IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

Integration of Blockchain and IoT (B-IoT): Architecture, Solutions, & Future Research Direction

To cite this article: Vikash Kumar Aggarwal *et al* 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1022** 012103

Integration of Blockchain and IoT (B-IoT): Architecture, Solutions, & Future Research Direction

Vikash Kumar Aggarwal[1], Nikhil Sharma[2], Ila Kaushik[3], Bharat Bhushan[4], Himanshu[5]
[1]RTC Institute of Technology, Ranchi, Jharkhand, India
[2]Ambedkar Institute of Advanced Communication Technologies & Research, Delhi, India
[3]Krishna Institute of Engineering & Technology, Ghaziabad, India
[4]School of Engineering and Technology (SET), Sharda University, India
[5]HMR ITM, Delhi, India
E-mail: vikashhagarwal@yahoo.com

Abstract. Internet of Things (IoT) plays a very important role in every field. With increase in its features it is almost used in every sector. As it is used everywhere so key elements of security are very much critical components which are to be preserved. For formulating these concepts, a new technology called blockchain can be used. In order to have secure transaction between various items, this technology is tremendously used without involving any third party. In this paper, we present introductory part of IoT enabled with blockchain, their key features, architecture layout, characteristic features of both the technologies, their futuristic solutions for different real-world problems, different communicational models etc. Both the technologies possess a number of characteristic features in every field but certain limitations too exist which gives futuristic direction for research.

Keywords: Blockchain, IoT, Security, B-IoT Communications Models, Privacy.

1. Introduction

The IoT is an emerging well-known technology whose aim is to connect various types of devices to the internet. The smooth convergence of Radio Frequency Identification, wireless communication and sensors helps in the evolution of IoT Devices. Using the smart features along with IoT services platforms gets embedded for providing smart services, using controllers and electromechanical system to establish integration between cyberspace and physical world. There are different types of IoT protocols such as MQTT (Message Queuing Telemetry Transport), Constrained Application Protocol (Co-AP), Bluetooth Low Energy. Due to heterogeneity of the IoT standards, protocol standards and IoT devices several problems get raised such as flexibility, lack of interoperability and scalability. In IoT systems designs, various architectural pattern gets followed such as microservices architecture and services-oriented architectures (SOA) which are a part of services-oriented solutions. In these solutions, using the communication protocol, the IoT devices provided service to other devices. The service is referred as an availability of business functionality through a service contract. A service contracts includes documentations, service policies, QoS, and a service interface for monitoring and ensuring the QoS and the performance of IoT transactions. The methods used for interoperability, integrations, and enabling seamless services composition among IoT platforms and applications which works on different devices over heterogeneous networking technologies is called service managements

[1]. The architecture of emerging Internet of Things (IOT) technology is largely adopting by the industries which results in opening up of new income streams for various industries. In the past several years, the usage of IoT solutions in industrial sector has grown rapidly. Cryptocurrency leads to formation of Blockchain which is considered to be as most encouraging technology. The data of regular transactions which is done by large number of users and devices is stored and track by decentralized applications (DApps). From cryptocurrency DApps arises [2]. The IoT can comprehend various networks of communication where the devices could interact with each other through internet. They are commonly known as “entities” or “things” and as delineated in Fig1, they have particular characteristics that are examined underneath.

- ***Identification***- All IoT devices require to have identification like sixth version of Internet Protocol (IPv6) address to share or exchange information with other objects.
- ***Sensing***- To collect information, the sensing methods are used to sense physical environment.
- ***Communication***- It means linkage methods and are exploit for communicating the objects.
- ***Computation***- These methods are adopted to gather the data that is obtained by objects.
- ***Services***- It refers to those methods that are given by objects in relation with information to the users that is received from the physical environment.
- ***Semantics***- It means objects have the power to use the correct information from environment.

