Systematic literature review in the area of Blockchain Technology, trying to identify what is the current state of affair in the banking sector. Challenges, opportunities and possible value creation for the banking system

Rafailoglou Miranda

SID: 3306170008

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Mobile and Web Computing

JULY 2019

THESSALONIKI – GREECE

Systematic literature review in the area of Blockchain Technology, trying to identify what is the current state of affair in the banking sector. Challenges, opportunities and possible value creation for the banking system

Rafailoglou Miranda

SID: 3306170008

Head Supervisor:	**Prof. Vasillios Peristeras**
Supervisor:	**Prof. Ioannis Magnisalis**

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Mobile and Web Computing

JULY 2019

THESSALONIKI – GREECE

Acknowledgements

This dissertation was supervised by professors Dr Peristeras Vasillios & Dr.Magnisalis Ioannis and their team who, with their helpful guidelines, contributed to the proper output of this effort. Finally, I would also like to thank my colleagues, who are members of Dr Magnisali's dissertation team for their contributions with remarks, suggestions and ideas.

Abstract

By the first half of the 21st century, humanity has been overwhelmed by technological revisions that will change the way it works daily, directly or indirectly.

Technologies around the blockchain transform the functioning of the economy and create the technological potential for the existence of a distributed form of trust. This is of great importance, as it may affect traditional confidentiality, transactions and e-services so far.

With blockchain technology, the trust that has so far existed due to a contractual relationship is created because of the distributed and secure way of storing, managing and exchanging information and conducting electronic transactions.

A new change is taking place in all the existing financial and business models that every day one uses. Blockchain technology can be applied to a number of branches of the economy and society.

This dissertation, as a part of the MSc in Mobile and Web Computing at the International Hellenic University, will try to explain, analyze and propose what blockchain is about, is consisted of and is usefulness to the financial, economic and generally social environment in the world of banks and the impact to the banking sector to client-users relationship and the society in general.

Its main scope is to indicate how this newly entry technology could operate as a "background assistant", for the end-users through the transaction channels that banking industry provides.

More specifically, the main goal of this dissertation is distributed in three core segments:

1. Explain the blockchain method.
2. The potential benefits of this method in many aspects of everyday life.
3. The potential benefits of this method if it is applied in the banking sector (theoretical approach).

The objective of this thesis was decided thanks to the encouragement of my supervisors and my strong desire to study the “hot subject” of the blockchain technology in a field such as banks where this method is considered to be rather a competitor than an assistant.

Rafailoglou Miranda

Thursday, November 30, 2019

Contents

1. Introduction

Companies dealing mainly with online transactions take the risks associated with cyber security seriously [1]. To address such issues, companies make significant investments in advanced technologies and blockchain quickly becomes the first choice of each company for secure online transactions.

Transparency, immediacy, security and decentralization in control are the main features of blockchain and are responsible for attracting companies to exploit technology.

However, although blockchain has begun to find applications in commercial, financial and trading services, there are many applications that can benefit the most from the cryptographic background technology. In this survey approach, there will be a more detailed analysis of the blockchain technology inside the banking sector either as an applied method in every day transactions or a more futuristic approach for several other tasks in the banks.

The blockchain technology, a distributed peer-to-peer linked-structure, could be used to solve the problem of maintaining the order of transactions and to avoid the double-spending problem. Thus, the blockchain structure manages to contain a robust and auditable registry of all transactions. Blockchain introduced serious disruptions to the traditional business processes since the applications and transactions, which needed centralized architectures or trusted third parties to verify them, can now operate in a decentralized way with the same level of certainty. The inherent characteristics of blockchain architecture and design provide properties like transparency, robustness, auditability, and security [2] [3]. A blockchain can be considered a distributed database that is organized as a list of ordered blocks, where the committed blocks are immutable. One can see that this is ideal in the banking sector as banks can cooperate under the same blockchain and for example, push their customers' transactions.

1.1 Technologies before blockchain

A network architecture such as "client-server" architecture is often used for a database running on the Internet. A user (client) with permissions associated with their account can change entries that are stored on a centralized server. By changing the

‘master copy’, whenever a user accesses a database using their computer, they will get the updated version of the database entry. Control of the database remains with administrators, allowing for access and permissions to be maintained be a central authority.

This is not at all the same as with a blockchain. For a blockchain database, each participant maintains, calculates and updates new entries into the database. All nodes work together to ensure they are all coming to the same conclusions, providing in-built security for the network.

1.1.1. The need for Decentralized control

Blockchain allow different parties that do not trust [4] each other to share information without requiring a central administrator. Transactions are processed by a network of users acting as a consensus mechanism so that everyone is creating the same shared system of record simultaneously. The value of decentralized control is that it eliminates the risks of centralized control.

1.1.2. The need for Performance

As database, blockchain can be considered very slow compared to what is possible for digital transaction technology that we see today with Visa and PayPal. In the very close future, there will inevitably be improvements to this performance, the nature of blockchain technology requires that some speed be sacrificed.

1.1.3. The need for Confidentiality & Trust

Blockchain technology gives the opportunity to everyone who participates in a transaction through it to write a new block into the chain and to read a block in the chain. A permissioned blockchain [5], like a centralized database, can be write-controlled and read-controlled. That means the network or the protocol can be set up so only permissioned participants can write into the database or read the database. So, confidentiality and consequently trust [6] is a fundamental issue for this technology.

1.2 Objectives and aims

Despite the fact that technology of blockchain for the past 10 years is interrelated to the bitcoin (cryptocurrency) [7] and every other this-sort-of-method-of-payment-coin, it

is more than certain that this technology has much more potentials of being successfully used in different and interesting aspects of human life.

In this point it should be clarified that the big issue for the blockchain technology is not the “where” is this method be used but “who” is going to be the vendor behind the cryptocurrency or any other usage/application.

The aim of current dissertation is to show what is the blockchain technology, strengths and weaknesses of it, the aspects is already being used and the potential benefits of its appliance into the banking sector.

To be more specific, the objectives of the current dissertation are:

Objective 1. To give a comprehensible description of what is the blockchain technology and the novelties it brings in the technology world with both its strengths and weaknesses.

Objective 2. To report the appliances in many aspects of humanity (science, industry, society).

Objective 3. To approach, in a theoretical base, the possible appliances the blockchain technology might have in the heavy sector of Economy, banking.

2. Literature

One of the most talked-about topics in the financial services industry today is blockchain banking [8]. If fully adopted, it will enable banks to process payments more quickly and more accurately while reducing transaction processing costs and the requirement for exceptions.

However, to capitalize on this potential, banks need to build the infrastructure required to create and operate a true global network using solutions based on this transformative technology.

Blockchain use is, indeed, top of mind among banking executives who lead payments businesses. This dissertation will try to denote where and how blockchain technology might be implemented and used in the banking sector and the problems and deficiencies, strengths and solutions the banks may have in order to adopt such an advanced and controversial method.

2.1 Depicting the technology of Web

When the World Wide Web (WWW, et. The Web) [9] was invented – less than thirty years, a new era arised for the whole world. During after a decade since Internet [10] was officially “born” for the public, the Web changed the way people thought of communication, technological boundaries and duration of a task. Hundreds of new technologies, programming languages and tools and thousands of applications were developed based on the environment of the World Wide Web [11].

The last ten years a great progress has been reported in addition to the Internet. Technology novelties, a new terminology and plenty amount of regulations and protocols has been created to support the speedy progress of the Web. Since mobile devices entered the technology environment, people’s everyday life changed dramatically and is still be changing.

2.1.1 How it works

First of all, it is essential to distinguish the difference between the Internet and the Web. A worldwide network of computers linked mostly by telephone lines is a basic

definition for the Internet. Many things run on the Internet and one of them is the application of the Web.

The Web collects text pages, digital photographs, music files, videos, and animations from all over the world. Everyone that has a connection to the Internet can access this material. Specific programming languages supported by network protocols and displayed through web browsers connect all this information so as to produce webpages. A website is a collection of web pages. Every web page has hypertext links (or just links). When a user clicks on a link, a redirection of the first page is committed to another web page on the same or on another website.

So, as far as the Internet is concerned it should be said that nobody controls his/her data or has a native value settlement layer. The basic architecture of the data is based on the stand-alone concept for computers, where the data are stored and managed centrally from a server and the same data is sent or retrieved by a client (3 Types of Tier Architecture).

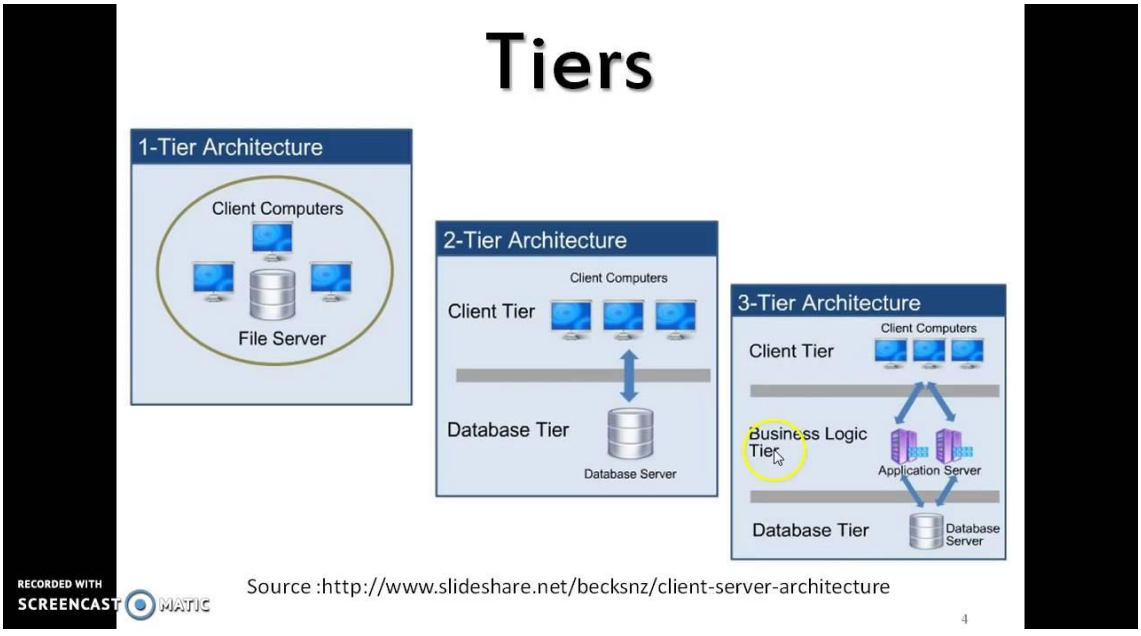


Figure 2.1

When one serfs (meaning interacts) through the Internet, a copy or copies of his/her data is sent to the server of a service provider. This means that at that moment the user loses control over his/her data. These data are still centrally stored either on user's computer or on other devices e.g. USB stick, cloud etc. despite the fact that every

moment that passes by more and more devices are getting connected with the Internet (e.g. watches, cars, TVs, and fridges). This raises issues of trust. [12]

To be more precise, for example, when one user sends a photograph to another user a copy of this session is made and sent to the other computer and when this happens, the control over data is lost on the other end of the Web, behind the walled gardens of a server. According to the privacy of world's personal data this is a serious issue and it is pretty obvious that causes issues in the backend of operations especially at the supply chain of goods and services.

Nowadays, the Internet has the client-server architecture [13] which means that it has also a centralized data management. Just like any architecture, the architecture of client-server one had also some serious issues. Firstly, the repeatedly data breache of online service providers, the increase of the cost for managing the enormous quantity of documents that passes through the Internet and certainly the lack of reinforcement of the transparency to the supply chain of goods and services. There are historic roots to these issues.

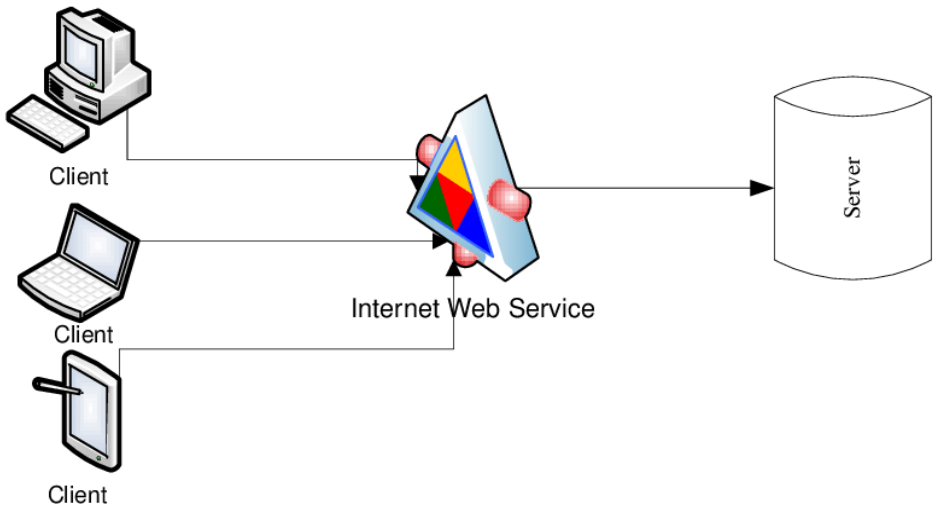


Figure 2.2

At this point is should be mentioned that through the years, the Internet was technically improved and evolved, giving the users the opportunity of a stronger, quicker and safer use of it. It started from a simple Web 1.0 (information economy) with the data transmission protocol of TCP/IP which simplified the transmissions of data

and reduced the transactions costs, to the Web 2.0 (platform economy) which introduced the social media and the e-commerce platforms to the users, established the peer-to-peer (P2P) interactions globally. Since then, the P2P interactions were accomplished with the use of a platform doing the job of a trustworthy mediator for two parties that were unknown to each other on the web. These platforms were equipped with a sophisticated content discovery, a value settlement layer and a set of rules for the execution of the transactions so, they controlled all data of their users (centralization).

The Internet we use today predominantly builds on the idea of the **stand-alone computer**. This means that data is centrally stored and managed on servers of trusted institutions. These servers use **firewalls** for protection and both are managed by systems administrators.

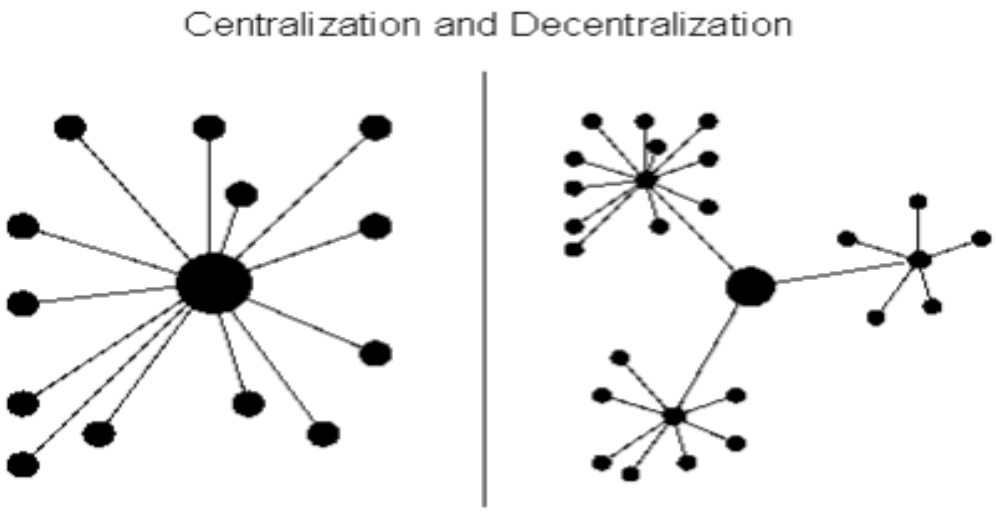


Figure 2.3

While the Web2 was a frontend revolution, the Web3 (token economy) is a backend revolution. More precisely, Web3 is a set of protocols using the technology and architecture of blockchain and intends to reinvent how the Internet is wired in the backend, combining two types of logic, this of the Internet and of the computer. This is why some refer to blockchain as a distributed world computer (decentralized). It is possibly the next big step in the development of computers and the Internet.

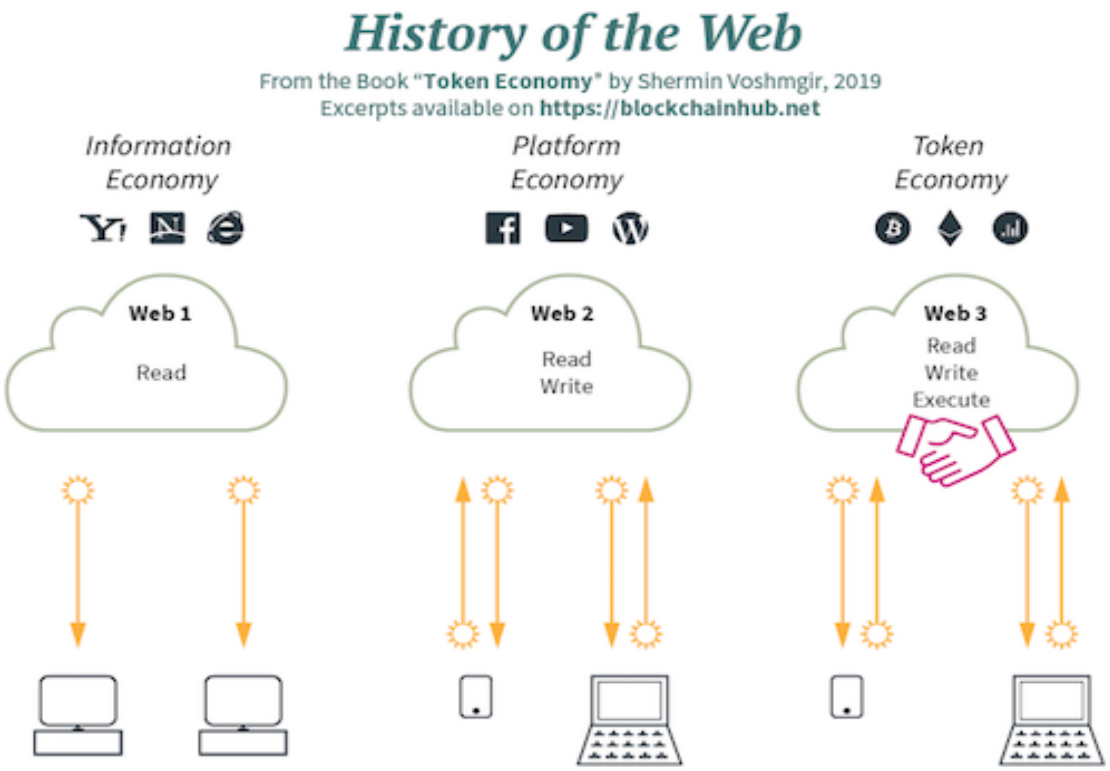


Figure 2.4

2.1.2 Strengths

"Information" [14] is the web's key value term. The web actually serves information to be stored, traveled, to be reached and to be available all over the world from everyone (internet connected). More detailed, the web is maybe the less expensive tool for one to communicate to others, share ideas, music, photographs using many applications such as text messages, video calls, uploading videos and so many other things. Also, in very little time, the web can inform and educate the users, can give the opportunity to users to do business and make different type of transactions.

