The Democratic and Popular Algerian Republic

Ministry of higher education and Scientific Research

Mohamed Khider University – Biskra

Faculty of Exact Sciences, Natural Sciences and Life

Department of Computer Science

RTIC10 **M**2/2022

THESIS

Presented for the diploma of

Master in Computer Science

Option**: Information and communication networks and technologies**

Academic certificates verification using Blockchain

Presented in 27/06/2022

By: **BENLAGHA ABDELOUAHEB**

Board of Examiners:

Mr.BELAICH HAMZA	**Supervisor**
Mrs.BELOUNAR SALIHA	**President**
Mrs.ZERARKA Nour Elhouda	**Examiner**

Academic year : 2021/2022

Contents

List of Figures

Abstract

Blockchain technology is one amongst the foremost powerful inventions within the previous couple of years.It has an immense result in our way of life , ranging from cryptocurrency exchanging cash to Supply chain and monitoring.
In simple words, we can say Blockchain is a system of recording information in a way that makes it hard or impossible to change or hack the system. A blockchain is largely a digital ledger of transactions that are duplicated and distributed across the whole network of laptop systems on the blockchain.Every block within the chain contains a variety of transactions, and every time a new transaction happens on the blockchain, a record of that transaction is added to each participant's ledger.
For our case we can use it for academic credential verification, which is useful for organizations that pay many money and hours per annum to validate new workers and avoid fraudulent credentials, the procedure is slow and pricey with ancient strategies and third party interference, blockchain offers distinctive digital assets that verify the credentials of educational degrees and certifications.

ملخص

تعد تقنية البلوكشاين واحدة من أقوى الاختراعات خلال الأعوام الماضية ، ولها تأثير هائل في أسلوب حياتنا ، بدءًا من تبادل العملات المشفرة إلى سلاسل التوريد والمراقبة.

بكلمات بسيطة، يمكننا القول أنه نظام لتسجيل المعلومات بطريقة تجعل من الصعب أو المستحيل تغيير أو اختراق النظام. البلوكشاين هو إلى حد كبير دفتر رقمي للمعاملات التي يتم تكرارها وتوزيعها عبر الشبكة الكاملة لأنظمة الكمبيوتر المحمول على البلوكشاين. تحتوي كل كتلة داخل السلسلة على مجموعة متنوعة من المعاملات ، وفي كل مرة تحدث معاملة جديدة على البلوكشاين ،يضاف تسجيل بتلك المعاملة إلى دفتر كل مشارك في النظام.

بالنسبة لحالتنا ، يمكننا استخدام اليلوكشاين للتحقق من بيانات الشهادات الأكاديمية ، وهو أمر مفيد للمؤسسات التي تدفع المال و الوقت سنويًا للتحقق من صحة العمال الجدد لتجنب الببيانات المزورة ، والإجراء بطيء ومكلف بسب الاستراتيجيات القديمة وتدخل الطرف الثالث ،تقدم تقنية البلوكشاين أصولًا رقمية مميزة للتتحقق من الأوراق الأكاديمية المعتمدة والشهادات التعليمية.

Dedication

I dedicate this dissertation work to My dear father Ahmed, my precious and beloved mother Souheila, and especially my grandfather Abdelouahab mercy be upon him who encouraged me to seek science during his life, who I truly wish he was with me today.
I don't forget my dear brothers and sisters and the beat of my heart my wife and of course the rest of the family and friends.

Acknowledgements

I am grateful to ALLAH for the guidance, good health, wellness and willpower that were necessary to complete this thesis.
I need also to thank my parents for their support during my studying journey and for believing in me, may ALLAH help me repay them.

Generale introduction

Academic credentials are a very important means to evaluate one's qualifications and set of skills in the job market. Employers depend on them in the process of identifying proper candidates for a certain job. The process of verifying these credentials has known slow improvements throughout the years compared to other fields which explain the growing cases of fraud related to academic credentials.
Furthermore, in this digital popular platforms are commonly used to publish people's qualifications without any background checks. Those checks are naturally ignored because they involve a complicated and lengthy procedure. So doing this kind of verification on such platforms is not even an option. Other e-learning platforms are facing similar problems when issuing certificates to users.
New solutions are continuously proposed to solve these problems but none proved to be really effective, like the digitization of credentials, which has been adopted by some higher education institutions and credential issuers where digital documents are signed using digital signatures and central databases are used for their storage. After a while, these solutions have proven to raise other issues, as relatively easy it is to forge paper-based credentials and documents, and it was also relatively easy to forge digitally signed ones.
The use of central databases has always had disadvantages and the lookup for alternatives is continuing. In these last few years, newer and more promising solutions have emerged using some newly developed technologies, important and even more promising ones are using what is now called Blockchain technology. Promising use-cases of blockchain technology were already identified in a multitude of stores, like logistics, payments, auditing and compliance, supply chain management, instance retail, and healthcare.
Research into how blockchain can be used in higher education is still in its first phases. In this work, we investigate the applicability of blockchain in the academic certification context.
In particular, we will focus on coming up with a blockchain-based solution to improve the processes of issuing and verifying academic credentials in the higher education system.
This thesis contains an Introduction that illustrates the context of our work, the targeted problem, and the solution we will try to apply.
The first chapter named "Blockchain technology" included a brief history and the used network before heading to the definition and explaining how it works, then moving to the structure of a blockchain mentioning the main types and characteristics. It was important to talk about Cryptography which is a big part of the technology, we included some use cases too.

In the second chapter "More in-depth", we went in-depth through Blockchain, explaining the details starting from Bitcoin and byzantine Generals Tolerance then Consensus algorithms the main component that affects the blockchain efficiency. After that, we talked about Ethereum so we can pass to the smart contract's part. The third chapter "Design and implementation" contains the objective and motivation of our work, the architecture of the system, and the tools we used. We finished the thesis with a General conclusion.

Chapter 1

Blockchain technology

1.1 introduction

The decentralized nature of blockchain networks makes industries like cryptocurrency and decentralized finance (DeFi) viable as evidenced by way of Bitcoin and Ethereum and supports hundreds of purposes throughout the spectrum of enterprise and human interaction.
Blockchain networks are driven by means of systems of aligned incentives.A well-functioning public blockchain requires a neighborhood of users, node operators, developers, and miners, who all play roles in a mutually really helpful community ecosystem. For instance : In many blockchain networks, rewards like newly minted cryptocurrency or transaction prices encourage network participants to compete to validate transactions and create new blocks. This incentive and validation structure also secures the community from criminal or fraudulent activity.

1.2 Blockchain History

It is essential to understand the history of Blockchain.So, to help knowing the Blockchain history and understand the Blockchain evolution, here we bring a brief the history of blockchain technology with its evolution[37].
In 1991, Stuart Haber and W. Scott Stornetta envisioned what has become known as blockchain. Their first project was to create a cryptographically safe chain of blocks that would prevent anyone from tampering with document timestamps.
They modified their system in 1992 to include Merkle trees, which increased efficiency and allowed them to collect more data on a single block. However, because to the activity of one person or group known as Satoshi Nakamoto, Blockchain History begins to take prominence in 2008.
Satoshi Nakamoto is accredited as the brains behind blockchain technology. Very little is known about Nakamoto as people believe he could be a person or a group of people that worked on Bitcoin, the first application of the digital ledger technology. Nakamoto conceptualized the first blockchain in 2008 from where the technology has evolved and found its way into many applications beyond cryptocurrencies. Satoshi Nakamoto re-

leased the first whitepaper about the technology in 2009. In the whitepaper, he provided details of how the technology was well equipped to enhance digital trust given the decentralization aspect that meant nobody would ever be in control of anything. Ever since Satoshi Nakamoto exited the scene and handed over Bitcoin development to other core developers, the digital ledger technology has evolved resulting in new applications that make up the blockchain History[1].

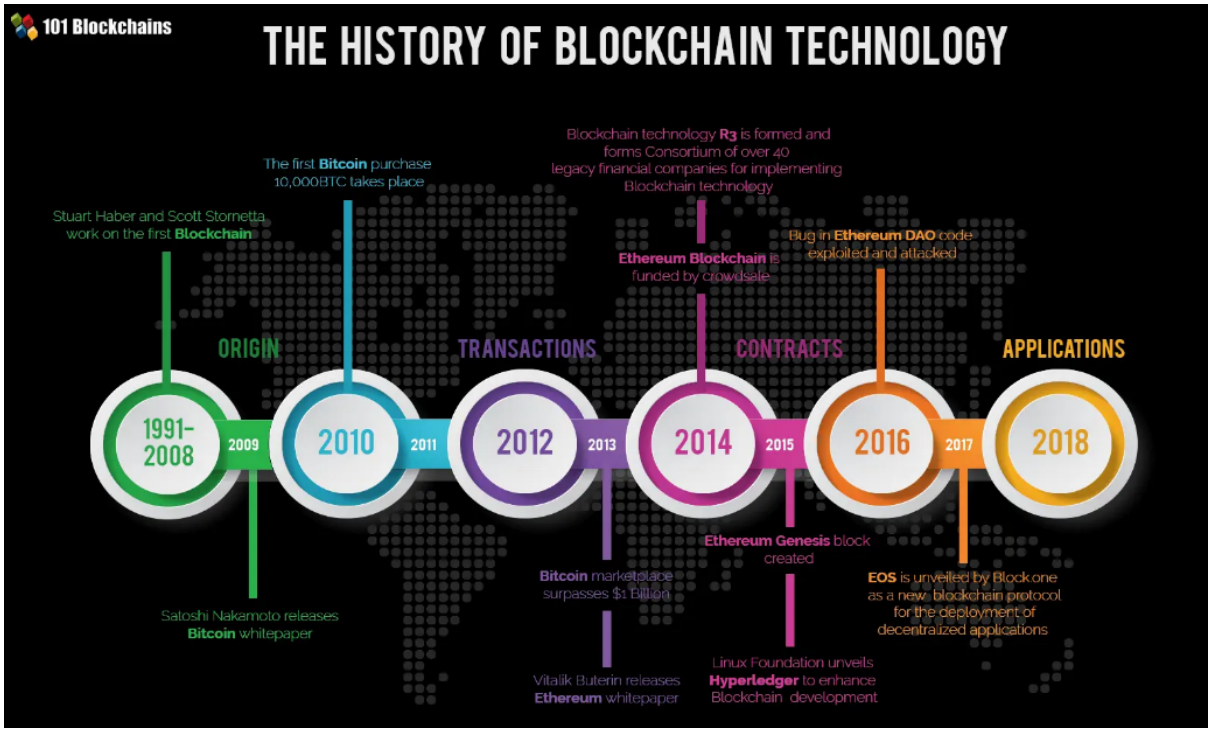


Figure 1.1: Blockchain example [1]

1.3 Blockchain Network

1.3.1 Decentralised network definition :

When discussing blockchain technology, the term “decentralized network” often comes up. But many individuals still have a problem with explaining what a decentralized network is.
Decentralised systems have no single authority to control the system or dictate the truth for other participants in the network and every participant can access the history of transaction and confirm new ones.
They are made possible by recent technological advancements that have equipped computers and other devices with a significant amount of processing power and can be synced up and leveraged for distributed processing[30].

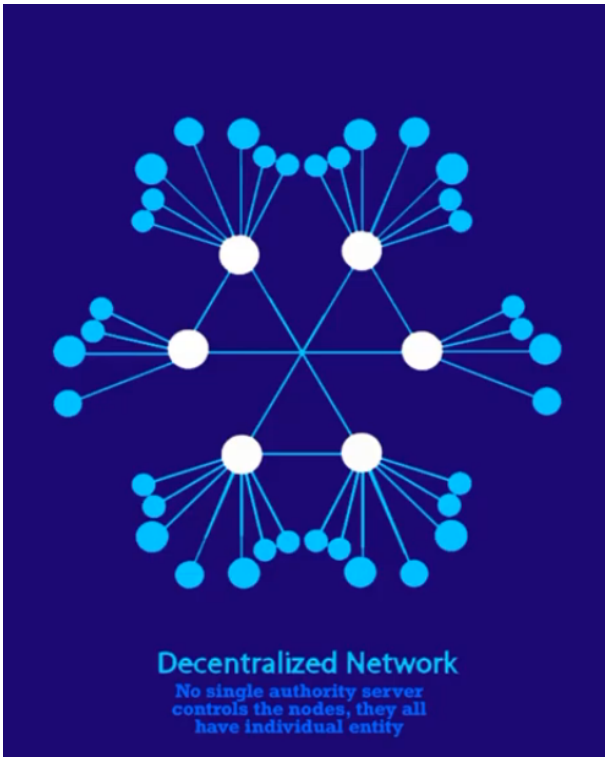


Figure 1.2: Decentralized network

1.3.2 Advantages

- Anonymity and privacy.
- Highly scalable ,and bandwidth is never an issue.
- Fraud Prevention: blockchains are open-sourced ledgers, all transactions are recorded all over the network, if there is fraud going on, it is quite easy to spot, The integrity of the system is monitored and maintained by a large number of miners who validate transactions , which gives decentralized blockchain an enormous amount of oversight and makes it nearly invulnerable to fraud .
- Faster transaction time .

1.3.3 Disadvantages

- More machines are needed in the system.
- High cost.

1.4 Blockchain definition

According to Don and Alex Tapscott a blockchain is: " The blockchain is an incorruptible digital ledger of economic transaction that can be programmed to record no just financial transactions but virtually everything of value "[2].

In other words a blockchain is a chain of data records that are distributed across a decentralised network of computers , with no central authority . each computer keeps its own copy of the ledger , and any update requires the approval of majority of machines in the network, that make it impossible to manipulate.
Each record is called a block, each block hold a section of data and a hash generated from the data contained in the block using cryptography . block are linked together by referring to the hash of the previous block .

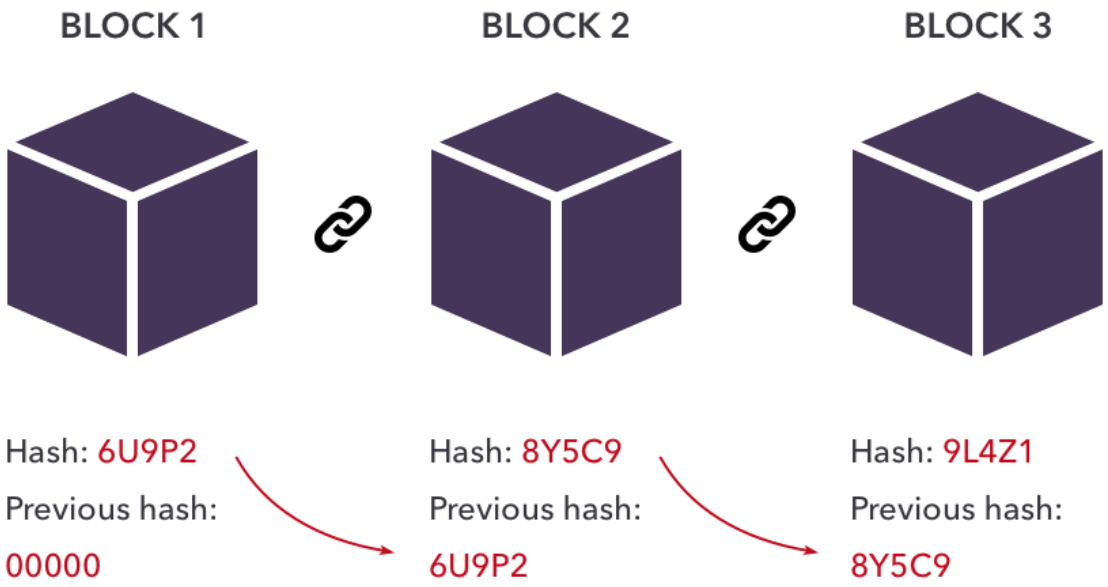


Figure 1.3: blockchain example

1.5 How it works

Blockchain protocol is essentially a digital ledger distributed, composed of digital transactions and shared over a network. This prototype is based on a peer-to-peer architecture, each participant constituting a node in the network. These participants store an identical copy of the general ledger then work together in the process of validating and certifying transactions digital, by adding new transactions to the general ledger[38].
The process of adding transactions involves evaluating the proposed transaction and to put it to a vote. If the majority of participants believe that the transaction is valid, it is added to the general ledger, which links it to the previous transaction, forming a chain that cannot be changed without breaking its integrity. Each transaction that goes through the binding process is grouped into a block, which additionally contains a cryptographic hash of the previous block, then is added linearly to the ledger in chronological order. Changes made to the general ledger are replicated throughout the network and, therefore, each participant has a complete copy of the ledger update. It also means that no participant has the capacity to attack easily the entire distributed network. Although the notion of transaction remains,the data associated with one can be of any type, because the Blockchain simply connects the data stored there.

The transaction format is defined by the underlying network supporting the Blockchain, while the data present in it is defined by the parties who create it. This data can be encrypted and digitally signed in order to provide the system with additional benefits such as authenticity, integrity and non-repudiation. Transactions are added to the chain when a specific consensus mechanism is verified.

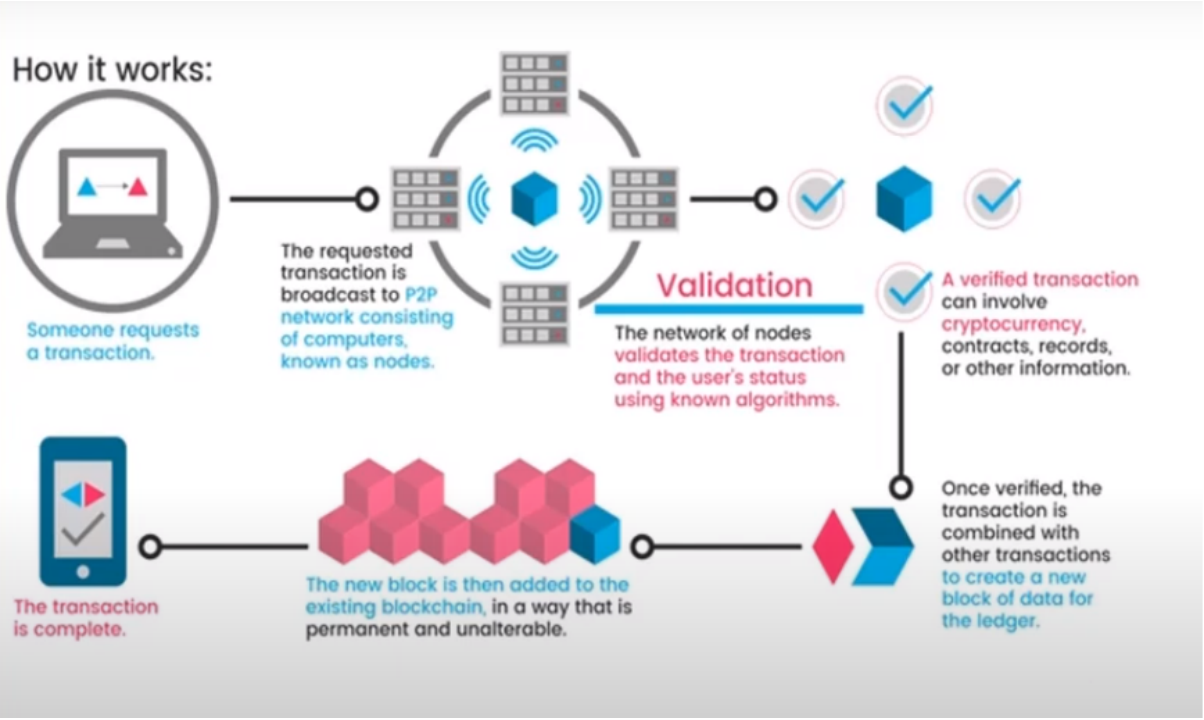


Figure 1.4: blockchain function

1.6 Blockchain Structure

A blockchain structure can be changed as need , here is a general structure :

- Block index : to identify the block in the serie
- Timestamp :a time of the creation of the block and time of records a transactions, its size 4 bytes.
- Nonce :an abbreviation for "number only used once" a random number needed for consensus process ,its size 4 bytes.
- previous hash : is hash of the preceding block which use to link it with the next block.This hash of block creates using cryptographic methods of SHA256 algorithm, the firs block(genesis) has no previous hash.
- Hash : hash of the actual block and its size is 32 bytes.

