Blockchain technology applications and challenges -Bitcoin cryptocurrency model-

تكنولوجيا البلوك تشين التطبيقات والتحديات –عملة البيتكوين نموذجا–

Bencherif Meriem[*]*, Digital Economy Laboratory, University Djilalli Bounaama**(ALGERIA)***
m.ben-cherif@univ-dbkm.dz

Received: 28/02/2023 ; **Revised**: 11/06/2023 ; **Accepted**: 20/06/2023

Abstract:

This study aims to shed light on the clarification of the concept of blockchain technology, and its various applications, with a focus on its use in the Bitcoin digital currency, and mentioning the various challenges facing blockchain technology. The problematic of this study revolves around the various applications and challenges of the blockchain technology, Which was treated through two sections which contain: the theoretical framework of the blockchain by defining this technology, its components and types, in addition to its various applications, especially Bitcoin and its challenges.

The study concluded with a number of results, the most important of which are: Blockchain is a system for recording information very quickly and with high accuracy in a way that makes it difficult or impossible to change or hack the system. Bitcoin is the most used application in the blockchain, but now it is applied in all fields, such as finance, health care and smart contracts. And so on, the blockchain faces many challenges and problems, such as scalability, cost problem, regulatory problem, and loss of privacy.

Key words: Blockchain technology, Bitcoin, hash, block, smart contracts.

Jel Classification Codes : XNN ; XNN

ملخص:

تهدف هذه الدراسة إلى إلقاء الضوء على توضيح مفهوم تكنولوجيا البلوكشين ، و تطبيقاتها المختلفة ، مع التركيز على استخدامها في عملة البتكوين الرقمية ، وأخيراً ذكر التحديات المختلفة التي تواجه البلوكتشين. إشكالية هذه الدراسة تتمحور حول التطبيقات والتحديات المختلفة لتكنولوجيا البلوكشين والتي تمت معالجتها من خلال محورين تطرقنا فيهما إلى الإطار النظري للبلوكشين من خلال تعريف هذه التقنية ومكوناتها وأنواعها بالإضافة إلى تطبيقاتها المختلفة ، وبالأخص البتكوين و التحديات التي تواجه هذه التقنية .

وخلصت الدراسة إلى عدد من النتائج أهمها: البلوكشين هو نظام لتسجيل المعلومات بسرعة فائقة وبدقة عالية بطريقة تجعل من الصعب أو المستحيل تغيير أو اختراق النظام، البتكوين هو التطبيق الأكثر استخداما في البلوكشين ، ولكن الآن يتم تطبيقه في كل المجالات ، مثل التمويل والرعاية الصحية والعقود الذكية وما إلى ذلك ، يواجه البلوكشين العديد من التحديات والمشاكل ، مثل قابلية التوسع ومشكلة التكلفة والمشكلة التنظيمية ، وفقدان الخصوصية.

الكلمات المفتاحية: تكنولوجيا البلوكشين، البتكوين، الهاش، الكتلة ، العقود الذكية.

[*] Auteur correspondant, *m.ben-cherif@univ-dbkm.dz*

I. INTRODUCTION

Blockchain technology is one of the most important topics that raised in the last decade. Blockchain has known wide and remarkable global interest and spread in recent years, given that it is one of the important technologies that are considered one of the elements of the Fourth Industrial Revolution, which will lead to a radical change in the features of the global economy and open new horizons to promote development.

Blockchain is the largest distributed and open digital ledger that allows the transfer of an asset from one party to another at the same time without the need for an intermediary. With a high degree of security for the transfer process in the face of fraud attempts, the Blockchain can be considered as the largest globally distributed database between individuals.

Blockchain was launched in 2008 by Satoshi Nakamoto, a year later, Bitcoin was launched as the first digital currency based on Blockchain. Blockchain technology is the backbone of cryptocurrencies such as Bitcoin and Ethereum, but this technology is not limited to Bitcoin only, but has several applications in various fields like : finance, healthcare, smart contracts, E-ommerce, and others.

Problimatic of study:

To study this subject we can ask the following problematic:

What are the different applications and challenges of blockchain technology?

Objectives of study:

Through this study, we aim to:

- Define Blockchain technology and its different types
- Clarify how blockchain work .
- Mention the various applications of Blockchain technology
- Focusing on the use of the blockchain in the Bitcoin digital currency
- Mention the various challenges facing the blockchain

In this study, we followed the descriptive approach and the analytical approach, which are suitable for this type of studies

In this study, we focused on the theoretical framework of the Blockchain in section 2 by defining this technology, its components, characteristics and different types, as well as its various applications. And the section 3, was about using the blockchain in the digital currency Bitcoin

Finally, we mentioned some challenges facing blockchain.

II. Theoretical framework of blockchain technology

We will focus in this part of the study to shed light on the theoretical literature for the study concerning the concept of blockchain, its characteristics, types, components, basic principles, as well as its various applications.

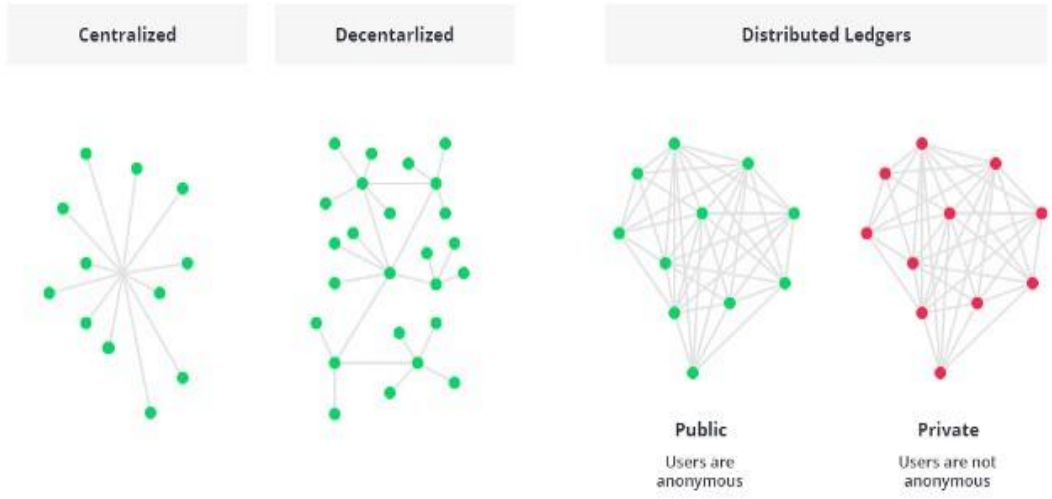
II.1 Definition of Blockchain Technology

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to participant's ledger. The decentralized database managed by multiple participants is known as Distributed Ledger Technology(DLT).

Blockchain is a type of DLT in which transactions are recorded with an immutabal cryptographic signature called a hash.[1]

Figure 1: types of Ledgers



The Source: Blockchain **Architecture Basics: components, structure, Benefits & creation, on line:** https://mlsdev.medium.com/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77, consulted on; 25/12/2022. At 00h15.

