JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A SURVEY ON COMPREHENSIVE BLOCKCHAIN TECHNOLOGIES WITH RECENT AFFINITIES

Bonagani Prathusha[1], Dr G Bindu[2]

[1]Research Scholar, Department of Computer Science and Engineering,

KL University, Guntur District, A.P, India.

[2]Associate Professor, Department of Computer Science and Engineering,

KL University, Guntur District, A.P, India.

Abstract

Blockchain has become a novel technology which has been utilized to provide innovative results across a wide range of sectors. A decentralized blockchain system is used in fields other than finance. Moreover, we can also design a transaction that's compatible with any requisition. If we consider medical field, the network known as blockchain is used for storing and exchanging clinical information across medical centres, laboratories for diagnosis, pharmaceutical business and medical professionals. Blockchain consists of multiple application likewise IOT. In IOT wireless gadgets and sensors deployed in healthcare systems constantly track and communicate information to adjacent devices or servers over an unprotected public channel. It also provides an enormous amount of opportunity for intruders for carrying out numerous cyber-attacks that might harm victims under crucial observation. Blockchain based methods are capable of accurately identifying major errors in the medical profession, even possibly fatal ones. This research article provides a detailed anatomy of blockchain technology with its categories. This investigation explores distributed ledger, consensus mechanism algorithm and its types, smart contracts along with Ethereum working architecture, security mechanisms. In future, research outline delivers security and privacy concerns with more accuracy related to blockchain.

Keywords: Blockchain, IOT, distributed ledger, consensus mechanism, smart contracts, Ethereum.

1. Introduction

Before going into blockchain we talk about linkedlist which is a data structure having a node connected with another node with the help of a pointer. Each node has two fields, one is data and the other is the address of the next node which was stored in the previous node. So the linked list was a data structure having connections of nodes. Similarly Blockchain is a chain of blocks connected with another block that can be compared with a multipurpose tool, operating system, and different platforms where we build applications. A blockchain technology supports applications in a non-trusted atmosphere by giving trust among different parties to work with others.

Blockchain can be defined in terms of Distributed ledger, Data structure, Database, Cryptocurrency where each terminology has been described below:

Blockchain is a distributed ledger where the same register or same ledger can be distributed among different stakeholders where we call them as nodes. Different nodes of the blockchain having their copy of ledger like financial transactions and any data or asset can be categorized, shared, and transacted with, to make them legitimate by using different complexity algorithms. Different nodes are connected with each other and communicate with each other to solve a task known as distributed computing. In distributed computing all nodes are masters with equal rights. As there are no single servers, all nodes are doing computation. The task is divided between all the nodes and each node drives to maintain the replica of the ledger which is known as distributed ledger used in blockchain. As there is no third party involvement the nodes will communicate with each other through peer-to-peer network by message passing. Distributed computing can also be summarized as geographically distributed.

Blockchain can also be compared as the Data structure as it holds different blocks, holding the data and blocks are being joined with each other and keep the records in a block. The inner framework of every single block is referred as the blockchain data structure. In the blockchain technology the transactions are capable of being sorted into blocks via a mining procedure. The transaction block includes a block header that contains block metadata and a block body that contains the transaction. The information within the block header varies significantly amongst blockchain platforms, can be separated into two groups. The first set contains mining related characteristics like timestamps, difficulties and nonce, while the second contains merkle root, parent block hash and block version. In normal blockchain systems, the practical complication of the files in the block header determines its difficulty.

Blockchain is the database used to keep the records. Each block is divided into several fields where one of the fields is known as transactions. A block can store the N number of transactions. It is an append only permissioned based database, where we can add a new block but to delete a block or to change anything in a block which is already joined in the chain is very difficult. As blockchain is a decentralized distributed network. In decentralized computing no single control exists because instead of one server we are having multiple central servers. Data is replicated on different central servers and each server will maintain a copy of data. If one server fails, users can access the data from another server and also provides data integrity, trust and security among the nodes, by avoiding the central authorities or intermediators.

Cryptocurrency is one of the major key terms used in blockchain. The currency used in computers is a digital currency which was introduced in the 1990s. Blockchain uses the concept of Cryptocurrencies to build applications and store the transactions with security. Cryptocurrencies must also ensure the interchangeability, measurable amount, and your financial worth in accumulating to security measures. Furthermore, cryptocurrencies are helpful since they allow additional benefits like pseudonymization, that covers the real characteristics of the participants engaged in a transaction, decentralization, which permits for multiparty authentication of transactions, cheaper transaction fees in comparison to traditional ways of paying, faster transfer of cash by eliminating organizational and geographical barriers and trustlessness, which does away with third-party centralized trusted verified users

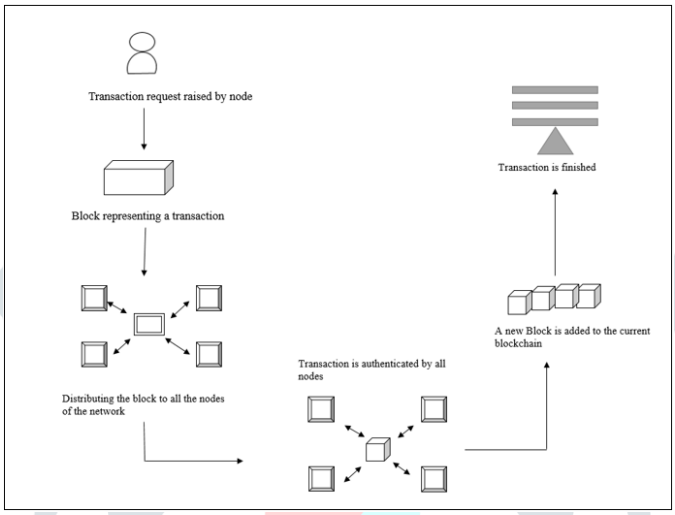

Figure 1: Stages in Blockchain

A number of articles have underlined the possible benefits of blockchain technology for the medical network, and it has recently emerged as a crucial technology in the digital revolution of the healthcare industry. This is prepared to modify the system conventional health institutions and companies have activated in the medical care business designed for many years. Blockchain in addition to information and interaction skills are important allowing tools used for the decentralization and digitization of medical care organizations, which helps patients and service providers in a modern and digitized medical care atmosphere. Healthcare institutions, patients, and doctors may all benefit from blockchain applications for handling healthcare data in the domains of handling claims and payments, maintaining patient records access and control, managing medical IoT security and exchanging and authenticating research data.