- Data :contains transactions or any type of shared information, it can be shaped as need.

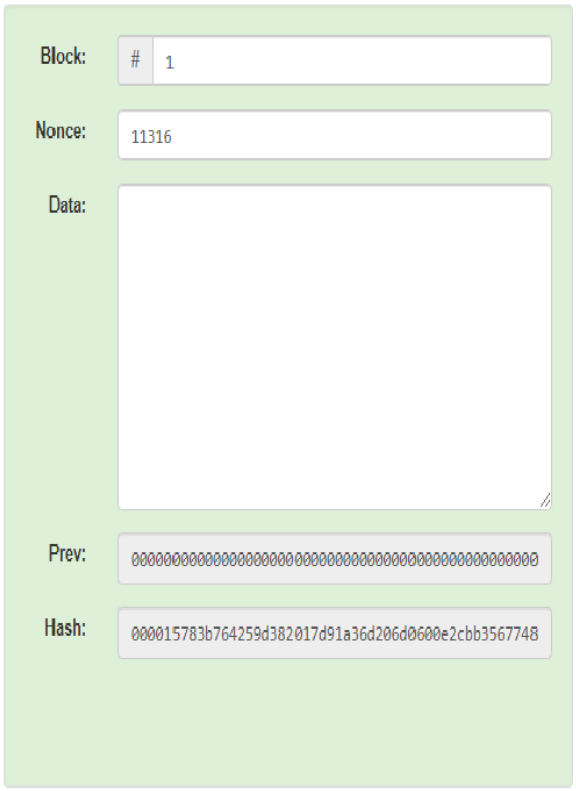


Figure 1.5: blockchain Structure

1.7 Blockchain characteristics

- Secure: blockchains are cryptographically secure, digital signatures ensuring that the data contained inside blocks has not been altered.
- Transparent: the ledger is shared among multiple peers of the network which means that any user of the network can see all the transactions from the creation of the blockchain to last recorded block.
- Immutable :Once you have agreed on a transaction and recorded it, it can never be changed. You can subsequently record another transaction about that asset to change its state, but you can never hide the original transaction. This gives the idea of provenance of assets, which means that for any asset you can tell where it is, where it's been and what has happened throughout its life[31].
- Decentralized: One of the core aspects of a blockchain is that it is a decentralized ledger, meaning that the data is maintained and held by all nodes in the network.

No central authority holds or updates the ledger. Also Every peer in the system has the authority to add new transactions. Every transaction that passes the consensus phase will get recorded on the ledger.

- Autonomy :"The computing power and the hosting space are provided by the nodes of the network, i.e. the users themselves. There is therefore no need for central infrastructures. Within a blockchain, the infrastructure is no longer concentrated in the hands of one organization but is, on the contrary, broken down into all the points of the network. A blockchain is therefore self-supporting and independent of third-party services"[4].
  Computing power and hosting space are provided by the network nodes, i.e. the users themselves. There is therefore no need for central infrastructure. Within a blockchain, the infrastructure is no longer concentrated in the hands of one organization but is, on the contrary, broken down into all the points of the network. A blockchain is therefore self-supporting and independent of third-party services[4].

1.8 Blockchain types

1.8.1 Public blockchain

A public blockchain is a permissionless blockchain. any one can join the network , they can read or write and participate freely.
public blockchain are decentralised, no one has control over the network and they are secure in that, the data can't be changed once validated on the chain [32].

example : bitcoin , etherium

Figure 1.6: Bitcoin and Ethereum

1.8.2 Private blockchain

Private blockchain is a permissioned blockchain, where it places restrictions on who is allowed to participate in the network and in transactions.
it can be adopted in the corporate sector where the details need to be shared only between certain nodes. A group of banks, for example, may create a private blockchain where financial transaction details are only shared with the parties involved.

Figure 1.7: private blockchain

1.9 Cryptography in blockchain

Cryptography tools are used to guarantee the integrity of the blockchain, the identity of the participant, the authenticity of the transactions and the confidentiality of the content. There is three types of cryptography :symmetric-key cryptography, asymmetric-key cryptography and hash.

1.9.1 symmetric-key cryptography(Private key encryption)

In this case data is encrypted using a single key which is known for both sender and receiver , the same key is used in decryption. It's an easy method but the problem is that the key should remain known only for sender and receiver, if any other one can reach the key , information would be exposed.
Example : in the figure , Tom shell send a message to Mary.

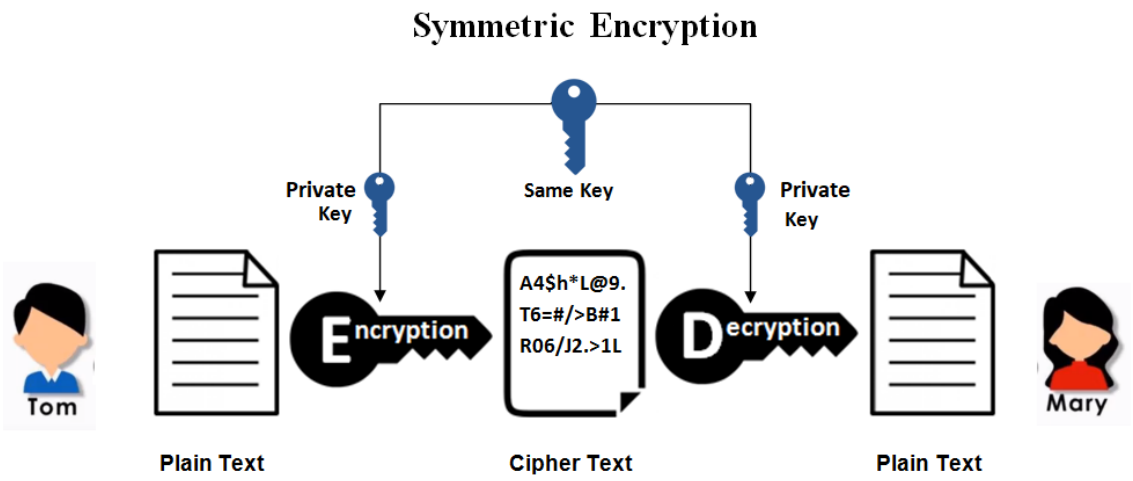


Figure 1.8: symmetric-Key cryptography

1.9.2 asymmetric-key cryptography(Public Key Encryption)

In Public key encryption two different keys mathematically related are used to encrypt and decrypt data .
The first one is public key which could be known for any one , the second is private key which is private and not shared .
Example : in the figure , Tom shell send a message to Mary .

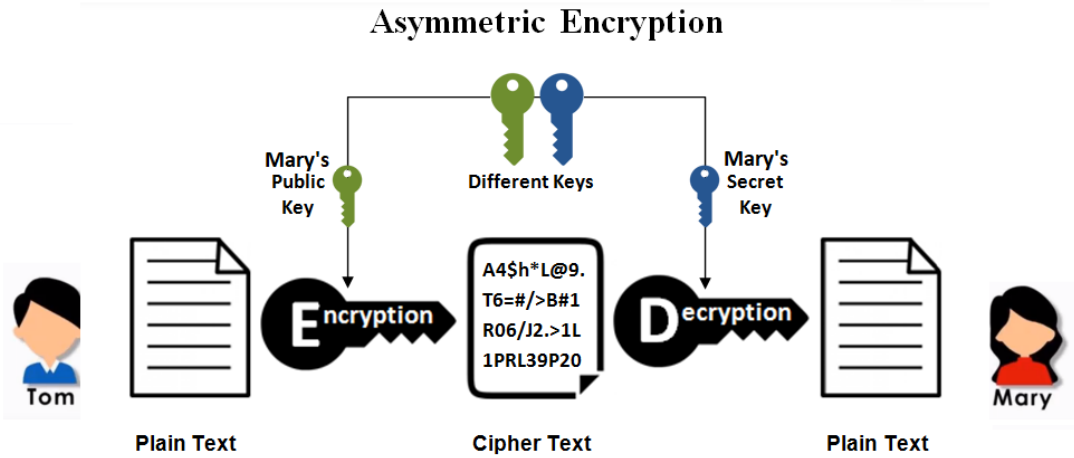


Figure 1.9: asymmetric-Key cryptography

1.9.3 Hash

A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic byproduct of a hash algorithm [5].

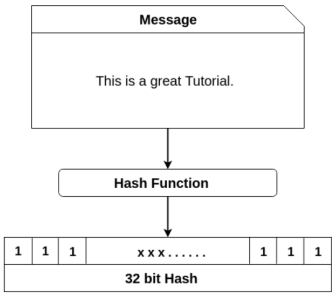


Figure 1.10: private blockchain

Hash must respect the following rules and properties:

- The length of the imprint must always be the same.
- It is not possible to find the original data from the fingerprints: the hash functions only work in one direction.
- It must not be possible to predict a signature.
- for different data the signatures must be different.

some of hash functions:
SHA256, SHA512, SHA1 , MD5 .
The hash function is used in particular to chain the blocks together. Thus, the header of a block contains the hash, result of the application of a hash function, of the previous block. This hash is a key part of the integrity of the blockchain. if an attacker of the system modifies the contents of a bm block, anyone can detect it by calculating the hash of the block, and comparing this result with the hash stored in the following block to see if there is an inconsistency.

1.9.4 Digital signature

Digital signatur is a cryptography proof technique that can aid in the establishment of trust on the blockchain.Trust in the blockchain system ensure that the message originate from a specific source, thereby avoiding out any concerns of hacking or other conflicts. Digital signatures are similar to stamped seals or handwritten signatures we use on paper.

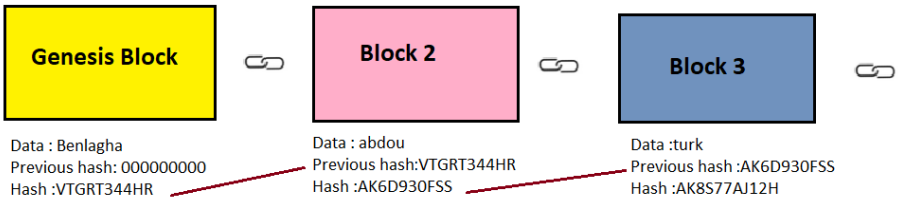


Figure 1.11: Hash

Digital signatures follow the specific precedents of asymmetric cryptography by linking two different keys with mathematical links. The keys include a private key and a public key. It is possible to deploy a digital signature system with the help of a secure hash function.[6]
Digital signature serves three purposes :

- Authentification : giving the receiver a proof that the message was created and send by the claimed person .
- Non-repudiation : the sender cannot deny sending the message .
- Integrity : ensures that the message was not altered in transit

The figure explains how Bob send a plain message with digital signature

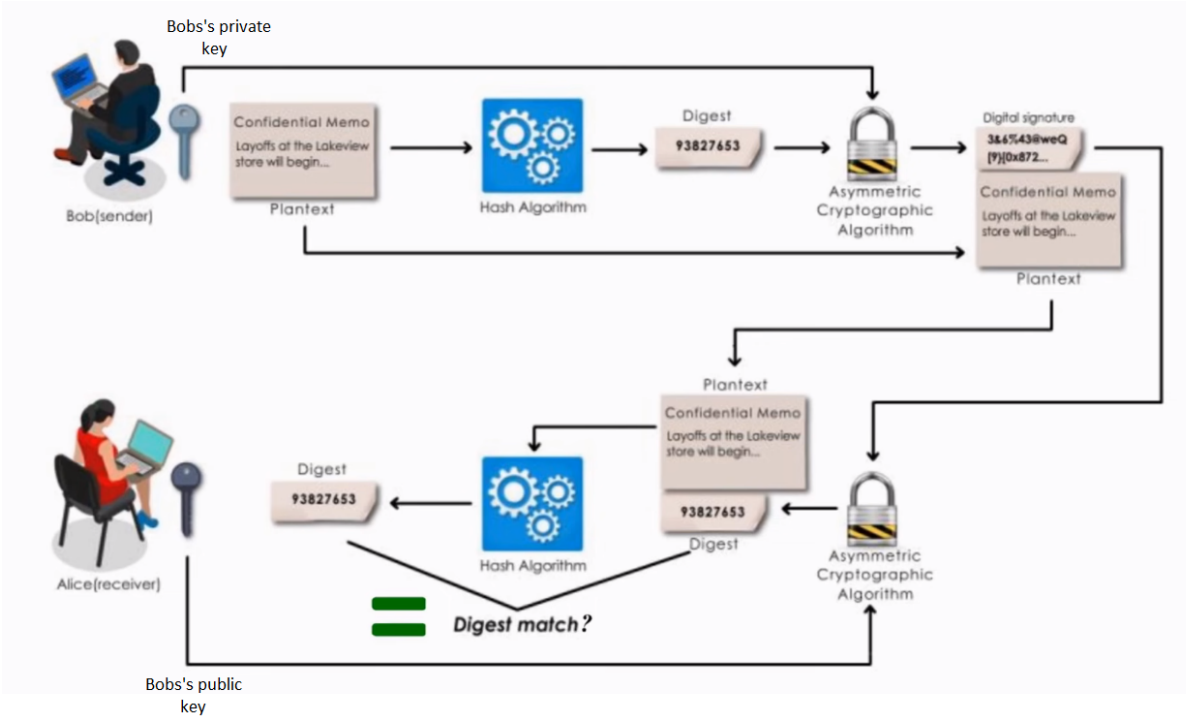


Figure 1.12: Digital signature

1.10 Blockchain use cases

1.10.1 Vote

Voting is a method allows a group to take a joint decision. Formal or informal organizations resort to this practice, of all kinds (economic, political, associative, etc.).Voting is used to add legitimacy to a choice by demonstrating that it is not the result of a single person's judgment.
Knowing that traditional elections require a significant investment of human, material, and financial resources, as well as tedious and unpleasant procedures for citizens in terms of time and effort. Furthermore, because this approach imposes intermediary authority who might fake the outcome, neither the traceability, integrity, nor openness of the vote computations can be guaranteed.
The traditional web's electronic voting system simplifies voting procedures and reduces resource and time consumption, but neither transparency nor data integrity are guaranteed because the whole electronic voting system is centralized on a server controlled by a third party. The data can be easily changed on the inside, knowing that the application's code is a black box. As a result, the issue of trust and transparency persists, and web-based voting apps face server overload throughout the voting phase.
the blockchain promises a secure and inviolable vote whose result transparent and reliable, is auditable by all, even if the results of votes are publicly displayed on the blockchain the identity of the people voting cannot not be known through the public key / private key system. The identity is thus protected, and questions related to a fraudulent selection are excluded.
Example of some Platforms use Blockchain for voting :

Figure 1.13: Platforms use Blockchain for voting

1.10.2 Insurance

Insurance is an agreement in which an individual or institution receives financial protection or compensation from an insurance provider in the event of a loss, represented by a policy. Insurance is a widely practiced method of security all over the world. According to a statistical report, the global insurance market is valued at over 5050.3 billion US dollars for 2021 [7]. There are various types of insurance policies for health, business,

and vehicles. These policies are prevalent in developed countries around the world. In much of Europe, Latin America, Canada, Australia, and Japan, national health insurance schemes are in existence through national policies[8].
Despite the widespread use of insurance plans, resolving claims is not always a simple and painless process. Insurance companies frequently refuse to pay the insured because the conditions and terms were misrepresented. False claims are another set of issues that insurance firms are dealing with.Contractual procedures that have been in use for a long time are not without flaws. These contracts are unclear and include loopholes. In many cases, both insurers and insureds take advantage of these loopholes. Smart contracts on the blockchain can change these conditions because they minimize the need for trust and financial risk in conventional agreements while still providing legal clarity like "ETHERISC" does , which is an open-source development platform that focuses on decentralized insurance applications.

Figure 1.14: ETHERISC

Six alternative decentralized insurance-related applications have already been created by therisc. One of these is a crop insurance app that allows farmers to track their land and crops, as well as any weather-related losses.

1.10.3 Medicine

Healthcare is a data-intensive clinical domain where a huge amount of data are generated, accessed, and disseminated on a regular basis. Storing and disseminating this large amount of data is crucial, as well as significantly challenging, due to the sensitive nature of data and limiting factors, such as security and privacy[9].
Through safe and secure data exchange, blockchain is changing existing healthcare methods to a more dependable way of successful diagnosis and treatment. In the future, blockchain might be a tool that helps with personalised, authentic, and secure healthcare by combining all of a patient's real-time clinical data and presenting it in an up-to-date secure healthcare setting.
BurstIQ's platform enables healthcare organizations to manage huge volumes of patient

data in a safe and secure manner. It could aid in the eradication of opioid or other prescription drug misuse since it contains full and up-to-date information about individuals' health and healthcare activity.

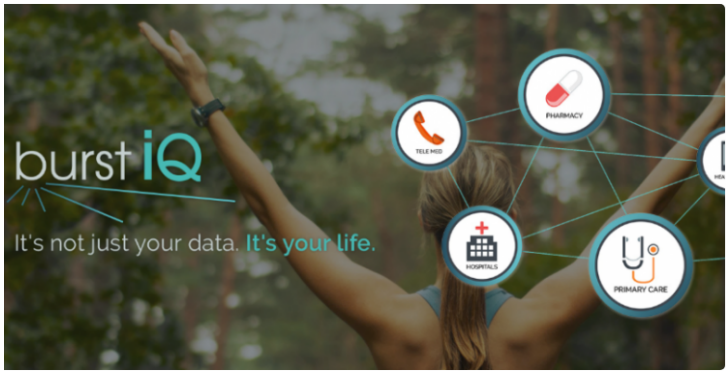


Figure 1.15: BurstIQ

Many other companies in health around the globe field are concerned with blockchain such as Factom ,Medicalchain , Guardtime.