Examples of IoT devices include beagle board, RFID (Radio Frequency Identification) tags, CubieBoard, Raspberry Pi, Beagle Board and Arduino [3]. Microcontrollers are a part of development boards, which have Random Access Memory, Read only memory, a processor along with various analog and digital input/output pins. Various sensors are usually connected (hardwired) to MCU processing, receptive trigger and transfer to more system. Some of the sensors include potentiometers, accelerometer, temperature, vibration sensor, proximity sensors, moisture sensor and air quality sensor. A real-time operating is required to process the information, allocate the memory and other utility services supporting communication. RTOS is selected on the basis of performance, functional need and security of the product. WSN generally known as wireless sensors network is among the top supporting technique for IoT currently [68,69]. Designing and setting up security is an extremely significant hurdle in WSN mostly caused by restricted availability of resources at every sensor. Alongside standard difficulties faced while designing security in WSN as well as IoT, many other uncommon features of IoT and WSN shows that security cases and situations in IoT are much more severe and complex than in WSN, reason being their non-similar features and uncommon targeted applications and systems. Firstly, WSNs are most commonly deployed in application made for collecting raw data for example environmental surveillance and inspection systems. All the data is mainly gathered and then stored by sensors and then sent to sinks through dependable multiloop routing protocols. Hence most of the communication is unidirectional, even though the reverse direction is also deployed for disseminating control signals and commands that in turn are used for controlling sensors. Secondly, sensors in Wireless sensor network as well as the end term system in IoT face the problem of limited provision of resources, although sensors might have more problems with power constraints [4]. Furthermore, a WSN is generally aloof from other WSNs and are generally made for a specific application. Opposite to this, IoT aims to join various domain specific and self-operating mechanisms. In the end, comparing general IoT systems like smart grid or intelligent residence projects with general WSN application like industrial surveillance, large data is gathered in IoT applications as compared to WSN. Depending upon all these facts, we can deduce that security demands of IoT is high and it’s more complex to structure a proper security solution for it than for WSN [5].

The later sections of the paper standardized as follows: Section 2 illustrated IoT architecture, Section 3 describes the Blockchain as a Solution for IoT, Section 4 explain Integration of Blockchain and IoT, Section 5 shows Future research directions followed by Conclusion in Section 6.

2. IoT- Architectural View

IoT doesn't have a standard architecture but is divided into communication layers similar to conventional I.T. networks. Various analysis efforts have presented their own models containing 3 layers, 4 layers or the 5-layers. A four layered architecture of IoT includes business layer, support layer, communication layer and perception layer. The perception layer consists of technical component like sensors and actuators to gain knowledge about the Physical environment [6]. The function of Communication layer is to provide dependable transfer of information between different layers. This layer includes 6 sublayers namely application, session, transport, network, MAC, Physical Layer. Support layer intensifies the working of rest of the layers by proving computing services and storage facility. The fog/edge and cloud computing are the principle technologies of support layer. The software application that are developed on the intel of industry description and user requirements are incorporated in business layer [7].

- IoT is a network which connects an enormous number of heterogenous and large-scale end terminal gadgets to each other. A very big amount of information bits is gathered and conveyed in IoT. As per the analysed information that was collected, IoT mainly aims to construct a self-regulated, automated and exceptionally smart world. IoT applications basically works at the peak of three layers i.e., the things layer, the cloud layer, and the edge layer. Every level has a perfect potential to collect, process and then analyse the data on its own. Bi commute that is both way communication is mostly possible, in spite of the fact most of the data starts travelling in things layer and end on the layer of cloud via going through edge layer than otherwise.
- Things layer accommodate a large amount of heterogenous stuff that includes actuators and sensors. End terminal gadgets are made by integrating physical and cyber parts together; physical consisting items that stretch out into real physical world whereas cyber consist of ways to establish connectivity and storage. The stuff may vary a lot in specifications like computation, power supply and reposting. As an ex-ample to support that, smart meters are capable to carry out complicated computations whereas smart bulbs are capable to carrying out only a little amount of simple computations. To conclude, mostly all items are resource-constrained and energy limited that makes them not very appropriate for running heavy tasks.
- Cloud layer is a strong layer and it have a lot of assets accessible for supporting major and complicated computing tasks like extracting information from a big storage of data and performing difficult and complex computations on it, for say distributed intrusion detection. Edge layer which is also known as gateway or fog layer was put forward with the aim of filling gaps within things-layer which lacks in resources as well as cloud layer which is rich in resources. Edge layer is one of the most important layers of the whole architectural layout. Mostly the edge devices are joined with physical things directly or sometimes they are just several hops away. In comparison with things layer, devices mostly have access to a lot number of resources just like big storage spaces, regular power supply and high computing power. It concludes every layer of IoT architecture has certain specifications that makes them irreplaceable. It's very important to organise them in a way that they can work collaboratively in building whole new smart and efficient IoT system.