The rate of growth is accelerating at constantly growing rates in the zone of medical care. Nowadays, increasing quality healthcare services accompanied by cutting-edge and sophisticated equipment are in abundance. Blockchain technology has the potential to revolutionize the medical sector. Additionally, the changing phase of the healthcare sector is moving around a patient-centred strategy that helps emphasis on two essential elements: possessing constant availability of the best medicine facilities. Blockchain technology helps healthcare organizations to supply appropriate patient care and first-class medical amenities. Leveraging this modern technology, the complicated and repetitive procedure for exchanging medical records, leading to elevated medical expenses, may be handled quickly. Blockchain technology allows citizens to engage in medical investigation efforts.

Furthermore, greater social wellbeing studies and information exchange will enhance treatment among numerous populations. A centralized database is used to administer the whole medical industry and institutions. Blockchain can be categorized as public, consortium, or private from a security perspective.

A.Public Blockchain

A public blockchain offers a number of properties, including a decentralized network that is available to all players without any restrictions and data that is indelible, forgery-proof and cannot be amended after the fact. The PoW consensus used in this form of blockchain makes transactions on the blockchain both incredibly easy to alter and difficult to forge. Public blockchain instances abound, including: ripple, Litecoin, Dash, Ethereum and bitcoin.

B.Consortium Blockchain

A variant of blockchain technology is known as consortium blockchain. These kinds of networks are made up of presently functioning units having accessibility constraints. This type of system has a lesser number of stations than public blockchain, however it offers greater trustworthy and extensible. It also reduces the burden on networks and allows for enhanced safety. Although potentially a bit more closed than a public chain, it however raises significant risks.

This is made up of a permitted blockchain, which is a bit decentralized and distinct from public blockchain due to the fact only a small number of users can access its network. It is mentioned that the majority of current consortium blockchain uses the proof of Authority approach. Ripple, Funds DLT, and other public blockchain are examples that we can use.

C.Private Blockchain

Private blockchain resemble distributed databases, compared to public blockchain. Some of the features are listed below.

i. Only a few people can access the network. Authentication towards different candidates can be done by central decision making body

ii. The central decision making body establishes the access rights of each node to determine which of the data is accessible.

iii. The consensus on a private blockchain is established by the confidence in each validator node.

Private blockchain governs the individual's access to the network. If the network supports extraction, its security elements may restrict the individuals who may participate in the consensus process that decides extraction powers and benefits. In addition, the shared ledger may only be modified by a small group of individuals. The person who owns or runs the system has the authority to triumph, change or remove any essential blockchain records.

Blockchain can be kept isolated are not decentralized. It is a distributed ledger that acts as an enclosed database secured by cryptographic concepts and organizational criteria. None is permitted to run a complete node, execute transactions, or verify or authorize blockchain alterations if there is no authorization

The article has been organised as follows, Section 1 explained introduction, Section 2 explains history, Section 3 explains technical overview, Section 4 explains about comparative analysis of state of art methods, Section 5 explains about recent trends in blockchain technology and Section 6 explains conclusion of the paper.

2. History of Blockchain

Blockchain is a distributed ledger technology as it forms a chain in the form of blocks connected with each other. The first time-stamp control of blockchain started from 1991 in the form of blockchain 1.0, blockchain 2.0 and currently we are living in an era of blockchain 3.0. In 1991 the first work of cryptographically secured block was done by Stuart Haber, who says that cryptographic technique was used to make a secured block to store the data. In 1998 the first decentralised digital currency was introduced in the name of 'bit gold' made by a computer scientist Nick Sazbo. In 2000, Stephen Konst was the first person to recommend the first theoretical concept of cryptographic secured chain of block which can be called a blockchain. There is a specific remarkable change that happened in 2008 by Satoshi Nakamoto, who introduced the term known as bitcoin. Bitcoin is an application of blockchain which was the first digital cryptocurrency and the first platform which was used now. One of the important features of bitcoin is preventing the double spending problem. There was a drastic change in financial institutions as it was going down due to the lack of trust among each other which was a very big issue in it.

The concept of bitcoin is trustworthy as it works without any interference of third party and he officially released the platform of blockchain in 2009. As Bitcoin is not application oriented it was only focused on cryptocurrencies which can be used by many financial institutions, companies and organizations in-order to perform transactions of the funds from one individual to another individual in the form of digital currency. To introduce the concept of bitcoin, Satoshi Nakamoto had collaborated on the concept of secured chain digital currency. In 2014, the system had changed from blockchain 1.0 to blockchain 2.0 with many new cryptocurrencies having come into the market like Ripple, Ether and many more.

The focus was still in crypto-currencies but the work shifted from cryptocurrencies to smart contracts due to Ethereum which was developed in 2013. In 2015 Ethereum was finally launched by virtuallynberrat in-order to think beyond cryptocurrencies. Here the concept was changed from bitcoin and cryptocurrencies to smart contract in-order to focus on other work but still the blockchain is improper. In 2015, a major blockchain project which is known as an enterprise blockchain hyperledger, which is an open source, started by Linux to maintain an application oriented blockchain. In 2018, the concept from bitcoin, smart contract, is shifted to an application oriented system which is used for different applications in different scenarios wherever the trust is required. In 2018 blockchain 3.0 had come into existence and the focus had changed the blockchain platforms Ethereum, Hyperledger. They can be used for different types of applications whether it is health, supply chain, finance, medical lines, government records, land registries and everywhere in which different people are involved. It is believed that by 2023 we will be having an industry of blockchain using 10 billion dollars of work. By 2025, the blockchain industry would be 176 billion dollars and by 2030 it can be 3.1 trillion dollars.

3. Technical overview

3.1 Architecture of Blockchain

Blockchain provides integrity of data which is difficult to change the data that has been recorded in the block. The main concept is that it stores the previous block hash, the norms and the list of transactions in the form of a merkle tree to achieve the integrity. A blockchain node consists of a block header and the transactions. Figure 2 describes the architecture of the bitcoin block.