1.10.4 Document certification

Certificates confirm the achievement of certain learning outcomes. Until today, certificates are usually issued on paper, which has several advantages. For example, recipients can easily store them and present them to any person and for any purpose. In addition, it is difficult to forge paper certificates if there are builtin security features. However, third parties need extra effort to verify paper certificates. Verification is usually achieved by asking the issuing certification authority, i.e. certification authorities have to maintain a long-term archive [10]. Various Blockchain-based implementations have been made. We can cite, for example, the civil status and the driving license based on Blockchain developed by the Australian government, the certification of diplomas or various notarial documents.

1.10.5 Art

Non-fungible tokens, or NFTs, have become a popular topic in the art world, with art pieces made using the technology selling for millions of dollars at auction. Crypto art and digital collectibles have emerged as a result of the development of NFTs, with artists, singers, and influencers increasingly turning to the technology to make more from their

authentic, one-of-a-kind work. NFTs may be used to authenticate real-world assets such as artworks and jewels, ranging from digital art and music to proof of authenticity paperwork. we would be explaining it with more details later.

Figure 1.16: NFT

That piece of NFT was bought by the the famous player Neymar Jr with more than 480,000 US dollars .

1.10.6 Cryptocurrency

One of the most significant creations of the recent blockchain technology in finance is cryptocurrency. Since the development of the first cryptocurrency, Bitcoin, in 2009, a number of cryptocurrencies have been initiated for fulfilling diverse needs and different purposes[11].
A cryptocurrency is a virtual currency used for a secure online payment without the use of third-party intermediaries Cryptocurrencies are digital or virtual currencies underpinned by cryptographic systems. They enable secure online payments without the use of third-party intermediaries.

Figure 1.17: Most popular cryptocurrencies

1.11 Conclusion

In the first chapter we have introduced blockchain with a short historical view and how the this technology works, we talked about the main structure and a few characteristics of blockchain then the types we should know, cryptography in blockchain and finally numbered important use cases. Blockchain is vast we can't cover it in one chapter, the second chapter would contain more valuable details.

Chapter 2

More in Depth

2.1 Introduction

In the previous chapter, we have seen the basics of the blockchain and a theoretical view, in order to fully understand we need to talk about cryptocurrencies which were the main reason for inventing the technology. And of course without forgetting the consensus algorithms and smart contracts.

2.2 The first application of blockchain (Bitcoin)

bitcoin was invented in 2008 with the publication of a paper titled "Bitcoin: A Peer- to-Peer Electronic Cash System," written under the alias of Satoshi Nakamoto . Nakamoto combined several prior inventions such as b-money and HashCash to create a completely decentralized electronic cash system that does not rely on a central authority for currency issuance or settlement and validation of transactions. The key innovation was to use a distributed computation system (called a "Proof-of-Work" algorithm) to conduct a global "election" every 10 minutes, allowing the decentralized network to arrive at consensus about the state of transactions. This elegantly solves the issue of double-spend where a single currency unit can be spent twice. Previously, the double-spend problem was a weakness of digital currency and was addressed by clearing all transactions through a central clearinghouse[12].
In 2009, the bitcoin network was launched based on Nakamoto's reference implementation that he published, which has since been modified by a number of other programmers. The Proof-of-Work algorithm (mining) that ensures bitcoin's security and resilience has grown exponentially in power, and now exceeds the combined processing capacity of the world's top supercomputers. Bitcoin's total market value has at times exceeded 135 billion US dollars, depending on the bitcoin-to-dollar exchange rate. The largest transaction processed so far by the network was 400 million US dollars, transmitted instantly and processed for a fee of one US dollar.

Satoshi Nakamoto withdrew from the public in April 2011, leaving the responsibility of developing the code and network to a thriving group of volunteers. The identity of the person or people behind bitcoin is still unknown. However, neither Satoshi Naka- moto nor anyone else exerts individual control over the bitcoin system, which operates based on fully transparent mathematical principles, open source code, and consensus among participants. The invention itself is groundbreaking and has already spawned new science in the fields of distributed computing, economics, and econometrics[12].

Figure 2.1: Bitcoin over the past few years

The bitcoin protocol stack, available as open source software, can be run on a wide range of computing devices, including laptops and smartphones, making the technology easily accessible. Users can transfer bitcoin over the network to do just about anything that can be done with conventional currencies, including buy and sell goods, send money to people or organizations, or extend credit.
Users of bitcoin own keys that allow them to prove owner- ship of bitcoin in the bitcoin network. With these keys they can sign transactions to unlock the value and spend it by transferring it to a new owner. Keys are often stored in a digital wallet on each user's computer or smartphone, Possession of the key that can sign a transaction is the only prerequisite to spending bitcoin, putting the control entirely in the hands of each user.

Figure 2.2: Most popular wallets

2.3 Byzantine Generals Problem

Most blockchains work as a decentralised digital ledger which is maintained by a distributed network of computers. such technology allowed the creation of trustless economic system with out involving third parties , since traditional banking and payment systems rely heavily on "trust".
cryptocurrencies are being adopted as viable alternative, because they are rely on blockchain technology and used within trustless systems. The participants of a cryptocurrency network have to regularly agree on the current state of blockchain and that's what we call a "consensus achievement",however reaching consensus in distributed systems in a secure and efficient way is far from been easy task.
How can a distributed network of computing nodes agree on a decision if some nodes may fail or act dishonestly ?! this is the fundamental question of the "Byzantine Generals Problem", which gave birth to the concept of "Byzantine Fault Tolerance"[34].
A Solution to a Distributed Computing Problem Satoshi Nakamoto's invention is also a practical and novel solution to a problem in distributed computing, known as the "Byzantine Generals Problem." Briefly, the problem consists of trying to agree on a course of action or the state of a system by exchanging information over an unreliable and potentially compromised network. Satoshi Nakamoto's solution, which uses the concept of Proof-of-Work to achieve consensus without a central trusted authority, represents a breakthrough in distributed computing and has wide applicability beyond currency. It can be used to achieve consensus on decentralized networks to prove the fairness of elections, lotteries. asset registries, digital notarization, and more[12].

For more explanation , let's imagine that each general has his own army and each group is deployed in different locations around the target city, the generals need to agree on either attacking or retreating.

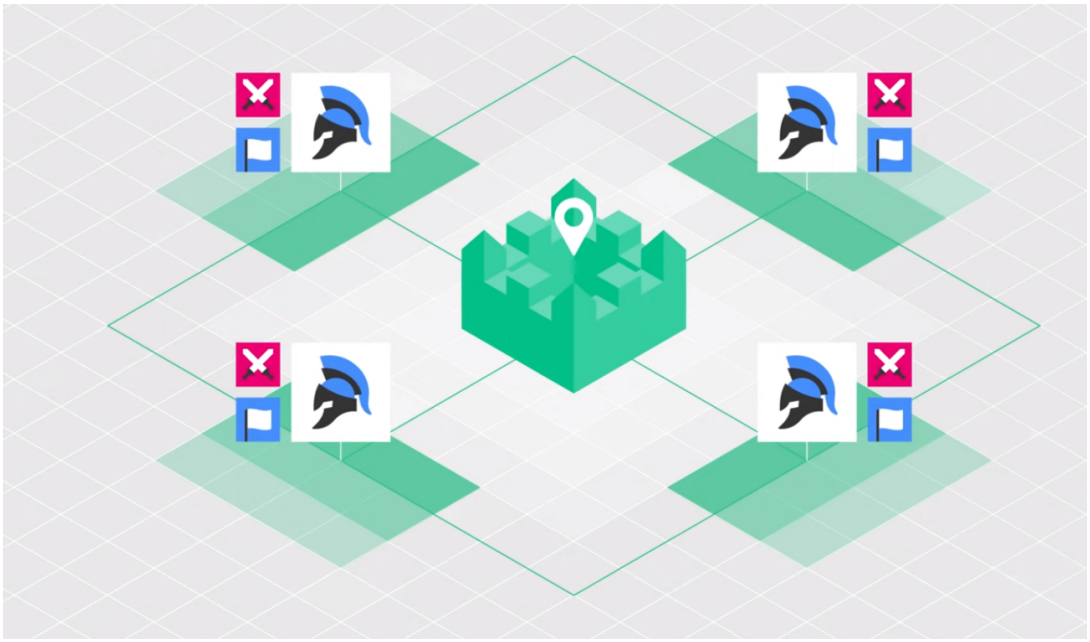


Figure 2.3: Byzantine Generals Problem

It doesn't matter whether they attack or retreat as long as they all agree on a common decision, so we should keep in mind the following requirements :
1) each general has to decide and vote on either attacking or retreating.
2)after the vote is made it can not be changed .
3)all generals must agree on the same decision and execute it in a coordinated manner .
however, they can only communicate through messages and the main challenge of the Byzantine Generals Problem is that the messages can somehow end up being delayed or destroyed or lost . even in the case of a successful delivery , one general or two may choose for whatever reason , to send fraudulent message to confuse the rest leading to a complete system failure .
if we apply the dilemma on the blockchains , each general represents a network node , they need to reach consensus on the current state of the system . this means that the majority of participates in a distributed network have to agree and execute the same action in order to avoid failures .

2.3.1 Byzantine Fault Tolerance

Byzantine Fault Tolerance : is a property of systems that are able to resist the types of faults derived from the Byzantine Generals Problem , in other words a Byzantine Fault Tolerance system is able to continue operating even when some nodes fails to communicate or act maliciously .
There are multiple ways to build a Byzantine Fault Tolerance blockchain, related to the different types of consensus algorithms. consensus algorithms are the mechanism through which a blockchain network reaches consensus, the algorithm used by Bitcoin is called proof of work and is one of the most common implementations.
While the bitcoin protocol defines the rules, the consensus algorithm determines how those rules will be followed, for example: during transaction validation.
The concept of proof of work is older than cryptocurrencies , but Satoshi Nakamoto developed a modified version that allowed Bitcoin to be created as a Byzantine Fault Tolerance system[33].

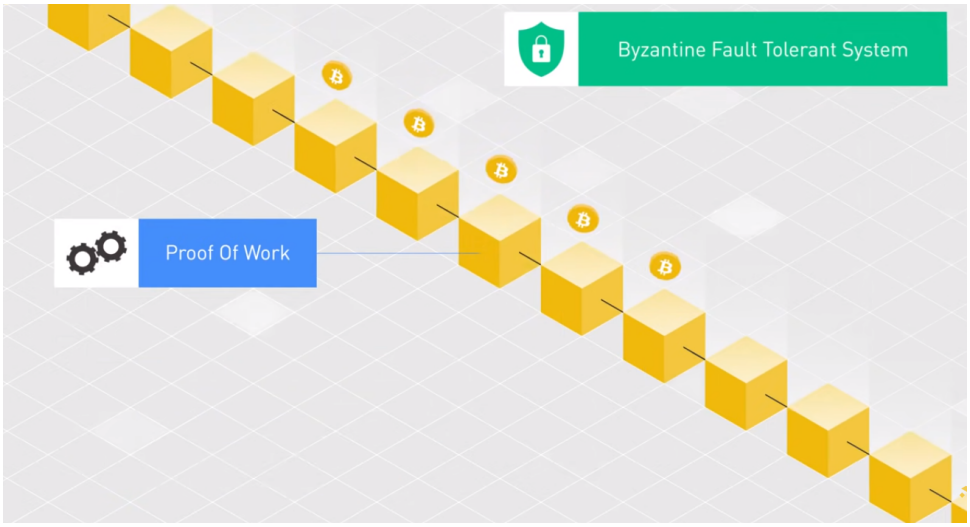


Figure 2.4: A Fault Tolerance system

2.4 Consensus algorithms

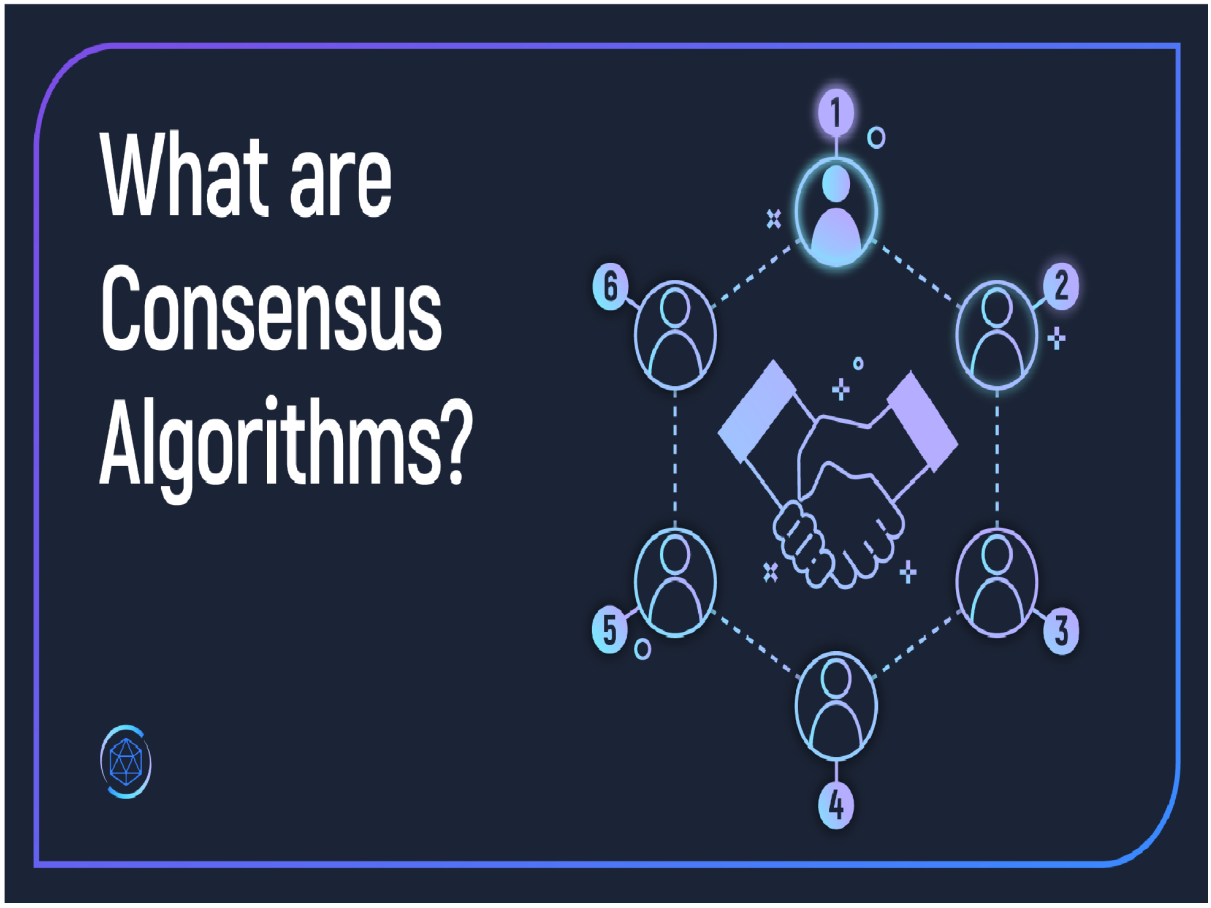


Figure 2.5: What are Consensus algorithms

To update the ledger, the network needs to come to consensus using an algorithm. Arriving at consensus on a distributed network means that everyone agrees on the current state of the ledger (e.g., how much money does each account have) and confirms that no one is double-spending their money.
Coming to consensus is a computer science problem in fault-tolerant distributed systems. Generating a consensus means that multiple servers on the distributed network agree on the current truth state of the system, or in the basic Blockchain case, values in the ledger. Once the network computers reach a decision on a value, that decision is final. In the classical computer science context, consensus algorithms are used to agree on the commands in the logs of the distributed servers. In Blockchain networks, the three main kinds of consensus algorithms for arriving at consensus in a distributed manner are Proof of Work (POW), Proof of Stake (POS), and Practical Byzantine Fault Tolerance (PBFT)[35].The main innovation of the Blockchain protocol is the Blockchain data structure on top of a consensus algorithm, which makes it possible to build an open distributed network in which all of the parties can reach agreement[13].

This section introduces the most popular proof-based consensus algorithms.The original work is PoW, Many different proof-based consensus techniques have been developed so far, which are based on PoW, PoS, their hybrid form, additional variations that are developed later.

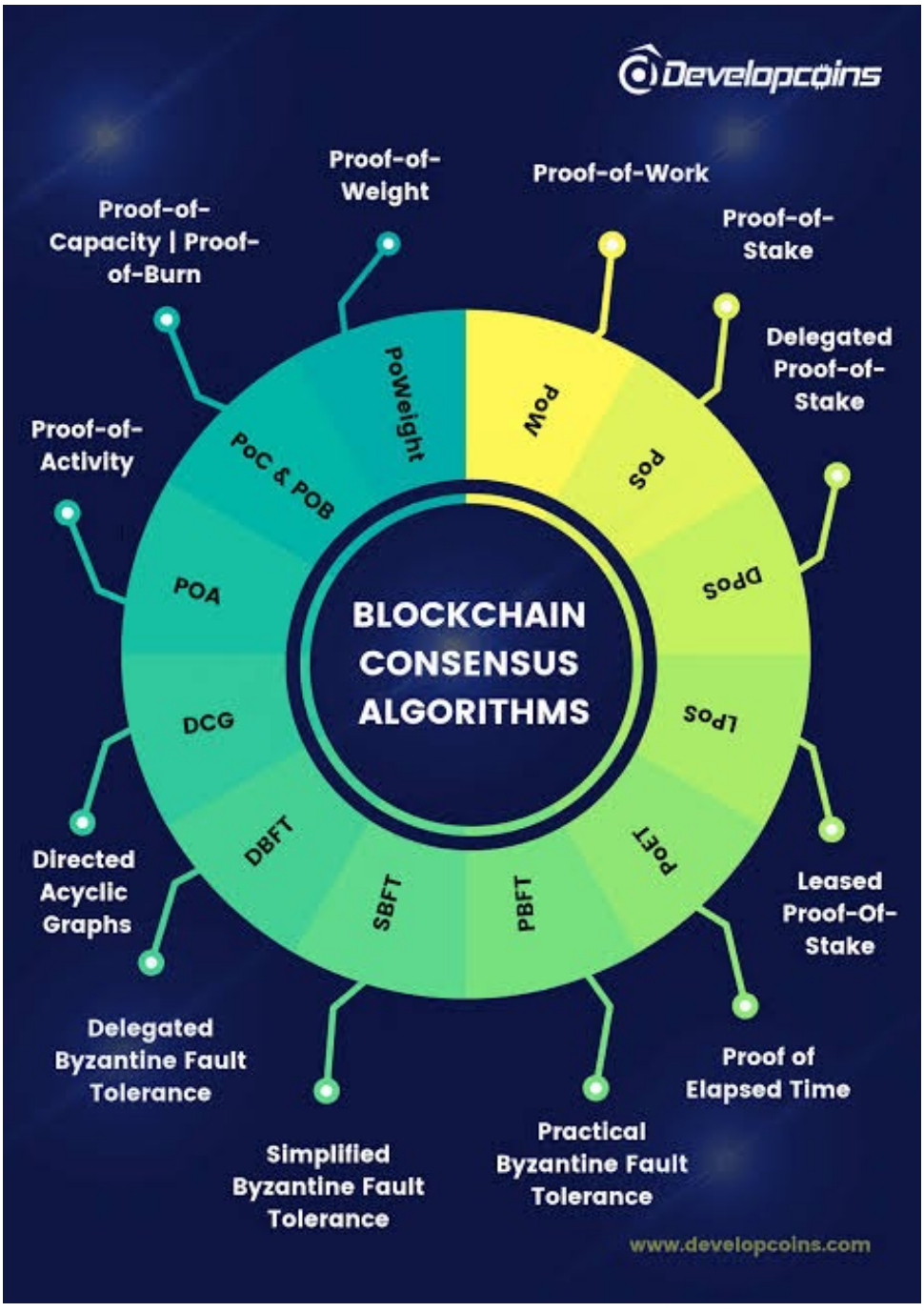


Figure 2.6: Consensus algorithms[14]

2.4.1 Proof of work

Proof of work is an algorithm or a system that uses significant amount of effort to deter or eliminate fake uses of computing power, launched on the bitcoin network in 2009 . Proof of work was designed to solve the problems of double spending which if unchecked could be a major issue for crypto projects[36].

