LUISS

Dipartimento di
Impresa e Management

Cattedra
Economia e gestione delle imprese

"BLOCKCHAIN TECHNOLOGIES''

RELATORE
Prof. Jannis Kallinikos

CANDIDATO
Angel Marfiuc
Matr. 231351

ANNO ACCADEMICO 2021/22

Ad maiora semper

Index

Chapter IV

Criminality and the future of the Blockchain

Introduction

The work presents a journey through a new technology called Blockchain, which has spread and developed in recent years.

The major purpose of the thesis is to describe what this technology is about, by delineating its history and characteristics, and by analyzing its complex structure made by a well-built architecture, tiers and different blockchain types.

The thesis also aims at describing the fundamental features used in a Blockchain such as exchanges and digital wallets, which are increasingly being used in our days. A final objective is to consider the benefits of using these technologies in different areas (such as healthcare, energy industry, stock markets, etc.), what aspects of these areas may be improved and to expose the risks and downsides of these technologies, such as criminality.

Chapter I

What is Blockchain?

1.1 History of Blockchain

Before talking about Blockchain, its history has to be known. Despite the widespread view of linking the origins of the technology of blockchain with the 2008 circulation of Satoshi Nakamoto's ''Bitcoin'' white paper and the 2009 launch of the Bitcoin blockchain (Nakamoto 2009, Wallace 2011 [1]), the story of the creation of the blockchain is different and it takes root in a much earlier project. Nakamoto's 2009 Bitcoin white paper has a total of eight footnotes: three of those eight are to the work of Scott Stornetta and Stuart Haber, the developers of the time-stamping structure, today known as blockchain structure, developed twenty years before Nakamoto's paper (Haber & Stornetta 1991a ; Bayer, Haber & Stornetta 1993; Haber & Stornetta 1997[4]). Haber and Stornetta were

particularly interested in the trust for the information in the digital age, while their central concern particularly informs applications of blockchain in the arts.

In the late 1980s, the physicist Stornetta and the cryptographer Haber were working together as researchers at Bellcore in Morristown, New Jersey (Haber, personal communication, May 2018, W.S. and M. Stornetta, personal communication, March 2018[4]). In this period the two scientists were studying and observing the early mainstream adoption of personal computing because, by 1984, eight percent of American households owned computers. After five years, by 1989, fifteen percent did (U.S. Census [2]).

After taking note of this new phenomenon concerning the growth of digital information development, the two scientists asked two questions, one regarding philosophy and one regarding politics.
The philosophical consideration was: ‘’If it is so easy to manipulate a digital file on a personal computer, how will we know what was true about the past? ‘’
On the other hand, the political consideration was: ‘’How can we trust what we know of the past without having to trust a central authority to keep the record? ‘’

These two inquiries led to what turned out to be a very difficult arithmetic problem. Building a trustworthy registry of digital files without having a central administrator proved so difficult that Haber and Stornetta almost gave up. Their idea of giving up as scientists were to attempt to formally demonstrate that the problem was, in fact, unsolvable. After some time, Stornetta was waiting for a table with his wife and his children in a Friendly’s restaurant in Morristown, New Jersey, when the seed of a possible answer came to him: the next day, Stornetta informed Haber, and the two set out to create the system (Whitaker 2018b [3]).
They conceived a time-stamped ledger (the fundamental underlying structure of a blockchain) that is both cryptographic and registrarial. The time-stamped series of records are linked together in such a way that one cannot tamper with one item without disrupting the whole chain while internally, the total ledgers are linked from one block of a transaction to the next, and then numerous connected copies of the ledger are disseminated, allowing for a ledger that depends on an algorithm rather than on a single central administrator (W.S. & M. Stornetta, personal communication, March 2018 [4]).
Haber And Stornetta presented their work at a 1990 cryptography conference before publishing it in *The Journal of Cryptography* in 1991 with ‘’ How to Time-Stamp a Digital Document’’ as title (Haber and Stornetta 1991a, 1991b [4]). They wrote their foundational paper (Haber and Stornetta 1991b) mentioning Shakespeare’s ‘’The Rape of Lucrece’’:

Time’s glory is to calm contending kings,

To unmask falsehood, and bring truth to light,
To stamp the seal of time in aged things,
To wake the morn, and sentinel the night,
To wrong the wronger till he render right.

- (Folger Digital Texts n.d. 1594)

In addition to citing The Rape of Lucrece, the article makes a good case for establishing a system of stamping that does not need faith in a central authority by mentioning Juvenal circa 100 A.D., ‘’But who will guard the guards themselves?’’ including also the original Latin phrase ‘*’Sed quis custodiet Ipsos Custodes?*’’ (Haber and Stornetta 1991b, p.4 [4]). Their work reveals a rare blend of technical and humanistic ideas in the blockchain’s beginning point, according to the paper and interviews with Haber and Stornetta. Legally Haber and Stornetta’s employer, Bellcore, owned their blockchain invention. (Whitaker A, 2019 [3]), but in 2003 they licensed Bellcore's technology and formed a company called Surety to time-stamp records. For example, scientists who previously kept numbered paper notebooks with stitched bindings (to prevent tampering with or rearranging pages) might now enter their scientific observations onto the Surety blockchain. (Haber, personal communication, May 2018[4]). Each week, Surety released an alphanumeric code that a computer scientist might use to verify that no one had tampered with the Surety blockchain, to adopt a radically transparent approach to the verifiability of their recordkeeping.

They also published the code in the “Notices” section of the classified advertisements of the Sunday national edition of the New York Times and their code is still published in the Sunday paper's "Notices" section, making it the world's oldest blockchain. Surety and Bellcore both had patents on the blockchain structure, however, they expired in 2004 due to a late patent maintenance fee, otherwise the blockchain technology would have remained patent-protected in the United States during the first year of the Nakamoto Bitcoin paper. (Haber & Stornetta 1992[4]).

Outside of computer programming circles, Bitcoin was launched in January 2009 with little excitement. In the fall of 2008, a white paper suggesting Bitcoin was shared on a cryptography listserve, and the Bitcoin blockchain was formally launched on January 3, 2009. (Burniske & Tatar 2018, p.7[5]). Satoshi Nakamoto, the white paper's author, is assumed to be a pen name for a person or group of persons. In fact, the Bitcoin blockchain is generally observed to have the kind of concerted, kaleidoscopically thoughtful presentation less likely to be the work of one individual’s thought process. Nakamoto adopted Haber and Stornetta's distributed ledger concept and added a monetary incentive for keeping the connected copies of the ledger up to date. Also the invention of

mining, which allows anyone to gain currency by solving mathematical problems connected to confirming transactions in a block, was a major breakthrough for Nakamoto. (Nakamoto 2009, p.3; Narayanan, Bonneau, Felten, Miller & Goldfeder 2016[6]).

Although blockchain is far more than a mechanism for cryptocurrencies, one early Bitcoin anecdote exemplifies the invention's extremely unexpected path in its beginnings. Someone attempted to force a transaction in which bitcoins were used to purchase something tangible on May 22, 2010, almost fifteen months after its introduction. Laszlo Hanyecz, a computer programmer, offered 10,000 bitcoins to anyone who could get him two pizzas. Two Papa John's pizzas were brought to Hanyecz in Florida by a British guy who consented and paid for the pizzas 30$. The 10,000 bitcoins he received in return for the pizzas were worth 82 million dollars by May 2018. (Suberg 2018[7]).