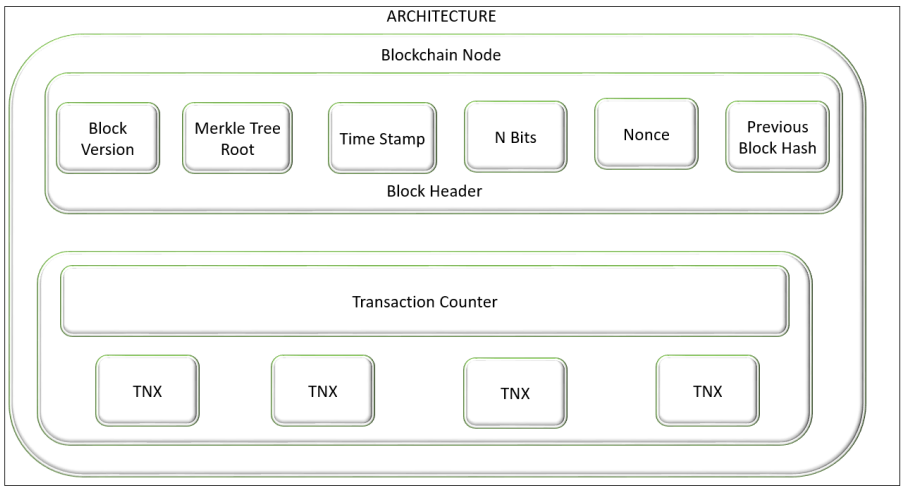

Figure 2: Architecture of Blockchain

As per figure 2 some of the key fields that exist in the block are defined below.

a. Block version

A blockchain node consists of a header, a header consists of the version of the blockchain platform like bitcoin 1.0, bitcoin 2.0 etc. Software or protocol updates can be traced by using a version number. The size of this field is 4 bytes. It is used to recognize the version of the specific block in the entire blockchain. There exists different version of blockchain such as:

1. Blockchain 1.0 implemented the concept of cryptocurrency and maintained a public ledger for the purpose of storing the data like bitcoin.

2. Blockchain 2.0 implemented the idea of smart contract, used for self-executing programs like Ethereum

3. Blockchain 3.0 implemented the concept of DAPPS or decentralized applications for creating decentralized structures like browsers.

4. Blockchain 4.0 is used in industries for generating a scalable, reasonable blockchain network so that many people can utilize it.

b. Merkle tree root

Merkle tree is also called a hash tree that uses the mathematical formulas for verifying whether the data is corrupted, hacked, or manipulated and synchronization. The size of the merkle root is 32 bytes. Let us consider an example, in bitcoin if a new block joins after 10 minutes, in those 10 minutes whatever transactions had been made will be combined together and stored as a tree. The root of the tree is hashed and the hash root is stored in the block, we call it a transactional route hash. This tree is a merkle tree. The block contains the root of a merkle tree and the transactions are linked with this tree. The leaves of the tree are storing the states and the child nodes are storing the hashes and the root is hashed which is stored in the block, this gives integrity to the data. This is how integrity to data is achieved, by storing it in a hashed way.

c. Nonce

It can be derived as “Number only used once” and can be used by proof of work algorithm. It is a 32 bit number which means 4-bytes, adjusted by miners to generate the usable number that can be used for hashing the value of the block. If the correct nonce is identified, then we can add it to the hashed block. The data stored in the block can be validated by using nonce.

d. Time stamp

In blockchain, timestamp can be used as proof to find the approximate time at which the transaction occurred. The size of the timestamp is 4 bytes, also used as a constraint to validate the genuineness of any block. In this, the random number is generated and stored in the block. It is also employed to generate the hash of the block

e. Previous Block Hash

As we defined earlier, blockchain is a collection of multiple blocks that are connected together. Each block will store the address of the previous block likewise the next block is joining with the previous block using this previous block hash and can be represented as a ledger as all the blocks are joining. The first block is known as the genesis block as it does not hold any previous block hash value.

f. Transaction

The transactions in blockchain are the same like conventional database systems except the way it is stored is different. Any operation which is grouped together and recorded in the database is a transaction such as transferring money between two people, purchasing something from someone, a land register writing a note that land belongs to some person by mentioning the land owner.

3.2 Distributed ledger

Although blockchain was designed to work as a digital currency, today it is regarded as an innovative form of distributed database or ledger due to the fact that every information might be stored in transactional metadata. Since 2014, the bitcoin blockchain has supported metadata. Although alternative blockchain implementations enable higher size, the primary bitcoin blockchain can handle only 80 bytes of metadata. For instance, BigdataDB does not have a strict limit in the size of metadata, while multi-chain offers metadata with configurable size. To maintain information pertaining to health for distributing, swapping, evaluating, preserving and authenticating objectives across stakeholders, blockchain is typically considered as a distributed ledger.

Distributed ledger is a record keeping data structure which is recording and storing the transactions. This ledger is distributed among different nodes of the blockchain. Depending upon application there can be one or more number of ledgers. A ledger will keep multiple transactions of the bank, in the land register office or any type of record.

In blockchain a group of transactions are grouped together and they are preserved in a ledger, which is distributed and replicated. So it is a replicated data structure which is appended only. It is replicated to different nodes to different participants of the blockchain

3.3 Consensus mechanism algorithm

Consensus means a mutual agreement between two parties, agreed with each other to do certain tasks. As blockchain is a trusted network, different parties unknown to each other want to perform transactions but they need to have trust that can be achieved by mutual agreement. In the consensus algorithm, if multiple parties agree with each other then only the certain work will be executed and a certain block will join into the chain. The reason behind the mutual agreement is, the distributed nodes which are playing from different geographical locations are unknown to each other, so those nodes should have the same ledger. The major point of consensus mechanism is that all nodes should have the same consistency of the data as there should not be any wrong data. As it is a peer-to-peer network, when different nodes are communicating with each other there may be a chance of malicious nodes coming in-between and applying the changes in the messages. If this is the case there is no mutual agreement. So a consensus algorithm is important because it is a peer-to-peer distributed network, and is a trade-off between consistency, availability and fault tolerance. We have to choose depending on these three trade-offs.

Before we move forward to different consensus algorithms we need to know about byzantine general problems. It is a problem considered to be as base of consensus algorithm

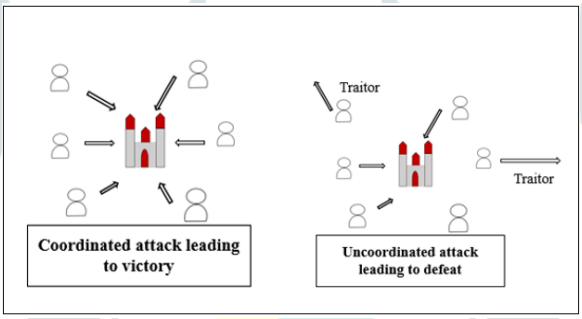

Figure 3: The problem of the Byzantine Generals

The major problem of the Byzantine general is, considering there exists a palace in-between, which is to be attacked by the army and the condition is that, the army can capture this palace only if attack has been done through all sides and at the same time. Now there are two generals one at left and another at right leading two different armies but they cannot communicate with each other directly except by passing messages to their soldiers. The attack is possible if-and-only-if there is coordination between them. So they have to work on the coordination and messages have to be passed between them. If there exists a traitor, who does not communicate the correct messages to other soldiers then there is a chance of losing the palace. Similarly in blockchain, there are different nodes and peer-to-peer messages have been passed between different unknowing parties and if there is a consensus mechanism by providing mutual agreement in-between all, then a system is secured. Therefore consensus mechanisms are so important to avoid byzantine general problems.

a. Proof of work (POW)

It is the main consensus mechanism algorithm which was widely utilised by the emergence of bitcoin which was introduced by Satoshi Nakamoto in 2008.For a block to join into the chain, the different participants of blockchain can participate in making the decision. In the case of bitcoin we say that there are specialised partners whose work is only to calculate or identify whether the block can join in the chain or not. They are known as miners. These miners will decide whether a block can join into the chain or not by using a proof of work algorithm used in bitcoin and litecoin.

b. Miners

Miners are a group of people who are responsible for joining the block into the chain. It should have a huge amount of computation power in terms of energy, computational resources is required from large companies to pool together to put high end computers together to find the hash, nonce which is less then target hash. Miners are getting rewards by identifying whether it's a valid block or not. This gives a security and trustworthy platform to blockchain as the block joins only if the miners accept to join the block.

