Implementation of Blockchain in IoT

Chapter · March 2022

DOI: 10.1007/978-981-16-8774-7_13

2 authors:

Rasmeet Kaur
Glocal University
10 PUBLICATIONS **17** CITATIONS
SEE PROFILE

Aleem Ali
Chandigarh University
44 PUBLICATIONS **68** CITATIONS
SEE PROFILE

Implementation of Blockchain in IoT

Rasmeet Kaur and Aleem Ali

Abstract The concept of the Internet of Things is arising and developing quickly. IoT addresses another innovation that empowers both virtual and actual items to be associated and interact with one another and gives rise to new digitized services that enhance our satisfaction. The IoT framework gives a few benefits; notwithstanding, the current incorporated design presents various issues including, security, protection, straightforwardness, and data integrity. The quick advancement and usage of IoT innovations have raised security concerns and made a sensation of vulnerability among IoT adopters. These difficulties impede the method of things to come improvements of IoT implementations. Shifting the IoT toward distributed ledger technology might be the right decision to determine such problems. Among the normal and well-known kinds of such innovation is the Blockchain. Coordinating the IoT with Blockchain innovation may induce incalculable advantages. The motivation behind this paper is to analyze the latest research patterns identified with security worries of the IoT idea and give an itemized comprehension of the point. Subsequently, this paper gives a thorough conversation of incorporating the IoT framework with Blockchain innovation. The study is elaborated into four segments. Segment 1 introduces the description of IoT. The next segment will present the fundamentals and working of Blockchain. Segment 3 portrays a few instances of utilization for Blockchain to give security and protection at IoT. In segment 4, various platforms for Blockchain are presented. Segment 5 presents the last contemplations.

Keywords IoT · Blockchain (BC) · Distributed ledger technology (DLT) · Security · Privacy

R. Kaur (✉) · A. Ali
Department of CSE, Global University Saharanpur, Saharanpur, U.P, India

N. Marriwala et al. (eds.), *Emergent Converging Technologies and Biomedical Systems*,
Lecture Notes in Electrical Engineering 841,
https://doi.org/10.1007/978-981-16-8774-7_13

1 Introduction to IoT

The IoT is an extensive term alluding to progressing endeavors to associate a wide assortment of physical things to communication networks as shown in Fig. 1. IoT has a framework of organization that is worldwide where any article that is associated with the web has an identity and can speak with different gadgets on the web [1]. The gadgets contain microchips that interconnect every one of the gadgets. These computer chips track the surroundings and report in the network as well as to the humans.

Started during the 1990s, the idea of IoT is to expand over the Internet as well as to broaden the Internet. The most awesome aspect of IoT is that every single-actual substance can be imparted and is accessible. Currently, the Internet has connected

