IOT Security with Blockchain

Abhinav kumar [1] Divyansh Dixit [2] Anish Raj [3] Geeta Nijhawan [4]
[1]*Manav Rachna International Institute of Research and Studies*
[2] *Manav Rachna International Institute of Research and Studies*
[3] *Manav Rachna International Institute of Research and Studies*
[4] *Manav Rachna International Institute of Research and Studies*
[1] *abhinavkumarpal890@gmail.com* [2] *Divyanshsec23@gmail.com* [3] 1999anishraj@gmail.com
[4] *geeta.fet@mriu.edu.in*

Abstract

Internet of Things (IoT) plays a very vital role in almost every field of technology. Its key elements of security are very much crucial elements which are to be maintained as it is used universally. Traditional security and privacy methods be likely to be inapplicable for IoT, mainly due to its distributed network topology and the supply-constraints of most of its devices. For creating these concepts, a new technology called blockchain can be used. Blockchain that reinforce the crypto- currency Bitcoin have been just now used to provide security and privacy in peer-to-peer networks with similar topologies to IoT. In this paper, we present basic part of IoT enabled with blockchain, their distinctive features of both the technologies, their futuristic solutions for different real-world issues, different communicational standards etc. Both the technologies have several distinctive characteristics in every field, but certain limits too exist which gives futuristic path for research.

Keywords: *Blockchain, IoT, Iot devices, Security, B-IoT Communications Models, Privacy, transmission.*

1. Introduction

The IoT is an evolving well-recognized technology whose purpose is to connect several sorts of devices to the internet. The smooth convergence of Radio Frequency Recognition, wireless transmission and devices helps in the development of IoT Devices. Using the intelligent characteristics along with IoT facilities, platforms get implanted for delivering intelligent critical services, using controllers and electromechanical structure to create integration between cyberspace and physical world. There are various types of IoT practices such as MQTT (Message Queuing Telemetry Transport), Constrained Application Protocol (Co-AP), Bluetooth Low Energy. Due to discrepancy of the IoT requirements, protocol requirements and IoT devices numerous challenges get raised such as flexibility, lack of interoperability and scalability. In IoT structures designs, various architectural projects get followed such as microservices design and services-oriented designs which are a part of services focused on solutions. In these solutions, using the communication protocol, the Iot devices aided other devices. The service is referred as an availability of business functionality through a service contract. A service agreement includes documentations, service policies, QoS, and a service interface for observing and ensuring the QoS and the implementation of IoT transactions. The techniques used for interoperability, incorporations, and enabling unified services structure among IoT platforms and applications whichworks on several different devices over heterogeneous networking technologies is called service managements [1]. The design of evolving Internet of Things (IOT) technology is mainly implementing by the industries which results in starting of new income streams for several industries. In the past several years,

the implementation of IoT solutions in industrial region has grown swiftly. Cryptocurrency head start to formation of Blockchain which is as most promising technology. The data of routine trades which is done by larger number of customers and devices is stored and track by decentralized applications (DApps). Decentralized applications arise from cryptocurrency [2]. The IoT can understand various systems of communication where the machines could interact with each other through internet.They are commonly known as "things" and as defined in Fig1, they have certain traits that are analyzed beneath.

- ***Identification-*** All IoT devices need to have identification like sixth edition of Internet Protocol (IPv6) address to communicate or trade information with other things.
- ***Sensing-*** To gather information, the sensing techniques are used to recognize physical ecosystem.
- ***Communication-*** It requires connection techniques and are exploit for communicating the things.
- ***Computation-*** These methods are adopted to gather the data that is obtained by objects.
- ***Services-*** It implies to those techniques that are certain by things in relation with data to thecustomers that is obtained from the physical ecosystem.
- ***Semantics-*** It implies things have the power to use the correct data from ecosystem.