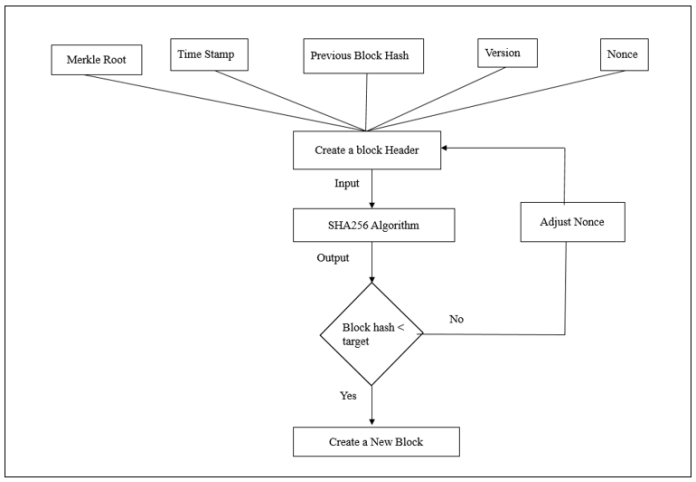

Figure 4: Representation of Data flow

Figure 4 stated that about how miners basically works, if a block has to be created, there are different kinds of information which are given into the block header like the merkle root, time stamp, previous block hash, version, nonce. This block header is given to the SHA256 algorithm which computes the hashing algorithm and generates the hash value for that particular block which can be called as a target block. If output is less then target, then the miners have to adjust the nonce by utilising huge amounts of computation power to generate the block hash which is less then target block, unless and until this nonce is not registered the miners cannot create a block and cannot join into the chain. If this case does not exist, then the miner should recompute the nonce and again generate the hash for all this recomputation. Here the computation hash remembers that miners are not doing on its own, instead the system will perform all calculations. If the correct hash has been generated and other miners agree with it, then the block joins its chain. But the disadvantage is that the more amount of computing is required to generate hash.

For every blockchain platform there exists a limited time period. For example in bitcoin the work has to be done in 10 minutes and to be verified by other miners, whether the result computed is correct or not. As it is an energy consumption algorithm, many consensus mechanism algorithms have been evolved and are compared to proof to work. For example ethereum itself using proof of work is shifted to another algorithm known as proof of stake.

c. Proof of Stake (POS)

Proof of stake works in a different way compared to POW. The platforms which are using POS are PPCoin, Nxt and Orobros. The concept of proof of stake defines as, the one who spends more time in blockchain platform and have earned cryptocurrencies with a certain value, then they can become a miner and a valid data block. There is no need to solve and find out the norms, but hashing is still done and hash value is computed. The proof of stake works in such a way that, they have to put the cryptocurrency on the stake and if the wrong calculations have been made then some amount of cryptocurrencies which have been earned by joining the blockchain platform will be deducted. This concept is known as coinage.

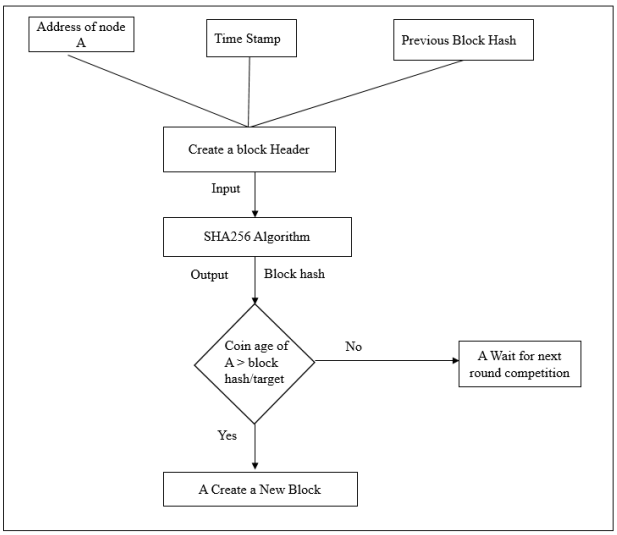

Figure 5: Steps in Proof of work

Figure 5 represents the working procedure of proof of work. A block header is created with a certain amount of information which includes address of node, time stamp, previous block hash, from the block which is given as an input to generate SHA256 algorithm as an output for the block hash. Instead of comparing with difficulty levels like whether the hash is less than the target hash or not, it is compared with the coinage of that miner. The Coinage of the minor means the amount of coins earned since joining the blockchain platform. If it is greater than the computed block hash, then only the block would be created otherwise the miner has to wait for the next round. In POW was a energy intensive algorithm which required a huge amount of energy consumption, huge amount of computation

because nonce was to be computed by the miners whereas in POS the miners were created and are allowed to join the block into the chain depending upon the time they had spent, depending upon the coinage, stake of coins they had in the particular blockchain.

There exists some more consensus algorithms such as Proof of activity, Proof of burntime and proof of capacity, proof of elapsed time.

d. Proof of Activity

It is one of the consensus algorithms which is a combination of POW and POS. The miners and the blockchain platform start joining and making a block by using the concept of POW, whereas the validation is done by POS. As POW is used by miners to create a block by computing nonce, hash and then block is created. After creating the block the miners will announce it in the network. But for validating the block, POS is required. The miners will give only the header and the winning miner address to the network. The validators are chosen from the network itself, those who are having more stake will become the validators and they sign onto the block. After receiving the sign of the validators onto the block, then the block actually joins into the chain and it is ready to accept the transactions to store into the block. POA will use the advantages of POW and POS, also reduce the amount of energy consumption. The example of POA is DCR

e. Proof of Burn Time

As the name itself suggests that the miners have to burn their coins by sending them to verified addresses but it is an unspendable address. The verifiable unspendable address can be defined as the coins that send to this address cannot be retrieved back because the address does not have the capacity, do not have the powers, or do not have the permission to either spend or transfer these coins to someone else. This is also known as eater address which means it will eat the coins. So miners send their coins to them and depending upon their power earned by burning their coins they become the miners. These miners will get the permission to mine the block. By burning the coins, miners will also earn the virtual mining rig through which the miners can mine the blocks. The reason behind burning the coins is that the amount of coins burnt is less as compared to the amount of incentives they get in mining the block. As the amount of incentive is more, the miners burn their coins to gain virtual mining rig.

