Blockchain in IoT: Research Challenges, Issues, and Future Directions - A Comprehensive Review

[1]Abhay Kumar, [2]Dr. P. Punitha , [3]Dr A L Sreenivasulu , [4]Gandhi Prakash Panem, [5]T Ratna Kumar,[6*]Dr.G.Ganesh Kumar

[1]Department of Artificial Intelligence and Data Science, B V Raju Institute of Technology, Telangana.
[2]Associate professor, Department of CSE(Data Science) , Vignana Bharathi Institute of Technology,
[3]Professor of CSE, Vignana Bharathi Institute of Technology, Telangana,Aushapur(V),Ghatkesar(M), Medchal (D),Hyderabad.
[4]Assistant Professor, Department of AI&DS, Lakireddy Bali Reddy College of Engineering.
[5]Assistant Professor,Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram,
[6*]Assistant Professor, Department of IT, Hindusthan Institute of Technology, Coimbatore, TN, India.

Abstract
Internet of Things (IoT) becomes vital source of converting things into smart, including smart homes, smart cities, smart industries etc. Internet of things have the ability to connect billions of things at the same time, which seeks to develop information sharing requirements that improve our daily lives. By seeing things on the Internet, traditional devices become intelligent and independent, and this vision becomes real and realistic. The Blockchain appears a great source of providing security to new era technological applications. The high growth of IoT based smart applications have high demand of security to manage and maintain the IoT based application's data safety, security integrity, and authentication. The merger of both technologies may provide our secure security solutions. This research explores the Internet of things security solutions by integrating IoT applications with blockchain. The research initially focused on the blockchain basics, types, design for Internet of things applications. Further we elaborate the several challenges and issue of BIoT applications linked to the energy efficiency, security, privacy, throughput, latency, block size, bandwidth, usability, multi chain management, versioning, forks, autonomy and enforcement. Finally, we explore the future directions of blockchain for the internet of things. The literature-based results showed, that the integration of Blockchain with Internet of things provides significant solutions of security and privacy to IoT based application.

Key words:
Blockchain, Internet of Things, Challenges, Future directions

1. Introduction

The term "Blockchain" originated from its technical structure (Chain Blocks), meaning the association of each block with the block that precedes it. The blockchain concept works to interlink the connections or transactions of data in the clusters. The cluster is defined as the data structure which includes many financial transactions. Individuals or entities exchange transactions. These transactions may be financial in nature and sometimes (smart contracts). Blockchain participants are any person or institution that accepts protocol strings and helps develop them. The organizers of these networks and those responsible for software maintenance do not share the blockchain. In this section, the basics of blockchain, basic functions of blockchain, types of blockchain, blockchain and (IoT) are highlighted.

The Basics of Blockchain

The Blockchain idea was developed by Distributed Ledger Technology (DLT). This technology is developed to provide Convention validation technology across a network that may cover the entire word to facilitate peer-to-peer transactions and all financial transactions. This mechanism marginalizes third party roles in financial transactions such as: Banks, agents, intermediaries or any authority that may be required to ensure and maintain the fulfillment or update of transaction data. Then ensure that each financial transaction is correct and save it as a new block for an existing transaction. Once the transaction is saved within the string, it cannot be changed, overwritten or deleted, which requires higher levels of security and transparency [1]. Figure 1 illustrates further about the primary idea of blockchain and IoT based integrated application domain for the users.

Fig. 1 How blockchain technology works. [3]

The Basic Functions of Blockchain

The Blockchain is an electronic mechanism that deals with financial transactions and uses the "Peer to Peer" technology. It has three basic functions:

1. Allow financial transactions between individuals and institutions around the world with a high degree of reliability and security because they destroy the so-called "double spending". [2]

2. Enable traceability (the ability to track something on the Internet to its assets) for transactions, which means that transactions will be clear, transparent and have higher levels of security.
3. Protect users from any attacks or violations by malicious users via the same system. And there is no need for central authorities to participate in financial transactions, and to ensure lower expenses.

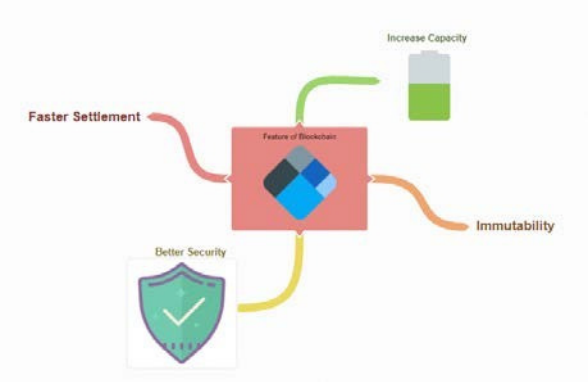

Fig. 2 Blockchain Features.

Figure 2 illustrates the main features of block chain which makes block chain safer, faster, with increased capacity. The simple blockchain network can be illustrated as shown in Figure 3.

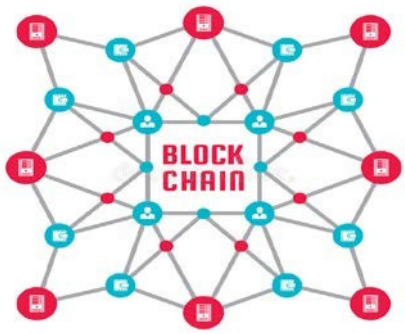

Fig. 3 Blockchain Network [1]

Types of Blockchain

By reviewing the previous literature, the researcher noted the existence of two major types of Blockchain known by those interested in this field, namely: Blockchain licensed and without permission:

1.2.1. Blockchain licensed

A licensed Blockchain is a network that is used by individuals or institutions to conduct their financial business, such as a group of institutions or banks that control financial transactions. This network is only delegated to a group of individuals or entities that can access data only. They have the ability to read target data and write only. The licensed Blockchain is more recent than permission without permission. Thus, a licensed Blockchain is a central entity such as a bank that has the ability to control the rights of individuals and identify them to participate in the process of reading or writing data. This type of Blockchain ensures higher degrees of privacy. With this in mind, the most widespread and known permissioned Blockchains are (Hyper ledger Fabric & R3). [1], [4].

1.2.2. Blockchain Permission

The Permission less Blockchain is an open network that can be accessed and used by any individual or entity. Bitcoin and Ethereum frozen hoops are good examples of unauthorized Blockchain because users can move to each other without any controller using bitcoin or ethereum as a method of payment. Since this cluster is open and decentralized, anyone (peer) can access or join this network and free to leave at any time. The counterpart is entitled to read or write what has been established for treatment. There is no central authority to manage peer interaction in this network, control membership, or read or write. The openness available means that the written content is readable by all individuals. However, the cryptographic features allow designing permission less Blockchain and hiding the information related to the peers' privacy. [5]

Blockchain and (IoT)

The concept of "IoT" is the interconnection of smart devices to gather information and make decisions. By combining Blockchain with Internet objects, things can eliminate the lack of security in Internet objects where Blockchain requires "security by design". Blockchain features, such as (incompatibility, transparency, readability, data encryption, and operational flexibility), can be used to overcome Internet security issues. The integration of Blockchain and IoT is a promising area of research which was tackled by a considerable amount of research but contains many uncovered areas. [6 – 7]. Table 1 shows comparsion between blockchain and IoT.