3. Blockchain as a Solution for IoT

IoT brings the revolution in today world because of its major contribution in various fields such as industries, healthcare, asset tracking, agriculture, telemetry, etc. The IoT gadgets are used to share data between gadgets. According to a survey [8], more than 20 billion IoT gadgets and smart phones are used nowadays. It supports accessibility and heterogeneity as multiple devices are connected with each other and share essential information [9]. These properties of IoT offers various problems and challenges related to trust, security, authenticity and privacy. The sensitive information belongs to various sectors like economics, military communication, and healthcare are affected by these challenges [10]. These problems can be resolved by the well-known technology known as blockchain because in this technology the various transactions related to confidential information will takes place between multiple participants [11]. It offers various intrinsic characteristics such as integrity, authentication, privacy and fraud protection which can help in IoT to resolve the demands of trust, privacy and security [12]. The IoT issues related to reliability and privacy can be solve by blockchain as this technology can trace billions of gadgets at a time, and can also operates communication and transactions between multiple participants [13]. The single point of failure issue can be eradicated by this technology because of its distributed nature and make the IoT system more versatile and irrepressible. The man in the middle attack cannot be performed on blockchain technology because it ensures data integrity of shared ledger which provides distributed location and to avoid wiretapping, multiple transmission channels are employed. All these characteristics of blockchain make it popular and secure technology. It also validated its role in financial and banking sector by providing cryptocurrencies platforms like Ethereum, Bitcoin etc. Therefore, without involving any third parties, the payment services between Peer to Peer and the transmission between multiple untrusted users can be possible. Many IoT organizations approved blockchain technology because of reliable, autonomous, authentic and distributed functionality which are beneficial IoT system. All the unchanging activities records related to smart devices and transmission will be managed by this technology. Without centralized access, these properties can permit independent use of smart devices. Due to all these features nothing can be impossible to implement in IoT scenarios. The role of blockchain into IoT is not a new idea as most of the drawbacks of the IoT technologies are reduced using this technology [14]. The limitations of IoT are high power consumption, large storage requirement, security, high computation etc. which makes it necessary to execute the fusion of blockchain technology into IoT (BIoT). In 2016, at Berkley [15], a working group of IoT protocol and Blockchain worked together to find an alliance called Trusted IoT Alliance, an association of 17 organizations whose objective is to validate flexibility, trust, security, reliability, privacy and heterogeneity by making use of blockchain technology into IoT framework in the decentralized network. In 2015, open source cooperative project was started called the Linux Foundation’s Hyperledger Project with 61 members. Many other projects are working by employing blockchain technology in IoT system are LO3ENERGY, IoTeX, Raspnode, EthEmbeded, CoT (Chain of Things).

3.1 Application of BIoT

By integrating blockchain into the IoT technology, the prediction of different application can be possible in various fields, such as it can be used for designing & modelling of network, also in industries (like smart grids, agriculture etc.), supply chain management, & data provenance etc.

3.1.1 Energy sector

In this sector, the executions of blockchain technology shows favourable influence by removing intercessors, & reducing cost. In a scattering manner without having a system which acts as central point, transactive energy permits the devices as well as the distributed energy resources to trade energy. In smart grids, the infrastructure for enabling a reliable, cost effective & secure transactive solution based on blockchain have been suggested by Lombardi et al. [16].

3.1.2 Smart Contract

In spite of the fact that blockchain delivers many solutions to the IoT issues, it has high computational demands, which needs resource consuming procedure, less time and cost effectiveness. Based on Ethereum, for implementing smart contracts in BIoT, Slock.it as a solution has been presented by G. Prisco [17] through which different gadgets can be connected to the blockchain to enable the Economy of Things.

