Framework for Securing IoT Ecosystem Using Blockchain: Use Cases Suggesting Theoretical Architecture

Anshul Jain, Tanya Singh, and Nitesh Jain

Abstract Blockchain is a distributed, open record between two customers for all trades. The decentralized nature is possible because each trade is controlled by the understanding of a larger number of customers, who are interested in anything in the system. The authors concentrate and present methods to address real issues of security in IoT. The authors review use cases and organize common issues of security with respect to IoT layered building. Despite the current plans for attacks, hazards and cutting-edge game, we are designing essential IoT security conditions. IoT security problems are also orchestrated against the current game plans discovered in writing and mapped against them. Furthermore, we are trying to discuss how blockchain, which is the fundamental development of Bitcoin, can be the primary enabling impact to deal with immeasurable IoT security problems. Besides, the paper includes open research issues and challenges to IoT security. In this paper, the potential informative applications are focused, along with explorations on how blockchain advancement can be used to address some preparation issues. In the wake of inquiring about security issues, authors present an architecture of IoT blockchain ecosystem. This paper also talks about the highlights and ideal states of blockchain improvement.

Keywords Blockchain · IoT · Data security · Network security · Blockchain IoT protocols · IoT security · IoT ecosystem · Blockchain-enabled IoT

A. Jain (✉)
AIIT, Amity University, Noida, Uttar Pradesh, India
e-mail: anshuljain13@gmail.com

T. Singh
ASET, Amity University, Noida, Uttar Pradesh, India
e-mail: tsingh2@amity.edu

N. Jain
JSSATE, Uttar Pradesh Technical University, Noida, Uttar Pradesh, India
e-mail: jainitesh@gmail.com

M. Tuba et al. (eds.), *ICT Systems and Sustainability*, Advances in Intelligent Systems and Computing 1270, https://doi.org/10.1007/978-981-15-8289-9_21

1 Introduction

Blockchain progress is generally referred to as appropriate record innovation. It allows people to efficiently check transactions performed, exchange and transfer advantages in [1]. A model flow of cryptographic currency blockchain exchange is technique of ease. To initiate a transaction with User B, a shared blockchain is used by Customer A. A cryptographic character check (two or three open keys and private key) is used to make an unusual correlation between Customer A and Customer B in the framework. At this stage, the exchange will be transferred strongly to the memory pool of the blockchain framework for transaction check and approval. The new block is shaped by acquiring a specific measure of the avowed center points; this is called arriving at a consensus. This square incorporates every one of the exchanges that have occurred during this minute. It is "connected" through the modern imprint to the main obstacle in the plan in [2]. The foundation of the accord is practiced utilizing an agreement calculation. This block embodies each of the exchanges taking place at this time. It is "connected" to the main obstacle in the plan through the modern imprint in [2]. The platform of the consensus is practiced using a consensus algorithm. This is referred to as mining industry. In particular, the peer-to-peer plan competes with the present circumstance of the spread record [3]. Each center can cast a vote by denying advances by taking increments or dismissing invalid blocks by their CPU ability to perceive authentic blocks. Any fundamental direction and propelling powers can be executed through this plan of understanding [4]. Any block of exchange is distinguished with a specific time mark. The two blocks are equally interfaced by a timestamp. The blockchain data thus demonstrates a property of time, and the span of the chain is always developing. It implies that the blockchain is a variety of transmitted transactions that upgrade the timestamp organization [5–8]. To create a notable chain of SHA-256 hash limit, explicit hardware is utilized by blockchain, and cryptographic data is used to prevent invincible client data from being adjusted [1].

The organization of this paper is as follows. Section 2 explains different applications in IoT ecosystem using blockchain technology, and it also describes its security requirements. Next Sect. 3 explains different benefits of blockchain which makes it robust and reliable. Section 4 describes a combined and modular architecture of IoT-enabled blockchain technology. A brief literature survey is done in Sect. 5 which goes through several papers and writes the outcome of the research done. This section also reviews several papers and presents them in a tabular format representing different IoT blockchain methods proposed, their benefits, shortcomings and future scope. Finally, conclusion is presented in last Sect. 6.

2 Internet of Things Domain Use Cases Using Blockchain and Their Security Requirements

This section includes various IoT applications which explains the problems faced due to lack of security in the study.

