Iraqi Journal of Science, 2023, Vol. 64, No. 10, pp: 5301- 5321
DOI: 10.24996/ijs.2023.64.10.36

ISSN: 0067-2904

Blockchain in Realistic Areas of Application and Difficulties Encountered: A Survey Study

Mina H. Madhi[1 *], Abbas M. Al-Bakry[2] , Alaa Kadhim Farhan[3]
[1]*The Informatics Institute for Graduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq*
[2]*University of Information and Communication Technology, Baghdad, Iraq*
[3]*Department of Computer Sciences, University of Technology, Baghdad, Iraq*

Received: 3/4/2022 Accepted: 11/11/2022 Published: 30/10/2023

Abstract

Blockchain technologies have grown in popularity over the last few years, with various experts touting the technology's potential applications in a range of businesses, markets, organizations, and governmental institutions. In the brief history of blockchain, an astounding number of incredible implementations have been done in terms of how it may be utilized and the potential effect it may have on a range of sectors. And, because of the great number and complexity of these characteristics, addressing the blockchain's potential and complications can be difficult, especially when seeking to address its purpose and fit for a certain activity. The blockchain's practical skills in fixing multiple challenges that are currently preventing further progress in various industrial fields are significant benefits. Securing and sharing transactional data, automating and optimizing supply chain procedures, and enhancing transparency throughout the value chain are just a few of the issues that companies are concerned about. Blockchain technology efficiently overcomes these challenges by leveraging distributed, shared, secure, and permission-based transactional ledgers. This paper concentrates on the many industrial application domains that blockchain technology offers. In addition, it examines and investigates the benefits, drawbacks, and challenges of incorporating blockchain into various industry applications, as well as defines the criteria for using blockchain in multiple industry applications and provides a brief overview of the technology.

Keywords: Blockchain, Technology, Distributed, Application, Cyber Security, IoT.

سلسلة الكتل في مجالات التطبيق الواقعية والصعوبات التي واجهتها: مراجعة

مينا حبيب [1*], عباس البكري[2], علاء كاظم[3]
[1]كلية المنصور الجامعة , بغداد، العراق
[2]جامعة تكنولوجية المعلومات والاتصالات , بغداد، العراق
[3]الجامعة التكنولوجية , بغداد، العراق

الخلاصة

ازدادت شعبية تقنيات سلسلة الكتل Blockchain على مدار السنوات القليلة الماضية ، حيث قام العديد من الخبراء بالترويج للتطبيقات المحتملة للتكنولوجيا في مجموعة من الشركات والأسواق والمنظمات والمؤسسات الحكومية. في التاريخ المختصر لـ blockchain ، تم إجراء عدد مذهل من التطبيقات المذهلة من حيث كيفية

*Email: mina.habeeb@muc.edu.iq

استعمالها والتأثير المحتمل الذي قد يكون لها على مجموعة من القطاعات. وبسبب العدد الكبير لهذه الخصائص وتعقيدها ، فإن معالجة إمكانات blockchain ومضاعفاته قد يكون أمرًا صعبًا ، لا سيما عند السعي إلى معالجة غرضه ومدى ملاءمته لنشاط معين. تعتبر المهارات العملية في تقنية blockchain في إصلاح التحديات المتعددة التي تمنع حاليًا المزيد من التقدم في المجالات الصناعية المختلفة فوائد كبيرة. يعد تأمين ومشاركة بيانات المعاملات ، وأتمتة إجراءات سلسلة التوريد وتحسينها ، وتعزيز الشفافية في جميع أنحاء سلسلة القيمة ، مجرد عدد قليل من المشكلات التي تهتم بها الشركات,تتغلب تقنية Blockchain بكفاءة على هذه التحديات من خلال الاستفادة من دفاتر المعاملات الموزعة والمشتركة والآمنة والقائمة على الإذن. تركز هذه الورقة البحثية على العديد من مجالات التطبيقات الصناعية التي تقدمها تقنية blockchain. بالإضافة إلى ذلك ، فإنه يفحص ويبحث في مزايا وعيوب وتحديات دمج blockchain في تطبيقات الصناعة المختلفة. بالإضافة إلى تحديد معايير استعمال blockchain في تطبيقات صناعية متعددة ، ويقدم نظرة عامة موجزة عن التكنولوجيا.

1. Introduction

The world of technology is advancing at an alarming rate. This trend will only worsen in the coming years as brilliant minds devise creative ways to make everyday life easier and more accessible to everyone [1]. Whether this trend continues or not, the consequences will be felt not just in daily life but also in the corporate sector as a whole [2]. And for this development, there is an urgent need to improve the business and trade markets, as well as all parts of the business, as well as the requirement for a safe and effective system, as well as the low demand for human labor [1]. For that reason, the concept of blockchain was born, introducing new technological features to the corporate and industrial worlds [3]. Because of blockchain, business models that would have been impossible to create just a few years ago are now feasible [4]. It employs a variety of strategies, which means it operates on a concept that can be reduced since everyone engaged can agree on its content, and all transactions are secure and cannot be changed once they have been added. It also allows for extensive tracking [5]. Using the blockchain, a group of businesses can agree on a certain activity and register it without the need for a regulatory authority. A blockchain can be used to record, secure, and transmit their agreed-upon action. Activities that are agreed upon include a monetary transaction between members, purchasing an item, voting, or entering a patient's medical lab test results. In addition to contractual arrangements and multi-party collaboration on specific tasks, logistics in the supply chain are also instances of such processes [6].

The most basic example of a blockchain is bitcoin. That is to say that there is no need to use a bank or a third party for any financial or commercial transfer because all transactions are available to all parties. Blockchain keeps a history or keeps records for everyone, and it is available, which means that anyone in the network can follow or track any conversion process for these parties [7]. In terms of structure and accessibility, blockchain technology (BT) is classified into three categories: first-generation public blockchains (blockchain 1.0), second-generation public blockchains (blockchain 2.0), and third-generation private blockchains (blockchain 3.0 and 0.2) [8]. Following this, the three generations have Blockchain 1.0 connects cryptocurrencies to traditional financial applications such as currency transfers, settlements, and digital payments. Smart contracts for commercial markets and financial applications are included in Blockchain 2.0. This group is in charge of much more than just money exchange. Stocks, bonds, loans, mortgages, titles, smart properties, and smart contracts are all included. Third-category applications are those that are unrelated to currency, money, or markets. They include sections on governance, health, science, literacy, culture, and art [8] and [9].

In addition to decentralized ledgers and distributed ledgers, blockchain technology also incorporates cryptography, a peer-to-peer network, consensus, and smart contracts. The

openness, security, and dependability of the blockchain can be attributed to these key technologies [10]. Creating blockchain applications is impossible without ensuring the security of the data stored on the blockchain. Assailants are already taking advantage of the blockchain's features to conduct multiple attacks on its data, placing it at risk and mandating its protection [11]. As a result, demand for blockchain cyber security was high [12]. This paper summarizes and examines the security of blockchain data. It's important to understand how blockchain data might be harmed and how it can be protected.