RFID (Radio Frequency Identification) tags, Cubie Board, Raspberry Pi, Beagle Board and Arduino UNO are some examples of IoT devices [3]. A part of advancement boards, which have Random Access Memory, read only memory, a processor along with several analog and digital input/output pins are called Microcontrollers. Several sensors are usually linked to MCU processing, responsive trigger, and transmission to more approach. Potentiometers, accelerometer, temperature, vibration sensor, proximity sensors, moisture sensor and air quality sensor are some of the sensors used. A real-time operating is necessary to manage the data, distribute the memory and further utility essential services maintaining communication. RTOS is designated on the base of performance, functional necessity and security of the invention. WSN generally known as wireless sensors network is amongst the top supporting method for IoT presently [68,69]. Creating and establishing up security is an exceptionally significant obstacle in WSN mostly formed by constrained accessibility of resources at each sensor. Together with standard difficulties handled while designing security in WSN as well as IoT, many other special features of IoT and WSN shows that security circumstances and situations in IoT are much more severe and complex than in WSN, cause being their non-alike features and uncommon targeted applications and systems. Firstly, WSNs are highly deployed in application made for gathering raw information for example ecological inspection and inspection techniques. All the information is primarily gathered and then kept by sensors and then delivered to be submerged through reliable multiloop routing protocols. Hence most of the communication is unidirectional, even though the inverse direction is also utilized for distributing control signals and controls that in turn are used for controlling sensors. Furthermore, sensors in Wireless sensor network as well as the end duration system in IoT face the challenge of restricted establishment of resources, although sensors might have other problems with power restrictions [4]. Furthermore, a WSN is commonly aloof from other WSNs and are usually made for a certain application. Parallel to this, IoT aims to join several domain specific and self- operational processes. In the end, comparing general IoT systems like smart grid or intelligent residence projects with common WSN application like industrial inspection, large data is collected in IoT applications as compared to WSN. Depending upon all these facts, we can conclude that security

requirements of IoT is high and it's more complicated to construct a appropriate security solution for it than for WSN [5].

2. IoT- Architectural View

IoT doesn't have a basic structural design but is divided into communication layers similar to standard I.T. networks. Numerous analysis attempts have stated their own models comprising 3 layers, 4 layers or the 5-layers. Business layer, support layer, communication layer and perception layer form a four layered design of IoT. The perception layer consists of technical elements such as sensors and actuators to obtain information about the physical ecosystem [6]. The purpose of Communication layer is to provide reliable transmission of data between various layers. This layer consists of 6 sublayers namely application, session, transport, network, MAC, Physical Layer. Support layer strengthens the functioning of remaining layers by establishing computing services and storage service. The fog/edge and cloud computing are the primary technologies of support layer. The software application that are built on the intel of industry explanation and user needs are included in business layer [7].

- IoT is a system which unites an immense number of heterogenous and large-scale end terminal devices to each other. A very big quantity of data bits is collected and delivered in IoT. As per the examined information that was gathered, IoT primarily aims to build a self-regulated, automated, and exceptionally smart world. IoT applications essentially works at the peak of three layers i.e., the objects layer, the cloud layer, and the edge layer. Every level has a perfect capacity to gather, process and then examine the data on its own. Bi commute that is both way transmission is mostly feasible, despite the fact most of the data starts travelling in objects layer and end on the layer of cloud via going through edge layer than otherwise.
- Things layers contain a large quantity of heterogenous material that includes actuators and sensors. End terminal devices are made by incorporating physical and cyber parts together; physical comprising of items that stretch out into real physical world whereas cyber consist of ways to create connectivity and storage. The material may vary a lot in terms like computation, power supply and reposting. As an example, to support that, smart meters are able to carry out complicated computations whereas smart bulbs are able to carry out only a slight amount of minimal computations. To conclude, usually all items are resource- restricted and energy restricted that creates them not very appropriate for operating heavy tasks.
- Cloud layer is a solid layer and it have a lot of resources available for maintaining main and complex computing tasks like obtaining data from a big storage of data and performing difficult and complicated computations on it, for about distributed invasion recognition. Edge layer which is also known as gateway or fog layer was put ahead with the aim of stuffing gaps within things-layer which deficiencies in resources as well as cloud layer which is valuable in supplies. Edge layer is one of the most crucial layers of the whole architectural design. Usually the edge devices are merged with physical objects directly or sometimes they are just numerous hops away. In contrast with things layer, devices usually have access to a lot quantity of resources just like big storage spaces, standard power supply and high computing power. It determines every layer of IoT design has specific requirements that makes them irreplaceable. It's crucial to establish them in a way that they can work collaboratively in developing whole new smart and efficient IoT system.

