risks and challenges that can impact the pharmaceutical supply chain. These include counterfeit drugs, product recalls, and disruptions to transportation and distribution and drugs theft. In a health-conscious society, it is more important than ever to manage these risks effectively in order to protect patients. [42]

2.2 Supply Chain Definition :

Supply chains are all activities related to the flow and manufacture of finished products from suppliers to the final consumer, in addition to the flow of information, both of which take place in both directions from suppliers to customers and vice versa. supply chain management includes transport companies, warehouses, retailers and consumers themselves (depending on logistical flows).It includes also new product development, marketing, distribution operations, financing, and customer service.

Figure 2.1: Supply Chain Management Flow.

2.2.1 Supply Chain Management :

Supply chain management (SCM) is defined as a set of methodologies used to effectively complement suppliers, manufacturers, warehouses and stores so that goods are produced and distributed in the right quantities to the right locations, and at the right time so that the total system cost is as low as possible while maintaining service level requirements. The goal or mission of supply chain management can be defined using Mr. Goldratt's words as "Increase throughput while simultaneously reducing both inventory and operating expense." there are five areas where companies can make decisions that will define their supply chain capabilities: Production; Inventory; Location;Transportation; and Information. these areas as performance drivers that can be managed to produce the capabilities needed for a given supply chain .[52]

- Production : The production plan guides the movement of raw materials to the production area. The raw materials are utilized in manufacturing the finished products as per customer orders. Once manufactured, the finished products are transferred to the warehouse where they are stored until they are ready for shipping.
- Inventory : The raw materials are received from the suppliers, checked for quality and accuracy, and moved into the warehouse.
- Location : People can add details about their business on the map.

- Transportation : the shipping department determines the most efficient method to ship the products so they are delivered on or before the date specified by the customer.
- Information : Information facilitates coordination, visibility, and decision-making throughout the entire supply chain.

2.2.2 How does SCM work ?

The success of SCM lies in the effective management of activities, information, and resources across the supply chain to ensure the smooth flow of products, from sourcing raw materials to delivering finished goods to customers. By recognizing the interdependencies and relationships between organizations, SCM aims to optimize efficiency, minimize costs, enhance customer satisfaction, and gain a competitive advantage in the market.

2.2.3 Supply Chain Management Processes

The supply chain management process plays a huge importance in running the main operations of almost every organization. For many decades, supply chains have evolved from being very simple to ones based on newly developed algorithms and using new technologies such as blockchain. With supply chain concepts constantly evolving, the supply chain management process has become a dedicated job. Supply chain managers are responsible for ensuring that the supply chain, whether external or internal, is both efficient and cost-effective. But the other question that arises is how do they do it? The mechanism to be followed for an effective supply chain management process includes five basic phases which are explained here. [36],

Figure 2.2: Supply Chain Management Process Phases.

2.2.3.1 Planning

Planning establishes parameters within which a supply chain will function over a specified period of time. In the planning phase, companies must include uncertainty in demand, exchange rates, and competition over this time horizon in their decisions. Given a shorter time frame and better forecasts than in the design phase, companies in the planning phase try to incorporate any flexibility built into the supply chain in the design phase and exploit it to optimize performance. As a result of the planning phase, companies define a set of operating policies that govern short-term operations. [53]

2.2.3.2 Source

sourcing is the choice of who will perform a particular supply chain activity such as production, storage, transportation, or the management of information. [53],The goal is to strike a balance between in-house and outsourced functions to achieve a responsive, efficient, and competitive supply chain.

2.2.3.3 Manufacturing

Manufacturing process can include various activities, including converting raw materials into finished goods, as well as repackaging, recombining, bundling, assembling, processing or grading. It is necessary to improve this process to reduce variations in results, increase predictability and reduce non-conformance to customer requirements. Continuous improvement is essential to optimizing the manufacturing process for the need to compete and satisfy the customer, even in highly advanced automated production lines.[51]

2.2.3.4 Delivering

delivery. The delivery channel must be able to withstand sudden surges in demand and have business continuity measures in place for common logistical problems such as port congestion or bad weather. In many organizations, the supply chain function is of low priority when compared to the sales function, yet it must be given funding to improve itself to keep pace with business needs and differentiate. [51]

2.2.3.5 Returning

In many cases, the customer would like to return the product for a variety of reasons, such as damage, non-conformity to quality specifications, defective products, products that are close to expiry dates or previous ones, or wrong products / quantities shipped, and the return process and dealing with it is a crucial element for the company to gain a reputation good . [51]

2.2.4 Decision Phases in a Supply Chain

Supply chain management involves coordinating all stages of a product's life cycle, from the procurement of raw materials to the final delivery to the end-user [44]. Successful supply chain management requires decisions on the flow of information, product, and funds that fall into three decision phases. These decision phases are:

2.2.4.1 Supply Chain Strategy

The company decides how to structure the supply chain over the long term. Decides what the configuration of the chain will be, how resources will be allocated, and what operations each stage will perform. The strategic decisions that companies make include outsourcing or internalizing a function in the supply chain, the location and capacity of production and warehousing facilities, the products to be manufactured or stored in different locations, the modes of transportation that will be available along the different shipping legs, and the type of information system to be used. [43]

2.2.4.2 Supply Chain Planning

Supply Chain Planning (SCP) sets the boundaries in which a supply chain will operate during a defined timeframe. During the planning stage, companies need to consider factors such as demand uncertainty, exchange rate fluctuations, and competitive dynamics when making decisions for this duration. The objective of planning is to optimize the surplus generated by the supply chain within the planning horizon, taking into account the constraints set during the strategic or design phase.[53]

2.2.4.3 Supply Chain Operation

Supply chain execution (SCE) focuses on maximizing the utilization of available assets, controlling costs, and ensuring timely and accurate delivery of products to customers. It relies on effective information management and communication, as well as the ability to address exceptions and disruptions that impact the balance between supply and demand. Supply chain managers must track the movement of goods, identify bottlenecks, and make decisions to optimize operations, such as rerouting products, adjusting workforce and machinery allocation, and modifying production or supplier orders .

2.3 Sensitive Products Supply Chain

The supply chain for dangerous products, particularly in the pharmaceutical industry, operates within a unique and complex framework. This is due to the inherent risks and regulatory requirements associated with these items, which demand stringent controls and meticulous oversight to ensure safety, security, and compliance. Managing pharmaceutical supply chains presents several complexities in the context of a health-conscious society, as it involves numerous components and stakeholders working together to efficiently deliver life-saving medicines to patients.

2.3.1 Pharmaceutical Drugs Supply Chain

Providing access to essential medicines is especially important during times of crisis such as pandemics, when health systems are strained and demand for rescue equipment increases. Effective drug management plays an important role in meeting these important needs.[22] Pharmaceutical supply management encompasses a comprehensive set of activities, including purchasing, purchasing, storage, distribution and delivery of pharmaceuticals. It includes important functions such as demand forecasting, raw material management, inventory management, production and storage, distribution management, logistics and product risk management. The success of pharmaceutical product management requires effective coordination and collaboration among suppliers, ultimately improving the strength and efficiency of the entire supply chain. Ensure healthcare systems meet patient needs and wants at critical times by implementing robust drug supply management systems that ensure access to essential drugs despite challenges.[2]

Figure 2.3: Pharmaceutical Supply chain

According to a recent report by the World Health Organization (WHO), drug

counterfeiting has emerged as a global issue. Particularly in low- and middle-income countries, it is estimated that approximately one in every ten drugs circulating in the market is either counterfeit or of poor quality. The utilization of such substandard products can have detrimental effects on the mortality rate. [40]

2.3.2 Pharmaceutical Supply Chain Strategies

The state plays an important role in the drug supply chain as the regulator of the bodies responsible for drug registration and issuance of licenses for their production, as well as the sale and issuance of prescriptions.[46] The pharmaceutical supply chain includes a set of strategies to ensure that medicines are transported effectively and efficiently from manufacturers to end users. The following are some of the main strategies used in pharmaceutical supply chain management:

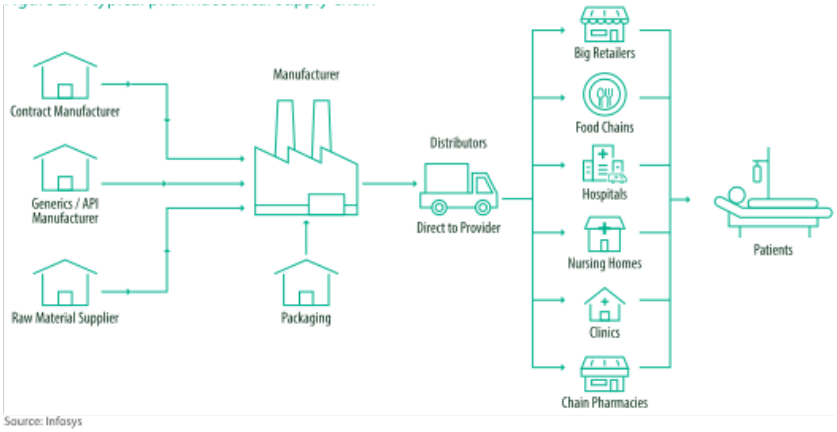


Figure 2.4: Pharmaceutical Supply chain Strategies

- **Pharmaceutical Manufacture :** The objective of pharmaceutical manufacturers is to meet the demand of the pharmaceutical sector by providing a diverse range of finished products. They undertake the responsibility of distributing medications from their facilities to drug wholesalers or directly to different types of pharmacies. These pharmacies encompass retail chains, mail-order and specialty pharmacies, hospital chains, as well as specific health plans.[38]
- **Pharmaceutical Inventory :** Effective management of pharmaceutical Inventory is critical to maintaining a steady supply of medicines to operating units and patients while minimizing wastage of medicines and financial loss. The latter include controlling inventory transactions, ordering, receiving, storing, issuing, and reordering medicines. Tracking is essential to keeping vital and commonly used medications close at hand while monitoring the use of addictive and harmful medications. Drug inventory management software is available to track orders, monitor the supply and

use of stocked medications, and facilitate the needs of both pharmacist and patient. [55]

- **Pharmaceutical Distributing Products :** Pharmaceutical distributors act as intermediaries between drug manufacturers and healthcare providers, ensuring that drugs reach patients in a timely and efficient manner. Their responsibilities include sourcing products from manufacturers, managing inventory, warehousing, and logistics, as well as delivering pharmaceutical products to pharmacies, hospitals, clinics, and other healthcare facilities. Drug distributors also comply with regulatory requirements, maintain product integrity, and implement quality control measures to ensure the safe and reliable distribution of pharmaceutical products throughout the healthcare system.
- **Pharmaceutical Retailer :** Drug retailers are establishments that specialize in selling drugs and healthcare products directly to consumers. Drug retailers are responsible for maintaining proper licensing, following regulations and guidelines related to the sale and distribution of drugs, ensuring product quality and safety, and providing accurate drug information to customers.

2.4 Traditional Pharmaceutical Supplychain Challenges

The traditional pharmaceutical supply chain faces a range of challenges, including lack of transparency, difficulty tracking products, lack of trust, and the shipment of expired products [48] , and counterfeit drugs and some common problems like :

- **Coordination issues :** The pharmaceutical supply chain requires careful coordination and adherence to regulatory guidelines at every stage, from the provision of raw materials to the delivery of medicines to patients. [38] To ensure that drug stocks are readily available for distribution to providers and patients, pharmaceutical supply chain strategies such as collaborative planning, forecasting, and replenishment can be implemented. Thus, the policies recommended in the studies lead to a more integrated drug supply chain. Where each of them works in isolation, and this creates a state of confusion and reduces the efficiency of making appropriate decisions within the pharmacy. Where each of them works in isolation, and this creates a state of confusion and reduces the efficiency of making appropriate decisions within the pharmacy.
- **Inventory management :** Inventory in operation and with an evolving environment are exposed to a lot of issues, which can affect the productivity and profitability of the entire company. Therefore, all companies need to monitor and track changes in the

business environment and adopt responsive solutions.