Table 1: Comparison Between Blockchain and IoT [8]

Blockchain	**IoT**
Decentralized	Centralized
Resource consuming	Resource restricted
Block mining is time-consuming	Demands low latency
Scale poorly with large network	IoT considered to contains large number of devices
High bandwidth consumption	IoT devices have limited bandwidth and resources
Has better security	Security is one of the big challenges of IoT

2. Literature Review

In this paper, the literature has been reviewed in three sections (architecture, current challenges and problems of BIoT applications and future trends). The review included a number of books, journals, letters, reports and other relevant documents as well as academic databases such as Science Direct, EBSCO, Emerald and SAGE. In order to search for relevant literature, a wide range of related terms, such as IOT, BIot, Block chain, Message Time, and Algorithms were used. With regard to the dates of review of sources of literature, the researcher reviewed a mixture of ancient and contemporary studies to provide an integrated account of the results in this field.

Blockchain Design for Applications of IoT

Blockchain technology is used in more than one Domain and situation. Different sources such as [9] It was suggested that progress in the application of blockchain started next to Bitcoin as Blockchain v1.0, and then changed with respect to smart conventions such as Blockchain v2.0 and subsequently progressed to justice, applications efionation, efiency and Blockchain v3.0.

The authors of "Blockchain everywhere" stated that the main aid of Blockchain usage with smart contracts is that it can automatically evaluate these contracts. Adopting smart contracts, temperatures can be automatically evaluated and the sender and receiver notified. Besides, the saved data were counter-manipulative and could be used for conducting check by outer parties to assure the practice of good distribution of medical products. With Ethereum, such a decentralized system can be fully used to resist tampering at low cost, on every contract basis and on a byte basis. With the participation of many stakeholders in the supply chain, Blockchain technology can be used to automate processes and eventually save costs by making sure trust among stakeholders. [10]

2.1.1. Architecture

Blockchain was a complex sort of Lego and must be adapted to specific business requirements. Because of different usage situations it is difficult to get a single simple structure, so they need to create different versions of Blockchain applications and architectural applications that suit individual business / industry needs.

The approach presented was a single hybrid. The Blockchain is used together with a centralized server and a database-based approach. The main architecture of blockchain can be viewed in Figure 4.

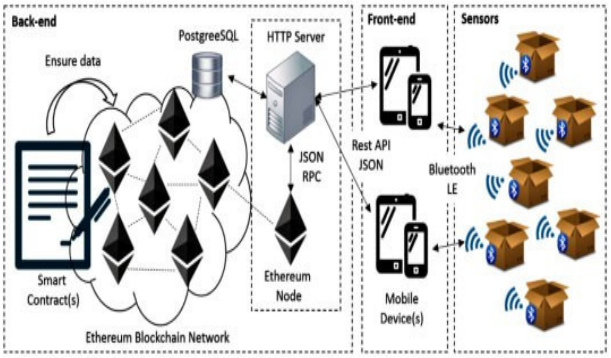

Fig. 4 Blockchain Architecture. [56]

The main components of this system are Etherrium Blockchain network, database, intelligent nodes, server, mobile devices and sensors.Where the temperature is secured by smart written contracts. For each new group of pharmaceutical products or shipments that involve excellent temperature requirements, intelligent contracts are configured and deployed by the server to ensure compliance requirements for good distribution practice (GDP). [11] Therefore, the map was drawn from the consignment to the contract title through a linked database at low cost. The server hosts the modum.io AG node Ethereum that is involved in the Etherreum network and may witness modifications to the smart nodes or produce a new contract or intelligent contracts. [12] The Ethereum node is connected to a Hyper Text Transfer Protocol (HTTP) server via JSON. The data that is stored is too large or too sensitive to be stored in the Blockchain stored in the PostgreSQL database and this involves raw temperature data, because large cannot be stored in intelligent nodes. The smart nodes verify the temperature range and store the verification result in the smart nodes with the global Uniform Resource Location (URL), which refers to the raw temperature data and the retail data.

Android clients communicate in the front end of the server through a Representative Transport Protocol (REST) interface designed with JSON to encrypt and decrypt requests / responses. Through the mobile phone, users can register new shipments including the administrative details within the system and create a smart contract for each shipment. The API should also allow the recipient of the shipment to download measurements of temperature measurements reported by the sensor to the server. Both the sender and receiver must be informed of the contract outcome and able to access the temperature measurements, preferably using the graphical representation. [10]A web portal and an infrastructure were the main components stand on Multichain and IoT devices as things were listed in. Figure 5 illustrated the blockchain prototype architecture.

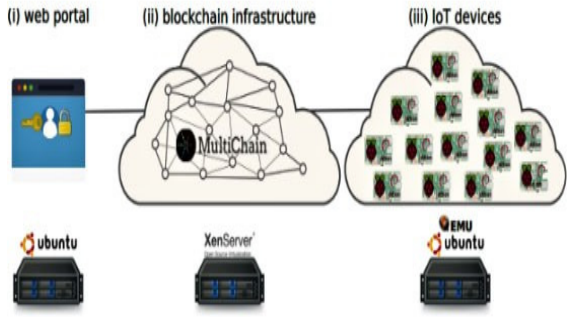

Fig. 5 Blockchain, Prototype Architecture. [57]

The web portal provides developers with safe and accurate control over software updates. The web portal is characterized by having an entrance to the Blockchain infrastructure, which is shared and shared by manufacturers. Each manufacturer must provide at least one business node for the development of computing power and availability of infrastructure. For the prototype, a Blockchain contract was hosted on the XenServer server and implemented as Virtual Machines (VMs). Web portal and Internet devices may share things with software updates and confirmations, through the Blockchain infrastructure. The system relies on asymmetric encryption to ensure data integrity and confidentiality. The Internet devices were either physically performed (i) by evolution panels, such as Raspberry Pi, which were closer to real field machines, or (ii) by virtual Qemu devices, to assess typical scalability. [14]

To push the software update:

1. The factory logs on to the gate.
2. Select the device to update it.
3. Download the software update package with metadata.
4. Choose one of these options (a) just sign the update, (b) sign and encrypt.

The first method is good for pushing an unencrypted file to a Blockchain, while the second method involves confidentiality. Many files are required because of hardware. However, the decryption key is supposed to be set for each existing device. Blockchain infrastructure, and ensure transactions are correct in less than a second. Each IoT Device communicates regularly with the Blockchain and then ensures that a new update is available for download. Therefore, IoT Device installs and downloads the update. Then, issue a Blockchain response to the modern hardware tracking. [15]

2.1.2. Cryptographic Algorithms

In general, a Blockchain can be considered as a permanent record whose records are stored in specific time blocks. Where one block contains transactions. The cluster is defined by its hash and refers to the previous cluster fragmentation. Everything is stored in the public Blockchain.

