IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A REVIEW ON BLOCKCHAIN BASED IOT SYSTEM

Ms.Snehal Sachin.Somwanshi,

Research Scholar

Dr.APJ Abdul Kalam University, Indore, India

Abstract:

The always increasing number of Internet net of Things (IoT) devices in the society, it makes a secure, accessible, and reliable infrastructure to process and store the computed data. The present IoT model uses a central cloud server model which leads to single point failures. To avoid this Blockchain technology is integrated with IoT because Blockchain uses a distributed network. Blockchain technology has tremendous development in the field of IoT security. In this paper, we conducted a systematic review of Blockchain based IoT application and its security issues. Comparison between IoT and Blockchain technology discussed. Based on an organized, evaluation and efficient content analysis of the academic literature, we discussed the broad classification of blockchain-based IoT applications through various segments such as Industrial, smart Health care, smart city, smart home, ad-hoc vehicle networks (VANET), eBusiness model, and supply chain management. We also pointed out the security issues of Blockchain based IoT application, particularly limitations the blockchain technology in IoT. This paper will help the academician and researcher further develop the IoT based Blockchain application.

Keywords— Blockchain; Internet of Things (IoT); VANET; Distributed network.

I. INTRODUCTION

The rapid progress in the Internet of Things (IoT) in this world, there are several of devices in the smart house, workshops, factory, healthcare sector, e-business model, vehicles, and lakhs of distant places. With the production of devices, people want to connect the devices, and collect information from the devices, store this information and analyze the information. IoT technology increases the world economy and gives a sophisticated life to society . IoT has following security challenge, and Many IoT devices are come in the market for the users to use, each device has its security policies, hackers will use these security policies as an entry point and attack the system on the INTERNET, THIS activates hackers to misuse the personal information and trust factor between public and internet connected devices will be accessed. In these situations, it is tremendously dangerous to safeguard the security, and reliability of internet apps to endorse the use of IoT devices amongst consumer's crossways the world. The probability of chasing and investigation of persons by private management, public sector and government rise as the devices are continually associated with the internet [6]. IoT devices gather consumer's data without their authorization, analyze them for commitments only known to the father business. Interoperability is one the major challenging issue in IoT since IoT devices exchange the information between connected devices. However, the real situation is fundamentally tricky and depends on communication protocols between such devices. In industry may use a lot of IoT devices to manufacture the product, another challenge is time to create consistent protocols mutual for all IoT devices.

IoT issues security issues is summarized as follows, which will be solved by blockchain (BC) technology are mostly the problems affected by the centralized architecture of present Internet of Things systems. 1. Centralized server failure 2.Single point failures 3. Lack of privacy. Blockchain technology will solve the problem mentioned above since its distributed architecture, and it prevents from the single point failures[5] . The specific methodology of how the agreement is transferred is an ongoing area of study and might differ to suit a wide range of utilization domains. New transactions are associated with previous transactions by cryptography which performs blockchain networks flexible and secure. Every network user can check for themselves if transactions are valid, which provides clarity and trustable, tamper-proof records[3].

II.The Use of Blockchain in IoT

A blockchain (a chain of linked blocks) is a distributed ledger with a list of linked data records or blocks, which are linked and secured by cryptographic hashes. Each block contains a set of new data records or transactions, as well as the hash value of the previous block, along with a timestamp that verifies the transactions at the time of the creation of the block, making the modification of records difficult, as they are dependent on prior records, as shown in Figure 1. Blockchain is characterized by the fact that data cannot be modified because they are copied and stored in a distributed and dependent manner

III.BLOCKCHAIN APPLICATION

Blockchain can enhance the IoT by giving secure service, where data is reliable and can be accessed. Data location can be recognized whenever data rests immutable over time, increasing its security. Blockchain IoT interactions can be categorized into three types.