3.1.3 Privacy

Privacy is another major challenge in the field of IoT as it is a large scale of network which is used to share the data. Therefore, it requires privacy to prevent the data from stealing. Many solutions have been introduced by the researcher to overcome the data privacy concern in IoT domain but that effects the expandability of IoT networks as the solutions are demand on the centralized network. Because of its decentralized structure, without causing the expandability concern, blockchain provides the data privacy techniques which helps to secure data from any intruder. Blockchain is used to store the IoT data and release it for limited period of time to make transactions. Lightweight blockchain solutions have been introduced by many researchers for permitting the privacy in the IoT data. A Lightweight blockchain with algorithm has proposed by Dorri et al [18] for managing throughput, distributed trust and lightweight consensus, which is minimized for IoT. For dispensing information privacy using InterPlanetary File System (IPFS) and blockchain, a network architecture has been proposed by Atlam et al. [19]. Chain of Things is a platform used to integrate IoT hardware and blockchain technology which provides solutions to IoT concerns associated with interoperability, security, privacy [20]. For transactions in IIoT & enterprises, Filament delivers hardware solutions between IoT gadgets using blockchain.

3.1.4 Industrial Internet of Things (IIoT)
IoT brings revolution in every sector like blockchain, healthcare, industry etc. It helps in improving the industry sector in terms of smart manufacturing, asset tracking, reducing latency, and supply chain management. The IIoT gadgets because of these various inherent properties such as security standards, low cost is highly vulnerable to various attacks related to trust, secrecy and security. Blockchain helps in preventing IIoT devices from these attacks by providing immutability and information provenance.

3.1.5 Expandability and decentralizations
As IoT network architecture is a centralized in nature, this make it difficult for the IoT ecosystem to be ascendable. This problem can be resolved by integrating blockchain technology in the IoT. Different solutions have been introduced by the researchers for resolving scalability concerns. For shifting the ownership of IoT gadgets between homogeneous blockchain, an ascendable peer to peer recognition procedure has been proposed by Ghuli et al [21]. In BIoT, for discovery, selection, payments and registration using smart contract, a Service-Oriented Architecture (SOA) has been introduced by Ruta et al [22]. It is based on semantic blockchain of IoT gadgets.

3.1.6 Database and storage
As blockchain technology is distributed in nature, therefore, it is used in developing distributed storage and database facilities. It also ensures security facilities to the users such as access control, authorization, authentication and data integrity. BeeKeeper, an IoT system based on blockchain have been proposed by Zhou et al. [23]. By using IoT gadgets computational energy, this system delivers secure dispensed storage as well as computation without losing data privacy. BigchainDB is a distributed storage software which delivers low latency, high transaction rate, query of structured data and indexing [24]. A dispensed storage solution which is used in managing data audit and for recording IoT information have been proposed by Shafagh et al. [25]. As IoT ecosystem gathered large amount of information, therefore, a solution based on blockchain for data analytics have been introduced by Xu et al. [26], which provides dispensed information storage.

3.1.7 Security
Many security solutions have been proposed by different researchers, most of them are relies on high computational cryptographic algorithms. The existence of blockchain technology brings solution in the IoT sector, as the integrations of blockchain in IoT leads to solve with respect to the security concern. In 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 presented by the Li et al. [28], in which the author has discuss about 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 IoT ecosystem. Jesus et al. [30] has also presented a survey for securing stalker attack and IoT using blockchain. As IoT infrastructure is centralized in nature, it brings multiple challenges. Therefore, most of the work is being done on securing BIoT and hence many solutions to these problems are introduced by the researchers. To maintain the accountability and availability of IoT gadgets and data, Boudguiga et al. [31] investigated that how integrity and confidentiality can be confirmed in BIoT.

3.2 Different communications models of BIoT

In BIoT, the IoT gadgets can be communicated either directly or through a cloud computing, fog computing model or blockchain [32]. The various paradigms of BIoT are explained as follows:

3.2.1 Direct IoT gadgets communication paradigm
In this paradigm, the communication between IoT devices takes place directly without involving blockchain or any other model. This is the fastest model because it works without involving time consuming and high computational algorithms of blockchain. But it doesn't ensure security, reliability, and privacy [33]. Therefore, to enable these security features, the historical details of the IoT devices transaction or communication is stored in the blockchain. This model offers fast transmission between IoT gadgets as it needed low security. Figure 1 shows the Direct IoT gadgets communication paradigm.