Moreover, in the whole world the communication happens in real time, many tasks are put through from users in less time, information, as it is already mentioned, is available in a massive way, people can communicate and be connected with each other very often, digital payments become a primary "cure" for the queuing at the public services, banks and many other companies and at the same time increase the speed of transactions. Goods and services are easier than ever before to be trade freely.

2.1.3 Weaknesses

Everyone can apprehend that using the Web has a risk. Many dangers and traps are concealed through the Internet usually because of the "gaps" that exist inside the network and the web browsers. Hacking [15] of users' personal data is the number one trap that users may meet by using the Web. When someone, a hacker, as this person is called, steals a user's name, address, credit card, bank details and other information actually causes to the user a big economic loss and establishes insecurity inside the user's mind.

Many solutions have taken place against hacking through the years but none of these can assure the users that danger is eliminated and traps are all tracked down and destroyed forever. Technology companies are aware that all the faults of the system can't be healed 100%. This is inevitable since of the nature of Web, and certainly, the Internet which is a big open network to the world. It becomes clear that every technological method has some defects, even the most high-tech ones.

The status of who is who, who owns what, and who has the right to do what is a native mechanism called state. The Internet everyone uses today doesn't have this sort of mechanism. State [16] is a key property for managing values. Finance and efficient markets transfer value peer-to-peer (P2P) [17] easily and with efficiency. Holding state in the Internet would mean that value can be transferred without centralized institutions acting as clearing entities. As it was previously mentioned, today's Internet doesn't hold state. This is the reason why everyone needs Internet platforms to broker his/her actions.

Stateless protocols regulate the transmission of data while the data storage is indifferent for these protocols. The current Web uses stateless protocols such as the data transmission protocol called TCP/IP, and a subsequent protocol stack of related technologies, like SMTP for the transmission of emails, or HTTP for the transmission of Hypertext. So, the Web manage the transmission of the data from one user to another and not the way and the place of the storage of these data.

Data storage could be done centrally or decentrally. Centralized data storage became mainstream often for settling payments between two untrusted parties. Nowadays, for some parties, centralized data storage because of the stateless status of the Web is thought to be a strong disadvantage of the Internet.

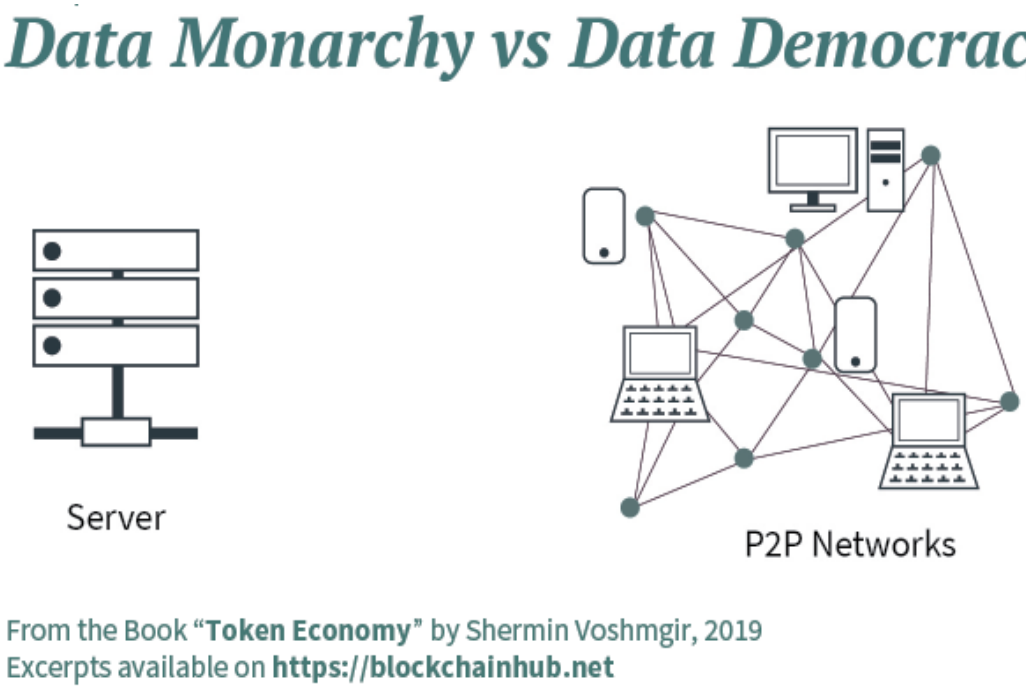


Figure 2.5

2.1.4 A new era arises – The Blockchain is a fact

A peer-to-peer version of electronic cash that allows direct online transactions between two parties without a third party was introduced in 2008 by Satoshi Nakamoto. This was the most serious attempt after the attempt on a cryptographically secured chain of blocks by Stuart Haber and W. Scott Stornetta [18] that was described in 1991. Originally blockchain, is a list of records that grows every minute. There are many of these lists that are called blocks and are linked and secured using cryptography [19].

Every block includes a cryptographic hash [20] of the previous block, a timestamp, and transaction data. The first block is called genesis block. This is an initiatory definition of the technology of Blockchain, a method that raises contradictions among scientists of many aspects all over the world because of the peculiar architecture it inherits.

2.2 Depicting the technology of Blockchain

As it was mentioned previously, the first blockchain was conceptualized by a person (or group of people) known as Satoshi Nakamoto [21] in 2008. Nakamoto used a Hashcash-like method to add blocks to the chain without requiring a trusted party to

sign them as checked and secure. Bitcoin cryptocurrency [22] is the most famous application of the blockchain. The bitcoin design has inspired other applications and blockchains are widely used by cryptocurrencies. At this point it should be mentioned that blockchain technology is readable by the public and this is an element that it is not easily seen in technologies in general.

In 1991 a paper was written by the researchers Stuart Haberand W. Scott Stornetta [23]. This paper proposed practical procedures for certifying when a digital document is created or modified. Over a decade later, in 2002, David Mazières and Dennis Shasha [24] took the concept further. In their paper "Building secure file systems out of Byzantine storage," [25] Mazières and Shasha studied how blocks can store data and developed the data structure and protocol of a multi-user network file system called SUNDR (Secure Untrusted Data Repository). That file system revealed blockchain's ability to store data in each block and consisted the framework for today's blockchain.

A whole new blockchain-based currency called bit gold was proposed by the computer scientist Nick Szabo [26] o in 2005. It was one of the earliest attempts at a decentralized currency, which changes control from a single entity to various smaller ones. The new currency was based on "computing a string of bits from a string of challenge bits," introducing innovative concepts such as "client puzzle function," "proof of work function" [27] and "secure benchmark function." Despite his pioneering cryptocurrency features like time-stamping and proof of work, his digital cryptocurrency coin failed to overleap the double-spending problem of electronic transactions. When an electronic transaction was taken place, the users of bit gold could duplicate transactions and therefore spend the same digital money more than once.

In 2008, the anonymous innovator known as Satoshi Nakamoto (it remains unknown if Nakamoto is a person of a group of people) introduced a peer-to-peer (P2P) version of electronic cash that allows direct online transactions between two parties without a third party. Implementing distributed peer-to-peer timestamp servers which generate computational proof for the chronological order of transactions was the idea that Nakamoto proposed as a solution to bit gold's double spending problem. Nakamoto's idea became a reality in 2009 when a transaction was verified and added to the base of the chain as the first block of this chain. That time was the kick off of a

chain of blocks, containing information on verified transactions and that was the first mining of a block.

2.2.1 Evolution of Web – Web 3.0

Different parties that do not trust each other can share information without requiring a central administrator is what blockchain method offers. A network of users is acting as a consensus mechanism (a protocol) and share the same system of records. The main target of this part of blockchain technology is to create a secure digital identity reference. This sort of identity is based on cryptography. It combines both private and public cryptographic [28] keys. Blockchain seems to lead the Internet to the next level, what some refer to as the Web3.

Blockchain reinvents the way data is stored and managed. A unique set of data (a universal state layer) is provided in such a way that is collectively managed. For the first time, due to the appearance of Bitcoin, this universal state layer enables a value settlement layer for the Internet. According to the latter, the user has the permission to send data in a copy-protected way and facilitate true P2P transactions without intermediaries.

The design and structure of the Bitcoin blockchain and similar protocols eliminate the possibility of breaking into the system and corrupt, steal or destroy any of the data that this technology facilitates. In blockchain method data is stored in multiple copies of a P2P network so it is almost impossible for someone to intrude to many of the nodes at the same time and make harm to the system with all the cryptography and hashing it is used. Small possibility and prohibited expensive.

In the Web3, as it was previously mentioned, data is stored in multiple copies of a P2P network (blockchain uses Web3). The majority consensus of all network participants formalizes the management rules and conditions in the protocol and secure them with a native network token for their activities. One can think of blockchain as the backbone of the Web3. So, it can be easily comprehensible that blockchain determines the data structure in the backend of the Web.

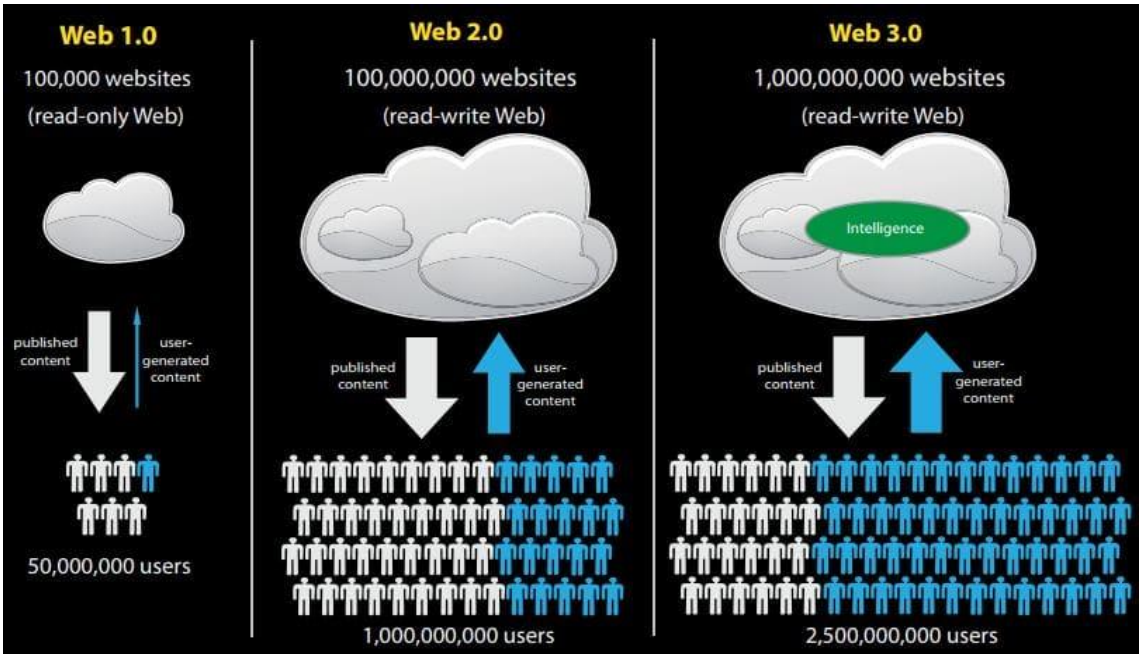


Figure 2.6

2.2.2 Distributed Ledger

At this point it is essential to mention that blockchain is a part of a technology known as Distributed Ledger. However, globally blockchain is the mostly known method instead of the initial technology basis of it which is the Distributed Ledger Technology (DLT). So, it is important to present the main segments of the DLT so as to understand deeper the blockchain method.

Ledger is a list or a group of data that is collected, stored and can be replicated, shared and be synchronized according to the need of the users. Distributed Ledger is a digital ledger geographically spread through a peer-to-peer network without any centralization of the data that is stored.

Today, cryptography and decentralization, wherever are applied help information to be stored on computers safer and faster. A distributed ledger is also a decentralized database across the nodes. Every node will maintain the ledger in this technology, and the ledger will get updated if any data changes occur. Each node does the update of the data independently. All the nodes have the same status in terms of authority. There isn't any centralized authority or server managing the database, which gives to the technology the element of transparency. When a node updates the ledger the rest of the

nodes verify its existence. Transaction will be verified by the consensus algorithm or voting.

It should be mentioned here that the rules of a ledger set the framework as far as voting right or participation of all the nodes is concerned. Sometimes all nodes can participate and sometimes only selected ones. Since all nodes approve the pending for approval transaction, the transaction gets a place on the ledger, and the updated status appear to all the nodes. So, this technology construct trust relationships and every user that uses this kind of method enjoy a lot of transparency and a key-value word for everything. Moreover, due to lack of centralized authority, all the distributed ledger technology provides a great deal of security. No single node is a single authority. Nodes will get a chance to perform verification so there's no point of corruption in this technology. This characteristic sets this technology interesting for many industries such as financial, government, medical, science industry or any other industry looking for more transparent technology and those that want to avoid central authority.

However, it is essential to mention some specific differences between blockchain and distributed ledger technology. Fist of all the structure of these two methods differ in main points. Blockchain consists of blocks of data whilst a distributed ledger is a database spread across different nodes with different representation of these data in each ledger. Secondly, there is a strong difference in the way the two methods work. For example, in the case of DLT a consensus is essential while in the blockchain multiple methods can be used to achieve a consensus such as Proof of Stake (PoS) and Proof of Work (PoW).

DLTs are not a new concept, although they have become popular only recently. The talk about decentralized databases it's a long and deep in the past story. One can find many applications that are currently using distributed ledger, for example IBM Fabric, R3 Conda, and Digital Asset Holdings. These DLT systems are similar to the blockchain mostly because the offspring or subset of distributed ledger technology is blockchain technology.

2.2.3 Peer-to-Peer network

The P2P architecture introduced itself to the mass market in 1999 by the file sharing application Napster [29], where files were stored across multiple computers. In

that way users could share, download, upload and store these files to their own computer devices at the same time without the need of a central server.

Peer to Peer network (P2P) is a network model with a totally different structure and architecture than other more traditional network models such as client-server ones. More detailed, in a P2P network, the "peers" are computer systems that are connected to each other via the Internet. Each peer is considered equal and are commonly referred to as nodes. The requirements needed for a user to join a P2P network is to have an Internet connection and software programs that supports P2P structure. Computing resources can be provided to many participants directly with a peer and therefore no centralized servers of stable hosts are needed.

Since a participant is connected to the network, P2P software allows him/her to search for files on other people's computers that join the same network and vice versa. This means that every user that participates to P2P can search for files in other participants' computers where typically these files are within a shared folder. It should be mentioned here that providing the resources is voluntary!

A core point of difference at P2P architecture is that the data storage is not centralized but every data is recorded and interchanged all the time among the participants (peers or nodes) on the network so, each computer on a P2P network becomes a file server as well as a client. It is also important to mention that at a P2P network can improve its power instantly with the acceptance of every new participant – node that joins the specific network.

A Peer to Peer (P2P) network is a very important element of the structure of blockchain technology and one can realize the contribution of this network to solidity and security of the blockchain.

Moreover, all nodes are equal into a peer-to-peer network but in a blockchain system they might take on different roles, such as that of a miner or a "full node". If a node has the role of a "full node", a copy of the whole blockchain is done in a single device which is connected to the network. This means is that if someone tried to steal of destroy the information stored on a blockchain, he/she should destroy every single full node on the network. If a node escapes the disaster, the network of blockchain can be rebuilt.

2.2.4 Cryptography

Disguising and revealing information through complex mathematics is called cryptography method, or also known as encrypting and decrypting. So, only the intended recipients and no one else can view the information. At a first look the concept of the method looks rather plain. Unencrypted data, for example a piece of text, gets encrypted by the use of a mathematical algorithm, known as a cipher. A piece of information is produced, the ciphertext, that is completely useless, making no sense, until it is decrypted. This method of encryption is called symmetric-key cryptography.

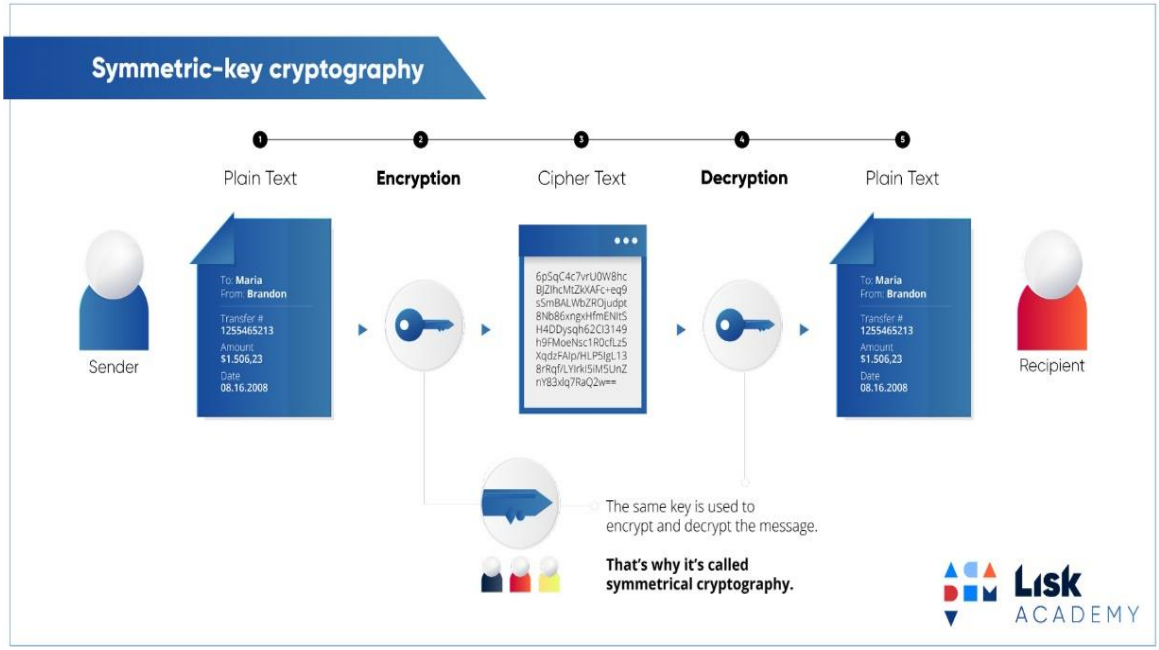


Figure 2.7

The code base for most ciphers are open source projects. This means that anyone can examine the code of a cipher. AES is the most widely used cipher in the world and its use is free for anyone. The AES libraries, which are the ones that implement the algorithm, have been investigated over the last five years and the result it was extracted was that no vulnerabilities were found. It worth mentioning that the cipher is also used by the National Security Agency (NSA), the United States intelligence agency, as the tool of choice for encrypting information.