3. Blockchain as a Solution for IoT

IoT is making a difference in today's world because of its significant contribution to various fields such as industry, health care, logistics, agriculture, telemetry, etc. IoT gadgets are used to share data between gadgets. According to a survey [8], more than 20 billion IoT gadgets and smart phones are being used these days. It supports accessibility and heterogeneity as multiple devices are connected and share important information [9]. These IoT structures offer a variety of problems and challenges related to trust, security, authenticity and privacy. Sensitive details of various sectors such as the economy, military communications, and health care are affected by these challenges [10]. These problems can be solved by a technology known as blockchain because in this technology various transactions related to confidential information will take place among many participants [11]. It provides a variety of internal features such as integrity, authenticity, privacy protection and fraud that can help IoT resolve the requirements for trust, confidentiality and security [12]. IoT problems related to trust and privacy can be solved via blockchain as these technologies can track billions of gadgets simultaneously, and can work with communication and transactions between multiple participants [13]. One point of failure can be eliminated by this technology due to its distributed nature and make the IoT system more flexible and unstable. The man in the middle attack cannot be made into blockchain technology because it ensures the reliability of shared ledger data that provides distributed space and avoids being caught by telephone, using multiple transmission channels. All of these blockchain features make it a popular and secure technology. It also reaffirmed its role in the financial and banking sectors by providing cryptocurrencies platforms such as Ethereum, Bitcoin etc. Therefore, without the involvement of any third party companies, payment services between Peer to Peer and transfers among many unreliable users are possible. Many IoT organizations have adopted blockchain technology because of its reliable, independent, realistic and useful IoT distribution. All fixed activity records related to smart devices and transfers will be managed by this technology. In addition to centralized access, these properties may allow for the independent use of smart devices. Because of all these factors there is no possibility that it can be implemented in IoT environments. The role of the blockchain in IoT is not a new concept as most of the barriers to IoT technology have been reduced by the use of this technology [14]. IoT limitations are high power consumption, high storage need, security, high calculation etc which necessitates the integration of blockchain technology integration into IoT (BIoT). In 2016, in Berkley [15], a working group of IoT protocol and Blockchain worked together to establish a trust called the Trusted IoT Alliance, an organization of 17 organizations whose mission is to ensure environmental change, trust, security, trust, privacy and heterogeneity using blockchain technology in the IoT framework in a low-level network. In 2015, an 61-member Linux Foundation's Hyperledger Project was launched. Many other projects working using blockchain technology in the IoT system are LO3ENERGY, IoTeX, Raspnode, EthEmbeded, CoT (Chain of Things).

3.1 Application of BIoT

By integrating blockchain into IoT technology, prediction of different applications can be possible in various fields, for example it can be used for network design and modeling, also in sectors (such as smart grid, agriculture, etc.), supply chain management, & data sources etc.

3.1.1 Energy sector

In this regard, the development of blockchain technology has shown a positive effect by removing intercessors, and reducing costs. In a scalable manner without having a centralized operating system, active power allows shared devices and resources to trade power. On the smart grids, the infrastructure to enable a reliable, efficient and secure blockchain-based solution developed by Lombardi et al. [16]..

3.1.2 Smart Contract

Despite the fact that the blockchain brings many solutions to IoT issues, it has high computational requirements, which require a process of consuming resources, minimal time and cost-effectiveness. The implementation of smart contracts in BIoT, Slock.it is presented by G. Prisco [17] as a solution that allows to connect various gadgets to the blockchain to enable the Economy of Things.

3.1.3 Privacy

Privacy is another big challenge in the IoT field as it is a large-scale network used to share data. Therefore, privacy is needed to prevent data theft. Many solutions have been introduced by researchers to address data privacy concerns in the IoT domain but which affect the expansion of IoT networks as solutions are sought in a single network. Due to its decentralized structure, without causing expansion problems, blockchain provides data privacy techniques that help protect data from intruders. Blockchain is used to store IoT data and release it for a limited period of time to carry out transactions. Lightweight blockchain solutions have been introduced by many researchers to enable privacy in IoT data.A lightweight blockchain with algorithms has been proposed by Dorri et al [18] to manage throughput, distributed trust, and lightweight consensus, which is minimized for IoT. To issue privacy information using the interplanetary file system & # 40; IPFS' and blockchain, the network architecture proposed by Atlam et al. [19]. Chain of Things is a platform used to integrate IoT hardware and blockchain technology that provides solutions to IoT issues related to interoperability, security and privacy [20]. For IIoT and business transactions, Filament provides hardware solutions between IoT gadgets using blockchain. IoT brings revolution in every sector like blockchain, healthcare, industry, etc. Help improve the industrial sector in terms of intelligent manufacturing, resource monitoring, latency reduction and supply chain management. IIoT gadgets are very vulnerable to various attacks related to trust, privacy and security because of these various inherent properties such as security standards, low cost and low cost. Blockchain helps prevent IIoT devices from these attacks by providing immutability and a source of information.

3.1.4 Expansion and decentralization

With the establishment of an IoT network in the middle, this makes it difficult to expand the IoT ecosystem. This problem can be solved by integrating blockchain technology into IoT. Various solutions have been presented by researchers to overcome these concerns. By shifting ownership of IoT gadgets between homogeneous blockchains, an upward peer-to-peer recognition procedure has been proposed by Ghuli et al [21]. In BIoT, Ruta et al introduced `Service Oriented Architecture` (SOA) [22] for discovery, collection, payment and registration via smart contracts. It is based on "IoT gadget semantic blockchain".