2.1 IoT Blockchain-Enabled Financial Services

Numerous IoT frameworks are likely to be subject to smaller-scale budget exchanges between computerized articles, requiring the IoT devices be associated in a manner that considers the so-called machine-to-machine (M2 M) economy–which is essentially the money trading between non-human devices. The number of transactions is concerned; countless blockchain schemes have restricted execution every time they can cope with it. This implies most blockchain executions of proof of work and proof of stake blockchain present the limited potential for versatility, making them unacceptable for large-scale handling of M2 M microtransactions. Nevertheless, it is worth mentioning that countless blockchain operations are shifting toward adaptability provisions, such as the Bitcoin lightning network and the Ethereum Plasma [9].

2.2 IoT Security with Blockchain

Another safety building that dodges the use of cryptography scheme based on the trade-in symmetric or asymmetric cryptography keys is suggested that is not prescribed in IoT devices due to their handling, storage and energy containment [10]. The suggested scheme relies on the multi-operator being used to guarantee the safety of related objects. With no compelling reason to register keys, these studies modified with specialists can speak to different items. The main goal of this job is to maintain an abnormal state of safety by enhancing the energy usage of IoT devices [11].

2.3 Privacy-Preserving Healthcare Blockchain for IoT

Designs are for confirming an unbound IoT-based implementation, especially concerning applications for medicinal services where customer approval is a key issue. The three procedural examples, i.e. Security Goal Documentation, Choose the Right Stuff and enroll from Outsider Pattern, are examined in [12]. Five other examples of approval are shown in this investigation as reference monitor, access

matrix role approval guidelines and role-based access control, remote authenticator/authorizer and file authentication patterns. For IoT-based E-healthcare applications, a protected gathering-based lightweight validation conspire has been proposed where the proposed model will provide shared validation and energy proficiency and calculation for IoT-based social insurance applications [13], which will use elliptic curve cryptography (ECC) guidelines that provide mention included of the suggested model [14].

2.4 IoT Blockchain Support to LoRaWAN Network Servers

An IoT framework model is presented that uses the LoRaWAN convention to transmit information from sensor hubs to our cloud administration and the things network stage that executes the backend administrations of LoRaWAN [15]. The authors have organized a structure that can be adapted and extended to expand new advantages just as other IoT phases are coordinated. It is also equally adaptable, which means that a presentation can be designed simply by creating new server instances (Fig. 1).

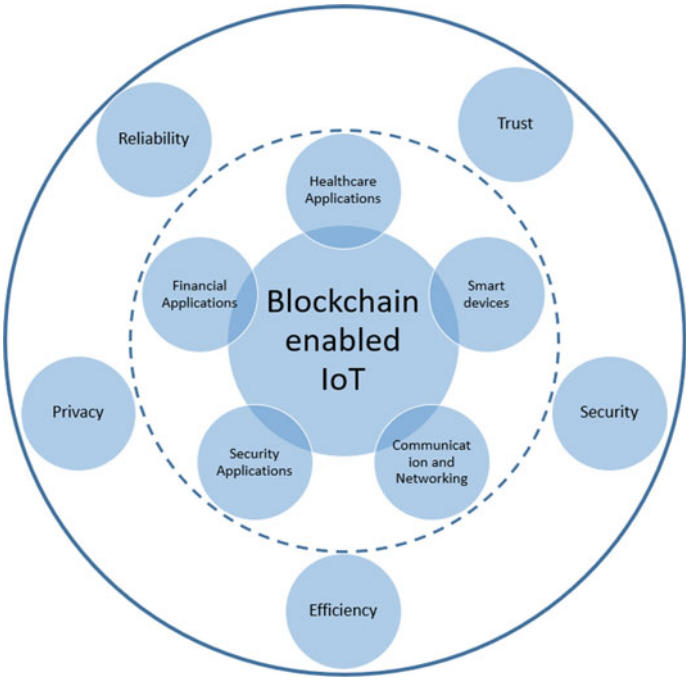

Fig. 1 Application and benefits of IoT blockchain security

3 Benefits of Blockchain

Reliability. The databases of the entire transaction records are changed by the decentralized concept. Cloud adds to the reliability where which helps data to be easily accessed and processed with security features like asymmetric encryption [16].