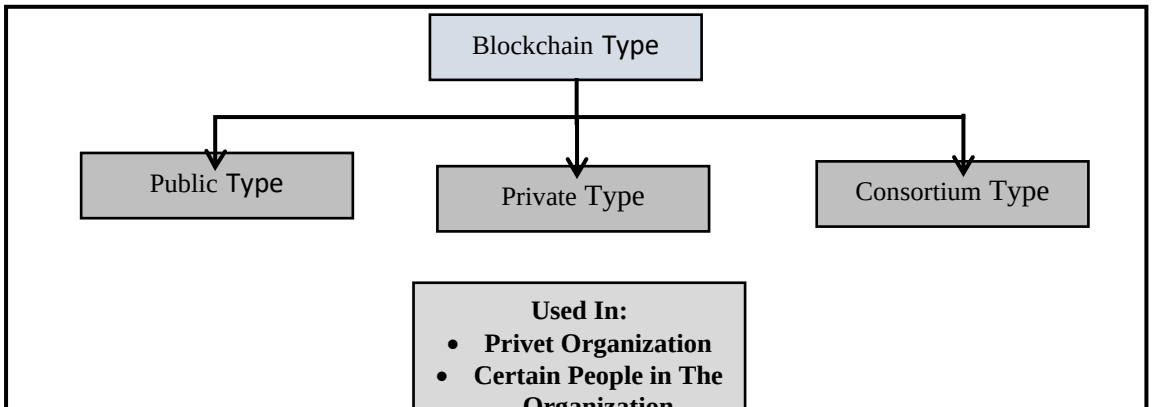
2. Blockchain

Similar to a typical public ledger, the blockchain is a collection of blocks that record every transaction [13]. Essentially, each block contains a hash of the previous block, which is referred to as a "parent block." In the Ethereum blockchain, the hashes of uncle blocks would be listed as "children of the block's forefathers" [14]. Consider "completed transaction blocks" as a data structure that is spread across a network, and the blockchain subdivisions are a subset of this data [15]:

- Public Blockchain
- Private Blockchain
- Consortium Blockchain

Because the public is available to everyone, there are no restrictions on who can participate or be a validator. On a public blockchain, no one has complete control over the network. For cryptocurrencies such as Bitcoin, Ethereum, and Litecoin, public blockchains are used because no single individual can change the blockchain, which guarantees data security and immutability [16]. Private means that only a limited number of people can access it and participate in transactions and validation (also known as "permissioned blockchain"). The blockchain can only be accessed by pre-approved organizations. Each of these businesses is selected by a reputable authority and permitted to operate by the blockchain developers. It is common for private organizations to utilize blockchains to store sensitive information that should only be accessible to a limited number of employees. There is no public access to data on a private blockchain because it's a closed blockchain [17]. One of the main features of a consortium blockchain is that some nodes are in charge of reaching consensus, while others can participate in transactions.

There are three types of blockchain: public, private, and consortium. The blockchain is public since it is shared by many nodes, but it is also private because only a small number of nodes can access it. This results in both public and private space [18]. Figure 1 shows how the subdivision above may be summarized:



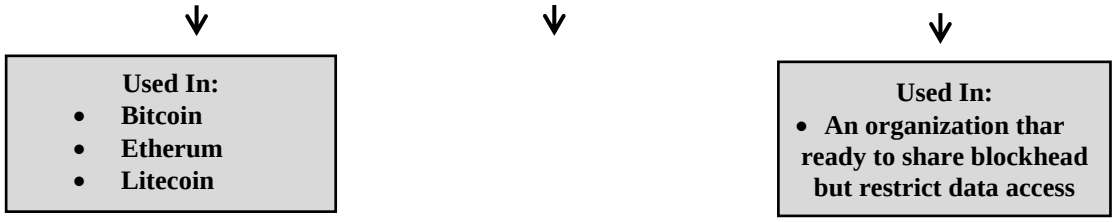


Figure 1: Blockchain Type and Used [19].

Blocks with transactions in a certain order make up the blockchain technology framework. All of the following information is available in the following formats: Consideration is required for both of the key data structures in blockchain [20]:

- Variables that keep track of the position of another variable are known as pointers. This indicates the position of a variable.
- A linked list is composed of a series of blocks, each containing its own set of data and a pointer to the next block.

The blockchain's structure is a block hash, which serves as unique identification as well as the timestamp and group of transactions. In the block's header, the hash value is kept [21]. The blockchain structure is depicted in Figure 2 as follows:

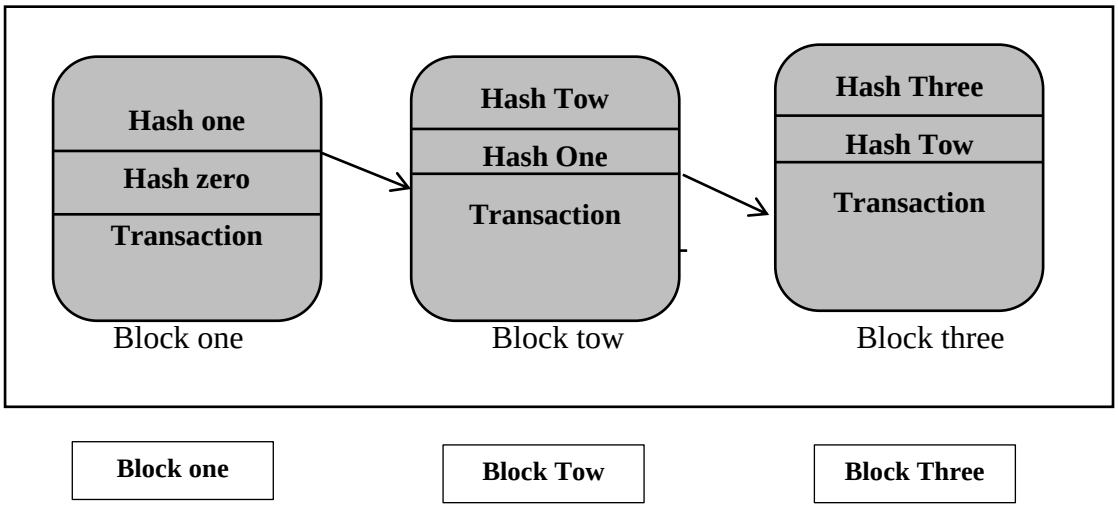


Figure 2: Block Structure [22].

And the important term is "blockchain secure." The fundamental reason for this is the fact that it has spread. Because the data is stored in numerous nodes, the person seeking to modify the record may need to change all of the nodes' records. The network will refuse any attempt to modify the block. Cryptography also contributes to the security of the data in the block. While any user may examine transaction data, they cannot read personal information about the individual who performed the transaction. As a consequence, the user's privacy is protected [23].

2.1 Block structuring of blockchain.

A block is composed of many parts, such as the block header and the block body. A transaction counter and transactions comprise the block body. The maximum number of transactions that may be stored in a block is determined by the block size and transaction size.

To validate transaction authenticity, Blockchain employs an asymmetric cryptographic technique. In an untrustworthy environment, an asymmetric cryptographic digital signature is used [3]. Table 1 shows the summary of the above, classified as follows:

Table 1: Data types in each block.

Ref	Section	Characterization
[24]	**Main Data**	Transaction data will be stored in blocks. This transaction data is determined by the blockchain's utilization factor or the relevant services for which the blockchain is used.
[25]	**Data**	Any data can be stored on the block. Transaction records, medical records, insurance records, legal records, property ownership records, and so on are all examples of transaction records.
[26]	**Timestamp**	The timestamp indicates the date and time when a specific block was created.
[27]	**Block Properties**	Each block in the blockchain is made up of three parts: the hash, the data, and the previous block.
[28]	**Hash value**	Each block's hash is a unique identifier generated by a cryptographic hashing method such as SHA-256. The hash of the current block as well as the hash of the prior block will be stored in the block. Due to hashes, the blocks are immutable. To generate hashes, the Merkle tree function is utilized. It is kept in the header of the block.
[29]	**Hash Function Operation**	A hash function accepts an integer as an input and returns a string of the given length. The hash function produces distinct outputs for various messages while producing similar results for the same input. There are various internal states in a hash function. It will make the necessary adjustments to those internal states in response to the message it receives. Internal states will vary as a result of permutations and combinations, making determining the input message from the hash output nearly impossible. This means we can't predict or know the outcome because we don't know what it is. In blockchain technology, hashing a block requires a significant amount of computational power.