3.1.5 Databases and storage

Since blockchain technology is distributed by nature, it is therefore used in the development of distributed databases and storage structures. It also ensures security structures for users such as access control, authorization, authentication, and data integrity. BeeKeeper, a blockchain-based IoT system proposed by Zhou et al. [23]. "Computational energy for IoT gadgets", this technique offers secure storage and compute sent even without loss of data privacy. BigchainDB is a distributed storage software offering low latency, high transaction speed, structured data queries, and indexing [24]. Shafagh et al. [25]. Since the IoT ecosystem has accumulated an excessive amount of data, therefore, Xu et al. introduces blockchain based solutions for data analysis. [26], which provides archiving of the information.

3.1.6 Security

Many security solutions have been proposed by different researchers, most of them are relying on high computational cryptographic algorithms. The presence of blockchain technology brings solutions to the IoT sector, as the integration of blockchain into IoT leads to the resolution of security concerns. In an IoT system, blockchain delivers access control, authorization, authentication, reliability, and privacy. Khan et al. [27] have discussed the security concerns in IoT, its solutions as well as open challenges to get the better of BIoT. A survey has been presented by Li et al. [28], in which the author has discussed diver's security solutions which can also be implemented by integrating blockchain in the IoT- based system. A review paper by Baneerjee et al[29] presented various security solutions that blockchain technology carrying to the IoT ecosystem. Jesus et al.[30] has also presented a survey for securing stalker attacks and IoT using blockchain. As IoT infrastructure is shaped in the environment, it presents many challenges. Therefore, much work is being done to find the BIoT, which is why many solutions to these problems are presented by investigators. To maintain the responsiveness and availability of gadgets and IoT data, Boudguiga et al. [31] investigated how authenticity and confidentiality could be verified in the BIoT.

4. Different communications models of BIoT

In BIoT, the IoT devices can be conveyed either directly or through a cloud computing, fog computing model or blockchain [32]. The numerous concepts of BIoT are explained as follows:

4.1 Communication theory for direct IoT gadgets

In this model, communication between IoT devices occurs directly without involving blockchain or other models.This is the swiftest model as it works without involving time utilizing and high computational algorithms of blockchain. But it doesn't guarantee security, reliability, and confidentiality [33]. Thus, to enable these security features, the chronological details of the IoT devices transaction or transmission is stored in the blockchain. This model offers fast transmission between IoT devices as it required low security. Figure 1 shows the Direct IoT gadgets communication standard.

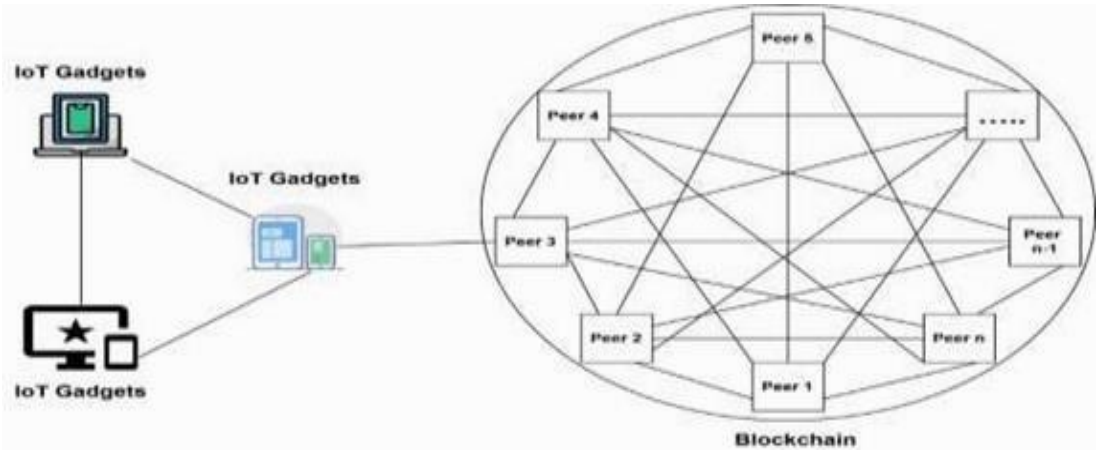

Figure 1. Direct IoT gadgets communication paradigm

4.2 Communication model for IoT machines on basis of Blockchain

It delivers the data consistency, security as well as privacy because all the transaction goes through blockchain in this model. In this the transmission between the IoT devices take places using blockchain technology where the fixed data is stored of every transaction [34] as shown in Figure 2.