The blockchain is a chain of blocks which contain specific information (database), but in a secure and genuine way that it grouped together in a network (peer-to-peer). in other words, blockchain is a combination of computers linked to each other instead of central server, meaning that the whole network is decentralized.[2]

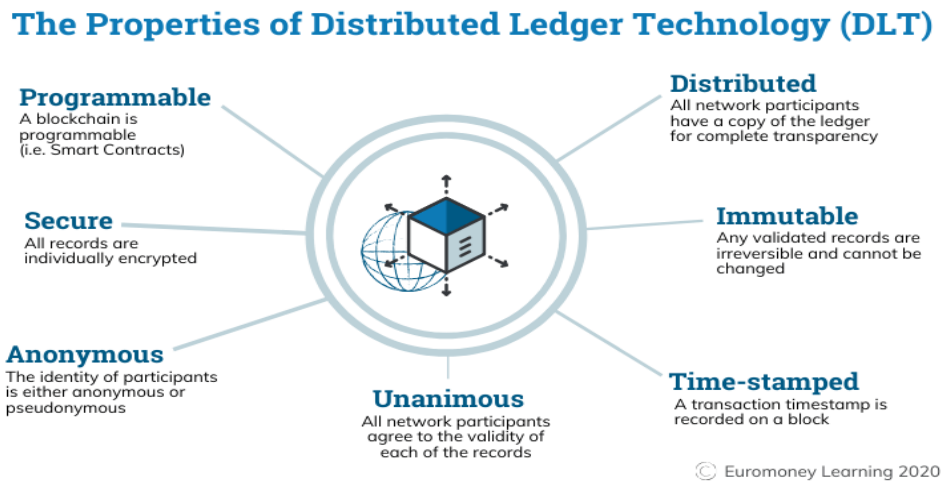
The evolution in the Blockchain has grown up exponentially from 1.0 to 4.0. The evolution originated with Blockchain 1.0 which was limited to store and transfer of value (e.g. Bitcoin, Ripple, Dash) followed by Blockchain 2.0 where its environment is programmable via smart contracts such as Ethereum and Cardano and Blockchain 3.0 in which the technology became applications-centric that reaches to daily lives by facilitating various industries such as healthcare, education, agriculture, e-commerce and many more. Next, Blockchain 4.0 removes almost all the limitations in the previous Blockchain. In Blockchain 4.0, it utilizes a distributed environment suffering from major issues like scalability and limited transaction per second. It has handle scalability, throughput, and latency.[3]

Figure 2 :Database blockchain system

The Source: Blockchain Architecture Basics: components, structure, Benefits & creation, op it.

We can illustrate the properties of Distributed Ledger Technology by the figure below:

Figure3: The properties of Distributed Ledger Technology

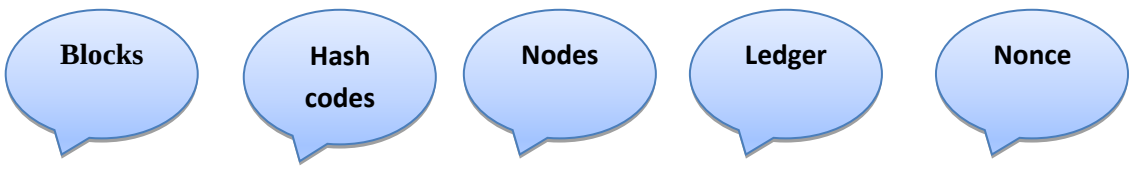


The Source: Blockchain explained ,What is blockchain? ,Euromoney Learning, 2020

This means if one block in one chain was changed, it would be immediately apparent it had been tampered with. If hackers wanted to corrupt a blockchain system, they would have to change every block in the chain, across all of the distributed versions of the chain.[4]

II.2 components of blockchain technology:

Blockchain has many powerful components that play an excellent role in storing and securing data. Let's discuss the components of blockchain in a detailed way below:[5]



II .2.1 Blocks:

blocks are the backbone of blockchains. You can store data in blocks permanently but cannot change or delete it after it is stored. Once a block is filled with the data of transactions, then it will be linked with previous blocks. Every block will have information such as block size, transaction counter, block header, the previous block's hash, timestamp, and transaction data.[6]

And this can be illustrated by the table 1.

Table 1: components of a block in the blockchain

Component	Meanimg
Data and transactions	The first element is data and transactions. A transaction in blockchain means an interaction between two entities. In case of cryptocurrencies, the transfer of bitcoin or any cryptocurrencies from one user to another is called as transaction .The data includes in a transaction generally are transaction input, output, sender's address, sender's public key, and digital signature..
Hash	Each block also includes a Hash- a unique identifier for the block and all of its contents.
Hash of the previous block:	Another important element that every block contains is the hash of the previous block. This piece of information is what links one block to another and makes the whole network safe and secure.
Timestamp	means "a proof that some data existed at a particular date and time." In other words, the timestamp can be referred to as "Proof of existence." Any digital data can be timestamped. The hash of the block containing data and transactions is timestamped and is then published on the network. By doing so, it is ensured that the transactions have existed at this point in time.
Nonce	The fifth element of a block is nonce. The nonce is an abbreviation for "number only used once." The Nonce is an integer number that, along with the block number, data, and previous hash, serves as an input for the hashing algorithm to calculate the valid hash for the block

The Source; author elaboration based on:

Techskill Brew (2021) , What is a block n the blockchain? (part-2 blockchain series), https://medium.com/techskill-brew/what-is-a-block-in-the-blockchain-part-2-blockchain-basics-53ad20c766cc**. Consulted on 28/12/2022.**

Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain, Blockchain Technology: Applications and challenges (2021), Springer Nature, Switerland, p4.

II.2.2 Hash Codes:

It is one of the vital security features used in blockchain technology. In its basic form, a hash code has a fixed length. It helps to ensure that no one can crack blockchains or alter block data. You can use Hash codes to verify the integrity of transactions as well as authentication. You can add new blocks only after solving hash codes. Note that it must generate the same output whenever you apply the hash function in data in a block. If not, it means that the data in the block is modified.[7]

II.2.3 Nodes:

Nodes validate and relay transactions and blocks to other nodes. They also maintain a copy of the Blockchain and help to keep the network secure.[8]

Nodes are storage units that store vast amounts of blockchain data. nodes can be computers, servers, and laptops. All nodes are connected in a blockchain network. If any change is made in the blockchain's data, nodes can detect it quickly. There are two types of nodes such as full nodes and light nodes or partial nodes.[9]

- **Full Nodes:** a full node stores the complete copy of a blockchain. Full nodes usually have more memory than light nodes. They can accept, reject, and validate transactions.
- **Light Nodes:** they don't copy all the blocks in the blockchain. Instead, they only store the recent blocks and access older ones only when users request the same. They maintain the hash code of transactions. You can access data only after solving the hash code.

II .2.4 Ledger:

Essentially, this component of a blockchain resembles a record-keeping mechanism. There are three types of ledgers: public, decentralized and distributed:[10]

- **Public Ledger:** In this type, anyone can access ledgers since it is open to all blockchain network participants. There is no central authority in this public ledger type. And it allows transactions only after verifying the identity of users.
- **Distributed Ledger:** In distributed type, all the nodes will have a copy of databases. A group of nodes will manage the tasks. You can access all the information stored in this ledger using cryptographic signatures and keys.
- **Decentralized Ledger:** In this type, no participant needs to trust others or know their [2]identities. This ledger lessens reliance on specific authorities that manage the network. It brings consistency and improves performance by decentralizing resources.

