Blockchain Internet of Things (BIoT), Architecture, Applications and Challenges: A Survey

S.Muthulakshmi

Research Scholar,
Computer Science and Engineering,
Noorul Islam Centre for Higher Education,
Kumaracoil, Thuckalay, India.

Dr.R.Chitra

Associate Professor,
Computer Science and Engineering,
Noorul Islam Centre for Higher Education,
Kumaracoil, Thuckalay, India.

Abstract: Internet of things is transforming the industries into smart industries and trending in recent years. Even though IoT has advantages, it has issues also. Some issues are privacy, security, interoperability etc. Blockchain technology is invented to overcome these issues. The investigation is done in this article about the integration of IoT and blockchain. It is named as BIoT. This article explains about the basic concepts of blcokchain in depth. The working flow of blockchain is discussed in the next chapter. Then the integration of IoT and blockchain is over viewed. There are many applications under BIoT such as smart manufacturing, smart grid, and health care applications etc which are discussed in further chapter. Then the open research challenges of Blockchain internet of things applications are discussed finally. The growth rate of IoT and BIoT applications and projects are explained through graphs.

Keywords: *Blockchain, BIoT, Architecture, Applications, Challenges.*

1. Introduction

Blockchain is a list of records, called as blocks which are linked by using cryptography [1] [2]. Each block contains the hash of the previous block, timestamp and transaction data [2]. Blockchain is the decentralized system. Blockchain works as an immutable ledger, which permits transactions to be happened in a decentralized fashion [3]. Blockchain is considered as a public ledger and all transactions are stored as a list of blocks. New blocks will be added and grows as a chain. To improve user security and ledger consistency the asymmetric cryptography and distributed consensus algorithms are used. In blockchain the payment is finished without the help of bank or third party. Therefore various financial services are preferring blockchain [4] [5]. Also it is used in smart contracts [6], public services [7], Internet of Things [8], reputation systems [9] and security services [10]. Transactions cannot be altered once it is added to the chain. Due to this reason all businesses who want high reliability are preferring blockchain.

Blockchain contains two elements [11]. They are as follows.

1. Transactions - Transactions are the activity generated by the users.
2. Blocks – blocks are used to record the transactions which are in correct sequence and not tampered with. When the new transaction is added, the blocks record the timestamp.
   The formation structure of blockchain is shown in the figure 1.

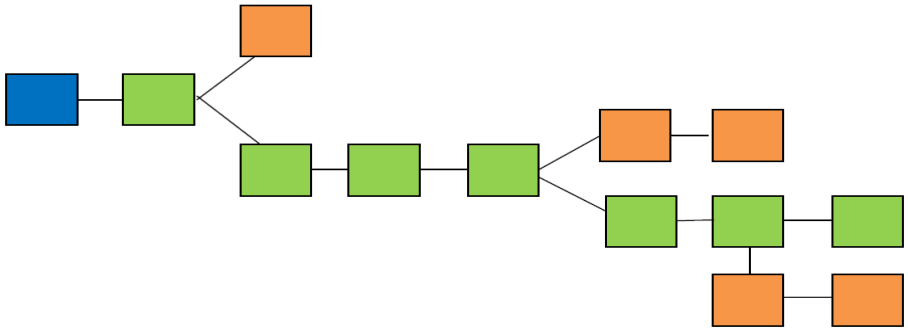

Fig 1: Blockchain Formation

Blue- Genesis Block

Green- Main Chain

Orange- Orphan Blocks

The main chain painted in red colour consists of the longest series of blocks from the genesis block which is in blue colour to the current block. Orphan block which is marked in yellow colour exist outside of the main chain.

Architecture of Blockchain

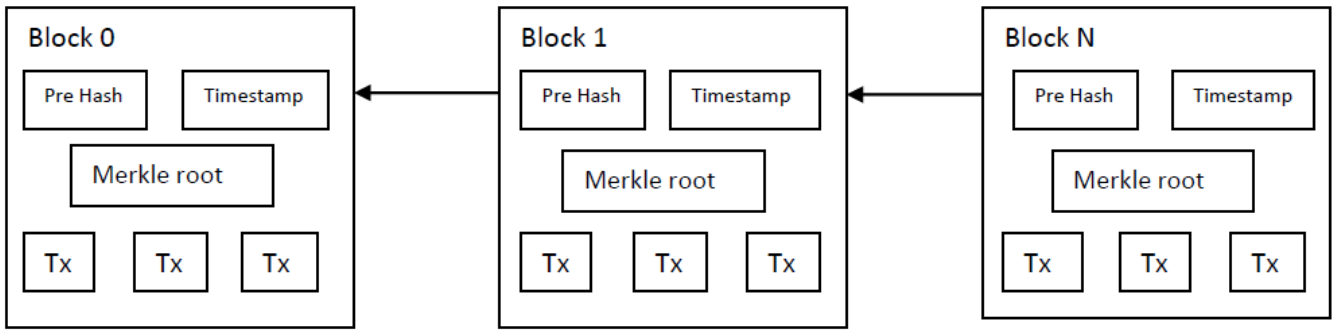

Fig 2: Basic Structure of Blockchain

The figure 2 shows the basic structure of blockchain. Each block contains the hash value, a timestamp and the transaction data. Header of the block is used to convey the information about the block such as the length of the block [12]. The header stores the value of the previous block. That is the hash value of block 1 will depend on the hash value of block 0. Due to this hash keys, it is very difficult to tamper with the blocks for the attackers [13].