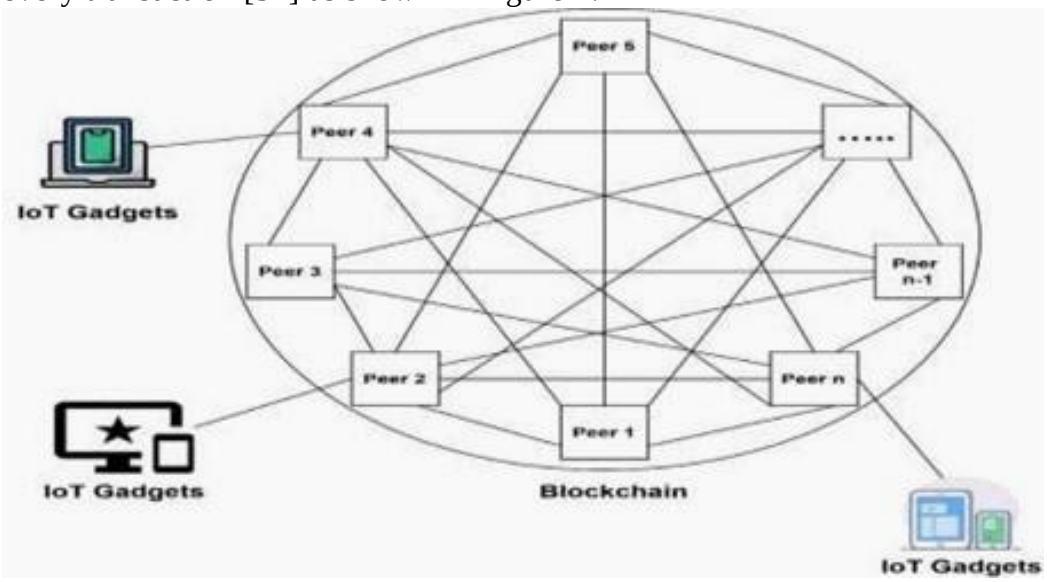

Figure 2. Blockchain based transmission standard for IoT devices

4.3 Cloud-based communication model for IoT machines

Fog computing generated revolution in the field of IoT by shifting computation load (such as compression, hashing, and encryption) from IoT devices to fog nodes [35]. In case of BIoT also, the load because of time consuming as well as high computational blockchain's algorithm can be transferred to the fog node so that the consistent transmission takes place between the IoT gadgets as shown in the Figure 3 [36].

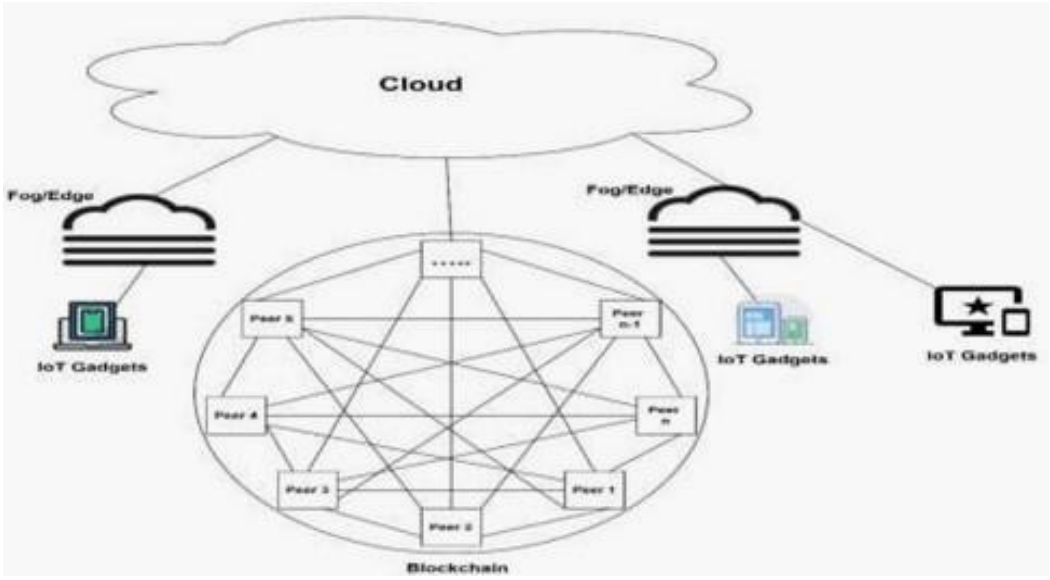

Figure 3. Cloud-based communication standard for IoT devices

5. Different platforms of Blockchain for Internet of Things

Different platforms get designed for the IoT networks due to various quality features and properties.