II.2.5 Nonce:

A nonce is an abbreviation for “number only used once,” which is a number added to a hashed or encrypted block in a blockchain. It is the 32-bit number generated randomly only one time that assists to create a new block or validate a transaction. It is used to make the transaction more secure.

It is hard to select the number which can be used as the nonce. It requires a vital amount of trial-and-error. First, a miner guesses a nonce. Then, it appends the guessed nonce to the hash of the current header. After that, it rehashes the value and compares this to the target hash. Now it checks that whether the resulting hash value meets the requirements or not. If all the conditions are met, it means that the miner has created an answer and is granted the block.[11]

II.3 Main concepts of blockchain:

At the top level, widely-known cryptographic like hashing, asymmetric key cryptography, digital signatures combined with principals in record keeping are used in blockchain technology. Some of the key components like Addresses Blocks, transactions, hashing and digital signatures are explained below in detail.[12]

II .3.1 Hashing methods:

Hashing is a cryptographic technique which simply converts a data of any size into a unique fixed size output. The input can be a text, file or image and the output is fixed size alpha-numeric string. Hashing in blockchain assure the users that the data transmitted is not changed. This can be done by comparing the hash values of the input data. That is, any minor change in the data will result in deferent hash values. The reason hashing technique used in blockchain is due to its security property. Pre-image resistant: hashing techniques are uni-directional. It is not possible to compute the input based on the output, second preimage resistant: based on the input given, it is impossible to compute the second output that generates the same output, collision resistant: it is highly infeasible to find two input generating same hash output.
Most of the blockchain implementations uses secure hashing Algorithm (SHA) that generates an output of size 256-bits.[13]

II. 3.2 Public key cryptography:

Public key cryptography otherwise called as Asymmetric key cryptography is used in blockchain for various operations. Asymmetric key namely public and private key which are computationally related to each other. The public key can be viewed by anyone whereas private key is kept secret. However it is not possible to compute the private key using the openly available public key .

At the same time, it possible to encrypt the data using a private key and can be decrypt using the corresponding public key.[14]

II.3.3 Address and wallet:

Addresses are usually a short alphanumeric character used as a sender and receiver's transaction point. A hash function is used to derive user's public key. The deferent users of blockchain network have to store their private keys in a secure place. Instead of storing them manually, software is used to store them. The software used to store the private keys is called as wallets. A part from private keys the wallets can store the user's address ad public keys as well. Wallets are used to calculate the number digital assets owns by a particular trusted user.[15]

II.3.4 Consensus mechanism:

There are several consensus models being used such as Proof of Work((PoW), Proof of Stake (PoS), Proof of Authority (PoA), Proof of Elapsed Time(PoET) etc.

The consensus mechanism is a proc ess of decision making where the network users agree and support a decision for the betterment of the network.[16]

II.3.5 Merkle trees:

Merkel trees are used for the efficient storage and verification of large data sets. In this type of data structure, leaf nodes contain the hash of the blockchain transaction, while non-leaf nodes contain the cryptographic hash of the labels of their child nodes. The root of the tree, also known as the Merkle root, contains the hash of all the transactions in a block . The Merkle tree's root is a commitment value, and it may alternatively be thought of as a vector commitment. The Merkle tree's leaf nodes collectively convey the message. An opening proof of vector commitment is formed by every sister node along the route from the leaf node

to the root node, and by the leaf nodes themselves. A traditional blockchain verifies the data's accuracy and consistency by using the opening proof of the Merkle tree.[17]

II.4 Types of blockchain:

There are four main types of blockchain networks: public blockchains, private blockchains,
consortium blockchains and hybrid blockchains. Each one of these platforms has its benefits, drawbacks and it uses. Sometimes, organizations will want the best of both worlds, and they'll use hybrid blockchain,a type of blockchain technology that combines elements of both private and public blockchain. It lets organizations set up a private, permission-based system alongside a public permissionless system, allowing them to control who can access specific data stored the blockchain, and what data will be opened up publicly.[18]

The main types of blockchain will be explained below:[19]

- **Public Blockchain:** A public blockchain architecture means that the data and access to the system is available to anyone who is willing to participate (e.g Bitcoin, Ethereum, and Litcoin Blockchain systems are public.
- **Private Blockchain :** As opposed to public blockchain architecture, the private system is controlled only by users from a specific organization or authorized users who have an invitation for participation.
- **Consortium Blockchain:** This blockchain structure can consist of a few organizations. In a consortium , procedures are set p and controlled by the preliminary assigned users.

Table2 :Differences between types of blockchain

Property	Public blockchain	Private blockchain	Consortium blockchain
Consensus determination	All miners	Selected set of nodes	Within one organization
Read permission	Public	public or restricted	public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Effitiency (use of resources)	Low	High	High
Centralization	No	Partial	Yes
Consensus process	Perissionless	Needs permission	Needs permission

The Source: Ravi Kumar Mathur, Introduction to Blockchain Technology, available at ; https://ntiprit.gov.in/pdf/blockchainanddistributed/Blockchain_Introduction_KR.pdf, consulted on 13/01/2023.

II. 5 How blockchain works?

Procedures of blockchain work are as follow:[20]

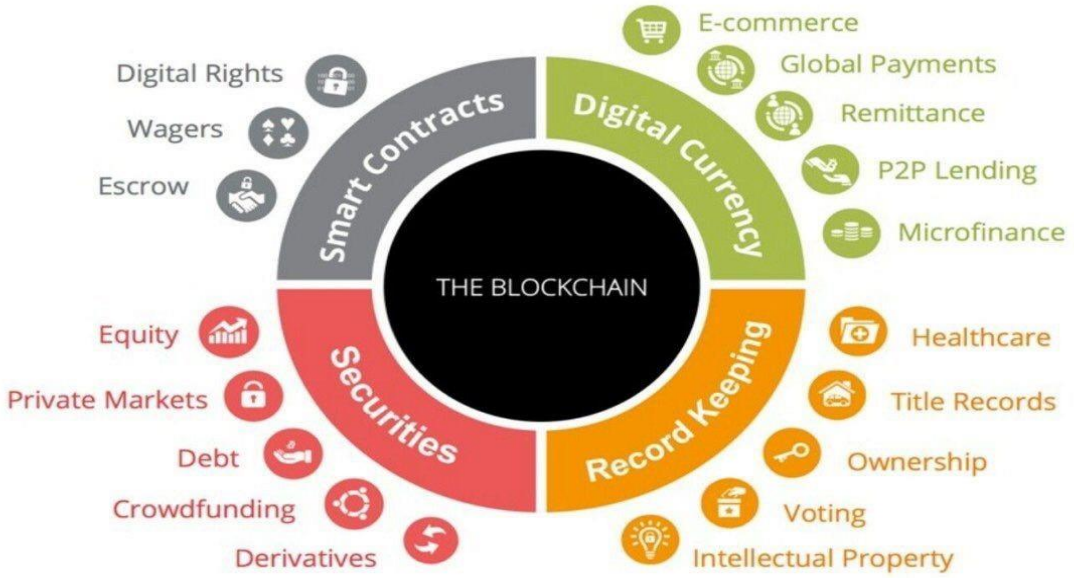
- Whenever any blockchain nodes send a new block data or an update comes in the chain, consensus algorithm broadcasting that change to network. Majority present in the chain to verifies the present blockain and check the history of that block.
- All nodes that receive new block in network perform execution algorithm of proof of work(PoW) or proof f stake(PoS) as it implemented in blockchain that block.