In blockchain, cryptography is primarily used to ensure that the identity of the sender of transactions is totally secured and that the past records can't be tampered.

Cryptography is used by the blockchain technology as a means of ensuring transactions are safely completed and as a means of securing all data and storages of value. These are the core reasons that every user of blockchain can feel trust to this technology that once something is recorded on a blockchain, it is done so legitimately and in a manner that preserves security.

Public-key cryptography, also known as asymmetric cryptography, is the type of cryptography used in blockchain method, represents an improvement on standard symmetric-key cryptography. A public key, which is shared to everyone allows information to be transferred to the nodes. Asymmetric cryptography uses two separate keys, a public and a private to encrypt and decrypt an information so as to deliver with security and authentication the data. the information can be encrypted with a combination of a user's public key and private key and decrypted with the recipients private key and sender's public key. It is absolutely impossible to discover what the private key is based on the public key. Therefore, a public key can be sent to anyone without the fear of someone can gain access to the private key. So, the sender can encrypt files that they can be decrypted only by the intended party.

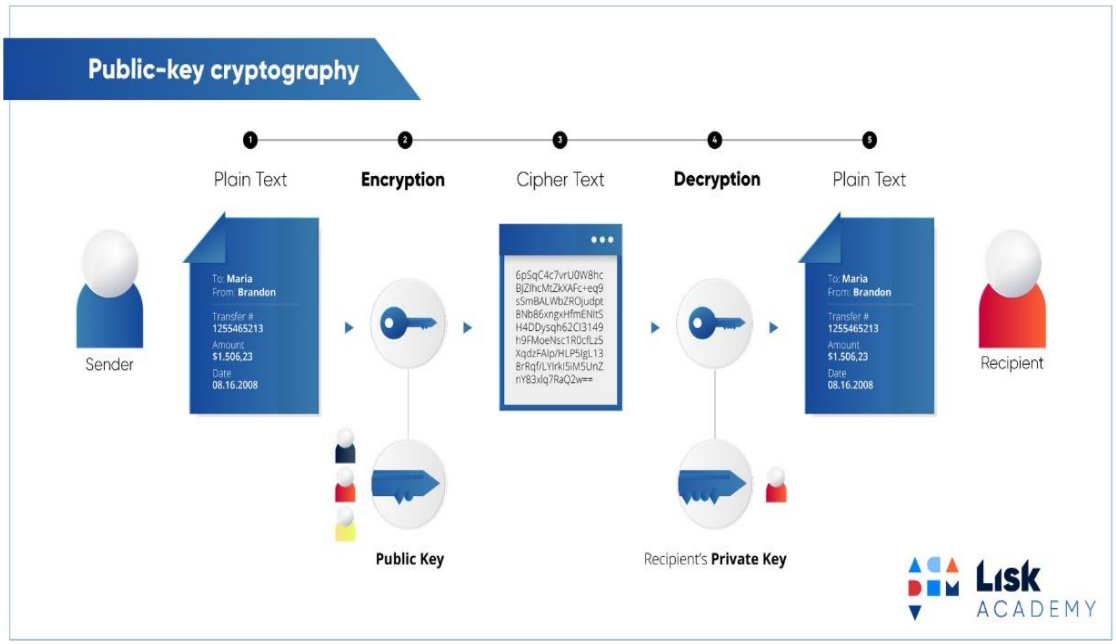


Figure 2.8

Furthermore, digital signature appeared due to public key cryptography to ensure the integrity and security of the data that is recorded onto a blockchain. In more detail, digital signatures utilize asymmetric cryptography so, information can be shared with anyone, with the use of a public key. Digital signatures are a standard part a blockchain protocols, mainly utilized for securing transactions and blocks of transactions, transferal of information, contract management and many other issues that deal with external tampering.

When blockchain uses digital signatures instantaneously it gains three main benefits as far as storing and transferring information is concerned. Integrity, as it mentioned previously, is maybe the core benefit blockchain perceives from digital signatures. This is achieved by combining a user's' private key with the information that they wish to sign, using a mathematical algorithm. The network will not recognize the data as valid if any part of it is tampered when the actual data itself is part of the digital signature. Since a small part of the data is edited the whole signature is reshaped so the signature gets false and obsolete. Through this, blockchain technology guarantees that any data being recorded onto it is true, accurate and untampered with. Using digital signatures, blockchain technology succeeds to keep the data that is recorded to, immutable to threats, corruption and destroy. Secondly, digital signatures can secure the identity of the individual sending it. The user of a digital signature and the owner of this signature are bounded.

A public key and a private key appear as strings of random numbers and letters used to blockchain. It is essential for the security of the transactions the private key to be kept in one's person's possession. It is equally important to have the private key written down and stored in a safe and secure place, not in a digital repository but preferably to a piece of paper or something that cannot be hacked. In case of losing the private key, the information that is controlled by the key, will be lost.

Lastly, digital signatures gain a quality of non-repudiation since private keys are linked to individual users. So, if a user signs information digitally, this data can be binded and associated with that user legally. As mentioned above, the data has signed with a private key that was seen and used only by its owner. At this point, it is important to be indicated that digital signatures are unique for the user that signs the information and are produced by utilizing three algorithms. These are, a key generation algorithm

that produces a private and a public key, a signing algorithm which produces a signature from a combination of the data and the private key and a verification signature algorithm which determines if the message is authentic or not.

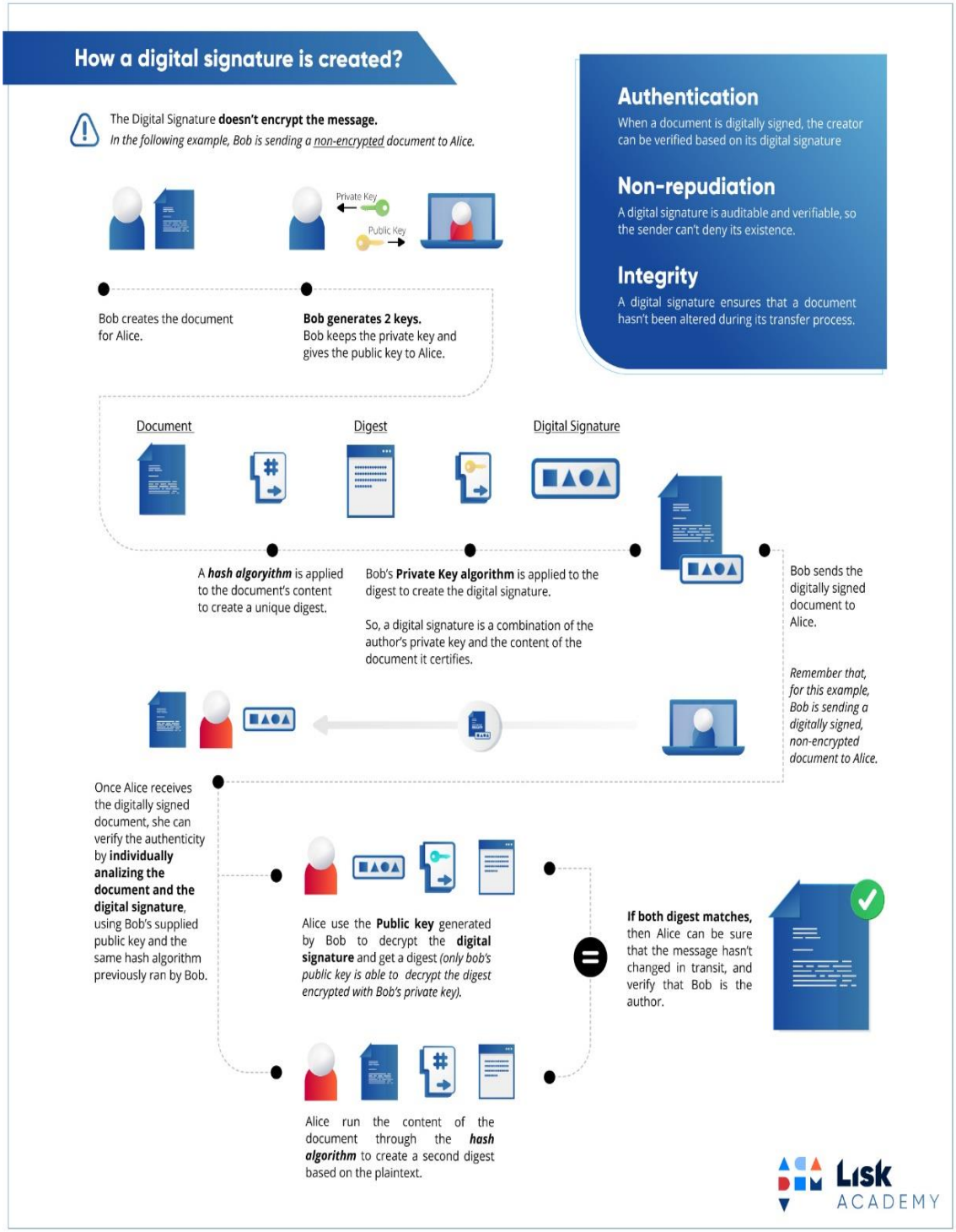


Figure 2.9

Zero Knowledge Proofs (ZKP)

Zero-Knowledge Proofs (ZKPs) [30] or **zero-knowledge protocol** is a method that allows data to be verified without revealing that data, for example, it would be difficult for someone to get a loan without disclosing credit information.

In cryptography, zero-knowledge proofs and proofs of knowledge are basic notions and powerful tools. In these kinds of systems, each transaction has a 'verifier' and a 'prover'. The prover attempts to convince the verifier that something is true without telling the verifier anything else about it but the validity of the assertion. These proof systems are the building blocks in many cryptographic constructions. This is the reason why these systems have the potential to revolutionize the way of the collection of the data that is used and the way of the collection of the information that is transacted. In a transaction using ZKPs, the prover proves that he/she can compute something without revealing the input or the computational process whilst the verifier only learns about the output. At the previous example, someone could get a loan, the prover, without revealing his/her specific credit information to the verifier. This tool can help users to gain control to their data and at the same time can maintain the privilege to use applications that facilitates them in many aspects of their lives. A true ZKP needs to prove 3 criteria, completeness which means convincing the verifier that the prover knows what they claim they know, soundness which means that if the information is false, the verifier cannot be convinced that the data of the prover is true and finally, zero-knowledgeness which means that it should reveal nothing else to the verifier.

Figure 2.10

2.2.5 Hash Functions

Hashing constitutes a fundamental element of blockchain so as to maintain the reliability that this technology offers. The term of hashing is not unknown to technology world. It is the process that with the use of a mathematical algorithm takes an input of any length and turns it into a cryptographic fixed output such as SHA-256 for Bitcoin. If someone tries to decrypt the data by looking at the hash it becomes impossible to work out the length of the encrypted information based on the hash. A cryptographic hash function is considered to be useful when the production of the same hash value is impossible for differing inputs so in that way the authenticity of input is preserved.

According to the previous one, the same hash value will always be produced by the same message. Also, a hash value never determines input and when an input is changed even in just a detail, the hash alters completely. The latter one is a serious matter of safety. If the hashing algorithm is really complex then the input is safer and the output is difficult to change. In that way, hashing provides the certainty to the intended recipient that data hasn't been tampered with through their "journey" to the recipient.

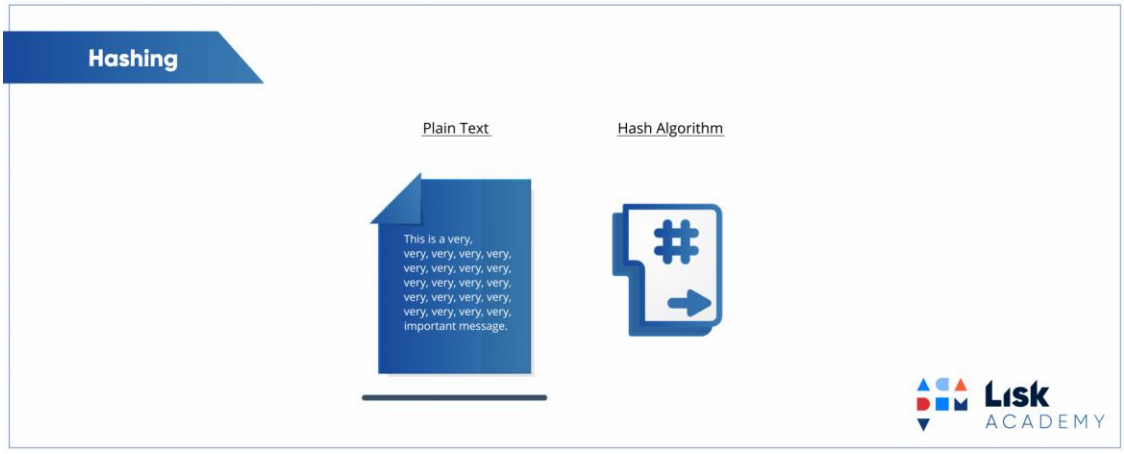


Figure 2.11

At this point it should be mentioned that a data structure of hashes is a Merkle tree [31] (or hash tree). It is used to record data onto a blockchain in a secure and efficient manner. A block of transactions is running through an algorithm to generate a hash. This specific, hash that leans on the original transactions, verifies that the data is valid. Each transaction is hashed and after a while an entire block of transactions has already run through a hash function so these transactions is linked and hashed together and

finally for the whole block one hash is created. When this process is visualized it gives the picture of a tree in a simplified way. Starting from the top, the upper hash is called the “root”, the middle hashes are called the “branches” and the bottom row has the “leaves”.

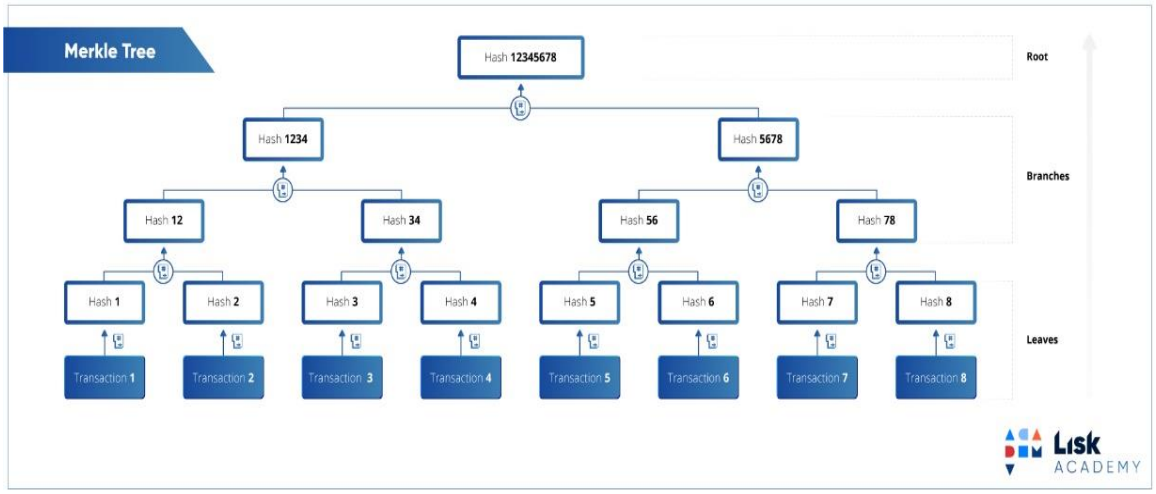


Figure 2.12

A user can confirm the validity of an individual transaction through Merkle trees without the necessity of downloading a whole blockchain. A block header contains the hash of the Merkle root with the hash of the previous block, the timestamp, the nonce, the block version number and the current difficulty target.

The function of blockchain is based on Merkle trees, hashes and consensus protocols and these are without doubt, the strong tools of the framework of blockchain technology that provide security, integrity and irrefutability.

2.2.6 Smart Contracts

A P2P network of computers manages a self-enforcing piece of software called smart contract. Smart contracts, otherwise called self-executing contracts, blockchain contracts, or digital contracts are efficient rights management tools since they are computer protocols. They set a specific digital framework for agreements between network participants that provide such a coordination and conditions that the need of traditional legal contracts is eliminated. Two parties can use smart contracts for an agreement, either is simple users or companies.

Decentralized ledgers were used for smart contracts since contracts could be converted to computer code. Also, in 1994 it was realized by Nick Szabo, a legal scholar, and cryptographer that these contracts could be stored and replicated on the system and that the network of the devices that run the blockchain could supervise them. Smart contracts facilitate users to exchange money, property, shares, or anything of value. This is succeeded in a transparent, conflict-free way and without centralized services.

Smarts contracts have been implemented in many sections such as in government, automobile real estate and others. At this point, it is essential to refer how smart contracts can be used and are used in Management and Healthcare.

Business operations are a core part of the management of a company. It is widely known that there is a great back-and-forth coming of documents until they get approved or disapproved. A blockchain ledger streamlines this. It also omits incompatibilities that typically occur with independent processing and they perhaps lead to lawsuits and settlement delays. It also could be used for regulation compliance, testing results and managing supplies.

Blockchain could encode and store personal health records in the sector of healthcare and with the use of a private key which would grant access only to specific individuals. Also, blockchain could store receipts of surgeries and send them automatically to insurance providers as proof-of-delivery.

It is really necessary to mention the existence of tokens [32]. Traditionally, tokens can represent any form of economic value and are used in many aspects of life, such as health, accommodation, entertainment, computing and so many others. Types of tokens are, for example, stock certificates, ID cards, casinos chips, vouchers, g- cards, bonus points in a loyalty program, club memberships, or train or airline tickets. Paper money or coins are also tokens. Most tokens have some inbuilt anti-counterfeiting measures so as to maintain the system secured.

Particularly in computing, they can represent a right to perform some operation or manage access rights. Cryptographic tokens on the blockchain have lower issuance and management costs involved and provide securely trade on the blockchain with no intermediaries. Fraud and corruption as far as good and services are concerned can become difficult for someone to succeed as long as tokens are used.

Cryptographic tokens represent a set of rules, encoded in a smart contract. These cryptographic tokens inside a smart contract are called the token contract. Every token belongs to a blockchain address. A dedicated wallet software can access these tokens by communicating with the blockchain and this software manages the public-private key pair related to the blockchain address. The person that has the private key for that address is called the owner or custodian of the token and he/she is the one that can have access to the tokens.