1. IoT–IoT: it establishes interaction IoT devices to IoT devices.
2. IoT–Blockchain: this enables the IoT devices to communicate with Blockchain network
.3. Hybrid approach. This approach could be a combination of IoT-IoT and IoT-Blockchain

IV.Overview of Blockchain based IoT application

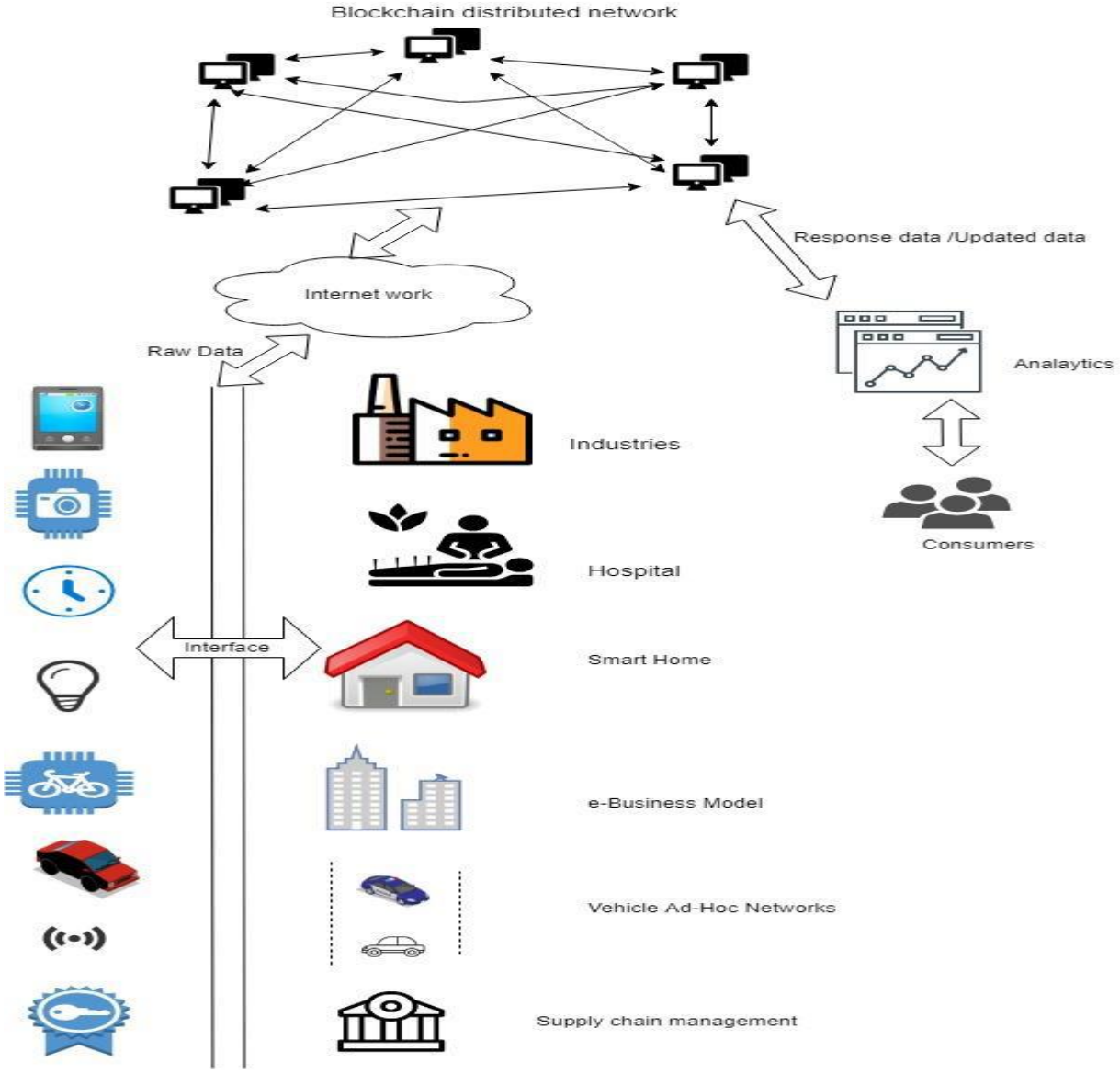

Fig.1 Overview of Blockchain based IoT application

Fig.1 shows the Overview of Blockchain based IoT application. The modern Internet of Things ecosystems trusts on centralized models, otherwise known as the client /server model. All devices are recognized, validated and joined through servers that have enormous storage capacity and processing power. Single point failures are an essential problem in the preset IoT model, to solve this issue IoT model is integrated with Blockchain technology. Blockchain technology uses a decentralized approach to IoT networking[15].