The importance of proof of burn time is that the burnt coins keep on digging and the miners have to burnt their coins at a regular interval. It is not possible for a miner to burn a huge amount of coins at a time and become a miner for a long period of time. One can become a miners by simply burning the coins of themselves or coins of other blockchain platforms. An example of proof of burn time is slim-coin. In this slim-coin the miners can burn the bitcoin by sending them to verifiable unspendable addresses and gain the power of a virtual mining rig.

f. Proof of capacity

This algorithm is a storage oriented consensus mechanism algorithm. It depends on storage capacity, which can be defined as how much storage is available with the miners or mining pool. This algorithm will store the possible results of the hash value which is required in proof of work. In pre-mining, it records the hash value, which will be used to mine the block. Therefore the miner who has the highest amount of capacity, in terms of storage, becomes the winner. The advantage of this algorithm is, it stops and saves a lot of energy consumption.

Two important steps exist in this algorithm such as plotting and mining .In plotting the miners store the nonce hashes in the hard-disk. In mining the miners use the stored value to mine the block. Some of the examples using proof of capacity are burst coin, storj.

As block chain is a decentralised distributed network, there is an attack known as 51% attacks. The 51% of the network or nodes are combined together to make a legitimate wrong transaction, resulting in wrong block creation. To prevent 51% attack these consensus mechanism algorithms are utilised. The attack can be stopped by just only a miner who is having the highest amount of capacity, who has spent the highest amount of burnt time and also allowed to become a miner.

g. Proof of Elapsed Time (PoET)

PoET is one of the consensus method algorithms created by Intel in 2016 on behalf of the permissioned blockchain to utilize a hyperledger saw-tooth which is nothing but a group of blockchain platforms. It works on the principle of a valid lottery system, where a leader is elected depending on random waiting time. Every node generates random waiting time by using specialized system developed by Intel which runs a secure code and for that wait time the system of the node goes to sleep as soon as the wait time of a node is over, the first node who awakes from the wait time wins the race so the winner is one which generates with the shortest wait time. It avoids a huge amount of computation which was required by proof of work and works on the principle of random wait time which was given to every node which means that the wait time should be random to every node, in order to avoid the node that manipulates the wait time. Intel has also developed a high-end system which is used by PoET in blockchain networks, in-order to prevent the node which becomes active before the wait time is over.

3.4 Smart contract

Smart contract has been introduced by nick szabo in the year of 1997 to define the code program that has been written in high-level language, can also be recognised by a location in the blockchain network. As the smart contracts are most familiar for the designers, the code can be developed in the high level language which can be domain specific languages, general purpose languages like solidity used in ethereum, pack used in kadena, java etc. The executable functions and state variables are considered to be some of the significant elements whereas the state variables can also be changed during the execution of logic.

The most important feature of the smart contract is to provide agreement that has been enhanced by the authorised centralised entity between two parties by fulfilling every parameter required for the successful transactions that can be transparent, traceable and irretrievable. The platforms that use the smart contracts are ethereum and bitcoin. For safe and secure transactions the automatic code execution is used in smart contracts which can be distributed and certified by the network nodes in order to avoid the third parties.

The major purpose of using Smart contracts is, as there are some of the platforms mainly hyperledger which can perform updates on the smart contracts but it is most complicated if it finds any vulnerabilities in the forthcoming. The important properties can also be stored and functioned in smart contracts. As we already knew that the smart contracts are also accessible over public blockchain, making the malicious users to perform attacks which is not an easy task as there exists a strong verification that can reduces the malicious attacks and provide security to smart contracts even in future.

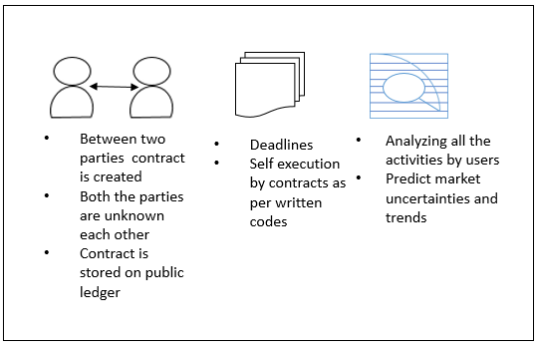

Figure 6: Smart Contract

The tracing of health equipment, medications, claims, settlements, knowledge exchange and the interchanging and usage of knowledge is a laborious task in today's healthcare environment. This can be overcome by blockchain technology, which offers harmless and protected medical care data management for a multiple purposes. Blockchain based medical care smart contracts are formed by means of the ethereum architecture, which enables us to manage claim payment, security, and privacy while maintaining patient records. Additionally, this provides efficient access to clinical data while safeguarding the privacy of the patient.

a. Ethereum

The Ethereum network, which runs on a blockchain, features a built-in Turing-complete programming language which may be utilized to develop a variety of decentralized apps and it is funded by its own money called "ether".

Solidity coded operations, instances and state variables represent almost all the Ethereum smart contracts. Turing completeness of the solidity programming language makes it ideal for developing smart contracts. A contract generation transaction records the smart contract code on the Ethereum blockchain after it had been compiled and turned into EVM byte code. A distinct contract address recognizes the smart contract during a successful contract creation activity.

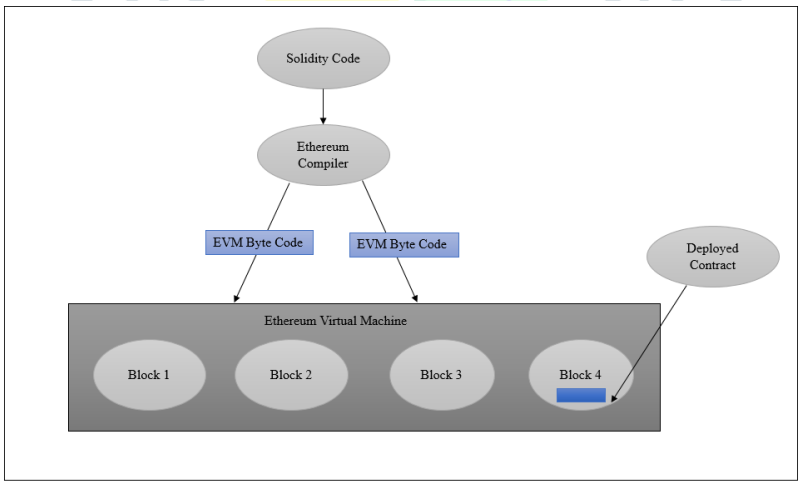

Figure 7: Ethereum Architecture

The executable code, contract address, state, made-up of isolated storing and stability in virtual currency called ether, makeup an Ethereum smart contract accounting. Using a contract initiating transactions to its distinctive location, a smart contract can be activated, with certain requirements such as invoking data and payment that take the shape of ether as the fee for transaction. The turning complete stake-based Ethereum virtual machine, or EVM is a virtual machine. It offers a network-isolated run-time environment where the smart contract code can be run. Transactions fees serve as the fundamental upper bound on computation in EVM. Ethers, a sort of cryptocurrency, are used as the balance in smart contracts. It is really important work because any weakness could result in the loss of millions of ether. Due to the immutable nature of the blockchain, a smart contract is unchangeable once it has been issued, consequently, manufacturers must think about privacy concerns while creating smart contracts and recommend them.