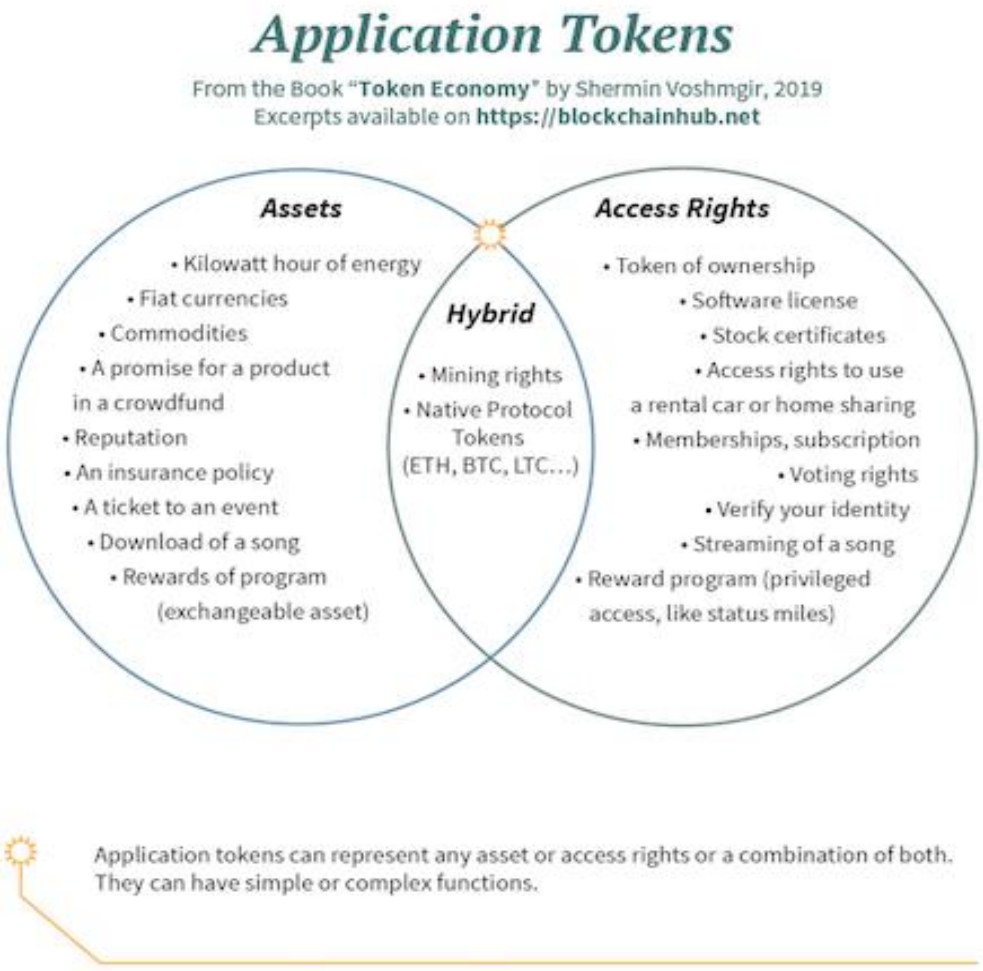


Figure 2.13

2.2.7 Consensus Mechanism

There are specific protocols that confirm that all nodes in a blockchain are synchronized, go along with the transactions that are legal and are added to the blockchain. These protocols are called consensus mechanisms. These mechanisms are fundamental and critical for a blockchain in order to function correctly. First of all, due

to consensus mechanisms it is certain that every participant uses the same blockchain and all transactions are checked all the time so that the users can submit things into the blockchain. All nodes can audit the blockchain constantly and with the help of these mechanisms blockchains are safe of various attacks. There are three main categories of Consensus mechanisms:

Proof Of Work (POW). It is the first blockchain consensus mechanism and Bitcoin was the first that used it. POW requires some work from the service requester so as to protect from attacks and other service abuses such as spam on a network by, usually meaning processing time by a computer.

The process of Proof of Work is widely known also as mining and the participants that take part in this procedure are called miners. Miners or nodes require a lot of computational power to execute mathematical procedures (called puzzles) which have specific properties like the verification of an answer to a puzzle. The participant that will guess the answer to the puzzle creates a block. For this block he/she gets a reward. These kinds of puzzles are solved only with the trial and error method and need a lot of computational power so as to find the solution quickly but if blocks are built too fast, the puzzles get harder. The puzzles' difficulty depends on how quick the blocks are mined. It is obvious that the more power a participant needs, the higher cost it has. So, within a certain timetable, blocks should be created so as to keep a certain supply of coins that are new.

However, Proof of Work uses a lot of resources and for this reason is thought to be unsustainable in the future. This is the main reason why some blockchains are moving to different consensus mechanism.

Proof Of Stake (POS) is a "sibling" of Proof of Work (PoW) protocol as far as the environmental part is concerned and was constructed as an alternative to PoW. In POS, instead of miners, there are validators (or participants or users). The validators use some of their cryptocurrencies as a stake in the blockchain. The core idea in PoS is betting only in this case the bet is on these blocks that look like they will be added next to the chain. When these blocks are added, the reward is a block in proportion to the validators' stake. PosS is an algorithm that helps a blockchain to achieve distributed consensus. In cryptocurrency terms, stake is the cryptocurrency that belongs to a participant and forfeits in order to partake in validation. To find the user that is going to produce the next block in a Proof of Stake system, the process which is used is random.

At this point it is essential to mention that Proof of Work system differs from Proof of Stake system into a serious point. Some or none of the cryptocurrencies that are mined may not belong to a miner in a PoW. This means that miners blindly care only how to maximize their profit without actually improving the network. In a Proof of Stake system this is out of the question since validators hold the coins of the blockchain on which they are validating and through this procedure the network is maintained.

Delegated Proof Of Stake (DPOS) is a consensus mechanism most known for its implementation in EOS[1]. Due to the stake-weighted voting system it preserves, it is often referred to as a digital democracy. In a Delegated Proof of Stake system has delegates. A delegate is a person or organization that wants to produce blocks on the network. The delegates are chosen by the participants who can stake their coins to vote for a certain number of delegates. Their vote is weighted and emerge from their stake.

There are also many other Consensus methods such as Proof of Capacity, Proof of Elapsed Time and others, yet at this point of the study, it is rather exaggerated to go further.

2.3 Blockchain In Details

As it is refered in deep in 2.2.2. section, blockchain is a type of a distributed ledger. In blockchain a user does a transaction and the whole transaction gets encrypted and is added to a ledger. A specific number of these transactions create a block of data. So, in this way many blocks are created and added to the system, secured and bounded to each other through cryptographic principles and strict security protocols. When a new transaction occurs, the existing copies of the ledgers are updated. No alteration or deletion of existing data can be done so every transaction exists in history. No central authority is required for managing the operations into a blockchain, so the it is considered as a decentralized system and this is a major difference from traditional databases.

In blockchain technology blocks are in a particular sequence whilst in distributed ledgers there is no need for having sequence of data. Since blockchain is a decentralized system, no intermediaries (Middlemen) are necessary between the participants so it is

[1] The main native **token**, **EOS**, is a **token of utility.** On the blockchain, it provides bandwidth and storage in proportion to total stake (owning 1% of **EOS tokens** allows for usage of up to 1% of the total available bandwidth).

faster, cheaper and more secure than the centralized systems and this characteristic is the main reason for governments, banks, science and so many other sectors to turn to them. In 2024[2] the blockchain market is expected to increase to 16 billion USD from 2.3 billion USD in 2021.

Blockchain embraces three core technologies and introduce them as principles to it system. First of all is the private key cryptography, secondly a distributed network with a shared ledger and lastly, an incentive to service the network's transactions, record-keeping and security.

2.3.1 Blockchain Structure & Architecture

Blockchain is a technology that embraces and combines different technologies and allows data in digital form to be distributed (not copied). In the previous sections of this dissertation all these different technologies have been analyzed in deep layer. At this point, the core blockchain architecture components will be mentioned and at the same time the use of these components into a blockchain system.

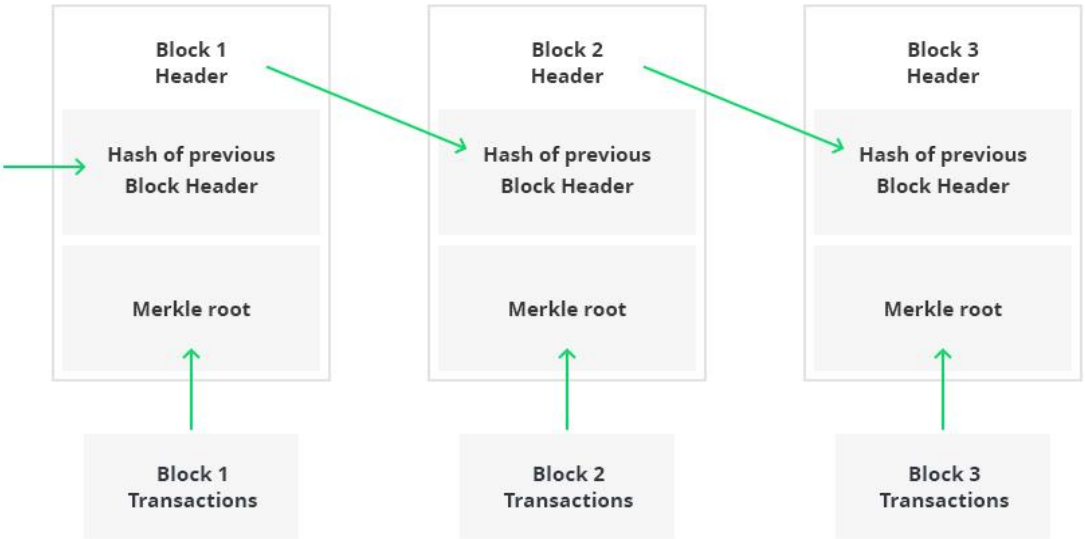
The Web uses servers which are located in specific places to store, update or delete data with the help of administrators with permissions. This data is exchanged among users. However, blockchain uses a distributed network (peer-to-peer network) in which data is controlled by individuals and participants. The P2P network embraces many computers. The data in these computers cannot be altered or erased without the participants to be aware of this movement and so give the consent for the specific movement.

First of all, every user or participant in a blockchain system is considered to be a node. Sometimes, a node is equated also with devices such as pc. Every node keeps an independent copy of the whole blockchain ledger. All data comes from transactions that happen among the participants. So, transactions serve the purpose of a blockchain since they bring all the data that are exchanged among nodes. The transactions are grouped into sets, they are distributed to all nodes and are kept in a specific data structure known as block. A sequence of blocks in a particular order constructs a chain. Therefore, this method is called, blockchain.

[2] https://www.wintergreenresearch.com/

More detailed, inside of a block the data is stored to lists as a flat file (i.e txt format) or in a form of a simple database. There is the pointers' data structure used to keep information into a blockchain system where pointers are variables that points to the position of another variable and keep information about the latter's location. Also, there is the linked lists' data structure, where each block has specific data and links to the following block through a pointer, except of course from the first block of this sequence of blocks that it won't have a pointer and the last block of the same sequence that its pointer won't have a value!

Blockchain Hashing



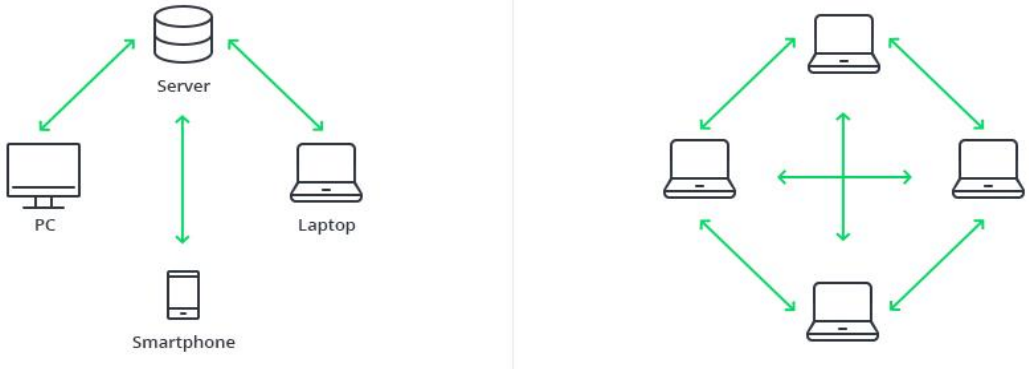
Blockchain Structure

Figure 2.14

At this point it should again be mentioned that not all nodes play the same role into a blockchain. Some nodes verify the whole process of this technology and they are called miners. A very important part of the blockchain method is the consensus protocol (see 2.2.7 Section) which is like every other physical or digital protocol. It contains all the rules and arrangements for the blockchain operations to be conducted properly, efficiently and securely.

Last but not least, a new block is built whenever a new record or transaction within the blockchain is carried out and for its genuineness every new record or transaction is digitally signed. This new block is added to the chain of the network only after the verification of the majority of the nodes into the system.

Moreover, it would be an omission not to underline once more that digital information is rather distributed than copied with blockchain and through the use of a distributed ledger, transparency, trust and data security is offered to every participant. Financial sector uses in expansion the blockchain architecture mostly, at least at the beginning of this technology, for cryptocurrencies and also for record keeping, digital notary, and smart contracts. The following picture shows the difference between the architecture of the centralized databases of a client-server system and the decentralized architecture of blockchain which eliminates the traditional way of storing data and records in a central point (server/s).



Client-Server P2P Network

Figure 2.15 Client-Server vs P2P Network

2.3.2 Basic Types of Blockchain

There are two basic types of Blockchain. The first one is the centralized or private blockchain system and the second is the decentralized or public one which is totally opposite to each other. Some very common examples of a centralized blockchain system is Facebook and Google and of a decentralized blockchain system is LimeWire and BitTorrent.

A centralized system keeps the control of an activity or information into a single authority. This means that platforms with centralized systems have a single point of contact i.e. a private hub.

A decentralized system keeps no control of the information or data into a single authority or point for example a server or an official and trustworthy authority or organization. On the contrary, the data is stored and distributed along the stations of the users or participants of the network (peer-to-peer network).

Certainly, there are some similarities and differences between the two systems whereas some advantages and disadvantages. Here are some of the most important ones:

- Centralized Blockchain Advantages:

Users (individuals or companies) gain a strong control over the network and enjoy the flexibility to customize the blockchain system according to their needs. Also, in a centralized blockchain network the users have the right to choose the participants in the network and either prove or disapprove them due to their rules and regulations. Moreover, since they need less resources than a decentralized blockchain system to implement and to secure the entire network, a centralized blockchain system does less harm to the environment. So, users can use them to store and protect information of the highest significance among the trustworthy nodes.

- Centralized Blockchain Disadvantages:

However, the data isn’t so spread in a centralized blockchain system and this element gives a lower security compared to a decentralized blockchain. Also, an outside audit is more difficult to be done to the user of the centralized blockchain than with decentralized system except for the users of a centralized blockchain that deploy the system themselves.

- Decentralized Blockchain Advantages:

Decentralized blockchains have a high degree of security due to the use of mining resources and also equally important is that the decentralized type of blockchain operates with no Middlemen (intermediaries).

- Decentralized Blockchain Disadvantages:

A public blockchain has higher risk to reveal information of the users that participate into the network (P2P). Also, a strong disadvantage of public blockchain is that the number of blocks can become big, so the need for miners can become also big so as to make the system work. This means that the need for computational power will also become big and this system will become a non-environmentally friendly system.

Similarities Between Centralized and Decentralized Blockchains

Public and Private blockchain systems are very similar, as far as technical features are concerned. These systems operate into peer to peer networks, meaning that all nodes have the responsibility to store and secure the shared data. They both use a consensus mechanism, according to their specific needs and aims, through the network and the nodes while establishing a single ledger. Lastly, both of the systems should define and set the bounds on the security and efficiency of the network.

Differences Between Centralized and Decentralized Blockchains

A very basic difference between these systems is the number of nodes that can participate and have the role of the administrator to make changes into the network. In a decentralized system there is no limit at the number of nodes that can insert the network such as the Bitcoin system. Typically, there is a restriction to the nodes in a centralized blockchain since it plays a great role the participants that will allow changes to the ledger since the private system is used to store, update and exchange internal records.

2.3.3 Technologies for Blockchain

Blockchain is evolving through the years and many programming languages and other technologies are set at blockchain's disposal. It is very important, especially for the developers to consider what kind of programming language they should use according to the development the need to undertake. Certain languages are used for certain applications in a blockchain system. More detailed:

- Solidity is a programming language used for developing smart contracts of Ethereum. It is used by many developers (over 200.000). The latter lead many platforms of blockchain to be Solidity compatible as far as smart contracts is concerned and give the ability to import smart contracts from Ethereum to these platforms.
- Ethereum embraces many languages such as C++, Python, Ruby, Go, and Java and works as an Ethereum Virtual Machine (EVM). The backbone of Ethereum is considered to be JavaScript that functions as a runtime environment with script execution.
- Java is an object-oriented, class-based programming language and one of the top used languages all over the world. NEM[3]'s core blockchain network has been written solely in Java.
- C# is an object-oriented language that runs on the .NET Framework since 2000. C# builds strong code for cross platform and can perform over multiple operating systems such as Windows, Mac, Linux, and Android. Many blockchain projects use C# which include for example Stratis, NEO and others.
- Javascript (JS) is a multi-paradigm language and one of the most popular programming languages in the world. It supports blockchain systems.
- Structured Query Language (SQL) is a programming language that communicates with databases and is used by a blockchain in the form of Aergo. The most popular databases of the world such as MySQL, Oracle, DB2 use this language that store, query, and manipulate data.
- Blockchain projects use EOS which the main programming language that it uses is C++ for running applications on the top of blockchain. At this point it should be mentioned that Bitcoin core's network is programmed in C++.
- HyperLedger Fabric is a framework where solutions and blockchain applications can be developed with a Java. Performance and privacy are the two benefits HyperLedger Fabric offers to consensus.
- Golang is also an open source language that is used by the consortium network and is based on the syntax of the C programming language. Moreover, most of the contracts that is built using HyperLedger Fabrics, the chaincode [33], is written in Golang.

[3] Network empowerment Mechanism – a P2P cryptocurrency and blockchain platform launched in 2015

2.3.4 Strengths

Blockchains use three main technologies that were previously analyzed and denoted for their usage and characteristics. These are the public key cryptography, peer-to-peer network [34] and the blockchain's protocol (platform). When a transaction is performed, every system sets as a goal to succeed the safe and faultless completion of the transaction. The same goal is also set for the distributed systems such as blockchain which has no central authority to take control of the system and retains at the same time the transparency of the system. Transparency is the ability of all the participants into a blockchain system to be able to view all the data and any changes that may occur. Last but not least, the core value of blockchain is that it is more secure because of the use of cryptography both for data and for users' identity.