Data integrity in Blockchain

There are cryptographic techniques to ensure data integrity in blockchain. There are 2 mechanisms.

1. Ordered linked list structure of blocks

   In this ordered linked list hash value of the previous block must be included by the newly added block. So that if something goes wrong in the previous blocks that will be invalidated the subsequent blocks [14].

2. Merkle Tree

To enhance the IoT security the merkle tree is added to the blockchain. By inserting the merkle tree, the number of blocks being added to the chain is reduced. The figure 3 shows the structure of the merkle tree. Merkle tree is a binary tree, in which all nodes consist of two child nodes except the leaf nodes. The leaf nodes consist of the transaction data and the root nodes consist of the hash values of the transactions [15]. To generate a single root hash, multiple transactions can be combined based on the size of the tree. The security of the data is enlarged due to multiple levels of hashing [16]. IoT devices include a lot of small communications. So that merkle tree along with blockchain can be the best solution to IoT security issues [17].

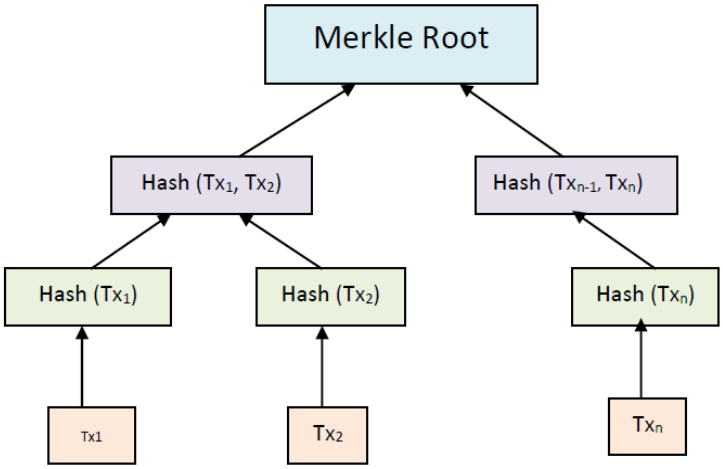

Fig 3: Structure of Merkle tree

Consensus Algorithm

The major advantage of blockchain is validating the trust of the block in decentralized environment without the help of third party [14]. It is difficult to achieve trustfulness in distributed environment. There are two categories of consensus algorithms. 1) Probabilistic consensus algorithms 2) Deterministic consensus algorithms. In Probabilistic consensus algorithm the validated block will be saved into the chain first and then search for consensus of all the nodes. Examples of this type of consensus algorithm are proof of work, proof of stack and delegated proof of stack. In deterministic consensus algorithm, the consent will be found first and then the validated block will be saved into the chain. Example is partial byzantine fault tolerance [18].

How does blockchain work?

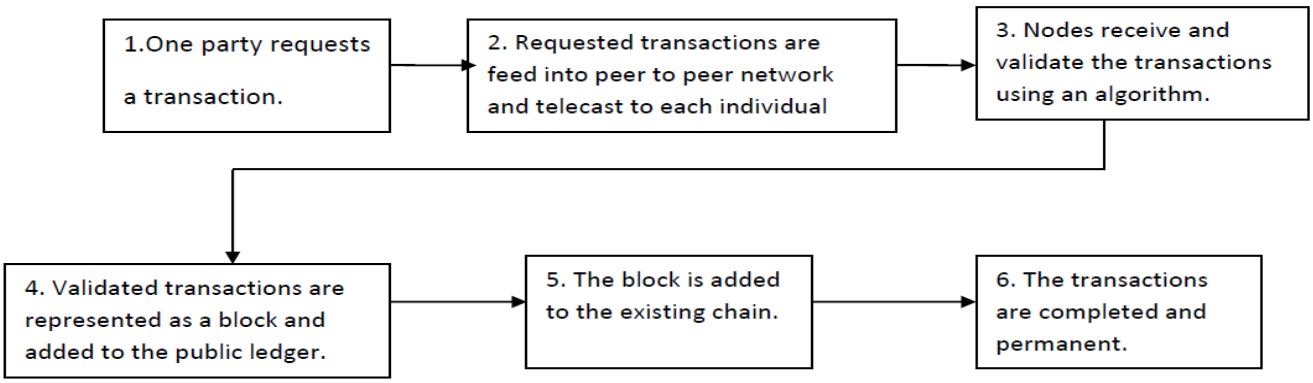

Fig 4: Working flow of Blockchain

The working flow of Blockchain is shown in the figure 4. The flow starts with the transaction. Whenever the user is initiating the transaction that time the new block is generated that represents the

transaction. It is shown in the second step. As soon as the block is created, it is sent to every node in the network as shown in step three. Once every node receives the data, they will validate the transaction. After validating the transaction the nodes will approve that transaction and the new block is added to the existing block. For validating the transaction all the nodes will get reward for the proof of work. Once the block is added, the transaction is completed. This is the flow how the blockchain works.

Types of Blockchain

There are three major types of blockchain. They are private blockchain and public blockchain, Consortium blockchain.

