SYSTEMATIC REVIEW BLOCKCHAIN MODIFICATION METHODS, CONSENSUS ALGORITHMS, AND BLOCKCHAIN APPLICATIONS (MAY 2021)

[1]OWAIS ZAID, [2] DERAR ELEYAN, [3]AMNA ELEYAN

[1] Department of Applied Computing, Technical University-Kadoorie, Tulkarem, Palestine
[2]Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, United Kingdom
E-mail: [1]o.o.zaid@students.ptuk.edu.ps, [2]d.eleyan@ptuk.edu.ps, [3]a.eleyan@mmu.ac.uk

ABSTRACT

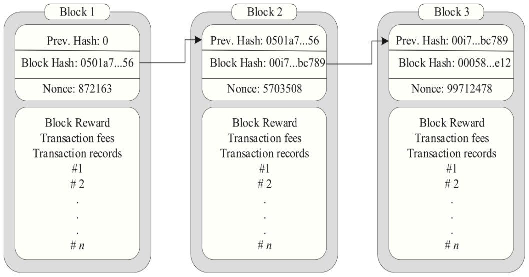
The Blockchain technology is a revolutionary technology for its stability in an environment that is predominantly unreliable, making it one of the most prominent technologies that everyone seeks to use and develop in a very wide range of applications, with all this when starting to expand using blockchain technology, defects appear quickly, especially when used in the applications in which they are made. Data modification and also when used in areas that contain simple processors such as the Internet of things, consensus algorithms and encryption are a heavy burden on these processors, and it is not possible to use the blockchain in applications that need to modify data such as the financial sector, so it was necessary to propose several Ways to make blockchain modifiable, so that the blockchain is applied to a wide range of applications.

In this study, we will be able to know the most popular modification methods on the blockchain and provide a comparison between them and which one is better, and we will also learn about consensus methods and whether they have an impact on modification algorithms How much will we know if it is possible to know whether devices that contain small processors will be able to apply the blockchain to them and the extent of the influence of encryption algorithms the consensus and amendment to it.

Keywords: *Blockchain, Right To Be Forgotten, Right To Be Modified, Consensus Algorithms, Blockchain Applications*

1. INTRODUCTION

Since blockchain was used in Bitcoin in 2008 [24], blockchain has evolved and became used in applications other than cryptocurrencies. It can be said that the blockchain is a chain of blocks each block consists of transactions, the hash value, and the hash value of the previous block. Linking blocks using the hash value of the previous block as shown in Figure 1, the blockchain has many advantages as it is not possible to tamper with the data recorded inside it and it does not accept any retraction, deletion or modification of the data, which made it with high characteristics and great in transparency and security Highly improved, and improved data traceability [25] , [3], the international data company has said that blockchain spending will reach $ 12.4 billion by 2022 [26].



However, if I distinguish the inability to modify, delete or return data, it represents a defect in some applications that want to integrate the blockchain in, for example the financial sector, also the health sector, as well as the Internet of things [27], and the regulation of the General Federation of Data in the United States and the European Union states However, the user has the right to delete or forget his data [29], [28], and also illegal and harmful data can be added due to the inability to impose censorship on it [30]. Therefore, what are the proposed methods for modifying the blockchain and its challenges will be studied. We must also know.

One of the most important algorithms on which blockchain algorithms depend are consensus algorithms, as verifying the block and its security are among the tasks of consensus algorithms [3], and because the blockchain is a decentralized network, it was necessary to design protocols indicating that the transactions are valid and valid. Consensus algorithms agree or reject a specific block [3]. Consensus algorithms are many and all have their own advantages and disadvantages. They will be quickly reviewed and a comparison made between all algorithms and their pros and cons.

After knowing the consensus algorithms and modification methods on the blockchain and their relationship and their effect on each other, it was obligatory for us to address the applications that used the blockchain, and what is the impact of the consensus algorithms on the possibility of applying the blockchain to wider areas? And do the modification algorithms and methods really offer a solution to the possibility of expanding the use of this technology in areas Other, and what are the challenges facing this technology, blockchain has been applied in several fields, where it has been applied in artificial intelligence because it provides high protection for data and not to be manipulated, which gave high effectiveness to artificial intelligence as it increased the safety of artificial intelligence and became able to face DDOS and DOS attacks [4], and blockchain has also been implemented in the health sector, where a blockchain-based system called Healthify has been proposed that provides high protection for medical data [6], and another system has been proposed to share medical data between the centers and the concerned medical authorities without Fear for data and the exchange of information easily between the concerned authorities [9], and in the field of transportation, a security system was introduced to share data between transportation means to identify accidents, crises, etc. A lot [7], the Internet of things, where much attention has been paid to this field because it tries to solve a very important problem, which is how to implement the blockchain on the Internet of things, and devices are limited in source, as all Internet of things devices are limited in source, so consensus algorithms have been introduced that do not require a large energy source or methods. Processing needs powerful processors, and other applications for the Internet of things were introduced [8] - [11] - [17], and the education sector also had a share in the application of the blockchain, where the blockchain was applied as a distributed and secure database where it could not be tampered with and the possibility of sharing The data in it is safe, as educational institutions can access students' certificates without referring to any other party because the certificates are entered by the responsible authorities and it is not possible to tamper with the data of the certificates, so it can be trusted that these certificates and transactions are original and have not been forged in any way, as the blockchain prevents Manipulating stored data [14], and for those who see any research paper that compared modification algorithms, explaining and comparing consensus algorithms, knowing their impact on modification algorithms, and presenting a group of blockchain applications, this is the paper. In order to present all these techniques in one go, this paper was organized where a summary of the paper, the introduction, and the method for identifying initial studies for systematic analysis were presented, and then an analysis and discussion of the questions posed was presented, and in the final section the results and future work were presented.

2. BACKGROUND

In this section, terminology related to blockchain will be reviewed and we will also review related works.

2.1 Background on Blockchain.

A blockchain is a distributed network where members can interact with each other without a third intermediary, as each member maintains a distributed ledger to record transactions and contracts. Each user must create an account in order to be a participant in the blockchain. Each account has two public keys and a private key. The use of the private key to sign the transaction [17], the blockchain relies mainly on Concurrent Distributed Ledger Technology (DLT) as it can be considered as a decentralized database. This technology was introduced by a person called Satoshi Nakmoto. The blockchain contains a set of parts (transaction, block, chain, markle tree, ... etc).

The blockchain is divided into three sections, the public blockchain, the consortium blockchain, and the private blockchain [3], each one will be explained separately later. The co-op algorithms are among the most important algorithms in the blockchain technology, where they determine whether or not the transaction is accepted. They will be explained in detail later and what they are. The most important and famous algorithms.