Figure 2.7: Proof of work

A Proof of Work (PoW) mechanism involves two different parties (nodes): prover (requestor) and verifier (provider). The prover performs a resource-intensive computational task intending to achieve a goal and presents it to a verifier or a set of verifiers for validation that requires significantly less resource. The core idea is that the asymmetry, in terms of resource required, between the proof generation and validation acts intrinsically as a deterrent measure against any system abuse[15].
Within this aim, the idea of PoW was first presented by Dwork and Naor in their seminal article in 1993. They put forward the idea of use PoW to combat email spamming. According to their proposal, an email sender would be required to solve a resource-intensive mathematical puzzle and attach the solution within the email as a proof that the task has been performed. The email receiver would accept an email only if the solution can be successfully verified.
Within the blockchain setting, a similar concept has been adopted. Each PoW mechanism is bound to a threshold, known as the difficulty parameter in many blockchain systems. The prover would carry out the computational task in several rounds until a PoW is generated that matches the required threshold, and every single round is known as a single proof attempt .PoW has been the most widely-used mechanism to achieve a distributed consensus among the participants regarding the block order and the chain state[15].

Currency	Genesis date (dd.mm.yyyy)	Block reward	Total supply (Million)	Block Time
Bitcoin/Bitcoin Cash [69] [70]	03.01.2009	12.5	21	10m
Syscoin [71]	16.08.2014	80.04659537	888	1m
Peercoin [72]	19.08.2012	55.17265345	2000	10m
Counterparty [73]	01.02.2014	All currency in circulation	2.6m	-
Emercoin [75]	11.12.2013	Smooth emission	41	10m
Namecoin [76]	19.04.2011	12.50000000	21	10m
Steem Dollars [77]	04.06.2016	Smooth emission	Unlimited	3s
Crown [78]	08.09.2014	1.8	42	1m
XP	24.08.2016		2220	NA
Omni (Mastercoin) [79]	31.07.2013	16.71249999 Omni	0.6	20s

Figure 2.8: cryptocurrencies that utlise Nakamoto consensus algorithm.

The provers are chosen according to their hash rate ,the higher hash rate was , the chances are higher to add the block . in general , any CPU can do mining but with a low hash rate , but nowadays special equipment is used .

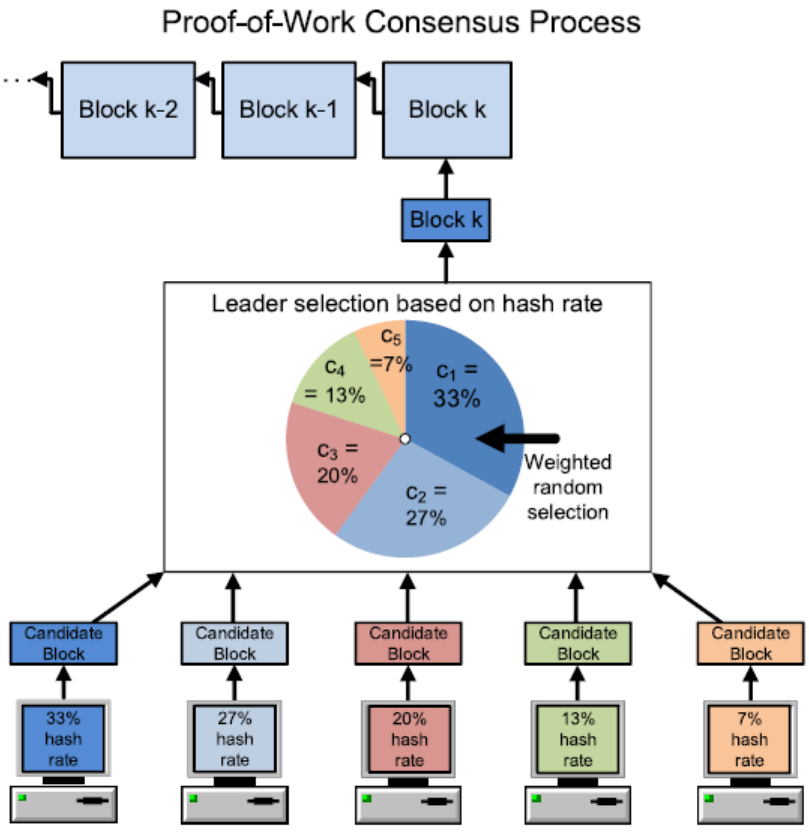


Figure 2.9: Leader selection in mining[16]

In Bitcoin which is maintained by the collective work of decentralized nodes, some of these nodes known as miners(prover) and are responsible for adding new blocks into the blockchain.
Miners on network will compete against each other in solving complex computational puzzles , these puzzles are difficult to solve but easy to verify the correct solution . Once a miner has found the solution to the puzzle , they will be able to broadcast the block to the network where all the miners will then verify that solution is correct .in order to do so , miners need to try and guess a pseudo random number named "Nonce" , when this number combined with the data provided in the block and passed through a hash function , must produce a result that matches given conditions.

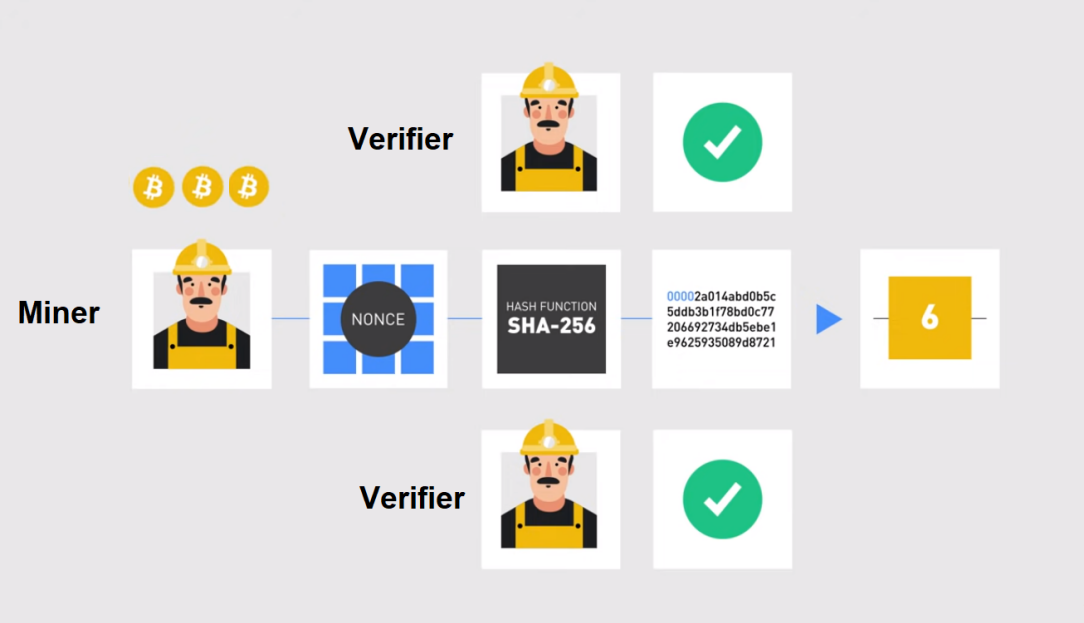


Figure 2.10: cryptocurrencies that utilise Nakamoto consensus algorithm.

When matching result is found , the other nodes will verify the validity of the outcome and the miner node is rewarded with the block reward. Therefore, it is impossible to add new block into the main chain without first finding a valid nonce . which in turn generates the solution of specific block called "block hash", each validated block contains a block hash that represents the work done by the miner, this is way it called Proof of work.
One issue with proof of work is that mining requires expensive computer hardware that consumes a large amount of power and while the complicated algorithme calculation guarantee the security of the network, these calculations are not able to be utilized beyound that.

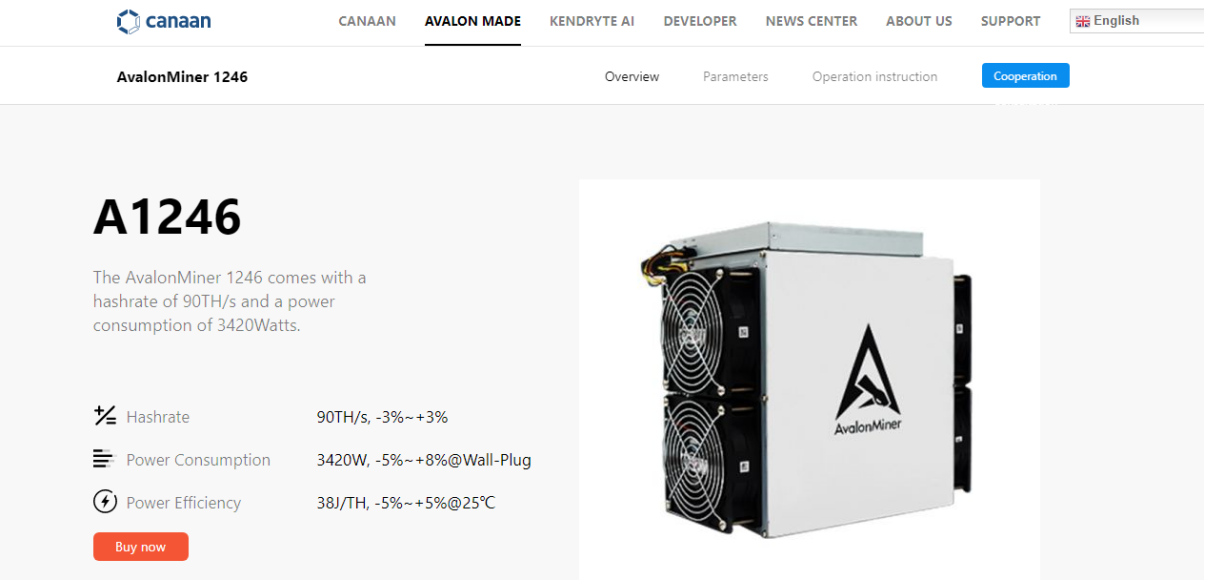


Figure 2.11: The AvalonMiner 1246

This beast coasts more than 7000 dollars which is really expensive , beside the issue of high cost there is the absence of penalties for malicious miners . Proof of work may be not the most efficient solution , but it is still one of the most popular methods of reaching consensus in blockchains.

2.4.2 Proof of stake

Based on the PoW framework, the Proof-of-Concepts (PoX) consensus mechanisms have been developed with two major aims: to replace the PoW solution searching with useful calculations and to improve the performance of PoW in terms of security, incentives, and resource usage. To make better use of the computational resource, several consensus mechanisms require the participants to solve practical mathematical problems such as searching for three types of prime number chains in Primecoin [17], solving matrix product problems in Proof-of Exercise [18], and calculating useful functions in Proof-of-Useful-Work [19].
The first Proof-of-Stakes (PoS) network, Peercoin [20], was developed as a PoX consensus mechanism with the aim to reduce the computational requirements of PoW. Participants with higher coin age, i.e., product of network tokens and their holding time, have higher chances to be selected. Specically, each node in Peercoin solves a PoW puzzle with its own difficulty, which can be reduced by consuming coin age.
In the more recent PoS networks, the solution searching is completely removed, and the block leaders are no longer selected by computational power. Instead, they are selected based on the stakes that they are holding[16].
With the stake-based leader selection process, a node's chance to be selected to be a leader no longer depends on its computational power, and thus energy consumption of PoS mechanisms is significantly reduced compared with that of PoW. Moreover, the block generation and transaction confirmation speeds are kept at relatively low constant rates

by the PoW networks to ensure security because there are many different blocks proposed by the miners. In contrast, since only one block is made in each round of PoS mechanisms, the block generation and transaction confirmation speeds are usually much faster, and thus PoS mechanism starts to become popular recently[15].

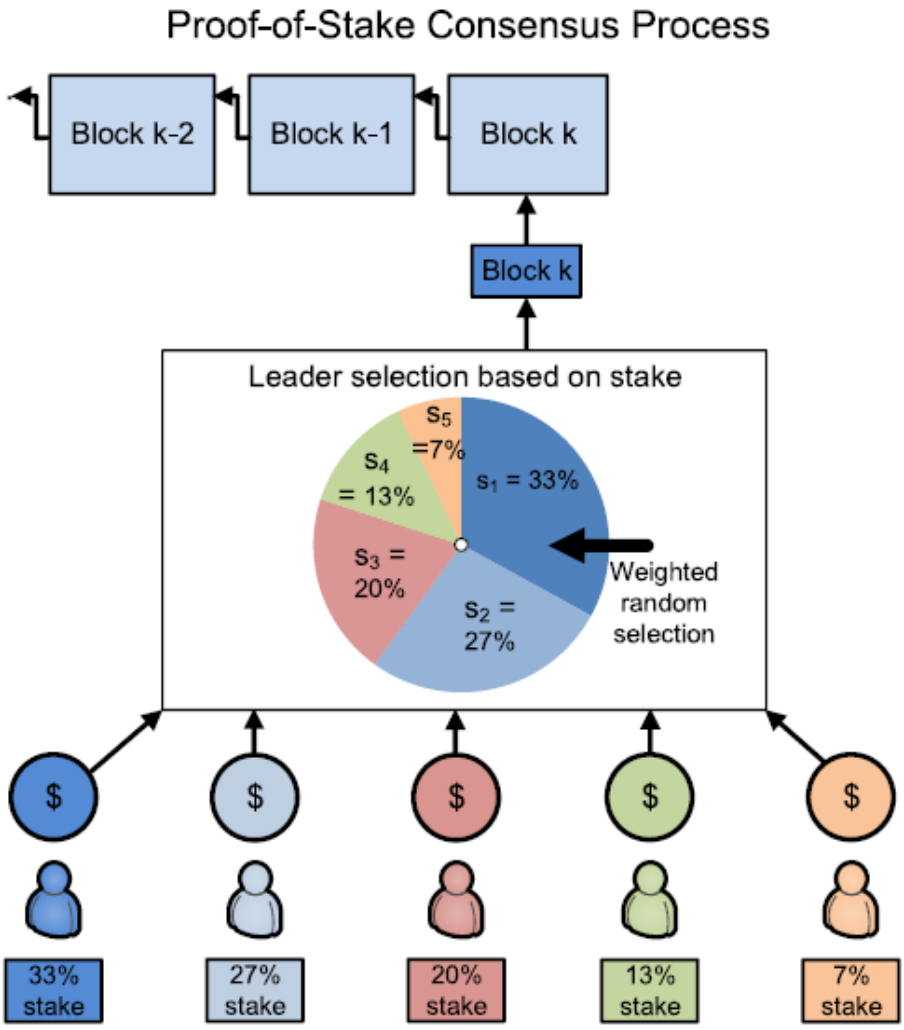


Figure 2.12: Leader selection in POS[16]

Proof-of-Stake (PoS) protocols were developed as energy-saving alternatives to PoW. Instead of computational power resources, leaders are selected based on their stakes, i.e., contributions to the blockchain network. Particularly in the PoS consensus mechanism, the stake of a node is the number of digital tokens, e.g., coins in cryptocurrencies, that it holds or deposits. Instead of consuming a lot of energy for the searching process as in the PoW, a leader will be selected based on its stakes to perform mining process and add a new block to the chain.
Besides the advantage of low energy consumption, the PoS mechanisms have faster trans-

action confirmation speed than that of the PoW mechanisms. In a blockchain network, the confirmation of a transaction depends on two main factors, namely transaction throughput and block confirmation time. The transaction throughput is the number of transactions per second Tx/s a network can process, which is vital to the performance of the network especially when there are many pending transactions[16].

2.4.3 Delegated Proof of stake

Delegated Proof of Stake (DPOS) is an innovation over standard PoS whereby each node that has stake in the system can delegate the validation of a transaction to other nodes by voting. This is used in the bitshares blockchain[21].

Figure 2.13: Delegated Proof of stake mechanism

With delegated proof of stake , computers don't compete over each other computational power or chosen based on thier stakes ,instaed the network users vote for the computers who they think are the best qualified to run the network .
the computers that run the network block producers , they are rewarded with tokens or a part of the fee of the transaction for running the network properly.

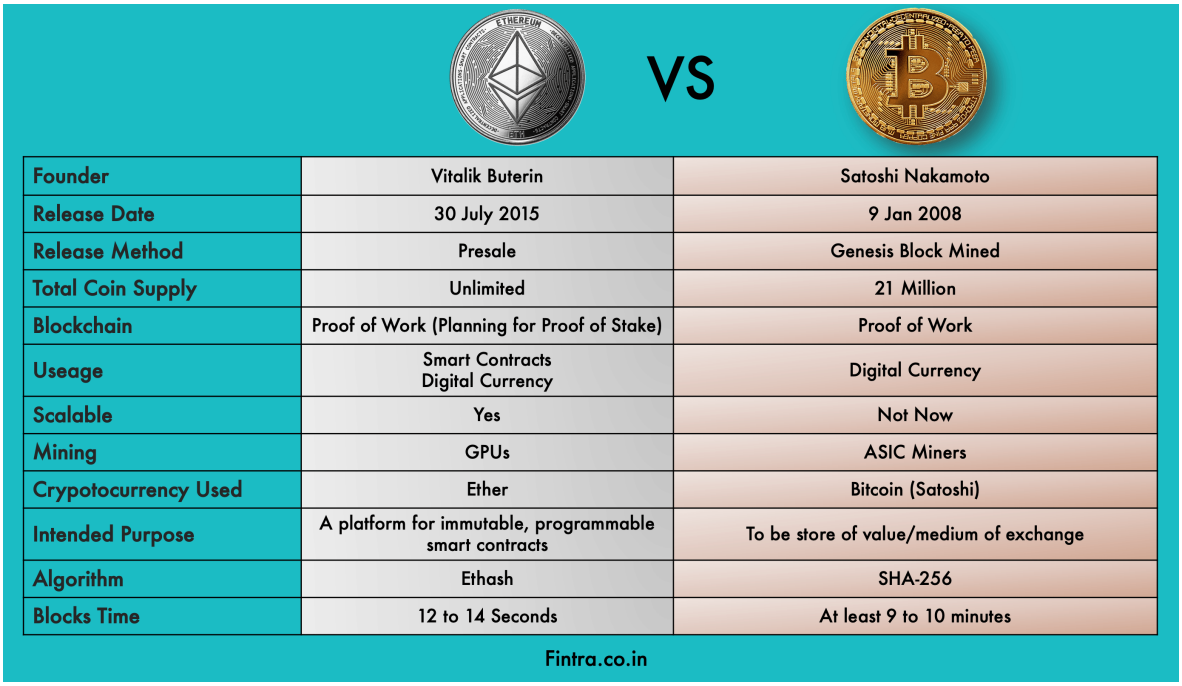
2.5 Ethereum

Ethereum was first described in a white paper written in 2013 by Vitalik Buterin, who was very active in the bitcoin community as an author and programmer. Vitalik saw that there was significantly more potential in Bitcoin than just the ability to transfer value without a central authority. He contributed to expand the utility of Bitcoin beyond trading its native token.