Publice Blockchain

Public blockchain is also called as permissionless blockchain. It is an open source. In public blockchain there is no need of any permission to become a part of the blockchain network. Anyone can join and leave the network at any time. The transactions take place in this blockchain is transparent to all participants in that chain. Bitcion is the best example of this type of blockchain.

Example: Bitcoin, Ethereum

Private Blockchain

The other type of blockchain is private blockchain. It is also known as permissioned blockchain. As said in the first type, it is not easy to join in this network. There are certain rules to join in this blockchain network. Only the authorised users who come under this rules can participate in this network. The transactions are private and visible to only the authorized users [19].

Example: Multichain, Blockstack

Consortium Blockchain

Consortium blockchain is controlled by a group rather than a single entity. It has all advantages of private blockchain and considered as a sub category of private blockchain and it is not a separate type of chain. It is more efficient. It will be able to include any one from banks to government into the supply chain.

Example: Ripple, Hyper ledger

The Comparison between three types of blockchain is shown in table 1. [20]

Table 1: Types of Blockchain – Comparison

Key Concept	**Public Blockchain**	**Private Blockchain**	**Consortium Blockchain**
Efficiency	Low	High	High
Centralized	No	Yes	Partial
Immutability	Impossible to tamper	Possible to tamper	Possible to tamper
Consensus Determination	All Miners	One organisation	Selected set of nodes
Read Permission	Public	Public or restricted	Public or restricted
Consensus Process	Permissionless	Permissioned	Permissioned

Key Concepts of Blockchain

There are major advantages in blockchain which is the pillars of blockchain that helped it to become an upcoming most wanted technology worldwide [21]. They are,

1. Decentralization
2. Immutability
3. Transparency
4. Non-repudiation
5. Persistency

Decentralization

In centralized system, there is a single authority that can approve the transaction. So every time the user should contact the central authorised person to approve the transaction. As it is centralized all the data is stored in one place. So it is very easy to hack the database. Also if one part of the network is corrupted, then the entire network will be collapsed. To overcome this major problem the decentralized concept is introduced in blockchain. In a decentralized network if one user wants to interact with his friend, it is done directly without the help of the third party. As all blocks are having the copy of transactions, it is very easy to retrieve the data during the network crash. Thus the service cost and single point of failure is reduced [22] [23].

Immutability

In blockchain, if the third party entered into it, it cannot tamper with. This property is called as immutability. This immutability is achieved in blockchian through cryptographic hash function. In general, taking an input string of any length and giving a fixed length string as an output is called as hashing. For an instant imagine, if the hacker attacks block 1 and trying to change the data. If the data changes, then it will be changed in all blocks because every block's hash value depends on the previous block's hash value. Therefore the entire chain will be changed. This is impossible in blockchain due to the cryptographic hash function. In Blockchain time stamped data is used. In that each and every link corresponds to the inverse hash point of previous block. Small piece of the change can be easily identified in this approach [24].So that immutability became a pillar of blockchain. This is how the blockchain achieves immutability.

Transparency

Some people think that, because of the transparency property of blockchian the personal identity of the user will be seen by all in the network. But actually it is not. The user's identity will be hidden by cryptography. So only transaction details will be visible to others, not about who sent. Due to this property the third party cannot enter into the chain without proper authorization. In public blockchain systems, each user has the equal priority to access and interact with the block chain network. Each and every new transaction is saved in the network and it can be further used by anyone in the network [25].

Non-repudiation

As we know private key is used to authenticate the transaction. After it authenticates others can access and verify the transaction by using public key. Even the transaction initiator cannot alter the authenticated transaction [14].

Persistency

All transactions take place in the network will escalate throughout the network. These transactions should be assured and recorded in blocks present in the whole network. So that it is impossible to tamper the transactions. Also every broadcasted block and transactions will be validated and verified by other nodes. Therefore it is easy to detect the forgery [20].

2.Blockchain in IoT

The basic concept of ToT is, the interconnection of smart devices to collect data and produce the response to the user [26]. Blockchain can be connected to IoT to remove all security problems in IoT. The characteristics of blockchain such as traceability, transparency, reliability are mainly used to overcome the security issues in IoT. By integrating IoT and blockchain more research issues are solved and still unsolved issues [27] [28]. Blockchain can be used in many areas of IoT [29]. Such areas are sensing [30] [31], data storage [32][33], identity management [34], time stamping services [35], smart living applications [36], wearable [37], intelligent transportation systems [38], supply chain management [39], mobile crowd sensing [40] etc. Research is going on to manage IoT devices through blockchain [41]. There are many reasons for using blockchain in IoT. Some of them are mentioned in the table 2 [42] below.

Table 2: IoT and blockchain: Comparison

IoT	Blockchain
Centralized	Decentralized
Limited bandwidth	High bandwidth
Security is the challenge	Security issues are solved
Restricted Resources	Resource consuming
Low latency	Block mining is time consuming

Due to the above reasons mentioned under IoT, blockchain is introduced and developed in recent years.

Blockchain Internet of Things (BIoT) Architecture

The architecture of blockchain internet of things (BIoT) is shown in figure 5 [14]. The architecture contains a blockchain composite layer which works as a middleware between IoT and industrial applications. There are two major advantages in this architecture. 1) It provides conceptualization from the lower layers of IoT. 2) Also provides blockchain based services to the users. It hides the heterogeneity of perception and communication layers.