2.2 Related works.

There are many studies and literature that have talked about blockchain modification and forgetting methods, in order to allow them to be used in a wide range of applications, and there are many studies that talked about blockchain problems, as well as consensus algorithms, and applications in which blockchain can be used, so we will present in This paper is a group of studies that talked about these topics mentioned above.

The general blockchain building algorithm was developed that can be modified based on a main chain and multiple side chains to modify the transaction as shown in Figure 2, where the hash value of the block is taken before the modification and then the modification is made to the block using modification algorithms through specific steps in TMC, so that The hash value after modification is equal to the hash value before modification so as not to become a defect in the chain and the chain remains consistent, as this algorithm is one of the latest and best algorithms that provide an actual solution to modifying the public blockchain [1].

Atenis and others proposed a modifiable blockchain by chameleon hash. The method is not scalable to a public blockchain [31]. Dewar and others proposed a new mechanism for modifiable blocks by users followed by a vote. He also suggested modifying the blockchain at the block level [32]. Modification of the blockchain to suit blockchain applications without the use of heavy encryption tools, where a chameleon hash system is used so that it is protected from the attack of key exposure to the single-trapdoor, where the distributed trapdoor sharing method is used to prevent collisions, and it can also be used in various types of blockchain [2] The consensus algorithms are among the most important algorithms on which the blockchain technology depends, as it determines how to reach an agreement in the blockchain network. The consensus algorithm POW and pos are among the most popular consensus algorithms, where the most popular consensus algorithms will be analyzed and explained [3] Table 3 presents a brief comparison of consensus algorithms. Blockchain.

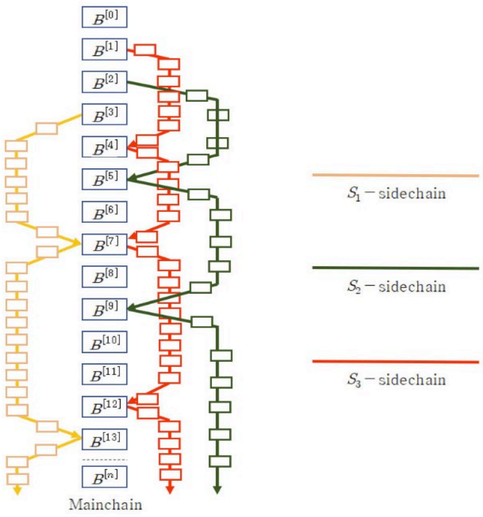
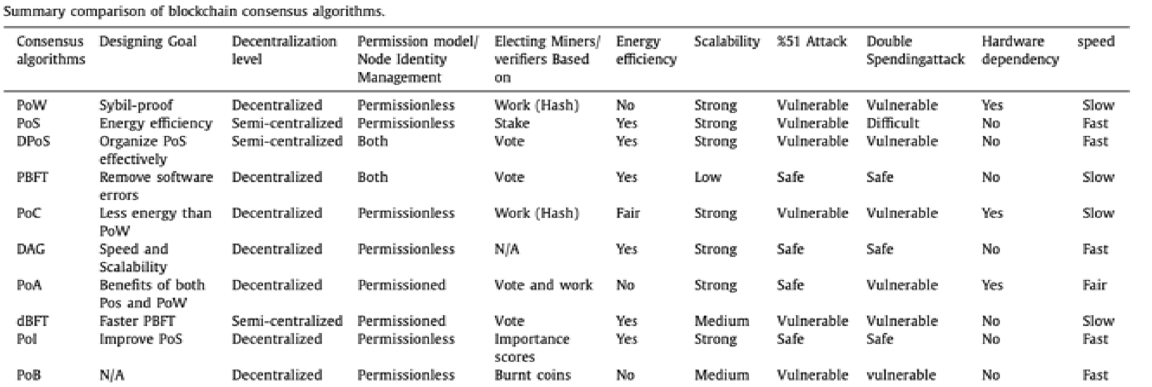


Figure 2: Mainchain-sidechain architecture

A distributed database can be created from blockchain technology, which ensures that data is not tampered with (as one of the features of the blockchain is that it is not possible to manipulate data) that is processed by artificial intelligence, as well as from DDOS AND DOS attacks, and it also gives privacy to data and authentication where personal information can be hidden (4], the security and privacy provided by blockchain is very strong. Nevertheless, there are challenges facing this technology and the expansion of its use in applications such as supply, finance, health, and energy [5]. The use of blockchain in the medical field is one of the important blockchain applications that are receiving wide attention. A health data protection system that provides easy access to information and smart tools as a system called Healthify has been proposed, and medical information for a specific person can be accessed by doctors in a secure manner [6]. Blockchain can be used in transportation means, which enhances data protection. However, the large energy consumption of the blockchain made it difficult to use and apply it in transportation. A proposal was made to reduce transaction processing, which led to a 40% energy reduction. The method is reliably ineffective [7], a blockchain-based IoT network has been proposed that provides security and data integrity. The fault-tolerant PBFT consensus algorithm has been used [8], a blockchain-based medical information exchange platform has been proposed where a new consensus algorithm has been proposed (MBFT) works to speed up transaction processing and increase scalability [9]. A set of threats and challenges facing the use of blockchain in the Internet of Things [10] have also been introduced.

Blockchain has been integrated with the Internet of Things to create a secure central infrastructure to provide a secure communication platform in smart cities. Where a mechanism for sharing data and analyzing it using data science was proposed where a blockchain-based secuchain architecture was proposed [11], and a study was presented on consensus algorithms in which the author mentioned the weaknesses and strengths of algorithms [12], and an explanation of what the applications are. Which is based on blockchain technology and what are its challenges [13], and this paper also introduces blockchain applications in education and its benefits[14]. This paper focuses on the set of challenges facing blockchain in privacy and anonymity. [15], this paper presents a solution to debug the blockchain using chameleon hashing technology, and sign linkable rings, where the updateable chameleon hash has been proposed [16]. This paper presents and discusses a literature review on blockchain and Internet of Things (IoT) control models [17] An alternative proposal to the POW consensus algorithm, which is the POAH algorithm, as it provides an excellent transmission speed of approximately 3 seconds in frontier source devices such as Internet of things [18]. This paper also talks about threats to blockchains and attacks with appropriate and countermeasures [20]. A modification algorithm was introduced to the error-tolerant Istanbul Byzantine algorithm providing a higher throughput of up to 1140 tax [21].

Table 1: Summary comparison of blockchain consensus algorithms



Summary comparison of blockchain consensus algorithms.