V. Benefits of merging IoT and Blockchain

There are a few clear benefits to building Blockchain based IoT application. 1. IoT based application can exchange information between numerous systems claimed and managed by various company or government it is creates security issue. Blockchain records are by their very nature straightforward – action can be followed and dissected by anybody approved to interface with the system. 2. Blockchain (which for this situation would be held by machines), no human will have the capacity to overwrite the record with erroneous data.3. A significant part of the information produced by IoT is profoundly close to home –for instance, shrewd home gadgets approach cozy insights regarding our lives and day by day schedules[20].

VI.Challenges to Block chain's adoption in IoT:

The presently used consensus protocols such as PoW,PoS and vote based consensus protocol is not suitable for IoT environment since it has less amount of processing power. If we trying to use the above consensus protocol in IoT environment it leads to the transaction late it is not suitable for real time IoT environment. Most of the IoT devices are used in centralized cloud server[12].

A. Blockchain Platform for Industrial Internet of Things

Blockchain Platform for Industrial Internet of Things (BPIIoT) can enhance the working of Cloud-based Manufacturing (CBM) by giving a decentralized, peer-to-peer network and suspicious, for the production environment. CBM is a service-oriented industrial prototype. Users use the services configure, production devices as per their need by using CBM model. BPIIoT is based on a BC network on which smart contracts are deployed[11]. The smart contracts act as arrangements between the service buyers and the manufacturing devices to provide on-demand producing services. BPIIoT enables mixing legacy shop floor machine into the cloud environment and allows strengthening decentralized and peer-to-peer production software. Industry production IoT components may access the controlling distribution services for making the complete product at that time there trust should be established between production IoT components and controlling distribution services, to solve this issue integration BC technology with IoT devices is a complex process in the BPIIoT.

B. Smart Health care in IoT with Blockchain:

Smart Health care will be the greatest leading IoT apps, Smart healthcare apps and services can perform real-time watching and actuation for healthcare needs of patients and use data analytics in the cloud to improve the quality of healthcare and experience for patients while reducing the cost of providing healthcare services. Security in smart healthcare includes numerous features based on the integrity of Health Record preserved in a hospital [14]. There are various advantages and disadvantages of data and decision fusion in IoT for healthcare. Data fusion consumes more bandwidth for transmitting raw sensory data, which could have numerous features with high dimensionality, e.g., data from image sensors used in endoscopy, Whereas decision fusion requires less bandwidth since the decision, that is refined information is transmitted over the network. Decision fusion results in loss of accuracy since raw sensory data processing will contain inherent rounding errors in computation based on processing accuracy of sensors. Alternatively, data fusion yields additional precise results because the computations are performed on sensor network gateways which have more power. Indeed, decision fusion consumes the constrained power of the sensors to compute and transmit the information, whereas, in data, fusion sensors consume more power to transmit high dimensional data. Since radio transmission consumes more power than processor computations [15].

C.Blockchain-based the smart city:

BC can be great to make the smart city idea a genuineness. The idea of the smart city is based on smart IoT devices. With IoT developing and flourishing, a large amount of data will be generated by various methods in the circumstances of smart cities. The smart city (SC) network is broken into two disparate groups – the core network and the edge network – using the BC technique. The center system contains mine nodes with high computational power and capacity gadgets, though the edge devices have deficient capacity gadgets and handling power. Miner node will be striven for making the block and checking confirmation of-work (PoW). Every node is allowed with SDN controller to deliver incredible agility and security, decline equipment organization cost, and understand the simplicity of arrangement in the smart city organize framework. Blockchain-based Smart city each edge node goes about as a centralized server for the explicit open framework to give first administrations and achieve confinements. It stores the way approaches and accreditations of its privately enlisted substances in its database and accomplishes low inertness and reduce bandwidth transmission capacity[10]. The proposed strategy is the circulated nature which can make the entire task increasingly flexible and confine the power of assaults notwithstanding when the node is imperiled. Alternatively, if the edge node is hacked, the effect must be confined to the local area. Managing low latency, disgracing bandwidth usage, and growing protection and privacy and scalability are significant difficulties in smart cities.