5.1 IoT Chain

It is latest platform for IoT devices, which work as decentralized network. It is not accessible widely to the participants for the development. It only shows securities, outcome, other matters, and consent to the IoT network. It differentiates result with SLOCK, IBM-ADEPT, IOTA, IT and various other subsequent projects. It underpins DAG and PBFT as agreement.

5.2 IOTA

It is defined as a distributed ledger design which is utilized to store and executes the transactions among IoT devices and machines. It intends to build the quality technique of supervising transactions on the devices. It is public permission-less support for the IoT devices which allows interoperability among multiple devices. Its main aim is to resolve the implementation concern and scalability with bitcoin by switching its blockchain with Tangle as it is a system of nodes in which new transactions assures the preceding transaction. It utilizes Directed Acyclic Graph which is mainly created for the Internet of Things ecosystem. Its major invention is Tangle that is used for the verification of transactions The IOTA system claims that the node system is well established, systematic, effective and faster than other blockchain prototypes used in cryptocurrency is Tangle, which is a decentralized acyclic chart whose purpose is to solve the problems of system flexibility and performance. During the transaction process, the tangle becomes more adaptable, secure and efficient as different systems are connected to it. Effort, memory, and time prerequisites are reduced to authenticate transactions as each new transaction is confirmed by the previous two nodes.

5.3 Walton chain

As IoTChain & IOTA, it is also created for the IoT system which functions as decentralized system. It comprises of software and hardware. In IoT devices, RFID is utilized as a communication approach, and the electronic transmission is implemented on recently proposed blockchain design. Software consists of Walton Coin and Walton Chain Practices. For the development of reliable IoT devices, an open secured and reliable hardware engine presented by the Open IoT Blockchain.

6. Blockchain and IoT Incorporation

The concept of IoT device ecosystem in order to convey it towards a decentralized architecture was advanced by the Brody et al [38] so that it maintains its sustainability. To overcome the privacy and trust concerns from customer's point of view, there is need of "security through transparency" method. To maintain the present centralized model, manufacturer has to spent huge amount on the maintenance and improvement. Blockchain has successfully overcome this problem because it works on a scalable peer-to-peer network replication that works transparently and spreads data securely. To see how this model works, let's assume a structure in which all IoT devices work on a separate blockchain network. The smart contract which is installed by the producer make possible to store the hash of the newest network firmware renovation. When the binary generates a certain number of competent nodes, the manufacturer's own node no longer meets the requirements of the original file. Devices that are configured are supposed to share their received binary, thus sanctioning firmware update retrieval by even devices that connect to the network after the manufacturer stops participating. This happens automatically and there is no involvement of any user relations. Also, the blockchain network is exchanged through cryptocurrency which allow for the easy exchange of assistance between devices and also provides a suitable billing layer. These devices store the binary edition to increase the price of the infrastructure or make a profit and they have deducted a certain amount to operate it.. Here are some examples: Filecoin [38] allows devices to donate their disk space for rental and EtherAPIs [39] helps monetize API calls.. With the help of microtransactions every device accepts actual payment for their usage.

After the integration of blockchain and IoT, it also facilitates the sharing of services and goods. The concept

of "Slocks" [40] was introduced by Slock.it. It is smart electronic lock which are unlocked only when there is relevant token present. In energy sector there is need to facilitate peer-to-peer market place so that on the basis of some user-defined criteria these machines are capable of buying and

selling energy automatically. The excess surplus on the blockchain is accounted for by the solar panels and the environment benefits after purchasing them.

6.1 Divers challenges of BIoT applications

IoT ecosystem technologies goes through numerous challenges like telemetry systems, RFID, and 5G/4G broadband communication [41]. These issues raise additional concerns in the case of evaluative applications, which we must investigate. Because of the intricacy of BIoT applications, including blockchain into this creates additional technological and operational needs. Now, in the upcoming subsections we will discuss about major factors that affect the development of the BIoT application.

6.1.1 Energy Efficiency

It is evident that blockchain requires a large amount of electricity for the mining and P2P communication. Because of consensus algorithm blockchains like bitcoin destroys extensive electricity in the mining procedure. There is lot of energy wastage because P2P communication consumes continuous power.

6.1.2 Security

Confidentiality, availability, and integrity are the three challenges which have to be fulfilled for a better security in any information systems. Data integrity is one of the major component for Iot applications data integrity. The service framework for integrity was proposed by the Liu et al. and it works on blockchain technology and it doesn't rely on third party for cloud based IoT applications.