Haber and Stornetta are the Vincent Van Goghs of cryptos in terms of the financial life of their invention; they did not generate revenue early on. Also Surety never grew into a significant company, and Haber and Stornetta moved on to other activities: Stornetta went on to become a high school math teacher, where he taught incoming ninth-graders the most basic arithmetic and graduating seniors the most advanced math; Haber later worked for Hewlett Packard and several start-up companies. Both are now working with blockchains.

1.2 Characteristics of Blockchain

This sort review of the history of the origins of Blockchain shows that it took root sooner than imagined. However what are the characteristics which made this technology so popular?

In today's world, each crypto money transaction must be transparent because there is a lot of personal information in these transactions that may do a lot of harm if it falls into the wrong hands. The technology, including hardware and software, that is linked with these transactions must also be taken into consideration, as any one of these component’s failure would fail a money transaction. A blockchain can be considered as a digitalized public ledger that would record all the digital transactions in chronological order or as ‘‘Completed Transaction Blocks’’ as a data structure and stores this in a distributed manner across a network. (M. Niranjanamurthy, B.N. Nithya, S. Jagannatha, 2018 [8]).

In addition anyone who can access this network would be able to get this ledger. To implement blockchains three technologies are used: Private Key Cryptography, Peer to Peer Network, and Program (the Blockchains protocol).

There are different benefits in a Blockchain for example it makes use of distributed computing technology, which helps it avoid load-sharing issues and is particularly reliable for storing sensitive information such as medical records, management operations, transaction processing, documenting derivation, food traceability, or voting, because distributed computing technology provides a progressive degradation.

Blockchain technologies have six main characteristics.

1. *Decentralized:* the core aspect of Blockchain is decentralization, which implies that data can be collected, stored, and updated on various systems rather than relying on a centralized node.

2. *Transparent:* the data's record is accessible to each node in the Blockchain system, and each of these nodes can update the data, keeping it transparent and trustworthy.

3. *Open source:* the majority of Blockchain systems are accessible to the public, allowing anybody to examine records and utilize Blockchain technology to build any applications they desire.

4. *Autonomy:* because of the consensus structure, any node on the Blockchain system can securely exchange or update data; the objective is to build confidence from a single person to the whole system, with no one able to intervene.

5. *Immutable:* any records will be reserved permanently and cannot be modified unless someone with control of more than 51 percent of the nodes in the network does so at the same time.

6. *Secrecy:* blockchain technologies have fixed the node-to-node trust problem, allowing data movement or even transactions to remain anonymous; all we need is the person's Blockchain address to complete a transaction.

In other words, the Blockchain is a unique peer-to-peer technology that links a sequence of transactions or events in such a way that they become immutable and was initially designed for the virtual cryptocurrency Bitcoin. [9] It is a transaction database that stores information about all previous transactions and is based on the Bitcoin protocol. It establishes a digital ledger of transactions and allows all network members to securely update the ledger, which is shared over a

distributed network of computers. [10] A Blockchain is something like a ledger in which all transactions have been recorded, and it is shared by the participants of a Bitcoin network. [11]

The most critical issue with the Blockchain is trust: the interactions between the network's nodes guarantee that trust is maintained in fact, instead of depending on trusted third-party entities to enable transactions, Blockchain network participants rely on the Blockchain network itself. The key qualities provided in existing Blockchains are immutability, non-repudiation, integrity, transparency, and equal rights. [12]

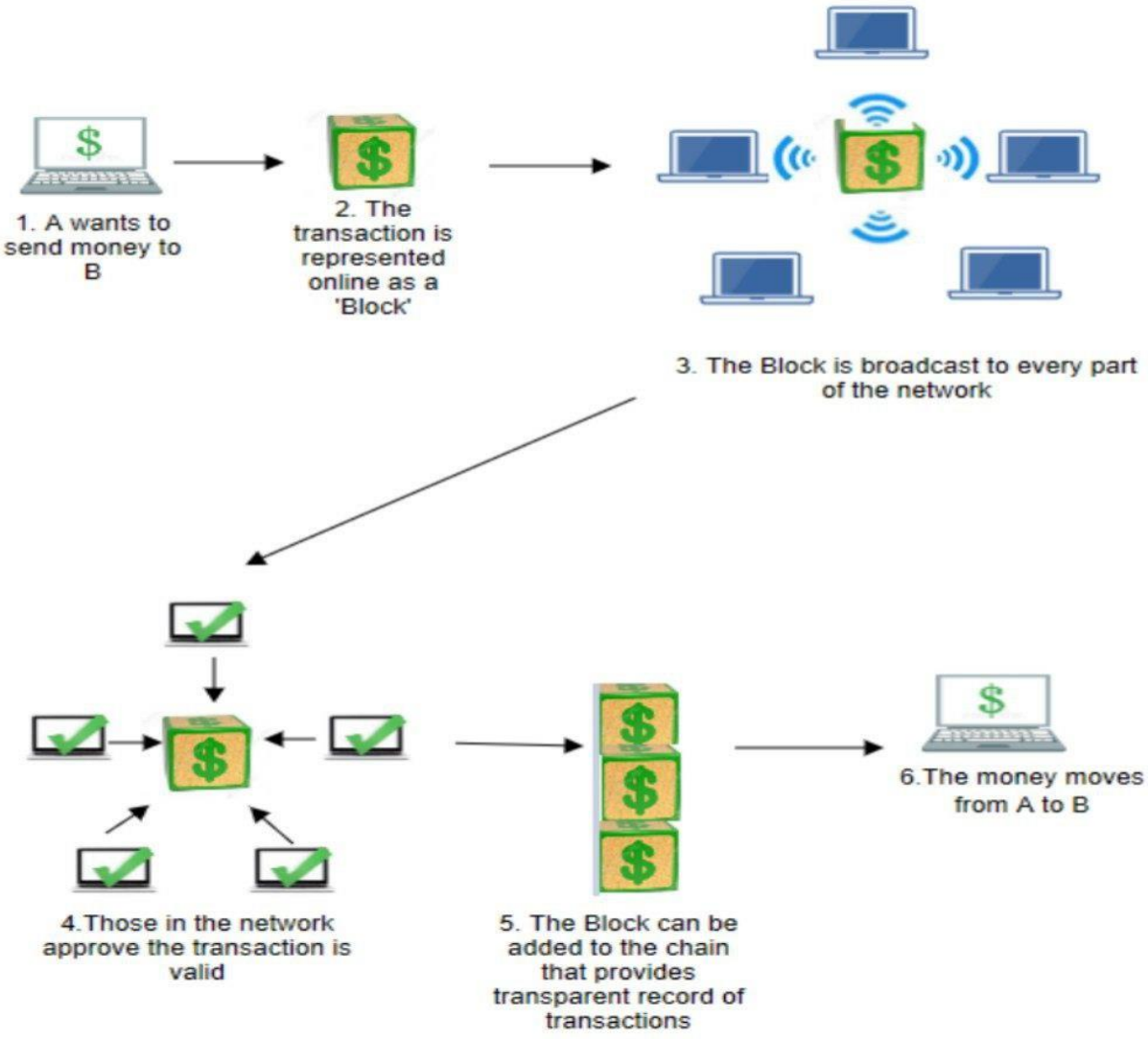
1.3 How Blockchain works?