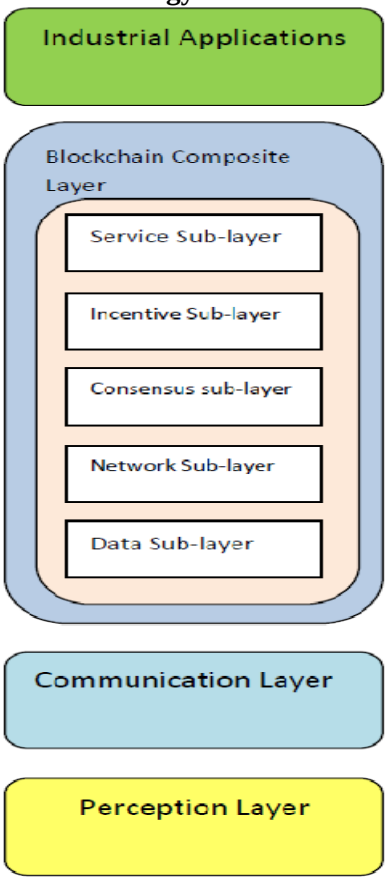

Fig 5: BIoT Architecture[14]

Blockchain composite layers consist of five sub layers.

1. Data sub layer
   Data sub layer is used to gather the IoT data from the lower layers and covers the encrypted data with digital signature through asymmetric cryptographic algorithms and hash functions.
2. Network sub layer
   Only one node broadcasts the block of transactions to its connected peers. The peers will verify the transactions after receiving it. The block will be impregnate to other nodes via network if it is failed.
3. Consensus sub layer
   Consensus sub layer is used to check the trustfulness of the block. There are many consensus algorithms used such as proof of work, proof of stack etc.
4. Incentive sub layer
   Incentive sub layer involves in following activities. a) Issuing digital currency b) Distribution of digital currency c) Reward mechanism design d) Handling transaction cost e) Designing monetary policy of digital currency.
5. Service sub layer
   Service sub layer is used to provide blockchain based services to the users.

3. Applications of BIoT

There are many BIoT based applications. Few of them are shown in figure 6 and explained below.

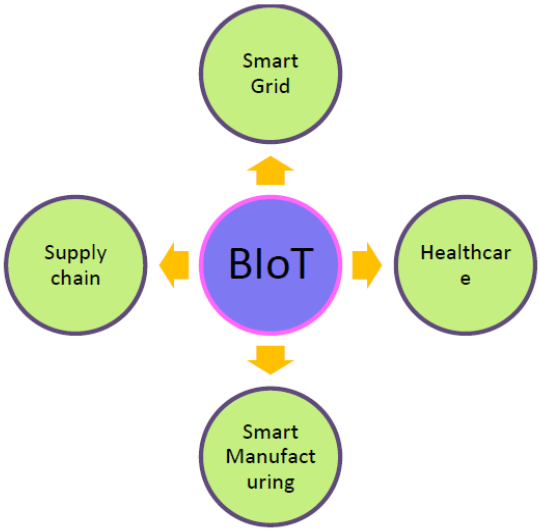

Fig 6: BIoT Applications

Smart Grid

Smart Grid is the application of smart metering. It is used to measure and monitor the electricity consumption [43]. Distributed renewable energy resources are used to reform the responsibility of energy buyers from pure customers to prosumers. The prosumers provoke energy from renewable energy resources and consume energy [44]. They can sell the extra energy to other consumers. Though it has advantages there is an open issue that it is difficult to provide sealed and safe keeping energy trading between two trading parties. To overcome this issue blockchain technology is used to provide secure energy trading. In [45], the author developed a secure energy trading system which is centred on consortium blockchain. In [46], the author flourished a decentralized energy trading system based on blockchain. In [47], the author introduced a transparent and secure energy demand-side management on smart grid based on blockchain.

Supply chain

Generally one product can contain many parts which are manufactured by different companies. Therefore there is a chance of including low quality parts in supply chain. By integrating blockchain with IoT this can be tackled. While integrating blockchain with IoT, unique id and immutable timestamp will be allotted to every part of the product. Then the identified part will be saved into blockchain which is track able. In [48] the author says that, the owner of the part of the product can be authenticated through blockchain based system. In [49] the researcher says about traceability ontology with the integration of IoT and blockchain based on Ethereum. In [50] the author explained about a use case of a motor insurance. In that smart contracts are used to automate the settlement of claims based on blockchain. The integration of IoT and blockchain will reduce cost and risk in supply chain [51]. In paper [52] the author proposed a blockchain based machine learning platform to secure data sharing.

Healthcare

Healthcare becomes very challenging industry in recent years due to the limited hospital resources. By the recent technologies the burden of the hospital resources are released [53].These IoT based devices will collect the information about the health condition of the patients and transfer the information to the health monitoring centre [3]. IoT devices are used in remote health monitoring and emergency notification systems [62]. Theses health monitoring devices can be used to monitor blood pressure, heart rate etc [63]. These devices can detect the heart rate of the person using heart beat sensors even when the person is at home [64]. IoT health

monitoring system can detect the deadly diseases in early stage itself [65]. IoT is used in stress recognition applications also [66]. That device will report using smart phone sensors. In [67] the author explains about an application which is used to measure the stress level of the college student and that is connected through his smart phone. There is a device called smart mat which is used to count the number of exercise steps done by the person [68]. However, the security and privacy of the healthcare data are in risk. By integrating blockchain with healthcare networks the above issues can be solved. In [54] the author says that the healthcare data stored in cloud server will be protected by blockchain technology. In [55] the researcher developed a blockchain based system to guarantee the private healthcare data management. In [56] the author proposed a solution which is based on blockchain to manage healthcare data and data sharing among hospitals and health related centres. In [57] an attribute based signature scheme in decentralized healthcare blockchain systems is proposed. In [58] the author says about an in-home therapy management framework to provide secrecy and anonymity assurance.