Pre-defined encryption keys were common on the Internet. Where they are executed in hardware firmware before shipment. Its purpose is to serve as a foundation in other encryption algorithms. However, there are a number of identical or non-random keys. These results allow an attacker to guess or know the encryption key used by the device. [16]

2.1.3. Message Time stamping

Data generated from IoT devices is extensive, combining simple data such as sites, and more complex data such as watch videos. For data analysis, historical data must be reverted, and data must be stored and stored somewhere. Thus, this means that data from Internet devices things will be high standards. This also means that given the variety of data acquisition devices, data will also be heterogeneous. Another aspect of Internet data object is the relationship between space and time. The Internet will place things in a specific location and will place a time dimension on important data in statistical analysis. Only a small amount of data captured by Internet devices will be useful. Visual video can be used as an example where some video frames you capture when someone breaks rules are useful, while working hours and working hours were not useful. [17]

Block chain updating and Protocol Stacks

It was said that the Blockchain update protocol achieves consensus (probabilistic) in a Byzantine environment if these characteristics (probabilistically) are achieved [18]:

1. Health (Health)

   That if all valid nodes that are activated on a shared state require a Blockchain to be augmented by the same block, each documented node moves to a new local copy state, which is Blockchain that is headed by that block.

2. Agreement (consistency)
   If the trusted node confirms that a new cluster header exists, any trusted node that updates the local Blockchain screen will be updated by using this cluster head.
3. Liveness (Termination)
   All transactions that come from shonest nodes will be assured in the end.
4. Total order

All valid nodes accept the same transaction order as long as they are certain in their views of the local Blockchain.

Protocols that are consensus differ with different Blockchain networks. Because allowed Blockchain networks to recognize more stringent control over the synchronization of consensus nodes, they may Byzantine Fault-Tolerant (BFT) protocols to present the needed compatibility characteristics. A typical application for such protocols can exist in the undulation network, where a group of concurrent Ripple servers extend Blockchain through the voting mechanism. Moreover, if an external Oracle is presented to set the initial node to generate the block, the practical BFT (PBFT) can be taken to implement a three-stage commitment schema to expand the Blockchain [19]. Table2 illustrated a comparison Between 4 Major Blockchain Protocols

Table 2: A Comparison Between 4 Major Blockchain Protocols.

Protocol type	Tasks	Key features
Bitcoin	Dealing with encrypted Bitcoin coin	Characterized as less authorized, because it is a public key chain. Thus, anyone can join. - Each node is characterized by having complete information about the Blockchain, and this makes the network a decentralized one - The protocol allows users to perform non-reversible transactions without having to explicitly trust the third part
Ethereum	Launch their own Blockchain projects, including specially encrypted currencies	The Blockchain is marked as generic, does not require permissions. - The same technological backbone, such as encryption defragmentation functionality, uses private and public key encryption.
Ripple Protocol	Facilitate the transfer of money at the lowest cost	- RPCA nodes are applied every second. - The contract will have the last closed ledger. -RPCA happens in tours, and in every tour.
Hyperledger	Design and develop enterprise Blockchain.	- It is an authorized key chain, and no entity can join except trusted by the organization. - Not suitable for coded currencies.

Current Challenges and Issue for BIoT Applications

Nowadays, developing the technologies in the BIoT environment is as Cyber-Physical Systems (CPS) [20] or RFID [21] and telemetry systems [22] or 4G/5G broadband communications [23] were lay in many challenges. In particular, the situation of the Mission and critical situations [24] Increased concerns were added. In addition, the mix indicates that the mix suggests additional operational and operational needs later, and the growth of BIoTs applications is a compound procedure, which was touched by numerous features, which were interconnected.

1.2.3. Energy Efficiency

BIoT endpoints typically benefit from the supplier of power-based coercive equipment with batteries. Thus, energy efficiency was essential to allow long-term node placement. On the contrary, many Blockchains are considered by the power driven. In these cases, most use is due to two elements:

1. Mining

Blockchain are similar to Bitcoin in providing use of large volumes quantities of electricity because of the mining process, that were implicates a consensus algorithm (PoW) which contains in a kind of physical power seek for a hash.

2. P2P communications

Communications need edge strategies, which have to be strengthened on constantly, that might chief to energy waste. There were some researchers suggested energy effective for P2P networks protocols; however, there is still a need to examine additional issues for the exact state of Internet objects [25].

With regard to mining, proposed that the energy consumed by work proofs can be used for useful things while at the same time providing the needed PoW [16] Getting These proofs must have a certain difficulty degree, while verification must be, actually fast. Some Blockchain-based initiatives, such as Gridcoin, reward research computing with volunteer coins (though, as an unanimity algorithm, Gridcoin uses PoS). There was another interesting example was Primecoin, whose PoW mechanism searches for chains of prime numbers. So, a huge infrastructure such as the one involved in IoT could also be with regard to P2P communications, it was necessary for a Blockchain to connect between blocks and peers, so the more updates a Blockchain performs; the more power consumption was allocated to communications. For decreasing the updates number, mini-Blokchains may permit IoT nodes for interacting straightly with a Blockchain, as they only retain the transactions that are final and decrease the computational demands of a full node [27]

Regarding hashing algorithms, SHA-256 was considered the base for being the one used by Bitcoin, but new

algorithms as X11 or Scrypt were faster and may decrease power consumption in mining [26]. Other hashing algorithms, like Blake-256, have been proposed and some Blockchains were able to benefit from various hashing algorithms, although more analyses should be performed on the improvement and performance of advanced hash functions for using on IoT devices [28].

1.2.4. Security

For a personal user, the key for keeping confidentiality is perfect management of his/her own particular keys, as what the attacker wants in conjunction with the public key is to steal something from him/her or embody someone. A good initiative about this subject was CONIKS [29]. A great management system was generated in order to free users from managing the encryption key. In equivalent a system the user first has requested for a public key to a provider, which requires only a username for registering in the CONIKS system [20]. When a user needs to send a message to another user, the CONIKS client searches for the key of the counterparty in the key directory. For avoiding key tampering from the provider of service (which might become involved) [30], two checks performed before sending any message: other clients confirmed the receiver's public key when connecting with the original user, and this key did not alter unusually over time. Identical answers have been presented for BIoT devices, using Blockchain technology in order to access management and foster their identity, presenting Blockchain is security against forgery attacks and IP spoofing [31].

Certificates were also necessary when ensuring security on the Internet. Thus, authorities of certificate use public-key infrastructure must provide trust to third parties [26]. However, such authorities have confirmed their failure on certain occasions, and then having to make previously presented certificates invalidated. Some latest initiatives have been sought to fix certain structural flaws existed in the Secure Sockets Layer (SSL) certificate system. In particular, the Google Transparency Certificate presents a framework for auditing and monitoring SSL certificates in real time. Because of using a distributed system based on Merkle a hash tree that permits third parties to verify and audit if a certificate was proper [32].