Consensus algorithms	Designing Goal	Decentralization level	Permission model/ Node Identity Management	Electing Miners/ verifiers Based on	Energy efficiency	Scalability	%51 Attack	Double Spendingattack	Hardware dependency	speed
PoW	Sybil-proof	Decentralized	Permissionless	Work (Hash)	No	Strong	Vulnerable	Vulnerable	Yes	Slow
PoS	Energy efficiency	Semi-centralized	Permissionless	Stake	Yes	Strong	Vulnerable	Difficult	No	Fast
DPoS	Organize PoS effectively	Semi-centralized	Both	Vote	Yes	Strong	Vulnerable	Vulnerable	No	Fast
PBFT	Remove software errors	Decentralized	Both	Vote	Yes	Low	Safe	Safe	No	Slow
PoC	Less energy than PoW	Decentralized	Permissionless	Work (Hash)	Fair	Strong	Vulnerable	Vulnerable	Yes	Slow
DAG	Speed and Scalability	Decentralized	Permissionless	N/A	Yes	Strong	Safe	Safe	No	Fast
PoA	Benefits of both Pos and PoW	Decentralized	Permissioned	Vote and work	No	Strong	Safe	Vulnerable	Yes	Fair
dBFT	Faster PBFT	Semi-centralized	Permissioned	Vote	Yes	Medium	Vulnerable	Vulnerable	No	Slow
PoI	Improve PoS	Decentralized	Permissionless	Importance scores	Yes	Strong	Safe	Safe	No	Fast
PoB	N/A	Decentralized	Permissionless	Burnt coins	No	Medium	Vulnerable	vulnerable	No	Fast

3. RESEARCH METHODOLOGY

3.1 Description of the research goals

Five research questions have been identified that will be answered in this review.

- Question 1: What are consensus algorithms and what are their challenges, advantages and disadvantages?

One of the most basic algorithms in the blockchain are consensus algorithms, as consensus algorithms are those that determine the conditions for accepting a transaction or block or validating a specific block, and also the ones that maintain the security of the blockchain as the verification methods that follow are strict, so it must be studied Consensus algorithms and their most popular, and the advantages and disadvantages of each algorithm.

- Question 2: What are the proposed methods of modifying the blockchain and the advantages and disadvantages of the proposed algorithms?

It is also known that the stability of the blockchain and the inability to manipulate data is one of its most prominent features, but although these are excellent features, they were reflected in them, as it became a problem in many applications and laws, where it is not possible to change the data or make any amendment to the data or even forget it. This is in addition to the list of European Union and United States laws for personal data laws that give anyone the right to delete or forget his data, and it is also possible to add harmful data to the blockchain without anyone knowing or even tracking it or modifying it or deleting it, as well as the inability to modify transactions. In the blockchain, to make the blockchain network so huge that the unwanted information could not be deleted or even an error occurred and it was added to the blockchain like what happens in the Internet of Things. We were able to delete it, although it is of no use, but rather the opposite harms it more than its benefit, so it became necessary to propose methods of modification to the blockchain without affecting its features and stability.

- Question 3: Are consensus algorithms related to the ability to modify the blockchain and how difficult it is?

As we mentioned earlier, one of the most basic algorithms in the blockchain are consensus algorithms, and if we want to build a modifiable blockchain, one of the consensus algorithms must be included in the modifiable blockchain, so we will know the answer to this question, is the modifiable blockchain affected by the chosen consensus algorithms or not, because for each A specific method consensus algorithm for accepting blocks in the blockchain.

- Question 4: What are the applications that have used blockchain technologies and their challenges?

Blockchain has been applied in several fields, including the medical field, the Internet of things, transportation, smart cities, and many other fields, as proposed systems and prototypes have been built to know the compatibility of this technology with such applications and what are the difficulties they face.

- Question 5: What are the challenges and limitations of this technology?

Blockchain technology is a distinctive technology and has many features and unparalleled stability, but because of these features there are challenges of how to apply it in wider areas of applications and how to benefit from them and their advantages as much as possible, so some of the challenges facing this technology have been presented, knowing that some The challenges that we will mention have been found solutions to, but the solutions are not comprehensive and face shortages and gaps in certain points.

Then, in the next step, I searched the Google scholar database with the keywords, “blockchain modification using hash”, “public blockchain modification using hash”, “blockchain modification using”, “blockchain applications”, “consensus algorithms”, and these papers were collected. All of them, and then in the next step of the filtering, all papers whose title indicates that they are irrelevant were removed. Searches were conducted on March 25, 2021, in the next step, the following exclusion criteria were used after reading part of them, which are the summary, introduction and results:

- All duplicate sheets have been removed with Mendeley.
- All papers that were not related to the topic have been removed.

The systematic review was summarized in this section using the aforementioned keywords, where 200 of the results were collected through the initial search process, where all the papers that were not relevant to the topic were filtered, then 118 research papers were left for different other researchers, and then we found about 25 duplicate papers. After reading the abstract, introduction and conclusion, 29 papers were removed, as they were not related to the topic, and then five other research papers were removed due to the limited capabilities, leaving 23 papers that were fully studied and reviewed, as shown in Figure 3.