- **Transportation management :** Although the global economy has become increasingly interconnected, it has not been difficult for pharmaceutical and life sciences companies to manage the transportation of the goods they depend on. Increased demand and limited supply has prompted many carriers to raise their prices dramatically. At the same time that freight rates are rising, delays and cancellations are also increasing.[11]

- **Order management :** The inability to fill medical prescriptions and to provide the necessary medicines, the poor quality of those prescriptions, and the misuse of medicines are among the negative effects of product shortages. These outcomes are documented health outcomes in terms of child mortality due to lack of treatment for cancer and poor use of antibiotics when first-line regimens are not available. The use of inappropriate regimens can contribute to the emergence of drug resistance and restriction of treatment options. In addition to the use of the second and third lines, the costs of these treatment regimens are often high. [61]

- **Drug expiration :** Pharmacies and drug stores suffer from the lack of an effective and strong mechanism to determine or know the approaching expiry date of medicines.which prevents warehouse and pharmacies officials from taking the necessary measures regarding these medicines that are close to expiring.

- **Temperature control :** Contamination can occur when products are stored or transported at temperatures too high or too low. Temperature monitoring allows cold supply chain companies to monitor the temperature and humidity of the storage environment, ensuring that products remain uncontaminated throughout the supply chain .[13]

- **Tracking :** Tracking medicines is very important for all parties in the supply chains, and this is to know the time and place of medicines and the quantity and hold the bearer accountable every time .

- **Geopolitical tensions :** The war between Russia and Ukraine and the resulting sanctions against Russia have made managing the pharmaceutical and life sciences supply chain more difficult. While Russia is not a major exporter of pharmaceutical products, the sanctions imposed on the country have forced many pharmaceutical companies to cut ties with Russian suppliers. But the biggest impact of the war in Ukraine is its impact on energy costs. Russia is one of the largest oil and natural gas exporters in the world. Losing access to this market for pharmaceutical companies is a major blow to an industry with exceptionally high energy consumption. [11]

2.4.1 Drug Supply Chain in Algeria

Algeria is considered one of the developing countries that relies on importing drugs from foreign countries, which leads to a shortage of coverage in the country. This has pushed Algeria to develop the local drug production sector by improving and facilitating local and foreign investment techniques. These efforts have achieved satisfactory results and a noticeable development in local companies such as Saidal , Which is the line of an ambitious strategic development plan since 2009 represented in raising the production capacity after its new units into service 130 million selling units at the present time to more than 300 million selling units by 2019 [60]. Local pharmaceutical companies have faced problems and challenges, both public and private, in protecting the supply chain of pharmaceutical products, especially sensitive drugs such as narcotics. These drugs represent most of the problems in this field, and the inability to determine responsibility for errors or their location is a significant issue. Lack of transparency, digitization, pharmaceutical fraud, compliance and regulations, rising costs, and the inability to easily identify potential disruptive events are some of the significant challenges faced by pharmaceutical supply chains. Lack of coordination in the pharmaceutical supply chain is a root cause issue that aggravates every other issue. To strengthen pharmaceutical supply chains and make the fight against global diseases more effective, measures are needed to address key areas of weakness such as human resource dependency, order management, shortage avoidance, expiration, warehouse management, temperature control, and shipment visibility.

2.5 The Utility Of Blockchain In Supply Chains

Blockchain technology can be used to build decentralized applications that do not need a central authority to verify transactions and can be directly handled by multiple parties via a peer-to-peer network. Each participant in the network has access to a shared ledger that records all transactions in immutable and cryptographic form, and there is no single owner of the network.

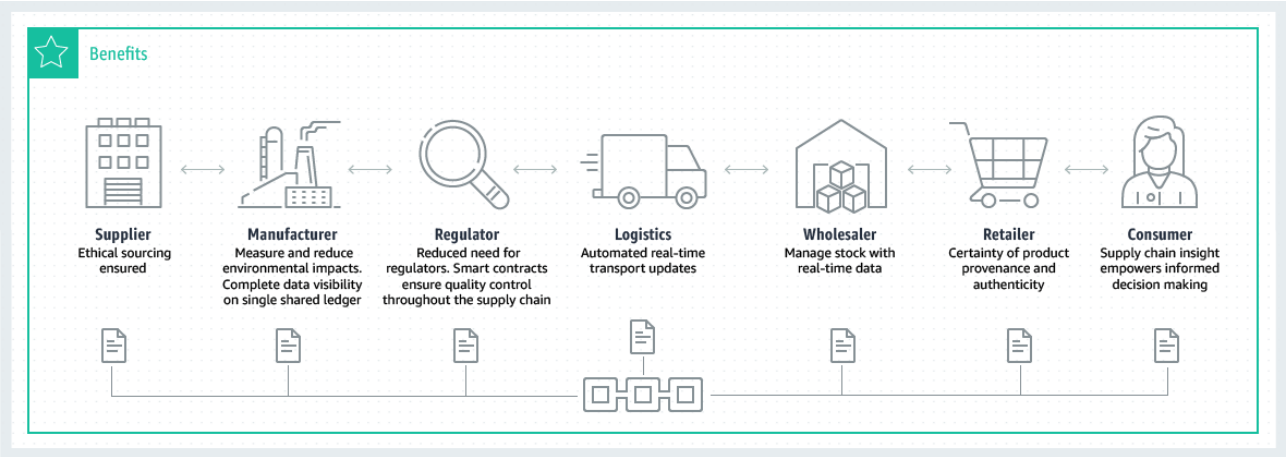


Figure 2.5: benefits of blockchain in supply chain

Blockchain technology has the potential to revolutionize the supply chain landscape through the utilization of these three compelling use cases :

- **Traceability :** In the realm of supply chain, traceability involves the meticulous task of precisely identifying the past and present whereabouts of inventory, while meticulously documenting the custody of products. This intricate process entails meticulously monitoring the intricate voyage undertaken by goods, traversing a complex labyrinth that stretches from the acquisition of raw materials to the involvement of merchants and customers, across diverse geographic zones. concerned parties can access price, date, origin, quality, certification, destination and other pertinent information using blockchain. [25]

  The adoption of cutting-edge supply chain technologies, specifically blockchain-driven solutions, bestows remarkable advantages in terms of traceability. By harnessing the power of decentralized systems and immutable data records, blockchain empowers real-time transactions and the establishment of an unyielding audit trail, thereby facilitating simultaneous visibility across the expansive expanse of the supply chain.

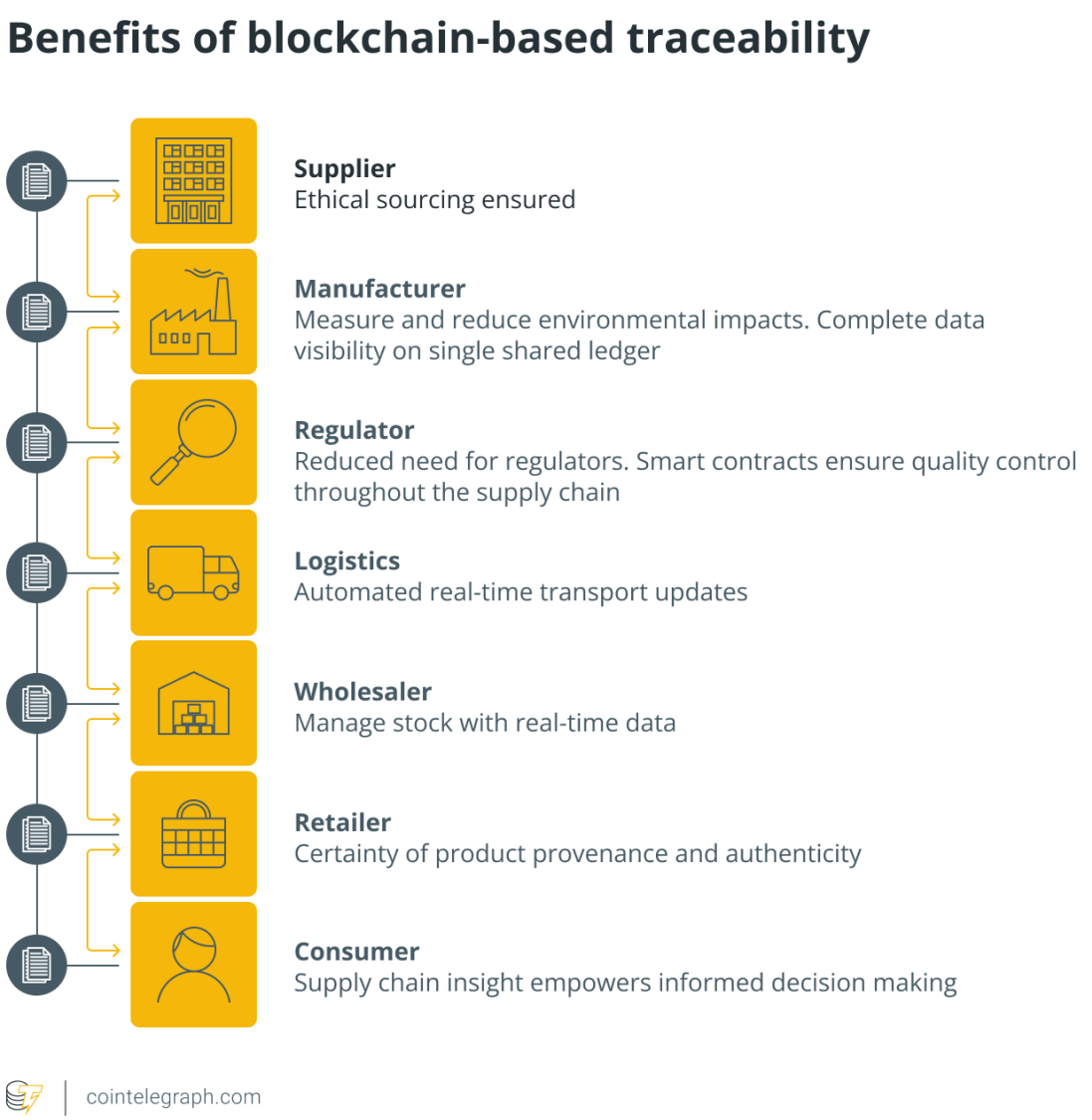


Figure 2.6: benefits of blockchain in supply chain

- **Transparency :** By using blockchain technology, trust increases between the parties to the supply chain through the availability of product information and certificates, providing open access to the public or private parties to the supply chain, and validating transactions from an external party, and they can be updated and validated in real time. enabling stakeholders to track and trace products, transactions, and information throughout the supply chain.

- **Tradeability :** Tradeability revolutionizes the traditional notion of marketplaces by introducing a groundbreaking blockchain solution. Leveraging the power of blockchain technology, it enables the "tokenization" of assets, dividing them into digital shares that embody ownership. Just as a stock exchange facilitates the trading of company shares, this fractional ownership model empowers tokens to represent the intrinsic value of an individual's stake in a specific asset. Remarkably, these tokens possess the remarkable trait of being readily tradeable, empowering users to transfer ownership seamlessly, all while eliminating the need for physical exchange of the underlying asset. [26]

2.5.1 Blockchain in Drugs Supply chain :

Implementing blockchain in the pharmaceutical supply chain is a complex task that requires cooperation, standardization, and integration with existing systems and ministries such as the Ministry of Health and the Ministry of Defense, due to its importance and seriousness, and preventing corruption in the product cycle.