The four principles of integrity build the trust among the participants into a system in which they exchange data. Blockchain embraces these principles and therefore, until now, it is considered to be a system to rely on. These are:

- Honesty
- Consideration
- Accountability
- Transparency

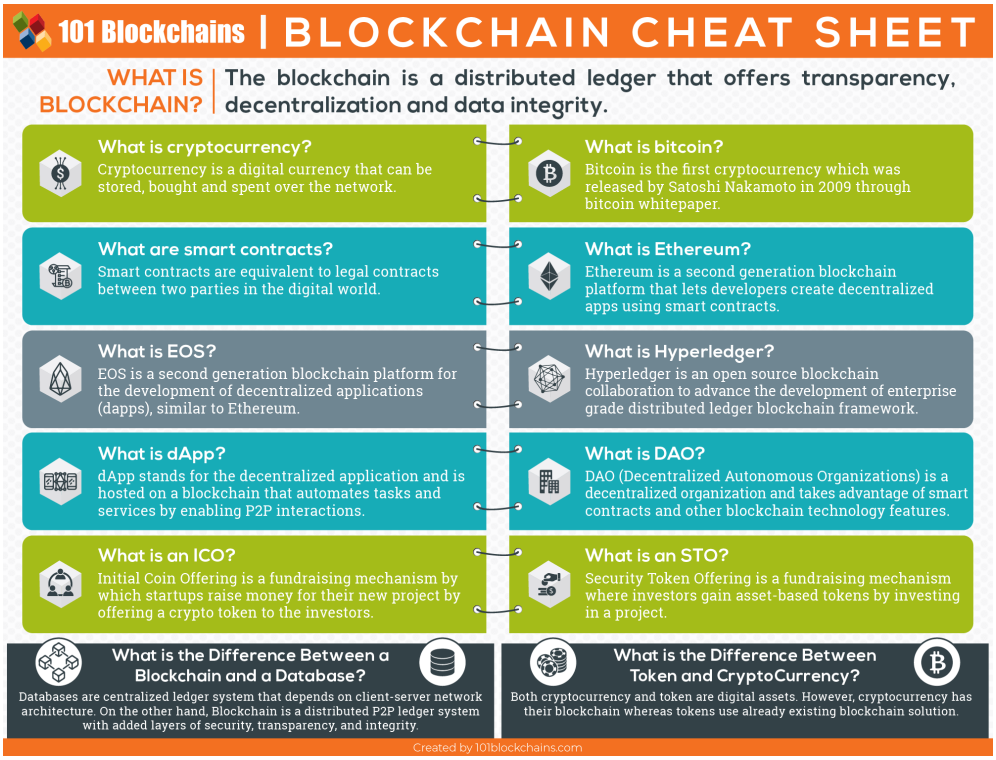


Figure 2.16

2.3.5 Weaknesses

One can understand that every technological method has it's "Achilles' heel". In the blockchain case, there are very specific ones. Three crucial disadvantages of this method are the size of blockchain since every day when new transactions happen, data are recorded to blockchain so blockchain grows every second, the resources (computer power etc) which are needed so as to operate adequately every task and the regulatory field that is still under construction.

Furthermore, it should be mentioned that mining risks network security and scalability remains one of the basic issues of blockchain. Last but not least, the structure of blockchain reveals the danger of complexity of the system since many technologies need to be bond together and work efficiently and at the same time the potential of enormous expansion of the system gives food for thought in troubleshooting.

2.3.6 Challenges

This dissertation will try to evaluate the pros and cons of this technology especially when many organizations, individuals and even some economies attempt to implement blockchain in banking industry, whether it will benefit or not the banking sector and with which approach (e.g. applications or agreements to be made among banks).

Everybody searches for a trust protocol, an unbiased, reliable, and robust uncorrupted system where through this system every transaction will be completed successfully without the anxiety of a mistake or an intrusion or even a fail inside or outside of this system. A part of users, scientists, businessmen, people of technology strongly believe that blockchain is the result of this search. Some others though disagree. There is no doubt that Blockchain is a very controversial subject and that only time can prove the usefulness or not of it!

2.4 Widely Known Blockchain Applications

2.4.1 What is the Bitcoin?

Bitcoin is a virtual type of money, an online type of cash with a digital form and therefore it is described as a cryptocurrency. It has printed private code inside its environment and the type of network it supports such type of cryptocurrencies is either the peer-to-peer networks or via servers. With Bitcoin one can buy goods and services if

the shop supports this type of payment. It should be mentioned that Bitcoin was a controversial issue for global economies and many countries all over the world since it was tied up in everybody's mind-at least at the beginning of its circulation-with the dark Web and therefore with illegal commercial activities. Nowadays, Bitcoin has inserted the global system of cash transactions. Since a transaction is executed, the currency network records them in a list called a block.

Blockchain is created by having one block linked to another as a chain. The data inside this trading chain is protected from changes due to the structure of the blockchain that forbids any modification or intrusion to it. To seal a transaction so the users can consider the transaction valid inside the blockchain system, the resources of any computer connected to the respective network need to be used. An advanced mathematical process provides the validation to each block by its solution and the reward to the user is units of the corresponding currency. This automated procedure, executed by specialized applications, is called mining. The adaption of the blockchain algorithm is made for avoiding inflation over time.

One could say that any user that left his/her personal computer open, could earn digital coins from mining. However, this approach is no longer sustainable since mining has become a complex procedure and is no longer for a plain user. In the first year of Bitcoin, having just a simple PC to mine thousands of coins in a short time was possible. Today, any user that desire to involve with mining need expensive and special equipment for a few coins.

2.4.2 How it works?

A computer, and everything that resembles to it, can store Bitcoin, which is a computer file, through a 'digital wallet' app. In that way Bitcoin (or part of it) can be exchanged from one user to another. Blockchain is a system that records all the transactions into a public list. At this point it should be underlined that for mining Bitcoins, a computer needs to be able to do difficult sums and provide enough computer power to execute the whole process. Through time, the sums are becoming even more difficult to stop too many coins to be generated and sometimes it takes years of mining of a user to get a single Bitcoin.

Bitcoin is free from centralized control such as government or banks and this can be considered as an advantage of it. These digital coins don't own, they don't make

copies or undo transactions. Also, Bitcoin retains anonymity of the users and the amount of Bitcoin they spend. Although all transactions are recorded, it would be impossible for anyone to know the exact account number of a participant unless the participant reveals it of his/her own. Since the transactions are publicly recorded it's very difficult for Bitcoins to be forged, copied or spent unless the participant in the blockchain of Bitcoin do it by him/herself by losing or deleting his/her wallet. It is essential to mention at this point that users of Bitcoin should be very careful on the Web because there are cases of impostures that let the users stored their Bitcoins to websites remotely and they stole Bitcoins from them.

2.4.3 What is the Ethereum?

Ethereum is a public blockchain and it was built in 2015 by developers that aimed to allow financial applications to be created without the need for a bank or broker. It is an open software platform based on blockchain technology and it gives the ability to developers to build and deploy decentralized applications. Ethereum can act both as a digital currency and as an open source blockchain platform with a programmable trading function and the main difference from Bitcoin is that Ethereum is not just a cryptocurrency but also a ledger technology that companies are using to build new programs. Its network gives the ability to the users to build and run **standalone** applications and to develop different applications from the applications they were developed until the time of its creation. Ethereum is a system that provides various tools and applications to its users such as the development of a new digital payment system, a new electronic currency or developing a marketplace with crypto trading.

The applications on the Ethereum network are called smart contracts and are constructed with the Solidity programming language and every creator inside Ethereum pays in Ether, the network currency, as a fee for the creation of the contract. Ethereum consists of tens of thousands of computers connected to the network so as to stamp transactions and their resources run the applications the users create. It is one of the most powerful digital currency including Bitcoin, based on the total value of its stock. This conclusion comes from the sum of its available currencies at the current value of its unit.

2.4.4 How it works?

Ethereum platform enables many ideas to be implemented such as the creation of an independent, autonomous organization with digital venture capital funds. These kinds of organization support startups financially and actually provide subsidy to new innovative business ideas for gain profit. Christoph Jentzsch a software developer announced in 2016 the creation of DAO [35] and DAO tokens which were created with the help of smart contracts. DAO is the abbreviation of the words “Decentralized Autonomous Organization”. Commercial and non-profit enterprises could have the opportunity of a new decentralized business model for organizing their businesses due to DAO. The latter is an open source software tool, stateless, with an unconventional management structure and it is instantiated on the Ethereum blockchain. Through the process of the Initial Coin Offering (ICO) investors can purchase them. The name ICO is based on the IPO (Initial Public Offering), a process that allows an enterprise to enter the market and offer to the public shares to purchase.

The procedure of raising the capital of an organization can be succeeded through the help of ICO which allows to each member to buy a percentage of the DAO tokens. Moreover, on the final selection of startups, each member has the right to vote the startup enterprises that will be funded. Some of the profits of the startups are returned to the investors with the form of dividends, if, of course the startups succeed. The amount of profit that it will be returned to the investors depends on the percentage of DAO tokens they own.

2.4.5 Ethereum and Smart Contracts

In 1993, the computer scientist and cryptographer Nick Szabo conceived the idea of smart contracts as a vending machine in which one can insert data or value and at the output receives a finite item from a machine. Nowadays, smart contracts are programs that execute exactly as they are set up to by their creators for example, Ethereum users can send 10 ether to a friend on a certain date using a smart contract. According to that, a contract would be created from a participant so as the data is pushed into the contract and execute the desired command by any system which operates with blockchain method. One of them is Ethereum which provides tools for making the usage of blockchain easier to participants.

2.4.6 Decentralized Applications (DApps)

Decentralized applications (DApps) are running on a peer-to-peer network (P2P) whilst a centralized application is running on a computer. Some examples of decentralized applications are widely known such as Tor, BitTorrent, Popcorn Time, BitMessage. At this point it should be mentioned that a decentralized application can run either on a P2P network without necessarily run on a blockchain.

Decentralized applications communicate with the blockchain, since they are a piece of software which manages the state of all network actors and their interface looks alike any website or mobile app today. The core logic of a decentralized application is the core logic of a smart contract. In 2.2.6 paragraph is was mentioned that blockchains use smart contracts as a core part for building their blocks. These contracts receive information from external sensors or events and help the blockchain manage the state of all network actors.

Every decentralized application consists of a frontend and a backend part. The frontend is what the user sees and understands and the backend represents the entire business logic. At the backend many smart contracts interact with the blockchain and in that way the business logic is built and functions.

Traditional Web applications use HTML, CSS, and javascript in the form of a webpage. A centralized database store all the data and the webpage interact with it. The webpage will call an **API** for processing the personal data of the user and other information that is stored on webpage's servers, to display them on the page. To identify and authenticate a user, specific credentials are needed such as user ID and passwords. This data is stored on the server of the service provider and it is important to mention that the security of forgery and corruption of the personal data is low.

There are similarities between a decentralized and a traditional Web application. Technology is exactly the same as far as the frontend is concerned to render a page. Blockchain receives data from a "wallet" which is responsible for the cryptographic keys and the blockchain address. To identify and authenticate a user, decentralized application uses a public-key infrastructure. Smart contract activities are triggered of a wallet software and interacts with a blockchain in contradiction to a traditional web application that uses an API for this cause. Decentralized storage networks such as Swarm or IPFS can host files like a photo, a video, or audio.

Last but not least, a strong difference between decentralized applications and traditional web ones are the Web3 and Web2 respectively (see also chapter 2). As it mentioned above, in decentralized application there is a wallet, an application that manages the connection between the applications of Web3 and the blockchain. It keeps a record of the private keys and blockchain address and manages the users' digital identity. In the backend of the decentralized applications that work on Web3 there is a totally new infrastructure layer to interact with – the decentralized protocol stack.

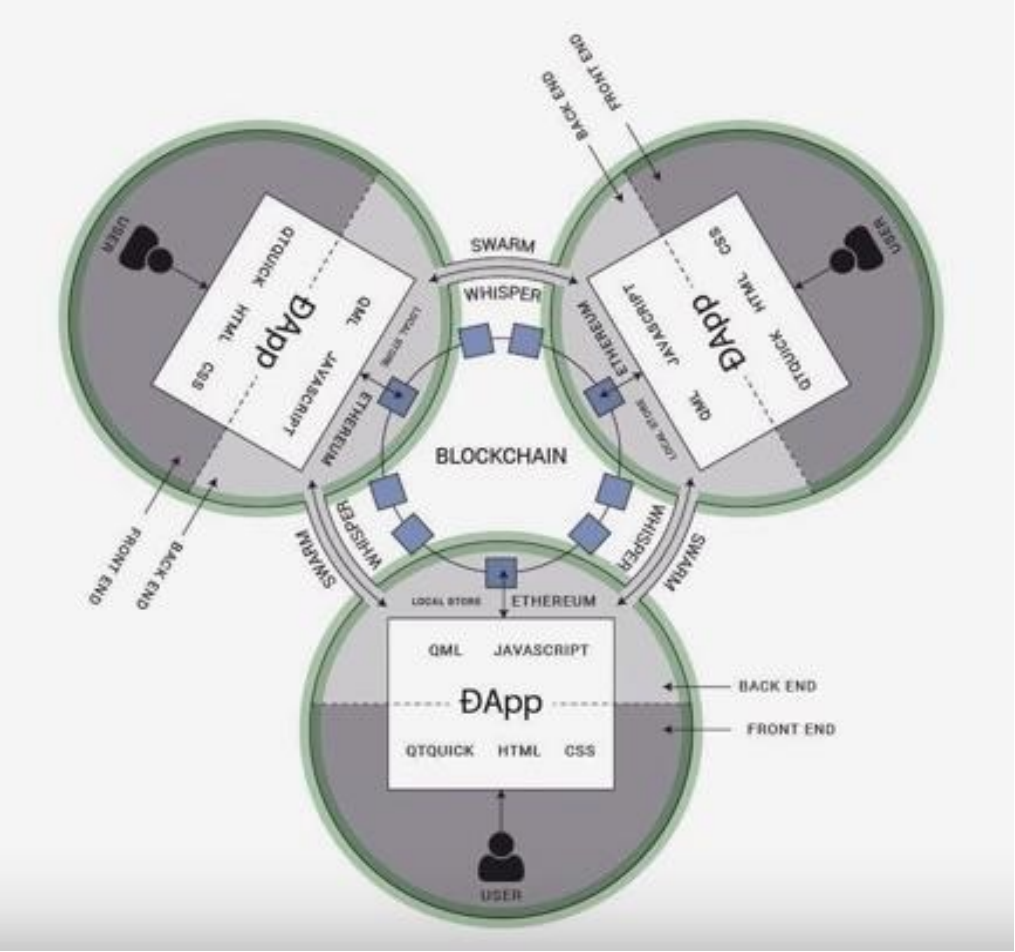


Figure 2.17

2.4.7 Decentralized Autonomous Organizations (DAO)

A collection of implemented Smart Contracts in the blockchain is called a Decentralized Autonomous Organization. Decentralized autonomous organizations use the technology of blockchain so as to track financial interactions across the internet by offering a secure digital ledger, provide a trusted timestamping and dissemination of a distributed database which makes the forgery a difficult issue for hackers. DAO

embraces the no Middlemen approach of blockchain method since it eliminates the intermediary factor and simplifies the financial transactions between the two parties that participate to transactions. It is a smart contract in a more complicated form that gather the regulations and rules of the decentralized organization and locate them embedded in the code of the smart contract. Inside this smart contract token management rules are also collected and specifically defined which are used in transactions. The first DAO is considered to be Bitcoin.

2.4.8 Old and New Ethereum

DAO was attacked online in June 2016, because there have been some security gaps in its smart contracts. The 1/3 of the organization's digital assets were stolen and the hacker gained almost $50 million instantly. Both DAO and Ethereum were severely hit since the technology they both were using was running on DAO's network and many users lost their money that had turned them into DAO tokens. In a few days, the Ethereum unit's exchange rate was dramatically decreased.

In order to recover from the damage, the Ethereum's developers executed an irrational decision and hacked the hacker that kept the electronic money by finding the address where the smart contracts were stored in the form of DAO's contract. Acting like that they managed to recover $ 48M worth of digital assets share them to their owners. The next movement of this team was to do a "reset" of the Ethereum system (called Fork) in order to distribute again the stolen tokens and put to the Ethereum network the blockchain as it was before the attack. It is essential to say at this point that blockchain at its by default architecture forbids any change or modification to occur inside its environment. Therefore, the Ethereum's team needed to have the consent of every member that was involved with the Ethereum Platform and they did. So, a major upgrade of the network security was successfully made and Ethereum was divided into two parts. Ethereum Classic was the first one and just Ethereum was the other. Most of the members were moved to the Ethereum which had the highest value. Ethereum managed to rebuild its reputation easily enough because it wasn't just a digital currency as others. It provided to users the ability to construct decentralized applications on its network.

2.4.9 What is the Hyperledger?

Over 270 well-known technology companies and organizations (e.g. Cisco, IBM, Intel) from the financial industry (e.g. ABN AMRO, J.P. Morgan), from business premises (e.g. SAP), educational organizations (e.g. UCLA Blockchain lab) uses Hyperledger4 (of Linux Foundation). The main idea is for the companies and organizations to use a commonly accepted platform instead of creating individual blockchain solutions. Hyperledger provides many solutions in vertical application fields and smart applications since Hyperledger is an open source software. It is essential that supply chain applications are easily supported by it and in that way a very crucial point for every enterprise such as supply chain is efficiently and safely executed. The information that is recorded inside the blockchain of a Hyperledger is private and is not available publicly. There are channels through which the participants can do the transactions and they also can have access to the transaction data. However, the participants are the only ones that have access to these transactions and data and no one else. The delegation of the decision about the members of a blockchain system based on Hyperledger is given to specific entities. Each participant has a role that defines the participant's access to the data and the rights of verification. The participants (or orderers) that submit the transactions, that verify the transactions and lastly the participants that should agree to record transactions on the blockchain systems. The last participants are called also committers.

2.4.10 Hyperledger Frameworks

Hyperledger provides specific frameworks that include tools and functions which offer abilities to the users. More detailed:

Hyperledger Fabric

The participants in this private blockchain can be connected with the help of a **Membership Service Provider** or MSP. Hyperledger Fabric supports many types of MSPs. There are many ways of storing the data in Fabric using internal configurations and consent mechanisms. Participants are allowed to create channels with a separate trading ledger and only the specific participants can keep copies of that channel. The Hyperledger Fabric contains either world state and transaction log (blockchain).

[4] https://www.hyperledger.org/

The current value of the attribute of an object at the current time as a unique ledger state is the world state and the whole transactions that drove to the current situation is the transaction log. It should be mentioned that chaincode is the tool for writing a smart contract and therefore can be implemented using different programming languages.