Figure 2.14: Delegated Proof of stake mechanism

To construct decentralized apps on the Bitcoin blockchain, Vitalik and others found that the blockchain would either need a significant code update or the community would have to collaboratively establish a new blockchain.
By that time, Bitcoin was already well-known. It was obvious that the level of improvement required in the core code would be difficult to achieve. Vitalik and his team established the Foundation Ethereum in early 2014 to raise funds to build a blockchain with a programming language built into it. The initial development was launched through online public funding during July and August 2014. The foundation initially raised a record 18 million dollars through the sale of its cryptocurrency token "Ether". The 18 million dollars raised from the token sale provided the foundation with the funds needed to recruit a large development team to create Ethereum. Ethereum Frontier, the first version of the Ethereum network, has been released released in July 2015.
Ethereum is an open source globally decentralized computing infrastructure that executes programs called "Smart contract". it uses a blockchain to synchronize and store the system's state change, along with a cryptocurrency called "Ether" to meter and constrain execution resource cost .The Ethereum platform enables developers to build powerfull decentralized applications with built in economic functions . while providing high availability auditability, transparency and neutrally , it also reduces or eliminates censorhip and reduces certain counterparty risks [22].

Compared to Bitcoin, Ethereum shares many common elements : a peer-to-peer network, a Byzantine fault-tolerant consensus algorithm for synchronization of state updates (a proof-of-work block- chain), the use of cryptographic primitives such as digital signatures and hashes, and a digital currency (ether).
But, both the purpose and construction of Ethereum are quite different from Bitcoin. Ethereum's primary goal is not to serve as a payment network for cryptocurrencies."Ether" is designed to be used to pay for the usage of the Ethereum platform as the world computer.Unlike Bitcoin, which has a very limited scripting language, Ethereum is designed to be a programmable blockchain that runs a virtual machine capable of executing code of an unbounded complexity. Where Bitcoin's Script language is constrained to simple evaluation of spending conditions .



Founder	Vitalik Buterin	Satoshi Nakamoto
Release Date	30 July 2015	9 Jan 2008
Release Method	Presale	Genesis Block Mined
Total Coin Supply	Unlimited	21 Million
Blockchain	Proof of Work (Planning for Proof of Stake)	Proof of Work
Useage	Smart Contracts Digital Currency	Digital Currency
Scalable	Yes	Not Now
Mining	GPUs	ASIC Miners
Crypotocurrency Used	Ether	Bitcoin (Satoshi)
Intended Purpose	A platform for immutable, programmable smart contracts	To be store of value/medium of exchange
Algorithm	Ethash	SHA-256
Blocks Time	12 to 14 Seconds	At least 9 to 10 minutes

Figure 2.15: Bitcoin vs Ethereum

Creating smart contracts was the main reason for building Ethereum platform , so what is smart contract exactly? and how does it work ? the answers would be discussed in the next subsection .

2.6 Smart contract

Smart contracts represent a next step in the progression of blockchains from a financial transaction protocol to an all-purpose utility. They are pieces of software, not contracts in the legal sense, that extend blockchain's utility from simply keeping a record of financial transaction entries to automatically implementing terms of multiparty agreements. Smart contracts are executed by a computer network that uses consensus protocols to

agree upon the sequence of actions resulting from the contract's code[23].
As a consequence, parties may agree on conditions and be certain that they will be carried out automatically, with minimal danger of error or manipulation.The approved contractual clauses are converted into executable computer programs. The logical connections between contractual clauses have also been preserved in the form of logical flows in programs (e.g., the if-else-if statement).

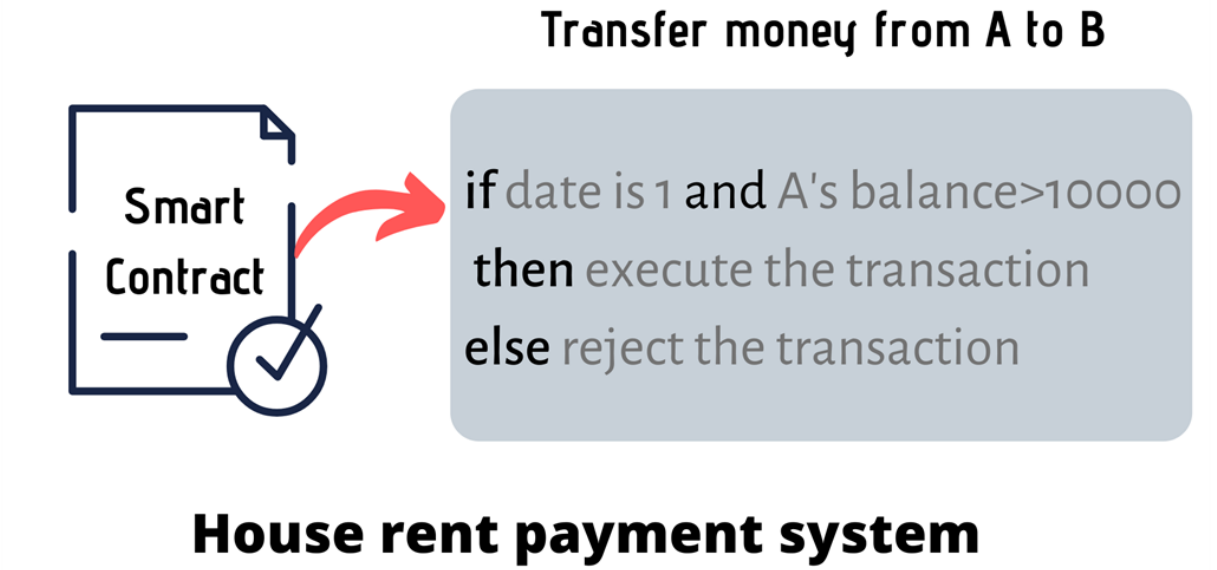


Figure 2.16: Transaction with a Smart contract

The execution of each contract statement is recorded as an immutable transaction stored in the blockchain. Smart contracts guarantee appropriate access control and contract enforcement. In particular, developers can assign access permission for each function in the contract. Once any condition in a smart contract is satisfied, the triggered statement will automatically execute the corresponding function in a predictable manner. For example, Alice and Bob agree on the penalty of violating the contract. If Bob breaches the contract, the corresponding penalty (as specified in the contract) will be automatically paid (deducted) from Bob's deposit [23].
The life cycle of a smart contract is divided into four distinct stages :

- Creation of smart contracts : In principle, the concerned parties negotiate to determine the terms and conditions that may be framed by consultants in the field in which they are applied. Then the developer converts the contract into commands using the programming language used. The two parties may not agree on the terms from the first round, after which there will be other rounds until a compromise is reached. As for those companies that provide fixed services, their terms are not negotiable.

- Deployment : after been validated , smart contracts can be deployed in blockchains

, it appears to public and it's impossible to change it , otherwise there is the possibility of creating new contracts . Freezing of digital assets of involved parties is required till the operation ends .

- Execution of smart contracts : After the deployment of smart contracts, the contractual clauses have been monitored and evaluated. Once the contractual conditions reach (e.g., product reception), the contractual procedures (or functions) will be automatically executed. It is worth noting that a smart contract consists of a number of declarative statements with logical connections. When a condition is triggered, the corresponding statement will be automatically executed, consequently a transaction being executed and validated by miners in the blockchains [24].

- Completion of smart contracts :After a smart contract has been executed, new states of all involved parties are updated. Accordingly, the transactions during the execution of the smart contracts as well as the updated states are stored in blockchains. Meanwhile, the digital assets have been transferred from one party to another party (e.g., money transfer from the buyer to the supplier). Consequently, digital assets of involved parties have been unlocked. The smart contract then has completed the whole life cycle [25].

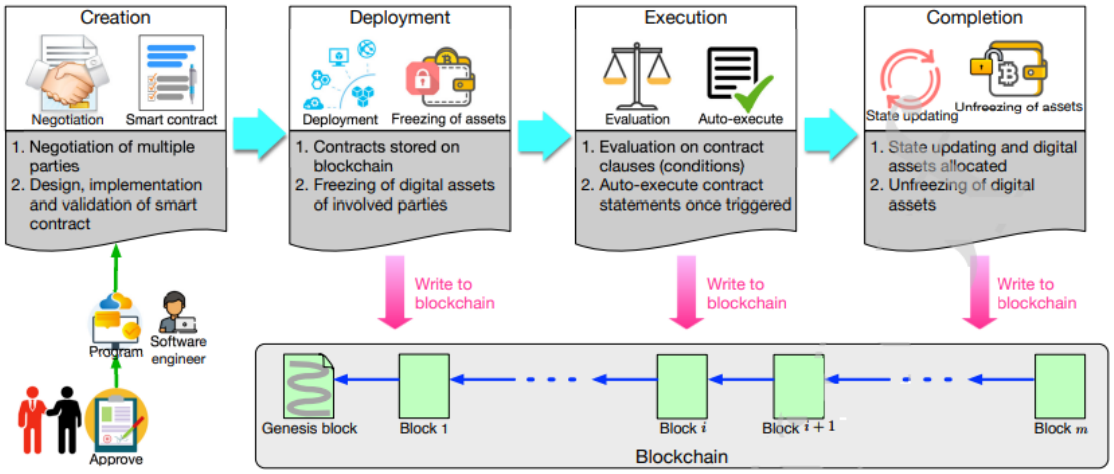


Figure 2.17: Smart contract life cycle [25]

2.7 Conclusion

in this chapter, we went throw more details about blockchain technology starting from the first application of blockchain "Bitcoin" which was the revival elixir and the key for a reliable and well-known technology. then we mentioned briefly the Byzantine Generals Problem explaining the dilemma and how it gave birth to the concept of "Byzantine Fault Tolerance". moving to the Consensus algorithms and primary "Proof of work" the most popular consensus algorithm, introducing how it works and the different parties involving the operation and more details. the second one was Proof of stake and finished with Delegated Proof of stake. although there are many other algorithms, these three were the main ones.
it was an obligation to talk about Ethereum, the platform that invented "Smart contracts", Smart contracts are the highest level in development that blockchain had reached to this day.

Chapter 3

Design and implementation

3.1 Introduction

Certificates indicate the completion of specific learning goals, they are crucial in education and business, as individual learning records are becoming increasingly vital for people's professional careers. As a result, these documents must be kept in long-term storage.
Old methods are efficient to some certain level because of some serious problems such as single point faille ,it needs to be replaced with more sophisticated tools to guarantee efficiency and blockchain is the key due to decentralisation .
In this chapter, we will discuss our proposed solution for the verification of academic certificates using blockchain technology, illustrating schemes of our work and how it should be designed then the implementation and how to apply the solution.

3.2 The issue and the objective

The certificates in the existing system are held in a centralized database, which has the disadvantages of centralized storage such as a single point of failure, which threatens data loss.
the procedure is slow and expensive, companies pay money and time to verify the certificates of new employees every year. The problem also affects the Job-seekers. there is a real need to find new methods to manage and verify credentials. Other countries have already started moving towards a completely digital academic credentialing system.
We will use a Blockchain system for certificates verification , exploiting the advantages of the technology ,high level of security and a guaranteed efficiency, low fees with decreasing the time of the procedure to seconds.

3.3 System representation

In this part, we will show the system representation of our blockchain-based system that aids in the procedure of academic certificates verification.
We utilized blockchain for security reasons; the system is based on the Ethereum blockchain,

which is associated with smart contracts, so there will be no need for third-party participation. The smart contract comprises the process of certificate verification; it offers data storage and retrieval from our blockchain ledger, which ensures the protection of certificates.

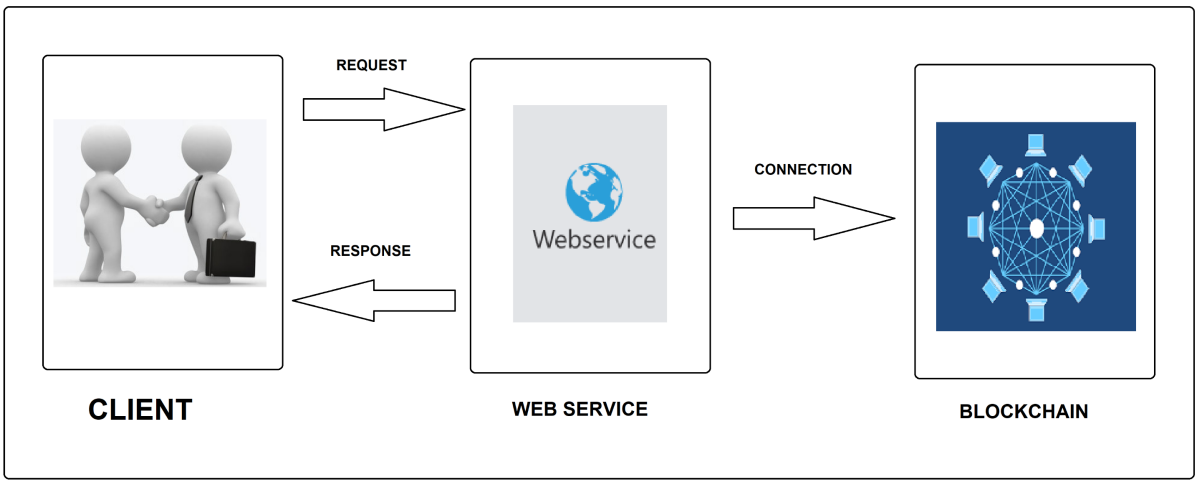


Figure 3.1: System representation

3.3.1 Client

The client can interact with our system and have the ability to sign up with his metamask wallet throw a private key, verify a certificate's existence using the certificate id, adding a certificate with the exact information, the last feature can be private or exclusive for certain parties according to the ministry view.

3.3.2 Web service

The set of tools that allows us to manage our client interface and the environment we work with that provides the connection between the ledger and users.

3.3.3 Blockchain

Blockchain is the main part of our system, it provides a high level of security with decentralization, and data is stored in a particular method that decreases the chances of data loss or system failure. nodes around the network have a copy of the blockchain, the copy is updated after every single transaction.
We chose Ethereum blockchain to create our system with the offered tools of Ethereum and wealthy resources.

3.4 Global architecture

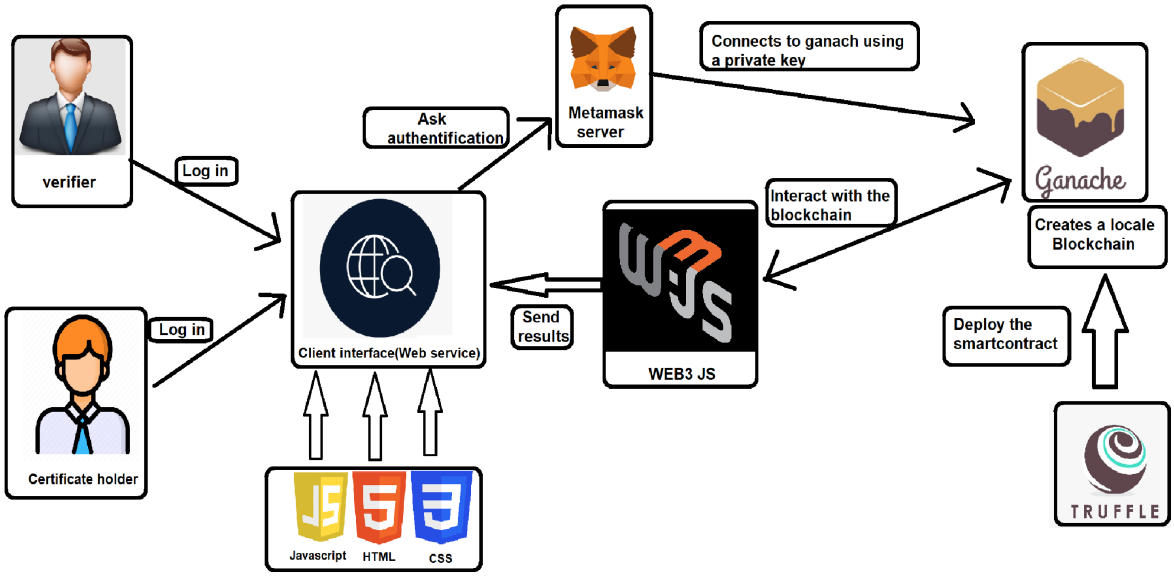


Figure 3.2: Global architecture

To understand more how the system works, we present the global architecture that illustrates the connection between a set of tools that we will talk about each of them later. First, we start with the user who could be a certificate holder or a verifier that interacts with the system through a web interface made with HTML, CSS, and javascript. The log-in would be with Metamask wallet by using a private key and that would allow to Facilitate the identification and payment process thanks to WEB3.
On the other side, we have Ganach our personal blockchain that provides us with 10 accounts with a private key for each that we can use after linking Metamask network to our locale network. Truffle tool helps us as developers to deploy our smart contracts that will manage our system, smart contracts would be deployed on Ganach the same for the transaction would be. We can interact with the smart contract to extract or inject information using WEB3.JS, then give results on the web interface.

3.5 Use case diagram

Use case diagrams in UML describe the behavior of a system and aid in the capturing of system requirements. Use case diagrams illustrate a system's high-level functionality and scope. These diagrams also show how the system and its actors interact with one another. In use-case diagrams, the use cases and actors define what the system does and how the actors interact with it, but not how the system internally runs.