2.2. Blockchain Technology

According to contemporary experts, the blockchain's essential concepts include the hash function, Merkle tree, timestamp service, consensus mechanism, peer-to-peer network technology, and asymmetric encryption technology. Numerous experts have undertaken pertinent research on the blockchain's previously outlined fundamental ideas. This section describes the hash function, Merkle tree, and consensus mechanism used to build a blockchain's private chain [20]. To accurately describe these three notions, they will be separated into Table 2, which details their characteristics:

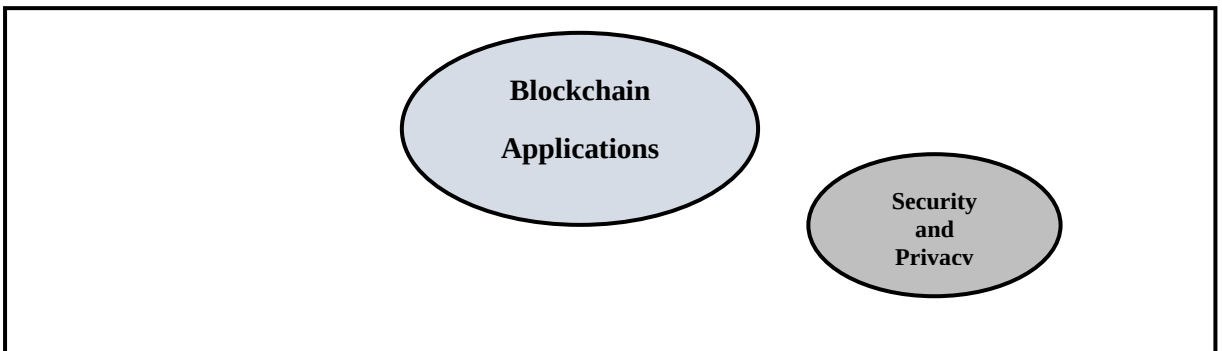
Table 2: Description of Fames Mechanism

Name of mechanism	Description	advantage
hash function [30]	A hash function is a mathematical procedure that produces an array from any given collection of data.	To avoid tampering with transaction and block data, hashed versions of the data are generated.

Merkle tree [31]	The data structure of a multiforked tree is similar to that of a binary tree, with leaf nodes, intermediate nodes, and root nodes. Details on the transactions and other information may be found on the bottom leaf.	Security and validity of data are ensured by proving that any malicious tampering with the data is quickly noticed by other nodes in the network.
Consensus [32]	The fundamental notions of the blockchain are predicated on the concept of consensus. Nodes on the blockchain network will be able to reach consensus more reliably with the help of this technology.	The blockchain network design must ensure that nodes generate consensus in the order in which they receive the same message within a specific period.
timestamp service [33]	However, it is the time at which a computer records the occurrence of an event rather than the event's actual time. It normally records the incident's date and time, which are precise to a fraction of a second.	It works with data that is consistent with the real data, making it simple to compare two separate records and track development over time.
P2P network [34]	Each node in the blockchain's peer-to-peer network design is treated equally to all other nodes, and each node may operate as both a client and a server, providing the network with a very broad margin of error for nodes going down and network transit difficulties.	The network is usually in charge of verifying ledger records. To make any modifications within blocks, more than half of the network's users must agree.
asymmetric encryption [35]	By providing authentication and authorization, it ensures the integrity, accountability, and nonrepudiation of power transactions. Additionally, in asymmetric cryptography, the public-private key pair can help ensure the secrecy of data.	The use of asymmetric encryption in blockchain technology can significantly increase authentication and authorization levels, thus safeguarding consumers' privacy and the integrity of electrical data.

2.3 Blockchain Applications

Blockchain technology offers a plethora of applications that extend far beyond electronic money and bitcoin. With its capacity to promote transparency and justice while simultaneously saving organizations time and money, technology is affecting a broad variety of sectors, from contract enforcement to government efficiency [36]. Figure 3 represents the application of blockchain [14].



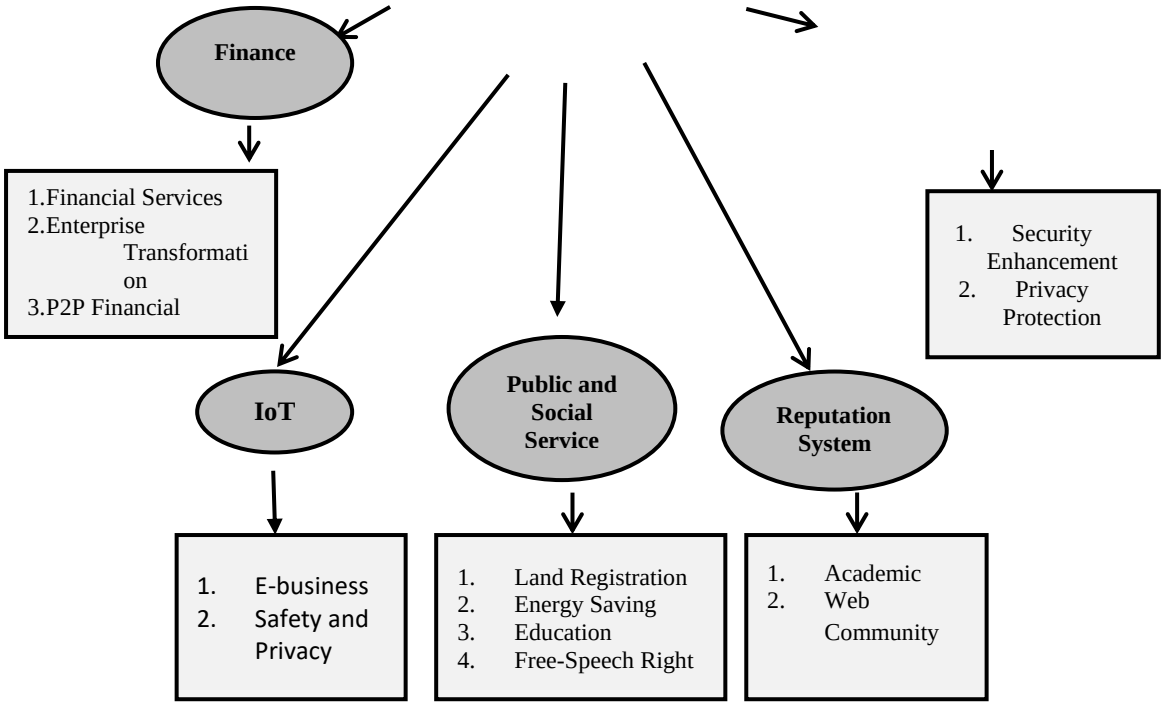


Figure 3: blockchain application [32]

As seen in the figure above, there are five critical areas for blockchain applications: finance, IoT, public and social services, reputation systems, and security and privacy. Table 3 summarizes the fields of application for these applications, along with their associated benefits and drawbacks.

Relying on Table 3, the most important applications that depend on blockchain technology can be listed [31], [39]:

- Blockchain for the health care industry.
- Electronic medical records.
- Bitcoin.
- Smart contact
- Ledger
- Ethereum.

Table 3: blockchain application [37],[38],[14].

Name	Domain	Advantage	Disadvantage

Finance	The critical nature of blockchain technologies such as Bitcoin	Traditional banking and commercial services have been greatly impacted.	Blockchain has the potential to revolutionize the financial industry.
IOT	Information and communication technologies that are most promising (ICT),	Consumers can access a variety of killer IoT applications, such as logistics management using Radio-Frequency Identification (RFID) technology, smart homes, smart grids, and the maritime industry.	We may need expensive materials and components.
Public and Social Service	The term is frequently used in public and social services.	It expands knowledge, creates social and educational opportunities, and preserves the zone's social cohesiveness and significance through marriage registration, patent management, and income taxation procedures. In this manner, considerable paperwork may be saved.	We need different types and stretches of blockchain.
Reputation System	A person's reputation can be assessed based on past transactions and contacts with the community.	It can potentially solve the problem of faking customers to achieve	There are an increasing number of instances of personal reputation records being fabricated, and these cases are growing at a rapid pace.
Security and Privacy	Security enhancement and privacy protection	might contribute to the enhancement of the security of dispersed networks. Specifically, it can safeguard data against these privacy concerns.	This sort of data may be impacted by the growing risk of our private data being exposed to malware, as well as the fact that numerous mobile services and social network providers are collecting our sensitive data.