It’s important to know how the blockchain works: when someone creates a transaction, the Blockchain face up a process with six steps:

1) The desired transaction is broadcast to a peer-to-peer (P2P) network of computers called nodes.
2) Validation: by using well structured and known algorithms, the network of nodes verifies the transaction and the user's status.
3) Crypto money, contracts, records, and other data can all be included in a confirmed transaction.
4) The transaction (after being confirmed) is connected to other transactions to create a new block of data for the ledger.
5) The new block is then added to the current Blockchain in an irreversible and permanent shape.
6) The transaction is completed.

Is important to point out that transactions do not become legitimate until they are added to the chain. It's easy to see tampering immediately. But because everyone in the network has a copy, the Blockchain is considered secure and the sources of any discrepancies are usually evident immediately. (M. Niranjanamurthy, B.N. Nithya, S. Jagannatha, 2018[8])

Picture from Simanta's Shekhar study [13]



1.4 Types of Blockchain

After all its development and upgrades, different types of Blockchain have been created, each one created for different purposes:

Public Blockchains: public blockchains are open to the public and any individual can be involved in the decision-making process by becoming a node, but users may or may not be benefited for their involvement in the decision-making process. The ledgers are owned by no one in the network and are

openly accessible to anybody who is a part of it. To conclude, blockchain users use a distributed consensus method and keep a copy of the ledger on their local nodes.

Private Blockchains: not every node will be able to join in this Blockchain, and data access will be controlled by rigorous authority management. Regardless of the type of Blockchain, it offers benefits: sometimes we need public Blockchain because of its convenience, but sometimes we maybe need private control like the private Blockchain, depending on what service we offer or what place we use it. These blockchains are not available to the general public, but rather to a select set of individuals or organizations, and the ledger is shared solely among the participants.

Semi-private Blockchains: in a semi-private blockchain, a portion of the blockchain is kept private and managed by a group of organizations, while the rest is accessible to the public and may be used by anybody.

Sidechains: these blockchains are also known as pegged sidechains because they allow currencies to be transferred from one blockchain to another. One-way pegged sidechains and two-way pegged sidechains are the two varieties of sidechains.
One-way pegged sidechains enable movement between two sidechains, but two-way pegged sidechains allow movement on both sides of two sidechains.

Permission Ledger: the participants in this sort of blockchain are already identified and trusted. Instead of using a consensus process, a permissioned ledger uses an agreement protocol to preserve a shared version of the truth.

Distributed Ledger: a distributed ledger blockchain is one in which the ledger is shared among all blockchain participants and can span various businesses. Records are recorded in a distributed ledger in continuous blocks rather than sorted blocks, and they might be private or public.

Shared Ledger: shared ledger can be an application or a database that is shared by the public or an organization.

Fully private of Proprietary Blockchains: these Blockchains are not used in any major applications and contradict the concept of decentralization. These blockchains are useful when it is necessary to transfer data inside an organization while also ensuring the data's legitimacy. An example could be the proceedings to transfer data between departments, government agencies deploy private or proprietary Blockchains.

Tokenized Blockchains: these are traditional blockchains that create currency through a consensus process that involves mining or initial distribution.

Tokenless Blockchains: these blockchains are not true blockchains since they cannot transfer assets, but they can be beneficial when no value is being transferred between nodes and only data is being transferred between previously trusted parties. [13]

1.5 Tiers of Blockchain

The story of the Blockchain its spreading and its development, allowed it to go through different stages called tiers.
The following three tiers of blockchain technology were originally described in the book 'Blockchain, Blueprint for a new Economy' by Melaine Swan based on the applications in each category.

Blockchain 1.0: this Blockchain was created with the introduction of bitcoin and is mostly utilized for cryptocurrencies. This stage of blockchain includes all alternative currencies as well as bitcoin and it also covers essential apps.

Blockchain 2.0: Blockchain 2.0 is used in financial services and industries which includes financial assets, options, swamps, and bonds, etc. Smart Contracts were originally presented in Blockchain 2.0 and can be characterized as a mechanism to check if the provider sends the items and services throughout a transaction process between two parties.

Blockchain 3.0: in comparison to Blockchain 1.0 and 2.0, Blockchain 3.0 delivers more security, is more scalable and flexible, and is more sustainable. It's utilized in a wide range of areas, including the arts, health, justice, journalism, and many government agencies.

Generation X: this idea is based on the concept of singularity, in which everyone may use the blockchain service. This blockchain will be accessible to everyone and run by autonomous agents. (Simanta Shekhar S. (2018) Understanding Blockchain Technology [13])

Chapter II

Analysis of Blockchain

2.1 SWOT analysis of Blockchain

In order to understand what are the real benefits but also the weaknesses of the Blockchain, different analysis and comparison have to be done such as the SWOT analysis.

SWOT analysis (or SWOTM matrix) is a short form for strengths, weaknesses, opportunities, and threats and is a structured planning method that evaluates those four elements of an association, project, or commerce endeavor, etc.

In the list below are going to be presented the strengths, the weaknesses, the opportunities, and the threats of the blockchain, through a general Swot analysis.

List is taken from Niranjanamurthy's M. and others study [8]

Strengths	**Opportunities**
100% transparency	Automation
Able to skip the intermediary	Business Process Optimisation
Auditable trail	Elimination of trust necessity
Business process efficiency and productivity	Faster (international) payment transfers
Decentralized approach	Improved customer experience
High quality and foolproof data	Increased quality of products and services
Higher efficiency	Innovation in almost every industry
Lower cost	Huge innovation in the Banking world
Lower risk	Instantaneous settlements
More secure	KYC (know your customer) database
No reliance on the third party	New Intermediaries
Robustness (no SPOF)	No reliance on rating agencies
Speed	Opportunities in IoT
Unharmed privacy	Programmable control mechanism
Trust in trustless networks	Smart contracts insurance
	Speedup bank processes

Weaknesses	Threats
Access challenge	A lot of research needs to be done yet
Change Management	The disappearance of existing bank jobs
Integration with Legacy Systems	Govt. Willingness to adopt
Lack of Standards	High investments for implementations
Low capacity and processing speed	Huge regulatory impact
Ownership challenge	Hype
Recent technology	Legal/regulatory and compliance
Scalability	Privacy and security
Security against cybercriminals	Time
Storage	Uncertainty about the impact
Technology Maturity	
Mass adoption	

2.2 Advantages and disadvantages of the Blockchain

As seen in the last paragraph, there are a lot of opportunities and benefits from the use of the Blockchain but, on the other hand, there are also weak points and risks. To be more detailed, what are the effective advantages and disadvantages of blockchain technologies?
Let's start with the advantages:

- *Disintermediation:* the main benefit of a Blockchain is that it allows a database to be shared directly without the need for a central administrator, rather than relying on centralized application logic to impose limits, Blockchain transactions have their own evidence of validity and authorization. The result of these features is that transactions may be confirmed and executed independently, thanks to the Blockchain functioning as a consensus mechanism to keep the nodes in synchronization. However, why is disintermediation beneficial to us? Because, although being made up entirely of bits and bytes, a database is nonetheless a physical object and if the contents of a database are kept in the memory and disk of a computer

system managed by a third party, even if that third party is a trusted entity such as banks or governments, anybody who gains access to that system can modify the data contained inside. As a result, third-party businesses, particularly those in charge of sensitive databases, must engage a large number of people and implement several processes to ensure that the database is not tampered with and all these elements, unavoidably, require a significant amount of time and money.