Smart manufacturing

The manufacturing industry is upgraded from automation system to smart system [59]. During every phase of the product development life cycle enormous data is generated. However, there is a difficulty in data aggregation and data analytics. The integration of IoT and blockchain is used to defeat the interoperability issue. In [60] the author proposed an automatic firmware upgrading solution based on smart contract and blockchain. In [61] a decentralized blockchain based automatic production platform was proposed to provide security and privacy. The figure 7 shows the growth rate of blockchain development in various industries.

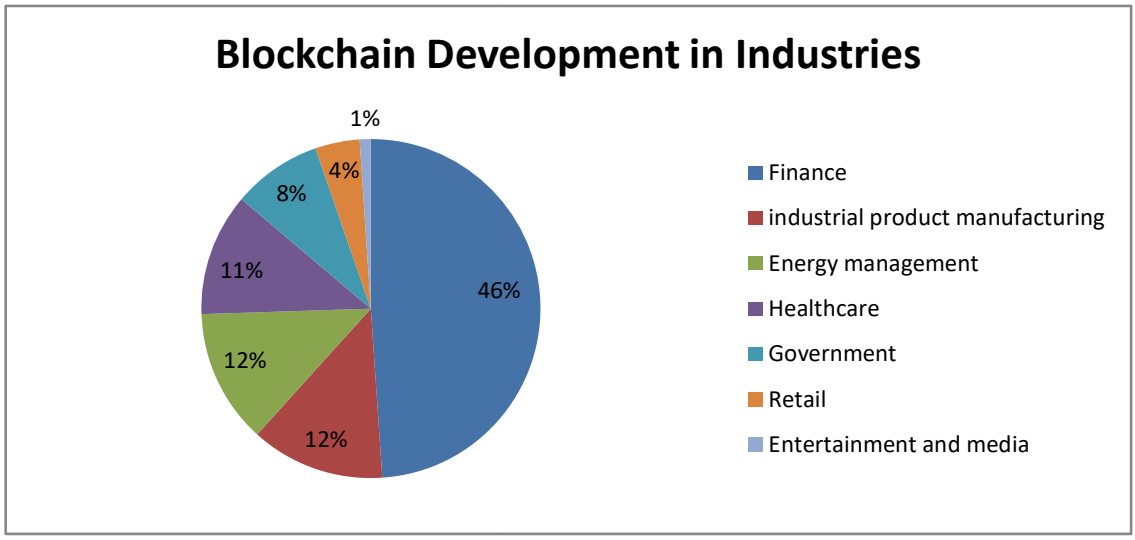

Fig 7: Blockchain Development in Industries

4. Challenges in BIoT

Scalability

The scalability of blockchain is computed by the throughput of the transactions per second in opposition to the number of IoT nodes and the number of concurrent workloads [69] [70]. Most of the blockchain applications have poor throughput. In [71] the author highlighted that bitcoin is able to process only seven transactions per second. The other author says in [72] that bitcion is not suitable for IoT because of the poor scalability.

Security and Privacy

There are certain apparatus in blockchain to conserve the privacy of transaction records which are saved in the chain [14]. In bitcoin the transactions are done by using IP addresses instead of the user ids. This security or protection scheme is not enough to improve privacy. In [73] the author says that the user pseudonyms can be destroyed by studying about the transactions associated with one particular user. Also by loading all the transaction data in blockchain, the privacy leakage may happen at any time [74]. Table 6 shows the possible open issues in blockchain internet of things. In [77], [78] the authors said that since the transaction balances and values are visible to all participants in the chain there is no guarantee for privacy.

Bandwidth

The developers are suggesting software defined networking tools to increase the bandwidth of IoT devices [75]. In [76] the author proposed a distributed IoT network construction, called DistBlockNet. It is very important that the transactions and block volume should be within the bandwidth limit [26]. Table 3 explains the challenges in BIoT.

Table 3: Challenges in Blockchain Internet of Things [26]

Challenges	In BIoT
Scalability	Blockchain can perform only less number of transactions per second
Privacy	The users of blockchain are identified by the hash value or public key. Due to this all transactions will be shared. So privacy leakage may occur.
Throughput	Blockchain internet of things requires a network which is capable to generate a large number of transactions.
Block size	The initial transfer time should be large for the operators to store transactions.
Bandwidth	Transactions and block volume should be within the bandwidth limits of IoT.
Energy efficiency	Energy efficiency is very essential to permit long term node placement.