Hyperledger Burrow

Hyperledger Burrow executes smart contracts efficiently while it is a fast and lightweight tool in the group of private blockchain that works according to Ethereum.

Hyperledger Composer

Hyperledger Composer provides applications to the participants to make transactions in order to achieve resource allocation. The Hyperledger Composer is designed to allow the direct collaboration between developers and businessmen so that they accomplish the desired business process. The Composer also offers the Hyperledger Composer Playground online service which provide the opportunity to the users to test new ideas and initial design.

Hyperledger Explorer

Hyperledger Explorer provides web interfaces to the users and through these interfaces to reach useful information about the network of blockchain. Hyperledger Explorer also offers information about network, blocks, nodes, transaction details shown through graphs.

2.5 Usages of Blockchain

Considering how innovative and trustworthiness this technology is, there will be a reference to the implementation of this technology to other sectors apart from financial ones, such as biology, music [36] and so many others. Many organizations prefer the structure and architecture of blockchain and integrate it into their systems. Leaders of the market such as IBM, Amazon, Oracle, Alibaba and others offer blockchain as an answer to enterprises problems.

2.5.1 Thesis approach

This thesis will attempt to answer the following questions taking into account all the similar approaches (see Section 0).

To give a comprehensible description of what is the blockchain technology and the novelties it brings in the technology world with both its strengths and weaknesses.
To report the appliances in many aspects of humanity (science, industry, society).
To approach, in a theoretical base, the possible appliances the blockchain technology might have in the heavy sector of Economy, banking.

2.5.2 Fields of Usage

In recent years, Blockchain has entered people's lives and it's here to stay. Since the introduction of Bitcoin cryptocurrency, which was the first implementation of the Blockchain technology (2008), the interest in Blockchain technology has been constantly increasing. Blockchain has started influence many aspects of society such as medicine, music, mobile phones, voting, financial systems and others. It is necessary to remind at this point that Blockchain takes into consideration three crucial for its function elements, the Blockchain ledger [37] , the peer-to-peer network and of course the participants (or clients). These kinds of implementations need to embrace some specific rules and limitations that the method of blockchain relies on to function adequately. Security, privacy, performance, data integrity, scalability and management energy resources are the core attributes of this technology.

Blockchain can be used as a repository of data that has already recorded and cannot be modified and at the same time to give the ability to new information to be appended when it is created. So, this method, especially private blockchain, can be used as a record of objects that should be unique such as patents, fines, businesses licenses and names. Also, as a record of events that register the exact time an event is attached into the system such as tracking of the payments of clients into a banking system or an organization or a municipality. Moreover, as a record of events that register with specific order such as the process of applications from start till the end or as a record of identity for humans, animals and goods.

Furthermore, in banking, blockchain could release time and money to the participants considering that it can eliminate the Middlemen that are involved to many transactions. Needless to mention that for just a simple transaction with a credit card, five middlemen are needed in order to elaborate the transaction.

Real estate is one of the markets that deals with deep issues as far as sale and purchase of premises (and not only) is concerned. Some of these are restricted client

access to real estate offerings, time-consuming procedures to complete transactions, errors in property registration, high transaction fees and fraud cases. Blockchain can offer solutions such as tokenization with the help of cryptocurrencies it is technically able to "break" a property into dividends stored on the blockchain. This gives the opportunity to the owners to sell only part of their property. The range of potential buyers is increasing and investors with smaller funds can invest in high value equity holdings. An example is the case of Templus Markets[5] in which investors were able to invest in the St. Regis26 in Aspen starting with a price of $ 10,000 while the total value of the hotel was estimated at $ 18,000,000.

Also, millions of people every day have no IDs (eg refugees) or have forged their identity documents and governments all over the world have to keep records of people's identity and property ownership or even a single data of them. The validity of the data should be protected even though many cases of infringement of personal data have been recorded frequently.

Blockchain can be the solution to the previous problem by issuing for example digital birth certificates that cannot be forged and accessible by anyone with the required access rating. This kind of solution produces benefits by reducing costs and time for the verification of the individuals' properties and identities and combating the phenomenon of human trafficking. Dubai, for example, aims to put all of its government documents on the blockchain by 2020. Stampd.io[6], the first Greek blockchain application, creates a cryptographic fingerprint of a document on the blockchain so that no one can forge any of the documents stored in the system (blockchain notarization).

Businesses are the most vulnerable industry of all as far as digital privacy violations are concerned. It is impossible for most of the companies to prevent hacking, fraud and corruption of their data 100% while as it is widely known every information system has its flaws. Blockchain can contain digital certificates issued by trusted and well-known consumer bodies (eg banks, telecommunications organizations, government agencies, etc.). These certificates can be used with the clear consent of the customer. In this way there will be a system with faster and more secure transactions.

[5] https://templuminc.com
[6] https://stampd.io

Many types of insurance exist such as car insurance, life insurance, health insurance and more. In healthcare it is tremendous important for the patients' medical records and financial data to be secure and safe within the health system of a medical center of a hospital. Until now, these kinds of data are stored and maintained in a central database (or on a cloud) and the access for these databases are given only to staff of the medical unit. These medical records can only be accessed by the staff of the medical unit where the data was selected and stored. The security of this data is in jeopardy, especially in security attacks. The blockchain can solve security issues by providing information at various levels of detail. Maintaining this information will make easier and quicker the process of payment to the patients by the insurance agencies while a detailed patient history will be accessible to the authorized medical practitioner or insurance agent.

In the insurance industry the security issues are the same as in healthcare. Blockchain enables the agencies to free themselves from the problem of security, forgery and hacking and at the same time offering easy solutions such as smart contracts blockchain reduces either the cost or the time of a traditional transaction. Smart contracts replace paper contracts with fully electronic contracts. This means less cost and less time and it is easier to verify any transaction that is running with third parties. In this way, insurance agencies have the opportunity to withdraw claims from insurers that have occurred in previous time and to deal with fraud more effectively. Blockchain has the ability to store huge amounts of data directly or through reports in which anyone can access to. Synaphea[7], is the first Greek blockchain application, is building smart contracts for the insurance market.

The pharmaceutical companies deal with a serious issue in the circulation of copies of drugs that produced and disposed of in uncontrolled ways, putting into danger the public health. The blockchain keeps the complete history of each drug package from its production to its final retail sale and in that way, it provides safety and authenticity of the procedure and of the drug.

Blockchain can improve the industry of education since in blockchain all information about students and everything that concern them, for their studies, can be retained. High level of safety is the key to the protection of the personal data of the students that this technology offers and at the same time the information assurance that

[7] https://synaphea.com

can be given to the employers about the fulfillment or not of the studies of a potential employee – ex-student.

2.5.3 Current approaches in the banking field

Finance Industry and specifically banking sector have been opposed to blockchain technology since the blockchain technology acts as a direct competition against the architecture of the banking structure which holds the control over the funds and accounts of their customers.

Among the most pioneering banks of this type are several banks from China[8] which through use cases have begun to apply this technology to their internal operations. These banks vary from state owned ones like the Bank of China, China Construction Bank and the Agriculture Bank of China, to privately owned ones, including China Merchants bank.

China Construction Bank in its financial statement it was mentioned that the Bank embraced a blockchain based platform which was running cross-bank and cross-border loan issuances for small businesses. Also, through an automatic process into a decentralized network that inherited, the Agriculture Bank of China offers unsecured loans for agricultural e-commerce merchants. Moreover, the Bank of China provides a blockchain-based digital wallet.

Furthermore, many banks at other big countries have started a collaboration with specific American companies based on blockchain applications. Some of these banks are IndiaALFA Bank from Russia, Yes Bank from India, UOB (United Overseas Bank) from Singapore, CommonWealth Bank from Australia and LatiPay from New Zealand. Kotak Bank in India has cooperated with Deloitte & JP Morgan Singapore and uses blockchain technology for financial operations.

Smart contracts provide many benefits to the process of transactions while they eliminate the need of the intermediaries and have the potentials to offer loyalty and rewards systems. In the financial sector there are many other use cases such as quicker payments as far as cross border is concerned, efficiency of trade accuracy, less steps of settlement processes and many others.

Verification and safety of the customers' data are crucial issues for banks either for their reputation or their integrity. It is vital for every bank to know for sure the identity

[8]https://medium.com/predict/comprehensive-list-of-banks-using-blockchain-technology-dc39ce5b6573

of every customer, user of its physical or digital system and anyone that deals with the bank that is a trustworthy member of its system. Recently, banks make a serious attempt to record and update users' identities through a shared digital system. Blockchain for banking is considered to be the solution for protecting and sharing updated record with counterparties in a tremendously short time with the help of its cryptographic mechanisms. The 'know-your-customer' (KYC) [38] and anti-money laundering algorithms could help the enormous amount of data to be moved through the banking network and system.

New payments infrastructures are being experimented by many central banks across the world. Blockchains can "accommodate" parts of such payments. Furthermore, commercial banks construct their own projects such as the Union Bank of Switzerland which has developed their "utility settlement coin". This coin was constructed in order to create their own cryptocurrency. So, having a new coin, tokens can be issued and convert into cash at banks and therefore the new coin can be used into the financial markets.

Swift is the system that enables cross-border payments to be executed and accomplished by any bank all over the world. This system makes serious attempts to experiment the Blockchain technology so as to simplify and facilitate the trillions of dollars transfers that services.

At this point it should be mentioned that if banks inherit parts of blockchain technology they will become able to change the infrastructure of clearing and settlement operations. The handling cost of information that all banks have to deal with is counted to billions. Studies have shown that $10 billion[9] could be saved from banks if they have implemented blockchain or some tools of the blockchain frame.

According to the previous ones, anyone can understand that if the blockchain technology and its tools become understandable from the banking world, the whole scenery of how things are taken place in this system will change.

Until now, most of the attempts as far as blockchain and banking are concerned, have been committed by foreign banks. In Greece these sorts of experiments were quite difficult to take place in, considering both the economic crisis Greece has gone through

[9] https://www.accenture.com/t20170120T074124Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf#zoom=50

for about a decade now and the conservative way in which new achievements are handled especially in environments that are still not very familiar with digital world.

It would be interesting if banks of Greece would participate to studies and attempts in adopting or embracing new technologies and tools such as blockchain offers. Therefore, it would be interesting to study the response such applications might have to the Greek public. In a country where people try to keep up with novelties as much as their background can offer them, even though there is a high percentage of older people living in Greece, penetrating to even more sophisticated applications where data is shared between banks and processes run without human intervention it is certainly a challenge. Needless to say, that a country like Greece, with a developed tourism industry and its shipping industry offering a significant share of **GDP**, could certainly benefit from applications, for example, that would be able to transfer money to and from abroad in much shorter time. from today's and at little or no cost.

Below there are some of the most-known crucial points of the banking system that Blockchain technology can contribute to improve and solve.

Internal banking problems	In terms of bank-client relationships
Process automation	Digitalization instead of Papers
Digitalization and Decentralization of banking information	Total operational simplification
Intra-bank settlements	Faster transaction handling
Product data structure	Customer data management
Reconciliation & Synchronization	Fraud reduction
Safer data storing	KYC and customer due diligence regulations
Auditing	Smart Contracts
Internal transaction messaging	

3. Problem Definition/Materials & Methods

3.1 General Scope

The general scope of this thesis is to study how blockchain can be implemented into the banking sector and the possible benefits of this theoretical implementation.

To accomplish this, there shall be an extensive study of the characteristics of blockchain and the uses of it into other aspects of life and also the current system banks use for many tasks inside and outside of their environment.

3.2 General Goals

Actually, this thesis intends to provide specific answers to the questions that presented in Section 0.Therefore, the general goals that it will try to succeed are:

1. To give a detailed but as plain as possible description of what is the blockchain technology;
2. To report the appliances in many aspects of humanity;
3. To approach, in a theoretical base, the possible appliances the blockchain technology might have in the banking sector;

3.3 “Implementing blockchain into banks”. Is it possible?

3.3.1 Scope

Nowadays, optimized services can be easily offered by financial sector, especially banks thanks to technology whose range is wide and helps to develop such services. The technology of blockchain has supporters and objectors, since the creation of the first cryptocurrency, Bitcoin. Scientists, economists, politicians and simple people believe that this technology will have a high impact in almost every aspect of life, similar to the Internet. It should be mentioned once again that blockchain uses new tools and parts of the existing technologies, with a unique combination that makes this technology worth studying. Data are stored without the need of a central authority and this characteristic

makes this sort of system invulnerable to malicious actions. Still, the core issue in the near future is the beneficial and intelligent use of existing infrastructure in many businesses by new technology and its innovations without wasting the resources of these commercial enterprises but by becoming a clever combination of existing and new technology to achieve business goals. The most important need blockchain can cover is security of the transactions. The peer-to-peer network and its tools is inviolable, since it operates despite the fact that a node or many nodes attached to the specific system might be shut down for any reason.

There are a lot to be done in the banking sector when the decision of adopting this new technology will be made from a group of banks. One can easily understand that blockchain encloses some contradictions compared with the current architecture of the banking system. Blockchain weaknesses were highlighted through the years by the use of the cryptocurrencies that have been on the market and some of them were mentioned in the 2.3.4 Section of this dissertation. If an implementation on banking services is decided, a detailed study needs to be preceded.

This dissertation will attempt to propose possible applications of blockchain technology in the banking sector and at the same time it will try to refer some possible problems and constraints this technology carries in it when centralized environments are involved.

3.3.2 Threats

Some years ago, serious problems were recorded for blockchain technology. These problems arise a very important issue, if this technology can be used for applications of this size. In 2015, a serious statement had been issued by Interpol[10] for the cryptocurrencies and how digital coins can operate. The mechanism of cryptocurrencies can be used to access information and applications that can infect the network terminals - nodes. Illegal material could be stored on a Blockchain network for example malware underneath “innocent” applications or child pornography. These kinds of data such as pornography can’t be removed from the network that blockchain is being using because of the structure of the network, since it would cause critical issues in the whole chain.

[10] https://www.refinitiv.com/content/dam/marketing/en_us/documents/expert-talks/world-check-expert-talk-fighting-financial-crime.pdf

A hash function generates a unique number for every new block that is added to the network. This unique number is the result of the data contained in the Block and the hash of the previous node. If in this specific function new data is added which is different, then the new number that is produced as a result, is quite different. The data of any block can't be changed because according to the principles of blockchain all the previous blocks should also change and of course this is practically impossible. This principle is one of the key foundations of the architectural design of blockchain method for providing security to the users of its network. Therefore, any incorrect or malicious information is stored in the chain of blockchain, it is practically impossible to correct it. This problem can be addressed first by checking the information that comes through the network that it meets the network criteria. If not, the information is rejected and it is discarded from the network. For example, the information stored in the chain when Bitcoin transactions are executed should be strictly financial in order to avoid double spending. Any information that isn't of practical use for the peer-to-peer network shouldn't be accepted. So, for the data of the transactions that meets the network criteria are stored in records with a specific structure.

3.3.3 Problems

In 2.3.4 Section it was mentioned that Blockchain has some disadvantages. The size of the chains in this method is a crucial issue, since every day new transactions happen. The chains are consisted of blocks where inside them data are recorded and stored which are gathered from the transactions that have been executed. To do this kind of recording and storing, blockchain needs resources such as computer power, space for the storing and so on. So, it is easy for everyone to understand that the main disadvantages of Blockchain are mainly focused into one issue, the storing of the data.

Blockchain technology provide tamper evidence, decentralization and transparency to everyone that uses it. Banks are the prime example of centralization authority in all their activities. So, at a glance, blockchain and banks are opposite one to the other. However, this is not correct. Banks need tamper evidence and transparency at all kind of their transactions and blockchain can offer both of these characteristics. As for the decentralization characteristic of the system of blockchain, it is already mentioned (2.3.2 Section) that there are also private blockchain systems with most famous ones,

Facebook and Google. So, if banks decide to use blockchain into their systems, the only question that arises is in what way will they store the data of the transactions.

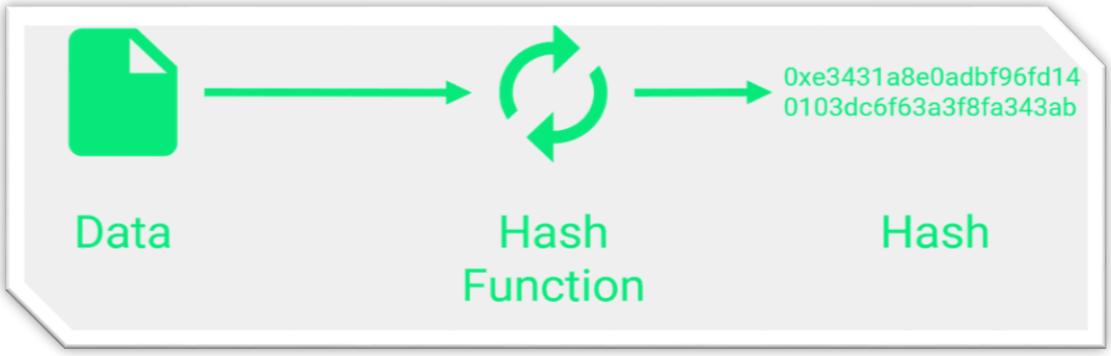
A transaction model is used to store data in a blockchain. If, for example, A sends money to B, this transaction holds the addresses of the sender and the receiver, A and B, respectively and the amount of money that is transferred. When it comes to money-transactions this approach seems very intuitive. However, to store custom data on the blockchain, data needs to be packaged into transactions so as blockchain can store it. Protocols of some blockchain may give the possibility of appending data to a transaction. So, in this case it is easy to append data to the transactions. This feature, in some blockchains, does not exist, so a tiny amount of data can be stored on the chain by using addresses. The data is saved and stored in the blockchain by encoding it and use it as an address to send a transaction to. So, the data is encoded into the receiving address.

Yet, there is a strong disadvantage in the latter storing technique, since the amount of data cannot be larger than the blockchains address size, which is extremely small. Also, a transaction fee should be paid because the address that the transaction is sent to, does not belong to the system, so the money that is transferred is lost. At this point, it is clear that there is a limit to the amount of data one can store in the blockchain by its protocol (some kilobytes). Moreover, it is difficult to store data into the blockchain because of the enormous transaction fees one should have to pay because the data for storing need to be stored to every single node of the system and this raises the cost. One could say that data can be split up into small chunks and store them but this solution would also increase the costs because the cost of a transaction would be paid multiple times!!