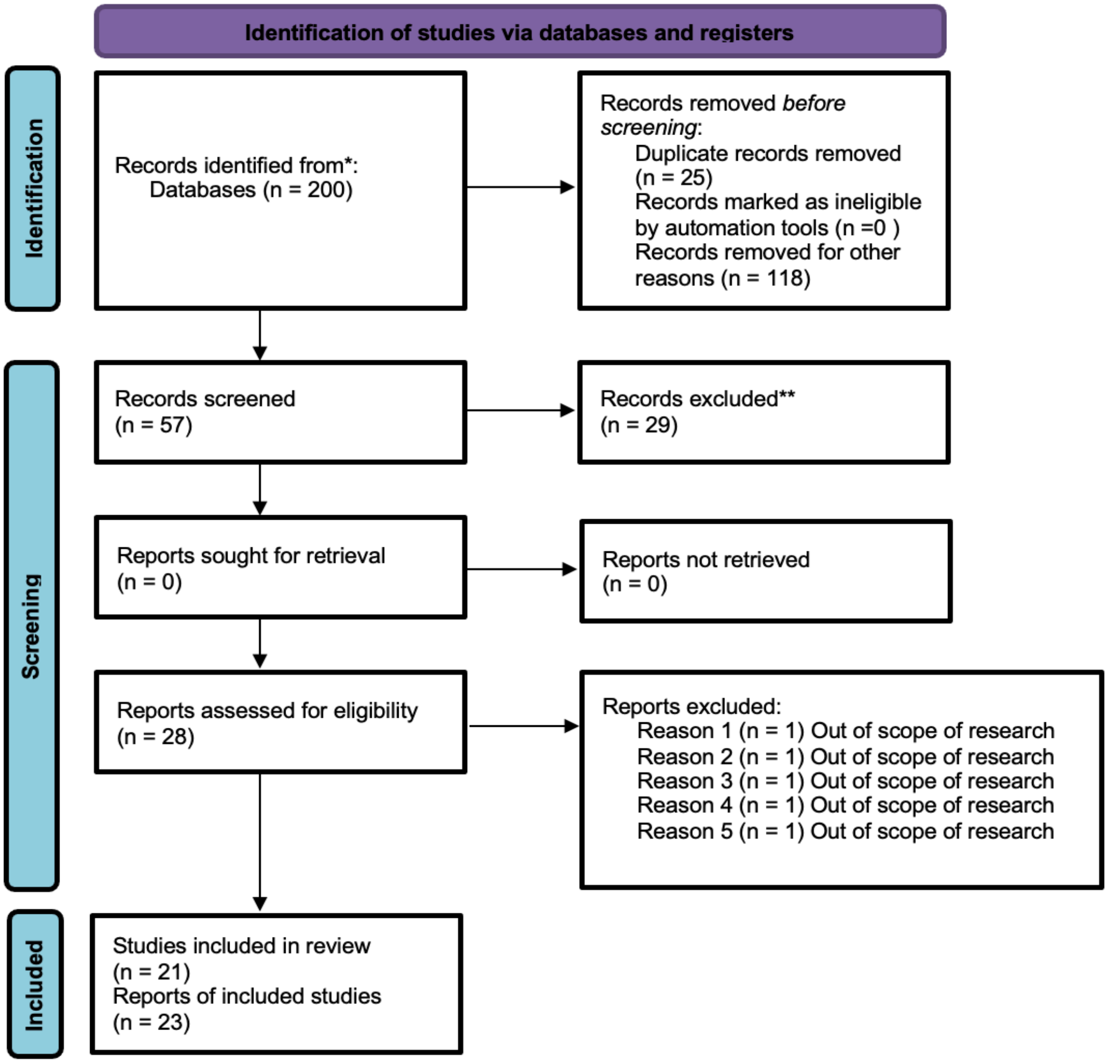

Identification of studies via databases and registers
Identification
Records identified from*:
Databases (n = 200)
Records removed *before screening*:
Duplicate records removed (n = 25)
Records marked as ineligible by automation tools (n =0)
Records removed for other reasons (n = 118)
Screening
Records screened (n = 57)
Records excluded** (n = 29)
Reports sought for retrieval (n = 0)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n = 28)
Reports excluded:
Reason 1 (n = 1) Out of scope of research
Reason 2 (n = 1) Out of scope of research
Reason 3 (n = 1) Out of scope of research
Reason 4 (n = 1) Out of scope of research
Reason 5 (n = 1) Out of scope of research
Included
Studies included in review (n = 21)
Reports of included studies (n = 23)

Figure 3: Shows the PRISMA flow of this systematic review

Then, in the next step, I analyzed all the remaining papers.

3.2 Research limitations

I faced a set of limitations that made me exclude some research papers as I mentioned above, as I could not access some papers for three main reasons.

1. Limited budget for this research
2. Difficulty in communicating with researchers whose research I requested and their delay in responding to me
3. The content of research that talks about the required topics is few, especially in the topics of modification to the blockchain

4. ANALYSIS AND DISCUSSION

After reading all the papers that have been identified, in this section the papers will be analyzed scientifically and the questions that we have previously identified will be discussed in a scientific discussion.

A blockchain is a distributed network where members can interact with each other without a third intermediary, as each member maintains a distributed ledger to record transactions and contracts. Each user must create an account in order to be a participant in the blockchain. Each account has two public keys and a private key. The use of the private key to sign the transaction [17], the blockchain was proposed as a tamper-resistant decentralized distributed architecture. This technology was introduced by a person called Satoshi Nakmoto who provided the first generation of the blockchain and was only limited to financial transactions [20]. The blockchain is basically a ledger. Distributed and decentralized, and the information in it cannot be changed, rather it is kept as it was recorded for the first time [23]. The blockchain is a series of blocks, and each block contains a set of transactions. The block contains a third of major sections: 1 data or transactions, 2 blocks Hash, 3 previous hash block [3], a hash block is like a fingerprint or eye print for each block as it links the blocks to each other, as Image No. 1 is the bitcoin blockchain structure.

There are three main sections of the blockchain [3].

- Public Blockchain: It is a decentralized blockchain in which everyone can see and participate in the information in it.
- Consortium or hybrid blockchain: it is a blockchain whose information can be seen by everyone, but it is controlled by a group of specific ones and it is not completely decentralized because it is controlled from a pre-defined group and not by everyone like a public blockchain, and it is usually used in institutions.
- Private blockchain: The information is exposed to specific people and is controlled by a specific party, and it is also less centralized than the federation blockchain and the public blockchain, and it is used in private companies.

4.1 Question 1: What are consensus algorithms, and what are their challenges, advantages and disadvantages?

To record any transaction in the distributed ledger, the contract (users participating in the blockchain) in the network must agree to the transaction, it is agreed to accept or reject a certain transaction by the contract based on laws and rules previously agreed upon between them, from here came the consensus algorithms. Where the contract will be collected based on previously agreed upon rules that this transaction is acceptable or rejected, and it has also been defined how to reach an agreement in the blockchain network [3], and there are many consensus algorithms, we will mention some of them in this section.

1. Proof of work (PoW): It is the most popular method of consensus, where the puzzle is solved using a lot of complex mathematical operations that require very strong time, energy, and hardware. Hash is relied upon to solve the puzzle, hash: is a complex mathematical formula used to verify the Correct transactions in a block [3].
2. Proof of stack (PoS): This algorithm is based on adding the second block and consensus on it through a different random set of nodes, as the random selection of nodes depends on the treasury transactions and the group of shares [3].
3. Delegated proof of stack (DPoS): This algorithm is improved from the quota proof algorithm as it does not depend on random selection, but rather depends on voting to choose the nodes representing the rest of the nodes to verify the validity of the block, the number of representatives of the nodes is limited, this makes it possible to effectively organize the nodes or more effectiveness [3].
4. Proof of elapsed time (PoET): similar to the (pow) algorithm to solve the hash problem but the miners that will solve the hash is randomly selected depending on the TEE [3].
5. Practical Byzantine fault tolerance (PBFT): This algorithm is used as a pattern where it is responsible for the nodes in the system where all nodes must be participating in the vote, if the vote to add the new block is by two-thirds of the nodes or more, then the block will be added to the string either If it is less than two thirds, it is rejected [3].
6. Delegated practical Byzantine fault tolerance (DPBFT): This algorithm is an improvement over the PBFT algorithm, but not all nodes vote to add a block but rather representatives of the nodes are chosen, and the actors vote to add a block [3].
7. Proof of weight (PoWeight): this algorithm is based on users' weight as habits depend on the amount of money they have [3].
8. Proof of burn (PoB): This method relies on burning a portion of the cryptocurrency to take the reward. The more burning, the greater the percentage of obtaining the next block [3].
9. Proof of Capacity (PoC): This algorithm relies mainly on the use of free space in the storage disk, as the layout of the hard disk, solution computing and storage is created before starting the mining, and whenever the fastest or closest solution is to fragment the last block, the block wins [3].