What is meant by "blockchain for the health care industry"? Nowadays, patients are hesitant to disclose their treatment plans to strangers. Patients can utilize this technology to keep all information private and secure from prying eyes in this scenario. A web browser or a mobile application can be used to access this blockchain. Each user on a blockchain has two keys. Keys are divided into two types: public and private. Only those with access to this can execute a transaction. Electronic medical records are also medical records. With the use of blockchain technology, all of this may be avoided .

Because blockchain was designed largely for the exchange of digital currency, a smart contract is sometimes known as a crypto contract, and paying a middleman is unnecessary. As a consequence, you will save time and effort. A ledger is used in smart contracts. Each participant

in a blockchain is issued a unique identification because it is a decentralized program. When a transaction is completed, it is immediately recorded in the ledger. Ethereum is a blockchain-based, decentralized network. Decentralized apps may now be constructed and deployed. Ethereum is a digital currency that works similarly to Bitcoin because it is a public blockchain network that is decentralized .

2.4 Challenge of Blockchain

As a new technology, blockchain is confronted with a slew of issues and concerns, which can be categorized into several challenges based on studies and research [32]. It is largely recognized as a significant technical achievement, having already attracted the interest of numerous big corporations. The application of blockchain technology has exploded in popularity during the last several years [40]. The most well-known of these challenges are illustrated in Table 4.

Table 4: Challenges of blockchain

Challenges name	Described
Internet of Things (IoT) [9]	Human-machine interaction and machine-to-machine communication are typically used to enable a smart workforce. While data suggests that IoT and blockchain technologies have several significant advantages, they also have several significant downsides. These obstacles stem from the need to address security and privacy concerns. Interoperability, legal problems, a lack of standards, access control, regulatory concerns, developmental concerns, and developing IoT economic concerns are just a few of the challenges that IoT and blockchain technologies must overcome.
Healthcare system [36]	The approach exemplifies an innovative use of blockchain technology. Adopting blockchain to pay fees in Bitcoin benefits all parties, including hospitals, healthcare providers, and health authorities, by publicizing consumer choices and maintaining patient privacy. When information consumers wanted to see a patient's paper medical record, they had to fill out a form and submit it to the registration office. Following approval, the information consumer will pay a copy charge to the cashier and be given a bill of sale. Following that, the information consumer takes the receipt to the registration office to receive a copy of the patient's medical records. However, a patient's medical data may be misplaced or reproduced for illegal purposes.
Spreading [41]	As more individuals became acclimated to it, the average transaction grew dramatically. It had a significant impact on transaction processing speed since a larger population indicates more computers writing to and accessing the network, resulting in a more cumbersome system overall.
Attack [42]	Due to the lack of government regulation in the blockchain industry, it is a volatile environment that is ripe for market manipulation. There is always a chance that your online wallet will be hacked or that it will be blocked by the government for engaging in any dubious activity.

Security [43]	A blockchain is a public ledger that can be viewed by anyone. In many circumstances, it is necessary, but when employed in a delicate context, it becomes a liability. Blockchain technology still has a long way to go before it is widely embraced. The ledger needs to be redesigned in such a way that it can only be accessed by those who are permitted to see it.
Economic aspect [44]	In the value transfer process, blockchain is often utilized to lower the costs associated with third-party intermediaries and middlemen. Although there are many advantages to blockchain technology, it is still in its infancy, making it difficult to integrate into existing systems. As a result, it's out of reach for the majority of businesses and the government alike.

3. Blockchain Security

Using cybersecurity frameworks, assurance services, and industry best practices, blockchain security mitigates the risk of attacks, fraud, and other criminal activities on blockchain networks. It is continually changing who may participate in blockchain networks and who has access to the data. The terms "public" and "private," as well as "permission" and "permission less," are occasionally used to distinguish between networks that are open to the public and those that are restricted to members only [45]. In terms of safety, the difference between a public and a private blockchain cannot be overstated. Table 5 shows a comparison of the differences in terms of features:

Table 5: difference between private VS, public Blockchain [46].

Action	private	public
Read Permission	Public	Could be public or restricted
Immutability	Approximately past the point of tampering	Could be tampered
Efficiency	Low	High
Centralized	Have	Have not Centralized

Because public blockchains are public, anyone can join and validate transactions on them. Furthermore, the use of private blockchains is limited, with most of them being used by commercial networks. A single corporation, or consortium, controls the membership [47]. Figure 4 illustrates what distinguishes both:

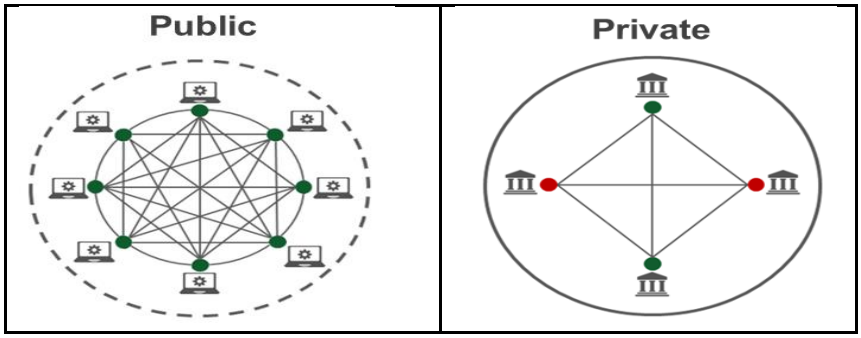


Figure 4: private and Public Blockchain Network [47]

In its simplest form, blockchain is a distributed technological foundation that enables users to maintain a reliable database in a distributed fashion. In a typical blockchain system, data is created and stored in blocks. A chained data structure is constructed by linking consecutive

blocks in chronological order. All user nodes are responsible for validating, storing, and maintaining data. Typically, a new block must be authorized by more than half of the users before it is broadcast to all user nodes for network-wide synchronization. Once data has been synchronized, it is not possible to change or delete it [48].

3.1 Cybersecurity in Blockchain

The unalterable record of transactions created by blockchain technology is not resistant to hackers or fraud. Malicious actors can take advantage of well-documented faults in blockchain technology, as several hacks and scams have shown over the years [49]. While blockchain technology significantly reduces the risk of adversary influence, it is not a one-size-fits-all solution for all cyber threats. Blockchain problems include attacks on node connections (such as the eclipse attack), consensus methods (51% attack), and code vulnerabilities. If any of these issues are exploited, the system's security might be compromised [50]. Table 6 illustrates a well-known example of the most prevalent faults:

Table 6: Famous Example of Defects [51][30].

Name	Description
Code exploitation	The code's popularity resulted in the portability of stolen bitcoin.
Stolen keys	Thieves can steal customers' digital money by just being able to recognize the private key and electronic signature.
computer hacked	The process of penetrating central computers through malware specially prepared for these matters causes the theft of information that is used for commercial purposes.