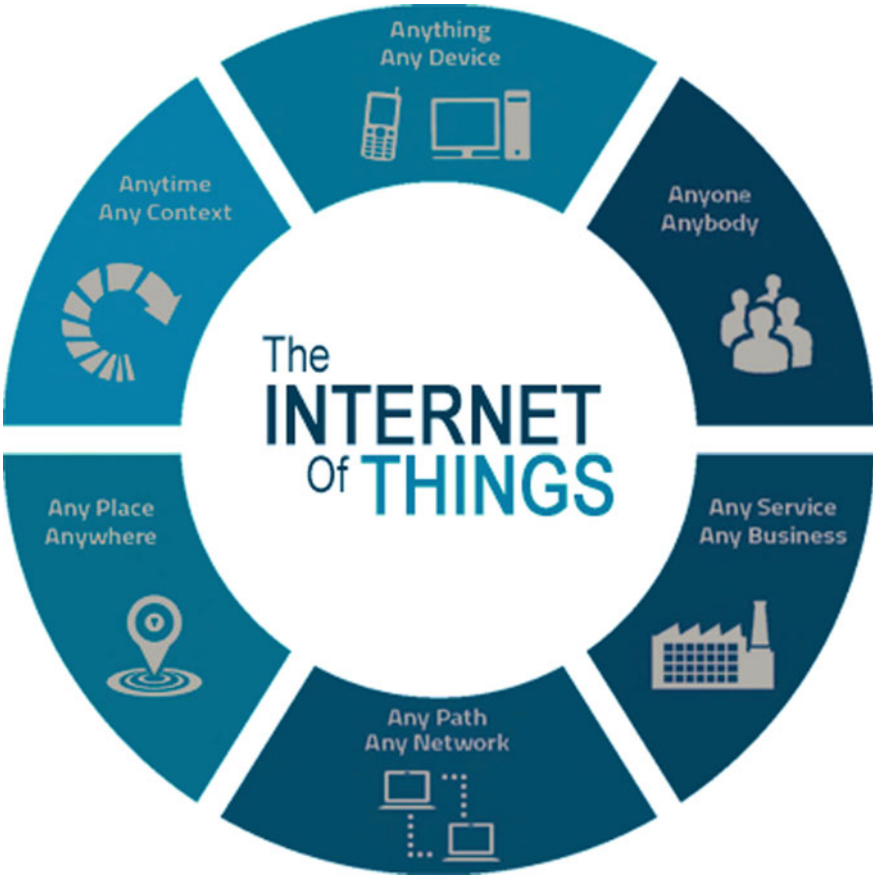

Fig. 1 Introduction to IoT

computers along with a wide heterogeneity of devices like TVs, workstations, refrigerators, ovens, electrical appliances, vehicles, and cell phones. In this new situation, projections show that the Internet will have more than 50 billion gadgets associated until 2020 [2].

The IoT framework offers various applications including, Smart homes, Smart cities, and Smart healthcare, etc. The essential component of this framework is the astute detecting assortment of information, which is then safely sent to the server [3]. The IoT domain has encountered fast advancement for over twenty years, and the quantity of IoT gadgets has developed dramatically, a pattern that enormously enhances social profitability and proficiency just as makes individuals' lives more helpful and astute.

There are remarkable benefits of IoT, still, it expanding the threat of openness to various privacy and security intrusions, and; a portion of such threats are new. Ahead of the concept of IoT, data leakage and denial of service were the most announced security concerns. Security and privacy alternatives need to be executed by attributes of heterogeneous IoT devices [4].

For these scenarios, BC plays a vital role, since one can use this technique to confirm, approve, and review the data given by the devices. Along with it, because of its decentralized nature, it disposes of the condition to trust in the outsider and doesn't have a single point of failure. BC is an idea that leads to decentralization as a safety effort, can make a worldwide file for all exchanges that happen in a given organization, and makes them permanent. It fills in as a public, shared, and general record.

Another main worry in the IoT domain is the secure storage of the data. Right now, numerous IoT data storage options preserve data on conventional centralized servers. Although, this strategy has some issues. First and foremost, all information is put away on a central server; hence, the performance needs, environment necessities, and upkeep expense for the central server are huge. The server must be equipped with a huge storage ability to preserve numerous data produces by IoT devices. When the server falls flat, the whole data storage framework won't work as expected.

Furthermore, as all IoT gadgets are associated with the central server, this will result in network blockage, high network delay, and non-sufficient space for data. At long last, when the main server is harmed by attackers, the data security will be incredibly compromised. Being a service of DLT, the Blockchain can take care of the issues that effectively happen in a centralized server [5].