- *Empowered users:* users have complete control over their data and transactions.
- *High-quality data:* the data on the blockchain is complete, consistent, fast, accurate, and publicly accessible.
- *Durability reliability and longevity:* blockchain does not have a centralized point of failure and is better equipped to survive malicious assaults because of its decentralized networks.
- *Process integrity:* users may be confident that transactions will be carried out exactly according to protocol directions, avoiding the requirement for a third party.
- *Transparency and immutability:* all transactions on blockchains are immutable, meaning they cannot be changed or erased, and they are openly available by all participants, establishing transparency.
- *Ecosystem simplification:* the clutter and difficulties of many ledgers are reduced when all transactions are merged to a single public ledger.
- *Faster transactions:* clearing and ultimate settlement of interbank transactions can take days, especially outside of business hours. Transactions on the blockchain may be completed in minutes and are handled 24 hours a day, seven days a week.
- *Lower transaction costs:* blockchains have the potential to drastically lower transaction fees by removing third-party intermediaries and administrative expenses associated with exchanging assets.
- *Blockchains can be used to:*

  Reduce total cost of ownership: at a fraction of the cost of typical proprietary stacks, blockchain stacks provide a reliable and verifiable alternative.

Manage system-of-record sharing: by using blockchain technology, diverse parties (such as customers, custodians, and regulators) can get access to their own live copies of a shared system of record.

Clear and settle transactions faster: the move from overnight batch processing to intra-day clearing and settlement can be made easier with blockchain technology.

Create self-describing electronic transactions: smart contracts may build context-aware transactions for advanced arbitration using Blockchain's programming language.
A credit default swap, for example, might payout automatically based on pre-agreed logic that analyzes market data sources.

- *Business benefits:* many companies can profit from incorporating Blockchain technology into the new trading platform. The most important advantages of using this technology are the following six:

Efficiency: Transactions are carried out directly between the two parties, without the participation of a third party, as is the case with Blockchain technology. As a result, transactions are carried out rapidly. Furthermore, the platform has the capability of autonomously managing smart contracts and business actions. As a result, every procedure is immediately streamlined, removing both cost and time from the transaction.

Auditability: each transaction detail is recorded afterward on the Blockchain network, providing audibility for the asset between two parties. It is especially advantageous for firms that require a data source to validate assets.

Traceability: tracking items in a supply chain is very simple and advantageous on the Blockchain. Information about the component can be conveyed to and from the new owner as needed for action.

Transparency: one of the key advantages of Blockchain for small, medium, and big organizations is transparency. As a result of a lack of financial and commercial transparency, unfavorable business relationships and delays in business may emerge. So, in order to provide transaction details in accordance with the commercial design, trust and transparency must be maintained throughout the process to keep a solid connection rather than negotiating.

Security: each transaction is recorded and validated in the Blockchain network by solving challenging cryptographic challenges. Complex mathematical techniques are used to ensure the accuracy of the data and the advantages of IoT (Internet of Things) include secure key information. This has previously been utilized in the defense industry to secure intellectual property and validate instructions.

Feedback: another advantage of Blockchain technology for businesses is feedback because the system allows for full traceability throughout the asset lifecycle, asset producers and designers can simply track assets and integrate asset management into products to improve efficiency. Information on installation, maintenance, shipping returns, and decommissioning is available through feedback.

The bottom line: while Blockchain has been designed to serve the digital currency, however, it can also help businesses in serving their needs. Therefore, business owners should use this technology in their business and make a boom in the industry. (M. Niranjanamurthy, B.N. Nithya, S. Jagannatha, 2018 [8]).

Disadvantages of Blockchain technology:

- Because of the nature of Blockchains, they will always be slower than centralized databases in terms of performance. When a transaction is performed, a Blockchain must do all of the same tasks as a traditional database, but it also faces three additional responsibilities:

  a) Signature verification: A public-private cryptography system must be used to digitally sign every Blockchain transaction and because transactions move between nodes on a peer-to-peer basis, their origin cannot be verified otherwise. The process of creating and verifying these signatures is computationally intensive, and it is the biggest barrier. In centralized databases, on the other hand, once a connection has been established, there is no need to manually validate each request that comes through it.

  b) Consensus mechanisms: in a distributed database like a Blockchain, effort must be put in to ensure that all nodes in the network accord. Depending on the consensus process employed, this might include a lot of back-and-forth communication as well as dealing with forks and rollbacks. While centralized databases must deal with conflicting and aborted transactions, these are significantly less common when transactions are queued and completed in a single area.

  c) Redundancy: this isn't about the performance of a single node, but rather the entire amount of processing required by a Blockchain. Unlike centralized databases, which process transactions once (or twice), a Blockchain requires each node in the network to execute transactions individually. As a result, a great deal more effort is being done for the same ending result.

- Nascent technology: to make Blockchain generally useful, issues like transaction speed, verification, and data restrictions must be solved.

- Uncertain regulatory status: because contemporary currencies are established and governed by national governments, Blockchain and Bitcoin might face a significant barrier to

widespread adoption by pre-existing financial institutions if the government's regulatory status remains unclear.

- Large Energy consumption: miners on the Bitcoin Blockchain network are attempting 450 trillion solutions every second in an attempt to validate transactions, consuming a significant amount of computing power.

- Control, security and privacy: while there are alternatives, such as private or permissioned Blockchains and robust encryption, there are still cyber security concerns that must be solved before the general public can trust a Blockchain solution with their personal data.

- Integration concerns: blockchain applications provide solutions that do necessitate large modifications to existing systems or their entire replacement. Companies must prepare in advance in order to make the move.

- Cultural adoption: blockchain represents a complete shift to a decentralized network that requires users and operators to buy in.

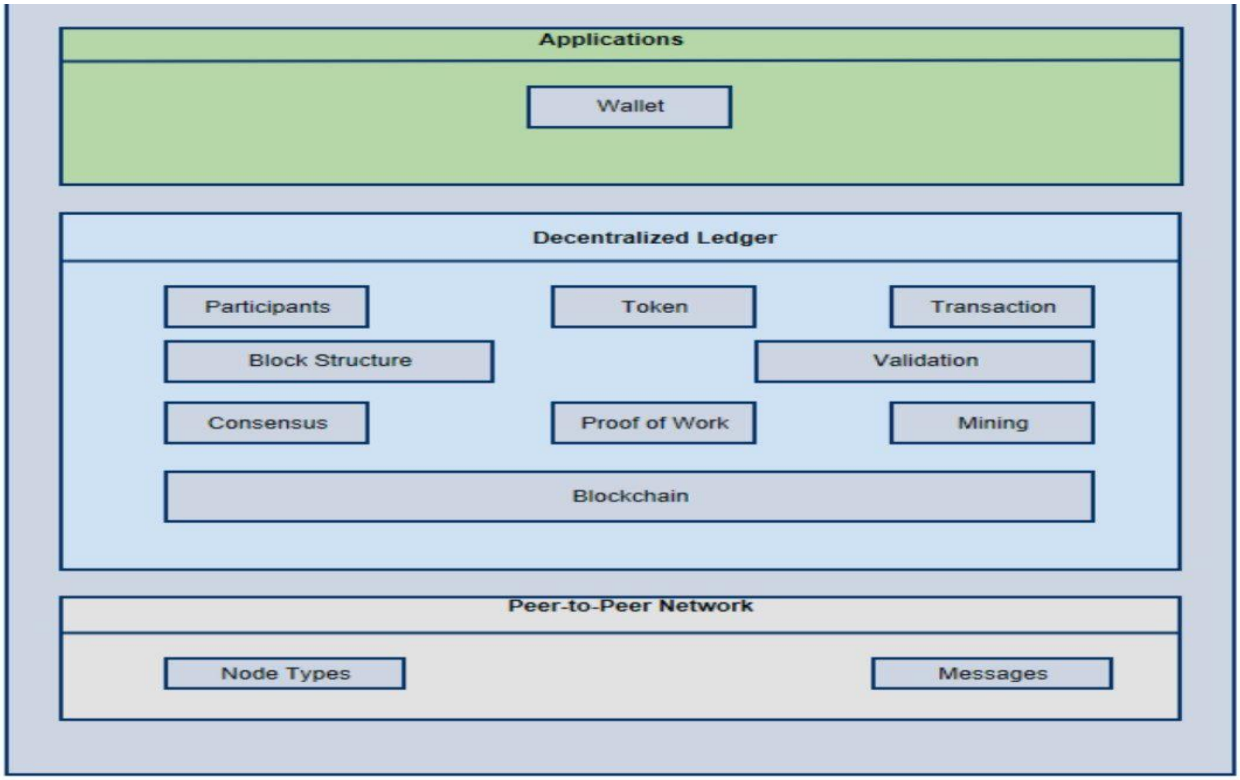
- Costs: although blockchain promises significant cost and time benefits, the high initial capital cost may be onerous.