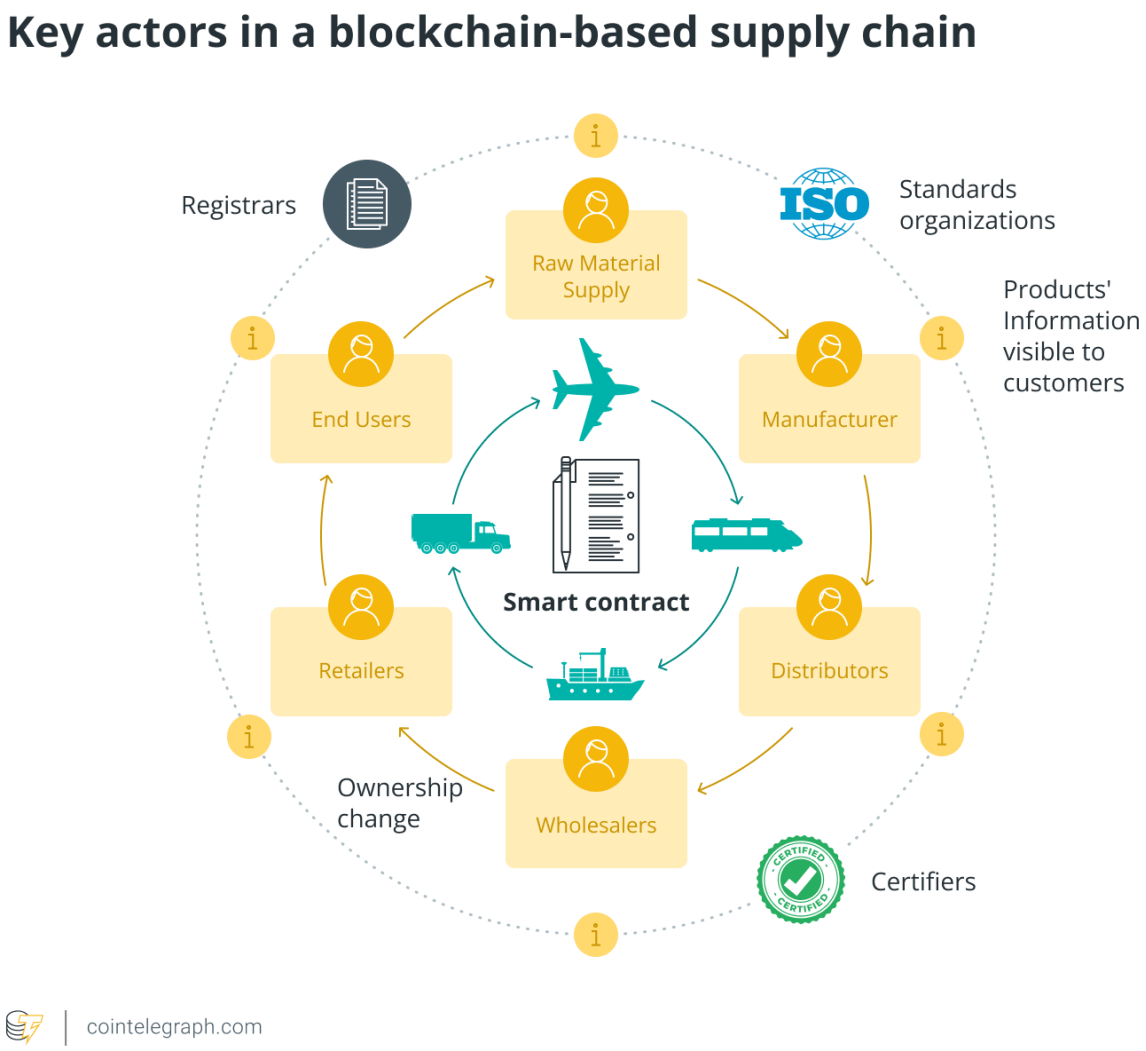


Figure 2.7:

Fortunately, blockchain technology has emerged as a viable solution to address these problems. By providing a transparent and immutable ledger, blockchain can prevent fraud and corruption by ensuring that transactions are secure, transparent, and verifiable. Additionally, smart contract conditions can be used to validate the exchange of goods or services before a product is transferred or sold to another actor, further enhancing the security and transparency of the transaction. Blockchain technology has the potential to combat fraud and corruption in various industries and improve transparency and traceability in supply chains.[30]

2.5.2 Conclusion

In the conclusion of this chapter, we delve into the definition of the supply chain and its management flow. We provide an in-depth explanation of the sensitive product supply chain, focusing specifically on pharmaceutical drugs. Furthermore, we discuss the challenges faced by traditional pharmaceutical supply chains. Lastly, we explore the utility of blockchain technology in revolutionizing supply chain management.

3

Chapter Three

Design and implementation of Blockchain in drugs supply chain .

3.1 Introduction

In this chapter, we will explore the development phase of our project. We'll define the Decentralized Application (DApp) and discuss our system design choices then We'll provide an overview of our system, including its components, interactions, and the physical and software tools used. Lastly, we'll explain the implementation of the supply chain smart contract. By the end of this chapter, you'll have a clear understanding of our development process and the key elements of our project.

3.2 Dapp (Decentralized Application)

A Decentralized Application (DApp) is an application built on a decentralized network that combines a smart contract backend and a user interface frontend. DApps are 'permissionless,' meaning anyone is free to use them. [28] Many DApps include smart contracts others have written, and they are transparent and 'trustless,' meaning anyone can verify their authenticity and functionality. DApps operate without human intervention and are not owned by any one entity, rather DApps distribute tokens that represent ownership. They can be developed for a variety of purposes including gaming, finance, and social media. DApps run on a blockchain network in a public, open-source, decentralized environment and are free from control and interference by any single authority.

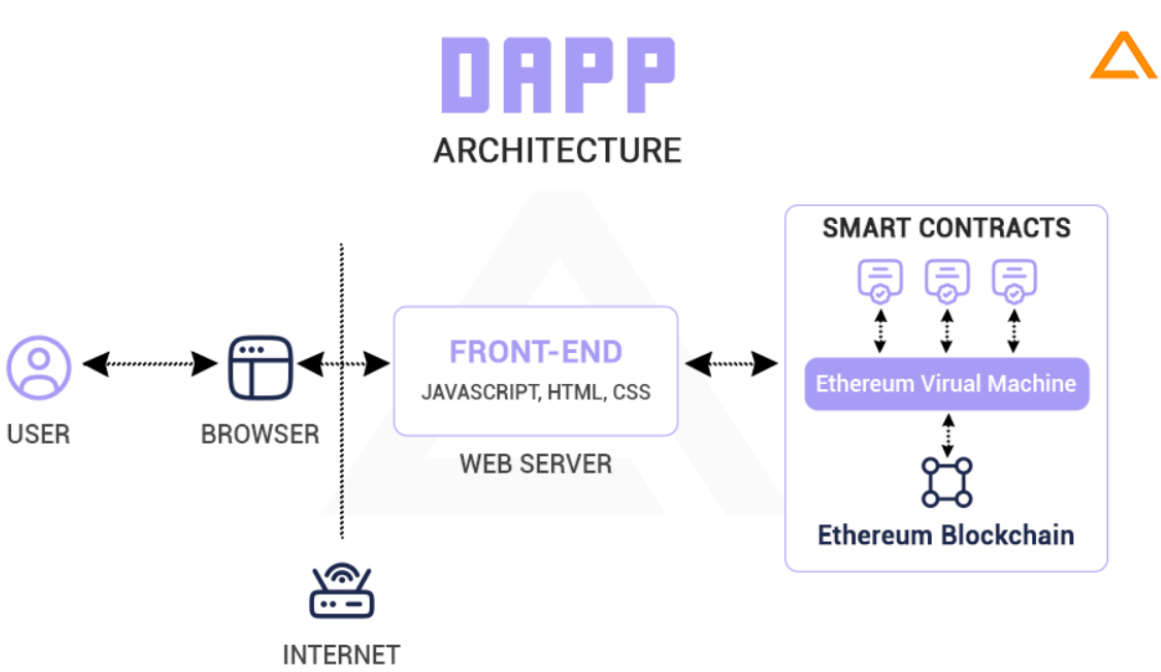


Figure 3.1: Dapp Architecture

3.3 System Design

We will choose in this section the design of blockchain system that helps solve a problem of drugs supply chain and use blockchain helpful features like traceability , security, transparency. We have selected ethereum blockchain network to work on this because of its advantages, uses and broad community, and to use smart contracts in our project to get rid of third party in scm process . Applications that do not need an intermediary or third party are called decentralized applications (Dapp) that are built on Blockchain .

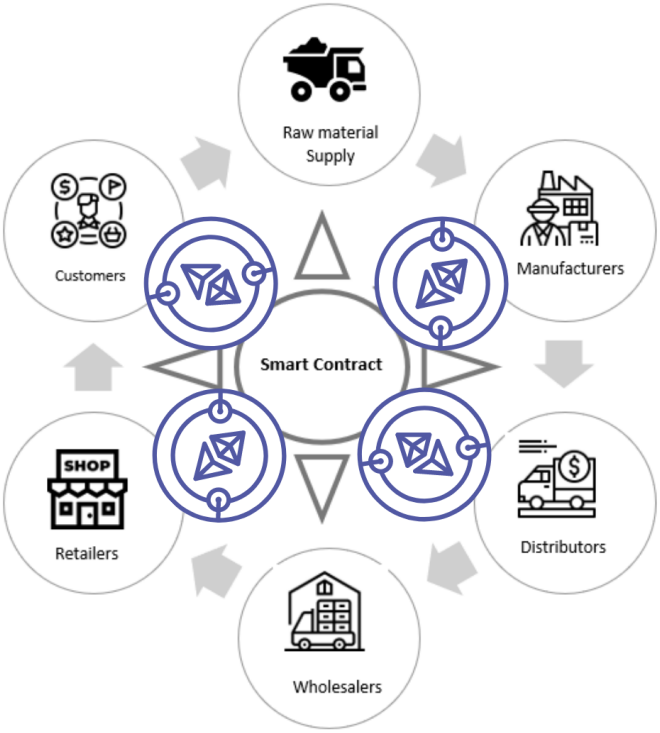


Figure 3.2: System Design Blockchain in Supply chain

3.3.1 System Elements

There are many components that we can use to come up with a secure and performing blockchain system, and I chose these particular components for their speed and outstanding performance.

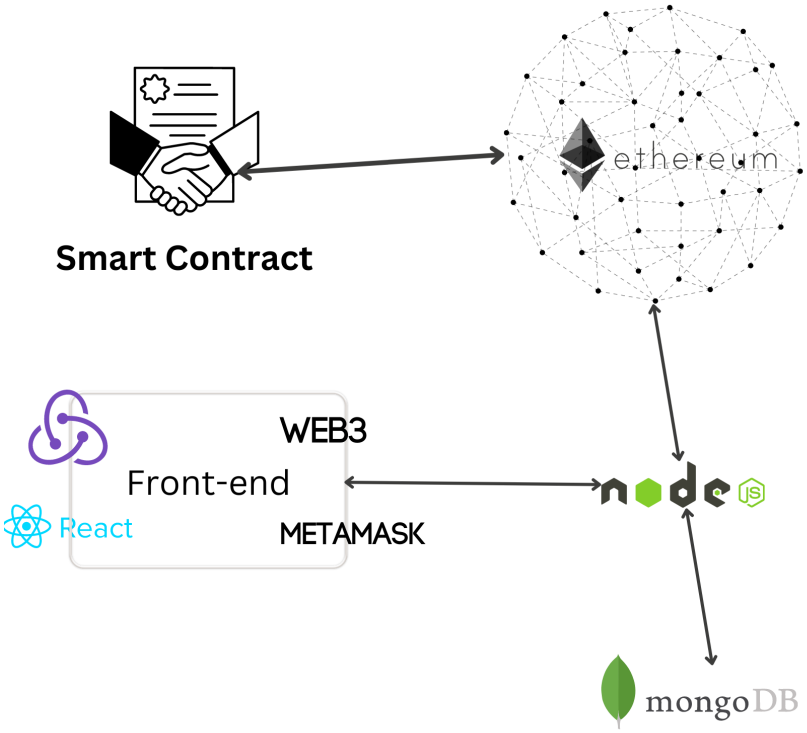


Figure 3.3: Structure of a typical Dapp for Ethereum Network

3.3.2 Using Blockchain in our Dapps

Blockchain technology can allow products in the supply chain to be readily traced and verified, and could enable easier detection and rectification of issues. If an issue such as a counterfeit drug is detected, the user could look at all previous data entries, touch points, locations, and timestamps to trace all the way back to find the origin of the product, the specific manufacturer, and even the specific batch that it came from. Blockchain technology can also use smart contracts to ensure that all participants in the supply chain agree to transactions, and proof of authority to ensure that only authorized participants are involved in the supply chain. By using blockchain technology, pharmaceutical companies can track products from manufacturer to consumer in real time, ensuring counterfeit drugs are not entering the supply chain . Blockchain technology can also manage inventory and reduce counterfeiting and theft issues in the pharmaceutical supply chain.