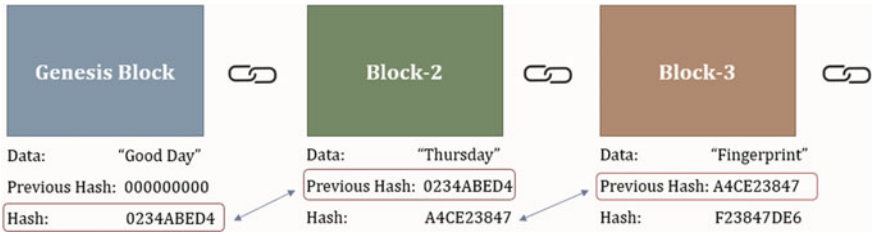

Fig. 2 Structure of blockchain

2 Blockchain

2.1 Introduction

Started in 2008, the embodiment of BC is to halfway keep a trustworthy data set arrangement through decentralization and distrust. The world kept using the centralized setup, where the main server is expected to manage the working until Szabo made decentralized computerized money toward the finish of 1990. After ten years, Bitcoin cryptographic money was advertised. BC turned out to be for the most part broad in 2009 after a study presented by Satoshi Nakamoto.

In a Blockchain, data is separated into a progression of blocks [6]. Every block of data can check the legitimacy of the data and create the succeeding block, which is associated in a sequential request into a chain-like arrangement as depicted in Fig. 2. BC is a non-centralized, distributed, and changeless log in which the data of the different exchanges that consistently occurred in a specific P2P network is kept. The process of storing an exchange/transaction in the distributed log demands a consensus mechanism.

A collection of exchanges are gathered and allocated a block in the ledger. To join a block to the preceding block, a hash function and timestamp of those blocks are used. In this way, numerous blocks are grouped as a chain and termed a Blockchain. The hash estimation approves the data integrity. The BC innovation advances sharing of information in which every taking part client/device in the structure maintains a duplicate of the actual ledger, hence every node is refreshed with recently added exchanges or blocks [7].

2.2 Components of Blockchain

The primary elements of the BC incorporate ledger, block, hash, transaction, minor, and consensus mechanisms shown in Fig. 3 [8].

A ledger can be defined as a data structure that is used to reserve different kinds of data.

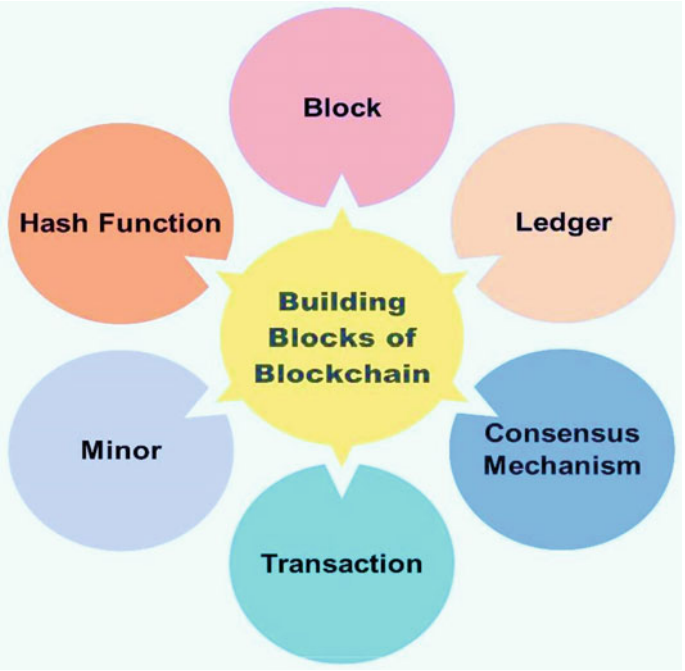

Fig. 3 Components of blockchain

A block is an essential part of the BC. Every block involves a bunch of exchanges.

The blocks were linked to one another by putting away a hash estimation of the preceding block in the recent block. These linked blocks create a BC.

The hash estimation is utilized to authenticate the data integrity. Fundamentally, it is a mathematical issue that minors must break to discover a block. The motivation to utilize this estimation is it's free from collision nature in due to which it is exceptionally difficult to make two indistinguishable hashes for two diverse computerized data. In this way, allocating hash estimation for every block can fill in as an approach to distinguish the block and validate the data inside it.