Furthermore, blockchain attacks could be accomplished through: user identify theft, fraudulent sender and receiver, targeting on Bitcoin miners, availability of distributed nodes, injection of malicious code into a distributed ledger, reputational risk, target reconnaissance, bypassing the onboarding and offboarding of the nodes and fictitious blockchain applications may appear to steal transaction details/personal information. (M. Niranjanamurthy, B.N. Nithya, S. Jagannatha, 2018 [8]).

2.3 Blockchain Architecture

As mentioned in the other paragraphs, Blockchain technology is based on the notion of a decentralized database, which is a database that exists on several computers and is identical in every edition: organizations store their data in a centralized database, making them an easy target for hackers, but the decentralized structure of blockchain has made it a tamper-proof system. On top of the internet, blockchain may be viewed as a peer-to-peer network, but what is its architecture? Blockchain architecture can be mainly divided into three layers which are Applications, Decentralized Ledger and Peer-to-Peer Network. Applications are the top layer, followed by the Decentralized Ledger and the bottom layer is the Peer-to-Peer Network. [13]

Picture from Simanta's Shekhar study [13]



The Blockchain software package is stored in the application layer; Bitcoin wallet software, for example, generates and maintains private and public keys, allowing users to preserve control of their unspent bitcoins. Users may keep track of their transactions via the application layer, which offers a human-readable interface. These applications also provide application interfaces on top of the blockchain, used for keeping cryptocurrencies secure. This software can be installed on every computer or mobile device or also can be hosted on a third-party platform.

The Decentralized Ledger is the intermediate layer of a blockchain architecture that ensures a reliable and tamper-proof global ledger. Transactions can be bundled into blocks that are cryptographically connected to others in this layer. These transactions are defined as the exchange of tokens between two parties, and each transaction is subjected to a validation procedure before being declared valid. In this process a proof-of-work procedure is used in the blockchain to identify which chain has needed the greatest cumulative effort to develop and to ensure consensus across all nodes to certify the blockchain's legitimacy. Finally, the Peer-to-Peer Network is the bottom layer of the blockchain architecture, where different Node types serve different functions and various messages are exchanged to maintain the Decentralized Ledger.

2.4 The Decentralized Ledger

The decentralized ledger needs a further paragraph because it is the most complex part of the blockchain: is a synchronized database that is shared and duplicated across network participants and it keeps track of the transactions that take place among the network's participants. The ledger is also in charge of keeping track of all transactions between the participants. Except for the fact that it keeps information in the header and data is saved in the form of a token or cryptocurrency, blockchain is similar to a database. As the initial stage in recording transactions in the ledger, it is necessary to aggregate recently verified transactions into blocks and any blockchain participant can collect new transactions and construct blocks that can be added to the network. A block mainly consists of transactions and has a pointer, timestamps and the nonce and depending on their role in the blockchain network, nodes perform a variety of roles. When a node proposes and verifies transactions, as well as does mining to create consensus and safeguard the blockchain, it can be called a ‘’miner’’. A miner may carry out tasks such as basic payment verification and others, depending on the blockchain in use. The consensus technique that checks the validity of data is known as proof of work: Bitcoin, for example, uses hashcash as a proof-of-work algorithm for bitcoin transactions. To be validated by the network, miners must perform a proof of work in order to validate the transactions in the block. In other words the blockchain network's security and consensus are ensured through proof of work. A hash (id) is assigned to a block during verification and this hash is applied to the current block of transactions to validate the following block. Proof of work is expensive to maintain, and because it is always dependent on the miners' incentives, it may have future scalability and security difficulties. There is a more advanced technique known as "proof-of-stake," which is profitable to implement and specifies who gets to update the consensus and prevents the underlying blockchain from forking. In a blockchain network, no secret information is exchanged, and all transactions are accessible to every node in the network. To conclude this peer-to-peer network requires no extra security and may be implemented on any physical infrastructure. [13]

Chapter III

3.1 Currency Exchanges

In our days many applications and software have been developed to create easy methods for using blockchain technology, such as currency exchanges.

With the currency exchanges, users can exchange bitcoins for traditional or virtual currencies. Most of the exchanges use multiple auctions, similar to traditional financial markets, with bids and requests, and impose a fee ranging from 0.2 to 2%. There are also more complex trading tools, including limit and stop orders, available on other different exchanges. Many bitcoin trades currently include one or even two conversions from and/or to traditional currencies. Furthermore, bitcoin price quotations are virtually always determined in real-time using a fixed quantity of traditional cash. As a result, Bitcoin now resembles a payment platform rather than a currency, as defined by economists. While there are minimal technological obstacles with establishing intermediaries in the Bitcoin ecosystem, there are several regulatory restrictions. For example, currency exchangers in the United States are classified as "money transmitters" and must register as money services firms with the Financial Crimes Enforcement Network (FinCEN). This registration process comprises a state-by-state licensing process that includes legal costs and the posting of bonds. The certification in a single state might cost upwards of $10,000, therefore fees alone for nationwide participation can quickly exceed six figures. Other countries follow a similar set of guidelines. Currency exchanges that manage customer deposits are classified as "deposit banks" in Germany, with a minimum capital requirement of €5 million. These exchanges also require digital infrastructure that can survive threats such as hacking and denial-of-service attacks. As a result of all these factors, the number of Bitcoin exchanges has remained low, and the number of Bitcoin exchanges with considerable volume has even decreased. In spring 2012, the Japan-based Mt. Gox exchange served over 80 percent of all Bitcoin transactions. However, Mt. Gox collapsed in early 2014 and reported in its bankruptcy filing “losing” 754,000 of its customers’ bitcoins worth approximately $450 million at the time of closure (Abrams, Matthew, and Tabuchi 2014)(Journal of Economics Perspectives [14])

3.2 Digital Wallet Services

After mentioning the blockchain, Bitcoin and their many branches, there is another essential element of this technology: the digital wallet services.