The aim of this work is to find an effective solution for recording details of digital assets and preventing manipulation of them. Ethereum was chosen because it is a public blockchain platform that uses smart contracts and allows for tracking of transactions. Smart contracts allow participants to interact with each other without a trusted central authority. Transaction records are immutable, verifiable, and securely distributed across the network, giving participants full ownership and visibility into transaction data.

Ethereum offers an extremely flexible platform on which to build decentralized applications using the native Solidity scripting language and Ethereum Virtual Machine. Decentralized application developers who deploy smart contracts on Ethereum benefit from the rich ecosystem of developer tooling and established best practices that have come with the maturity of the protocol.

3.3.3 Supply Chain Smart Contract Design

3.3.4 Infura Deployment Tool

Infura is a popular infrastructure provider for Ethereum and other blockchain networks. It offers developers a reliable and scalable way to connect to the Ethereum network without needing to run their own Ethereum node. Infura acts as a remote Ethereum node that developers can access through an API. By utilizing Infura, developers can interact with the Ethereum blockchain, send transactions, and read data without the need for setting up and maintaining their own node infrastructure.[12] By addressing the difficulties of establishing and administering blockchain infrastructure, this service streamlines the development process and frees developers to concentrate on creating their apps.

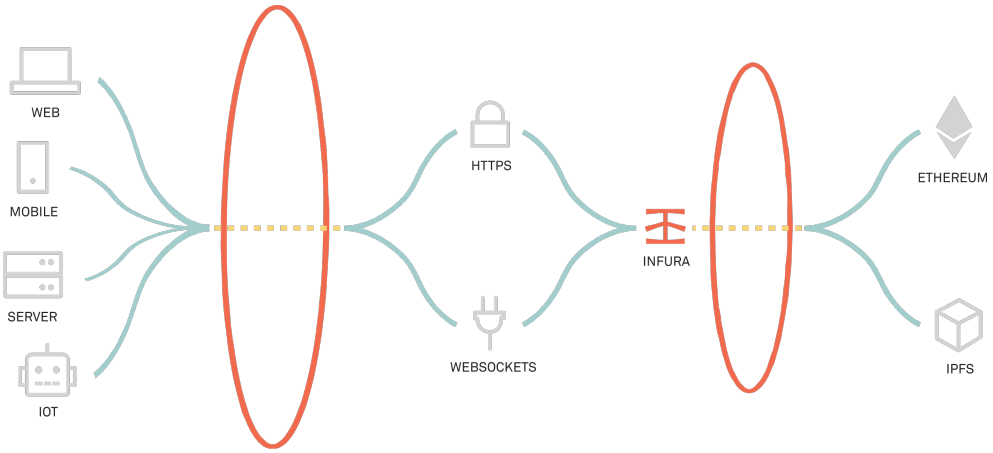


Figure 3.4: How Infura Work ?

3.3.5 Web3.js Library

Web3.js is a JavaScript library that allows developers to interact with the Ethereum blockchain and build decentralized applications (DApps). It serves as a bridge between the Ethereum network and web applications, enabling seamless integration of blockchain functionalities into web-based projects. Web3.js provides a set of APIs and methods to connect to Ethereum nodes , The JavaScript API enables us to communicate with an Ethereum node using the JSON RPC endpoints exposed on top of the HTTP, IPC or WebSocket transfers from the web page, through give json interface of smart contract and

web3 will auto convert all function into low level ABI calls over RPC.

3.3.6 Offchain Backend

The smart contract controls all functions in the system and to make it more flexible we linked it with nodejs api , and that's what we can connect with the desktop or mobile application , this api it's connected with blockchain and another database, which enables us to control what we cannot control through smart contracts, i use MongoDB database to store the data in an orderly manner and make it easy for the user to view. using ExpressJs freamwork we can make nodejs api simple and connect it with a smart contract using web3 and MongoDB database using mongoose orm.

- **NodeJs :** is an open source, cross-platform runtime environment for executing JavaScript code . [10]
- **Express.js :** is a popular Node.js web application framework that provides a robust set of features for web and mobile applications. It works on top of Node.js web server functionality to simplify its APIs and add helpful new features. [4] Express.js makes it easier to organize your application's functionality with middleware and routing. It adds helpful utilities to Node.js HTTP objects and facilitates the rendering of dynamic HTTP objects. Express.js is the most popular web framework for Node.js[23].
- **MongoDB :** is a source-available cross-platform document-oriented database program. Classified as a NoSQL database program, MongoDB uses JSON-like documents with optional schemas. MongoDB is developed by MongoDB Inc. and licensed under the Server Side Public License which is deemed non-free by several distributions.

3.3.7 Frontend

We need an interface to control smart contract function which we translated into Api in backend of node js and to facilitate the service for users , we use React js which is an open-source JavaScript library , based in components you can building interactive user interfaces [35], and use Redux make state management for our application after get data from node js api .

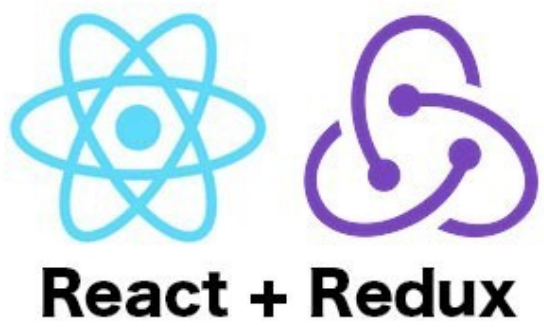


Figure 3.5: react and redux logo

3.3.8 Communication Between Web Application & Blockchain

JSON-RPC is a remote procedure call (RPC) protocol It is well known in the world of distributed systems that uses JSON to encode messages. In other words, JSON-RPC is simply another API standard.

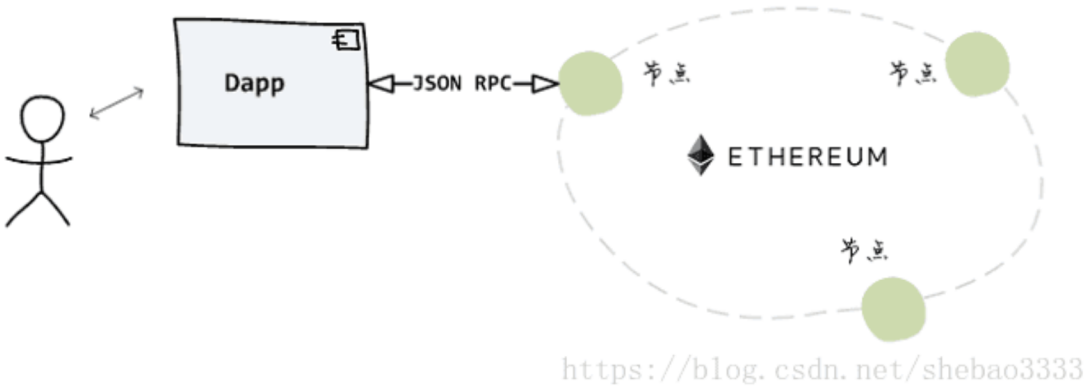


Figure 3.6: Communication Dapp with Ethereum & Blockchain

JSON-RPC is a widely adopted, simple protocol utilized in the cryptocurrency industry. It serves as a means of communication between wallet applications and full nodes within various cryptocurrencies, including Bitcoin and Ethereum. With JSON-RPC, wallet applications can request information from a full node and execute actions such as sending transactions. For instance, a wallet application can utilize JSON-RPC to retrieve the current balance of a specific address or broadcast a trade to the network. This protocol enables seamless interaction and data exchange between wallet applications and the underlying blockchain network, facilitating efficient cryptocurrency transactions and operations.

JSON-RPC facilitates communication with the node by means of a Web3 provider. The Web3 provider acts as a software component, exposing a JSON-RPC API to the client

application. Through this API, the client application establishes a connection with the node and transmits JSON-RPC requests. The Web3 provider serves as the intermediary, enabling the client to interact seamlessly with the node using the JSON-RPC protocol.

```
{
    "jsonrpc": "2.0",
    "method": "eth_getBalance",
    "params": [
        "0x15463F7566d797a4b36517eB3A1cAFaB58f1A381"
    ],
    "id": 0
}
```

Figure 3.7: Json Rpc Form

Json-Rpc form consisting of :

- **Jsonrpc :** the JSON-RPC protocol version (usually "2.0")
- **Method :** the name of the method to be called, in this case, "eth$_getBalance$"
- **Params :** an object containing the parameters for the technique, such as the transaction data and the recipient address
- **Id :** a unique identifier for the request

3.4 The Big Picture of Our System & Their Interaction

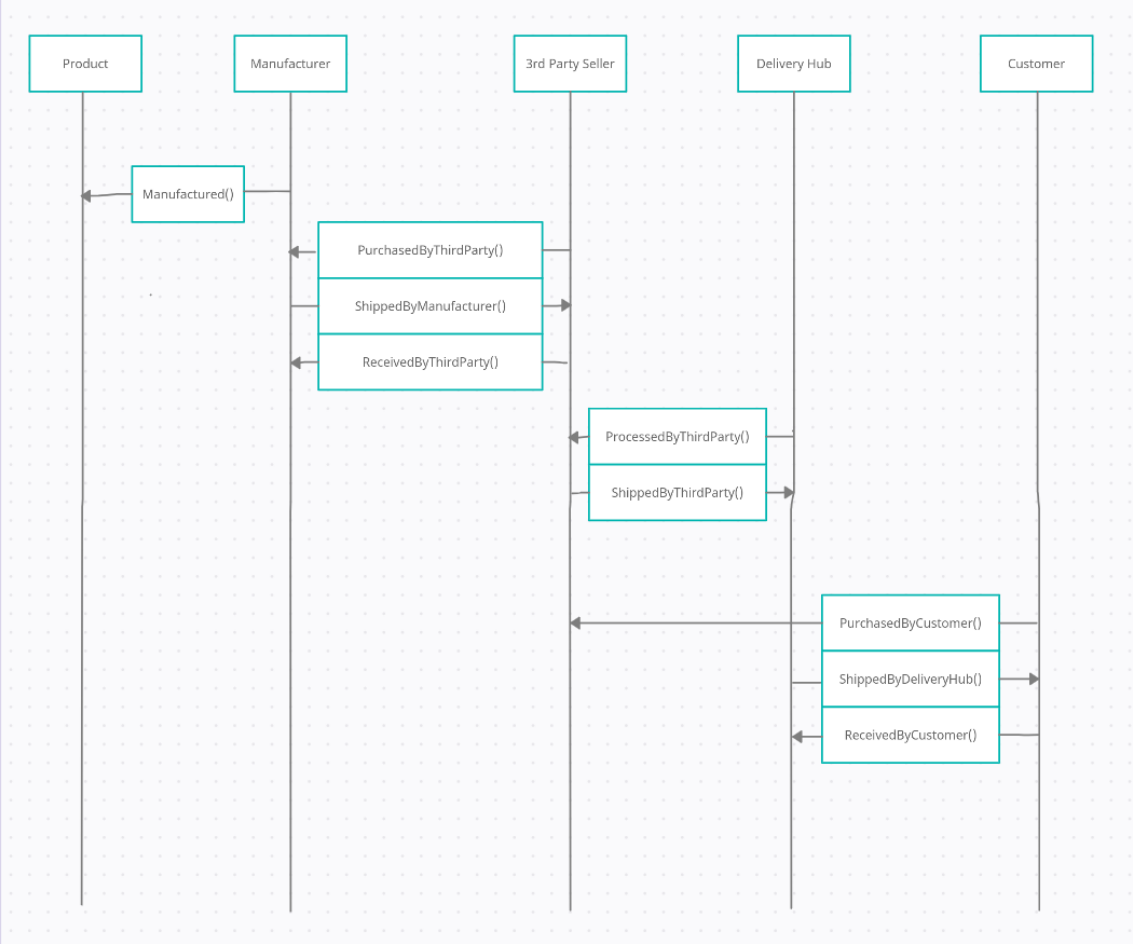


Figure 3.8: Sequence diagram of our Dapp

the manufacturer plays a crucial role. The manufacturer produces drugs and includes important details such as product code, drug name, quantity, and information about the manufacturer. This information is then stored on the blockchain, ensuring transparency and enabling traceability for other stakeholders.