6.1.3 Privacy

A major concern in IoT environments is privacy due to which IoT applications faces certification issues. To overcome this privacy issue Zero knowledge proof come into an action which do not count identities of user during any transaction and supply desired level of authentication.

6.1.4 Throughput and latency

An architecture like the blockchain should be needed to regulate a large number of transactions per unit time when positioning an IoT. In addition, it becomes a difficult factor for networks like Bitcoin, which support up to seven transactions per second.

7. Future research directions

After numerous advantages, blockchain faces several challenges in its adoption in IoT. These challenges comprise of privacy preservation, utilization, and scalability. In below section, we will discuss about challenges and future research that how blockchain will be integrated in IoT.

7.1 Scalability issues in blockchain

There are numerous researches evident which explains that blockchain is a scalable and there are still so many researches going on [42]. One only clause which restricts the scalability is the demand for high networking and high performance this issue is still a worry for blockchain networks distributors

7.2 Privacy concerns related to permission-less blockchains

Every transaction detail of bitcoin is made available to their network distributors. In such sort of structure users are capable of transferring out transaction on numerous addresses. To avoid the leakage of information, all the information related to the transaction is kept at one point. Due to some disturbance these open records disclose user information and from this, IP address of the user is easily tracked. With the assistance of multi-step hierarchy architecture privacy of the blockchain is maintained.

7.3 Decentralizing IoT with machine learning (ML) and big data

Now a days, machines are easily trained and many devices learn from their former experience with the help of new and emerging Machine learning technology and it is

an Artificial Intelligence (AI). In this process machines are not depending on the complicated mathematical algorithms. Decentralizing IoT with the ML face a crucial challenge in the field of authentication of the training sets. There are transitory identifications, anonymity ensures data security, encryption is required, and moral considerations such as why and how to use the created massive IoT data must be considered. Huge amount of data needs further investigation and are still in their infancy. Majority of the suggested strategy connected to decentralization of IoT using ML.

7.4 Complex infrastructure and technical challenges

There is requirement of such trustworthy infrastructure that fulfils all the requirements for using blockchain in IoT ecosystems. Although, blockchain also has to faces some challenges in designing, in transaction capacity or in validation protocols. In addition to the technical challenges, there are a few other challenges, such as decentralized ownership and international jurisdiction, which are important issues for developing capable BIoT values.

8. Conclusion

IoT plays a very important role in all areas due to its advancement of the latest technologies used. In this paper a brief introductory part focuses on key elements making this technology at utmost priority with blockchain enabled features with it. A number of characteristic features of both the technologies along with their framework, applications are discussed. As security is main concern in any model therefore many challenges do exist in this part which are used as guiding principle and open challenges. With use of these open issues a new futuristic approach can be formulated which gives rise to a new research-based feature in these types of system.

References

[1] *Nikoukar, A., Raza, S., Poole, A., Gunes, M., & Dezfouli, B. (2018). Low-power wireless for the internet of things: Standards and applications. IEEE Access, 6, 67893–67926. https://doi.org/ 10.1109/access.2018.2879189.*

[2] *Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics, 14(11), 4724– 4734. https://doi.org/10.1109/tii.2018.2852491.*

[3] *Fan, K., Luo, Q., Zhang, K., & Yang, Y. (2020). Cloud-based lightweight secure RFID mutual authentication protocol in IoT. Information Sciences, 527, 329–340. https://doi.org/10.1016/j. ins.2019.08.006.*

[4] *Chowdhury, A., & Raut, S. A. (2018). A survey study on internet of things resource management. Journal of Network and Computer Applications, 120, 42–60. https://doi.org/10.1016/j. jnca.2018.07.007.*

[5] *Kaushik, I., Sharma, N., & Singh, N. (2019). Intrusion Detection and Security System for Blackhole Attack. 2019 2nd International Conference on Signal Processing and Communication (ICSPC). doi: 10.1109/icspc46172.2019.8976797*

[6] *Tran-Dang, H., & Kim, D. (2018). An information framework for internet of things services in physical internet. IEEE Access, 6, 43967–43977. https://doi.org/10.1109/access.2018.2864310.*

[7] *Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the internet of things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. International Journal of Information Management, 51, 101952. https://doi.org/10.*

1016/j.ijinfomgt.2019.05.008

[8] Statista. (2018). Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025 (in Billions). Accessed: Sep. 2018. [Online]. Available: https://www.statista.com/statistics/471264/iotnumber-of-connected-devices-worldwide/

[9] T.-T. Kuo, H.-E. Kim and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications", J. Amer. Med. Inf. Assoc., vol. 24, pp. 1211-1220, 2017.