Bitcoin wallets are data files that include Bitcoin accounts, transactions, and the private keys required to spend or move the currency held. To keep control of their bitcoins, some users install dedicated wallet software (like Armory, Electrum, or Hive) on their own devices. This task, however, is unattractive to many users because installing Bitcoin wallet software may be complicated, and it might come with onerous technological requirements, such as holding a copy of the full blockchain, which at the time of writing was 30 gigabytes. (While not everyone is required to download the complete chain, the system does rely on certain users doing so.) Other users are concerned about security: a computer crash or attack on the digital wallet may result in the loss of a user's bitcoins. Because of these factors, many users rely on a digital wallet service, which stores the necessary data on a shared server and allows access through the web or mobile apps. The knowledge of the account's private key is a fundamental differentiator among digital wallet providers: some services (such as Blockchain.info, Crypto.com, and CoinPunk) allow users to keep ownership of their private keys, which means that the service is unable to spend the user's bitcoin (and hackers would not be able to do so even if they have totally hacked the wallet service). For such firms, the user must keep and present the private key when needed, and a user who loses the key or allows it to be compromised is at high risk. Other services, like Coinbase and Xapo, on the other hand, require customers to allow the service to keep their private keys, which raises the danger of the digital wallet service being hacked.

(Journal of Economics Perspectives [14])

3.3 Blocks

The blocks of a blockchain have a big role in this articulate structure: users of the blockchain network submit potential transactions to the network using software (desktop applications, smartphone applications, digital wallets, web services, etc.) and these transactions are sent to a node or nodes inside the blockchain network by the program. The submitted transactions are subsequently broadcast to the rest of the network's nodes, although this does not automatically add the transaction to the

blockchain. For many blockchain implementations, once a pending transaction has been distributed to nodes, it must then wait in a queue until it is added to the blockchain by a publishing node. (Dylan Yaga and others (2018) Blockchain Technology Overview [15]). When a publishing node publishes a block, transactions are added to the blockchain. A block is made up of two parts: a block header and block data. This block's metadata is contained in the block header while a list of authenticated and verified transactions that have been uploaded to the blockchain network is contained in the block data. Validity and authenticity are assured by verifying that the transaction is properly constructed and that the suppliers of digital assets in each transaction have all cryptographically signed the transaction. This confirms that the digital asset providers for a transaction have access to the private key that allowed them to sign over the accessible digital assets. The legitimacy and authenticity of all transactions in a published block will be checked by the other full nodes, and a block will not be accepted if it includes invalid transactions.

3.4 Mining Pools

In the next chapter, the mining pools will be mentioned so it’s better to specify what it’s all about. When a miner successfully solves a mathematical puzzle, bitcoins are generated but, over time, the puzzles have gotten substantially more complex, and lumpy payouts mean that a single miner now runs the risk of giving resources in the hopes of solving a challenge but receiving no compensation.
As a result, mining pools have emerged, combining the resources of several miners: miners labor separately, but when they succeed, they split their earnings with the rest of the pool (similar to how people pool their money to buy lottery tickets).
AntPool and F2Pool are the two largest pools and, in March 2015, they shared around one-third of Bitcoin mining activity. The decentralization that supports Bitcoin's reliability was compromised by huge mining pools such as GHash, which temporarily had more than 50% of total mining power on multiple occasions, including a twelve-hour period in June 2014, which might have allowed GHash pool owners to undertake manipulations. Also an attacker with a majority of Bitcoin's processing resources can change portions of the system's records, such as introducing fraudulent transactions and rejecting legitimate transactions or violating protocol norms. ([14] Journal of Economic Perspectives)

Chapter IV

Criminality and the future of the Blockchain

4.1 Blockchain fighting crime

For its many opportunities, the blockchain isn't ignored by criminality. In fact Bitcoin receives regulatory scrutiny for three classes of criminal concerns: Bitcoin-specific crime, money laundering, and Bitcoin-facilitated crime.

Bitcoin specific crimes: assaults against the currency and its infrastructure, including bitcoin theft, attacks on mining pools, and denial-of-service attacks on exchanges to manipulate exchange rates, are all examples of Bitcoin-specific crimes. Due to their novelty, lack of clarity as to whose agency or jurisdiction is liable, technological complexity, procedural uncertainty, and limited resources, law enforcement frequently fails to prevent or investigate these crimes.

Money laundering: money laundering using Bitcoin might grow more and become more difficult to track in the future, especially if payments are channeled through mixers, where mixing records are hidden from the public and perhaps unavailable to law enforcement. These qualities may aid criminals in hiding or mischaracterizing their proceeds. However, Bitcoin incorporates design characteristics that may help with fund tracking, such as the publication of the blockchain (which provides permanent publicly accessible records of what funds traveled where).

Bitcoin facilitated crime: Payment for illicit services supplied (or apparently delivered) offline, such as the illegal goods and services sold on Silk Road and payment of funds in extortion. Criminals may be driven to virtual currencies due to a perceived lack of regulatory monitoring, a preference for irreversible transactions, or because they have been banned or evicted from existing payment methods. ([14] Journal of Economic Perspectives)

4.2 A look towards the future

What is the future of Blockchains, Bitcoin and other virtual currencies? To take the place of credit cards for everyday payments? To supplant Western Union and other international cash-transfer companies? To take the place of banks in terms of short-term deposits? Will Bitcoin and other virtual currencies prioritize cheap prices (to undercut rivals), privacy (to accommodate customers who need that advantage specifically), or decentralization (to prevent a single point of control)? Do Bitcoin service providers defend sellers (who want closure) or purchasers (who frequently demand refunds) when disagreements arise? Bitcoin's original vision provided one set of solutions, but as more people use the service, it's becoming less evident that early design decisions suit current needs and it's also unclear if a single provider will be able to meet everyone's demands. Those who want more privacy, for example, may be willing to incur more technological complexity and possibly more expenses. Recruiting mainstream customers and merchants, on the other hand, appears to necessitate a concentration on simplicity and cheaper pricing. Bitcoin's roots may be able to allow a community of experimentation. Mixers have already solved the most prominent privacy issues in Bitcoin's early architecture, while pools assist miners to decrease risk, and wallets address some of the usability and security concerns of users.

The protocol design of Bitcoin has essentially locked in other features of its architecture. The blockchain, for example, is the core of Bitcoin. There is no apparent method for Bitcoin to switch to a new approach to record-keeping while keeping the installed Bitcoin software, staying compatible with intermediate systems, and, most crucially, maintaining the overall consensus that has developed around Bitcoin. Instantaneous transaction confirmations appear to necessitate similar adjustments. Bitcoin will struggle to make improvements in these and other areas.

There are also plenty of rival virtual currencies on the horizon. Litecoin, for example, verifies transactions four times quicker than Bitcoin, which might make it easier to use for retail and other time-sensitive transactions. For example, by replacing proof-of-work mining with proof-of-stake mining and allocating blockchain duties in proportion to currency ownership, NXT minimizes the electrical and computing cost of Bitcoin mining. Zerocash (Ben-Sasson et al. 2014 [16]), which is still in development, will attempt to increase privacy safeguards by masking identities in public transaction histories.