The other security feature was the availability although it is really considered the simplest to be achieved by Blockchain, which they were is designed by design to be handed out systems, allowing them to continue employing even when some nodes were under attack. However, the availability may be in compromise by other kinds of attacks. The most feared attack was a 51% attack (also known as the majority attack), where one miner controls a whole Blockchain and perform transactions at wish. In this case, the data is available, but the availability for doing transactions may be stopped by the attacker that controls the Blockchain. It is obvious that this type of attack has an effect on the integrity of data [30].

1.2.5. Privacy

All the Blockchain users were known by its hash or their public key. It implies that anonymity was not achieved, because whole transactions were shared, it was potential for third parties to analyze and identify these transactions and infer the participants' identities [33]. Privacy was more complicated in BIoT environments, because BIoT devices may discover special user data that can be saved in a Blockchain whose privacy requirements are different from a country to another country [34].Thus, in comparison with conventional online payments, which were general only seen to transacting parties and to an intermediary (such as, financial government, institutions), transparent transactions promoted by Blockchain were a privacy challenge.

In a personal Blockchain, subsequently approach controls were achieved later, there was the smallest node which was identified with accesses the scheme. Supposing the neutrality of the access controller, the situation was likely to decrease exposure by founding an impartial Blockchain with each object a user's were participating with. This system develops communications difficulty, although separates the user from none of the wanted to observe. For example, Multichain presents an explanation for organizing personal Blockchains which were assures that the events on the Blockchain may be checked by selected members [35].

Mixing methods may also help to improve privacy. Such methods may aggregate communications from varied IoT strategies and output actions or other transactions to dissimilar directs that were not connected to the unique strategies. These methods expand privacy, but they were not complete, thus they may be deanonymized over numerical detection attacks. Moreover, the mixing facility must be confidential, while a malicious mixer may depiction users and, in the economic transactions, it may stop stealing of coins. To processing such subjects, various proposals proposed subjecting theft over an accountability instrument or beating the input/output address charting from the mixing server [36].

Privacy may also be extended to none knowledge showing techniques such as those operated by Zerocoin and Zerocash or Zcash [37]. A zero of knowledge evidence was a technique that allows for showing to counterparty, which the users were recognized obvious information deprived of uncovering such information. In the case of BIoT applications, zero of knowledge proofs may be used for verification or through reliable transactions for preventing user identity detection or appropriate. However, notice that such evidences were not immune to attacks [38].

In detail, as in the case of mixing methods, they were vulnerable to de-anonymization across statistical detection attacks, but they develop mixing methods by preventing the requirement for a mixing server, which may position pose and present a security and functioning bottleneck.

A solution for achieving privacy was the homomorphic encryption use [39]. Like this type of encryption permits third-party BIoT facilities to procedure a transaction deprived of the reveal of the unencrypted data to those facilities. Many researchers have presented differences in the protocol of Bitcoin for achieving use of homomorphic promises.

1.2.6. Throughput and Latency

BIoT positions may require a Blockchain network capability to generate huge amounts of transactions per time element in clear networks. For example, a Blockchain of Bitcoin contains the highest default level of 7 transactions per second, while it can be extended by dealing with distinct clusters or by adapting the obvious features of node behavior upon receipt of transactions. The assessment did not make the other networks unusually fast. For example, VisaNet (VisaNet) may control 25,500 transactions per second.

With regard to the disappearance, it was important to note that Blockchain transactions are appropriate for some time to deal with. In the case of Bitcoin, for example, the times of mass formation maintain Poisson distribution at a rate of 10 minutes, while, in order to prevent double spending, the wholesalers were delayed for about an hour, and then six or seven blocks are often necessary to be extra for the series Earlier the deal was founded. This individual latency includes a few seconds in the visa position. [40]

As for the assent latency, it may be determined that the difficulty of the consensus procedure was more important regarding latency than unusual hashing, but various blockchain's, such as those verifications of Litecoin, which chosen for scrypt using, a hashing algorithm which was faintly faster than SHA-256 [41].

1.2.7. Block size

Operators store their transactions, requiring larger initial transfer times and benefiting from the most powerful miners. Blockchain methods will be further studied, but the fact is that the largest Internet object node may not be able to handle a small fraction of traditional templates. He noted that different nodes had to store large amounts of data that were not of interest to them, and which could be observed as a loss in arithmetic supplies. This topic may be stopped using lightweight nodes that were able to achieve transactions on the Blockchain. On the contrary, this method needs to stay in the Internet hierarchy of things from the powerful nodes that may clearly Blockchain support for a restricted contract resource, indicating a clear data concentration.

May contain different additional materials when using a mini-series/block [42]. This type of Blockchain produces a version tree usage, which provides supplies for the current state of each user of the Blockchain. Therefore, only the largest current transactions on the Blockchain must remain composed of the version tree. Thus, Blockchain only improves when new users have increased to Blockchain.

1.2.8. Bandwidth

To rise IoT's bandwidth, developers have been suggesting the Software Defined Networking (SDN) tools, which offers smart routing and facilitate the process of making decisions through the SDN manager. [42] In recent times, Sharma et al. [43] suggested a distributed IoT network construction, called DistBlockNet. Depend on the blockchain equipment, DistBlockNet construction can offer extending and elasticity, deprived of the essential for a centralized controller. The distributed blockchain network usages two kind of nodes, specifically, I) the controller/confirmation node, which preserve the improved flow rules table information. II) The invitation/reaction node, which improved its flow rules table in a network of blockchain. [44]

Moreover, it is important to note that transaction and block volume were to be climbed agreeing to the bandwidth limits of IoT networks: various transactions that are small might increase the energy consumption connected to communications, although few great ones may include big payloads that may not be controlled by several IoT strategies.

1.2.9. Usability

In instruction to facilitate the designers' work of Blockchain entering Application Programming Interface (APIs) would be as user welcoming as likely. The same would be operated to the APIs to perform accounts' user. When creating a blockchain, it must be examined according to agreed standards to check if the blockchain is working as necessary. In the situation of the testing stage, various criteria must be evaluated in terms of privacy, safety, power effectiveness, productivity, latency, blockchain capability or usability, among others.

1.2.10. Multi chain management

In many situations, the propagation of Blockchain has originated into the requirement of having to contract with many of them at the same time. This may also occur in case of BIoT, where, for example, sensor standards may be deposited in a personal Blockchain, during economic transactions amid nodes which present offer facilities may be restricted by Ethereum's and Bitcoin's Blockchain.

MultiChain support the institution to create and deploy blockchain applications with speed.

1.2.11. Versioning and forks

Blockchain may be forked for versioning or administrative reasons. Formerly a Blockchain were forked, it was not simple to perform transactions between both chains. The fork occurs when the Blockchain is divided into two sections. This can occur as an outcome of a change in the consensus algorithm or other program changes. based on the kind of the change, the fork can be classified into Soft Fork and Hard Fork.

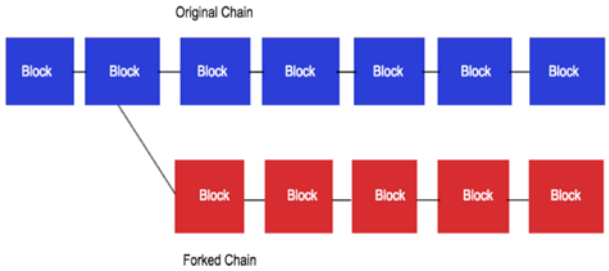

Fig. 6 Fork of Blockchain. [58]

The following figure is a summarized description of the evolution of blockchain and version set technology from 1.0 to 3.0.