The distributors validate the received medicines and digitally sign the transaction they can verify the origin of medicines with the help of product code stored on the blockchain. They can trace back the information added by manufacturers such as the quantities of medicines, where it was manufactured. which is then recorded on the blockchain.

Retailers receive drugs that can be traced back to their origin using product codes stored on the blockchain.If any illegal distributor attempts to steal or delay the delivery of medicines, the transaction is considered invalid due to the fraudulent information recorded on the blockchain. Retailers have the ability to quickly identify any anomalies in the transactions,

ensuring the integrity of the supply chain. Once the pharmacist approves the received medicines, the transaction between the retailer and the distributor is added to the blockchain, validating the legal transaction. Additionally, retailers sell the drugs to clients, and these transactions are also recorded on the blockchain, providing a transparent and auditable record of the sales process .

3.5 Development Tools

we need many tools and language , operating system to make this system interact :

3.5.1 Our Hardwar & Operating System

The project is being implemented on CPU AMD Ryzen 5 4600H with Radeon Graphics 3.00 GHz, with 16 Go Ram in Windows 11 Famille.

3.5.2 Remix IDE

Remix IDE is a comprehensive smart contract development tool used for the entire journey of smart contract development by users at every knowledge level . [7] It is an open-source web and desktop application that fosters a fast development cycle and has a rich set of plugins with intuitive GUIs . Remix IDE comes in two flavors: web app or desktop app, and as a VSCode extension . It requires no setup and supports Solidity language as well as a playground for learning and teaching Ethereum. [6]

Figure 3.9: RemixIde Logo

3.5.3 Visual Studio Code

Visual Studio Code is a free, lightweight, and powerful source code editor that runs on desktop and web platforms and is available for Windows, macOS, Linux, and Raspberry Pi OS. It is built on open-source technologies such as Electron shell, Node.js, TypeScript, and the Language Server Protocol . [5] Visual Studio Code combines the simplicity of a source

code editor with powerful developer tooling, like IntelliSense code completion and debugging . [34]

Figure 3.10: visual studio Code Logo

3.5.4 Truffle Framework

Truffle is a comprehensive development framework for Ethereum decentralized applications (dapps). It simplifies the development process by providing tools such as a smart contract compiler, automated testing, and deployment scripts. With Truffle, developers can efficiently write and manage smart contracts using the Solidity programming language. It offers features like contract migration, network management, and debugging capabilities. To install the Truffle framework : **npm install -g truffle**

Figure 3.11: Truffle Logo

3.5.5 Ganache

Ganache, is a personal blockchain that provides a local Ethereum network for developers to test their decentralized applications (dapps) in a sandboxed environment. It offers a user-friendly interface for managing accounts, simulating transactions, and inspecting blockchain activity. By eliminating the need for connecting to the live Ethereum network, Ganache enables faster iterations and improved debugging capabilities. It also includes advanced features such as network snapshots and deterministic blockchain behavior, allowing developers to precisely reproduce and test specific scenarios for their dapps.

Figure 3.12: Truffle Logo

3.5.6 Metamask

MetaMask is a browser plugin and Ethereum wallet that allows users to store Ether and other ERC-20 tokens, enabling them to transact with any Ethereum address. It serves as an entry point into the world of decentralized finance (DeFi), allowing users to spend coins in games, stake tokens in gambling applications, and trade on decentralized exchanges. MetaMask offers ease of use, security through encryption and secret recovery phrases, support for Ether and ERC-20 tokens, MetaMask provides a simple and intuitive interface for accessing Ethereum-based applications and exploring the possibilities of the decentralized web . [47]

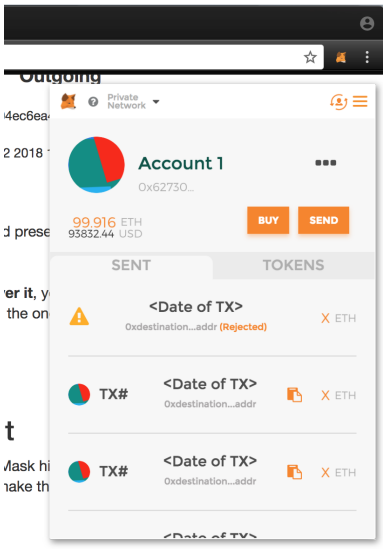


Figure 3.13: Metamask interface

3.6 Implementation Of Our SupplyChain Smart Contract

we will discuss in this section about the implementation of the system and steps of this projects the first step we will create files and install tools with commands :

```
create file with name senstive-products-supplychain
```

Installing **NodeJs** from official website , after that install **Metamask** in browser . The second step install **Truffle** with NPM

```
\$ npm install -g truffle
```

when Truffle installed we will make set up with this commande

```
\$ truffle init
```

after the last command we will see three Folders and one file :

- **Contract :** we will add smart contract code here
- **Migrations :** which help deploy new changes in the contract to the ethereum blockchain
- **Test :** add test for our smart contract
- **truffle-config.js :** Javascript file and can execute any code necessary to create your configuration.

3.6.1 Download & Install Ganache

Download ganache software and install it for quickly fire up a personal Ethereum blockchain , and get 10 accounts with here hash like normal nodes in networks , this softwar for working in local and test it before deploy smart contract in Ethereum blockchain .

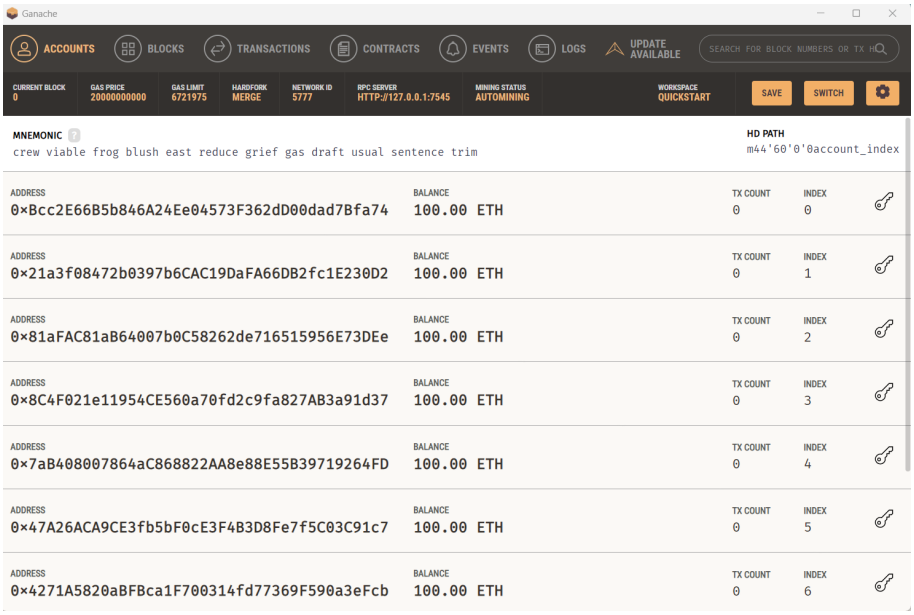


Figure 3.14: ganach interface

3.6.2 Config truffle with Ganach

inside **truffle-config.js** add identifier of virtual network and nodes of ganach

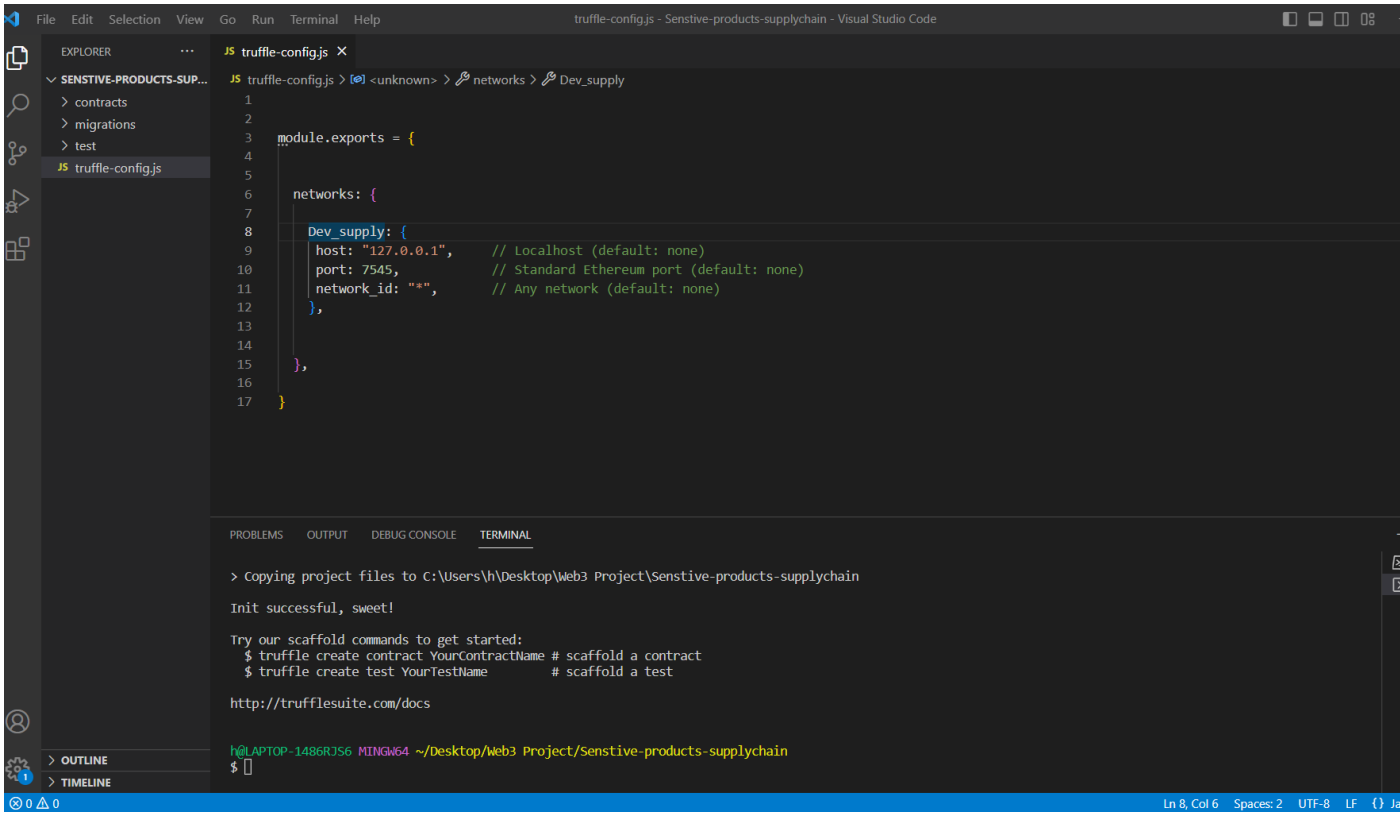


Figure 3.15: config truffle with ganache

after that test connection with terminal and get all account with this commands :

```
truffle console --network Dev_supply
```

```
let accounts = await web3.eth.getAccounts()
```

and display all accounts to verify:

```
accounts
```

3.6.3 Our Supply Chain Smart Contract

We will build Dapp (decentralized application) for supply chain managment of sensitive products like drugs and trace it from manufacturing to sale to the consumer and to do that we will create new ethereum smart contract with **Drugsupply.sol** in contract folder , we specify smart contract version bigger than **0.4.16** and small than **9.0.O** , smart contract contains states to save data and functions to do something , and events .