D.Blockchain-based smart home:

Blockchain (BC) -based smart home be dissimilar from a conventional IoT based home. BC-based smart home has a design standard, which including turns as an ACL that permits the proprietor to regulate all the activity occurring in her house. The miner issues a shared key between corresponding methods as per policy set by the proprietor in device-to-device communication. The BC-based smart home scheme provides commanded access to IoT information. It additionally safeguards data integrity, availability, and message confidentiality along with security against distributed denial-of-service (DDoS) attacks.

E.BC-based self-managed VANET

The traditional Vehicular Ad-hoc Networks (VANET) has a centralized management right. This planning has several disadvantages. 1. Hackers use a single point of failure to attack the VANET.2. It has rarer consumer's confidentiality. To solve this problem, BC-based decentralized, self-managing Vehicular Ad-hoc Networks is introduced. The total VANET is directed by Ethereum-based software, which is utilized to give various administrations. Every consumer is enrolled and recognized by its Ethereum address. To get to administrations given by Ethereum-based software, each consumer needs to pay as Ethers. Along these lines, the clients finance the system foundation. The installment made by the clients fills in as the impetus for the sellers giving Ethereum-based software and related administrations. In a whole situation, the Ethereum record of a client can be utilized to make robotized installments of vehicle protection, enlistment, new administrations like ongoing traffic refresh and installment of criminal traffic offense fines. BC-based self-guided vehicle specially appointed systems have following downsides. 1. The main problem in the BC protocol is latency issues since it works based on the decentralized network.

VII.CONCLUSION

Blockchains become more developed in IoT devices are likely to move in more businesses/educations/ field than the ones discovered in our study. Numerous users try to recommend blockchains as a solution and a substitute for databases system. There are many situations where traditional databases system should be used in its place. This paper simplifies the selection of the correct blockchain and the corresponding method to secure the IoT application in the real-time requirements. We presented the distinct features that are frequently essential per each domain in the IoT application. Finally, we discussed the Blockchain based IoT application and its security issues in real time environment.

REFERENCES

[1] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," Telemat. Informatics, no. November, pp. 0–1, 2018.

[2] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards Blockchain-based Auditable Storage and Sharing of IoT Data," pp. 45–50, 2017.

[3] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, no. June, pp. 32979–33001, 2018.

[4] Https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html, "No Title." .

[5] K. R. Özyılmaz and A. Yurdakul, "Integrating low-power IoT devices to a blockchain-based infrastructure," Proc. Thirteen. ACM Int. Conf. Embed. Softw. 2017 Companion - EMSOFT '17, pp. 1–2, 2017.

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

[7] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: The challenges, and a way forward," J. Netw. Comput. Appl., vol. 125, no. October 2018, pp. 251–279, 2019.

[8] C. F. Liao, S. W. Bao, C. J. Cheng, and K. Chen, "On design issues and architectural styles for blockchain-driven IoT services," 2017 IEEE Int. Conf. Consum. Electron. - Taiwan, ICCE-TW 2017, pp. 351–352, 2017.

[9] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Futur. Gener. Comput. Syst., vol. 88, pp. 173–190, 2018.

[10] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A BLockchain-ENabled Decentralized Capability-based Access Control for IoTs," 2018.

[11] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," Procedia Comput. Sci., vol. 132, pp. 1815–1823, 2018.

[12] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Futur. Gener. Comput. Syst., vol. 82, pp. 395–411, 2018.

[13] A. Bahga and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," J. Softw. Eng. Appl., vol. 09, no. 10, pp. 533–546, 2016.

[14] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," J. Med. Syst., vol. 42, no. 7, 2018.

[15] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of internet of things infrastructure for secure and smart healthcare," Computer (Long. Beach. Calif)., vol. 50, no. 7, pp. 74–79, 2017.

[16] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," Futur. Gener. Comput. Syst., vol. 86, pp. 650–655, 2018.

[17] C. Qu, M. Tao, and R. Yuan, "A hypergraph-based blockchain model and application in internet of things-enabled smart homes," Sensors (Switzerland), vol. 18, no. 9, 2018.

[18] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017, no. March, pp. 618–623, 2017.

[19] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," Proc. 2016 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput. Adjun. - UbiComp '16, pp. 137–140, 2016.

[20] J. W. Yu Zhang, "The IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Netw. Appl., no. 4, p. 11805258, 2018.