- Blockchain 1.0: Currency.
- Blockchain 2.0: Smart Contracts.
- Blockchain 3.0: DApps.

Fig. 7 Blockchain Version. [59]

1.2.12. Autonomy and Enforcement

Legal rules to stress smart contracts and dispute resolution have yet to be developed properly. Some work was being done to conclude realistic contracts with intelligent contracts, but this still needs further study. [34] The smart contract code is stored on the key chain block, and each contract is marked with something unique so that users can work with them, and only send a message by sending one message to that address. The correct execution of the nodes is done by the Blockchain protocol. Blockchain technology enables next-generation application features, enabling the development of assets and smart devices as a service. With Blockchain, devices are able to interact with each other without interference from the server.

Table 3: Current Challenges and Issue for BIoT Applications.

No	Challenges	Issue for BIOT Applications
1.	*Energy Efficiency*	BIoT endpoints typically benefit from the supplier of power-based coercive equipment with batteries. Thus, energy efficiency was essential to allow long-term node placement.
2.	*Security*	For a personal user, the key for keeping confidentiality is perfect management of his/her own particular keys, as what the attacker wants in conjunction with the public key is to steal something from him/her or embody someone. A good initiative about this subject was CONIKS
3.	*Privacy*	All the Blockchain users were known by its hash or their public key. It implies that anonymity was not achieved, because whole transactions were shared, it was potential for third parties to analyze and identify these transactions and infer the participants' identities
4.	*Throughput and Latency*	BIoT positions may require a Blockchain network capability to generate huge amounts of transactions per time element in clear networks. As for the assent latency, it may be determined that the difficulty of the consensus procedure was more important regarding latency than unusual hashing.
5.	*Block size*	Operators store their transactions, requiring larger initial transfer times and benefiting from the most powerful miners.
6.	Bandwidth	it is important to note that transaction and block volume were to be climbed agreeing to the bandwidth limits of IoT networks.
7.	Usability	In instruction to facilitate the designers' work of Blockchain entering Application Programming Interface (APIs) would be as user welcoming as likely.
8.	Multi chain management	In many situations, the propagation of Blockchain has originated into the requirement of having to contract with many of them at the same time. This may also occur in case of BIoT.
9.	Versioning and forks	Blockchain may be forked for versioning or administrative reasons. Formerly a Blockchain were forked, it was not simple to perform transactions between both chains.
10.	Autonomy and Enforcement	Legal rules to stress smart contracts and dispute resolution have yet to be developed properly. Some work was being done to conclude realistic contracts with intelligent contracts.

Future Directions

Based on the security of existing Blockchain systems, we include some future trends to stimulate research efforts in this area. The mixture between blockchain and IoT can suggestion a strong methodology which can meaningfully cover the path for new business methods and spread applications. Develop several of IoT challenges. [1]

1.2.13. BIoT usability

Usability is aspect of the wider expression "user experience" and refers to accessibility. There will be a need to develop a comprehensive trust infrastructure or framework that meets all Blockchain requirements in BIoT systems. Trust depends on the control between areas and policies. For example, governments must create a Blockchain infrastructure to promote use of cases of public interest.

1.2.14. BIoT security

There were remaining topics to be handled concerning the security, scalability, cryptographic development and stability requirements of novel BIoT applications. Besides, Blockchain technologies face limitations of design in transaction capacity, at validation protocols or in the implementation of smart contracts. Moreover, methods to solve the tendency to centralized approaches should be presented. Thus, in a BIoT publishing process, the computing energy brought through miners must be high enough to handle the cooperations be given from the IoT devices. The BIOT was created to send information instead of receiving commands to control objects. For this cause, the possibility of a hacker infecting the system environment with BIOT is very low.

1.2.15. BIoT memory management

Memory management is the method of controlling and managing the memory of computer, specifying parts named clusters to different drivers to improve overall system performance. Memory management occupy in hardware, in the operating system, and in applications and programs. As a result of the growth in Blockchain technology, there are new opportunities for artificial intelligence applications (AI). Which can help solve many Blockchain challenges Like, Oracle was responsible for ensuring that the contract condition was met. Overall, this Oracle was a trusted third party. Artificial intelligence technology has enhanced Oracle's intelligent building. It is not controlled by anyone. He trains himself only and learns from abroad. Thus, there will be no point in the intelligent contract, and the smart contract may be smarter. On the other hand, Amnesty International has been penetrating our lives now. Smart nodes and Blockchain can help decrease misconduct by artificial intelligence products. For example, the written laws of the Smart Contract can help to limit the misconduct of cars without a driver.

1.2.16. BIoT device processing capabilities

In the Internet of Things devices, attackers look for exfiltration the IoT devices data by usage of the cunning codes in malware, particularly on the open source Android platform. With statistical analysis method. Introduced a malware detection system relied on the consortium Blockchain, known as CB-MDEE, which was consisted of detecting consortium Series by test members and the users' general series [43]. The system of Consortium Blockchain for Malware Detection and Evidence Extraction (CB-MDEE) selects a blurred comparison method and multiple labeling functions to decrease the false positive rate and develop the detection capability of malicious variables. Protecting devices embedded in BIoT, ME and others. The firmware update system is based on Blockchain technology, which contains two different hardware-specific process processes, specifically [44]:

1. Responding from a verification node for a requiring node,
2. Responding from a response node for requiring node.

1.2.17. BIoT Access management

For handing devices of BIoT, the technology of Blockchain can be used to provide a new way to handle BIoT devices as a distributed system [45]. This system has 6 constituents which are the following:

1- Manager
2- Wireless sensor network (WSN)
3- Smart contract
4- Management hub
5- Agent node
6- Network of Blockchain

This framework carries benefits for the IoT control in the access of the system, for example,

1- Mobility, that might be utilized in separated authoritative frameworks;
2- Accessibility, that guarantees the guidelines for control of access to be accessible whenever;
3- Concurrency, that permits the policies for control of access to be altered at the same time;
4- Lightweight, that implies the IoT gadgets needn't bother with any alteration to be implemented in this framework;
5- Scalability, the IoT gadgets might be associated via various obliged systems;
6- Transparency means that the framework protects the info of location.

1.2.18. BIoT Intrusion detection

A few proposed methods for Intrusion Detection Systems (IDSs) can be implemented in BIoT system, theses proposed methods are founded using machine-learning techniques. IDSs help detect attacks on systems and networks.

For enhancing collaborative IDSs (CIDSs), in [46 the authors presented using Blockchain so as to verify the trading of cautions between the teaming up hubs.

The two main ways of detection are signature-based and anomaly-based. Any kind of IDS (HIDS or NIDS) can identify attacks depend on signatures, anomalies, or both. The HIDS observe the network traffic flow attainment it's NIC, and the NIDS observe the traffic on the network.