I.Different types of Ethereum Accounts

An Externally Owned Account (EOA) and a Contract Account are the two different types of versions available on Ethereum. The below are explanations of these:

1. **Externally Owned Account:** Private keys are used to manage accounts that are owned externally. Every EOA includes a pair of public-private keys. Users can create and sign transactions to convey messages.

2. **Contract Account:** Contract codes regulate contract accounting. The account is where these codes are kept. There is an ether balance linked to each contract account. Each time one of these accounts receives a transaction from an EOA or a note from a different contract, the contract code for that account is active. Once the contract code is active, it enables the sending of messages, reading and writing of messages to local storage, and the creation of contracts.

II. Working of Ethereum

The Ethereum Virtual Machine (EVM) is the execution framework that Ethereum uses.

i. All of the network's nodes will carry out each command when a smart contract is activated by a transaction.

ii. During block authentication, each node will execute the EVM, which causes the code to be executed in response to each transaction that is listed in the block.

iii. To maintain their ledgers in sync, every node on the network needs to do the identical calculations.

iv. Each transaction must contain

- Gas Limit
- Fee for the transaction that the transmitter is prepared to pay

v. The transaction will be processed if the whole quantity of gas essential to practise is a smaller amount than or equivalent to the gas limit. Otherwise, the transaction will not be managed and the associated fees will still be fortified.

vi. As a result, it is allowed to transmit transactions with gas limits that are higher than the estimated, to improve the likelihood that they will be executed.

b. Bitcoin

Instead of being printed, currency in the bitcoin network is mined using widely dispersed computational resources. Users in a network run the miners independently utilizing tools created to assist the initial algorithms. The beauty of the concept is that in addition to creating bitcoins, the exchange of bitcoins between users is handled by the mining network. A protocol is suggested by a bitcoin that permits exchange of fiat money among participants on the basis of a finite source. When it comes to bitcoin, the finite resources remains as a remedy to a mathematical issue that is exceedingly complex to solve. In simpler terms, the bitcoin technique creates currency by using programming to deal with a challenging issue that demands a significant amount of effort. Leveraging bitcoin during transactions is comparable to utilizing standard fiat currencies. Regardless of the reality we happen to use bitcoin, the consumer. Regardless of the reality we happen to use bitcoin, the consumer pays attention towards our electronic signature, and it's a code of authorization encoded with sixteen different symbols. To gain the cryptocurrency, the consumer utilise their device to decode the secret code. So we can express cryptocurrencies as a transaction of digital information which allows the obtaining or trade of commodities and services.

3.5 IOT

The Internet of Things enables electronic devices to communicate with one another over an internet protocol, allowing for continuous data sharing. In IOT Functioning of gadgets and products are largely detectors and microcomputers which could be readily infiltrated by fraudulent attempts. As per several sources, IOT devices are made up of three layers likely the application layer, the network layer, and the perception layer.

1. The application layer includes smart energy, health care and smart cities.
2. The network layer contains equipment's like switching devices, routers, gateways and firewalls.
3. In contrast the perception layer incorporates embedded systems and detectors.

The use of blockchain – based technologies in the internet of things offers an intriguing strategy for improving integrity of information and privacy. One of the advantage that blockchain may offer for healthcare and Internet of Things is privacy that comprises of safeguarding information, devices and networks, most importantly data protection. It is emphasized that the mainstream of research focus on the following topics such as integrity of data, restriction of access and safeguarding confidentiality. There also exists several ways of attacking methods where a blockchain technology might be infiltrated likely race attack, Finney attack, Sybil attack, DDOS attack and many more. Access control, impersonation attack, eavesdropping attack, Denial of Service (DoS) and routing attack were the most. To guard against assaults, blockchain employs a variety of consensus algorithms, including Proof of Work (POW), Proof of Stake (POS), and Practical Byzantine Fault Tolerance (PBFT).

4. Comparative analysis of state of art methods

Table 1: Comparative analysis of state of art methods

Article Title	Year	Methodology	Key Findings	Downsides
Zhjie Sun, Dezhi Han – A Blockchain based Secure Storage	2022	Attribute based access control framework	Permitting for flexible and extremely fine utilization of healthcare information, and then records the health-related information on the	• Improving the optimization in distributed systems.

Scheme for Medical Information			distributed ledger, which may be protected and tamper-proof by implementing appropriate smart contract functionality.	• Reducing the arithmetic power and improve the efficiency of consensus algorithm in different scenario
Tehreem Ashfaq, Rabiya Khalid - A Machine Learning and blockchain based Efficient Fraud Detection Mechanism	2022	Machine learning algorithm – SMOTE, XGBoost, Random Forest Algorithm.	SMOTE – • Eliminates the over fitting issue triggered by random sampling data. • Generating minority class samples is the primary responsibility of the SMOTE. XGBoost – • This algorithm estimates upcoming transactions that will arrive by connecting to the blockchain smart contract. • The suggested model anticipates the transaction and returns it to the blockchain with its outcome. • Additionally, hyper parameter adjustment enhances the process of learning algorithm performance. • XGBoost features a vast parameter space and a high number of hyper parameters, which makes it efficient and extensible. Random Forest – • In an uneven dataset with fewer instances of fraud, random forest is utilized for identifying fraudulent activity.	• Tuning is challenging due to the wide parameter range. • There is a significant flaw as there is an effect of adversarial attack.
Sumaya Sanober, Mohammed Aldawsari – Blockchain integrated with Principal Component Analysis: A Solution to Smart Security against Cyber-Attacks	2022	PCA – Principal Component Analysis	• Improper information will be deleted from real- time dataset before being processed by the blockchain method in order to identify hazards and also implemented Covariance Matrix to identify basic features of the information. • Integrating PCA with Blockchain can provide more precise as well as robust security over malware penetration by including two factors i-e key matching and feature extraction.	Should consider the feasibility of working with just one blockchain to construct data privacy, as most present methods employ multiple blockchain, making integration difficult
Jung-San Lee, Chit-Jie Chew – Medical Blockchain: Data Sharing and Privacy Preserving of EHR based on smart contract	2022	HIPAA – Health Insurance Portability and Accountability Acts, AVISPA - Automated Validation of Internet Security protocols and Application	• To provide Security by preventing inappropriate breach and verified exposure. • It refers to a protocol for protection that is frequently utilized to validate the resilience as well as verification characteristics of a protocol.	To accomplish viable information one should emphasis on access control as well as partial grant, full grant, proxy grant of health facts
D Doreen Hephzibah Miriam, Deepak	2023	Optimal LHE-HES – Optimal Lionized	• The best key is chosen in the proposed LGE – HES technique,	There are also a few other difficulties, which include the