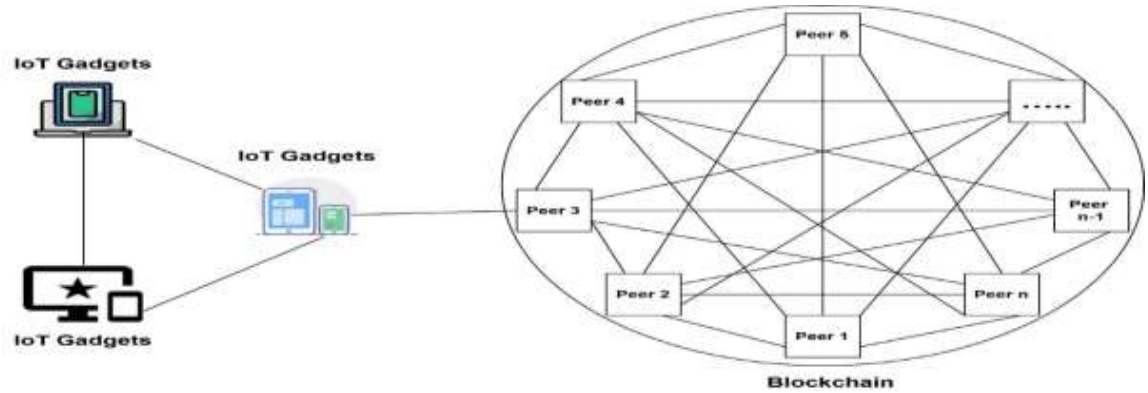

Figure 1: Direct IoT gadgets communication paradigm

3.2.2 Blockchain based communication model for IoT devices
It provides the information reliability, security as well as privacy because all the transaction goes through blockchain in this model. In this the communication between the IoT gadgets take places using blockchain technology where the fixed record is stored of every transaction [34] as shown in Figure 2.

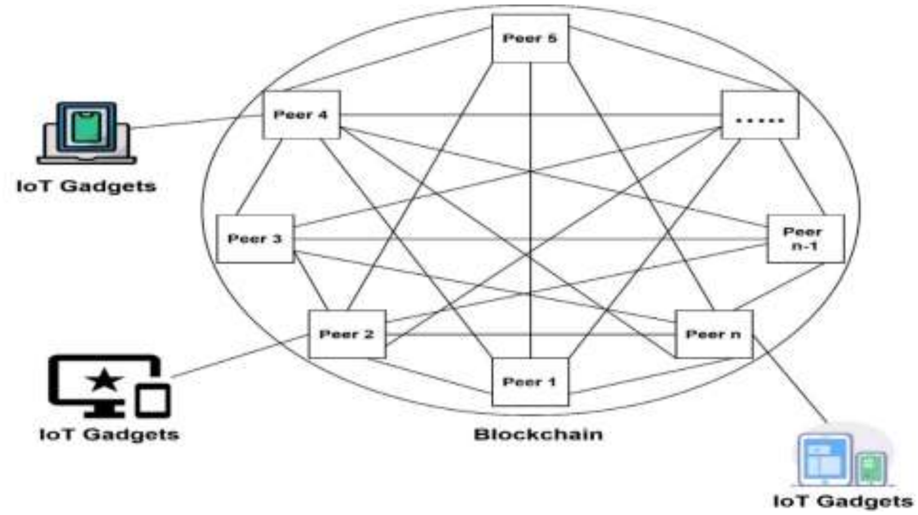

Figure 2: Blockchain based communication model for IoT devices

3.2.3 Fog/cloud-based communication model for IoT devices

Recently, Fog computing brings revolution in the field of IoT by moving 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 reliable communication takes place between the IoT devices as shown in the Figure 3 [36].