Current IDSs must be founded on the cooperation between different IDSs, requesting broad information sharing and trust between elements. In [47], to manage privacy worries that are upraised by the information trade and to prevent insider assaults, Blockchain was implemented. Along these lines, the utilization of trusted outsider, which was likewise a single point of failure required in customary CIDSs, might be stay away from.

1.2.19. BIoT and real-time video delivery

The dissemination of top-notch media in the BIoT these days encounters from the internet service provider. Nonetheless, in [48] proposed a brokering decentralized method for media transfer based on the collaborative Blockchain, that is depending on cutting edge arrange administrations chains. In particular, this management way was made out of 3 Blockchain, explicitly,

1- The Blockchain of brokering of content,
2- The Blockchain of monitoring the delivery,
3- The Blockchain of provisioning.

Moreover, this management way was implemented using the Hyperledger-Fabric project where the outcomes demonstrate that the quantity of hubs somewhat expands the time of convergence.

1.2.20. BIoT Edge Computing

Fog Computing that is also named Edge computing, is an extensive virtual system that empowers processing and capacity between clients and the server farm of the conventional cloud computing system. With not needing to outsiders, Fog gadgets may speak with one another. Nonetheless, the Blockchain might be utilized to encourage interchanges between fog hubs and BIoT gadgets. In [49], the authors proposed a reasonable payment way for redistributing calculations of Fog gadgets. In the light of bitcoin, this plan thinks about the accompanying security properties, explicitly, fairness, accountability, and completeness.

1.2.21. BIoT Data storage

The storage of data may manage varied information assets for BIoT data storage frameworks. Systematically instructions to share and ensure this important information were the principle encounters in the storage of BIoT information. In light of Blockchain, the authors in [50] proposed a private search for keywords, based on decentralized storage. The Blockchain design incorporates two parts, explicitly,

1- Transaction hubs in network of peer-to-peer (P2P).
2- Blockchain for the coordinated blocks.

Likewise, the Blockchain framework gives clients accountability, privacy, and indistinguishability.

Where it is stored by collecting user data in similar blocks associated with its block number. Where the block number and data stored by the user are used only for segmented authentication. The volume is checked if the volume can be located by using only a specific block number and segmentation. The received data packets are stored from users in the first order at the first checkout in blocks along with the fragmentation of stored data. The new cluster number is then encrypted using the shared key derived from the Davy Helman algorithm. This means that no one can tell the cluster number that owns the key. Since partitions are crash resistant and the real user knows only the cluster number.

Table 4: Future Directions.

No	Directions	Discussion
1.	*BIoT usability*	Usability is aspect of the wider expression "user experience" and refers to accessibility. There will be a need to develop a comprehensive trust infrastructure or framework that meets all Blockchain requirements in BIoT systems.
2.	*BIoT security*	Blockchain technologies face limitations of design in transaction capacity, at validation protocols or in the implementation of smart contracts.
3.	*BIoT memory management*	Memory management is the method of controlling and managing the memory of computer, specifying parts named clusters to different drivers to improve overall system performance.
4.	*BIoT device processing capabilities*	In the IOT devices, attackers look for exfiltration the IoT devices data by usage of the cunning codes in malware. Introduced a malware detection system relied on the consortium Blockchain, known as CB-MDEE.
5.	*BIoT Access management*	For handing devices of BIoT, the technology of Blockchain can be used to provide a new way to handle BIoT devices as a distributed system.

6.	BIoT Intrusion detection	A few proposed methods for Intrusion Detection Systems (IDSs) can be implemented in BIoT system, theses proposed methods are founded using machine-learning techniques.
7.	BIoT and real-time video delivery	The dissemination of top-notch media in the BIoT these days encounters from the internet service provider. proposed a brokering decentralized method for media transfer based on the collaborative Blockchain.
8.	BIoT Edge Computing	Fog Computing that is also named Edge computing, is an extensive virtual system that empowers processing and capacity between clients and the server farm of the conventional cloud computing system.
9.	BIoT Data storage	The storage of data may manage varied information assets for BIoT data storage frameworks. Systematically instructions to share and ensure this important information were the principle encounters in the storage of BIoT information.

Table 5: Selected Studies Result.

N0	Authors	Year	Title	Results
[8]	Melanie swan	2015	Blockchain: blueprint for a new economy	Suggested that progress in the application of Blockchain started next to Bitcoin as Blockchain v1.0, and then changed with respect to smart conventions such as Blockchain v2.0 and subsequently progressed to justice, applications efionation, efiency and Blockchain v3.0.
[10]	Thomas bocek et al.	2017	Blockchains everywhere a use-case of blockchains in the pharma supply-chain	Block-chain technology can be used in various non-financial fields, such as modum.io AG and many other non-financial start-ups. The survival rate of these startups and the success rate of Blockchain technology in private and public applications will determine whether All or only part of those features technically available in practice
[12]	Afzaal ahmad	2017	Integration of IoT Devices via a Blockchain-based Decentralized Application	An idea was introduced to integrate Internet of Things (IoT) systems through a Blockchain based decentralize application depended on Ethereum. The application includes front-end application which can be defused for any web server, and a smart contract which will be deployed on private Blockchain network comprises of Peer-to-Peer (P2P) connected IoT systems acting as a complete Ethereum node.
[11]	Antony oroko orange	2018	Blockchain-based Provenance Solution for Handcrafted Jewellery	Provide solutions, solutions and options based on the technology of the Blockchains to conduct background checks and implement a solution based on the circle of blocks Etherum to control the origin of crafts. The results of the study will contribute to the development of background control mechanisms and will help implement them to make the global supply chain more transparent.
[14]	Shane Brady et al.	2017	Towards an Emulated IoT Test Environment for Anomaly Detection using NEMU	A new way of emulate an IoT environment was proposed utilizing the Network Emulator for Mobile Universes (NEMU), which was built on the known QEMU system emulator, for test bed of inter-related, emulated Raspberry Pi devices. In Addition, demonstrate empirically how the way can be successfully implemented for IoT through demonstrating how this simulation environment can be utilized for reveal anomalies in an IoT system.
[15]	Boudguiga et al.	2017	Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain	Blockchain infrastructure, and ensure transactions are correct in less than a second. Each IoT Device communicates regularly with the Blockchain and then ensures that a new update is available for download.
[16]	Consult, S. E.	2015	House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide	Proposed that the energy consumed by work proofs can be used for useful things while at the same time providing the needed PoW.
[17]	Chen et al.	2014	Big data: A survey. . Mobile Networks and Applications	Visual video can be used as an example where some video frames you capture when someone breaks rules are useful, while working hours and working hours were not useful.
[19]	C Cachin	2016	Architecture of the hyperledger Blockchain fabric	An external Oracle is presented to set the initial node to generate the block, the practical BFT (PBFT) can be taken to implement a three-stage commitment schema to expand the Blockchain.
[22]	Hernández-Rojas	2017	Design and Practical Evaluation of a Family of Lightweight Protocols for Heterogeneous Sensing through BLE Beacons in IoT. Sensors	A series of protocols named Lightweight Protocol for Sensors (LP4S) have been proposed that provides rapid restraint and a lows plug-and-play mechanisms that enable IoT measurement systems to detect new nodes and to describe and record sensors and actuators connected to a beacon.