10. Proof of importance (PoI): This algorithm came to solve the problems and criticisms of the pos algorithm as it depends on the scores and to get the marks there are three factors that will not be mentioned [3].
11. Proof of active (PoA): is a consensus algorithm that combined and combined the POW algorithm and the pos algorithm and is considered a firewall to protect bitcoin [3].
12. Directed Acyclic Graphs (DAGS): It is basically a form of data structure and not a real blockchain network, but it is important and very successful in the Internet of things, the data is stored by means of a graph, the graph is divided into two parts, the first is a non-periodic graph: where no other node can be reached Or refer to it except by passing another node, as for the periodic graph, the path must be predefined [9].
13. Mixe Byzantine falut tolerance (MBFT): This algorithm reduces the branching of the blockchain, or the so-called forks of the blockchain, while ensuring a high tolerance for errors, as it divides the blockchain into two levels, the first being a low level, and the second level being a high level [9].
14. Proof of authentication (PoAH): It is a new consensus algorithm as it is lightweight and compatible with devices of limited sources such as IoT devices. This method follows the traditional communication method where there are only updates, termination of block validation and this consensus algorithm uses the ELGMAL method. To encode [18].
15. Modified algorithm based on the Istanbul algorithm based on fault tolerance: where the algorithm works to reduce the message delay between (COMMIT, PREPARE, PRE-PREPARE), then when choosing the presenter, the block proposal is sent to the rest of the auditors to start creating or launching the pre-preparation stage Then each auditor checks the block proposal and begins the preparation stage through the pre-preparation stage [21].

Table 2

Algorithm	Name consensus algorithms	How to work or what it depends on
POW	Proof of work	Solve the puzzle based on the hash
POS	Proof of stack	Through a random set of nodes
DPOS	Delegated proof of stack	It depends on a group of nodes that have been voted on by the other nodes
POET	Proof of elapsed time	The miners is randomly selected to solve the hash value because it is similar to the POW path
PBFT	Practical Byzantine falut tolerance	All blocks are voted unanimously on the block
DPBFT	Delegated Practical Byzantine falut tolerance	Representatives are chosen for the decade and the cast are the ones who vote to add the block
POWeight	Proof of weight	It depends on the weight of the users, usually on how much they are with
POB	Proof of burn	It depends on burning some or part of the cryptocurrency
POC	Proof of Capacity	It depends on the free space usage of the hard disk
POI	Proof of importance	This algorithm relies on grades, as nodes with more scores are rewarded
POA	Proof of activity	It relies on PoW and PoS algorithm as it merges them together
DAGS	Directed acyclic graphs	The form of data is based on the graph
MBFT	Mixe Byzantine falut tolerance	It depends on dividing the blockchain into two levels, the first low and the second high

POAH	Proof of authentication	It is based on the traditional method of connection
modfiy IBFT	Modified algorithm based on the tolerance-based Istanbul algorithm	It depends on reducing the message timeout and the pre-preparation stage

Table 2

Algorithm	The type of the blockchain network	Energy consumption
POW	decentralization	It needs very high power
POS	There is a kind of centralization	You do not need high energy
DPOS	It has a high central part	It gives excellent energy efficiency
POET	Centralized	You do not need high energy
PBFT	decentralization	Low power
DPBFT	It has a central part	Low power
POWeight	It has a central part	Very efficient in using the energy source
POB	It has a central part	You don't need high power
POC	decentralization	Energy saving due to hard disk usage
POI	It has a central part	You do not need high energy
POA	decentralization	It needs very high power
DAGS	decentralization	Very low power
MBFT	decentralization	You do not need high energy
POAH	decentralization	You do not need high energy
modfiy IBFT	decentralization	Low power

Table 2

Algorithm	Advantages	Defects
POW	High security, and decentralization	High energy needs, computational capabilities and expensive equipment, takes a lot of time, and is not suitable for large and rapidly expanding networks
POS	Mass construction is fast, high productivity, energy efficiency and scalability	There is some kind of centralization, nothing is preventing it from misbehaving in the network
DPOS	Scalability, energy efficiency, low cost transactions	More centralized, it can be used in a private blockchain
POET	High security	Centralized due to dependence on Intel
PBFT	Energy efficiency and high productivity, decentralized	Possible delay due to waiting for the vote
DPBFT	Energy efficiency, delay or wait time is short	It has a central part
POWeight	Takes a lot of customization and is scalable, confirms transactions very quickly and efficiently, i.e. no delay, .energy efficient	There is no reward system
POB	Long-term reward	Suffer from the presence of some central
POC	You do not need special devices, energy-saving, and decentralized	Needs a large amount of storage space in hard drives

POI	Solved the problem of not continuing to participate in PoS, it does not need high power, fast, efficient, there are no special mining devices	Suffer from the presence of some central
POA	Offers high security, especially against .51% attacks	You need a lot of energy
DAGS	Very fast, secure, low power consumption, low transaction fee, its ability to repel 51% attack, and double attack	————
MBFT	Transaction processing speed, increase scalability, do not need high power	There is a kind of centralization
POAH	Fast as it is 200 times faster than PoW, saving energy	————
modfiy IBFT	Fast, ultra-high throughput, low power	————

In the previous table, a quick comparison was made with consensus algorithms, where it was found that each algorithm has advantages and disadvantages, and also that each consensus algorithm can be used in the blockchain to be built according to its work function, but it was also found that the greater the computing process to find the hash value, the safer the algorithm and the more The energy consumption was greater, based on the algorithms mentioned above, and there are great challenges in obtaining a single consensus algorithm that we can apply to a very wide range of applications that provide comprehensive solutions to most problems.

4.2 Question 2: What are the proposed methods of modifying the blockchain and the advantages and disadvantages of the proposed algorithms?

One of the most difficult challenges facing the blockchain is how to modify the blockchain without contradicting any of the blockchain philosophies and without affecting the security and quality of the blockchain, and because the nodes are linked to each other through the hash value, as we mentioned earlier, any modification in a block of blocks is The hash value will change, and if the hash value changes, then the hash values of the whole chain must be changed so that the chain remains consistent, for this modification to the blockchain is impossible in this case, so a set of algorithms and blockchain networks have been built that can be modified without affecting any of the blockchain properties.