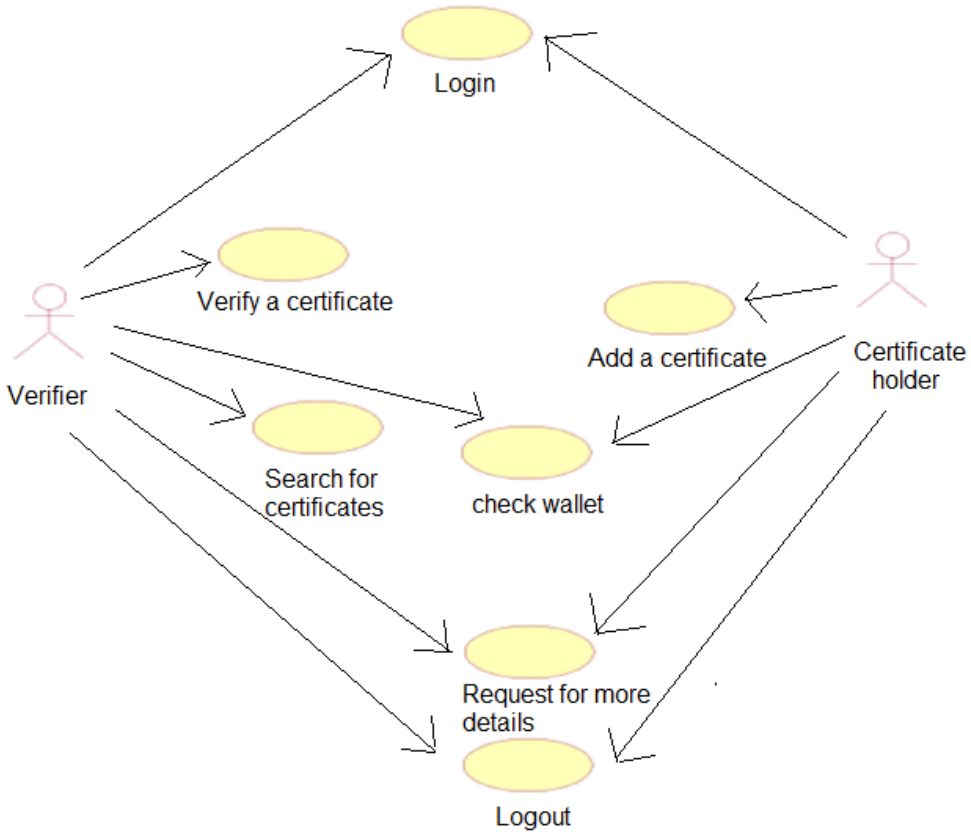


Figure 3.3: Use case diagram

3.6 Sequence diagram

The sequence diagram specifies message exchanges (triggering events) between actors and objects (or between objects and objects) in a chronological way, the evolution of time is read from top to bottom. For a clear view, we split the sequence diagram into two diagrams as shown below.

3.6.1 Certificate holder sequence diagram

The diagram shows the procedure steps, a certificate holder needs to interact with the system's interface so he can be connected to metamask wallet using a private key. After receiving the request, the smart contract manages the procedure and adds blocks to the blockchain.

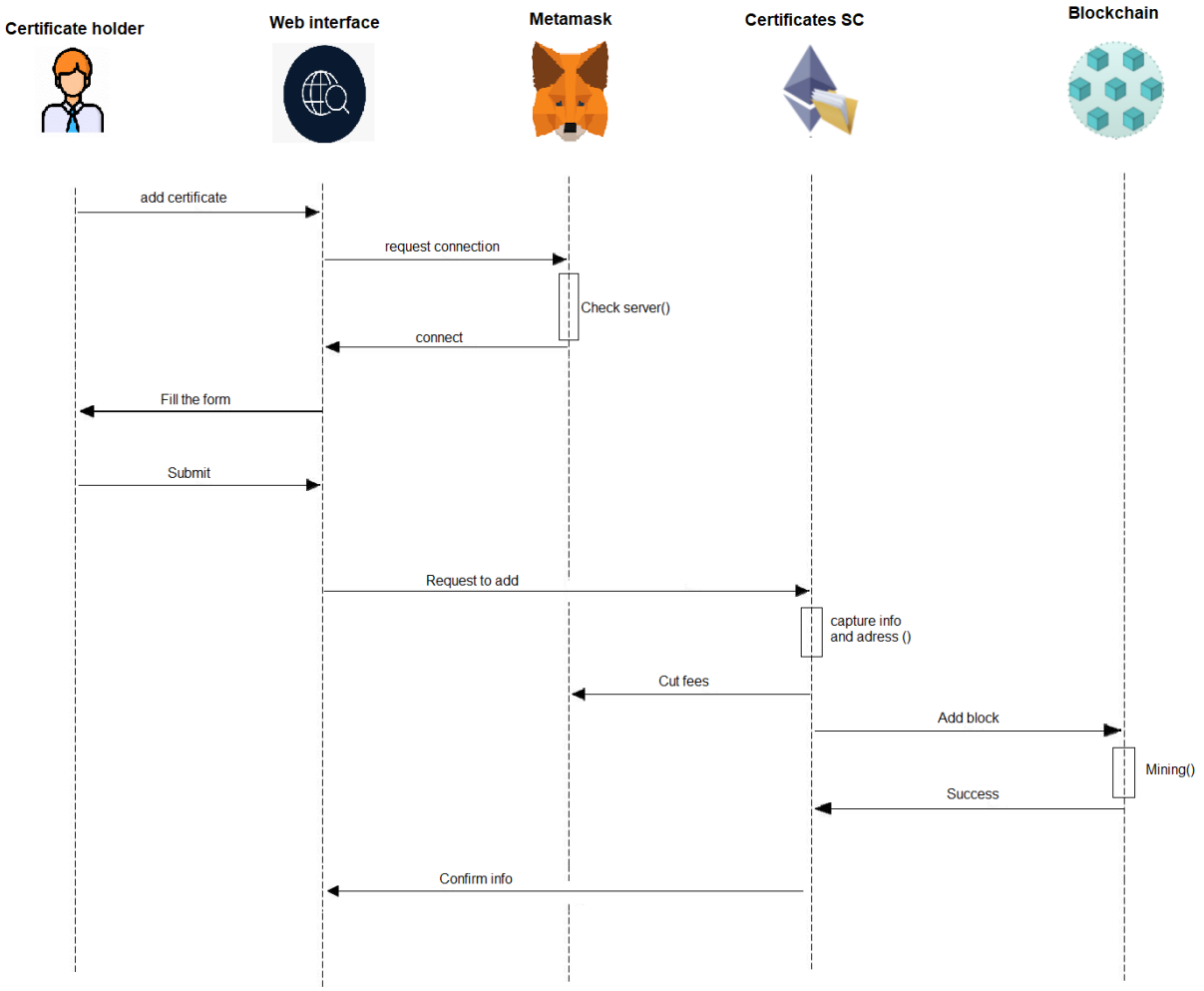


Figure 3.4: Certificate holder sequence diagram

3.6.2 Verifier sequence diagram

The second diagram is quit similar to the first one but with different parameters, interacting with the interface and concerting to the metamask wallet is always necessary.and then the smart contract using a given ID checks the existence of the certificate in the blockchain and sends results.

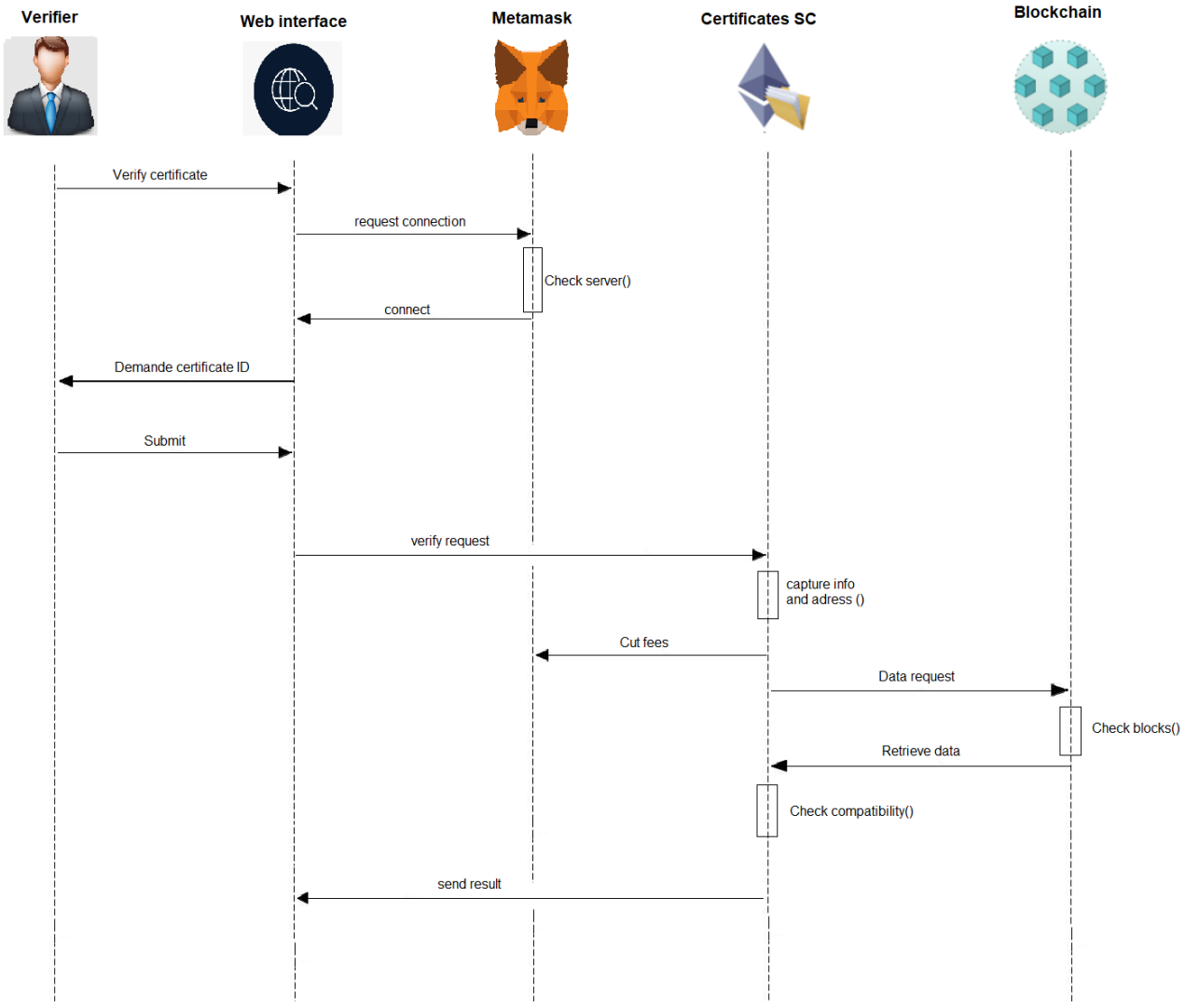


Figure 3.5: Verifier sequence diagram

3.7 Class diagram

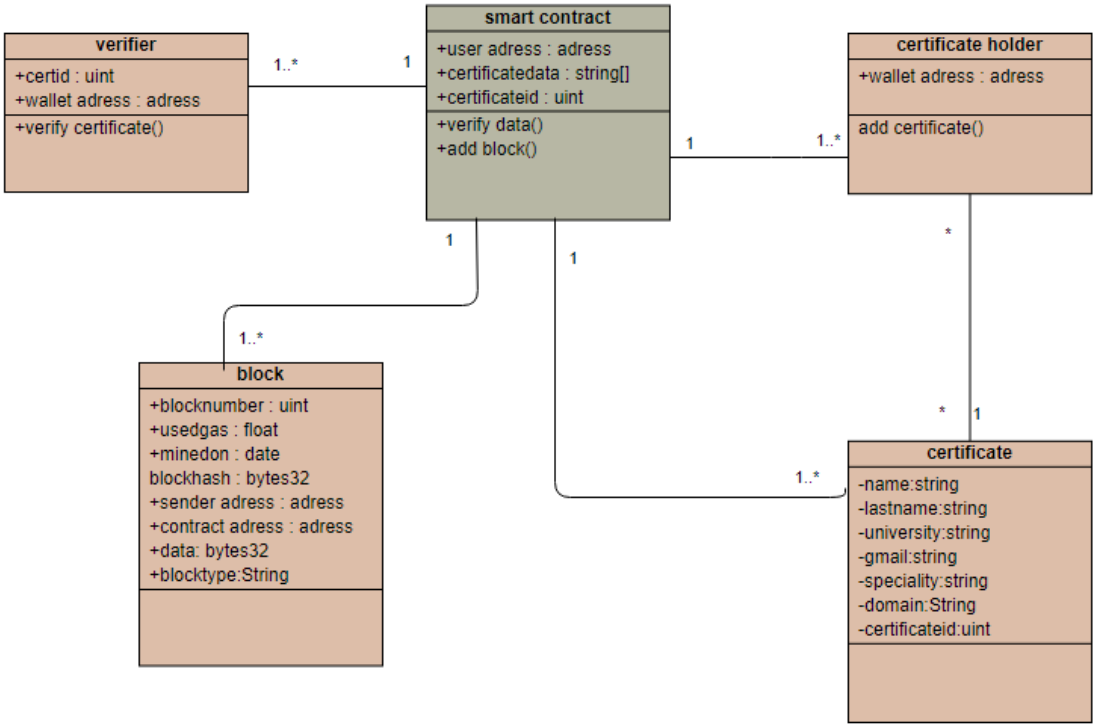


Figure 3.6: Class diagram

3.8 Development Tools

We employed the following tools and technologies and programming languages in the development of our system to facilitate user interaction:

3.8.1 Operating System

The project is performed on CPU 2.20 GHz 2.20 GHz Intel(R) Core(TM) i3-2330M, with 4 Go of RAM. We implemented the project using Windows 10 64bits.

3.8.2 Ganache

Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development. You can use Ganache across the entire development cycle; enabling you to develop, deploy, and test your dApps in a safe and deterministic environment. Ganache UI is a desktop application supporting both Ethereum and Corda technology. The command-line tool, ganache-cli (formerly known as the TestRPC), is available for Ethereum development.All versions of Ganache are available for Windows, Mac, and Linux[26].

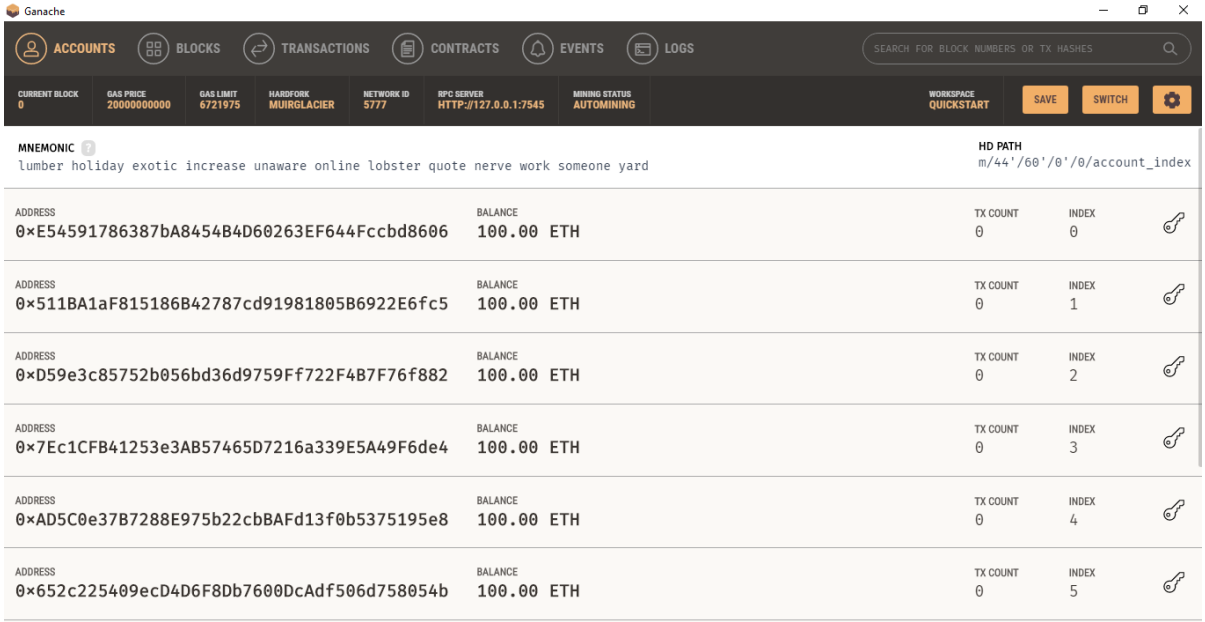


Figure 3.7: Ganache

3.8.3 Truffle

Truffle is a world-class development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM),Truffle is widely considered the most popular tool for blockchain application development with over 1.5 million lifetime downloads. Truffle supports developers across the full lifecycle of their projects, whether they are looking to build on Ethereum, Hyperledger, Quorum, or one of an ever-growing list of other supported platforms. Paired with Ganache, a personal blockchain, and Drizzle, a front-end dApp development kit, the full Truffle suite of tools promises to be an end-to-end dApp development platform[27].

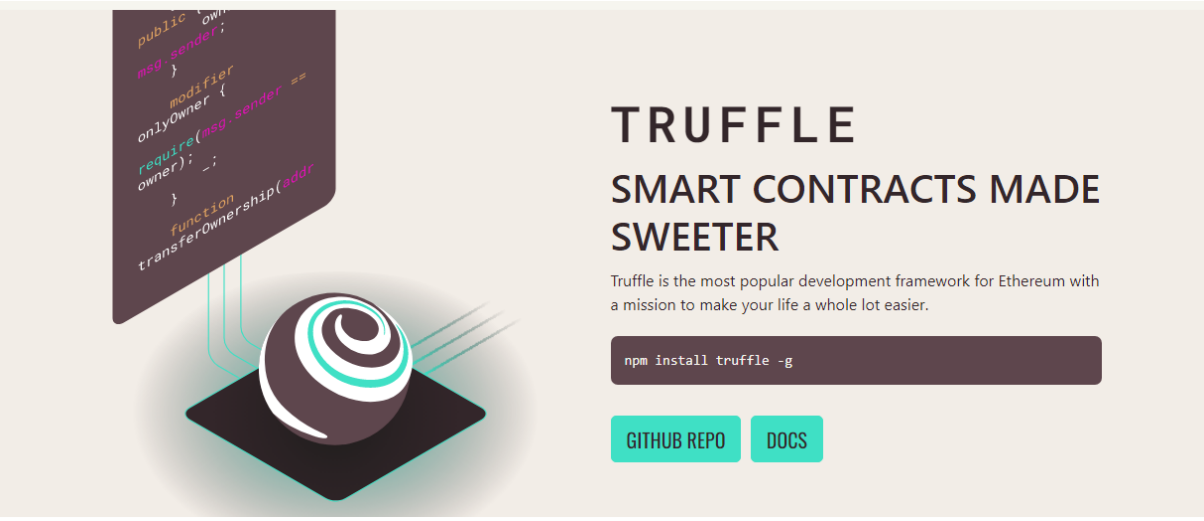


Figure 3.8: Truffle [27]

3.8.4 Node js

Node.js is a platform built on Chrome's JavaScript runtime for easily building fast and scalable network applications. Node.js uses an event-driven, non-blocking I/O model that makes it lightweight and efficient, perfect for data-intensive real-time applications that run across distributed devices. Node.js is an open source, cross-platform runtime environment for developing server-side and networking applications. Node.js applications are written in JavaScript, and can be run within the Node.js runtime on OS X, Microsoft Windows, and Linux.5[29] Node.js also provides a rich library of various JavaScript modules which simplifies the development of web applications using Node.js to a great extent.