Trust. The blockchain structure is happening as new trust providers with decentralized data. These data is distributed across a system of fixed centers [17].

Security. The blockchain framework uses one-way hash work. The yield has no unmistakable connection to the information.

Efficiency. Blockchain advancement could accelerate the clearing and repayment of specific exchanges identified with cash by decreasing the number of middle people included and making the trade-off procedure faster and gradually profitable [18].

4 Literature Review

Another IoT access control structure is based on the blockchain's development. The objective of the study is to provide a reference model for the proposed structure in the IoT objectives, models, architecture and mechanism [19]. In addition, fair access is presented as a full pseudonymous and security-saving executive system authorization that empowers customers to own and regulate their data. For updating the model, the blockchain is used and adjusted to decentralized control of access.

A decentralized trust system, called IoT passport, is suggested using innovation in blockchain for coordinated cross-stage efforts [20]. A reference design for shared IoT applications based on blockchain, featuring the main correspondence channels anticipated to interface the IoT layer with the blockchain layer, was shown in [21]. By establishing frameworks and conventions for shared IoT applications based on blockchain, the practicality of the suggested engineering has been explained.

A successful and controlled blockchain plot-based transmitted cloud architecture is discussed in CRVANET's biological system instead of custom cloud engineering to protect driver safety with minimal effort and on-demand detection in [22].

In addition to providing research methodology to identify concerns and arrangements, an efficient survey of existing IoT security and protection systems is provided in [23]. It discusses IoT design, characterizes the distinct areas of safety and security and provides a scientific classification and close investigation to plot safety goals, risks and attacks and agreements suggested late (2015–2018) (Table 1).

Table 1 Review of proposed methods

Reference No	Proposed method	Benefits	Shortcomings	Future scope
[20]	IoT passport	It helps in commodity user interfaces	It is completely dependent on trust and is very susceptible to security threats	Future work calls for collaborative IoT
[6]	IoT chain	It provides a flexible authorization	The performance and robustness have not been much evaluated	Private ethereum blockchain network needs upgradation to be used in the PoS-based version of the ledger
[8]	A blockchain-based proxy re-encryption scheme	It provides scalability and security to the automated payments	The number of mined transactions depends on various factors including gas price and limit	Future implementation includes implementation on different blockchain platform, e.g., hyperledger
[24]	An over-the-blockchain firmware update framework	It provides a secure verification to the firmware	The firmware mechanisms are too lengthy to operate	Future work includes the development of a robust and lightweighted protocol
[25]	Unibright	New templates are created to recognize different industries	A huge number of risks are associated with it	Future work needs to focus mostly on the risks associated
[26]	A decision framework to support blockchain platforms for IoT and edge computing	It shows the systematic identification of blockchain characteristics suitable for IoT platform	This framework still did not provide any specific	This decision framework can be improved into a recommender tool

5 Proposed Architecture–Blockchain in IoT Ecosystem

The architecture of IoT ecosystem as explained in [27] is fully modular, and all the modules can be easily decoupled from one another in order to add a module and keeping the rest of the system intact. [28] Further provides a comparative study on the architecture, which shows security issues and solutions on application layer. Integrity-related problems can be handled by blockchain solutions discussed in this paper.

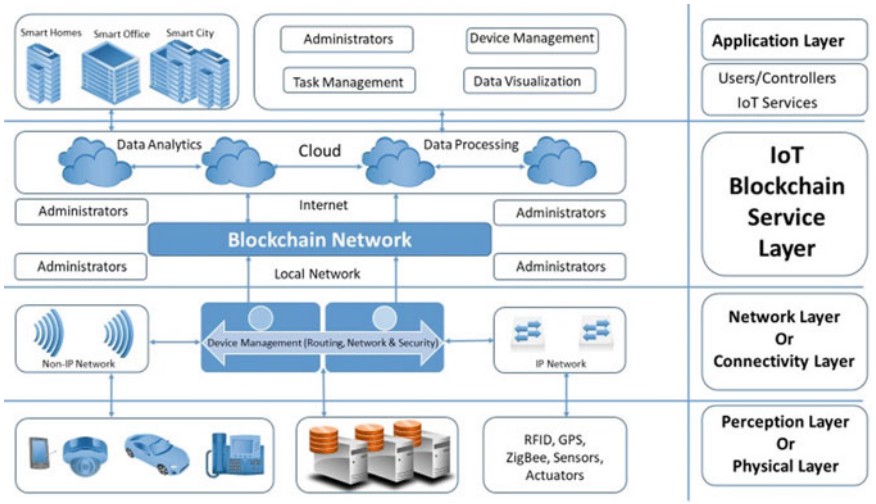

Fig. 2 Proposed architecture for blockchain in IoT ecosystem [27, 28]