3.2 Attack on blockchain

As Internet technologies evolve, the number of threats and assaults against networks and systems increases [52]. Attackers develop new attack strategies or improve on current ones. Phishing, routing, Sybil, and 51 percent attacks are some of the most prevalent serious risks in which fraudsters attempt to gain user credentials using fraudulent emails or websites, or a combination of the two. As a result of massive expenditures and weaknesses in national rules, attackers are increasingly attacking blockchain efforts. Following a series of attacks on blockchain projects around the world, the issue of blockchain cybersecurity has received a lot of attention [53] and [11]. The next Table 7 shows the famous types of attacks on the blockchain:

Table 7: Attacks types on blockchain

Name of Attack	Description

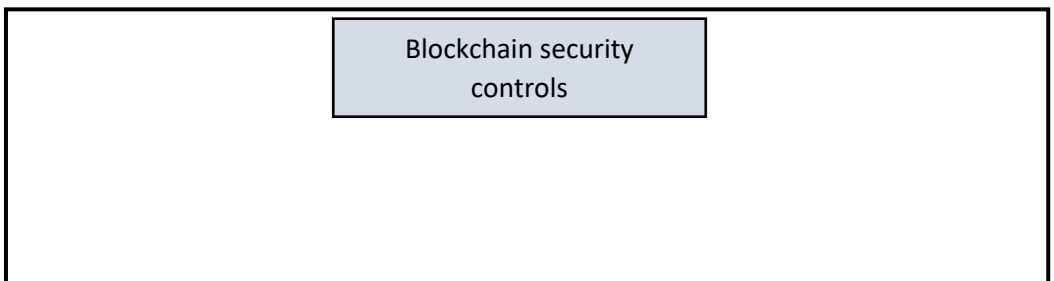
Phishing attacks [54]	Phishing is a technique for deceptively obtaining a user's credentials. Emails purporting to be from a credible source are sent to wallet key owners by fraudsters. Users are prompted to enter their credentials via bogus URLs in email messages. Accessing a user's credentials and other sensitive data can result in financial damage for both the individual and the blockchain network.
Routing attacks [29]	Blockchains allow for large amounts of data to be sent in real-time. Data might be intercepted when it is sent to ISPs by hackers. Since blockchain participants are unaware of the threat posed by a routing attack, everything appears to be normal. On the other hand, scammers have extracted sensitive data or money from behind the scenes.
Sybil attacks [55]	In a Sybil attack, hackers create and utilize a huge number of bogus network identities to flood the network and cause damage.
51% attacks [56]	Mining requires a lot of computational power, especially for large-scale public blockchains. It's possible, though, for one mining pool to control more than 50% of the mining power on a blockchain network if they combine their resources sufficiently. More than half of the power comes from having control over the ledger and the capacity to make changes to it. Your blockchain design and surroundings must be safe in today's digital environment. For this, the blockchain testing services given by X-Force Red may be of value.

3.3 Blockchain security in the organization

When creating a blockchain application for a business, security at all layers of the technology stack must be considered, as well as how the network's governance and permissions will be controlled. Traditional security controls, as well as technology-specific controls, are all part of the entire security plan for an enterprise blockchain system [57]. The following are certain security features that are unique to business blockchain platforms [58]:

- Identity and access management
- Key management
- Data privacy
- Secure communication
- Smart contract security
- Transaction endorsement

And the following Figure (5) shows the security controls in blockchain based on the above points:



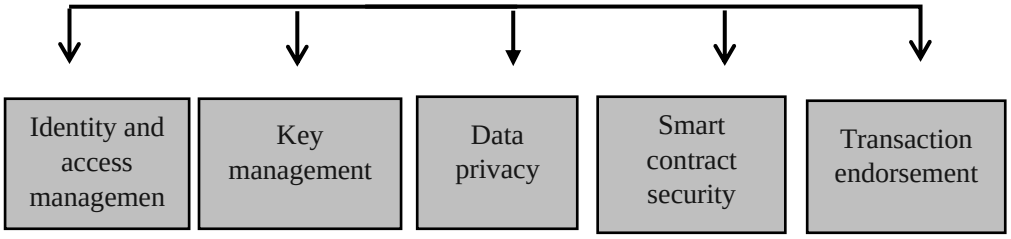


Figure 5: Blockchain Security Controls [59].

4. IOT Conception in blockchain

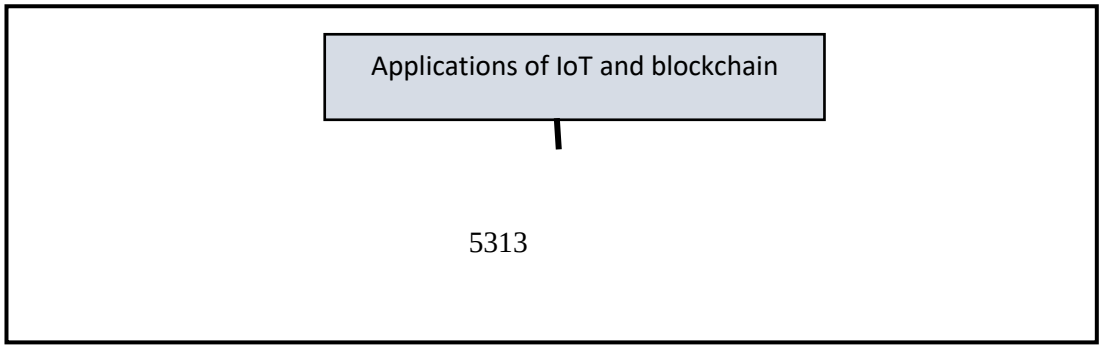
Understanding how IoT networks are used in a range of home, industrial, and military applications is crucial. These IoT networks all share a plethora of sensors and actuators. Sensors and actuators are low-resource devices that can communicate without human involvement [60]. In addition to these devices, other network entities connect the sensors and actuators to the backbone network architecture [61]. The components that regulate resource provisioning and sharing are routers, switches, aggregators, and cloud infrastructure (including virtual servers and storage). Dynamic and verifiable device group membership, authentication and data integrity, resilience against a single point of failure, resource-light operations, and low latency communication are just a few of these requirements [62]. The Internet of Things enables Internet-connected items to transfer data to private blockchain networks, which provide tamper-resistant records of shared transactions. Blockchain enables you to exchange and access IoT data with your business partners without the need for centralized management and administration. Each transaction may be examined to avoid disputes and create confidence among all network members with authority [33].

4.1 Benefits and Application of IoT in Blockchain

The following points summarize the significance of the Internet of Things in blockchain [1], [63]:

- Build trust in your IoT data.
- Rely on added security.
- Gain greater flexibility.
- Generate new efficiencies.

Each transaction is logged, saved in a data block, and added to an immutable, secure data chain that can only be added to and deleted from. By utilizing data from IoT devices and sensors, you can pick which data to manage, analyze, customize, and share with clients and partners with permission using the Watson IoT® Platform, and blockchain streamlines processes and generates new business value across your ecosystem [64]. The domain of the most important applications of the blockchain that allow the Internet of things can be summarized in the following Figure (6):



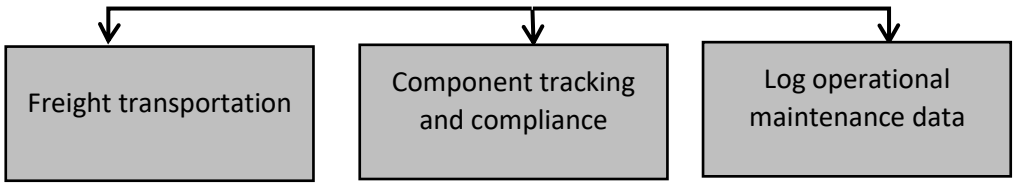


Figure 6: Domain Applications of IoT And Blockchain [65]

Where Moving freight is a difficult process that involves several stakeholders, each with their own set of goals. Temperatures, location, arrival times, and status of shipping containers can all be tracked using an IoT-powered blockchain as they travel [64]. Immutable blockchain transactions ensure that all parties can trust the data and move things quickly and effectively. The ability to track components that go into an airplane, automobile, or other product is vital for both safety and regulatory compliance. All stakeholders may examine component provenance throughout the life of a product thanks to IoT data stored in common blockchain ledgers [66]. It is risk-free, simple, and cost-effective to communicate this information with regulatory bodies, shippers, and other interested parties and manufacturers. IoT devices monitor the safety and maintenance of vital machinery. Blockchain enables the establishment of a tamper-proof database of operational data and the accompanying maintenance of everything from engines to elevators. Third-party repair partners can use the blockchain to track their work after monitoring it for preventative maintenance. Furthermore, government bodies may be provided access to operating papers in order to ensure compliance [14].