3. Discussion

This paper is a review of the Blockchain for Internet of things (IoT). Which discusses about the basics and types of Blockchain such as: Blockchain licensed, Blockchain Permission. Many studies and research have dealt the types of plaque as a study Michael et al. (2018), Brown et al. (2016), and Sasson et al. (2014). We also discussed Blockchain's design for Internet of applications things, including Architecture; according to Boudguiga (2017) and Brady et al (2017), Cryptographic Algorithms; based on Consult study (2015), Message Time stamping based on Chen study (2014), then Block chain updating and Protocol Stacks; according to Bano (2017) and Cachin (2016), The current research has also discussed the current challenges and issues of BIoT applications, and many previous studies and research have addressed the challenges and obstacles facing the applications of BIoT like Atya (2017), Liu (2017), Liao (2017), Fabiano (2017), and Meiklejohn (2016). Then the researchers talked about future Blockchain trends for Internet of things, the current research has agreed with some previous studies such as Jiang study (2017), Huang (2018), Herbaut (2017), Cruz (2016), and Lee study (2017). Internet of Things is the state of the art application area, even though it demands for the more secure applications in all domains ranging from smart homes to smart industries [60-63].

A licensed Blockchain is a network that is used by individuals or institutions to conduct their financial business, such as a group of institutions or banks that control financial transactions. The Permission less Blockchain is an open network that can be accessed and used by any individual or entity. Blockchain technology can be used to automate processes and eventually save costs by making sure trust among stakeholders. Blockchain technology is used in more than one Domain and situation. Such as Architecture, Cryptographic Algorithms, Message Time stamping, Block chain updating and Protocol Stacks. BIoT applications face a range of challenges and issues related to Energy Efficiency, security, privacy, Throughput and Latency, Block size, Bandwidth, Usability, Multi chain management, Versioning and forks, and Autonomy and Enforcement.

Based on the security of existing Blockchain systems, we included some future trends to stimulate research efforts in this area. Like BIoT usability, BIoT security, BIoT memory management, BIoT device processing capabilities, BIoT Access management, BIoT Intrusion detection, BIoT and real-time video delivery, BIoT Edge Computing, and BIoT Data storage.

The results of the study showed that the security and privacy of Internet of things are factors of success with the expectations of technology in the development of a number of aspects of our society and our economy. The proposed IoT architecture with Blockchain deals with most security and privacy threats, taking into account resource constraints on many Internet devices. It showed that Blockchain's integration with Internet Objects provides good features through which to solve the problems and challenges of Internet objects, however, the emergence of new challenges and solutions must be considered.

4. Conclusion

The current era witnessing a great technological revolution in various domains such as Health, Finance, Education, Economics and many more. This main reason of this revolution is the Internet of things emerging. The world has begun to resort too many of these techniques that help people to meet their demands within the shortest time and efforts. Besides that, the emerging of Blockchain technology is also an addition in this revolution. The Blockchain is a real revolution in the financial and non-financial trading/transaction around the globe. These techniques play a vital role in the lives of individuals, and institutions. The term "Blockchain" originated from its technical structure (chain blocks), meaning the association of each block with the block that precedes it. The cluster is defined as the data structure that includes many financial transactions. Individuals or entities exchange transactions. These transactions may be financial in nature and sometimes (smart contracts).

This research has presented a scientific addition to the attention of researchers in the domain of Internet of things and Blockchain integration. The study shows a great sign of both technologies on an individual basis and on a collective basis. The current literature shows that the security and privacy is the major concern of organizations especially in case of the internet of things and the addition of Blockchain with the internet of things for providing security and privacy is a better possible solution. Moreover, the study further shows that the integration between the Blockchain and Internet Objects provides great features, which could provide significant help to find proper solutions for the Internet objects security challenges. In this research, The Basics of Blockchain, The Basic Functions of Blockchain, Types of Blockchain, and Blockchain and (IoT) was highlighted. We found based on the literature, that the integration of both technologies will be able to address the existing security issue of IoT based applications.

5. Future work

Blockchain further can be used exclusively in the field of encrypted currencies, where it will greatly increase the compatibility of the Internet of things and blockchain. In addition, blockchain can be further explored to integrate with IoT for providing better security and privacy in different smart application domains.

References

[1] Michael, J., Cohn, A., & Butcher, J. R, "BlockChain technology," *The Journal. Retrieved from: https://www.steptoe.com/images/content/1/7/v2/171967/LIT-FebMar24-Feature-Blockchain.pdf,* 2024.

[2] Lin, J., Shen, Z., & Miao, C. , "Using blockchain technology to build trust in sharing LoRaWAN IoT.," *In Proceedings of the 2nd International Conference on Crowd Science and Engineering,* pp. 38-43, 2023.

[3] Progressif, "The Blockchain": https://progresif.com/how-blockchain-will-revolutionise-our-lives/, retrieved 2023.

[4] Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. , "Corda: An introduction," *R3 CEV,* 2023.

[5] Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. , "Zerocash: Decentralized anonymous payments from bitcoin," *IEEE Symposium on Security and Privacy (SP),* pp. 459-474, 2022.

[6] Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A., " Blockchain and iot integration: A systematic survey.," vol. 18, no. 8, pp. 25-75, 2020.

[7] Wüst, K., & Gervais, A. , "Do you need a Blockchain?," *Crypto Valley Conference on Blockchain Technology (CVCBT) ,* pp. 45-54.

[8] h. atlam, "Blockchain with Internet of Things: Benefits,Challenges, and Future Directions," *I.J. Intelligent Systems and Applications, published online,* vol. 6, pp. 40-48, 2018.

[9] Swan, M. , "Blockchain: blueprint for a new economy," *NY: O'Reilly Media,* 2015.

[10] T. Bocek, B. B., " Blockchains everywhere a use-case of blockchains in the pharma supply-chain," *Symposium on Integrated Network and Service Management (IM),* pp. 772-777, 2017.

[11] A. O. Orenge, "Blockchain-based Provenance Solution for Handcrafted Jewellery," 2018.

[12] M. Taylor and P. Liddle, "Deploy smart contracts to your private Ethereum blockchain network on AWS," *AWS Database Blog,* 2019.

[13] A. Ahmad, "Integration of IoT Devices via a Blockchain-based Decentralized Application," 2017.

[14] S. Brady, A. Hava, P. Perry and J. Murphy, "Towards an Emulated IoT Test Environment for Anomaly Detection using NEMU," France, 2017.

[15] A. Boudguiga, N. B. , "Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain.," *E European Symposium on Security and Privacy Workshops (EuroS PW) ,* pp. 51-55, 2017.

[16] Consult, S. E. , " House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide," *International Symposium on Consumer Electronics ,* pp. 23-30, 2015.

[17] Chen M, M. S. , " Big data: A survey. . Mobile Networks and Applications," pp. 171-209, 2014.

[18] S. Bano, A. S.-B. , " Sok: Consensus in the age of blockchains. arXiv preprint arXiv," no. 1711, 2017.