3.8.5 Web3.js

A collection of libraries for designing DApps, it makes interaction with smart contracts on the Ethereum blockchain easy using HTTP, IPC, or WebSocket.
Web3.js API helps developers to manipulate the blockchain and use the nodes facility using JSON RPC endpoints accessible on top of the HTTP, IPC, or WebSocket transfers from the web page, via the smart contract's JSON interface, and web3 will auto-translate all functions into low-level ABI calls over RPC.

3.8.6 Metamask

"A crypto wallet gateway to blockchain apps",Available as a browser extension and as a mobile app, MetaMask equips you with a key vault, secure login, token wallet, and token exchange—everything you need to manage your digital assets.MetaMask generates passwords and keys on your device, so only you have access to your accounts and data. You always choose what to share and what to keep private[25]. Metamask extension injects the Ethereum web3 API into the website's JavaScript context so that the blockchain can be read by DApps.

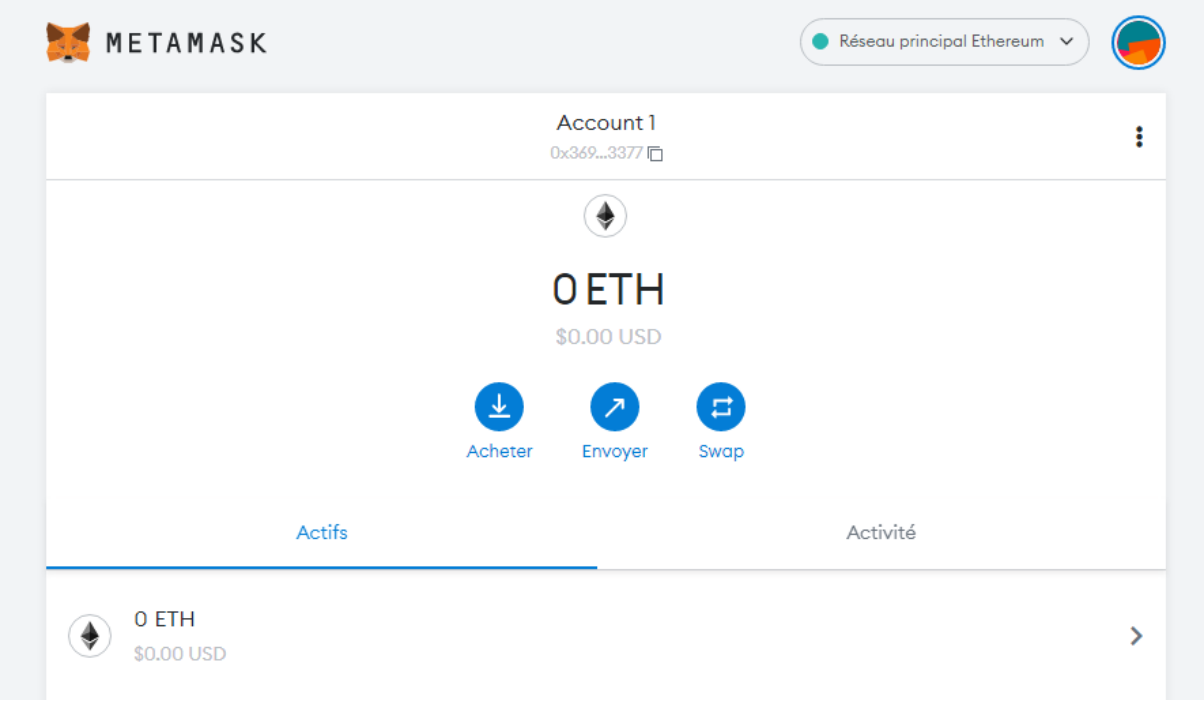


Figure 3.9: Metamask

3.8.7 Visual Studio

Microsoft Visual Studio is an integrated development environment for Microsoft Windows. It is a tool for writing several computer programs such as websites, web apps, and web services. It includes a code editor, debugger, GUI design tool, and database schema designer, and supports most major revision control systems. It is available in both a free "Community" edition and a paid commercial version.

Figure 3.10: Visual Studio

3.8.8 HTML

Hypertext Markup Language, a markup language for the web that defines the structure of web pages and how to display text, images or other forms of multimedia using tags. It isn't a programming language, HTML is parsed by the browser.

Figure 3.11: HTML

3.8.9 CSS

Cascading Style Sheets , it used to style Web pages and describe the presentation of the document written in HTML .

Figure 3.12: CSS

3.8.10 JavaScript

JavaScript is a programming language used to create a dynamic and interactive web content like applications and browsers, it allows to implement complex features on web pages such as User's Input validating and handling dates and time.

Figure 3.13: JavaScript

3.8.11 Solidity

An object-oriented programming language created specifically by the Ethereum Network team for constructing and designing smart contracts. Solidity is the official and most widely used language in the Ethereum network; using it, smart contracts are written that are agreed on between two parties. It may seem like JavaScript, but actually it's more like Java for its statically typed feature[28].

Figure 3.14: Solidity

3.9 Configuration and Implementation

In this section, we'll illustrate briefly how this project was implemented and the necessary configuration, mentioning how we used the tools we already talked about earlier to make the procedure go straight.

3.9.1 Truffle initiation

The first step is creating the file that will contain our project and the smart contracts, then initiating truffle at the directory we created to provide the necessary files.

```
PROBLEMS   OUTPUT   DEBUG CONSOLE   TERMINAL
Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS D:\Project\Front-end> mkdir CertificatesVerification


    Répertoire : D:\Project\Front-end


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        29/05/2022     15:46                CertificatesVerification

PS D:\Project\Front-end> cd CertificatesVerification
PS D:\Project\Front-end\CertificatesVerification> truffle init

Starting init...
================

> Copying project files to D:\Project\Front-end\CertificatesVerification

Init successful, sweet!

Try our scaffold commands to get started:
  $ truffle create contract YourContractName # scaffold a contract
  $ truffle create test YourTestName         # scaffold a test

http://trufflesuite.com/docs

PS D:\Project\Front-end\CertificatesVerification>
```

Figure 3.15: Truffle initiating

Using Visual Studio we can check the created folders and files :

- contracts:The directory of Solidity contracts, our written smart contract should placed there.
- Migrations:The directory for scriptable deployment.
- test: The directory of testing contracts and application.
- truffle-config.js: Truffle configuration file.

Figure 3.16: Truffle initiating

Now configuring the network part according to the chosen parameter :

```
networks: {
  // Useful for testing. The `development` name is special - truffle uses it by default
  // if it's defined here and no other network is specified at the command line.
  // You should run a client (like ganache, geth, or parity) in a separate terminal
  // tab if you use this network and you must also set the `host`, `port` and `network_id`
  // options below to some value.
  //
  development: {
    host: "127.0.0.1",     // Localhost (default: none)
    port: 7545,            // Standard Ethereum port (default: none)
    network_id: "*",       // Any network (default: none)
  },
```

Figure 3.17: Truffle's network

3.9.2 Ganach setting

We need to choose "NEW WORKSPACE" for advance setting,then adding the truffle-config.js file from our project folder. setting host-name and port number with same parameter we used in truffle. We also need to precise the default account balance and the number of accounts generated.

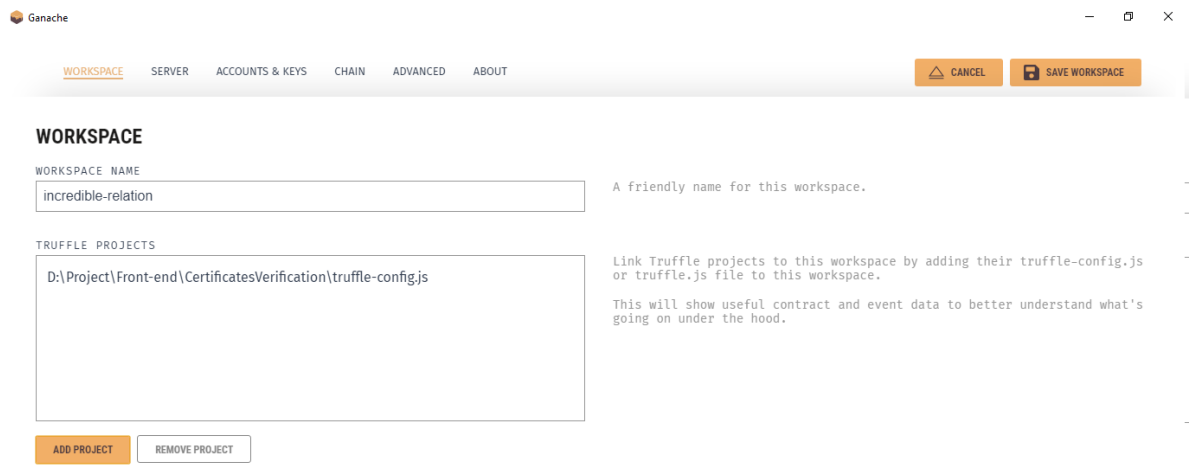


Figure 3.18: Ganach setting

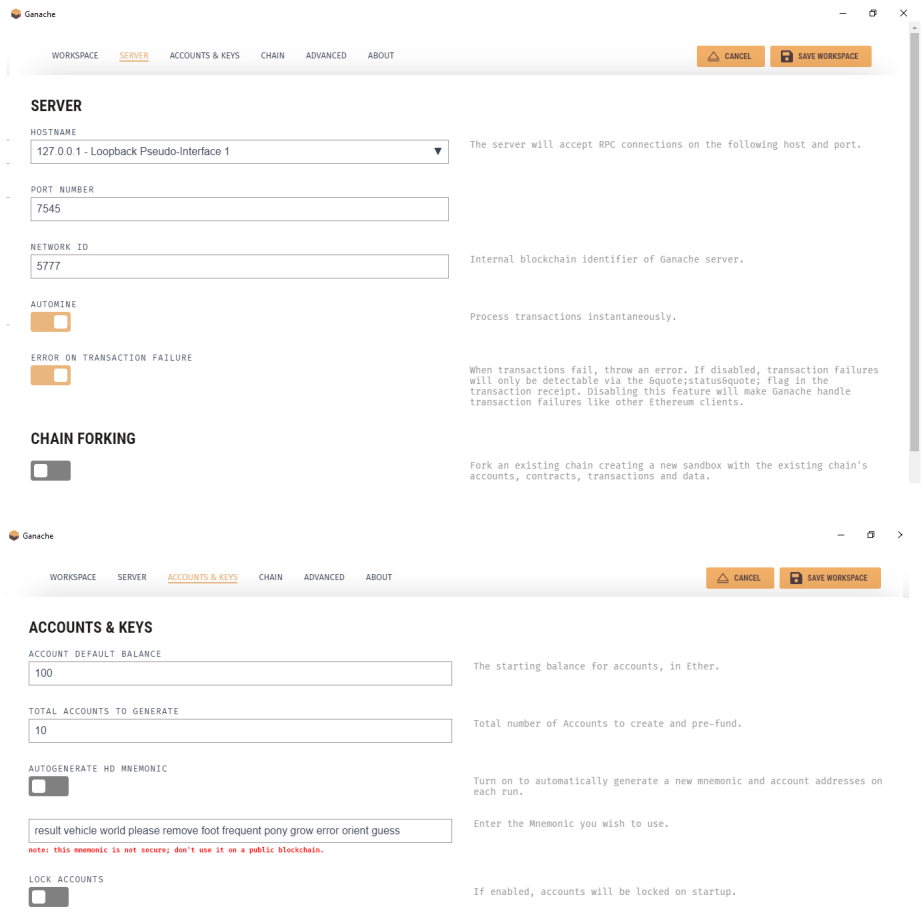


Figure 3.19: Ganach setting

3.9.3 Metamask connection

Metamask by default uses the Ethereum mainnet, in order to connect metamask to ganach we will create a locale network as shown in figure 3.19.
Next,using a private key from Ganach we can now add an account containing 100 ETH so we can handle transactions fees.

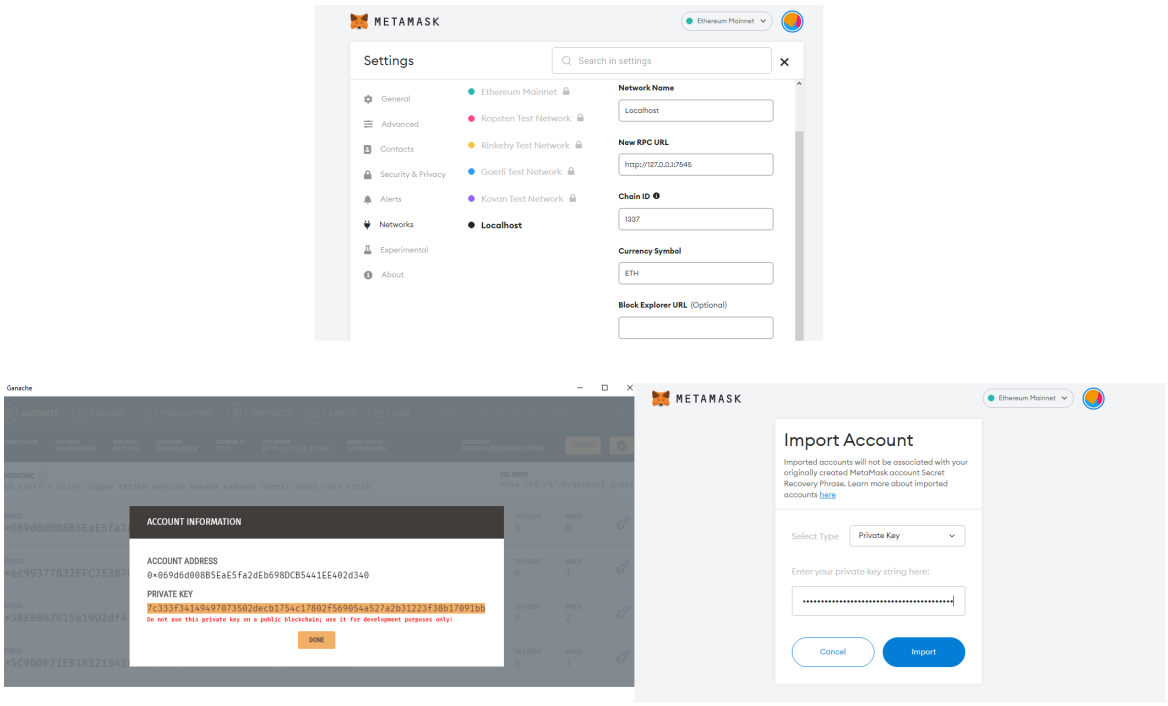


Figure 3.20: Metamask connection

3.10 Block structure

After compiling the smart contract and deploying it, the deployed smart contract would mentioned and the genesis block should be created as shown in figure 3.21. A blockchain is simply a chain of blocks, each block has a sequence number and a unique hash, it consists too of a transaction hash, data hash, contract address, sender address, mined date ,and transaction fees. the figure 3.22 shows the detailed structure of a block.

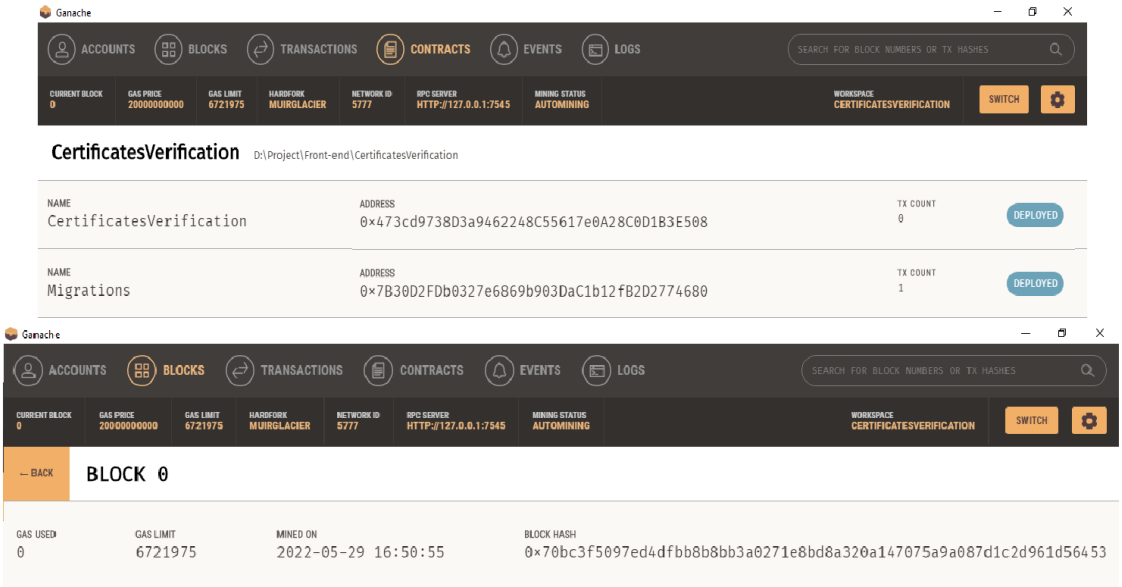


Figure 3.21: Genesis Block

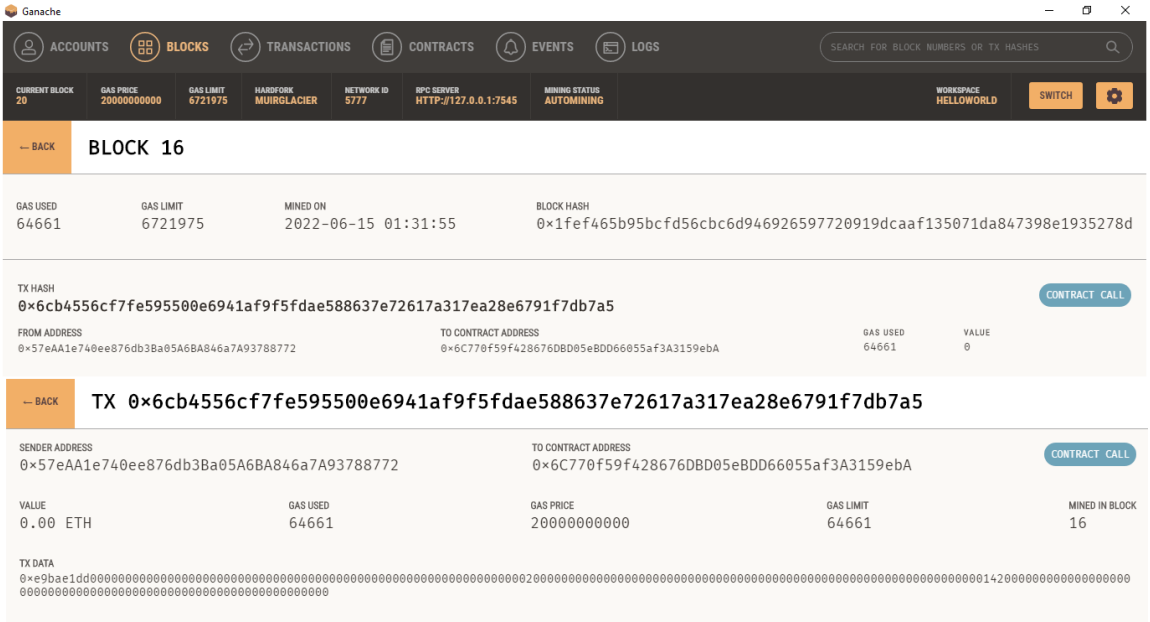


Figure 3.22: Block structure

3.11 Application interface

In this part, we will present the interface of our blockchain application and how it is running by mentioning printed screens of our application. Visiters choose between adding a certificate(a certificate holder) or verifying a certificate (verifier).