Dahiya – Secured Cyber Security Algorithm for Healthcare System using blockchain Technology		Golden Eagle Based Homomorphic Elapid Security Algorithm	which also ensures an elevated degree of privacy for delivering healthcare signals with already encrypted data.	whole size of the key and the calculation used in the previous method is pretty big. The growth of privacy in medicine will be high if a hybrid optimization has been implemented.
Fadwa Alrowais, Heba G. Mohamed – Cyber-attack detection in healthcare data using cyber – physical system with optimized algorithm	2023	FCM- ABC – Fuzzy C-Means Algorithm with Artificial Bee Colony Optimization	• The goal of FCM is to recognize fraudulent people who attempt to obtain data from health care equipment. Which can be accomplished by locating the cluster centroids. Here multiple clusters can be generated through health records to each health care system. • In ABC the observation of the patient is done by attaching several detecting machines and also extracts clinical information through several detectors.	Should improve the storage by providing the protection in the distributed ledger.
Rui Guo, Huixian Shi, Dong Zheng – Flexible Efficient Blockchain based ABE Scheme with multi-authority for Medical-On-Demand in telemedicine system	2019	ABE - Attribute Based Encryption Algorithm	• An ABE technique is used to perform validation and identification with greater versatility and effectiveness for Medical-On-Demand amenities like healthcare systems.	The ABE model can efficiently identify collusion attacks in multiple authorities and shows better performance compared with other models.
Junsong fu, Na wang, Yuanyuan cai - Privacy preserving in healthcare blockchain systems based on Lightweight Message Sharing	2022	Lightweight privacy preserving mechanism	• According to the reliability of evidence and evaluation, the suggested system can preserve the confidentiality and safety of individuals' health data.	Effective Electronic Medical Record search tools are difficult.
Haibing Liu, Ruben Gonzalez Crespo - Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts	2020	BDL-IBS – Blockchain and Distributed Ledger based Improved Bio-Medical Security System	• It was designed to optimize the exchange amount of protected documents while minimizing the adversial consequences of digitizing transferable medical files.	It restricts calculations and resolution time when dealing with the context of authorization.
Bessem Zaabar, Omar Cheikhrouhou - Health Block: A secure Blockchain - based healthcare data management system	2021	OrbitDB with Interplanetary File System - IPFS	• In a distributed concept, a peer-to-peer record exists which is named as OrbitDB. • To recognize distinctive files in every texture pointing we use IPFS which is known as peer-to-peer hypermedia. • In the blockchain database, IPFS computes and delivers the hash information recorded in OrbitDB.	In the method of assessing acquired clinical knowledge and automated medical diagnostic decisions, incorporate artificial intelligence and machine learning elements.

Table-1 describes different methodologies that have been used in blockchain technology such as attribute base access control framework, SMOTE, XGBoost, Random Forest Algorithm, Health Insurance Portability and Accountability Acts, Automatic Authentication of Internet Security Protocols and Application, Optimal Lionized Golden Eagle Based Homomorphic Elapid Security Algorithm, Attribute Based Encryption Algorithm, Lightweight privacy preserving mechanism, Blockchain and Distributed Ledger based improved bio-medical security and many more such algorithms accomplished the efficiency of smart contract authorization, identifies fraudulent activities in all scenarios as well as propagates the robust security for all vulnerabilities.

5. Recent Trends in Blockchain

The finest part of blockchain technology development is the fact that it can't be accessed or altered, and it can be employed to keep information about transactions in a verified and identifiable fashion. Let us discuss some of the applications are listed in table-2:

Table 2: Recent Trends in Blockchain

Block chain technology	Objective
Finance Industry	• Blockchain technology has the ability to alleviate problems in the worldwide financial system • In finance industry the blockchain technology generates high level security while performing transactions, also decreases the scams. some of the benefits like * High security * Transparency * Trust * High Performance * Scalability
Cyber Security	• The swift identification and avoidance of potential cyber threats is a smart notion for ensuring the adequate protection of the current and prospective blockchain. • Cyber security in blockchain also avoids deception and misuse of identity. • The majority of the security measures, which include flow controls and credential rotation, could be administrated more distinctly. • Legally approved individuals only will gain permission to use particular features.
Cloud Storage	• Integrating of cloud storage with blockchain results in highly scalable integrated solution. • The inter-cloud architecture can allow the distributed ledger system to continue operating regardless of whether a specific cloud-based server undergoes assault.
IOT and Networking	• IOT applications like confidentiality, security and third party reliance concerns can be resolved by using blockchain. • The incorporation of the blockchain with IoT could assist people as well as the community.
Supply Chain Management	• Blockchain technology might offer the complete transparency that current supply chains require in order to monitor every step of their manufacturing procedure while boosting effectiveness. • The fundamental feature of BCT in supply chain management is traceability.

6. Conclusion

Blockchain technology is expanding its uses and assisting the world in changing more safely and feasibly. This article first undertook a more in-depth survey of blockchain technology in terms of overview, consensus algorithms, smart contracts and Ethereum with its framework. It provided blockchain history and compared the five years of literature review in much detail and quantitatively as possible by elaborating different methodologies, advantages and limitations. Finally this investigation gives the brief description about recent trends in blockchain technology with its objectives.in the forthcoming, we may develop future-oriented medical facilities that will assist the proprietors by retaining confidentiality while also supporting caretaker demands.