- If the majority of nodes in the chain approves that received changeis legal, then the present block is added to the chain or update stored to a block of blockchain.
- If the majority of nodes in the chain does not approve the received change(i.e addition or validation of block then that change will be discarded.
- Distributed consensus algorithm permits blockchain to be distributed ledger. It means that is no need of centralized database d all nodes in blockchain network prove this blockand will incessantly extend the chain on this blockchain.

II.6 Applications of blockchain technology:

The figure below illustrates the deferent applications of the blockchain:

Figure 4: deferent applications of the balockchain



The Source: Thijs Maas (2017), Blockchain the 3 Core Components, https://www.linkedin.com/pulse/blockchain-3-core-components-thijs-maas. Consulted on 28/12/2022.

Bitcoin is the most commonly used application using blockchain technology. But now days it is applied in almost every filed, like finance, ownership, healthcare, smart contracts, E-commerce…etc:

II.6.1 Smart contracts:

The smart contract is a computer program based on transaction protocol that executes the term of a contract. Smart contracts allow the execution of programs without the intervention of any third party. The sale of goods or services can be realized through a transaction, cryptically signed by the seller and the purchaser, and joining a smart contract for sales transactions.[21]

Smart contract systems based on distributed cryptocurrencies enable mutually distrustful parties to conduct secure transactions without the use of trusted third parties. The decentralized system guarantees that only honest parties participate are compensated fairly in the event of contractual violations or aborts. Existing schemes, on the other hand, do not have transactional privacy. On the blockchain, all transactions are visible, involving the flow of money among pseudonyms and the amount transacted.[22]

II.6.2 Healthcare:

The Healthcare industries are very much attracted by Blockchain Technology as it is a sensitive field that requires reliability and efficiency . There is a dire need of tracking and storing the medical data obtained from patients and predicting medicines or possibilities of curing some disease based on that data where a small mistake can make the results lethal. With the help of Blockchain, the data can easily be available to use without getting it mixed.[23]

II.6.3 Finance and Cryptocurrencies:

Finance is the section where the Blockchain is being used mostly and largely and it starts with

the emergence of Bitcoin which uses the Blockchain Technology to make the transactions direct and digital, eliminates the middlemen & keeps a record of all the transactions in a digital ledger which is further used to trace any of the transactions . Blockchain Technology and Bitcoin cultivated many other cryptocurrencies in the whole world that's why the world trade in hundreds of cryptocurrencies(Bitcoin, Etherium, Ripple…) these days.[24]

II.6.4 Internet of Things:

The term "Internet of Things (IoT)" is referred to a network of resources or devices as well as some sensors that are linked through the internet and share the necessary information among them just to provide us an easier lifestyle. Linked devices & other gadgets in factories provide the capability for a fourth industrial revolution and it is predicted that more than half of new ventures will be running on the Internet of things (IoT) by 2021. The Internet of Things has undoubtfully made the surroundings smart and easier as well as they exposed us to vulnerabilities).Blockchain Technology provides a foolproof and decentralized industrial system associated with IoT.[25]

II.6.5 Private securities:

It is very expensive to take company public. A syndicate of banks must work to underwrite the deal and attract investors. The stock exchanges list company shares for secondary market to function securely with trades settling and clearing in a timely manner. It is now theoretically possible for companies to directly issue the shares via the blockchain. These shares can then be purchased and sold in a secondary market that sits on top of the blockchain.[26]

II.6.6 Anti-Money Laundering and know your customer:

"Know Your Customer" (KYC) and "Anti-Money Laundering"(AML) are two widely recognized practices that stand to benefit from blockchain innovation. Monetary establishments currently need to finish a concentrated multi-step KYC/AML measure for every customer, which is extremely expensive. If the blokchain were brought into this cycle, it could decrease costs by running a KYC/AML check on a given costumer once and making the outcomes accessible to every monetary organization while also expanding the proficiency of examination and observation.[27]

II.6.7 Transparent management

Straightforwardness is fundamental when you work for a business, and in this specific circumstance; blockchain innovation is changing the administration scene. As the blockchain's circulated data set innovation empowers straightforward and available agreements, associations are nearly on blockchain-based choices. For example , Ethereum-based brilliant agreements are used to help resources or hierarchical data for executives to use.[28]

II.6.8 Hyperledger:

Hyperledger is not a crypto currency, a blockchain or a company. It is the project under Linux Foundation.it is the open source umbrella project of development blockchain, where individuals and company from all over the world can help in developing heperleder and build specialized blockchain platforms and tools as a software and as platform to different industry use cases. Hyperledger Fabric is mast mature robust and popular open sourced community of communities of all hyperledger platforms.[29]

II.6.9 Information systems:

The blockchain provides a secure autonomous, and cost-effective proof-of- concept system that ensures that entries cannot be moved or changed. The blockchain technology can reduce costs and increase accuracy while exchanging and storing vast amount of data.[30]

II.6.10 Governmental services:

Using blockchain based distributed ledgers to manage registries give the necessary transparencies to reduce fraud while also allowing for real-time modifications.

Blockchain-based administration solutions allow for real-time collaboration cross a wide range of stakeholders while also providing the necessary transparency.[31]

II.6.11 Defense:

Information which is strongest foundation of any country is also critical to national security which is like defense infrastructure and computer system. Because of his blockchain comes and plays an important part, it is distributed across different locations to prevent unauthorized access and alteration. Blockchain can be used as advantage to provide consent based access for altering data and distributing access over different system resources such as hardware equipment, data center's and networks.[32]

III. Bitcoin Blockchain: Use case

Blockchain was used for the first time in Bitcoin cryptocurrency, so we will focus in this part of the study on Bitcoin Blockchain

III.1 Short history of Bitcoin:

In year 2008, an individual or group writing under the name Satoshi Nakamoto published a paper entitled" Bitcoin: A Peer-To- Peer Electronic Cash System". This paper described a peer-to-peer version of the electronic cash that would allow online payments to be send directly from one party to another without going through a financial institution. Bitcoin was the first realization of this concept, Now world cryptocurrencies is the label that is used to describe all networks and mediums of exchange that uses cryptography to secure transactions- as against those systems where the transactions are channeled through a centralized trust entity.