4.2. Protocols of Consensus on IoT

Consensus procedures are the techniques that allow nodes in a blockchain network to agree on adding a new block to the chain. The technique that allows a distributed blockchain network to function is consensus. A blockchain-based system is only as safe and reliable as the consensus process it uses [49]. Proof of work, which is utilized by bitcoin, is the most well-known consensus technique. However, in recent years, a variety of consensus mechanisms have emerged. They are designed and constructed to be used in a variety of situations [27]. This paper reviews existing consensus procedures and analyzes their benefits and limitations. They have the potential to be employed in a blockchain-based Internet of Things network.

Furthermore, Table 8 compares the protocols indicated in the previous research that affect the Internet of Things:

Table 8: Protocols That Have an Impact on The Internet of Things [67],[68],[27].

mode	Decentralization	Network access	Scalability	Latency	Computing	Network overhead	Storage overhead	IoT suitability

PoET	Moderate	Private	High	Low	Low	Low	High	High
PoS	High	Public	High	Moderate	Moderate	Low	High	Moderate
DPoS	Moderate	Public	High	Moderate	Moderate	Moderate	High	Moderate
PoI	High	Public	High	Moderate	Low	Low	High	Moderate
PBFT	Moderate	Private	Low	Low	Low	High	High	High
Dpbft	Moderate	Private	High	Moderate	Low	High	High	Moderate
Stella	High	Public	High	Moderate	Low	Moderate	High	Moderate
Ripple	High	Public	High	Moderate	Low	Moderate	High	Moderate
Tendermint	High	Public	High	Moderate	Low	Moderate	High	Moderate
Omni Ledger	High	Public	High	Moderate	Moderate	Low	Low	Moderate
Rapid Chain	High	Public	High	Moderate	Moderate	Low	Low	Moderate
Raft	Moderate		High	Low	Low	Low	High	Moderate
Tangle	Moderate	Public	High	Low	Low	Low	Low	High

5. Agents in Blockchain

Many people are looking at the blockchain as a way to solve long-standing problems or obtain unexpected benefits because the blockchain concept and technology are influencing many different study and application disciplines [75]. Several authors in the agent community are proposing their own hybrid of agent-oriented technology and blockchain to address both old and new problems [76]. A computer program that can adapt to a specific type of environment and take autonomous actions to achieve its goals is referred to as an agent [77]. Multiple agents can work together on large-scale, difficult activities. An agent-based method is generic and strong when a distributed system needs to synchronize its behavior with several entities [78] because it allows for intricate interaction between several stakeholders. The system's dynamic consensus emerges through the interaction of agents, in which each agent's behavior is dictated by a shared cognitive framework. Furthermore, the agents' pervasiveness and multilateral perspective result in a broader vision and, in many cases, higher overall quality output [79]. Using agent-based systems to assist blockchain applications has been proposed in a number of recent research initiatives [80].

6. comparison of survey study

The topic of blockchains is one of the modern topics that keeps pace with the rapid progress of technology and has an important future in our world. Based on what was mentioned in this study and previous studies, Table 9 shows and compares them from several aspects that give a glimpse into the last six years.

Table 9: a comparison study

Survey	Another name	Year of publisher	Attack security	classification	Application	challenge	Cybersecurity	security controls

[69]	**E.bouscoren**	**2016**	✔	×	×	✔	×	×
[70]	**I.lin &liao**	**2017**	×	×	✔	✔	×	×
[68]	**A.reyua.et al .**	**2018**	✔	×	✔	✔	×	×
[12]	**T.salman.et al**	**2019**	×	×	×	✔	×	×
[71]	**P.taylor. et al.**	**2019**	×	×	✔	✔	×	×
[72]	**M.hassan. et al**	**2019**	✔	✔	×	✔	×	×
[8]	**S.sing .et al**	**2020**	✔	✔	✔	✔	×	×
[73]	**E.de aguiar .et al**	**2020**	×	×	×	✔	×	×
[74]	**M.saad .et al .**	**2020**	✔	×	×	✔	×	×
[9]	**M.buhutta. et al.**	**2021**	×	✔	✔	✔	×	×
[32]	**S.sing.et al.**	**2021**	✔	✔	✔	✔	×	×
This survey		**2021**	✔	✔	✔	✔	✔	✔

7. Discussion

In this paper, blockchain technology and its applications are reviewed, along with the most important challenges it faces. As shown in Table 2, blockchain is not limited to digital currencies but has entered into many applications such as blockchain for the health care industry, electronic medical records, and smart contacts. Blockchain integration with these applications provides a lot of benefits and improvements to applications; for example, when integrating the blockchain with IoT, consumers can access a variety of killer IoT applications, such as logistic management using Radio-Frequency Identification (RFID) technology, smart homes, smart grids, and the maritime industry, but it is also accompanied by some challenges, as indicated in Table (4).

The security aspects related to the blockchain technology were also reviewed in Section 3 of this paper, and it was concluded that the blockchain technology provides many security features, such as integration, but we would have been exposed to many attacks, as shown in Table 7. This paper ends in comparison with previous studies and topics that have been covered, as shown in Table 9.

8. Conclusion

Blockchain is a game-changing technology that paves the way for the development of distributed and secure applications in industries other than finance. Blockchain for trusted transactions is expected to achieve what the Internet has done for communications due to its large and rapid development of applications. The concept of blockchain has received a lot of attention from the academic and scientific communities since Bitcoin debuted in 2008.

This study reviews the significant work of previous researchers from 2016 to 2021 and comments on their contributions based on a detailed and complete analysis of the evolution of blockchain frameworks, architectures, security, and features related to privacy. This paper

provides a perspective on discussing blockchain structures around crypto currencies and applications, as well as the attacks that can be carried out on the blockchain. All are summarized in a table to make the information more accessible to the reader. This paper also reviewed the concept of the Internet of Things and its relationship to the blockchain in terms of applications and the most important protocols that affect it. The main idea presented by this article is to separate the concept of blockchain from Bitcoin and the traditional idea associated with it, since blockchain exists and can be used in life applications. The basic idea is the paradigm shift that occurred on the subject of the Internet of Things (IoT) and its transformation from centralization to decentralization, that is, helping to get rid of single points of failure and off-chain transactions. It also provided a basic overview of the concept of agents and their relationships.

References

[1] X. Wang *et al.*, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, 2019, doi: 10.1016/j.comcom.2019.01.006.

[2] S. Demirkan, I. Demirkan, and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *J. Manag. Anal.*, vol. 7, no. 2, pp. 189–208, 2020, doi: 10.1080/23270012.2020.1731721.

[3] J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," *IEEE Access*, vol. 7, no. c, pp. 1–16, 2019, doi: 10.1109/ACCESS.2019.2903554.

[4] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things," *IEEE Wirel. Commun.*, vol. 25, no. 6, pp. 12–18, 2018, doi: 10.1109/MWC.2017.1800116.

[5] R. Neisse, J. L. Hernandez-Ramos, S. N. Matheu, G. Baldini, and A. Skarmeta, "Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices," in *2019 IEEE Conference on Standards for Communications and Networking, CSCN 2019*, 2019, pp. 1–8, doi: 10.1109/CSCN.2019.8931384.

[6] R. I. O. Dqg *et al.*, "A survey of blockchain and its application," in *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2019, pp. 7–9, doi: DOI: 10.1109/ICAIIC.2019.8669067.