This paper proposes in Fig. 2 a modification to the architecture discussed in [28], where blockchain is introduced before the application layer which can address some of the security issues addressing our concerns related to confidentiality, integrity and accountability. Several linked devices possessing the capabilities of communication, data storage and computing are present in the IoT physical layer. The connectivity layer provides services which include managing the networks, managing the security and passing of messages. The IoT blockchain service layer provides all services including managing identities, peer-to-peer communication and consensus. The application layer consists of the interfaces which visualize the data from all the physical devices for regulating and manipulating devices.

6 Future Projection of an IoT and Blockchain Authorization Model

The Internet of things (IoT) has stretched the Web availability to reach PCs and people, yet most of our population is missing Internet of things. The IoT may be able to combine billions of articles at the same time, which has the effect of improving the sharing of data needs as a result of improving our lives. Even though the advantages of IoT are boundless, due to its concentrated server/customer model, the IoT are facing numerous difficulties. For example, the versatility and security issues that arise as a result of the unreasonably large number of IoT issues in the system. The server model requires all devices to be linked and verified through the server, which is the single point of failure. In this way, moving the IoT framework in a decentralized direction

could be the right choice. One of the well-known frameworks for decentralization is blockchain. The blockchain is a ground-breaking innovation that decentralizes computation and board forms that can capture a vast number of IoT issues, security. Blockchain innovation is the missing link to solve the problems of versatility, protection and reliability in the Internet of things. Blockchain advances might be the silver slug required by the IoT business. New Innovations in Blockchain technology can be used to track billions of devices, empower exchanges and coordination between devices are considered as significant reserve funds for IoT industry. This decentralized methodology would be used for the sole purpose of disappointment, creating a stronger biological system for devices to keep going. Cryptographic calculations used by blockchains would make purchaser information confidential. Blockchain-based IoT arrangements are appropriate for streamlining business forms, improving customer experience and achieving significant cost efficiencies.

7 Conclusion

As we envision the future growth of IoT, we must also discuss about its security as one of the utmost requirements of IoT ecosystem. In this paper, we have addressed security issues in IoT ecosystem using blockchain technology. We have also discussed a few domains like finance, healthcare, network, smart devices, etc., all these domains have their specific security requirements and challenges. This paper discusses the probable models which can be used by these domains to address security issues using blockchain technology. The broad overview provided in this paper also discusses about the combined and modular architecture of IoT and blockchain, and this architecture is designed in such a flexible way that all the devices and layers can be coupled or decoupled as per the domain's requirement. This paper also sheds some light on the benefits of blockchain which gives us confidence of using this technology in our future deployments. Furthermore, we have done a brief literature survey on the solutions discussed by several technical papers on this technology. Different solutions provided by several writers are compared based on their benefits, shortcomings and future scope on the proposed method. Before concluding this paper, we have also discussed a future projection of an IoT and blockchain-based authorized model, which mentions specific details required for this model. This paper is just a drop in the ocean of blockchain technology, there is long way to go and much more to dive into, but we expect that we are able to address some of the challenges of IoT ecosystem using blockchain technology and we hope that paper will be helpful in researches going to happen in near future. We are hopeful that blockchain is going to be one of the pioneer technologies in addressing security issues.