[10] Chakarverti, M., Sharma, N., & Divivedi, R. R. (2019). Prediction Analysis Techniques of Data Mining: A Review. SSRN Electronic Journal. doi: 10.2139/ssrn.3350303

[11] Nguyen, D.C., Pathirana, P.N., Ding, M., & Seneviratne, A. (2019). Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. IEEE Access, 7, 66792-66806.

[12] A Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ''On blockchain and its integration with IoT.
Challenges and opportunities,'' Future Gener. Comput. Syst., vol. 8, pp. 173–190, Nov. 2018

[13] I Eyal, ''Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities,'' Computer, vol. 50, no. 9, pp. 38–49, 2017.

[14] Varshney, T., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Architectural Model of Security Threats & their Countermeasures in IoT. 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). doi: 10.1109/icccis48478.2019.8974544

[15] U. Trust IoT Alliance. (2018). Trusted IoT Alliance. Accessed: Oct. 10, 2018. [Online]. Available: https://www.trusted-iot.org/

[16] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, ''A blockchain-based infrastructure for reliable and cost-effective IoTaided smart grids,'' IET, London, U.K., Tech. Rep. CP740, 2018.

[17] G. Prisco. (2016). Slock. it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy. Bitcoin Magazine. Accessed: May 20, 2016. [Online]. Available: https:// bitcoinmagazine.com/articles/sloc-itto-introduce-smart-locs-lined-tosmart-ethereum- contractsdecentralizethe-sharing-economy-1446746719

[18] A Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, ''LSB: A lightweight scalable blockchain for IoT security and privacy,'' 2017, arXiv:1712.02969. [Online]. Available: https://arxiv.org/abs/1712.02969

[19] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, ''Blockchain with Internet of Things: Benefits, challenges, and future directions,'' Int. J. Intell. Syst. Appl., vol. 10, no. 6, pp. 40–48, 2018

[20] (2018). Chain of Things. Accessed: Sep. 2018. [Online]. Available: https://www.blockchainofthings.com/

[21] P. Ghuli, U. P. Kumar, and R. Shettar, ''A review on blockchain application for decentralized decision of ownership of iot devices,'' Adv. Comput. Sci. Technol., vol. 10, no. 8, pp. 2449–2456, 2017.

[22] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, ''Semantic blockchain to improve scalability in the Internet of Things,'' Open J. Internet Things, vol. 3, no. 1, pp. 46–61, 2017.

[23] L. Zhou, L. Wang, Y. Sun, and P. Lv, ''Beekeeper: A blockchain-based IoT system with secure storage and homomorphic computation,'' IEEE Access, vol. 6, pp. 43472–43488, 2018.

[24] T. McConaghy, A. Marques, Rodolphe, D. De Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare, and A. Granzotto, ''BigChainDB: A scalable blockchain database,'' BigChainDB, ascribe GmbH, Berlin, Germany, White Paper 1.0, 2016.

[25] *H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, ''Towards blockchain-based auditable storage and sharing of iot data,'' in Proc. Cloud Comput. Secur. Workshop, 2017, pp. 45–50.*

[26] *Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong, ''A blockchain-based storage system for data analytics in the Internet of Things,'' in New Advances in the Internet of Things. Zürich, Switzerland: Springer, 2018, pp. 119–138*

[27] *M. A. Khan and K. Salah, ''IoT security: Review, blockchain solutions, and open challenges,'' Future Gener. Comput. Syst., vol. 82, pp. 395–411, May 2018.*

[28] *X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ''A survey on the security of blockchain systems,'' Future Gener. Comput. Syst., vol. 2017, pp. 1–13, Aug. 2017.*

[29] *M. Banerjee, J. Lee, and K.-K. R. Choo, ''A blockchain future for Internet of Things security: A position paper,'' Digit. Commun. Netw., vol. 4, no. 3, pp. 149–160, 2018.*

[30] *E. F. Jesus, V. R. Chicarino, C. V. 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. Netw., vol. 2018, no. 1, pp. 1-27, 2018.*

[31] *A Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, ''Towards better availability and accountability for IoT updates by means of a blockchain,'' in Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW), Apr. 2017, pp. 50–58.*

[32] *S. Underwood, ''Blockchain beyond Bitcoin,'' Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.*

[33] *Tiwari, R., Sharma, N., Kaushik, I., Tiwari, A., & Bhushan, B. (2019). Evolution of IoT & Data Analytics using Deep Learning. 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). doi: 10.1109/icccis48478.2019.8974481*

[34] *H. Subramanian, "Decentralized blockchain-based electronic marketplaces", Commun. ACM, vol. 61, no. 1, pp. 78-84, 2017.*