[7] G. Huberman, J. D. Leshno, and C. Moallemi, "Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System," *Rev. Econ. Stud.*, vol. 88, no. 6, pp. 3011–3040, 2021, doi: 10.1093/restud/rdab014.

[8] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Inf. Process. Manag.*, vol. 58, no. 1, p. 102397, 2021, doi: 10.1016/j.ipm.2020.102397.

[9] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[10] L. Zhu *et al.*, "Research on the Security of Blockchain Data: A Survey," *J. Comput. Sci. Technol.*, vol. 1, pp. 1–48, 2018, doi: 10.1007/s11390-020-9638-7.

[11] L. Bahack, "Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft)," *J. Comput. Sci. Technol.*, vol. 1, pp. 1–18, 2013.

[12] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/COMST.2018.2863956.

[13] L. P. Nian and D. L. K. Chuen, "Introduction to Bitcoin," in *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, Elsevier Inc., pp. 5–30, 2015.

[14] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: a survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/ijwgs.2018.10016848.

[15] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, "Analysis of Blockchain technology: pros, cons and SWOT," *Cluster Comput.*, vol. 22, pp. 14743–14757, 2019, doi: 10.1007/s10586-018-2387-5.

[16] M. Grabisch and A. Rusinowska, "Public Blockchain versus Private blockchain," *Doc. Trav. du Cent. d'Economie la Sorbonne*, vol. 38, pp. 1–6, 2017, [Online]. Available: url:

https://halshs.archives-ouvertes.fr/halshs-01524440/document.

[17] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on Private Blockchain Consensus Algorithms," *Proc. 1st Int. Conf. Innov. Inf. Commun. Technol. ICIICT 2019*, no. July, pp. 1–6, 2019, doi: 10.1109/ICIICT1.2019.8741353.

[18] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Trans. Ind. Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018, doi: 10.1109/TII.2017.2786307.

[19] E. Anceaume, A. Del Pozzo, R. Ludinard, M. Potop-Butucaru, and S. Tucci-Piergiovanni, "Blockchain abstract data type," in *Annual ACM Symposium on Parallelism in Algorithms and Architectures (Conference: The 31st ACM)*, 2019, pp. 349–358, doi: 10.1145/3323165.3323183.

[20] J. Xu, H. Liu, and Q. Han, "Blockchain technology and smart contract for civil structural health monitoring system," *Comput. Civ. Infrastruct. Eng.*, vol. 36, no. 10, pp. 1288–1305, 2021, doi: 10.1111/mice.12666.

[21] F. Sabrina, "Blockchain and Structural Relationship Based Access Control for IoT: A Smart City Use Case," *Proc. - Conf. Local Comput. Networks, LCN*, vol. 2019-Octob, pp. 137–140, 2019, doi: 10.1109/LCN44214.2019.8990757.

[22] X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao, and A. V. Vasilakos, "Designing blockchain-based applications a case study for imported product traceability," *Futur. Gener. Comput. Syst.*, vol. 92, pp. 399–406, 2019, doi: 10.1016/j.future.2018.10.010.

[23] A. Ben Ayed, "A Conceptual Secure Blockchain Based Electronic Voting System," *Int. J. Netw. Secur. Its Appl.*, vol. 9, no. 3, pp. 01–09, 2017, doi: 10.5121/ijnsa.2017.9301.

[24] G. Albeanu, "Blockchain Technology and Education," in *the 12th International Conference on Virtual Learning ICVL 2017*, pp. 271–275, 2017.

[25] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, 2018, doi: 10.1109/TKDE.2017.2781227.

[26] B. Gipp, C. Breitinger, N. Meuschke, and J. Beel, "CryptSubmit: Introducing Securely Timestamped Manuscript Submission and Peer Review Feedback Using the Blockchain," *Proc. ACM/IEEE Jt. Conf. Digit. Libr.*, no. June, pp. 7–11, 2017, doi: 10.1109/JCDL.2017.7991588.

[27] T. Alam, "Blockchain and its Role in the Internet of Things (IoT)," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 5, no. 1, pp. 151–157, 2019, doi: 10.32628/cseit195137.

[28] G. Srivastava, S. Dhar, A. D. Dwivedi, and J. Crichigno, "Blockchain Education," *2019 IEEE Can. Conf. Electr. Comput. Eng. CCECE 2019*, 2019, doi: 10.1109/CCECE.2019.8861828.

[29] A. Malik, S. Gautam, S. Abidin, and B. Bhushan, "Blockchain Technology-Future of IoT: Including Structure, Limitations and Various Possible Attacks," *2019 2nd Int. Conf. Intell. Comput. Instrum. Control Technol. ICICICT 2019*, pp. 1100–1104, 2019, doi: 10.1109/ICICICT46008.2019.8993144.

[30] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey," *IEEE Trans. Ind. Informatics*, vol. 17, no. 1, pp. 3–19, 2021, doi: 10.1109/TII.2020.2998479.

[31] R. Stephen and A. Alex, "A Review on Blockchain Security," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 396, no. 1, 2018, doi: 10.1088/1757-899X/396/1/012030.

[32] S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[33] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "*Blockchain and iot integration: A systematic survey*," *Sensors*, vol. 18, no. 8. 2018.

[34] J. Cheng, L. Xie, X. Tang, N. Xiong, and B. Liu, "A survey of security threats and defense on Blockchain," *Multimed. Tools Appl.*, vol. 80, no. 20, pp. 30623–30652, 2021, doi: 10.1007/s11042-020-09368-6.

[35] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *J. Netw. Comput. Appl.*, vol. 166, no. May, p. 102693, 2020, doi: 10.1016/j.jnca.2020.102693.

[36] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," *Int. Conf. Inf. Netw.*, no. January 2018, pp. 473–475, 2018, doi: 10.1109/ICOIN.2018.8343163.