References

1. Amritraj Singh, Reza M. Parizi, Zhang Qi, Choo Kim-Kwang Raymond, Ali Dehghantanha, **"Blockchain smart contracts formalization: approaches and challenges to address vulnerabilities"**, Volume 88**,** January 2020, 101654
2. Daniel Macrinici, Cristian Cartfeanu, Shang Gao**, "smart contract applications within blockchain technology: A systematic mapping study",** Volume 35, Issue 8, December 2018, pages 2337-2354.
3. Ioannis Karamitsos, Maria Papadaki, Nedaa Baker Ai Barghuthi, **"Design of the Blockchain smart contract: A Use Case for Real estate",** Volume 9, Issue 3, July 2018.
4. Satpal Singh Kushwaha, Saneep Joshi, Dilbag Singh, Manjit Kaur, Heung-No Lee, **"systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract",** Volume 10, January 4, 2022**.**

5. **Asma Khatoon, "A Blockchain Based Smart Contract system for Healthcare management",** 3 January 2020.
6. Tsung-Ting Kuo, Hyeon-Eui, Lucila Ohno-Machado, **"Blockchain distributed ledger technologies for biomedical and health care applications",** Volume 24, Issue no 6, September 2017.
7. Joao Cunha, Ricardo Duarte, Tiago Guimaraes, Cesar Quintas, Manuel Filipe Santos, "**Blockchain analytics in Healthcare: An Overview",** page no 708-713, 2022.
8. Abid Haleema, Mohd Javid a, Ravi Pratap Singh b, Rajiv Suman c, Shanay Rab d, **"Blockchain technology applications in healthcare: An Overview",** September 2021.
9. Tarek Frikha, Faten Chaabane, Nadhir Aouinti, Omar Cheikhrouhou, Nader bem Amor and Abdelfateh Kerrounche, **"Implementation of Blockchain Consensus Algorithm on Embedded Architecture",** Article-id 991869, 2021.
10. Muhammad Habib ur Rehman, Khaled Salah, Ernesto Damiani, Davor Svetinovic, **"Trust in blockchain Cryptocurrency Ecosystem",** Volume 67, Issue 4, 06 November 2020.
11. Victor Gayoso Martinez, Luis Hernandez-Alvarez and Luis Hernandez Encinas, **"Analysis of the cryptographic tools for blockchain and bitcoin"**, Issue 8, 15 January 2020.
12. Danny Bradbury, **"The Problem with Bitcoin"**, Volume 12, Issue 11, November 2013.
13. Sumaya Sanober, Mohammed Aldawsari,Abdurakhimova Dilora Karimovna, Isaac Ofori, **"Blockchain integrated with Principal Component Analysis: A Solution to Smart Security against Cyber-Attacks"**, 10 August 2022.
14. Tehreem Ashfaq, Rabiya Khalid, Adamu Sani Yahaya, Sheraz Aslam, Ahmad Taher Azar, Safa Alsafari and Ibrahim A.Hameed, **"A machine learning and Blockchain based Efficient Fraud Detection Mechanism",**Volume 19**,** September 2021.
15. Jung-San Lee, Chit-Jie Chew, Jo – Yun Liu, Ying – Chin Chen, Kuo – Yu Tsai, **"Medical Blockchain: Data Sharing and Privacy Preserving of EHR based on smart contract"**, Volume 65, 2022.
16. D Doreen Hephzibah Miriam, Deepak Dahiya, Nitin, C N Rene Robin, **"Secured Cyber Security Algorithm for Healthcare System using Blockchain Technology"**, Volume 35, Issue 2, 2023.
17. Zhjie Sun, Dezhi Han, Dun Li, Xiangsheng Wang, Chin – chen Chang, Zhongdai Wu, **"A Blockchain based Secure Storage Scheme for Medical Information "**, Volume 40, 2022.
18. Fadwa Alrowais, Heba G. Mohamed, Fahd N. Al-Wesabi, Mesfer AI Duhayyim, Anwer Mustafa Hilal, Abdelwahed Motwakel, **"Cyber-attack detection in healthcare data using cyber – physical system with optimized algorithm"**,volume 108,2023.
19. Rui Guo, Huixian Shi, Dong Zheng, Chunming Jing, Chaoyuan Zhuang, Zhengyang Wang, **"Flexible and Efficient Blockchain Based ABE Scheme with Multi-Authority for Medical On Demand in Telemedicine System"**,Volume 7,2019.
20. Junsong fu, Na wang, Yuanyuan cai, "**Privacy preserving in healthcare blockchain systems based on Lightweight Message Sharing",** 2020.
21. Haibing Liu, Ruben Gonzalez Crespo, Oscar Sanjuan Martinez,**"Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts"**, Volume 8, July 2020.
22. Bessem Zaabar, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, Mohamd Abid, **"HealthBlock: A secure blockchain based healthcare data management system"**, Volume 200, December 2021.
23. Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, Shahbaz Khan, "**A review of Blockchain Technology applications for Financial Services**", Volume 2, Issue 3, July 2022.
24. Alex. R. Mathew, "**Cyber Security through Blockchain Technology**"**,** Volume 9, Issue 1, October 2019.
25. Ravi Prakash, V.S.Anoop, S Asharaf, "**Blockchain technology for cyber security: A text mining literature analysis**", Volume 2, Issue 2, November 2022.
26. Sanjay S, Praveen S Kamath, "**Blockchain Vulnerability and Cyber Security**", Volume 6, Issue 11, 2021.
27. Dinh C. Nguyen, Pidipi N Pathirana, Ming Ding, Aruna Seneviratne, "**Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges**", August 2020.
28. Randhir Kumar, Prabhat Kumar, Rakesh Tripathi, Govind P. Gupta, Sahil Garg, Mohammad Mehedi Hassan, "**A Distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network**", Volume 164, June 2022.
29. Aichih (jasmine) Chang, Nesreen EI – Rayes, Jim Shi, "**Blockchain Technology for Supply Chain Management: A Comprehensive Review**", Volume 1, Issue 2, June 2022.
30. Qian Wei, China Bingzhe Li, USA Wanli Chang, UK Zhiping Jia, China Zhaoyan Shen, China Zili Shao, "**A Survey of Blockhain Data Management Systems**", Volume 1, November 2021.
31. Prabhat Kumar, Randir Kumar, Govind P. Gupta C, Rakesh Tripathi C, Alireza Jolfaei, A.K.M. Najmul Islam, **"A blockchain – orchestrated deep learning approach for secure data transmission in IOT - enabled healthcare system"**,2023.
32. Xiao Li, Weilli Wu, **"Recent Advances of Blockchain and Its Applications"**, August 2022.
33. Endale Mitiku Adere, **"Blockchain in healthcare and IoT: A Systematic Literatire review"**, volume 14, July 2022.
34. Aarju Dixit, Aitya Trivedi, W. Wilfred Godfrey, **"A Survey of Cyber Attacks on blockchain Based IoT systems for industry 4.0"**, October 2022.
35. Vinay Gugueoth A, Sunitha Safavat B, Sachin Shetty C, Danda Rawat, **"A Review of IoT Security an Privacy Using Decentralized Blockchain Techniques",** 2023.