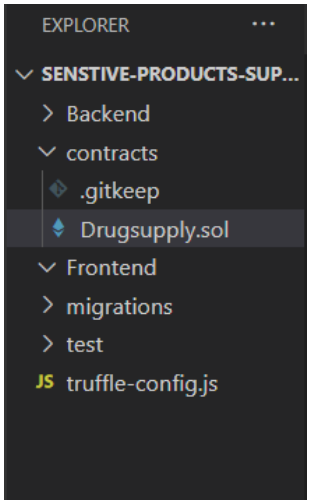


Figure 3.16: adding Drugsupply contract

3.6.4 Smart Contract States

we create states in our contract to save data , it like column in relational database

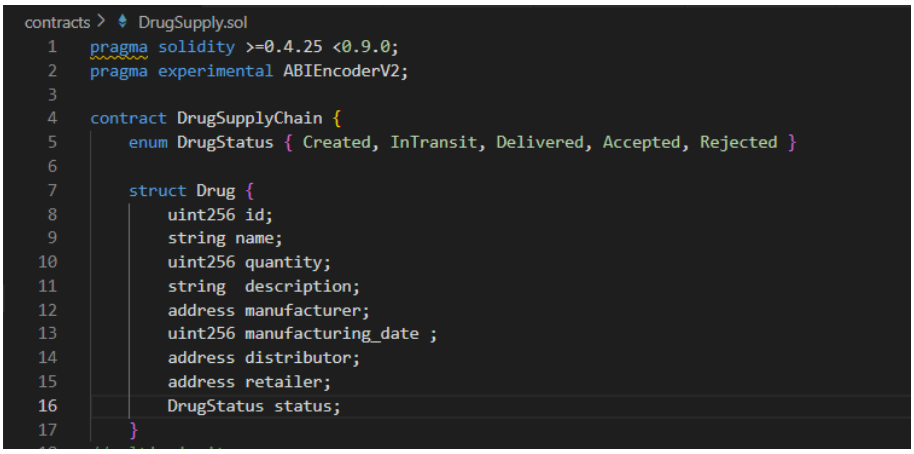


Figure 3.17: Smart Contract States

we explain our states and we begin with define a variable called '**ID**' its the identifier of our drug , and define '**name**' name of drug , '**Quantity**' determin how much of this medicine do we have ,'**description**' a short definition of this medicine, its symptoms and why it is used . '**Manufacturer**' the name of the manifacture that made this medicine , '**Manufacturer date**' a time that went out of manufacturing '**distributor**' The distributor responsible for distributing this medication '**retailer**' The retailer to whom the product arrived from the distributor '**status**' every time the condition of the product changes, this way we know the location of the product or track it .

3.6.4.1 Mapping in solidity

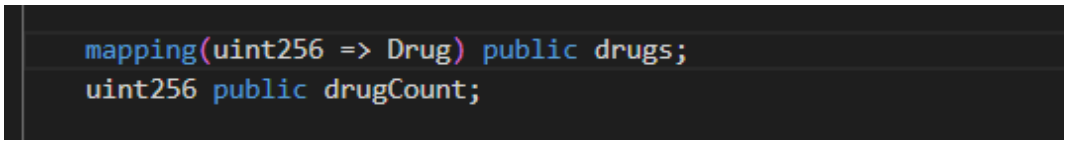


Figure 3.18: Mapping in solidity

We store data in mapping which is basically hash tables that store data as key-value pairs . [14]

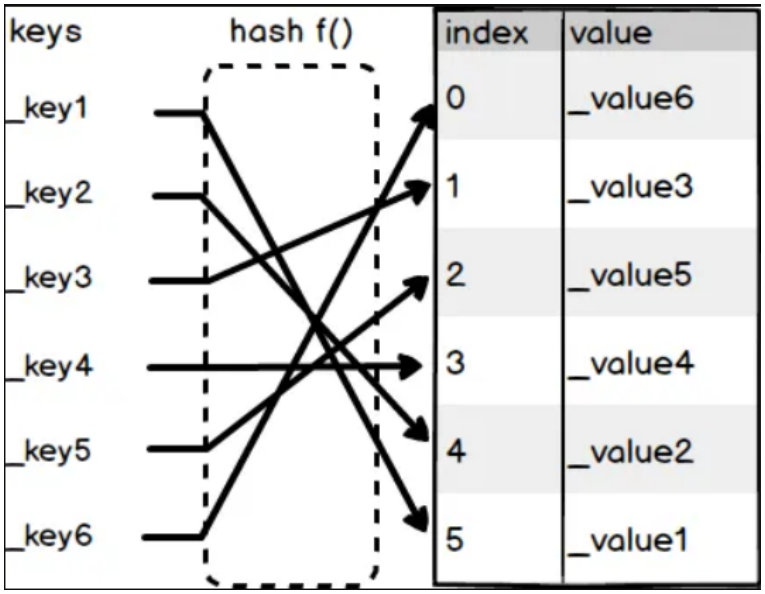


Figure 3.19: Hash tables example

3.6.5 Smart Contract Functions

we create solidity functions to perform specific tasks , solidity enables developers to achieve modularity in their code by utilizing functions, thereby eliminating the need to repeatedly rewrite redundant code segments . I started writing createdrugs function to create products by Manufacture.

```
function createDrug(string memory _name, uint256 _quantity,string memory _description) public {
    require(_quantity > 0, "Quantity should be greater than zero");
    drugCount++;
    drugs[drugCount] = Drug(drugCount, _name, _quantity,_description, msg.sender, block.timestamp , address(0), address(0), DrugStatus.Created);
    emit DrugCreated(drugCount, _name, _quantity, msg.sender);
}
```

Figure 3.20: Create Drug function

this solidity function is to create new project and add it to the blockchain

```
function transitDrug(uint256 _id, address _distributor) public {
    Drug storage drug = drugs[_id];
    require(drug.status == DrugStatus.Created, "Drug is not in the Created state");
    require(drug.distributor == address(0), "Drug is already in transit");
    drug.distributor = _distributor;
    drug.status = DrugStatus.InTransit;
    emit DrugTransit(_id, _distributor);
}
```

Figure 3.21: Make transaction function

Transitdrug when the drug is successfully transit . the status changed to **InTransit**

```
44    function deliverDrug(uint256 _id, address _retailer) public {
45        Drug storage drug = drugs[_id];
46        require(drug.status == DrugStatus.InTransit, "Drug is not in transit");
47        require(drug.retailer == address(0), "Drug is already delivered");
48        drug.retailer = _retailer;
49        drug.status = DrugStatus.Delivered;
50        emit DrugDelivered(_id, _retailer);
51    }
```

Figure 3.22: Deliver Drug function

The deliverdrug function in the Solidity smart contract is used to transfer the ownership of a drug product from the current owner manifacture to a new owner delivery man . It facilitates the transfer of ownership within the supply chain when a product is sold or transferred between entities.

```
68
69    function getAllDrugs() public view returns (Drug[] memory) {
70        Drug[] memory structs = new Drug[](drugCount);
71        for (uint256 i = 0; i < drugCount; i++) {
72            Drug storage member = drugs[i];
73            structs[i] = member;
74        }
75        return structs;
76    }
```

Figure 3.23: Get all drugs information

The Getalldrugs function to get all information of drugs and the state of drugs.

3.6.6 Events And Emits In Solidity

An event is a way to log specific occurrences or state changes within a smart contract. It's a way for a contract to communicate with external applications or other smart contracts, notifying them of important actions or updates.

```
21
22    event DrugCreated(uint256 id, string name, uint256 quantity, address manufacturer);
23    event DrugTransit(uint256 id, address distributor);
24    event DrugDelivered(uint256 id, address retailer);
25    event DrugAccepted(uint256 id);
26    event DrugRejected(uint256 id);
27
```

Figure 3.24: Events code on solidity

3.6.7 Compiling and Deploying the Smart Contract

To compile a Truffle project, change to the root of the directory where the project is located and then type the following into a terminal:

```
truffle compile
```

this command runs to compile solidity code, contracts are compiled into bytecode that is executed on the EVM add create **ABI I (Abstract Binary Interface)** file in location "/build/contracts/Drugsupply.json", It includes The JSON format of a contract's ABI is given by various functions and/or events descriptions. Now to deploy this contract on a test or local blockchain network we must create a new file on the migration file with this code.

```
1  var SupplyChain = artifacts.require(" ../Drugsupply.sol") ;
2  module.exports = function ( deployer ) {
3      deployer.deploy ( SupplyChain ) ;
4  };
```

Figure 3.25: code of migration to deploy

then we write this command: `truffle migrate --network Dev_supply`

Truffle provides a convenient and structured way to manage the deployment and updating of smart contracts. By utilizing migration files and Truffle's migration system, you can easily maintain and version your contracts across different environments and networks.

3.6.8 Testnet Deployment

the term testnet describes when a blockchain protocol or network is not yet up and running at its full capacity. A testnet is used by programmers and developers to test and troubleshoot all the aspects and features of a blockchain network before they are sure the system is secure and ready for the mainnet launch. Testnet is any testing environment where fake money can be used instead to test contracts . we have three testnet in ethereum :

- Goerli : Goerli was the first Ethereum testnet, is cross-client, and features all the mainnet features in a safe environment for development and testing. Developers making Ethereum-destined DApps first deploy to the Goerli testnet for no gas fees to make sure their use cases are well-met before deploying to the mainnet for immutability .
- **Sepolia :** is a stable Ethereum testnet that merged from Proof of Work to Proof of Stake along with the Ethereum mainnet and serves developers with the infrastructure to deploy and test Solidity smart contracts. Sepolia has a faucet service to ensure developers only use Sepolia ETH for gas when staging DApps on the testnet.

- **Rinkeby :** is a staging blockchain for Ethereum DApp and smart contract developers to test and optimize their smart contracts before going live in Eth-main. The Rinkeby dashboard features a faucet to dispense test ETH tokens for pseudo transactions, and a block explorer to facilitate analysis when creating Solidity smart contracts and executing transactions.

I use Sepolia Testnet with metamask .

3.6.9 Backend & Frontend Development

We choose Node.js to build backend because has a vast and active ecosystem with a wide range of libraries and packages available through its package manager.and we choose react js because follows a component-based architecture, allowing you to break your user interface into reusable and self-contained components. enabling you to describe the desired UI state.

3.6.10 Backend

we develop normal API with multi-role and each role has its own business like manufacture create products in the system buying it or transferring the owner to the distributor who also has his business ... we have many authority and authorization . now add api key in variable of environment and use it to make api interact with smart contract .

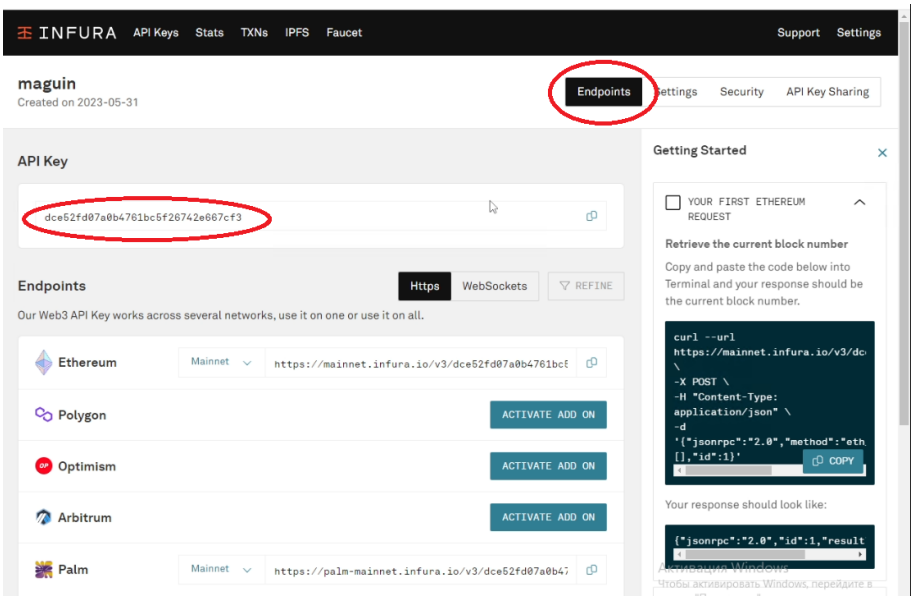


Figure 3.26: API Key Infura

after we complete the connection and prepare the local server we make routes using web3 and HDWalletProvider function to connect with our smart contract Before that, we must open an account in infura website to get API KEY to connect to it.

```
const infuraKey = process.env.INFURA_KEY;

const web3 = new Web3(new Web3.providers.HttpProvider( `https://ropsten.infura.io/v3/${infuraKey}`));

const helloWorld = new web3.eth.Contract([
  {
    "constant": true,
    "inputs": [],
    "name": "output",
    "outputs": [
      {
        "internalType": "string",
        "name": "",
        "type": "string"
      }
    ],
    "payable": false,
    "stateMutability": "pure",
    "type": "function"
  }
], '0x35c113E1AB11B3001e9085CBafD224FfC3470C67');

helloWorld.methods.output().call({from: '0x8863ae48646c493efF8cd54f9Ffb8Be89669E62A'}, function(error, result) {
    console.log(result);
});
```