Peercoin provides for an annual increase in the money supply of 1%. Alternative virtual currencies would need to gain trust in their worth and popularity before they could provide their competing

design ideas. Bitcoin profited from early enthusiasm for its service, as well as buyers and sellers on Silk Road and positive news attention but a new virtual currency would struggle to achieve this mix of benefits, and few people would be ready to change existing cash into a competitive coin if growth prospects were uncertain. Whether Bitcoin spreads as its proponent's hope, it remains a fascinating experiment, a research lab, and an appealing method of trade for a select group of businesses and consumers. ([14] Journal of Economic Perspectives)

4.3 Blockchain Applications

Blockchain technology has a wide range of applications and it's vital to remember that bitcoin isn't the same as blockchain; rather, it's one of the most popular uses of the technology. In fact Bitcoin is a cryptographic digital money that is exchanged on a blockchain network that is open, public, and anonymous. Experts, on the other hand, suggest that this technology may be used to identify remedies in a variety of fields, including healthcare, voting, identity management, governance, supply chain, energy resources, and so on. Furthermore, some futurists believe that blockchain will have a comparable impact on the digital world as the internet. We had no clue how the internet would forever affect our lives when it initially came out and no one could have predicted how the Internet would revolutionize the world, from smartphones and text messaging to streaming movies and video chats with loved ones, as well as attending meetings and interviews. In our days, we are still in the early stages of blockchain, and there is still a lot of potential to be unleashed. The areas suggested by experts around the globe, which could have advantages by using blockchain technologies are many but the following ones are the most important:

- **Healthcare:** health services could be revolutionized by distributed ledger technology [17]: drug traceability and patient data management can both benefit from blockchain. In fact, in the pharmaceutical sector, drug counterfeiting is a big issue: according to reports from the Health Research Funding Organization, counterfeit pharmaceuticals account for 10% to 30% of all drugs marketed in underdeveloped nations [18]; according to the WHO, 16 percent of counterfeit pharmaceuticals have inaccurate substances, while 17% contain an inexact quantity of essential constituents. As a result, these treatments may endanger a patient's life because they do not treat the diseases but instead cause side effects that might lead to death. In terms of money, medicine counterfeiting costs European pharmaceutical companies 10.2

billion euros every year [19]. Because all transactions added to the distributed ledger are immutable and digitally timestamped, blockchain may be used to trace products and make information tamper-proof. One more primary problem for the healthcare business is maintaining patient data integrity [20]: because each patient is different in terms of physical characteristics, a treatment method for a common disease differs based on the circumstances. As a result, to provide individualized care, it is vital to have access to a patient's whole medical history. Medical data, on the other hand, is delicate and requires a safe exchange platform. In these days medical records are kept in a system that lacks both privacy and interoperability. Through its immutable ledger technology, blockchain can already provide an infrastructure for the integration of medical records among multiple healthcare institutions, as well as data integrity aspects. Blockchain is also capable of providing a stable and transparent framework for keeping digital medical information, leading to better patient care and lower treatment costs. B Shen et al. introduced MedChain, a permissioned blockchain-based system built on Hyperledger Fabric that gives patients complete control over their own medical information [21]. With this system, patients can use this distributed storage technology to share access to their health information with doctors or health clinics. Deloitte also issued a study on the benefits of blockchain-based healthcare solutions in 2016[22]. The article of this study explains how smart contracts may be used to establish interoperability in the healthcare system, as well as how removing intermediaries can save money and make the system more effective.

- **Energy Industry:** Microgrids are one of the most common uses of blockchain in energy-related applications. First of all, a microgrid is a locally connected and controlled network of electric power sources and loads with the goal of improving energy production and consumption efficiency and reliability [23]. Distributed power generators, renewable energy stations, and energy storage components in facilities built and operated by various organizations or energy suppliers can all be used as electric power sources. One of the key benefits of microgrid technology is that it not only allows residents and other electric power users, such as industries, to obtain the energy they require, but it also allows them to create and sell extra energy to the grid. In microgrids, blockchain may be used to simplify, record, and confirm power selling and purchasing transactions [24]. Similarly, at bigger scales, blockchain may be utilized to facilitate energy trade in smart grids: blockchain can be utilized in smart grids with bidirectional communication flow to provide safe and privacy-preserving

consumption monitoring and energy trade without the need for a central intermediate [25]. Furthermore, blockchain can be utilized in the Industrial Internet of Things (IIoT) to facilitate energy trade [26]because using blockchain for energy-related applications offers the potential to lower energy costs and boost reliability in general.

- **Stock Market:** interoperability, trust, and transparency are all difficulties that fragmented market systems encounter [27] but blockchain technology may be able to address these concerns. All transactions take more than 3 days to complete and finish due to the participation of intermediaries, the regulatory procedure, and operational trade clearance. As a result, stock market members, such as traders, regulators, brokers, and the stock exchange, are subjected to a complex procedure. In this case, blockchain might be the answer: it can improve the stock exchange's efficiency by decentralizing and automating it [28]. Blockchain can also help to cut costs by removing intermediaries and speeding up transaction settlements. Furthermore, the technology has the potential to be useful in transaction clearing and settlement, as well as in reducing the laborious paperwork of trade and legal ownership transfer, as well as in the secure post-trade process. Finally, blockchain also eliminates the need for a third-party regulator by serving as a regulator for all transactions by creating smart contracts.

- **Voting:** Blockchain may be used in a variety of sectors to solve difficulties that a traditional database could have: voting is one example of such an issue. It was recently found that a major voting machine manufacturer in the United States had placed remote access software on certain of its machines [29]: when calculating the totals, this program allowed for the change of votes. Instances such as this create a lack of trust in America's voting system as seen in a recent poll: ''Exclusive poll: Majority expects foreign meddling in midterms''. According to this study, just around a quarter of Americans are confident that their vote is being registered. Blockchain would solve this issue by providing a distributed ledger that would ensure votes are counted since the ledger a voter owns is the same as the one counting the total. [34]

- **Insurance:** blockchain can be used to enable transactions between customers, policyholders, and insurance firms in the insurance business. Insurance businesses may utilize the blockchain to negotiate, acquire, and register policies, file and handle claims, and assist reinsurance

activities. Also smart contracts can automate a variety of insurance plans, lowering administrative expenses dramatically [30]. Processing insurance claims, for example, comes with a considerable administrative expense: due to misunderstandings and misinterpretations of the conditions, the administration of claims may be a highly complicated process in many circumstances. By arranging insurance plans in more specific ‘’if-then’’ connections, smart contracts can avoid these issues. These policies enable the execution of terms to be automated using digital protocols that precisely apply the agreed upon insurance policies, minimizing the work and costs of implementation. Moreover, insurance businesses can lower the cost of their insurance products and become more competitive as a result of this decrease, attracting more clients. Simultaneously, it enables insurance firms to introduce new automated insurance solutions for their customers without having to worry about administrative overhead and expenses. In addition, blockchain allows insurance businesses to operate worldwide.

- **Identity Management:** personal identity may be authenticated in the real world using identification credentials such as a driver's license, national ID card, or passport. However, there isn't much of a comparable framework for protecting online identities. Blockchain might provide a solution to this problem: this technology may be used to build a platform that protects a person's identity against theft and decreases fraudulent activity. Individuals may be able to construct an encrypted identity that does not require a login or password, while still providing more security and control over their personal information. A digital ID may be created by combining identity verification with the decentralized blockchain idea and this ID, which functions similarly to a watermark, may be provided to every online transaction. As a result, confirming identification on every real-time transaction, will assist organizations in detecting and eliminating the risk of fraud. Instead of requiring a username and password or biometric techniques, blockchain-based identity management systems might allow consumers to access and authenticate online payments by just using an app for authentication [31].