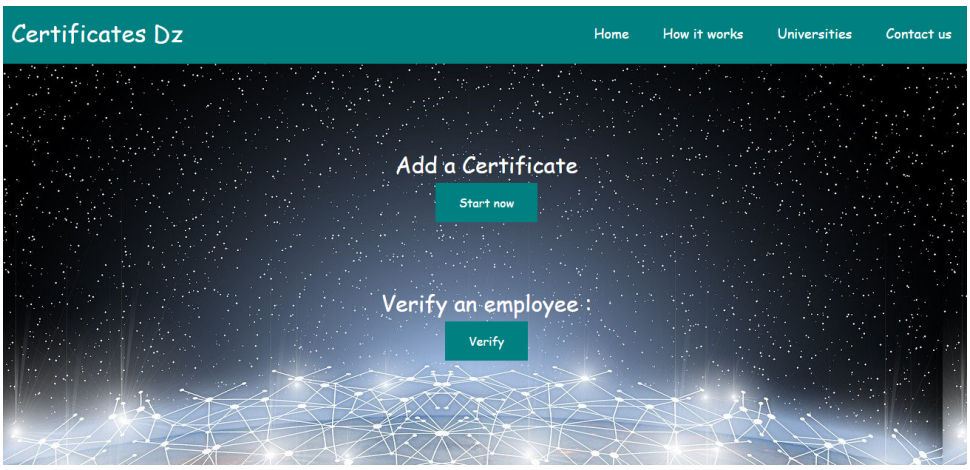


Figure 3.23: Application interface

3.11.1 Adding a certificate

By clicking the button "Start now" you'll be able to accede the login page with metamask. If the metamask extension is not installed you won't be able to proceed till the extension is installed.

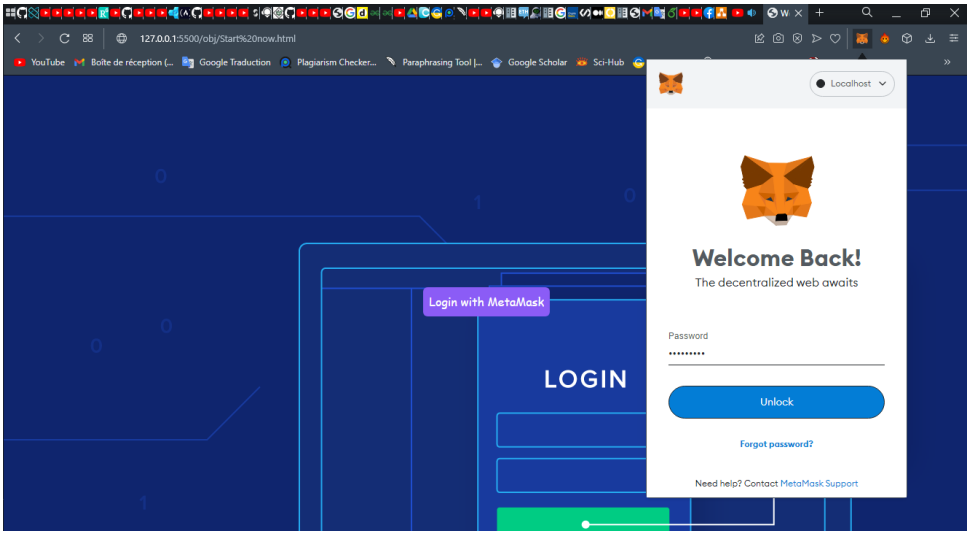


Figure 3.24: Log in with Meatamas

Once a private key is inserted,metamask will connect and the user address would appear.

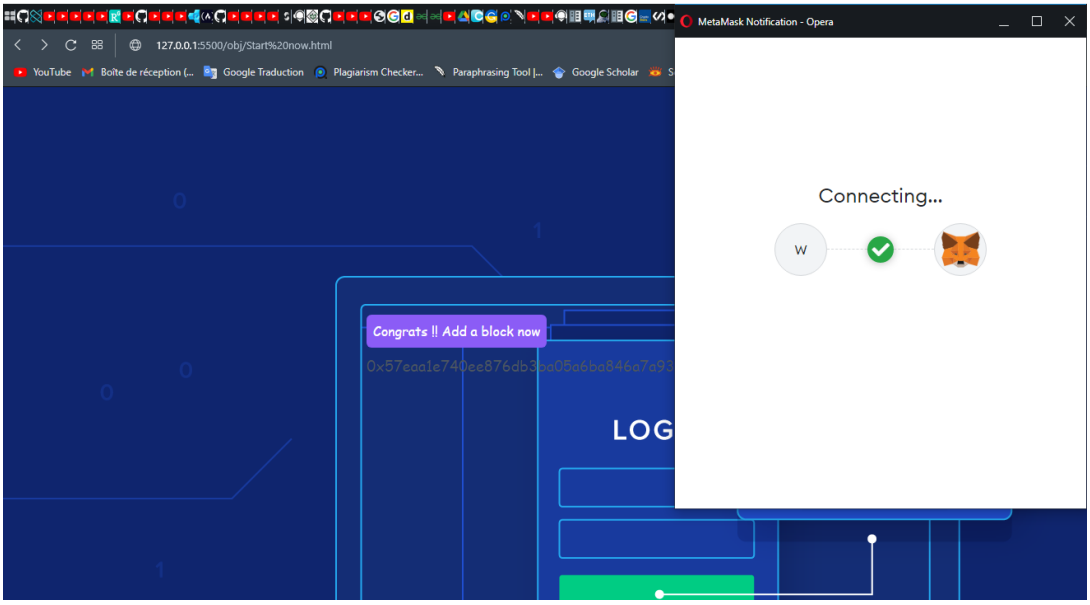


Figure 3.25: Log in with Meatamas

After connecting to metamask ,now a certificate holder can add the certificate information by filling the form.

Figure 3.26: Certificate form

After submitting, information would be confirmed.

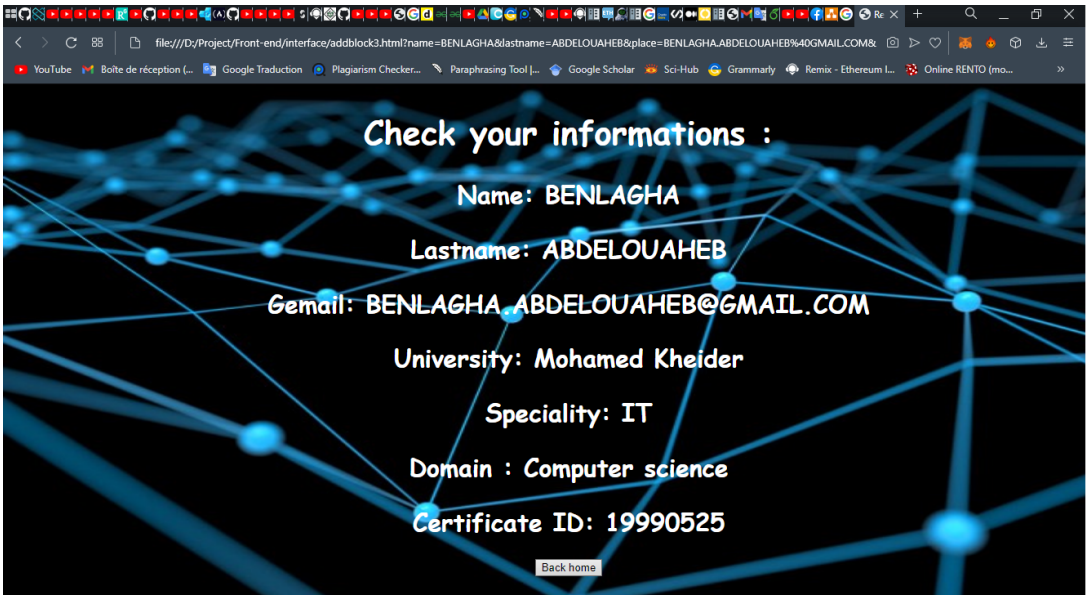


Figure 3.27: Information check

3.11.2 Verifying a certificate

To verify existence of a certificate in the system you need to choose the verify button,connection to metamask is required then a page with a search bar will appear.A certificate ID is needed to proceed, if the certificate does really exist in the blockchain the result will be full information about the certificate as shown in the figure3.29.

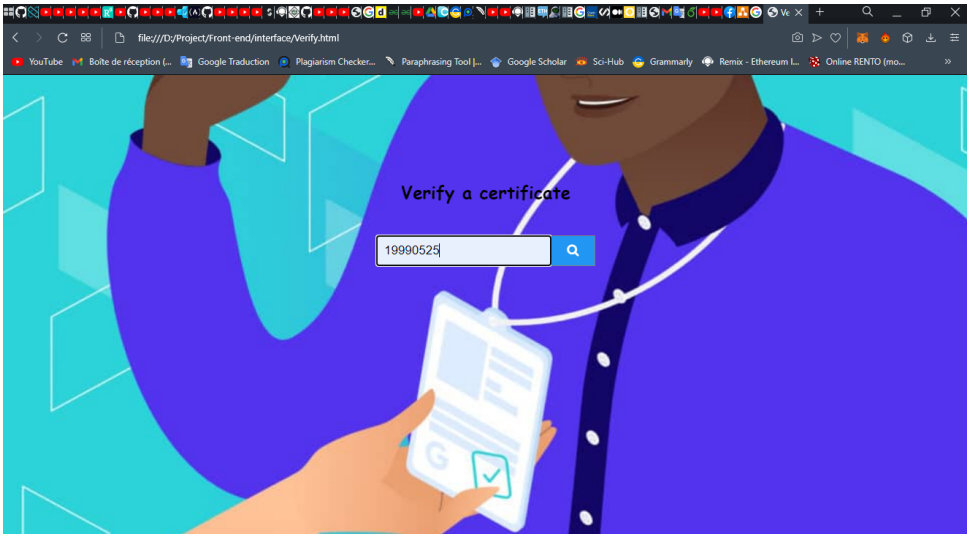


Figure 3.28: Verify a certificate

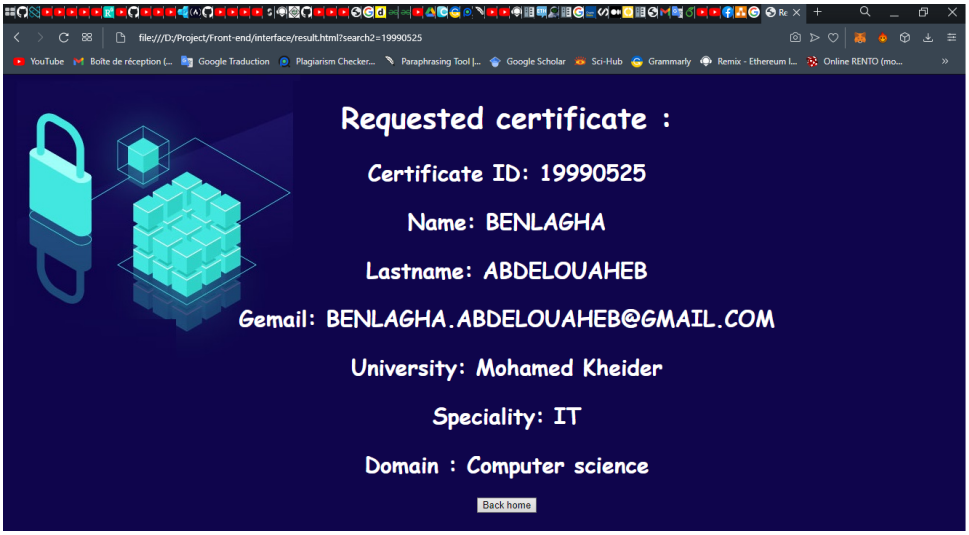


Figure 3.29: Result

3.12 Conclusion

The chapter provided the objective we seek, and the global architecture of the system, well explained for a clear view. Mentioning the necessary tools in building the project with a brief illustration of how the procedure was configured and executed, and finally the results we worked for.

General conclusion

Blockchain technology has gone far beyond its classic application of electronic money without a central authority. This technology has brought new concepts that ensure immutability and enhances security. These characteristics make blockchain technology appropriate for several domains, such as voting systems and health and academic credentials.
The purpose of this thesis was to utilize the benefits of the blockchain in the academic certificates verification context and to come up with a blockchain-based system to improve the processes of verifying academic credentials. This project gave us a chance to explore the techniques of the blockchain, their definition and their composition, and how it does work and applied in the real world, working with advanced technologies and development tools including Truffle,Ganach,Metamask, and web3.js.
However, the field is yet vast and this is just the beginning of the road, many future ideas could be realized such as : A mobile application uses several wallets or extending the solution to other sectors in the same context with the same problem.

Bibliography

[1]. rshdeep Bahga and Vijay K Madisetti. Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications, 9(10):533-546,2016.
[2]. https://101blockchains.com/history-of-blockchain-timeline/
[3]. https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain.
[4]. Comprendre la blockchain, Livre blanc sous licence Creative Commons,´ edit´ e par uchange.co, janvier 2016.
[5]. https://www.javatpoint.com/blockchain-hash-function
[6]. https://101blockchains.com/hashing-and-digital-signature-in-blockchain/
[7]. "Estimated Size of the Global Insurance Market 2020, with Forecasts up until 2025," 2020, https://www.statista.com/statistics/1192960/forecast-global-insurance-market/.
[8]. E. M. Immergut, "Health policy," in International Encyclopedia Of the Social Behavioral Sciences, pp. 6586–6591, Elseiver, Amsterdam, Netherlands, 2001
[9]. Griebel, L.; Prokosch, H.U.; K¨ opcke, F.; Toddenroth, D.; Christoph, J.; Leb, I.; Engel, I.; Sedlmayr, M. A scoping review of cloud computing in healthcare. BMC Med. Inform. Decis. Mak. 2015, 15, 17.
[10]. Grech, A., Anthony F. Camilleri: Blockchain in Education. No. JRC108255. Joint Research Centre (Seville site). (2017).
[11]. Joo, M.H., Nishikawa, Y. and Dandapani, K., 2019. Cryptocurrency, a successful application of blockchain technology. Managerial Finance.
[12]. Mastering Bitcoin: Programming the Open
[13]. Melanie Swan,Chapter Five - Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems, Editor(s): Pethuru Raj, Ganesh Chandra Deka, Advances in Computers, Elsevier,2018,Pages 10-11.
[14]. www.developcoins.com
[15].Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., Colman, A. (2020). Blockchain consensus algorithms: A survey,Pages 9-10 . .[69]. "Bitcoin". [Online] Available: http://www.bitcoin.org/ Accessed on April 24, 2022.
[70]."Bitcoin Cash". [Online] Available: https://www.bitcoincash. org/ Accessed on April 24, 2022.
[71]. "Syscoin". [Online] Available: http://syscoin.org/ Accessed on April 24, 2022.
[72]. "Peer Coin". [Online] Available: https://peercoin.net Accessed on April 24, 2022.
[73]. "Counterparty". [Online] Available: https://counterparty.io Accessed on April 24, 2022.
[75]. "Emercoin. [Online] Available: https://emercoin.com/ Accessed on April 24, 2022.
[76]. "Namecoin". [Online] Available: https://namecoin.org/ Accessed April 24, 2022.

[78]. "Crown". [Online] Available: https://crown.tech/ Accessed on April 24, 2022.
[79]. "Ommi (Mastercoin)". [Online] Available: http://www. omnilayer.org/ Accessed April 24, 2022.
[16]. Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access.Apr 26 2022.
[17]. S. King. (Jul. 2013). Primecoin: Cryptocurrency with prime number proof-of-work, Self-Published Papers. Accessed: Apr. 24, 2022. [Online].Available:http://primecoin.io/bin/prim paper.
[18]. A. Shoker, "Sustainable blockchain through proof of exercise," in Proc. IEEE 16th Int. Symp. Netw. Comput. Appl.
(NCA), Cambridge, MA, USA, Jan. 2017, pp. 1-9.
[19]. M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan, "Proofs of useful work," Int. Assoc. Cryptologic Res., Tech. Rep. 2017/203, 2017.
[20]. I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity:Extending bitcoin's proof of work via proof of stake [extended abstract]y," ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34-37,Dec. 2014.
[21]. Bashir I. Mastering blockchain. Packt Publishing Ltd; 2017 Mar 17 , page 74.
[22].https://fintra.co.in/blog/bitcoin-vs-ethereum
[23]. Kevin Delmolino, et al., Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab, University of Maryland, November 18, 2015 .
[24]. R. Koulu, Blockchains and online dispute resolution: smart contracts as an alternative to enforcement, SCRIPTed 13 (2016) 40 (2016).
[25].https://metamask.io
[26].https://trufflesuite.com/docs/ganache/
[27].https://trufflesuite.com/truffle/
[28].Mohanty, Debajani. "Ethereum Architecture." Ethereum for Architects and Developers. Apress, Berkeley, CA, 2018. page 41.
[29].https://www.tutorialspoint.com/nodejs/nodejs ntroduction.htm
[30].Benisi NZ, Aminian M, Javadi B. Blockchain-based decentralized storage networks: A survey. Journal of Network and Computer Applications.
[31]. Viriyasitavat W, Hoonsopon D. Blockchain characteristics and consensus in modern business processes. Journal of Industrial Information Integration.
[32].Yang R, Wakefield R, Lyu S, Jayasuriya S, Han F, Yi X, Yang X, Amarasinghe G, Chen S. Public and private blockchain in construction business process and information integration. Automation in construction.
[33].Zivic N, Ruland C, Ur-Rehman O. Addressing byzantine fault tolerance in blockchain technology. In2019 8th International Conference on Modeling Simulation and Applied Optimization (ICMSAO) 2019 Apr 15 (pp. 1-5). IEEE.
[34].Lamport L, Shostak R, Pease M. The Byzantine generals problem. InConcurrency: the works of leslie lamport 2019 Oct 4 (pp. 203-226).

[35].Alsunaidi SJ, Alhaidari FA. A survey of consensus algorithms for blockchain technology. In2019 International Conference on Computer and Information Sciences (ICCIS) 2019 Apr 3 (pp. 1-6). IEEE

[36].Schinckus C. Proof-of-work based blockchain technology and Anthropocene: An undermined situation?. Renewable and Sustainable Energy Reviews.

[37].Sarmah SS. Understanding blockchain technology. Computer Science and Engineering.

[38].Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. arXiv preprint arXiv:1906.11078.