The author of the first paper wanted to remain anonymous and hence no one knows Satoshi Nakamoto to this day. A few months later , an open source program implementing the new protocol was released that began with the Genesis block of 50 coins. Anyone can install this open source program and become part of the Bitcoin peer- to- peer network. It has grown in popularity since then. [33]

-2008

- August 18 Domain named "bitcoin.org" registered.
- October 31 Bitcoin design paper published.
- November 09 Bitcoin project registered at SourceForge.net

-2009

- January 3 Genesis block established at 18:15,05 GMT
- January 9 Bitcoin v0.1 released and announced on the cryptography mailing list.
- January 12 First Bitcoin transaction, in block 170 from Satoshi to Hal Finney.

The popularity of the Bitcoin has never ceased to increase since then. The underlying BlockChain technology is now finding new range of applications beyond finance. [34]

III.2 Definition of Bitcoin cryptocurrency:

A cryptocurrency is a digital asset designed to work as a medium of exchange using cryptography to secure transactions, to control the creation of additional value units, and to verify the transfer of assets. Many different cryptocurrencies exist. [35]
Cryptocurrencies are digital tokens. They are a type of digital currency that allows people to make payments directly to each other through an online system. Cryptocurrencies have no legislated or intrinsic value. They are simply worth that people are willing to pay for them in the market. There are a number of cryptocurrencies- the most well-know of these are Bitcoin and Ether.[36]

Cryptocurrency received its name because it uses encryption to verify transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers. The aim of encryption is to provide security and safety.[37]

Bitcoin is a decentralized digital currency network that employs blockchain technology to facilitate digital transfers of value, without the need for a centralized or trusted middelman.[38]

Bitcoin is an open- source, peer to peer digital currency. Among many other things, that makes Bitcoin unique is that it is the world first completely decentralize digital-payments system.[39]
Bitcoin is secured with the SHA-256 algorithm, which belongs to the SHA-2 family of hashing algorithms, which is also used by its fork Bitcoin Cash (BCH), as well as several other cryptocurrencies.[40]

Some differences between Bitcoin and traditional currencies are illustrated in the table below.

Table3: Differences between Bitcoin and traditional currencies

	Bitcoin	**Traditional Currency**
Tangibility	It is a virtual currency and can only be used in its digital form	It is a physical currency in the form of notes and coins. However, we can use it in both physical and digital forms.”
Regulation	Issued through mining and controlled by a decentralized distributed network of computers	Issued and controlled by central government authorities, i.e., central banks. Owing to this, the traditional currency is the legal tender in the country governed by the issuing authority.
Governance	Governed by a consensus mechanism in which the majority rules	Purely governed by the central bank
Value	Value is backed by the trust of its users. The more users are willing to transact with Bitcoin, the more stable it becomes.	Value is determined by forces of supply and demand and is thus vulnerable to inflation

Supply	Capped at 21 million bitcoin	Fiat currency has no supply limit
Validation of transactions	Bitcoin transactions are validated using blockchain technology and so do not require an intermediary for validation	Transactions involve an intermediary such as a bank or a payment provider
Transaction fees	Minimal or no associated fees as intermediaries have been eliminated	Transactions attract considerable charges
Transaction time and speed	The transaction is almost always instantaneous or greatly depends on the network speed	Transactions may take time before verification or before they reflect on the system
Security	The concepts of decentralization, cryptography, and consensus guarantee a secure network and security of bitcoin transactions	Less secure as it can be negatively affected by fluctuations in government policies
Reversals	Bitcoin transactions cannot be charged back, reversed, or canceled	Chargebacks, reversals, and cancellations are commonplace with traditional currency transactions

Source: Shivam Arora(NOV 18,2022), What is Bitcoin Mining? How Does It Work, Proof of Work and Facts You Should Know, https://www.simplilearn.com/bitcoin-mining-explained-article, consulted on 10/01/2023.

Blockchain and Bitcoin are two completely separate things[41]: there are some differences illustrated in the table below:

table 4: Differences between blockchain technology and Bitcoin

BITCOIN	BLOCKCHAIN
Bitcoin is a cryptocurrency	blockchain is a distributed database
Bitcoin is powered by blockchain technology	blockchain has found many uses beyond Bitcoin.
Bitcoin promotes anonymity	blockchain is about transparency. To be applied in certain sectors (particularly banking), blockchain has to meet strict Know Your Customer rules.
Bitcoin transfers currency between users	blockchain can be used to transfer all sorts of things, including information or property ownership rights.

The Source: realized by the researcher based on:
Bernard Marr, What is the Difference Between Blockchain And Bitcoin?, https://bernardmarr.com/what-is-the-difference-between-blockchain-and-bitcoin/, consulted on 10/01/2023.

III. 3 What is bitcoin mining?

Bitcoin mining is the process of creating new bitcoins by solving extremely complicated math problems that verify transactions in the currency. When a bitcoin is successfully mined, the miner receives a predetermined amount of bitcoin.[42]

Mining is the process that maintains the bitcoin network and also how new coins are brought into existence. All transactions are publicly broadcast on the network and miners bundle large collections of transactions together into blocks by completing a cryptographic calculation that's extremely hard to generate but very easy to verify. The first miner to solve the next block broadcasts it to the network and if proven correct is added to the blockchain. That miner is then rewarded with an amount of newly created bitcoin.

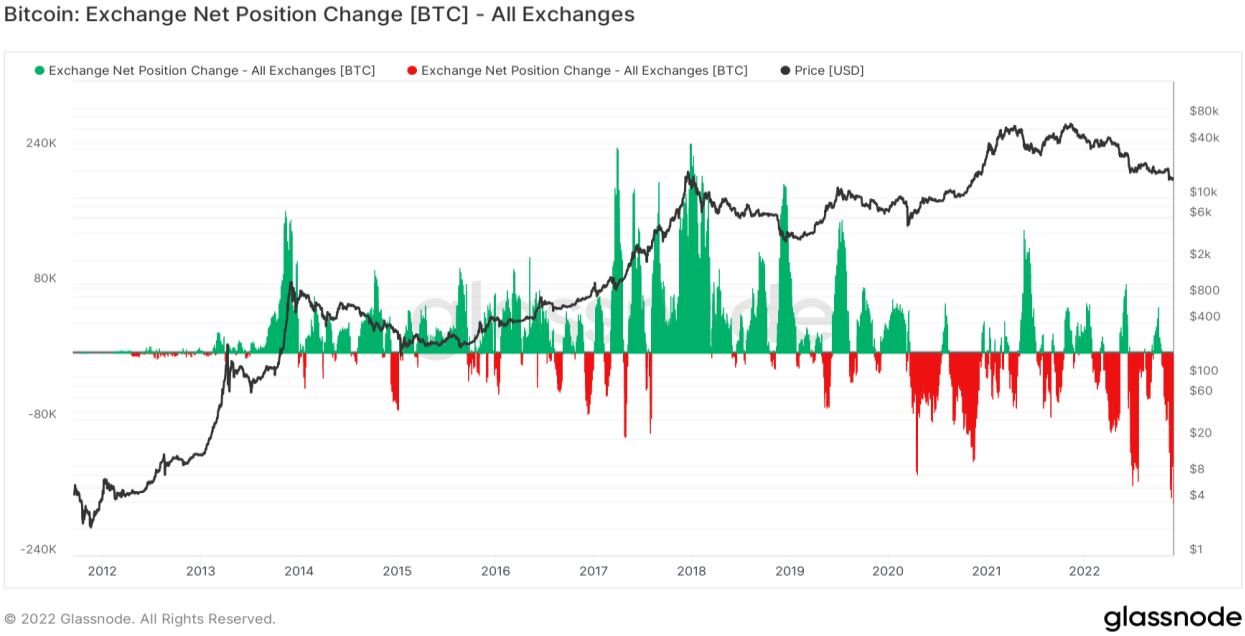
Inherent in the bitcoin software is a hard limit of 21 million coins. There will never be more than that in existence. The total number of coins will be in circulation by 2140. Roughly every four years the software makes it twice as hard to mine bitcoin by reducing the size of the rewards.[43]