[19] Cachin, C. , "Architecture of the hyperledger blockchain fabric," *Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Chicago.,* 2016.

[20] Fraga-Lamas, P. C.-R. , " Evolving military broadband wireless communication systems: WiMAX, LTE and WLAN," *Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS),* pp. 1-8, 2016.

[21] Barro-Torres. , "Maritime Freight Container Management System Using RFID," *Proceedings of the Third International EURASIP,* pp. 6-7, 2014.

[22] Hernández-Rojas. , "Design and Practical Evaluation of a Family of Lightweight Protocols for Heterogeneous Sensing through BLE Beacons in IoT. Sensors," vol. 18, no. 1, pp. 1-33, 2017.

[23] Fraga-Lamas, P. N.-D. , "Smart Pipe System for a Shipyard V4.0. In Sensors," vol. 16, no. 12, pp. 1-43, 2016.

[24] Fraga-Lamas, P. , " Enabling Technologies and Cyber-Physical Systems for Mission-Critical Scenarios.," *Coruña: PhD dissertation. University of A Coruña,.,* 2017.

[25] Liao, C. C. , "On Designing Energy Efficient WiFi P2P Connections for Internet of Things. IEEE 85th Vehicular Technology Conference (VTC Spring),Sydney, Australia.," pp. 5-10, 2017.

[26] Bruce, J. D. , "Mini-Blockchain Scheme.," 2018.

[27] Aumasson, J.-P. H. , "SHA-3 Proposal BLAKE, submission to NIST.," 2018.

[28] Atya, A. , " Malicious co-residency on the cloud: Attacks and defense. Atlanta, United States," *Proceedings of the IEEE Conference on Computer Communications.,* 2017.

[29] Liu, B. Y. , "Blockchain Based Data ntegrity Service Framework for IoT Data," *International Conference on Web Services ,* pp. 25-36, 2017.

[30] Kshetri, N. , "Can Blockchain Strengthen the Internet of Things? IT Professional," vol. 19, no. 4, pp. 68-72, 2017.

[31] Chen, T. M. , " Lessons from Stuxnet. Computer," vol. 44, no. 4, pp. 91-93, 2014.

[32] Meiklejohn, S. , "A fistful of bitcoins: Characterizing payments among men with no names," *Communications of the ACM,* vol. 58, no. 4, pp. 86-93, 2016.

[33] Fabiano, N. , "The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard. 1-7:," *Proceedings of the International Conference on Internet of Things for the Global Community*

(IoTGC), , Portugal., 2017.

[34] Danezis, G. S. , " Statistical Disclosure or Intersection Attacks on Anonymity System," *Toronto, Canada: Proceedings of the 6th International Workshop on Information Hiding, ,* 2014.

[35] Valenta. , " Blindcoin: Blinded, Accountable Mixes for Bitcoin. San Juan, Puerto Rico," *International Workshops on BITCOIN, WAHC, and Wearable.,* 2015.

[36] Schukat, M. F. , "Zero-knowledge proofs in M2M communication. Limerick, Ireland: Proceedings of the 25th IET Irish Signals & Systems Conference and China-Ireland International Conference on Information and Communications Technologies," 2014.

[37] Moore, C. , " Practical homomorphic encryption: A survey," *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS).,* 2014.

[38] Hayouni, H. H. , "Secure data aggregation with homomorphic primitives in wireless sensor networks: A critical survey and open research issues. Mexico City:," *Proceedings of the IEEE 13th International Conference on Networking, Sensing, and Control (ICN,* 2016.

[39] Taylor, B. , "The Evolution of Bitcoin Hardware. Computer , v," vol. 50, no. 9, pp. 58-66, 2017.

[40] Courtois, N. T. , " Could Bitcoin transactions be 100x faster?," *Proceedings of the11th International Conference on Security and Cryptography (SECRYPT), . Vienna, Austria.,* 2018.

[41] França, B. F. , "Homomorphic Mini-blockchain Scheme.," 2018.

[42] J. Gu, B. S. , "Consortium Blockchain-Based Malware Detection in Mobile Devices. IEEE Acc," vol. 6, pp. 12-118, 2018.

[43] Lee, B. L.-H. , "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. J. Supercomput," vol. 73, no. 3, pp. 1152-1167, 2017.

[44] Novo, O. , "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet Things J," vol. 5, no. 2, pp. 1184-1195, 2018.

[45] N. Alexopoulos, E. V. , "Towards blockchain-based collaborative intrusion detection systems," *Proc. Int. Conf. Critical Inf. Infrastruct. Secur,* pp. 1-12, 2017.

[46] T. Cruz, L. R. , "A cybersecurity detection framework for supervisory control and data acquisition systems. IEEE Transactions on Industrial," vol. 12, no. 6, pp. 2236-2246, 2016.

[47] Herbaut, N. N. , "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains. IEEE Commun. Mag," vol. 55, no. 9, pp. 70-76, 2017.

[48] H. Huang, X. C. , "Bitcoin-based fair payments for outsourcing computations of fog devices. Futur. Gener Comput. Syst," vol. 78, pp. 850-858, 2018.

[49] P. Jiang, F. G. , "Searchain: Blockchainbased private keyword search in decentralized storage. Futur. Gener Comput. Syst .," 2017.

[50] K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," *IEEE Commun,* 2017.

[51] K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," *IEEE Commun,* 2017.

[52] P. K. Sharma, S. Singh, Y.-S. Jeong and J. H. Park, "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks," *IEEE Commun,* vol. 55, no. 9, p. pp. 78–85, 2017.

[53] M. A. Ferrag, M. Derdour and M. Mukherjee, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," *IEEE,* 2018.

[54] O. Daniel, "How Blockchain Technology Works in Layman's English – Infographic," techatlast, 2010.

[55] H. ANWAR, "Web 3.0 Will Be Powered by Blockchain Technology Stack," 2018.

[56] H. Noon, "The Blockchain & IoT Tech Stack," 2018.

[57] A. Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," Raja Jurdak is with CSIRO Brisbane, 2016.

[58] JavaTpoint, "javatpoint," blockchain tutorial , 2018 . [Online].

[59] S. Ray, "Blockchain Forks," hackernoon, 2017.

[60] ZA Almusaylim, N Zaman, A review on Smart home present state and challenges: linked to context awareness internet of things (IoT), in Journal Wireless Networks, 2018, pp. 1-12.

[61] M. Almulhim and N. Zaman, Proposing secure and lightweight authentication scheme for IoT based E-health applications, 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 481-487.

[62] Maher Omar Alshammari, Abdulmohsen A. Almulhem and Noor Zaman, Internet of Things (IoT): Charity Automation, International Journal of Advanced Computer Science and Applications (IJACSA), 8(2), 2017. http://dx.doi.org/10.14569/IJACSA.2017.080222.

[63] Almulhim, Maria, Nazurl Islam, and Noor Zaman. "A Lightweight and Secure Authentication Scheme for IoT Based E-Health Applications." International Journal Of Computer Science And Network Security 19, no. 1 (2019): 107-120.