1. Modification of the public blockchain using the segmented hash value and side chains: where the modification will be allowed at the transaction level based on the choice of the owner, as the proposed method will be to use side chains to modify the blockchain where a main chain is created to record transactions in the blockchain and then control the start and end of the chain. using the encryption methods that were used in the blockchain in order to adapt easily to the rest of the chain, and also the hash value of the blocks is saved before modification and compared after modification, as the hash value of the block must be equal before modification with the hash value of the block after modification in order to preserve the format of the blockchain, the steps in which this algorithm works will be mentioned without explaining them, as the method works as follows, the transaction is classified, then it is made into a multi-chain structure (main chain and side chains), then approved for a transaction in the main chain, and after that the side chain is controlled from the main chain, after that, the transaction is modified in the side chain, and finally the amendment is executed [1].
2. Chameleon segmentation in the blockchain: This algorithm provides a blockchain model that can be debugged without using heavy cryptographic tools using chameleon hash. The chameleon hash system is built so that it is free from key exposure to a single- trapdoor, where distributed trapdoor technology is used to calculate collisions, merge Polling and consensus strategies, as this technology can be easily integrated with all types of blockchain [2].
3. Segmentation Chameleon updateable TUCH: as it allows automatic loop formation and does not

depend on any other entities to generate the key, as well as the signature of a linkable ring [16].

Table 3

Algorithm	The type of blockchain	Consensus algorithms	Encryption algorithms	Applications
Blockchain modification algorithm using hash value and side chains	Generic blockchain	PoW	Bitcoin crypto algorithms	It cannot be applied in a wide range of applications due to its large energy consumption
Modification algorithm using chameleon segmentation and distributed trapdoor	Public blockchain, federation blockchain, private blockchain	Combining recommendation and consensus algorithms	Light encryption algorithms	It can be applied in many fields because it is based on the voting algorithm and tolerates errors and also does not .consume high energy

Table 4

Algorithm	The type of blockchain	On what he depended on
Blockchain modification algorithm using hash value and side chains	Public blockchain	Hash value, and side chains
Modification algorithm using chameleon segmentation and distributed trapdoor	All kinds of blockchains	Chameleon segmentation, distributed trapdoor
Atines et al	A private or federation blockchain	Chameleon segmentation, use the chameleon scan door key
Delare et al	A private or federation blockchain	Chameleon segmentation
Puddu et al	No mention of the type of blockchain	Fiat was used alongside meta parameters to control unauthorized modifications
Deuber et al	No mention of the type of blockchain	By consensus, if the amendment receives a sufficient number of votes, the amendment is made
Cheng et al	No mention of the type of blockchain	Adjustment based on computing difficulty using Lagrange
Rajasekhar et al	(Private Blockchain (Licensed	Chameleon hash, and a secret magic door key

4.3 Question 3: Are consensus algorithms related to the ability to modify the blockchain and how difficult it is?

From previously reviewed studies and blockchain modification algorithms, it was found that consensus algorithms have a direct relationship to blockchain modification. This is due to the reason that each consensus algorithm has a dedicated method for accepting and verifying new block transactions. The table above shows that the first algorithm has a modification method that fits with my algorithm. PoW as it verifies the transactions through complex mathematical operations through the hash value so that the hash value has been adopted before modification must be equal to its value after modification and this does not fit with all consensus algorithms because not all consensus algorithms depend directly on the hash value but rather on Voting, as for what depends directly on the hash value such as the PoW algorithm, it is possible to apply this algorithm to it, but it needs to be experimented, and we also need to experiment with applying it to other consensus algorithms to see how compatible they are with the existing consensus algorithms, and likewise for the second algorithm, it should be applied to a group. Other consensus algorithms to find out their compatibility with consensus algorithms, because the more consensus algorithms are applied to an algorithm. Modification Mates We could have used modulation algorithms more widely and better and not be forced to specific consensus algorithms.

4.4 Question 4: What are the applications that used blockchain technologies and their challenges?

1. Artificial Intelligence: Blockchain was used in artificial intelligence, as it enabled the creation of a distributed database without manipulating the data because the blockchain does not allow data to be manipulated and this gave a very high efficiency to the blockchain as it also provided high protection against DDOS and DOS attacks, as well as such attacks Blockchain is very expensive, as it gives artificial intelligence a very high data privacy [4].
2. The health field: where a distributed security application called Healthify was established, which is a wide-ranging approach to protecting health data, as a practical application was provided that provides a permanent database and provides easy access to data and smart tools, as it is easy for doctors to access patient data and read patient reports in full. And seeing his medical record in full, as well as users can see their entire medical record in a very easy and secure manner [6], and a platform for exchanging medical information between the responsible authorities such as medical centers, hospitals and the concerned authorities has been proposed in a very safe and effective way. Without being tracked by anyone other than the medical authorities, as this method provides data sharing between medical authorities for users after the user has agreed to each participation request with the ability to track the user's data in detail, and also this system provides a reward for users for sharing information on the reward system Which is in the blockchain [9].
3. Transportation: where transport was used to share data between transportation means in a safe and efficient way, and the paper [7] talks in a large and detailed way about how the blockchain integrates with the automobile system [7].
4. Internet of things: Much emphasis has been placed on the Internet of Things sector and how to make the blockchain applicable to the Internet of things and the limited resources because it is the basis of smart cities and because Internet of things devices have become widespread in the world and need high protection of data, and because IoT devices are present in every detail. Life, including wearable medical devices, as preserving the privacy of data is very important as it relates to human life. This is why there is a lot of interest in the application of the blockchain in the Internet of things and devices with limited resources. The fitness log and the proposed blockchain model protects against the false data injection attack, which could cause someone to die because of this false data [8]. IoT has been integrated with the blockchain to create a secure decentralized infrastructure to provide a secure and scalable communication platform in the smart city [11]. Bookchin has been integrated into control models for the Internet of Things [17].
5. Business sector: where the blockchain has been integrated into the business sector so that data can be accessed in a very easy and secure manner [13].
6. The education sector: The blockchain has been integrated into the education sector, in order to facilitate access to any student's data in a safe and fast manner, for example if a student wants to transfer from school to school or from university to university, he must attend official papers in order to transfer and the procedures are complicated until verification is achieved. From the certificates and the transfer process takes place, with the integration of the blockchain, it is possible to store student data and testimonials without anyone tampering with them as the blockchain guarantees that the data will not be tampered with because it is not subject to modification and only the educational authorities and students can access student data, and thus the blockchain provides a system for sharing data In an effective and safe manner, which facilitates transfer and admission procedures in schools and universities [14].

4.5 Question 5: What are the challenges and limitations facing the blockchain?

There are many challenges and limitations facing the blockchain technology until it is completed or even more widely used in applications, as due to the many challenges and limitations and its difficulty, full studies have been made mentioning what the challenges and limitations of the blockchain are, some challenges and some problems have been resolved, but the rest of the many challenges and restrictions have not been Solve it after.