Bitcoin mining is the process by which Bitcoin transactions are validated digitally on the Bitcoin network and added to the blockchain ledger. It is done by solving complex cryptographic hash puzzles to verify blocks of transactions that are updated on the decentralized blockchain ledger. Solving these puzzles requires powerful computing power and sophisticated equipment. In return, miners are rewarded with Bitcoin, which is then released into circulation hence the name Bitcoin mining.[44]

III. 4 Some statistics about bitcoin and Blockchain:

Over the last 30 days , the change of supply held in exchange wallets dropped by a net 170,000 bitcoin. These are the highest-ever outflows from exchanges in bitcoin's history.[45]

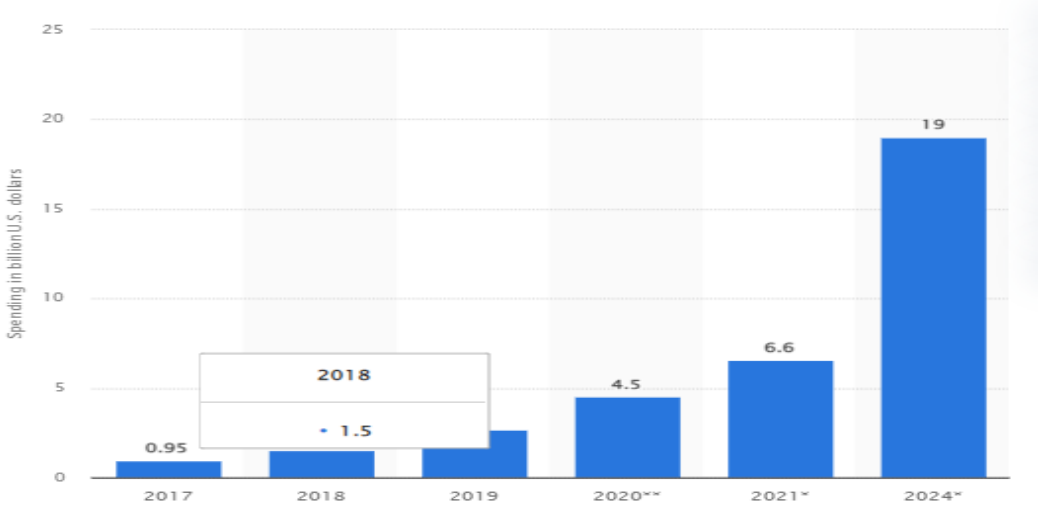
Figure 5: Bitcoin exchange net position change- All exchange



The Source: WILLIAM SUBERG (NOV 24, 2022), Bitcoin exchanges see 180K BTC supply decrease amid Mt. Gox BTC sales, available at; https://cointelegraph.com/news/bitcoin-exchanges-see-180k-btc-supply-decrease-amid-mt-gox-btc-sales, consulted on 10/01/2023.

Research published by the Statista Research Department found global spending on blockchain solutions accelerated from 4.5 billion to 6.6 billion in 2021. In the years to come, increasing demand for security with digital identities and Web 3.0 is set to increase demand for blockchain. By 2024, Blockchain spending is set to increase to around $19 billion, with more businesses leveraging the technology across data validation, data access, and identity protection strategies.[46] The figure below illustrates the Worldwide spending on blockchain solutions during 2017-2024

Figure 6: Worldwide spending on blockchain solutions during 2017-2024



The Source: Rebekah Carter (5, 2022), The Ultimate List of Blockchain Statistics (2023) available at; https://findstack.com/resources/blockchain-statistics/, consulted on 11/01/2023.

This figure clarify the increase of the worldwide spending blockchain during the period of 2017-2024, from 0.95 billion US dollars in 2017 to 6.6 billion US dollars in 2021. and by 2024, Blockchain spending is set to increase to around $19 billion, an increase of more than three times compared to 2021, This is due to the widespread in blockchain technology in different filed especially in cryptocurrencies and finance.

Here are some key statistics about blockchain and cryptocurrency: [47]

- Worldwide spending on blockchain solutions amounted to $6.6 billion in 2021.
- It's projected that companies will spend almost $19 billion on blockchain technology in 2024.
- Over 300 million people, or 3.9% of the global population, use blockchain for cryptocurrency.
- 90% of U.S., Canadian and European banks have started exploring blockchain technology.
- There are over 82 million Bitcoin wallets in the world.

There have been several criticisms of bitcoin, including that the mining system is enormously energy hungry. The University of Cambridge has an online calculator that tracks energy consumption and at the beginning of 2021 it was estimated to use over 100 terawatt hours annually. For perspective, in 2016 the United Kingdom used 304 terawatt hours in total.

The cryptocurrency has also been linked to criminality, with critics pointing out to it being a perfect way to make black market transactions. In reality, cash has provided this function for centuries, and the public ledger of bitcoin may actually be a tool for law enforcement.[48]

III.5 Challenges of blockchain technology

As an emerging technology, blockchain is facing multiple challenges and problems.

Scalability, cost problem, regulatory problem, and loss of privacy, which we will summarize it in the table below:

Table 5 :Blockchain challenges

challenges	
scalability	as the number of transaction increases, the chain of blockchain will growing, loading of computing and store will also become more difficult. A lot of computing power and time it will be taken synchronize data, at the same time, chain still continually get bigger and bigger which brings problems to clients when running blockchain.
Cost problem	A lot of costs including time and money it will have pay to change current system, particularly when it's an infrastructure.
Regulatory problem	Use Bitcoin for example, the characteristics of decentralized system , will weak the central bank's ability to control the economic policy and the amount of money, that makes government be cautious of blockchain technologies.
Loss of privacy	In blockchain a considerable amount of privacy is maintained by using public key cryptography mechanism in tractions to keep the user identity anonymous . however the transactional anonymity cannot be assured by blockchain because the identities of all transactions and balances for each cryptographic key are publicly accessible.
Criminal activities	The absence of stringent legislation and the fact that blockchain is still a developing technology have fueled the rise of fraudulent projects and other bad actors seeking to profit from inexperienced investors. There have also been several high-profile cryptocurrency exchange thefts, including Mt. Gox's infamous bitcoin theft in 2014, nearly destroying the entire cryptocurrency industry.

The Source, author elaboration based on:
Mustafa A, Ali and Wesam S bhaya (2020), op cit.
Ajay Kumar, Sujata Priyamada Dash, Blockchain Technology: Introduction, Applications, Challenges, p9,https://www.researchgate.net/publication/351346456_Blockchain_Technology_Applications_and_Challenges, consulted on 09/02/2023.
Eray eliacik, blockchain brings tough challenges befitting revolution, May,30, 2022, https://dataconomy.com/2022/05/blockchain-implementation-challenges/#51_attacks, consulted on 09/02/2023.