The transaction is the littlest unit of an activity or process wherein a bunch of transactions is joined and reserved in a block. It is not easy to add a certain transaction in the block except if most of the co-operating nodes in the BC network mark their assent. The transaction size is significant for minors because the compact transactions consume limited energy and are simpler to approve.

Minors are PCs/specialists that endeavor to tackle a tough numerical issue to investigate another block. Finding another block is begun by communicating fresh transactions to every node, and afterward, every node consolidates a bunch of transactions into a block and starts finding the POW of the block.

3 Highlights of Blockchain

3.1 Decentralization

BC is commonly a decentralized and distributed setup that depends on the P2P correspondence among distributed nodes. The decentralization empowers using the handling force of every partaking client, which diminishes inactivity and abolishes the single point of failure issue. This attribute of BC technology helps in resolving the issue of a single point of failure [9–13].

3.2 Transparency

Rather than the centralized system, in which the central server is taking care of the whole control and admittance to all information, BC provides a decent degree of transparency wherein all nodes approach every one of the subtleties of the transactions that consistently occurred in the network. Furthermore, a copy of the distributed ledger is provided to every node to keep updated with modifications. Likewise, the shortfall of an outsider expands business agreeableness and trust [14, 15].

3.3 Immutability

The most vital attribute of BC is the capacity of ensuring the transactions' integrity by delivering unchanging records. In the case of the centralized model, the integrity of data is just overseen and safeguarded by the central authority, and this leads to a threat. On the other hand, the Blockchain utilizes collision-free hash estimations to connect every block to the preceding block which keeps up the respectability of the content of the block. Furthermore, blocks stored in the ledger are changeless, just if the greater part of the clients affirms that change.

3.4 High Security

Contrast to the existing solutions, BC innovation gives better security. Using the public key, BC gives a safe environment contrary to different sorts of attacks. Additionally, the consensus mechanism gives a reliable strategy that upgrades the security of the BC. Moreover, the shortfall of the single point of failure in the BC innovation gives higher security as compared to the centralized architecture [16, 17].

3.5 Anonymity

Regardless of BC using a record that is dispersed among all clients, BC gives an anonymous identity to secure the privacy of a node. This attribute can be used to give a protected and private democratic framework [18, 19].

3.6 Cost Decrease

As compared to a centralized model wherein the high level and complete equipment and programming framework is needed to assemble the centralized server, the BC innovation diminishes the costs identified with fitting and supporting enormous centralized servers as it uses the processing power of imparting gadgets [20].

3.7 Autonomy

The capacity to settle on self-ruling choices is amidst the highlights that Blockchain innovation can give. It permits the assembling of new gadgets that can make intelligent and self-sufficient choices [21]. For example, BC highlights including carefully designed and better security can be utilized to assemble better and secure independent vehicles.

4 Integration of IoT & Blockchain

Blockchain was initially utilized for monetary exchanges and digital currency where exchanges are executed and put away by every in the BC network. At that point, Blockchain is incorporated in different spaces because of the colossal advantages it gives [9, 22]. IoT framework is among these spaces. Joining Blockchain with IoT can give innumerable advantages to different IoT applications as shown in Fig. 4 [11–13, 23].

Here is the layered architecture, at the perception layer all the gadgets like sensors, actuators collect the data from the surroundings and pass it to the network layer. The network layer performs routing due to which all the devices that are joined together can interact across the internet. The third layer enables all the features associated with Blockchain. At last, the application layer which is the topmost layer provides the users with the features of data visualization and helps them to make appropriate decisions based on the gathered data.

Additionally, in this segment, we present a study on some use cases in which Blockchain is deployed with the IoT ecosystem.