4.5.1 Blockchain challenges and limitations

I will mention part of the challenges and limitations facing this promising technology. For example, one of the most common problems that are being solved is the problem of the large energy consumption of the blockchain, as such a problem restricts its ease of use for excessive energy consumption of some consensus algorithms and also increases its challenges for its developers and operators on how to break This limitation, some solutions have been developed by suggesting other consensus algorithms, but other problems appear, such as that consensus algorithms do not depend on strong encryption algorithms such as those in Bitcoin, and also the problem of modifying the blockchain or the right to be forgotten as there are no effective algorithms as they should be so that it is easy to use And in order to comply with the restrictions of use in the United States and the European Union, as well as the 51% attack, as there are some consensus algorithms that cannot repel the 51% attack, as well as the double attack, and the size of the blockchain is very large, and the blockchain also suffers from a lack of productivity, and also the difficulty of using Blockchain in devices with limited source, this makes it slow to spread and this is one of the important limitations of blockchain technology and makes the challenge difficult for the developers of this technology because E. The easier the spread of this technology, the easier it is to use, and the longer life remains. There are many and many challenges facing the blockchain, which are being worked on by researchers. Of course, there are some problems that have been solved, but the solution is either for one of the cases of the blockchain or one of the problems Blockchain problems and not a radical solution that makes us able to use the blockchain easily and apply it to a wide field of applications or generalize it to a wide range of applications.

5. CONCLUSION AND FUTURE WORK

It is clear that blockchain technology is considered a very promising and very important technology and will revolutionize the world of information technology, as it will give new concepts of privacy, as data manipulation is impossible, so it can be applied in several important areas, and on the other hand it faces significant limitations and challenges, and this makes it difficult Its application in a group of other applications that need to modify data while preserving all the advantages of the blockchain, and other problems previously mentioned, where all restrictions must be overcome and all challenges resolved in order for it to spread on a large and large scale and easy to use in all applications, this study will contribute positively to knowing And understanding what the blockchain is and its advantages, and also contributed to the presentation of a group of applications that have been studies and applications for the application of the blockchain in a group of important sectors, such as smart cities, the Internet of things and medical sectors, and the very important thing presented by this study is to focus on ways to modify the blockchain and a good understanding of the challenges Modifying the blockchain and its limitations, which made us work on displaying consensus algorithms that are an important part of the blockchain, modifying them, and applying them to a wide and important group in the industry. This study presented a set of important limitations and challenges facing such an exciting technology.

1. Investors and businessmen are afraid of adopting it mainly because it is a new technology and faces a set of restrictions and challenges.
2. The difficulty of verifying transactions by governments as they may contain illegal information.
3. Incompatibility with the EU and US list.
4. consensus algorithms that have high protection against attacks consume too much power and the solutions presented are not as complete as they should be.
5. The possibility of spreading over a wide field requires a very high effort, as consensus algorithms must be compatible with energy consumption, and the ability of processors to process consensus algorithms.
6. The difficulty of being able to modify the blockchain while fully preserving the characteristics and advantages of the blockchain, because the spread of the blockchain on a wide

field includes its entry into the Internet of Things and its likes that need the necessity of verification and modification of transactions in the blockchain because of the errors resulting in the Internet of things and similarities as mentioned previously.

7. Some consensus algorithms that provide solutions to avoid excessive energy consumption, need high storage space.

And also our study indicates that a set of methods and algorithms have been developed to modify the blockchain in safe and effective ways, but it needs further study, as two methods were presented in detail, where the first method proposes modifying the blockchain using the hash value with side chains where the hash value of the block before modification is equal to it after modification. In order for the chain to remain consistent, of course, modification in this method is based on the degree of difficulty [1], and the other method suggests using chameleon and trapdoor segmentation to calculate collisions and integrate voting and consensus strategies [2]. The previously proposed amendment was proposed to the private or licensed blockchain, and the amendment to the public blockchain was not proposed in this way, as well as the most famous consensus algorithms and knowledge of their working methods and their advantages and disadvantages as shown in Table 2, as it turned out that the most common problems related to consensus algorithms are High energy consumption, how to make consensus algorithms compatible with devices with limited resources, whether they are limited in energy or processing, and also how Making consensus algorithms faster and better, as it has also been shown that consensus algorithms may affect modification methods, as consensus algorithms are the basis for accepting and verifying transactions in the blockchain. From this matter through experience, as the blockchain has been applied to a range of applications, including artificial intelligence, where the use of blockchain as a distributed database for artificial intelligence applications has made artificial intelligence safer and more effective due to the inability to tamper with the data and the blockchain has been able to provide a safe environment from attacks. Malicious and stable [4], and in the health field, a proposal has been submitted for a blockchain-based system called Healthify that provides a safe environment for health data [6]. Also, another system has been proposed that shares medical data using blockchain as it provides a stable and decentralized database that provides ease. Sharing information in a safe and effective way, where the author says that users can also get some money (rewards) in exchange for sharing a statement Charged based on the way the blockchain works as it provides rewards based on the way the consensus algorithm works, and the user can track his data and where it was shared and used easily [9], and in the field of transport a mechanism was proposed to share data between transportation means in a secure and decentralized manner [7], In the Internet of Things, several mechanisms and methods were proposed to make the blockchain applicable to Internet of things devices. A fitness model based on the blockchain was proposed that protects data, especially from false injections or false data [8], and the blockchain has also been integrated into the Internet of Things (IoT) control models [8],[17], and in education, a model was proposed for sharing student data and educational data in a safe, stable and decentralized environment that facilitates access to original information and certificates and verification of them in a fast and safe way from manipulating data [14]. Development and testing of algorithms for modification and consensus will enable this technology to spread widely and will be used in most applications, and it will play a major role in changing concepts and changing users' perceptions of safety and stability of the product. In technology, the prototypes were very promising and confirm that blockchain technology is very promising, and in the future more studies and evaluations of the blockchain will be conducted, and most importantly, we hope to provide practical solutions that make the application of blockchain in a wider range of applications very easy.

6. ACKNOWLEDGMENT

The authors wish to thank Palestine Technical University-Kadoorie (PTUK) for supporting this research work as part of PTUK research fund.

REFERENCES:

[1] Nam-Yong, Et Al, "Modifiable Public Blockchains Using Truncated Hashing And Sidechains." Ieee Access, No. 7, 2019, Pp. 173571-173582.

[2] Wu, Chunhui, Lishan Ke, And Yusong Du. "Quantum Resistant Key-Exposure Free Chameleon Hash And Applications In Redactable Blockchain." Information Sciences, No. 548, 2021, Pp. 438-449.