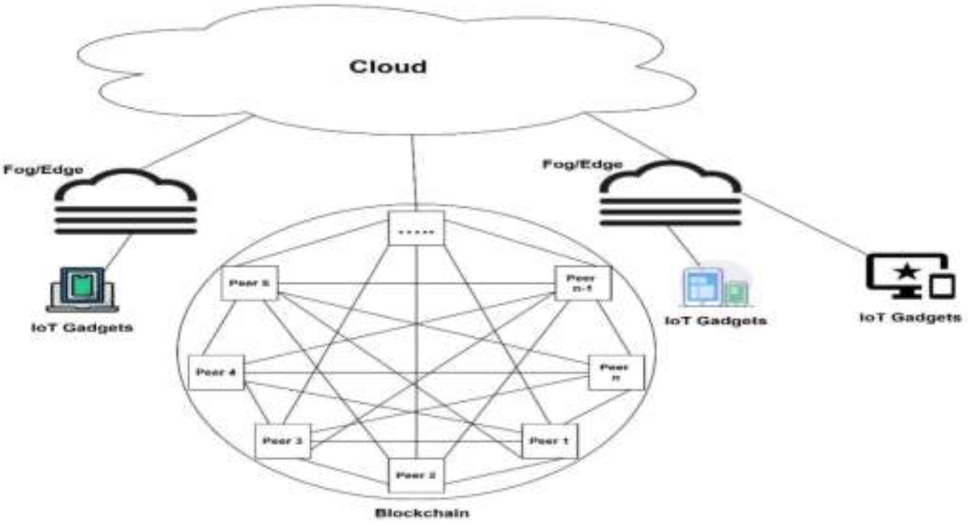

Figure 3: Fog/cloud-based communication model for IoT devices

3.3 Different platforms of Blockchain for Internet of Things

Because of various quality features and properties, different platforms get designed for the IoT networks.

3.3.1 IoT Chain

For IoT gadgets, it is latest platform which employ as decentralized network. It is not available publicly to the participants for the development. It only shows securities, result, other concerns and consensus to the IoT network. It differentiates outcome with SLOCK, IBM-ADEPT, IOTA, IT and various other corresponding projects. It underpins DAG and PBFT as consensus.

3.3.2 IOTA

It is defined as a distributed ledger design which is used to store and executes the transactions between IoT gadgets and machines. It plans to become the excellence method of supervising transactions on the gadgets. It is public permission-less backbone for the IoT devices which permits interoperability between multiple gadgets. The main objective of IOTA is to resolve the performance concern and scalability with bitcoin by replacing its blockchain with Tangle as it is a system of nodes in which new transactions assures the preceding transaction. It employs Directed Acyclic Graph which is especially designed for the Internet of Things ecosystem. The major invention of IOTA is Tangle that is used for the confirmation of transactions. IOTA system assert that the system of nodes is well organized, systematic, efficient and faster than any other prototypical blockchain used in the cryptocurrencies is Tangle i.e. Decentralized Acyclic Graph whose aim is to solve the flexibility and performance concerns of the system. While transaction process, tangle become more flexible, secure and efficient as multiple systems are connected to it. It reduces the efforts, memory and time requirement to validate a transaction as every new transaction get confirmed by its two preceding nodes.

3.3.3 Waltonchain

Like IoTChain & IOTA, it is also designed for the IoT system which works as decentralized network. It consists of software and hardware. In IoT gadgets, RFID is employed as a transmission approach, and the electronic communication is executed on newly planned blockchain architecture. Software comprises of Walton Coin and Walton Chain Protocols. For the evolution of secure IoT gadgets, an open secured and reliable hardware engine offered by the Open IoT Blockchain.

4. Integration of Blockchain and IoT

The idea of ever-expanding IoT device ecosystem in order to convey it towards a decentralized architecture was advanced by the Brody et al [37] so that it maintains its sustainability. According to customer's point of view, to overcome the privacy and trust issues, there is need of "security through transparency" approach. To maintain the present centralized model, manufacturer has to spent huge amount on the maintenance and improvement. Blockchain successfully countered this problem because it is working on a scalable peer-to-peer network replica which is functioning transparently and spreading data securely. In sequence to perceive that how this model is working, let us assume a structure where all IoT devices functions 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 to some proficient number of nodes then the manufacturer's own node cease serving the initial file requirement. Devices which are configured are assumed to share their received binary thereby sanctioning the retrieval of the firmware updates by even those devices that connect the network after the manufacturer has ceased participating. This happens automatically and there is no involvement of any user relations. Moreover, the blockchain network is exchanged via cryptocurrency which allow for the easy exchange of service between devices and also supplies a suitable billing layer. These devices are storing the binary edition in order to comfort infrastructure price or to make some profit and they deducted some amount for serving it. Some examples of it are as follows: Filecoin [38] facilitates devices to grant their disk space on rent and EtherAPIs [39] assists to monetize API calls. With the help of microtransactions every device accepts actual payment for their usage.