IV. CONCLUSION

Blockchain technology has become widespread in recent years and there is a growing world trend to adopt this technology because it provides several advantages such as the transparency and the lower transaction costs.
Through this study, we conclude to the following results:

- Blockchain is the largest distributed and open digital ledger that allows the transfer of an asset from one party to another at the same time without the need for an intermediary. With a high degree of security for the transfer process in the face of fraud attempts.

- Blockchain is a system of recording information-Super fast and whith high accuracy in a way that makes it difficult or impossible to change, hack, or cheat the system.
- Blockchain has many powerful components that play an excellent role in storing and securing data; blocks, hash codes, nodes, ledger; nonce. And every block will have information such as block size, transaction counter, block header, the previous block's hash, timestamp, and transaction data.
- Bitcoin is the most commonly used application using blockchain technology. But now days it is applied in almost every filed, like finance, ownership, healthcare, smart contracts, E-commerce…etc.
- Blockchain has witnessed a wide spread recently in different filed, especially in cryptocurrencies, like Bitcoin. As an emerging technology, blockchain is facing multiple challenges and problems. Scalability, cost problem, regulatory problem, and loss of privacy.
- Lack of sufficient knowledge of blockchain technology is an obstacle for countries to adopt this technology.

So, We can cite the following recommendations:

- ❖ Seeking to understand blockchain technology very well in order to activate it in various economic fields.
- ❖ Work on developing this technology to reach maturity to benefit from its advantages and avoid its risks.
- ❖ Finding effective solutions to the challenges faced by the Blockchain, especially the challenge of scalability and attacks.

Bibliography List :

Books :

- Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain (2021), Blockchain Technology: Applications and challenges, Springer Nature, Switzerland.
- A C Sountarraj, Michael Raj TF(2021) ,The science and the secret of blockchain technology, Sankalp Publication, France.
- Mustafa A, Ali and Wesam S bhaya, Blockchain technology's applications and challenges: An overview(2020), AIP Conference proceeding 2290, 040019.
- Jerry Brito ,Andrea Castillo(2013) , BITCOIN A Primer for policymakers, MERCATUS CENTER, George Mason University.

Journal articles :

- Bila Shrimali, Hiren B.Patel (2021), Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities, Journal of King Saud University –computer and Information sciences.
- Gousia Habib, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Chaima Qureshi(2022), Blockchain technology: benefits, challenges, applications ,and integration of blockchain technology with Cloud Computing, " Future Internet, MDPI, vol. 14(11).
- Maher Fuad Abu Farhah(2022), The Blockchain: The Next Technological Revolution in The world of the Economy, journal of Economic, Administrative and Legal Science, Volum 6, issue 15.
- Pervez Ahmed, Muhammad Ahmed, Usman Ahmed Raza, A review on Blockchain's applications and implementations(2021), ADCAIJ Advances in Distributed Computing and Artificial Intelligence Journal, VOL 10, No 2.
- Muhammad Nouman, Muhammad Azam, Ahsan Rehman Gill (2022) , Systematic Review of Blockchain Technology in Current Epoch: Applications, Adoption Challenges, and Opportunities, University Faisalabad, Pakistan, preprint .
- Vipul H.Navadkar, Ajinkya Nighot, Rahul Wantmure (2018), Overview of Blockchain Technology in Gouvernment/Public sectors, Intrnational Research Journal of Engineering and Technology (IRJET), Volume 05, Issue 06.

Internet websites:

- Blockchain explained ,What is blockchain? ,Euromoney Learning, 2020 , on line, https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain, consulted on 24/12/2022, at 18h09.
- Blockchain Architecture Basics: components, structure, Benefits & creation, on line: https://mlsdev.medium.com/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77, consulted on ; 25/12/2022.
- SaiKumar Kalla(2022), Components of Blockchain, https://mindmajix.com/components-of- blockchain, consulted on 27/12/2022
- Great Learning, What is Blockchain Technology(2022), https://www.mygreatlearning.com/blog/what-is-blockchain-technology/, consulted on : 12/01/2023.
- Components of blockchain Network, available at , https://www.geeksforgeeks.org/components-of-blockchain-network/,consulted on 13/01/2023.
- Ravi Kumar Mathur, Introduction to Blockchain Technology, available at ; https://ntiprit.gov.in/pdf/blockchainanddistributed/Blockchain_Introduction_KR.pdf, consulted on 13/01/2023.
- Moez Krishen, Meryem Ammi, Alaeddine Mihou and Mutiq Almutiq(2022), Blockchain for Modern Applications: A Survey, Sensors 2022, 22, 5274.https://www.mdpi.com › pdf, , consulted on 31/12/2022.
- Michael Crosby, Nachlappan, Pradhan Pattanayak, BlockChaine Technology Beyond Bitcoin, working paper , University of California, October 16, 2015. P5 . on line , https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf, consulted on 24/12/2022.
- Wolfgang KARL Hardel , Compbell R. Harvey, Raphael C. G . Reule(3rd August 2019), Understanding Cryptocurrencies, International Research Technology Group 1792Discussion paper 2018/-44, p3. https://ies.keio.ac.jp/upload/20191125econo_Wolfbang_wp.pdf. Consulted on 01/01/2023.
- RESERVE BANK OF AUSTRALIA, Digital Currencies, https://www.rba.gov.au/education/resources/explainers/pdf/cryptocurrencies.pdf, consulted on 01/01/2023.
- Bernard Marr, What is the Difference Between Blockchain And Bitcoin?, https://bernardmarr.com/what-is-the-difference-between-blockchain-and-bitcoin/, consulted on 10/01/2023.
- Brian baker(2022), what is bitcoin mining and does it work?, https://www.bankrate.com/investing/what-is-bitcoin-mining/. Consulted on 04/01/2023.
- Matthew Sparkes, what is bitcoin and how does it work, https://www.newscientist.com/definition/bitcoin/,consulted on 04/01/2023.
- Shivam Arora(NOV 18,2022), What is Bitcoin Mining? How Does It Work, Proof of Work and Facts You Should Know, https://www.simplilearn.com/bitcoin-mining-explained-article, consulted on 10/01/2023.

- Nik Bhatia, Joe Consorti, Exchange Outflows, BlockFi Bankruptcy Analysis, & Miner Capitulation, https://thebitcoinlayer.substack.com/p/exchange-outflows-blockfi-bankruptcy, conslted on 15/01/2023.
- Rebekah Carter (2022), The Ultimate List of Blockchain Statistics (2023) available at; https://findstack.com/resources/blockchain-statistics/, consulted on 11/01/2023.
- Abby McCain (2022), Essencial Blockchain STATISTICS: Market size Trends,

Available at https://www.zippia.com/advice/blockchain-statistics/, consulted on 1/01/2023.

- Matthew Sparkes, what is bitcoin and how does it work, https://www.newscientist.com/definition/bitcoin/, consulted on 09/02/2023.