- **Trade Finance:** Banks facilitate the trade finance process using a letter of credit (LC) as a payment settlement method, which has been proven effective for risk mitigation [32]. However, because of the complexity of the procedure, high costs, and contractual delays, it still accounts for less than one-fifth of global commerce. When it comes to low-value transactions, the increased time and expense of

issuing LC makes it less advantageous to trading parties: this event disintermediates banks and contributes to the development of free commerce. Blockchain may be able to alleviate these difficulties by automating LC, resulting in lower transaction costs and less operational complexity. The smart contract on the blockchain may be modeled in accordance with all specified conditions in the LC between the supplier and the client, ensuring payment once the trade product is delivered to the buyer. This technique may minimize the time and expense of LC modifications by reducing contractual ambiguities and information conflicts [33]

Conclusion

Blockchain is a revolutionary concept since it has effectively brought transparency to users and has been a game-changer for a variety of sectors. Blockchain promotes entrepreneurship by eradicating corruption, dismantling bureaucratic barriers, and establishing common ownership. This peer-to-peer technology has offered a personal platform for economic empowerment and has opened the door to new possibilities. The technology combines peer-to-peer networks with distributed consensus algorithms to solve traditional distributed database synchronization problems: it's a multifield infrastructure architecture that includes cryptography, mathematics, algorithms, and economic models. Blockchain technology is made up of six main components: Anonymity, Decentralization, Transparency, Open Source, Autonomy, Immutability.

By adopting this technology in different areas such as healthcare or industrial areas, many benefits could be brought. It is too early to predict what lies ahead, but the future of blockchain is bright, and blockchain technology appears to be here to stay.

Bibliography

[1] Wallace, B. (2011, November 23). The rise and fall of Bitcoin. Wired.

[2] US Census Bureau. Percentage of households with a computer at home in the United States from 1984 to 2010. Retrieved from https://www.statista.com/statistics/184685/percentge-of-households-with-computer-in-the-unitedstates-since-1984/

[3] Whitaker, A. (2018b, May 25). The eureka moment that made Bitcoin possible. Wall Street Journal. Retrieved from https://www.wsj.com/articles/theeureka-moment-that-made-bitcoin-possible-1527268025

[4] Haber, S. & Stornetta, W.S. (1991a). How to timestamp a digital document. In A. Menezes & S.A. Vanstone (Eds.)

Haber, S. & Stornetta, W.S. (1991b). How to timestamp a digital document. Journal of Cryptology, 3(2), 99–111.

Haber, S. & Stornetta, W.S. (1992). Method for secure time-stamping of digital documents. US Patent 5,136,647.

Haber, S. & Stornetta, W.S. (1997). Secure names for bit-strings. In Proceedings of the th ACM Conference on Computer and Communications Security (pp. 28–35). New York: ACM. Retrieved from https://dl.acm.org/citation.cfm?id=266430

[5] Burniske, C. & Tatar, J. (2018). Cryptoassets: The innovative investor's guide to Bitcoin and beyond. New York: McGraw-Hill.

[6] Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton, NJ: Princeton University Press

[7] Suberg, W. (2018, May 22). Bitcoin Pizza Day 2018: Community celebrates a takeout order now worth 82$ million. CoinTelegraph. Retrieved from https://cointelegraph.com/news/bitcoin-pizza-day- 2018-community-celebrates-a-takeout-order-nowworth-82-mln

[8] Niranjanamurthy M. and others, (2018) Analysis of Blockchain technology: pros, cons and SWOT

[9] Dennis, R., Owenson, G., Aziz, B.: A temporal Blockchain: a formal analysis. In: 2016 International Conference on Collaboration Technologies and Systems-978-1-5090-2300-4/16 PP 430-437 IEEE (2016)

[10] Singh, S, Singh, N.: Blockchain: future of financial and cyber security. In: 978-1-5090-5256-1/16/PP463-467 IEEE (2016)

[11]Fu, D., Fang, L.: Blockchain-based trusted computing in social network. In: 2nd International Conference on Computer and Communications-978-1-4673-9026-2/16/IEEE (2016)

[12] . Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of Blockchain-based systems for architecture design. In: International Conference on Software Architecture 978-1-5090-5729-0/17 IEEE (2017)

[13] Simanta Shekhar S. (2018) Understanding Blockchain Tecnhnology

[14] Journal of Economic Perspectives – Volume 29, Number 2- Spring 2015- Pages 213-238

[15] Dylan Yaga and others, (2018) Blockchain Technology Overview https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

[16] Ben-Sasson, Eli, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. "Zerocash: Decentralized Anonymous Payments from Bitcoin." Proceedings of the 2014 IEEE Symposium on Security and Privacy, May 18–21, 2014.

[17]] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, ''Blockchain in healthcare applications: Research challenges and opportunities,'' J. Netw. Comput. Appl., vol. 135, pp. 62–75, Jun. 2019.

[18] B. D. Glass, ''Counterfeit drugs and medical devices in developing countries,'' Res. Rep. Tropical Med., vol. 2014, pp. 11–22, 2014.

[19] Counterfeit of Medicines Causes 37, 000 Job Losses in Eu Pharma Industry—ECA Academy. Accessed: May 21, 2019. [Online]. Available: https://www.gmp-compliance.org/gmp-news/counterfeit-of-medicinescauses-37000-job-losses-in-eu-pharma-industry

[20] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, ''MedRec: Using blockchain for medical data access and permission management,'' in Proc. 2nd Int. Conf. Open Big Data (OBD), Aug. 2016, pp. 25–30.

[21] B. Shen, J. Guo, and Y. Yang, ''MedChain: Efficient healthcare data sharing via blockchain,'' Appl. Sci., vol. 9, no. 6, p. 1207, Dec. 2018.

[22] M. Pilkington, ''Can blockchain improve healthcare management? consumer medical electronics and the IoMT,'' Tech. Rep., 2017.

[23] R. H. Lasseter and P. Piagi, ''Microgrid: A conceptual solution,'' in Proc. IEEE 35th Annual Power Electron. Spec. Conf., vol. 6, Jun. 2004, pp. 4285–4291.

[24] A. Cohn, T. West, and C. Parker, ''Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids,'' Georgetown Law Technol. Rev., vol. 1, no. 2, pp. 273–304, 2017.

[25] N. Z. Aitzhan and D. Svetinovic, ‘‘Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams,’’ IEEE Trans. Dependable Secure Comput., vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018

[26] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, ‘‘Consortium blockchain for secure energy trading in industrial Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[27] L. Lee, ‘‘New kids on the blockchain: How bitcoin’s technology could reinvent the stock market,’’ Hastings Bus. Law J., vol. 12, no. 2, p. 81, 2015.

[28] D. Tapscott and A. Tapscott, ‘‘How blockchain will change organizations,’’ MIT Sloan Manage. Rev., vol. 58, no. 2, p. 10, 2017.

[29] Fair Fight Donate Via Actblue. Accessed: May 21, 2019. [Online]. Available: https://secure.actblue.com/donate/fair-fight-reproductive-rights

[30] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, ‘‘Blockchain and smart contracts for insurance: Is the technology mature enough?’’ Future Internet, vol. 10, no. 2, p. 20, Feb. 2018.

[31]] O. Jacobovitz, ‘‘Blockchain for identity management,’’ Dept. Comput. Sci., Ben-Gurion Univ., Beersheba, Israel, Tech. Rep., 2016.

[32] H. Harfield, ‘‘Identity crises in letter of credit law,’’ Ariz. L. Rev., vol. 24, p. 239, 1982

[33] G. Fridgen, S. Radszuwill, N. Urbach, and L. Utz, ‘‘Cross-organizational workflow management using blockchain technology-towards applicability, auditability, and automation,’’ Tech. Rep., 2018

[34] Ahmed Afif Monrat, Olov Schelen (Member IEEE), and Karl Andersson (Senior Member, IEEE) (2019) A Survey of Blockchain from the Perspectives of Applications, Challenges, and Opportunities.

[35] U