Conclusion

Internet of things is growing globally in recent years. As all industries are willing to get connected with IoT devices and application, it is very important to provide flaw less devices to them. Everything is changing to IoT nowadays. So researchers are very busy to make IoT little better. To achieve flaw less solutions it is necessary to overcome the present issues in IoT. It is done by integrating blockchain with IoT. Blockchain provides solutions to the issues present in IoT. IoT increases the level comfort of the user. This article is useful to understand about the basic concepts of Blockchain. Architecture and working process of blockchain is also explained. The BIoT architecture is explained in the further chapter. There are many BIoT applications as like as IoT which is explained in this article. However, BIoT has challenges also. The main challenges are scalability, privacy, security, resource impediment which is mention in this article. By improving throughput of the application, the scalability problems can be solved. The research is required in those areas to provide good products to the society.

References

1. Blockchain: The great chain of being sure about things, The economist, (2015).
2. Narayanan, Arvind, Bonneau, Joseph, Felten, Edward, Miller, Andrew, Goldfeder, Steven, Bitcoin and Cryptography technologies: A comprehensive introduction, (2016).
3. Zheng Z., Xie S., Dai H., Chen X., Wang H., An Overview of Blockchain Technology: Architecture, Consensus and Future Trends, IEEE International congress on Big Data, (2017), DOI 10.1109/BigDataCongress.2017.85
4. Peters G W., Panayi E., Chapelle A., Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective, (2015).
5. Foroglou G., Tsilidou L A., Further applications of the blockchain (2015).
6. Kosba A., Miller A., Shi E., Wen Z., Papamanthou C., Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, Proceedings of IEEE Symposium on Security and Privacy, (2016), pp: 839-858.
7. Akins B W., Chapman J L., Gordon M., A whole new world: Income tax considerations of the bitcoin economy, (2013).
8. Zhang Y., Wen J., An IoT electric business model based on the protocol of bitcon, International Conference on Intelligence in next Generation Networks, (2015), pp. 184-191.
9. Sharples M., Domingue J., The blockchain and Kudos: A distributed system for educational record, reputation and reward, European Conference on Technology Enhanced Learning (EC-TEL) (2015), pp.490-496.
10. Noyes C., Bitav: Fast anti-malware by distributed blockchain consensus and feed forward scanning, (2016), arXiv preprint arXiv: 1601.01405.
11. Banafa A., How to secure the internet of things (IoT) with blockchain, (2016), http://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228.
12. Resstuccia F., Kanhere S S., D'oro S., Melodi T., Das K S., Blockchain for the internet of things: Present and Future, IEEE Internet of Things Journal, 1(1)(2018).
13. Orman H., Blockchain: The emperor's new PKI?, IEEE Internet Comput., 22(2)(2018), PP: 23-28.
14. Dai H., Zheng Z., Zhang Y., Blockchain for Internet of Things: A Survey, IEEE Internet of Things Journal, (2019), DOI 10.1109/JIOT.2019.2920987.
15. Koo D., Shin Y., Yun J., Hur J., An online data-oriented authentication based on merkle tree with improved reliability, in proc. IEEE Int. Conf. Web Services (ICWS), (2017), 840-843.
16. Wang J., Li M., He Y., Li H., Xiao K., Wang C., A Blockchain based privacy-preserving incentive mechanism in crowd sensing applications, IEEE Access, 6(2018), 17545-17556.
17. Munoz M C., Moh M., Moh T S., Improving Smart grid security using merkle trees, in proc., IEEE Conf. Commu. Netw. Secu. (2014), 522-523.
18. Miguel C., Barbara L., Partial Byzantine Fault Tolerance, in proceeding of the third symposium on operating systems design and implementation, 99(1999) 173-186.
19. Hassija V., Chamola V., Saxena V., Jain D., Goyal P.,Sikdar B.,A Survey on IoT Security: Application Areas, Security Threats and Solution Architectures, IEEE Access,doi:10.1109/ACCESS.2019.2924045,7(2019),82721-82743.
20. Zheng Z., Xie S., Dai H., Chen X., Wang H., Blockchain challenges and opportunities – A Survey, Int. J. Web and Grid Services, 14(4)(2018),352-375.
21. Rosic A., What is blockchain technology? A Step-by-Step Guide for beginners, (2016), blockgeeks.com/guides/what-is-blockchain-technology/.
22. Conoscenti M., Vetro A., DeMartin J C., Peer to peer for privacy and decentralization in the internet of things, IEEE/ACM International Conference on Software Engineering Companion, ICSE-C (2017), pp. 288–290, IEEE, Buenos Aires, Argentina, (2017).