[37] K. Sengupta, "Blockchain Applications in Supply Chain," *Emerald Handb. Blockchain Bus.*, vol. 2, pp. 21–46, 2021, doi: 10.1108/978-1-83982-198-120211025.
[38] D. Di Francesco Maesa and P. Mori, "Blockchain 3.0 applications survey," *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, 2020, doi: 10.1016/j.jpdc.2019.12.019.
[39] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Futur. Gener. Comput. Syst.*, vol. 107, no. Xiaoqi Li, pp. 841–853, 2020, doi: 10.1016/j.future.2017.08.020.
[40] H. Hasanova, U. jun Baek, M. gon Shin, K. Cho, and M. S. Kim, "A survey on blockchain cybersecurity vulnerabilities and possible countermeasures," *Int. J. Netw. Manag.*, vol. 29, no. 2, pp. 1–36, 2019, doi: 10.1002/nem.2060.
[41] C. A. García-Pérez, "The Blockchain Impact on the Current Auditing Standards," *Geotech. Geol. Earthq. Eng.*, vol. 16, no. 03, pp. 129–145, 2016, doi: 10.1007/978.
[42] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Systematic Overview," pp. 1–30, 2019, [Online]. Available: http://arxiv.org/abs/1904.03487.
[43] A. Lewis-Pye and T. Roughgarden, "How Does Blockchain Security Dictate Blockchain Implementation?," 2021, doi: 10.1145/3460120.3484752.
[44] M. Osmani, R. El-Haddadeh, N. Hindi, M. Janssen, and V. Weerakkody, "Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis," *J. Enterp. Inf. Manag.*, vol. 34, no. 3, pp. 884–899, 2021, doi: 10.1108/JEIM-02-2020-0044.
[45] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *J. Bank. Financ. Technol.*, vol. 3, no. 1, pp. 1–17, 2019, doi: 10.1007/s42786-018-00002-6.
[46] K. Radtke, "Public versus private Blockchains," *BRL (Blockchain Res. lab)*, no. 14, pp. 31–64, 2018, doi: 10.4324/9780203962282.pt1.
[47] B. C. Ghosh, T. Bhartia, S. K. Addya, and S. Chakraborty, "Leveraging public-private blockchain interoperability for closed consortium interfacing," *Proc. - IEEE INFOCOM*, vol. 2021-May, 2021, doi: 10.1109/INFOCOM42981.2021.9488683.
[48] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues," *2017 4th Int. Conf. Syst. Informatics, ICSAI 2017*, vol. 2018-Janua, no. 61471129, pp. 975–979, 2017, doi: 10.1109/ICSAI.2017.8248427.
[49] M. Mylrea and S. N. G. Gourisetti, "Blockchain for Supply Chain Cybersecurity, Optimization and Compliance," *Proc. - Resil. Week 2018, RWS 2018*, no. January, pp. 70–76, 2018, doi: 10.1109/RWEEK.2018.8473517.
[50] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity Enhancement of Power Trading within the Networked Microgrids Based on Blockchain and Directed Acyclic Graph Approach," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7300–7309, 2019, doi: 10.1109/TIA.2019.2919820.
[51] A. R. Mathew, "Cyber security through blockchain technology," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1, pp. 3821–3824, 2019, doi: 10.35940/ijeat.A9836.109119.
[52] A. Kadhim and M. Salih, "Proposal of New Keys Generator for DES Algorithms Depending on Multi Techniques," *Eng. Technol. J.*, vol. 32, no. 1 Part (B) Scientific, pp. 94–106, 2014.
[53] E. F. Jesus, V. R. L. Chicarino, C. V. N. De Albuquerque, and A. A. D. A. Rocha, "A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack," *Secur. Commun. Networks*, vol. 2018, pp. 1–27, 2018, doi: 10.1155/2018/9675050.
[54] A. A. Andryukhin, "Phishing Attacks and Preventions in Blockchain Based Projects," *Proc. - 2019 Int. Conf. Eng. Technol. Comput. Sci. Innov. Appl. EnT 2019*, pp. 15–19, 2019, doi: 10.1109/EnT.2019.00008.
[55] T. Rajab, M. H. Manshaei, M. Dakhilalian, M. Jadliwala, and M. A. Rahman, "On the Feasibility of Sybil Attacks in Shard-Based Permissionless Blockchains," 2020, [Online]. Available: http://arxiv.org/abs/2002.06531.
[56] C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, "Analysis of security in blockchain: Case study in 51%-attack detecting," *Proc. - 2018 5th Int. Conf. Dependable Syst. Their Appl. DSA 2018*, pp. 15–24, 2018, doi: 10.1109/DSA.2018.00015.
[57] H. Zheng, Q. Wu, J. Xie, Z. Guan, B. Qin, and Z. Gu, "An organization-friendly blockchain system," *Comput. Secur.*, vol. 88, no. 47, p. 101598, 2020, doi: 10.1016/j.cose.2019.101598.
[58] M. Toapanta, J. Mero, D. Huilcapi, M. Tandazo, A. Orizaga, and E. Mafla, "A Blockchain

Approach to Mitigate Information Security in a Public Organization for Ecuador," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 423, no. 1, 2018, doi: 10.1088/1757-899X/423/1/012164.

[59] N. Chondamrongkul, J. Sun, and I. Warren, "Formal security analysis for blockchain-based software architecture," in *Proceedings of the International Conference on Software Engineering and Knowledge Engineering, SEKE(European Conference on Software Architecture)*, 2020, vol. PartF16244, pp. 21–38, 2020.

[60] J. R. Naif, G. H. Abdul-Majeed, and A. K. Farhan, "Secure IOT System Based on Chaos-Modified Lightweight AES," in *2019 International Conference on Advanced Science and Engineering, ICOASE 2019*, 2019, pp. 12–17, doi: 10.1109/ICOASE.2019.8723807.

[61] A. Emerita, "Convergence Between Blockchain and The Internet of Things Alma Emerita," *Int. J. Technol. Innov. Manag.*, vol. 1, no. 1, pp. 35–56, 2021, doi: DOI: https://doi.org/10.54489/ijtim.v1i1.11.

[62] M. Maroufi and R. Abdolee, "On the Convergence of Blockchain and Internet of Things (IoT) Technologies," *J. Strateg. Innov. Sustain.*, vol. 14, no. 1, pp. 1–11, 2019, doi: 10.33423/jsis.v14i1.990.

[63] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," *2017 IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017*, no. 2016, pp. 137–141, 2017, doi: 10.1109/TEMSCON.2017.7998367.

[64] C. Nartey *et al.*, "Blockchain-IoT peer device storage optimization using an advanced time-variant multi-objective particle swarm optimization algorithm," *EURASIP J. Wirel. Commun. Netw.*, vol. 2022, no. 1, 2022, doi: 10.1186/s13638-021-02074-3.

[65] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," *Blockchain Res. Appl.*, vol. 2, no. 4, p. 100027, 2021, doi: 10.1016/j.bcra.2021.100027.

[66] A. A. Alfa, J. K. Alhassan, O. M. Olaniyi, and M. Olalere, "Blockchain technology in IoT systems: current trends, methodology, problems, applications, and future directions," *J. Reliab. Intell. Environ.*, vol. 7, no. 2, pp. 115–143, 2021, doi: 10.1007/s40860-020-00116-z.

[67] M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in blockchain for resource-constrained IoT networks," *Internet of Things (Netherlands)*, vol. 11, p. 100212, 2020, doi: 10.1016/j.iot.2020.100212.

[68] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT . Challenges and opportunities," vol. 88, no. 2018, pp. 173–190, 2018, doi: 10.1016/j.future.2018.05.046.

[69] E. Bouscaren, "Elementary pairs of models," *Ann. Pure Appl. Log.*, vol. 45, no. 2 PART 1, pp. 129–137, 2016, doi: 10.1016/0168-0072(89)90057-2.

[70] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, vol. 19, no. 5, pp. 653–659, 2017, doi: 10.6633/IJNS.201709.19(5).01.

[71] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Networks*, vol. 6, no. 2, pp. 147–156, 2019, doi: 10.1016/j.dcan.2019.01.005.

[72] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 512–529, 2019, doi: 10.1016/j.future.2019.02.060.

[73] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A Survey of Blockchain-Based Strategies for Healthcare," *ACM Comput. Surv.*, vol. 53, no. 2, 2020, doi: 10.1145/3376915.

[74] M. Saad *et al.*, "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020, doi: 10.1109/COMST.2020.2975999.

[75] S. B. Sadkhan, A. M. Al-bakry, and N. N. Muhammad, "An Agent based Image Steganography using Information Theoretic Parameters," MASAUM Journal of Computing, vol. 1, no. 2, pp. 258–264, 2009.

[76] G. Ciatto, S. Mariani, A. Omicini, and F. Zambonelli, "From agents to blockchain: Stairway to integration," *Appl. Sci.*, vol. 10, no. 21, pp. 1–22, 2020, doi: 10.3390/app10217460.

[77] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarné, "Using Blockchain in a Reputation-Based Model for Grouping Agents in the Internet of Things," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4,

pp. 1231–1243, 2020, doi: 10.1109/TEM.2019.2918162.

[78] Y. Yao, M. Kshirsagar, G. Vaidya, J. Ducrée, and C. Ryan, "Convergence of Blockchain, Autonomous Agents, and Knowledge Graph to Share Electronic Health Records," *Front. Blockchain*, vol. 4, no. April, pp. 1–7, 2021, doi: 10.3389/fbloc.2021.661238.

[79] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Eng. Technol. Appl. Sci. Res.*, vol. 10, no. 2, pp. 5441–5447, 2020, doi: 10.48084/etasr.3394.

[80] S. Bayar, "A Generalized Agent Based Framework For Modeling A Blockchain System," *Proceedings of the 2018 Winter Simulation Conference*, pp. 1001–1012, 2018.