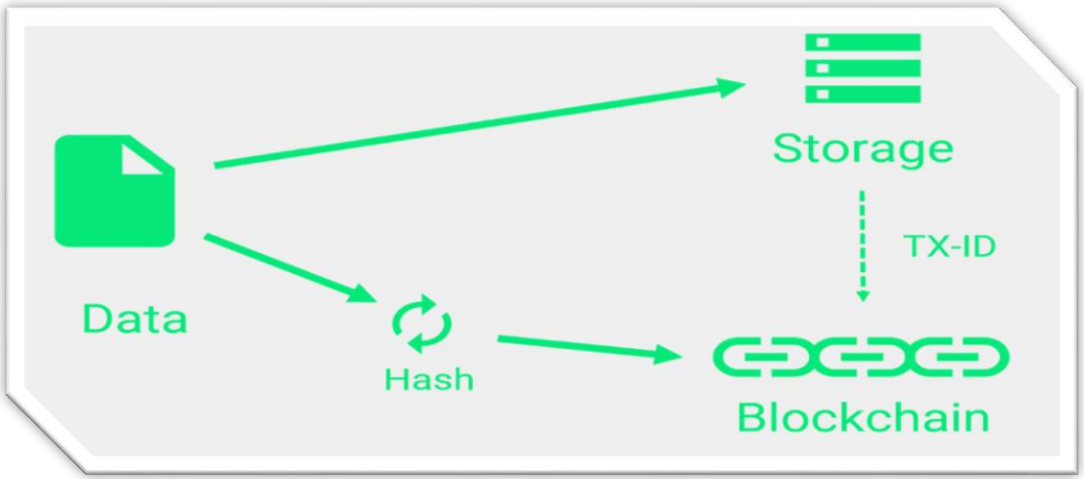
Last but not least, is the problem of saving and managing confidential data, either it is personal or not especially, into a banking system, saving and deleting confidential information is a major issue, considering also the new GDPR. Deleting data into a blockchain is impossible by design.

If there is a public blockchain, the stored data is available to everyone that participates to the system. If there is a private blockchain, every participant also gets a copy of the stored data with the difference that in the private blockchain system there is an authority that controls the participants of the specific network. The latter model can be adopted from the banking system.

The encryption of the data can be a solution to the storing data problem. The issue that arises with this solution is that the encryption keys need to be stored also and should be distributed. Another solution could be to hash the data with a hash function and store the hashes than the data in its primary form. It is important to restate that a hash is a generated string, that is computed using the raw data which is inserted. The output hash will never change as long as the input is the same. Another hash is generated by a changed or another input. So, with the help of hashing it is easy to tell if data was modified or not. Banks use already many of these mechanisms for their data.

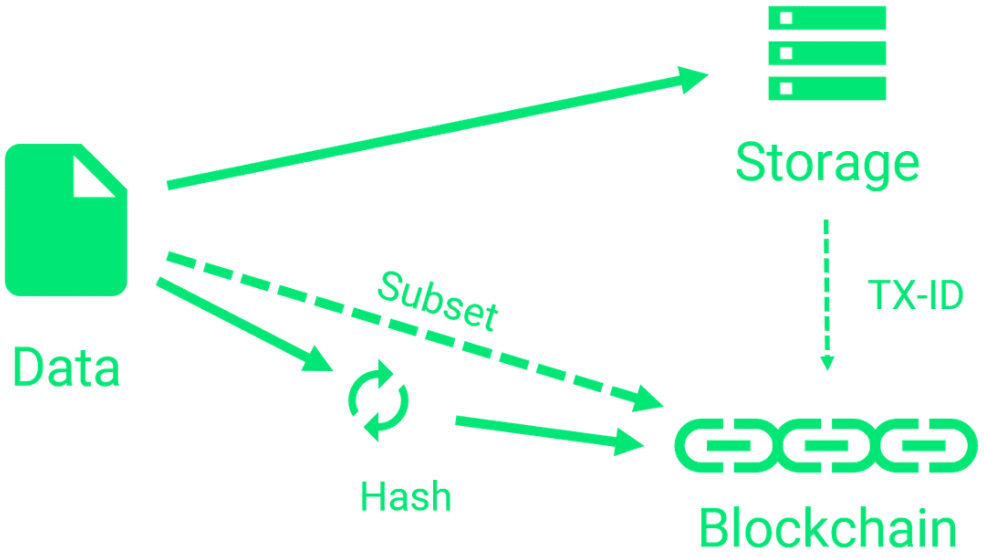


According to the previous ones, on a blockchain is stored the hash of the data that was assigned to the raw data. Hash is extremely small comparing to the data itself so the cost of a transaction is also low. Using this traditional way of storing, the primary data can be stored by using a file system or a relational database [38] in which an added column would store the transaction id.



Furthermore, using traditional storage mechanisms (like queries) the tamper-evidence of the blockchain is gained for a centralized system. The integrity of the data

can be checked any time by hashing the primary data and comparing it to the hash that is in the assigned transaction in the blockchain. The benefits of decentralization and transparency can be gained to a certain level by storing the hash of the data and parts of the data on the blockchain.



It is possible that some transparency of the data can be obtained because now the data is publicly accessible since part of the data is stored decentralized and not in a central database. Using some sort of off-chain mechanism to store large amounts of data, such as a traditional database like MongoDB, helps the whole system and the participants to save resources and money respectively. The data is replicated to many nodes, located in many places, in a distributed database. This can reduce latency for world-scale applications and can offer a redundancy in case of failure of a single machine for example MongoDB with replica-sets enabled or cloud-solutions like Azure CosmosDB. Finally, a distributed filesystem stores its files into many machines, such as distributed databases do for creating redundancy to a failure possibility. However, a file system doesn't obtain the strong query capabilities and therefore it can only be accessed by knowing the name/path of the file.

Consultation and modeling are two crucial points for banks to overcome in order to use effectively blockchain networks inside their system. If every bank develops its own applications without considering the banking environment, these applications will be incapable of bringing the goal they were constructed for because it could be impossible to cooperate with the applications of the other banking institutions. It is totally

comprehensible that such applications and networks are extremely useful, yet bank applications are obliged to work together for a common goal; maximize the efficiency and maintain trustworthiness of the processes of the transactions. To succeed the latter, it is essential to create working groups so as to produce models. Taking into account the technological constraints and the needs of institutions, these standards should cover the needs of banks as far as security, validity, immediacy and other basic principles are concerned. So, at this point the banks need to develop their own information systems, since the standards that are fundamental to be set to be applied will have been reached and, in that way, the interconnection will be ensured.

Last but not least, a serious issue as far as the implementation of blockchain technology in the banking sector is concerned is the fact that the legal framework of this technology is still vague. Although, the existence of Bitcoin is counting over a decade now, yet the legislation for this technology and its tools hasn't been fulfilled in an adequate degree and therefore crucial sectors such as banking hesitates to adopt and implement inside its delicate system.

3.3.4 Constraints

As it mentioned in 2.3.1 section, a new block can be added in the blockchain order when the 51% of the nodes involved should approve the block. Since the approval is given from the majority, the block is logged and the registration is getting through all nodes. So, data that aren't corresponding to real transactions and try to intrude the network without the approval of the nodes will be rejected by the nodes. For fake data and illegal attempts, the technology of blockchain have the mechanisms to ensure the proper operation of the network. In theory, the latter is correct and it works.

At this point it should be mentioned that there were network instances where the rule that blockchain has the tools to avoid fake data and intrusions was violated and virtually those networks could not function properly, since those who controlled the majority of the nodes could prevent real transactions from passing through the network or even executing double spending. A representative example is in August 2016 for Blockchain Krypton and Shift [39].

So, one can easily understand some weaknesses blockchain networks hide inside them. Yet, inside a banking environment these weaknesses can be tested. Banking networks are private, pose limitations and of course control the users that have access to

the network. On the contrary, anyone can participate from anywhere into the cryptocurrency networks.

It is obvious that the banking network is more manageable, and therefore more secure. Yet, banks store all their data to some of their servers using computer networks. This means that if one of the servers is shut down for example due to a technical problem or a hacker attack the entire network will be rendered unable to provide any service. It is considered as a Single Point of Failure. Banks know this situation and take measures to ensure that this never happens. This is not a problem in a blockchain network where all nodes maintain a copy of the data, so even if only a node remains operational, it will be able to provide services and this is one of the core features of a blockchain network. So, no matter what damage it might happen to the network infrastructure, the part that will remain untouched will be able to function. That's why blockchain networks are not an easy target for hackers.

A centralized infrastructure is much easier to troubleshoot than a non-host-based network. However, a centralized system is an easier target to destroy or hack that a public network. In a blockchain network, one should hit the network nodes, which are of course many in number and need a large amount of computing power.

Transactions, especially in the financial sector should be assured that they are not altered and that data is transferred safely and integrity. A private blockchain network with controlled access to its terminals will be much safer than today's banking networks, since only bank employees will be able to use them.

3.3.5 Goals

Transactions made in banking sector need to be executed in a safe environment and this is a core characteristic that financial services through banks promise and provide to their customers and users. Also, for those with a financial surplus, banks offer safety for their savings and provide trust. It is out of the question for every human being on the planet to save money in a bank that doesn't provide safety and trustworthiness. This is the reason why banks implement the stringent security requirements and invest on the most modern systems, firewalls, software and hardware. Trying to have a competitive edge, especially in the IT framework, banks invest much money. Since there have been many cases of fraud and hacking in banking network, banks' information systems are always covered by a disaster plan. Resources are used much more than is needed. Due

to the latter if one part of the system is shut down, the rest will be able to work properly and offer the same services the banking system supposed to offer. Banks may succeed to expand their customer base with the help of developing systems which have the ability to process data faster and provide quality and secure services. Many people think that blockchain can insert innovative suggestions and tools and change the banking scenery of the financial services. However, blockchain technology needs to ensure that it meets all the requirements that provide security, confidentiality and integrity which are binding on the financial industry, especially banking.

4. Contribution / Experiments

4.1 Attempts and Thoughts

For years, banking sector has a very strong placement into the financial environment. So, the entrance of Bitcoin felt indifferent to them since they knew that their position and role into the market was firmly established and nothing could be seen as a threat against them. After all, for so many decades, banks were the institutes that served the financial needs of the whole planet and nothing seemed capable of change this fact. At the beginning, banks viewed Bitcoin as the "hobby" of some who interfered with technology and invented new applications that had no real-life impact.

However, situation changed. Through the years, people trusted this particular currency and money in this form could transfer abroad. Beside Bitcoin, other electronic currencies began to emerge, claiming a part in the market and improving some of Bitcoin's original pathogens. Banks started to realize that the technology of these cryptocurrencies could produce results while people would start using it and for some of their services this technology offered some tools that banks could use for these services without their interference. People that were using this technology enjoyed the speed and the efficiency it offered encountering no geographical restrictions and fees and that was something that banking sector perceived quickly. Therefore, in Greece, there are many ATMs11 that serve cryptocurrencies to the clients, where one can buy or sell cryptocurrencies. Banks nowadays, show interest in Blockchain method and study this technology, while they trying to integrate this technology into their own activities, improving the services provided.

It should be noted that facebook, considering the large customer base that maintains with huge amount of users worldwide, tries to open its facilities by offering payment services to people that either aren’t able to use the conventional banking system or to people they wish to use an alternative way of payment, different that banking one. The enterprise will also launch the electronic currency with the name “Libra” which will be available in 2020 and will support blockchain operations. So, Facebook does a breakthrough to the financial environment by providing services that until now were

[11] https://www.startup.gr/epikairotita/politiki-amp-amp-oikonomia/edo-tha-vreis-ta-simeia-stin-ellada-poy-yparchoyn-atm-gia-to-nomisma-bitcoin/

treated by the banks with extremely simplified procedures. At this point, it should be mentioned that this project is also supported by companies such as VISA, Mastercard, Uber, Vodafone, Ebay, Spotify and others that are targeted.

Furthermore, Apple also launches Apple card, which is a digital credit card, Google provides a payment way with Google pay while Amazon offers short term loans to sellers to renew their stock by using Amazon's platform. Banks should consider deeper the evolution of applications based on blockchain technology inside banking system, since the European Union assigned secured authorization towards Google, Apple and Amazon so as to conduct electronic transactions. In this field, Chinese colossus have done serious attempts and, in many cases, very successful ones such as Alibaba which has even set up the online bank Mybank12 for Europe.

According to a new study that Juniper Research13Ltd company carried out, significant cost reductions can be accomplished if banking institutions can integrate blockchain and its applications into their operating process. Blockchain deployments will be able to offer to the banks a cost savings over than $ 27 billion a year by the end of 2030 (reducing cross-border transaction costs and compliance costs.).

On the other hand, the research makes clear that the steps of the integration of blockchain into banks will not be straightforward. Also, the benefits of the implementation will be reflected indirectly in the operations of banking system, through time and not in short term.

4.1.1 Ideas and Proposals

Banks try to take advantage of the technologies they are at the disposal of enterprises such as high-speed networks, wired and wireless. Through technology, banks compete one another to novelties providing advanced services to their customers and at the same time expanding their customer base. This attitude is very common to such environments, and beside this philosophy, banks could adopt blockchain to store their data either in a common blockchain network or in their own environment. Inevitably, the implementation of a quite new technology such as blockchain in new and controversial aspects arises legal issues and creates ambiguities and questions that need to be answered.

[12] https://www.mybank.eu/mybank/what-is-mybank/

[13] https://www.juniperresearch.com/press/press-releases/blockchain-deployments-save-banks-27bn-by-2030

Nevertheless, both for the customers and the staff of the banks, the experience of using blockchain inside the banking system can become effective with the prerequisite of a stable and defined legal framework. In that way, data will be available and updated to all the banks involved in the specific system thus, there won't be necessary to save the same documents and data for opening a new bank account! So, the bureaucracy will be shortened and the customers will be less annoyed since for a transaction or a specific task they would have to bring their credentials and related documents only once. The system of common blockchain will take over to inform all the nodes-banks for everything. If a private blockchain network is adopted, it will provide the required security, accessible by banking institutions and then the large amount of work that banks have to deal with, will be reduced and therefore the cost of operations will be reduced and finally the banks will succeed to offer more competitive services.

New opportunities are offered through a blockchain network in which all banking groups can participate, especially when the customer data is digitized and therefore operations can be automated and, in that way, to reduce the resources they are needed. Automation of operations and smart contracts (Section 2.2.6), could succeed to push up the financial services such as customer evaluation and risk assessment. As long as the data is stored into the blockchain network, there could also be free knowledge about the "quality" of each client and his/her financial history if any old contracts were signed. Smart contracts could also provide similar data.

Moreover, a specific "e-bill" can set the frame of this information and give rate for each customer. This rate can show a tendency of the risk that each bank can take (or not) over if this customer provides any form of financing. At this point it should be mentioned that the latter process is completely automated. Of course, this process can evaluate only the new customers and not the old ones. In this procedure, only the weigh factor that is given to each offense is set manually and not automatically as the rest steps of the process and is the only factor that can be reassessed. Until now, banks have a common system named "Teiresias" which is constructed for a similar use. Teiresias is an organization that requires from the banks to update their data constantly so as to provide efficient and safe information to all banks.

Furthermore, these kinds of implementations are nowadays feasible in the banking sector and can provide many benefits toward their participants, banks and customers. If

a customer has a high solvency from previous activities, it would be easy to have access to financing through simple procedures. This also applies to companies that they are consistent with their obligations against the banking institutes. Banks need these kinds of customers, since they manage to avoid high risks and at the same time increase their profits.

Transferring funds from one country to another is quite easy today with the banking sector doing a great job in that aspect. Banks are the intermediates between a sender and a recipient. Sometimes, it needs more than one banks to play the role of the Middleman for a money transaction to be completed. It is obvious that the more banks are involved the more time is needed to complete the money transaction. Also, the opening days and hours of banking institutions in several countries differ. Therefore, the required procedures should be done at the same time but this is impossible for the banking world to accomplish.

For facing these kinds of problems there are various networks that offer services of money transfer which operate decades now, for example Western Union and MoneyGram. These are global networks that can transfer money very fast but there is a high transfer cost when using these networks. On the contrary, cryptocurrencies can execute such transactions very easy, fast and with a low cost (in some cases there is zero cost on the transaction). So, banking institutions could adopt the way cryptocurrencies execute money transactions and provide these kinds of services fast and cheap.

Processing time can be shortened and banks can benefit from this. Santander[14] , a Spanish bank, used blockchain technology in 2018 for sending money in various currencies in many countries (England, Spain, Poland and Brazil). The system was developed by Ripple[15] Labs. Exploiting blockchain technology, Santander and Ripple experiment with the platform Santander uses which allows partner institutions to process money transfers extremely fast, even for other currencies. JP Morgan Investment Bank announced in 2018, that targets to launch a blockchain-based payment system across a 75 banks network. Therefore, through blockchain applications money transferring can be executed with high speed and low cost and more and more banks adopt similar practices.

[14] https://www.santanderbank.com
[15] https://www.ripple.com/y

Last but not least, crowdfunding is a service that usually is offered by websites through internet into individuals or startup companies and help them financially, with no interference of the banks, to start their enterprise. Such websites are Kickstarter, Indiegogo, Rockethub, Gofundme and many others give the opportunity to people with new, fresh ideas to get the funds they need to turn their idea into a product for the market. The procedure provides the usage of exchange information from the prospective entrepreneurs demonstrating their idea in a concrete way to the stakeholders who may find the idea interesting and lend money to startupers converting the idea into a product, expecting future business profits.

With blockchain, crowdfunding is feasible for the banks to deliver. Until now, investment packages such as real estate, a set of bonds and others are provided by banks to interested parties. Startups could be promoted in the same way as investment products. Banks are able to operate the way crowdfunding websites work because they already have the structure in their systems. There are enterprises that succeeded funding by issuing their own digital currency by selling this currency to stakeholders. Paying digitally enlarges immediately the target group of such an endeavor since anyone from all over the world can take part in this procedure.

The verification of the previous theoretical approach is an OpenLedger project that facilitates such processes. Open Ledger provides an “initial coin” to startups to select and to investors the ability to purchase this “initial coin” by paying through Open Ledger in electronic currencies. Since there is no bureaucracy, the procedure is simpler than the traditional one through banks. It is undeniable that startups move the whole procedure, trying to persuade the stakeholders that their idea is viable and it worth investing on it.

At this point a serious issue arises, since investors must be sure that their money are placed for the purposes of the enterprise and there is no fraud. The solution is given by implementing a smart contract that will be created from the outset which will have the rule to release part of the funding from investors whenever a set of contracts is fulfilled. If the latter is disobeyed, the next tranche of funding will be invalidated automatically by the smart contract.

All of the above, regarding crowdfunding, works for companies outside the banking system meaning in a decentralized way. However, sites as Kickstarter, Indiegogo,

Rockethub, Gofundme etc earn money by charging their clients with a percentage of the funding collected in each campaign and this is their profit. So, despite using blockchain technology, they act pretty much as banks do. Therefore, if blockchain technology is adopted by banks, similar services could be offered, complementing the ones already are in use, thus having a wider variety that could meet any financial need.