23. Wood G., Ethereum, A secure decentralisedgeneralised transaction ledger, Ethereum Project Yellow Paper, vol. 151(2014).
24. Crosby M., Pattanayak P., Verma S., Kalyanaraman V., Blockchain technology: Beyond bitcoin, Applied Innovation, 2(2016) pp. 6–10.
25. Pilkington M., Blockchain technology: principles and applications. research handbook on digital transformations, Olleros F. X., Zhegu , Eds., (2016).
26. Alamri M., Jhanjhi N Z., Humayun M., Blockchain for Internet of Things (IoT) Resarch Isuues challenges and future directions: A review, International Journal of Computer Science and Network Security, 19(5)(2019), pp. 244-258.
27. Panarello A., Tapas N., Merlino G., Longo F., Puliafito A., Blockchain and iot integration: A systematic survey, 18(8)(2018), pp. 25-75.
28. Wüst K., Gervais A., Do you need a Blockchain?, Crypto Valley Conference on Blockchain Technology (CVCBT) , pp. 45-54.
29. Conoscenti, M., Vetrò, A., De Martin, J. C., Blockchain for the Internet of Things: A systematic literature review, in Proceedings of the IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 Nov. - 2 Dec. 2016.
30. Wörner D., vonBomhard T., When your sensor earns money: exchanging data for cash with Bitcoin, in Proceedings of the Ubi Comp Adjunct, Seattle, United States, 13-17 Sep. 2014.
31. Tiago M., Carames F., Lamas P F., A Review on the use of Blockchain for the Internet of Things, IEEE Access, 2018.
32. Wilkinson S., Boshevski T., Brandoff J., Prestwich J., Hall G., Gerbes P., Hutchins P., Pollard C., Buterin V., Storj A Peer-to-Peer Cloud Storage Network, Available online: https://storj.io/storj.pdf (Accessed on 10 April 2018)
33. Ateniese G., Goodrich M T., Lekakis V., Papamanthou C., Paraskevas E., Tamassia R., Accountable Storage, in Proceedings of the International Conference on Applied Cryptography and Network Security, Kanazawa, Japan, 10-12 July 2017.
34. Wilson D., Ateniese G., From Pretty Good To Great: Enhancing PGP using Bitcoin and the Blockchain, in Proceedings of the International Conference on Network and System Security, New York, United States, 3-5 Nov. 2015.
35. Gipp B., Meuschke N., Gernandt A., Decentralized Trusted Time stamping using the Crypto Currency Bitcoin, in Proceedings of the iConference, Newport Beach, United States, 24-27 Mar. 2015.
36. Han D., Kim H., Jang J. Blockchain based smart door lock system, in Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, South Korea, pp. 1165-1167, Dec. 2017.
37. Siddiqi M., All S T., Sivaraman V., Secure lightweight context-driven data logging for body worn sensing devices, in Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, pp. 1-6, 2017.
38. Lei A., Cruickshank H., Cao Y., Asuquo P., Ogah C P A., Sun Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems, in IEEE Internet of Things Journal, 4(6), pp. 1832-1843, Dec. 2017.
39. Kshetri N. Can Blockchain Strengthen the Internet of Things?, in IT Professional, 19(4), pp. 68-72, 2017.
40. Tanas C., Delgado-Segura S., Herrera-Joancomartí J. An Integrated Reward and Reputation Mechanism for MCS Preserving User's Privacy, in Revised Selected Papers of the 10th International Workshop on Data Privacy Management, and Security Assurance - vol. 9481. SpringerVerlag New York, Inc.,USA, pp. 83-99, 2016.
41. Huh, S., Cho, S., Kim, S., Managing IoT devices using blockchain platform, in Proceedings of the 19th International Conference on Advanced Communication Technology(ICACT), Bongpyeong, SouthKorea,19-22 Feb. 2017.

42. Atlam H., Blockchain with Internet of Things: Benefits, Challenges, and Future Directions, International Journal on Intelligent Systems and Applications, 6(2018).
43. Xia X., Xiao Y., Liang W., ABSI: An adaptive binary splitting algorithm for malicious metre inspection in smart grid, IEEE trans. Inf. Forensics Security, 14 (2) (2019), 445-458.
44. Zhang C., Wu J., Zhou Y., Cheng M., Long C., Peer-to-peer energy trading in a micro grid, Applied Energy, 220, pp. 1 – 12, (2018). [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0306261918303398.
45. Li Z., Kang J., Yu R., Ye D., Deng Q., Zhang Y., Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things, IEEE Transactions on Industrial Informatics, 14(8), pp. 3690– 3700, (2018).
46. Aitzhan N Z., Svetinovic D., Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Transactions on Dependable and Secure Computing, 15(5), pp. 840–852, (2018).
47. Pop C., Cioara T., Antal M., Anghel I., Salomie I., Bertoncini M., Blockchain based decentralized management of demand response programs in smart energy grids, Sensors, 18(1),(2018).
48. Konstantinidis I., Siaminos G., Timplalexis C., Zervas P., Peristeras V., Decker S., Blockchain for business applications: A systematic literature review, in Business Information Systems, Abramowicz W., Paschke A., Eds. Cham: Springer International Publishing, (2018), pp. 384–399.
49. Kim H. M., Laskowski M., Toward an ontology-driven blockchain design for supply-chain provenance, Intelligent Systems in Accounting, Finance and Management, 25(1), pp. 18–27, (2018).
50. Tapscott A. Tapscott D., How blockchain is changing finance, Harvard Business Review, 1(2017).
51. Kshetri N., blockchains roles in meeting key supply chain management objectives, International Journal of Information Management,39, pp. 80 – 89, (2018).
52. Li V., Guo H., Wang W. M., Guan Y., VatankhahBarenji A., Huang G. Q., McFall K. S., Chen X., A blockchain and automl approach for open and automated customer service, IEEE Transactions on Industrial Informatics, pp. 1–9, (2019) (Early Access). [Online]. Available: https://doi.org/10.1109/TII.2019.2900987.
53. Wang K., Shao Y., Shu L., Zhu C., Zhang Y., Mobile big data fault-tolerant processing for ehealth networks, IEEE Network, 30(1), pp. 36–42, (2016).
54. Esposito C., Santis A. D., Tortora G., Chang H., Choo K. R., Blockchain: A panacea for healthcare cloud-based data security and privacy?, IEEE Cloud Computing, 5(1) pp. 31–37, (2018).
55. Griggs K. N., Ossipova O., Kohlios C. P., Baccarini A. N., Howson E. A., Hayajneh T., Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, Journal of Medical Systems, 42 (7), p. 130, (2018). [Online]. Available: https://doi.org/10.1007/s10916-018-0982-x.
56. Bhuiyan M. Z. A., Zaman A., Wang T., Wang G., Tao H., Hassan M. M., Blockchain and big data to transform the healthcare, in Proceedings of the International Conference on Data Processing and Applications, ser. ICDPA. ACM, (2018), pp. 62–68.
57. Sun Y., Zhang R., Wang X., Gao K., Liu L., A decentralizing attribute-based signature for healthcare blockchain, in 2018 27th International Conference on Computer Communication and Networks (ICCCN), (2018), pp. 1–9.
58. Rahman M. A., Hossain M. S., Loukas G., Hassanain E., Rahman S. S., Alhamid M. F., Guizani M., Blockchain-based mobile edge computing framework for secure therapy applications, IEEE Access, 6, pp. 72469–72478, (2018).
59. Kusiak A., Smart manufacturing, International Journal of Production Research, 56, (1-2), pp. 508–517, (2018).
60. Christidis K. Devetsikiotis M., Blockchains and smart contracts for the internet of things, IEEE Access, 4, pp. 2292–2303, (2016).