After integration of blockchain and IoT, the sharing of services and property also facilitates. Concept of "Slocks" [40] was introduced by the 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 a blockchain is registered by the solar panels and neighbourhood get benefited from it after purchasing it.

4.1Divers challenges of BIoT applications

IoT ecosystem technologies have to face several challenges like telemetry systems, RFID, and 5G/4G broadband communication [41]. In the case of evaluative applications these challenges arise further concerns and we have to look into that challenges. Integration of blockchain to this conduct forth supplementary technical and operational requirements owing to the complexity associated with the BIoT applications. Now, in subsections we will discuss about major factors that affect the development of the BIoT application.

4.1.1 Energy Efficiency

Blockchains consume lots of power because of 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.

4.1.2 Security

Confidentiality, availability, and integrity are the three challenges which have to be fulfilled for a better security in any information systems. For IoT applications data integrity is another major component. Integrity service framework 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.

4.1.3 Privacy

Privacy is the main concern in the IoT environments and IoT applications faces certification problem. 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.

4.1.4 Throughput and latency

Architecture which is similar to the blockchain should be needed for regulating large amount of transactions per unit time at the time of positioning of an IoT. Moreover, this will become challenging factor for such networks such as bitcoin which only support maximum up to seven transactions per second.

5. Future research directions

After so many advantages, blockchain faces several challenges in its adoption in IoT. There are three main categories in which these challenges are broadly classified: privacy preservation, utilization, and scalability. In below section, we will discuss about challenges and future research that how blockchain will be integrated in IoT.

5.1 Scalability issues in blockchain

There are so many researches presented which proves that blockchain is a scalable and there are still so many researches going on [42]. When the appliances demand for the high networking and high performance then this scalability is still an open issue for the blockchain.

5.2 Privacy concerns related to permission-less blockchains

Transaction records of bitcoin are available to the network contributors. 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 help of tiered architecture privacy of the blockchain is maintained.

5.3 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 temporary identifications, anonymity enforces data security, encryption and decisions has to be make according to moral factors like why and how to use the generated big IoT data. 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.

5.4 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. There are several other challenges besides technical challenges, like decentralized ownership and international jurisdiction are major issues for unbolting the capable BIoT values.

6. Conclusion

IoT plays a very important role in every field due to its advancement in latest used technologies. 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.

[35] Goyal, S., Sharma, N., Kaushik, I., Bhushan, B., & Kumar, A. (2020). Precedence & Issues of IoT based on Edge Computing. 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT). doi:10.1109/csnt48778.2020.9115789

[36] C. Esposito, A. De Santis, G. Tortora, H. Chang and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?", IEEE Cloud Comput., vol. 5, no. 1, pp. 31-37, Jan./Feb. 2018.

[37] Brody, P., & Pureswaran, V. (2014). Device democracy: Saving the future of the Internet of Things. IBM Institute for Business Value, technical report, September 2014. [Online]. http:// www935.ibm.com/services/us/gbs/thoughtleadership/internetof things/.

[38] EtherAPIs: Decentralized, Anonymous, Trustless APIs, accessed on March 15, 2019. [Online]. https://etherapis.io/.

[39] Filecoin—A cryptocurrency operated file storage network [Online]. http://filecoin.io/. Accessed on March 15, 2019.

[40] Slock.it—Blockchain? IoT [Online]. https://slock.it/faq.md. Accessed on March 15, 2019.

[41] Ellis, R. D., Flaherty-Walia, K. E., Collins, A. B., Bickford, J. W., Boucek, R., Burnsed, S. L., et al. (2019). Acoustic telemetry array evolution: From species- and project-specific designs to large-scale, multispecies, cooperative networks. Fisheries Research, 209, 186–195. https://doi.org/10.1016/j.fishres.2018. 09.015.

[42] Zhong, L., Wu, Q., Xie, J., Guan, Z., & Qin, B. (2019). A secure large-scale instant payment system based on blockchain. Computers & Security, 84, 349–364. https://doi.org/10.1016/j.cose. 2019.04.007