4.1.2 Legal Framework

The blockchain is a technology that exists almost a decade now and it was used mostly in cryptocurrencies at first since it was widely known from the bitcoin application. Nowadays, serious attempts have been taken place, as far as blockchain method is concerned, in almost every aspect of life such as trade, finance, science, agriculture, medicine, health, banking and others. At this point a great issue raises, the legal framework in which blockchain should be developed.

Moreover, blockchain inserted a new approach of managing transactions and data. The registration and storing of the data should be seen from the point of the law for the personal data protection (GDPR) [40]. This means that specific information such as the personal identity of the processor of a transaction inside the blockchain system or the identity of the miner of a node is difficult to be answered especially when public blockchain is concerned. Needless to say, that the right of the deletion or update of data is also a crucial issue to denote in this technology that keeps a copy of all data decentralized, in every node of its network at the same time and in a way that no one can corrupt or modify the data inside the system.

Also, cryptocurrencies is an important element of the blockchain technology and their legal characterization becomes a prerequisite for their legal treatment and their embracement into the set of regulations according to the law. It should be mentioned that cryptocurrencies are coins but not in the traditional way, so they need special legal approach. Every open blockchain protocol provides for the creation of tokens that are required to participate in this platform. So, participants in a transaction should provide their tokens of the blockchain protocol so as to execute or conclude a smart contract. Furthermore, how the protocol works, the technical characteristics of it and how quickly and in how many users inside the community this protocol arrives determine its value.

The Court of Justice of the European Union in October 2015 in the context of the interpretation of VAT Directive 2006/112 / EC considered that bitcoin could not be

classified as a tangible good within the meaning of Article 14 of the VAT Directive and it was considered strictly as a payment means and was exempt from VAT. The European Central Bank (ECB) categorizes bitcoin as a "convertible decentralized virtual currency" and therefore the European Union plans to regulate, at least in part, the disposal of virtual currencies in the context of the revision of the 4th Directive (EU) 2015/849 on legalization.

The relationship between blockchain and the General Data Protection Regulation (GDPR) is always a strong point of debate among scientists, economists and politicians. Two are the main factors of this debate. First, the data controller is the key word for processing personal data based on the GDPR framework. A natural or legal person (i.e. the data controller) is in every step of the procedure of personal data and checks if the GDPR regulation is applied correctly and securely. Secondly, modification or deletion of the data in a GDPR framework is acceptable since it is required and certainly in compliance with legal requirements.

On the other hand, in a distributed database such as in blockchain's it is highly important according to the principles of trust and security in a system like blockchain the delegation of responsibility for data processing since this technology does not modify data unilaterally so as to establish the integrity of the system and build relationships of trust into the network. From the above, it becomes clear that blockchain technology is in conflict with GDPR provisions and key recommendations are definitely required for their resolution.

4.1.3 Tools[16]

1. **Geth** is the command line interface into the Go programming language that runs a full Ethereum node. It can be installed on any operating system and it offers mining and transfer of tokens between addresses and create smart contracts and through Ethereum Virtual Machine all the previous are executed
2. **Mist**. Before start using Ethereum Mist was the tool that stored the Ether tokens and execute the smart contracts and now is the official wallet of Ethereum. Linux, Mac, and Windows support Mist tool.
3. **Solc** is a tool that enables Solidity script to be converted to a format readable by the Ethereum Virtual Machine. Solidity as a programming language has many

[16] https://blockgeeks.com/guides/15-best-tools-blockchain-development/

similarities to JavaScript and its use is for creating smart contracts on the Ethereum blockchain.

4. Small contracts use **Remix** as a compiler.
5. **Blockchain Testnet** is used for simulating mining and to confirm transactions on projects that are characterized as "sensitive" to attacks, hacking and other similar risks. There are three kinds of testnets: Public Test - Private Test – Ganache CLI (or Testrpc).
6. **Coinbase** is a San Francisco-based "fiat-to-crypto" exchange. It gives the ability to collect read-only data and build something really new. Moreover, Coinbase's APIs offers an environment to create bitcoin wallets and addresses. Also, this API provides the system for buying, selling, sending and receiving bitcoins worldwide while offering libraries for clients and mobile SDKs, especially for developers. With Coinbase businesses can intergrade cryptocurrencies into their environments according to REST API it uses.
7. **EtherScripter** provides an interface that can be used to start coding basic contracts. With a simple drag and drop wherein one must connect jigsaw puzzle pieces to make his/hers contract come to life.
8. **BaaS** (equals to "Blockchain as a Service") allows its users to leverage cloud-based solutions. In that way the users, either individuals or companies can build, host and use their own smart contracts and applications and functions on the blockchain and at the same time the cloud-based service provider takes care all the activities that will preserve the infrastructure agile and operational. Many startups and big companies offer BaaS services such as Microsoft with Azure.
9. **Metamask** is a tool that allows the users toserve Ether and other ERC-20 assets and at the same time to interact with Ethereum Dapps through their browser! This tool can be installed as an extension to Google Chrome or Firefox add-on.
10. **Ethers.js** is used by ethers.io and it enables users to write client-side JavaScript based wallets, keeping the private key on the owner's machine at all times. Ethers.js is the most commonly used library for Ethereum applications and acts as an alternative to web3.
11. **Tierion** helps users to create a verifiable database of data and processes on the bitcoin blockchain through tools & API so as to add data to the distributed ledger.

Tierior uses another tool that has developed called ChainPoint to record data and generate receipts. The latter have all the information a user needs to verify the data without relying on any intermediaries.

12. **Embark** is a developer framework that it allows one to easily develop and deploy dapps for Ethereum dapps and a serverless html5 application that uses decentralized technologies. Smart contracts can be created by this tool and be available in the JavaScript code.
13. **Truffle** is framework with a development environment and asset pipelines for Ethereum development. It provides support to Ethereum applications and makes new contracts coding simpler by offering custom deployments.
14. **MyEtherWallet** is a way to store cryptocurrency.
15. **Paper wallet** is also a way for one to keep one's cryptocurrency with safety. It is a form of cold storage[17] and it can print out the public and private keys of a user in a piece of paper (hence the term paper wallet) in the form of QR codes which they are scannable for all the transactions of the user in the future. They are stored and kept in safety and the user has the full access and control on them. That's why paper wallet considered to be safe since the user need to take care only a piece of paper!

[17] Keeping a reserve of cryptocurrency offline

5. Conclusions

At this point of the dissertation, it can be mentioned with certainty that the objectives that were set at the beginning of this paper are accomplished. Blockchain technology has been examined thoroughly, analyzing every tool that participates to this technology and its usage thus the cases of implementation of this method not only in ordinary aspects of life but also the approach of using the blockchain in a very crucial and sensitive environment, the banking one.

Financial sector does its first steps towards blockchain and tries to exploit it with safety and by taking advice from the leaders in technology innovations such as Google, Facebook and IBM.

More detailed, banks are very conservative as far as innovations are concerned, and nobody blames them, since they are responsible for the safety of the economical savings and premises of the whole world! They are very precautious by their nature because adopting a new idea or technology without the right technical and legal framework could lead to a disaster for their reputation and their trustworthiness.

Especially in the case of blockchain, some people believe that it will bring a great revolution in the financial sector and the impact it will have in this sector will be similar with the impact of the internet on humanity.

However, time, labor hours but mainly money should be invested by banks and any other organization so as to insert the blockchain technology into the finance and banking system. Specialized staff, new departments and new up-to-date equipment should be purchased and organized.

Bitcoin and other cryptocurrencies, as well as anything that uses Blockchain-based technology, has the main advantage of eliminating all intermediaries and free, peer-to-peer data sharing between participants. This also removes the duties that intermediaries have so far charged to carry out such processes. But the way this is done is not, at least in its current form, cost-free. These costs may not be economical, but they are a major obstacle to the further development of such technology.

So, in order for blockchain technology to deliver what we all expect from it, we need to find a way to work with lower energy costs[18] and this is something that is not easily achievable.

Blockchain networks that support functions of financial institutions are essentially private networks. The process by which any changes to their proper functioning and troubleshooting could be implemented, should be considered which are likely to arise in the future. So, on one hand there is Blockchain networks and applications that can take advantage of the technology and on the other hand there is a central authority that is able to intervene and make the necessary decisions where this is the case. essential. This central authority may not be a specific bank or organization, but it may be a committee of representatives of various institutions whose purpose is to oversee the proper functioning of the network and to make immediate decisions whenever they wish. it seems necessary.

It should be noted, therefore, that in its original form, a blockchain network is technically not easy to deal with any future malfunctions. Still, blockchain is an unexplored technology in many fields and especially in banking sector but its potentials are high and with the proper framework it can bring a revolution to the banking environment.

[18] https://www.theguardian.com/technology/2018/nov/05/energy-cost-of-mining-bitcoin-more-than-twice-that-of-copper-or-gold

6. Bibliography

[1] Dana Schwartz, Jeffrey W. Merhout, Blockchain - a Solution to Age-old Problems: Overview,, Miami, USA: Miami University - Oxford, 2019.

[2] Greenspan, Ending the bitcoin vs blockchain debate, http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate, 2015.

[3] C. a. Devetsikiotis, Blockchains and Smart Contracts for, North Carolina State University, 2016.

[4] Vitalik Buterin, A Next Generation Smart Contract & Decentralized Application Platform, USA: Ethereum White Paper, 2014.

[5] C. G. Harris, The Risks and Challenges of Implementing Ethereum Smart Contracts, Nothern Colorado, USA: IEEE, 2019.

[6] Haan Johng ; Doohwan Kim ; Tom Hill ; Lawrence Chung, Using Blockchain to Enhance the Trustworthiness of Business Processes: A Goal-Oriented Approach, San Francisco, USA: IEEE, 2018.

[7] Staci Duros, Cryptocurrency and Blockchain: Background and, Wisconsin, USA: Wisconsin Legislative Reference Bureau, 2018.

[8] Haiss Peter, Andreas Moser, Blockchain-Applications in Banking & Payment Transactions: Results of a Survey, Vienna: WU University of Economics and Business Department of Global Business and Trade, 2017.

[9] B.-K. Kim, Internationalising the Internet the Co-evolution of Influence and Technology, Northampton, USA: Manton Typesetters, Louth Linkolnshire, MPG Books LTD, 2005.

[10] M. S. Hart, A Brief History of the Internet, USA: CreateSpace Independent Publishing Platform, 2015.

[11] McPherson, Stephanie Sammartin, Tim Berners-Lee: Inventor of the World Wide Web, USA: Twenty-First Century Books., 2009.

[12] S. Voshmgir, Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy, Vienna: Shermin Voshmgir, BlockchainHub Berlin; Edition ed. edition, 2019.

[13] Haroon Shakirat Oluwatosin, Client-Server Model, School of Computing Universiti Utara Malaysia Kedah, Malaysia: IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 1, Ver. IX (Feb. 2014), PP 67-71, 2014.

[14] Hilbert, Martin; López, Priscila , The World's Technological Capacity to Store, Communicate, and Compute Information, Catalonia, USA: https://science.sciencemag.org/content/suppl/2011/02/08/science.1200970.DC1, 2011.

[15] T. O'Reilly και J. Battelle, What Is Web 2.0; The security risks of AJAX/web 2.0 applications, USA: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html, 2005.

[16] Quoc-Cuong To, Juan Soto, Volker Markl, A Survey of State Management in Big Data Processing Systems, USA: German Research Center, 2017.

[17] B. Yang ; H. Garcia-Molina, Improving search in peer-to-peer networks, Vienna, Austria: IEEE, 2002.

[18] S. Haber και W. S. Stornetta, How to time-stamp a digital document, Journal of Cryptology, 1991.

[19] Iansiti, Marco; Lakhani, Karim R., "The Truth About Blockchain", Harvard University, Cambridge, Massachusetts: Harvard Business Review, 2017.

[20] Zibin Zheng ; Shaoan Xie ; Hongning Dai ; Xiangping Chen ; Huaimin Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, Honolulu, HI, USA: IEEE International Congress on Big Data (BigData Congress), 2017 .

[21] Bearman, Sophi, "Bitcoin's creator may be worth $6 billion — but people still don't know who it is", New Jersey. USA, 2017.

[22] The technology behind bitcoin lets people who do not know or trust each other

build a dependable ledger. This has implications far beyond the crypto currency, USA: The Economist, 2016.

[23] Stuart Haber,W. Scott Stornetta, How to Time-Stamp a Digital Document, New Jersey: Journal of Cryptology, Vol. 3, No. 2, 1991.

[24] M.K.D.M.D.S. Jinyuan Li, Secure Untrusted Data Repository (SUNDR), New York, USA: NYU Department of Computer Science, 2004.

[25] David Mazieres and Dennis Shasha, Building secure file systems out of Byzantine storage, New York, USA: NYU Department of Computer Science, 2002.

[26] Matt Ridley, The Bitcoin revolution is only just beginning, UK: The Times, 2017.

[27] F. Coelho, A constant-effort solution-verification proof-of-work protocol based on Merkle trees, AfricaCrypt 2008, 2007.

[28] Brito, Jerry; Castillo, Andrea, Bitcoin: A Primer for Policymakers, Mercatus Center, George Mason University: Mercatus Center, George Mason University, 2013.

[29] R.S.R. Ku, The Creative Destruction of Copyright:Napster and the New Economics of Digital Technology, Chicago: University of Chicago Law Review, 2001.

[30] A.S. Jitendra Kurmi, A Survey of Zero-Knowledge Proof for Authentication, India: International Journal of Advanced Research in Computer Science and Software Engineering, volume 05, January 2015.

[31] E.G.S.D. Williams, Optimal parameter selection for efficient memory integrity verification using Merkle hash trees, Cambridge, MA, USA: Third IEEE International Symposium on Network Computing and Applications, Proceedings, 2004.

[32] D. Everitt, Simple Approximations for Token Rings, England: IEEE Transactions on Communications , 1986.

[33] Qassim Nasir ,Ilham A. Qasse, Manar Abu Talib, Ali Bou Nassif, Performance Analysis of Hyperledger Fabric Platforms, Hindaw: Electrical and Computer

Engineering Department, University of Sharjah, Sharjah, UAE, 9 September 2018.

[34] R. Schollmeier, A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications, Proceedings of the First International Conference on Peer-to-Peer Computing, USA: IEEE, 2002.

[35] S. Wang, W. Ding, J. Li, Y. Yuan, L. Ouyang and F. Wang, Decentralized Autonomous Organizations: Concept, Model, and Applications, IEEE Transactions on Computational Social Systems, vol. 6, no. 5, pp. 870-878, Oct. 2019, 2019.

[36] I. Heap, Blockchain Could Be Music's Next Disruptor, UK: https://fortune.com/2016/09/22/blockchain-music-disruption/, 2016.

[37] BOJANA KOTESKA, ELENA KARAFILOSKI, ANASTAS MISHEV, Blockchain Implementation Quality Challenges: A Literature Review, Skopje: Cyril and Methodius,Faculty of Computer Science and Engineering, , 2017.

[38] E. F. CODD , A Relational Model of Data for Large Shared Data Banks, USA: IBM Research Laboratory, San Jose, California,volume13, number06 , 1970.

[39] Olivier Boireau, Securing the blockchain against hackers, https://doi.org/10.1016/S1353-4858(18)30006-0, 2018.

[40] E. Parliament, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detectio, Brussels: European Parliament, 2016.

7. Appendix A. Timetable

The main phases of the current dissertation are presented in the following approximate timetable:

Project Phase	**15-Jul**	**22-Jul**	**29-Jul**	**5-Aug**	**12-Aug**	**19-Aug**	**20-Aug**	**25-Sep**	**10-Oct**	**30-Oct**	**02-Noe**
Roadmap – Basic Guidelines					VACATION						
Study of the Web											
Study of the Blockchain											
Study of implementation in non-banking fields											
Study of implementing in banking fields											
Proposals											
Conclusions											

8. Glossary

- **51% attack**: 51% attack refers to an attack on a blockchain system organized by a set of miners having the most 50% of the computing power of the miners participating in the system. In this case, the attackers would be able to block transactions verify, cancel transactions that have been completed, and make blockchain transactions for their benefit.
- **Bitcoin:** Bitcoin is a cryptocurrency, and it is an electronic form money. It is a decentralized digital currency that does not depend on one a central bank or an individual manager who can is sent by one user of the peer bitcoin network to another without it use of intermediaries.
- **Blockchain:** Blockchain is a distributed ledger, public or private, in which transactions or data are linked to each other linked data blocks making the practice unchanged and unquestionably from all the distributed nodes it has become updating the directory**.**
- **Consensus mechanisms:** allow secure updating of a distributed shared state.
- **Decentralized Autonomous Organization (DAO):**
- **Ethereum:** Ethereum is a blockchain platform that runs remotely code in a distributed computing system called Ethereum Virtual Machine.
- **Full nodes:** Nodes containing the complete blockchain.
- **Genesis block:** The first block on a blockchain.
- **Initial Coin Offering (ICO):** Financing mechanism for business ideas which are based on blockchain. A new currency is required to allow the use of the application through which it will be implemented business idea. A number of these coins are available for sale before launching the application so that anyone interested can can get them.
- **Light nodes:** Nodes of the blockchain network that only download their heads blocks and therefore have lower execution requirements. Using a method called Simplified Payment Verifications (SPV), a light node can query a full node for verifying a transaction. Cryptographic wallet is a characteristic example of light nodes

- **Miners:** Blockchain is consisted of nodes that are constructed by miners. When a miner succeeds in attaching a new block then he receives both the mining fee and the transaction costs. This method motivates miners to validate new transactions on a continuous basis and thus to support its operation blockchain.
- **Nonce:** A number that one has to guess through many trials (type of trial and error). This number when combined with the other elements of a block and the hash value of the previous block will lead to a new hash value that will cover the required level of difficulty (number of zeros at the beginning of the hash value) as dynamically defined by the network.
- **Permissioned blockchain:** The kind of blockchain in which the participants are known and licensed to participate in the system. There is some degree trust between participants. Also referred to as private blockchain.
- **Permission-less blockchain:** The kind of blockchain it can participate in anyone who confirms the transactions on the basis of their consent is created by its members who must devote computing power to the verification of transactions. Also referred to as public blockchain.
- **Proof of Stake (PoS)**: A form of algorithm through which a blockchain system aims to achieve a shared consensus. In a PoS system the creator of the next block is randomly selected based on value acquired or based on time of participation in the system.
- **Proof of Work (PoW):** A form of algorithm through which a blockchain system aims to achieve a shared consensus. In a PoW the effort focuses on the process of finding a suitable nonce. The basic idea is that the nonce is hard to find but easy to verify.
- **Smart contract**: Smart contracts are self-executing contracts containing the terms of agreement between the buyer and seller directly recorded as lines of code. The smart contracts make transactions discoverable, transparent and irreversible by the moment they have taken place.