[3] Seyed Mojtaba Hosseinibamakan, Et Al ,"A Survey Of Blockchain Consensus Algorithms

Performance Evaluation Criteria", Expert Systems With Applications, No. 154, 2020, Pp. 113385.

[4] Panda, Soumyashree S, And Debasish Jena, "Decentralizing Ai Using Blockchain Technology For Secure Decision Making." Advances In Machine Learning And Computational Intelligence. Springer, Singapore, 2021, Pp. 687-694.

[5] Tuan-Vinh Le, And Chien-Lung Hsu, "A Systematic Literature Review Of Blockchain Technology: Security Properties, Applications And Challenges" Journal Of Internet Technology, 2021.

[6] Sharma, Pratima, Rajni Jindal, And Malaya Dutta Borah. "Healthify: A Blockchain-Based Distributed Application For Health Care." Applications Of Blockchain In Healthcare. Springer, Singapore, 2021,Pp. 171-198.

[7] N.Khoshavi,G.Tristani, And A.Sargolzaei ,"Blockchain Applications To Improve Operation And Security Of Transportation Systems: A Survey", Electronics ,No. 10, 2021.

[8] Jamil, Faisal, Et Al. "Towards Secure Fitness Framework Based On Iot-Enabled Blockchain Network Integrated With Machine Learning Algorithms." Sensors ,No. 21, 2021.

[9] M. Du, Q. Chen, J. Chen And X. Ma, "An Optimized Consortium Blockchain For Medical Information Sharing," Ieee Transactions On Engineering Management, 2020,Pp. 1-13.

[10] V. Manjula, R. Thalapathi Rajasekaran "Security Vulnerabilities In Traditional Wireless Sensor Networks By An Intern In Iot, Blockchain Technology For Data Sharing In Iot" Principles Of Internet Of Things (Iot) Ecosystem: Insight Paradigm, No. 174,2020.

[11] A. E. Bekkali, M. Boulmalf, M. Essaaidi And D. E. Majdoubi, "Towards Blockchain-Based Architecture For Smart Cities Cyber-Security," International Conference On Electrical And Information Technologies (Iceit), 2020, Pp. 1-6.

[12] Khamar, Jalpa, And Hiren Patel. "An Extensive Survey On Consensus Mechanisms For Blockchain Technology." Data Science And Intelligent Applications. Springer, Singapore, 2021, Pp. 363-374.

[13] S.Gomathi, Et Al "A Survey On Applications And Security Issues Of Blockchain Technology In Business Sectors" Materials Today: Proceedings, 2021.

[14] J.Kaur,J.Oswal "A Review Of Blockchain Technology In Education" Jac : A Journal Of Composition Theory, 2020.

[15] Jorge Bernal Bernabe, Et Al. "Privacy-Preserving Solutions For Blockchain: Review And Challenges" Ieee Access, No. 7, 2019, Pp. 164908 - 164940.

[16] Huang, Ke, Et Al, "Scalable And Redactable Blockchain With Update And Anonymity." Information Sciences, No. 546, 2021, Pp. 25-41.

[17] I. Riabi, H. K. B. Ayed And L. A. Saidane, "A Survey On Blockchain Based Access Control For Internet Of Things," International Wireless Communications & Mobile Computing Conference (Iwcmc), 2019, Pp. 502-507.

[18] D. Puthal, Et Al, "Proof-Of-Authentication For Scalable Blockchain In Resource-Constrained Distributed Systems," Ieee International Conference On Consumer Electronics (Icce), 2019, Pp. 1-5.

[19] L.Alharbi,D.Aljeaid "A Blockchain Review: A Comparative Study Between Public Key Infrastructure And Identity Based Encryption Bt - Advances In Data Science, Cyber Security And It Applications" Springer, Cham, 2019 ,Pp. 69-81.

[20] Bhushan, Bharat, Et Al. "Untangling Blockchain Technology: A Survey On State Of The Art, Security Threats, Privacy Services, Applications And Future Research Directions." Computers & Electrical Engineering, No. 90, 2021, Pp. 106897 .

[21] Samy, Hossam, Et Al. "Enhancing The Performance Of The Blockchain Consensus Algorithm Using Multithreading Technology." Ain Shams Engineering Journal ,2021.

[22] Kakarlapudi, Prasanth Varma, And Qusay H. Mahmoud. "A Systematic Review Of Blockchain For Consent Management." Healthcare, Vol. 9, No. 2, 2021.

[23] H.Atlam,M.Azad,A.Alzahrani, Et Al "A Review Of Blockchain In Internet Of Things And Ai" Big Data And Cognitive Computing, Vol. 4, 2020.

[24] S. Nakamoto. (2008). Bitcoin: A Peer-To-Peer Electronic Cash System. [Online]. Available: Https://Bitcoin.Org/Bitcoin.Pdf.

[25] T. Mcghin, K.-K. R. Choo, C. Z. Liu, And D. He, ''Blockchain In Healthcare Applications: Research Challenges And Opportunities,'' J. Netw. Comput. Appl., Vol. 135, 2019, Pp. 62–75, Jun.

[26] M. M. H. Onik And M. Ahmed, ‘‘Blockchain In The Era Of Industry 4.0,’’ In Data Analytics, M. Ahmed And A. K. Pathan, Eds. Boca Raton, Fl, Usa: Crc Press, 2018, Pp. 259–298.

[27] Worldwide Semiannual Blockchain Spending Guide. [Online]. Available: Https://Www.Idc.Com/Tracker/Showproductinfo.Jsp? Prod_Id=1842,4, /Mar. /2019).

[28] General Data Protection Regulation (Gdpr). [Online]. Available: Https://Eugdpr.Org/,14/Apr / 2016.

[29] P. Carey, Data Protection: A Practical Guide To Uk And Eu Law. New York, Ny, Usa: Oxford Univ. Press, 2018.

[30] (Mar. 20, 2018). Child Abuse Imagery Found Within Bitcoin’s Blockchain. [Online]. Available: Https://Www.Theguardian.Com/Technology/2018/ Mar/20/Child-Abuse-Imagery-Bitcoin-Blockchain-Illegal-Content.

[31] G. Ateniese, B. Magri, D. Venturi, And E. Andrade, ‘‘Redactable Blockchain—Or—Rewriting History In Bitcoin And Friends,’’ In Proc. Ieee Eur. Symp. Secur. Privacy (Eurosp), Apr. 2017, Pp. 111–126.

[32] D. Deuber, B. Magri, And S. A. K. Thyagarajan, ‘‘Redactable Blockchain In The Permissionless Setting,’’, Arxiv:1901.03206. [Online]. Available: Https://Arxiv.Org/Abs/1901.03206, Jan/ 2019.