61. Wan J., Li J., Imran M., Li D., e-Amin F., A blockchain-based solution for enhancing security and privacy in smart factory, IEEE Transactions on Industrial Informatics, pp. 1–9, (2019) (Early Access). [Online]. Available: https://doi.org/10.1109/TII.2019.2894573.
62. Karthik B N., Parameswari D L., Harshini R., Akshay A., Survey on IOT & Arduino Based Patient Health Monitoring, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, (IJSRCSEIT), 3(1)(2018) , ISSN : 2456-3307, PP-1414-1417.
63. Kumbi A., Naik P., Kirthishree C., Kotin K., A Survey Paper on Internet of Things Based Healthcare System, Internet of Things and Cloud Computing. Special Issue: Advances in Cloud and Internet of Things. 5(5-1)(2017), PP. 1-4. doi: 10.11648/j.iotcc.s.2017050501.11.
64. Gurjar A A., Neha A., Heart Attack Detection By Heartbeat Sensing using Internet of Things: IoT, International Research Journal of Engineering and Technology (IRJET), 5(3)(2018), pp-3332-3335.
65. Savaliya A., Bhatia A., Bhatia J., Application of Data Mining Techniques in IoT: A Short Review, International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), 4(2)(2018).
66. Frank K., Robertson P., Gross M., Wiesner K., Sensorbased identification of human stress levels, IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops '13), (2013)pp. 127– 132.
67. Wang R., Chen F., Chenetal Z.,Student life: assessingmental health, academic performance and behavioural trends of college students using smart phones, ACM International Joint Conference on Pervasive and Ubiquitous Computing(UbiComp'14),(2014)pp.3–14.
68. Sundholm M., Cheng J., Zhou B., Sethi A., Lukowicz P., Smart-mat: recognizing and counting gym exercises with low cost resistive pressure sensing matrix, ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14), (2014) pp. 373–382.
69. Dinh T. T. A., Wang J., Chen G., Liu R., Ooi B. C., Tan K.-L., Blockbench: A framework for analyzing private blockchains, in Proceedings of the 2017 ACM International Conference on Management of Data, ser. SIGMOD '17. New York, NY, USA: ACM, (2017), pp. 1085–1100. [Online]. Available: http://doi.acm.org/10.1145/3035918.3064033
70. Dinh T. T. A., Liu R., Zhang M., Chen G., Ooi B. C., Wang J., Untangling blockchain: A data processing view of blockchain systems, IEEE Transactions on Knowledge and Data Engineering, 30(7), pp. 1366–1385, (2018).
71. Croman K., Decker C., Eyal I., Gencer A. E., Juels A., Kosba A., Miller A., Saxena P., Shi E., Sirer E. G., et al., On scaling decentralized blockchains, in International Conference on Financial Cryptography and Data Security. Springer, (2016), pp. 106–125.
72. Conoscenti M., Vetro A., DeMartin J. C., Blockchain for the internet of things: A systematic literature review, in 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), (2016), pp. 1–6.
73. Conti M., E S. K., Lal C., Ruj S., A Survey on Security and Privacy Issues of Bitcoin, IEEE Communications Surveys Tutorials, (2018).
74. Dorri A. Kanhere A., Jurdak R., MOF-BC: A memory optimized and flexible blockchain for large scale networks, Future Generation Computer Systems, 92, pp. 357 – 373, (2019). [Online]. Available: http://www.sciencedirect.com/science/article/pii/ S0167739X17329552.
75. Gu J., B. S., Consortium Blockchain-Based Malware Detection in Mobile Devices. IEEE Acc, 6, pp. 12-118, (2018).
76. Lee B., L.-H., Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. J. Super comput, 73(3), pp. 1152-1167, (2017).
77. Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D, Voelker G M., Savage S., A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference, pages 127–140. ACM, (2013).

78. Kosba A., Miller A., Shi A., Wen Z., Papamanthou C., Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In IEEE Symposium on Security and Privacy (SP), 2016, pages 839–858. IEEE,(2016).