Citations:

[1] Blockchain explained ,What is blockchain? ,Euromoney Learning, 2020 , on line, https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain, consulted on 24/12/2022.
[2] Blockchain Architecture Basics: components, structure, Benefits & creation, on line: https://mlsdev.medium.com/blockchain-architecture-basics-components-structure-benefits-creation-beace17c8e77, consulted on ; 25/12/2022.
[3] Bila Shrimali, Hiren B.Patel (2021), Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities, Journal of King Saud University –computer and Information sciences, 34, p 6795.
[4] Blockchain explained ,What is blockchain? ,Euromoney Learning, 2020. https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain#, 26/12/2022
[5] SaiKumar Kalla(2022), Components of Blockchain, https://mindmajix.com/components-of-blockchain, consulted on 27/12/2022
[6] SaiKumar Kalla(2022), op cit.
[7] Ibid.
[8] Great Learning(2022), What is Blockchain Technology; https://www.mygreatlearning.com/blog/what-is-blockchain-technology/, consulted on : 12/01/2023.
[9] SaiKumar Kalla(2022), op cit
[10] Ibid.
[11] Components of blockchain Network, available at , https://www.geeksforgeeks.org/components-of-blockchain-network/,consulted on 13/01/2023.
[12] Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain(2021), Blockchain Technology: Applications and challenges, Springer Nature, Switerland, pp 3-4
[13] Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain, op cit, p3.
[14] Ibid, p3
[15] Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain, op cit, p4.
[16] Ibid, p4.
[17] Gousia Habib, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Chaima Qureshi(2022), Blockchain technology: benefits, challenges, applications ,and integration of blockchain technology with Cloud Computing Future Internet,14 (11).
[18] A C Sountarraj, Michael Raj TF(2021) ,The science and the secret of blockchain technology, Sankalp Publication, france, pp4-7.
[19] Ravi Kumar Mathur, Introduction to Blockchain Technology, available at ; https://ntiprit.gov.in/pdf/blockchainanddistributed/Blockchain_Introduction_KR.pdf, consulted on 13/01/2023.
[20] Mustafa A, Ali and Wesam S bhaya(2020), Blockchain technology's applications and challenges: An Overview, AIP Conference proceeding 2290, 040019. https://aip.scitation.org/doi/pdf/10.1063/5.0027424. Consulted on 30/12/2022.
[21] Gousia Habib, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Chaima Qureshi(2022), op cit.
[22] Maher Fuad Abu Farhah(2022), The Blockchain: The Next Technological Revolution in The world of the Economy, journal of Economic, Administrative and Legal Science, Volum 6, issue 15, 30 may 2022, p133.
[23] Pervez Ahmed, Muhammad Ahmed, Usman Ahmed Raza, A review on Blockchain's applications and implementations(2021), ADCAIJ Advances in Distributed Computing and Artificial Intelligence Journal, VOL 10, No 2, p203.
[24] Ibid ,p203.
[25] Ibid, p203.
[26] Michael Crosby, Nachlappan, Pradhan Pattanayak, op cit

[27] Muhammad Nouman, Muhammad Azam, Ahsan Rehman Gill (2022) , Systematic Review of Blockchain Technology in Current Epoch: Applications, Adoption Challenges, and Opportunities, University Faisalabad, Pakistan, pp6-7, www.preprints.org. 29/12/2022.
[28] Muhammad Nouman, Muhammad Azam, Ahsan Rehman Gill, op cit, p6.
[29] Mustafa A, Ali and Wesam S bhaya (2020), op cit.
[30] Moez Krishen, Meryem Ammi, Alaeddine Mihou and Mutiq Almutiq(2022), Blockchain for Modern Applications: A Survey, Sensors 2022, 22, 5274.https://www.mdpi.com › pdf, consulted on 31/12/2022.
[31] Moez Krishen, Meryem Ammi, Alaeddine Mihou and Mutiq Almutiq(2022).
[32] Vipul H.Navadkar, Ajinkya Nighot, Rahul Wantmure (2018), Overview of Blockchain Technology in Gouvernment/Public sectors, Intrnational Research Journal of Engineering and Technology (IRJET), Volume 05, Issue 06, 06 june 2018. P2289.
[33] Michael Crosby, Nachlappan, Pradhan Pattanayak, BlockChaine Technology Beyond Bitcoin, working paper , University of California, October 16, 2015. P5 . on line , https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf, consulted on 24/12/2022.
[34] Michael Crosby, Nachlappan, Pradhan Pattanayak, op cit.
[35] Wolfgang KARL Hardel , Compbell R. Harvey, Raphael C. G . Reule(2019), Understanding Cryptocurrencies, International Research Technology Group 1792Discussion paper 2018/-44, p3. https://ies.keio.ac.jp/upload/20191125econo_Wolfbang_wp.pdf. Consulted on 01/01/2023.
[36] RESERVE BANK OF AUSTRALIA, Digital Currencies, https://www.rba.gov.au/education/resources/explainers/pdf/cryptocurrencies.pdf, consulted on 01/01/2023.
[37] What is cryptocurrency and how does it work?, https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency, consulted on 03/01/2023.
[38] Paul, Weiss, Rfing, Wharton , garrison llp, Cryptocurrency, https://www.paulweiss.com/media/3978877/cryptocurrency_whitepaper.pdf, consulted on 02/01/2023.
[39] Jerry Brito ,Andrea Castillo(2013), BITCOIN A Primer for policymakers, MERCATUS CENTER, George Mason University, p3.
[40] Today's Cryptocurrency Prices by Market Cap , https://coinmarketcap.com/currencies/bitcoin/consulte on 02/01/2023.
[41] Bernard Marr, What is the Difference Between Blockchain And Bitcoin?, https://bernardmarr.com/what-is-the-difference-between-blockchain-and-bitcoin/, consulted on 10/01/2023.
[42] Brian baker(2022), what is bitcoin mining and does it work?, https://www.bankrate.com/investing/what-is-bitcoin-mining/. Consulted on 04/01/2023.
[43] Matthew Sparkes, what is bitcoin and how does it work, https://www.newscientist.com/definition/bitcoin/,consulted on 04/01/2023.
[44] Shivam Arora(2022), What is Bitcoin Mining? How Does It Work, Proof of Work and Facts You Should Know, https://www.simplilearn.com/bitcoin-mining-explained-article, consulted on 10/01/2023.
[45] Nik Bhatia, Joe Consorti, Exchange Outflows, BlockFi Bankruptcy Analysis, & Miner Capitulation, https://thebitcoinlayer.substack.com/p/exchange-outflows-blockfi-bankruptcy, conslted on 15/01/2023.
[46] Rebekah Carter (2022), The Ultimate List of Blockchain Statistics (2023) available at; https://findstack.com/resources/blockchain-statistics/, consulted on 11/01/2023.
[47] Abby McCain (2022), Essential Blockchain STATISTICS : Market size Trends, Available at https://www.zippia.com/advice/blockchain-statistics/, consulted on 1/01/2023.
[48] Matthew Sparkes, what is bitcoin and how does it work, https://www.newscientist.com/definition/bitcoin/, consulted on 09/02/2023.