References

1. F. Tschorsch, B. Scheuermann, Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutorials **18**(3), 2084–2123 (2016)
2. J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?—a systematic review. PLoS ONE **11**(10), e0163477 (2016)
3. D. Kraft, Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking Appl. **9**(2), 397–413 (2016)
4. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008)
5. S. Haber, W. Stornetta, How to time-stamp a digital document, Crypto'90, LNCS 537 (1991)
6. O. Alphand, M. Amoretti, T. Claeys, S. Dall'Asta, A. Duda, G. Ferrari, F. Rousseau, B. Tourancheau, L. Veltri, F. Zanichelli, IoTChain: a blockchain security architecture for the internet of things, in *2018 IEEE Wireless Communications and Networking Conference (WCNC)* (IEEE, 2018), pp. 1–6
7. S. Mendhurwar, R. Mishra, Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges, in *Enterprise Information Systems* (2019), 1–20
8. A. Manzoor, M. Liyanage, A. Braeke, S.S. Kanhere, M. Ylianttila, Blockchain based proxy re-encryption scheme for secure IoT data sharing, in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE, 2019), pp. 99–103
9. The derivative effect how financial services can make IoT technology pay off. Retrieved from https://www2.deloitte.com/us/en/pages/financial-services/articles/the-derivative-effect-how-financial-services-can-make-iot-technology-pay-off.html. Last accessed 15 Jan 2020
10. B.A. Abdelhakim, B.A. Mohamed, B. Mohammed, B.A.O. Ikram, New security approach for IoT communication systems, in *Proceedings of the 3rd International Conference on Smart City Applications* (ACM, 2018), pp. 2
11. How to secure the internet of things with blockchain. Retrieved from https://www.devteam.space/blog/how-to-secure-the-internet-of-things-iot-with-blockchain/. Last accessed 15 Jan 2020
12. M. Aydar, S.C. Cetin, S. Ayvaz, B. Aygun, Private key encryption and recovery in blockchain, arXiv preprint (2019), arXiv:1907.04156
13. A. Pazaitis, P. De Filippi, V. Kostakis, Blockchain and value systems in the sharing economy: the illustrative case of backfeed. Technol. Forecast. Soc. Chang. **125**, 105–115 (2017)
14. A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for iot. Sensors **19**(2), 326 (2019)
15. Network Architecture, https://www.thethingsnetwork.org/docs/network/architecture.html. Last accessed 25 Jan 2020
16. Y. Zhang, C. Xu, J. Ni, H. Li, X.S. Shen Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage. IEEE Trans. Cloud Comput. (2019)
17. S. Underwood, Blockchain beyond bitcoin. Commun. ACM **59**(11), 15–17 (2016)
18. H. Wang, K. Chen, D. Xu, A maturity model for blockchain adoption. Finan. Innov. **2**(1), 12 (2016)
19. S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, M. Imran, Securing IoTs in distributed blockchain: analysis, requirements and open issues. Future Generation Comput. Syst. **100**, 325–343 (2019)
20. B. Tang, H. Kang, J. Fan, Q. Li, R. Sandhu, IoT passport: a blockchain-based trust framework for collaborative internet-of-things, in *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies* (ACM, 2019), pp. 83–92
21. G.S. Ramachandran, B. Krishnamachari, A reference architecture for blockchain-based peer-to-peer IoT applications. arXiv preprint (2019), arXiv:1905.10643
22. S. Nadeem, M. Rizwan, F. Ahmad, J. Manzoor, Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. Int. J. Adv. Comput. Sci. Appl. **10**(1), 288–295 (2019)

23. M. Gulzar, G. Abbas, Internet of things security: a survey and taxonomy, in *2019 International Conference on Engineering and Emerging Technologies (ICEET)* (IEEE, 2019), pp. 1–6
24. A. Yohan, N.W. Lo, An over-the-blockchain firmware update framework for IoT devices, in *2018 IEEE Conference on Dependable and Secure Computing (DSC)* (IEEE, 2018), pp. 1–8
25. S. Schmidt, M. Jung, T. Schmidt, I. Sterzinger, G. Schmidt, M. Gomm, K. Tschirschke, T. Reisinger, F., Schlarb, D. Benkenstein, B. Emig, Unibright-the unified framework for blockchain based business integration, in *Unibright Project White Paper* (2018)
26. N. El Ioini, C. Pahl, S. Helmer, A decision framework for blockchain platforms for IoT and edge computing. *SCITEPRESS* (2018)
27. A. Jain T. Singh, in *Security challenges and solutions of IoT ecosystem*, ed. by M. Tuba, S. Akashe, A. Joshi. Information and Communication Technology for Sustainable Development. Advances in Intelligent Systems and Computing, vol. 933 (Springer, Singapore, 2020)
28. A. Jain, T. Singh, S.K. Sharma, Threats paradigm IoT ecosystem, in *2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (Noida, India, 2018), pp. 1–7