Figure 3.27: Connection with our smart contract

using ABI and web3 nodejs to connect easily to blockchain smart contracts. the goal of connecting smart contracts with nodejs to produce an restful api connection on multi interfaces and get authentication and authorization for all user and make multi role apps, simply and secure .

```
const infuraKey = process.env.INFURA_KEY;

const web3 = new Web3(new Web3.providers.HttpProvider( `https://ropsten.infura.io/v3/${infuraKey}`));

const helloWorld = new web3.eth.Contract([
  {
    "constant": true,
    "inputs": [],
    "name": "output",
    "outputs": [
      {
        "internalType": "string",
        "name": "",
        "type": "string"
      }
    ],
    "payable": false,
    "stateMutability": "pure",
    "type": "function"
  }
], '0x35c113E1AB11B3001e9085CBafD224FfC3470C67');

helloWorld.methods.output().call({from: '0x8863ae48646c493efF8cd54f9Ffb8Be89669E62A'}, function(error, result) {
    console.log(result);
});
```

Figure 3.28: Connection with our smart contract

3.6.11 Frontend

Now, using ReactJs frontend Library make a small interface for users interaction to make react app you need to tap this command : `npx create-react-app supply`

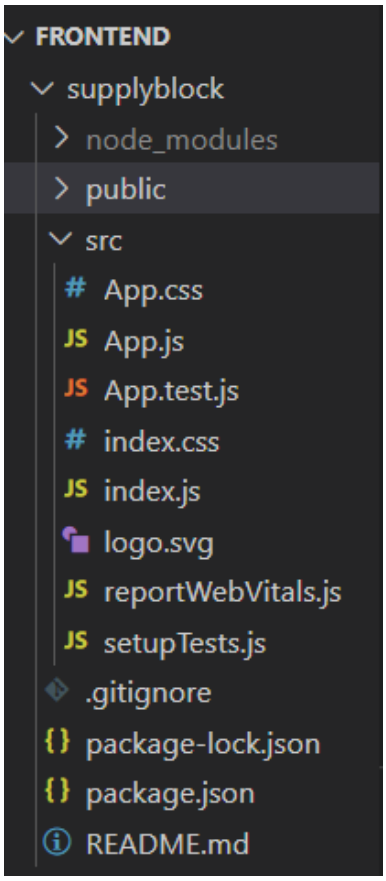


Figure 3.29: login for users

make login page for users and apply authentication and authorization using express jwt token , and redirect according to the user.

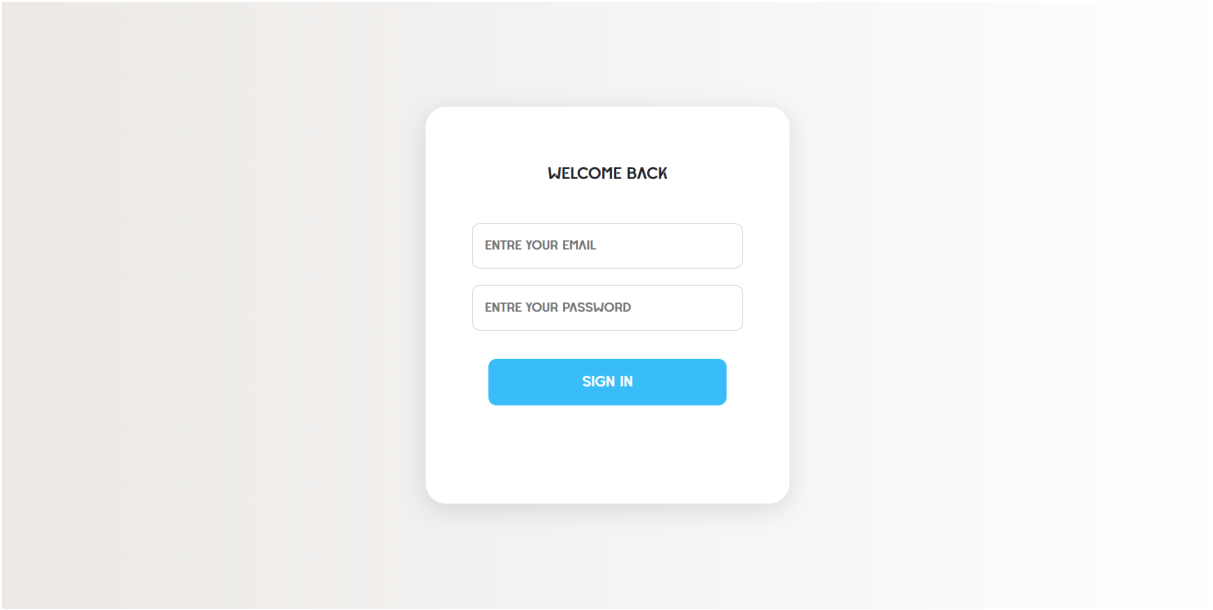


Figure 3.30: Login Page

This page for creating new products by Manifacture

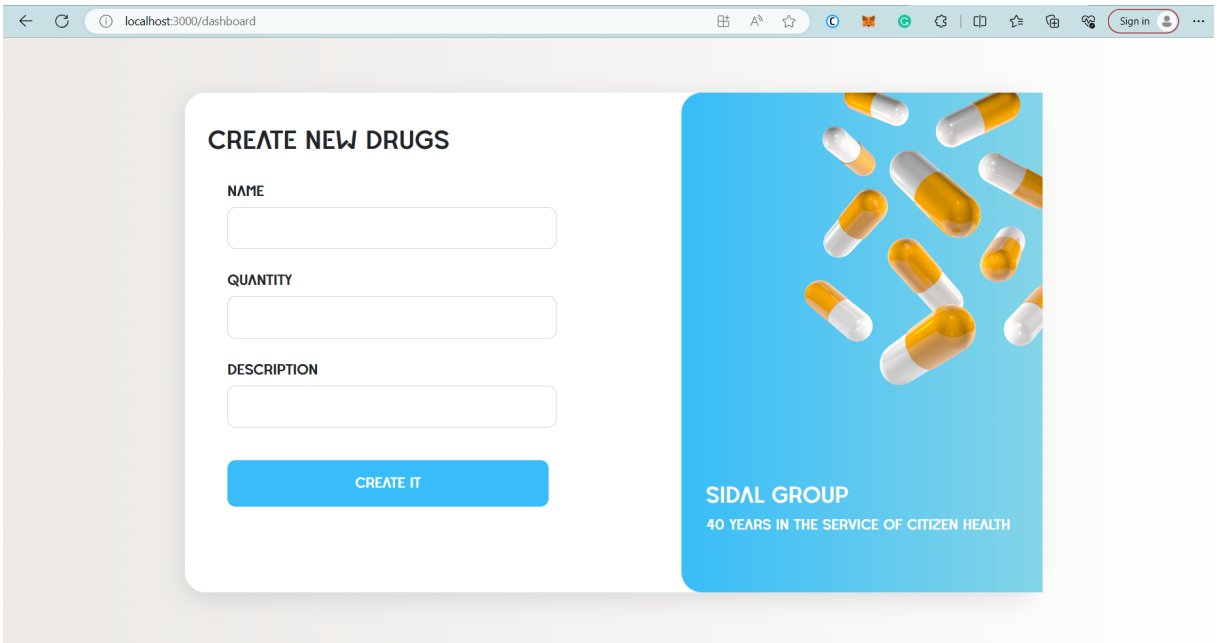


Figure 3.31: add drugs on blockchain

all users must have metamask account

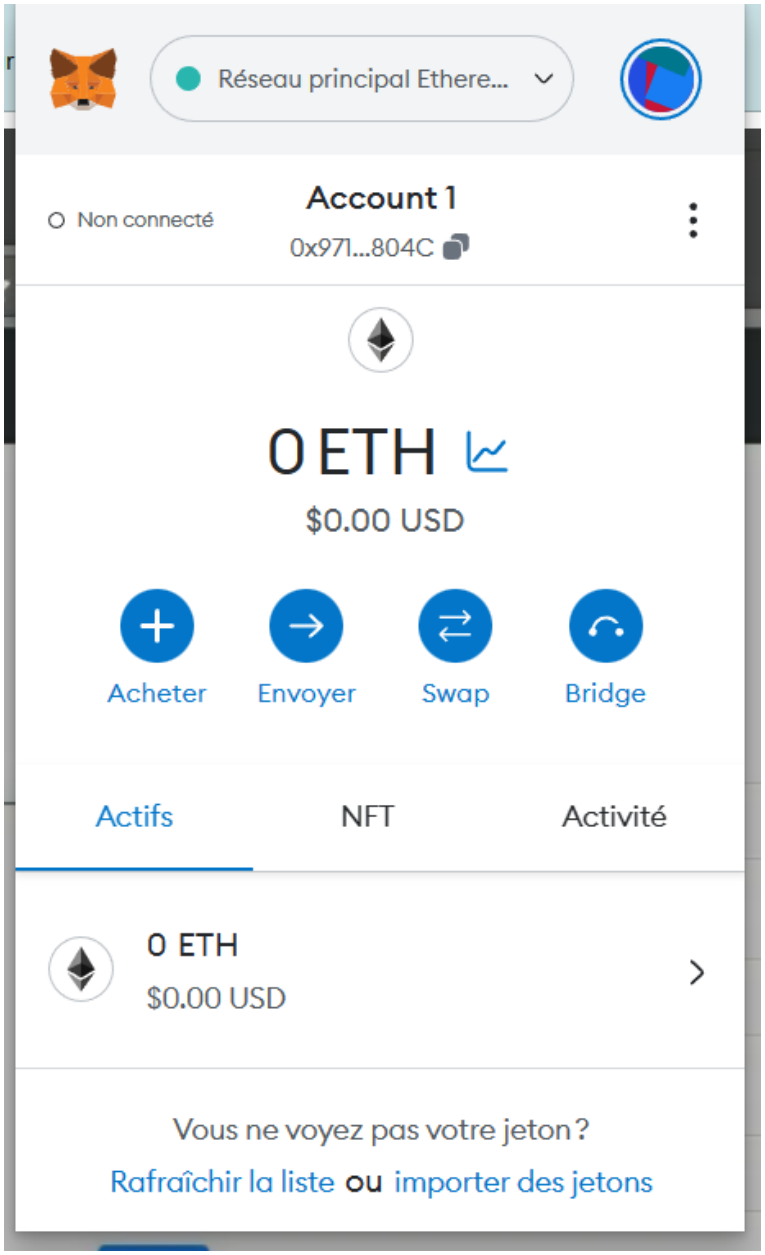


Figure 3.32: Metamask interface

this interface for distributor, Here we hold the responsibility of the medicine for distributor

.

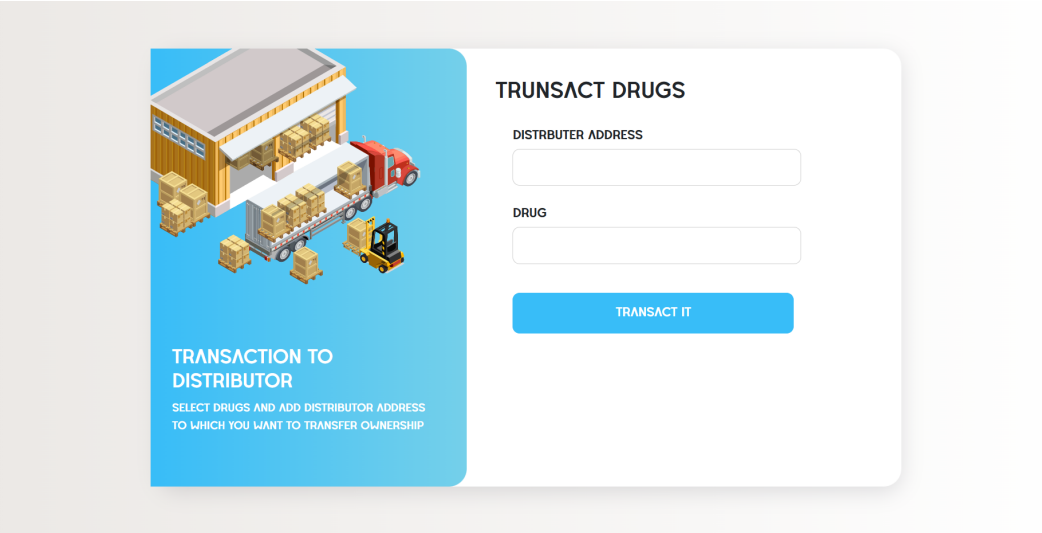


Figure 3.33: distributor interface

this interface for retailer, Here we hold the responsibility of the medicine for retailer .

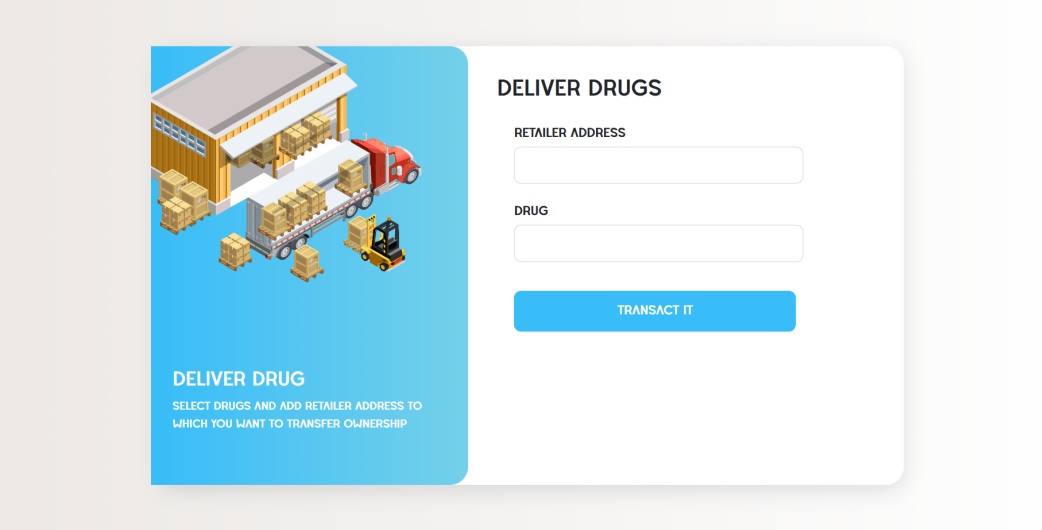


Figure 3.34: distributor interface

this how i can get data with web3 library in react

```jsx
import React, { useState } from "react";
import './Products.scss';
import Web3 from 'web3';
import { Drugsupplycontract } from "../../ABI/abi";
import { useEffect } from "react";

function Products() {

  const [mappingValues, setMappingValues] = useState([]);

  const contractAddress = "0xe2eE740Dc2e0C8bb8CC0756AFEA020C672aED89A";
  const web3 = new Web3("HTTP://127.0.0.1:7545" || Web3.givenProvider);
  const drugcontract = new web3.eth.Contract(Drugsupplycontract, contractAddress);

  async function fetchData() {
    const count = await drugcontract.methods.drugCount().call();
    const t = count.toString();
    console.log(t);

    for (var i = 0; i < t; i++) {
      mappingValues.push(await drugcontract.methods.drugs(i).call())
      console.log(mappingValues);
    }
  }

  useEffect(() => {
    fetchData();
    console.log(mappingValues);
  });
```

Figure 3.35: web3 to get drug data

Figure 3.36: data getting from blockchain

3.7 conclusion

In the conclusion of this chapter, We find that this technology is indispensable because of its additions to companies and factories and a strong addition to competition between producing companies and to protect its name in the market from adulterated products.

Bibliography

[1] Bitcoin script. https://docs.ivylang.org/bitcoin/language/BitcoinScript.html.

[2] Drug supply management. https://www.tracelink.com/agile-supply-chain/drug-supply-management.

[3] Ethereum. https://docs.infura.io/networks/ethereum.

[4] Express nodejs. https://developer.mozilla.org/en-US/docs/Learn/Server-side/Express_Nodejs.

[5] official website visual studio code. https://code.visualstudio.com/.

[6] Remixide docs in github. https://github.com/ethereum/remix-ide.

[7] Remix's documentation. https://remix-ide.readthedocs.io/en/latest/.

[8] utxo model explained. https://www.nervos.org/knowledge-base/utxo_model_explained.

[9] What is the byzantine generals problem? https://river.com/learn/what-is-the-byzantine-generals-problem.

[10] Node js. https://nodejs.org/en/, 2022. Last accessed 16 April 2022.

[11] , 2022-08-05.

[12] Why infura is the secret weapon of ethereum infrastructure. https://consensys.net/blog/news/why-infura-is-the-secret-weapon-of-ethereum-infrastructure/, April 27, 2018.

[13] The importance of temperature monitoring in cold chain management. https://www.rkfoodland.com/the-importance-of-temperature-monitoring-in-cold-chain-management/, February 9,2023.

[14] alchemy. What is mapping in solidity ? https://www.alchemy.com/overviews/solidity-mapping.

[15] Amazon. What is blockchain technology?

[16] Gavin Wood Andreas M. Antonopoulos. Mastering ethereum. https://learning.oreilly.com/library/view/mastering-ethereum/9781491971932/, December 2018. December 2018.

[17] Andreas M. Antonopoulos. Mastering bitcoin. https://learning.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/.

[18] Angela Beklemysheva. Making effective use of smart contracts. https://steelkiwi.com/blog/making-effective-use-of-smart-contracts/, 25/05/2023. Last accessed 10 Mars 2022.

[19] binance. Double spending explained. https://academy.binance.com/en/articles/double-spending-explained.

[20] binance. Byzantine fault tolerance explained. https://academy.binance.com/en/articles/byzantine-fault-tolerance-explained, 25/05/2023. Last accessed 10 Mars 2022.

[21] binance academy. Blockchain use cases. https://academy.binance.com/en/articles/blockchain-use-cases, Feb 27, 2019.

[22] b Peter Beyer c Yohann Lacotte d DG Joakim Larsson e Marie-Cécile Ploy d John-Arne Røttingen f Christine Årdal, corresponding authora Enrico Baraldi and Ingrid Smithg. Supply chain transparency and the availability of essential medicines. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8085627/, 03/10/2022. 2021 Apr 1; 99(4): 319–320.

[23] codeacademy team. What is express.js? https://www.codecademy.com/article/what-is-express-js.

[24] coinmarketcap. market cap. https://coinmarketcap.com/.

[25] cointelegraph. How blockchain technology is used in supply chain management ? https://cointelegraph.com/explained/how-blockchain-technology-is-used-in-supply-chain-management.

[26] consensys. Blockchain in supply chain management. https://consensys.net/blockchain-use-cases/supply-chain-management/.

[27] Cryptopolitan. What is blockchain and how does it work ? https://www.binance.com/en/feed/post/188473, 30-01-2023. Last accessed 10 Mars 2022.

[28] ethereum. ethereum docs. https://ethereum.org/en/developers/docs/.

[29] ethereum official. Introduction to smart contracts. https://ethereum.org/en/smart-contracts/, 25/05/2023.

[30] fightfraud. how blockchain technology can help fight fraud corruption singh. https://www.linkedin.com/pulse/how-blockchain-technology-can-help-fight-fraud-corruption-singh/.

[31] JAKE FRANKENFIELD. Cryptocurrency explained with pros and cons for investment. https://www.investopedia.com/terms/c/cryptocurrency.asp, April 21, 2023.

[32] Sirine HAMLAOUI. Blockchain for the drug supply chain management. http://archives.univ-biskra.dz/bitstream/123456789/15767/1/Sirine_HAMLAOUI.pdf, 2020.

[33] hashcash. hashcash. http://www.hashcash.org/.

[34] Martin Heller. What is visual studio code? microsoft's extensible code editor. https://www.infoworld.com/article/3666488/what-is-visual-studio-code-microsofts-extensible-code-editor.html, JUL 8, 2022.

[35] David Herbert. What is react.js? (uses, xamples, more). https://blog.hubspot.com/website/react-js.

[36] holisollogistics. Supply chain management process : Five key steps for building excellence . https://holisollogistics.com/supply-chain-management-process-five-steps-for-building-excellence/, 08/12/2016. Last accessed 10 Mars 2022.

[37] imran Bashir. mastering-blockchain. https://learning.oreilly.com/library/view/mastering-blockchain/9781788839044/, 03/2018.

[38] Alivia Kaylor. Fundamentals of the pharmaceutical supply chain. https://pharmanewsintel.com/news/fundamentals-of-the-pharmaceutical-supply-chain, March 23, 2023.

[39] Mubashir Ahmed Malik. What is the gas price in smart contracts? https://www.educative.io/answers/what-is-the-gas-price-in-smart-contracts.

[40] medical products. medical products. https://www.who.int/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-fa
28 November 2017.

[41] oreilly. Mastering ethereum by.

[42] Pharmanewsintel. Fundamentals of the pharmaceutical supply chain. https://pharmanewsintel.com/news/fundamentals-of-the-pharmaceutical-supply-chain, 03/23/2023. Last accessed 10 Mars 2022.

[43] Shubhajna Rai. Decision phases of supply chain management. https://studentprojects.in/civil-engineering/supply-chain/decision-phases-of-supply-chain-management/, 03/10/2022. Last accessed 10 Mars 2022.

[44] Shubhajna Rai. Three supply chain decision phases. https://talkforbiz.com/three-supply-chain-decision-phases/, 03/10/2022.

[45] NATHAN REIFF. What was the first cryptocurrency? https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/#citation-7.

[46] A A Borodinov1 S R Bryatov1. Blockchain technology in the pharmaceutical supply chain: researching a business model based on hyperledger fabric. https://ceur-ws.org/Vol-2416/paper18.pdf, 03/10/2022. Last accessed 10 Mars 2022.

[47] Hitesh Sant. guide to metamask. ttps://geekflare.com/beginners-guide-to-metamask/, April 28, 2023. Last accessed 10 Mars 2022.

[48] Shahriar H Zhang C Sinclair, Shahriar Zhang Sinclair D. Security requirement prototyping with hyperledger composer for drug supply chain: a blockchain application. https://dl.acm.org/doi/abs/10.1145/3309074.3309104, 2019.

[49] Sphinx. Solidity docs. https://docs.soliditylang.org/en/v0.8.20/.

[50] sudarshandixit29. What is consortium blockchain? https://www.geeksforgeeks.org/what-is-consortium-blockchain/, 25/05/2023. Last accessed 10 Mars 2022.

[51] supplychainComponents. The 5 basic components of supply chain management.

[52] supplychainEssensial. Fundamentals of the pharmaceutical supply chain michel hugo.

[53] supplychainManagement. Supply chain management strategy, planning, and operation ,fifth edition , sunil chopra peter meindl, 2013. Last accessed 10 Mars 2022.

[54] Arturo Viveros Sven Bernhardt. Blockchain across oracle , the incentive layer.

[55] Awol Jemal and Tadesse Gudeta Tadesse Jobira, Habtamu Abuye. Evaluation of pharmaceuticals inventory management in selected health facilities of west arsi zone, oromia, ethiopia. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7882713/, 03/10/2022. Last accessed 10 Mars 2022.

[56] Written By Editorial Team. The keys to crypto kingdom: Wallet address, public and private keys explained. https://blocktrade.com/wallet-addresses-public-and-private-keys-explained/, August 5, 2021. August 5, 2021.

[57] techtarget. distributed ledger technology (dlt).

[58] Megha Thakkar. Sha 256 algorithm explained by a cyber security consultant. https://sectigostore.com/blog/sha-256-algorithm-explained-by-a-cyber-security-consultant/.

[59] Kathleen E. Wegrzyn Eugenia Wang. Types of blockchain: Public, private, or something in between. https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between, 19 August 2021.

[60] . . . https://dspace.univ-ouargla.dz/jspui/bitstream/123456789/22970/1/03.pdf, 03/10/2022. Last accessed 10 Mars 2022.

[61] . . https://apps.who.int/gb/ebwha/pdf_files/WHA69/A69_42-ar.pdf, 03/10/2022. Last accessed 10 Mars 2022.