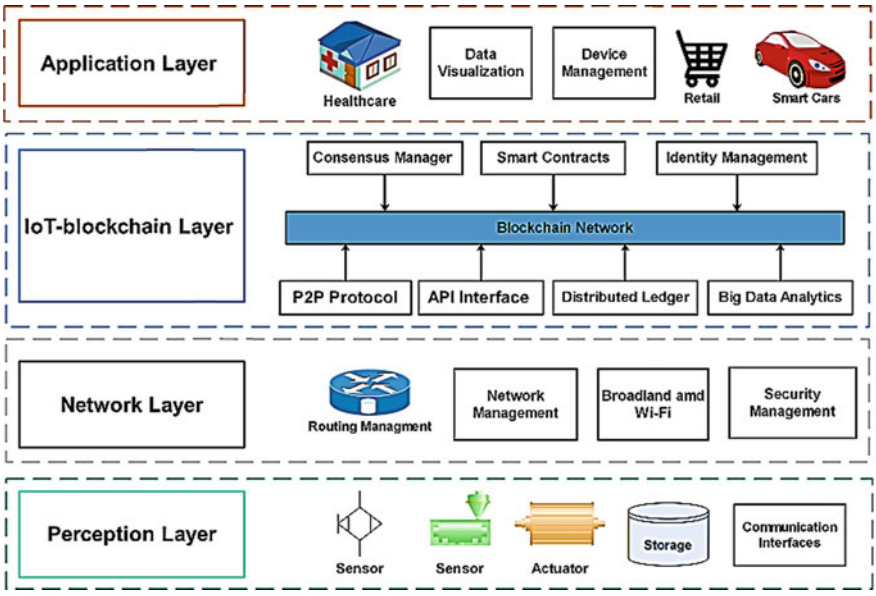

Fig. 4 Working of IoT with blockchain [21]

Oscar Novo addresses the scalability issue of overseeing access to a wide number of obliged gadgets in the IoT. Centralized frameworks come up short on the capacity to manage the increased load efficiently. The study presents another access management framework that resolves the problems related to dealing with various obliged IoT gadgets. The alternate is completely decentralized and dependent on BC innovation. Since most IoT gadgets are generally compelled to help BC innovation straightforwardly, the IoT gadgets in the proposed plan don't have a place with the BC network that makes the joining of the current IoT gadgets simpler to adjust to the proposed framework. The study gives a conventional, adaptable, and easily managed access control framework for IoT and implements a proof of concept (POC) model. All in all, the presented solution can adjust to different IoT situations affirming that Blockchain innovation can accept IoT innovation at its fullest [24].

Ali Dorri et al., design a lightweight BC-driven setup for IoT. This innovation essentially takes out the concerns of traditional BC, while keeping up the majority of its security and privacy advantages. IoT gadgets get an advantage from a private changeless log that acts like Blockchain yet is overseen centrally, to enhance energy utilization. The authors present a system that utilizes distributed trust to diminish the processing time of block validation. The methodology was investigated in a smart home [25].

Lei Hang and Do-Hyeun Kim proposed an incorporated IoT platform utilizing BC innovation to ensure observing data integrity. This designed framework aims to manage the cost of the gadget proprietor a useful application that gives an extensive, changeless record and permits easy access to their gadgets conveyed in various

spaces. It likewise gives qualities of general IoT frameworks takes into account continuous checking, and control among the end client and gadget. The presented system is upheld by proof of idea execution in practical IoT situations, using Raspberry Pi gadgets and Hyperledger Fabric. The examination outcomes demonstrate that the fabricated setup is well-suited for the resource-constrained IoT setup and is versatile to be stretched out in different IoT situations [26].

Aafaf Ouaddah et al. demonstrate how BC can be appealing to confront various emerging difficulties. The authors present FairAccess that utilize the consistency of BC innovation to oversee access control for the benefit of obliged gadgets. In this study, the authors introduced another applicability space of BC that is access control through the FairAccess system. The proposed system uses the consistency provided by BC-based cryptocurrencies to tackle the issue of centralized and decentralized access control in IoT. In FairAccess, a straightforward and strong access control tool are provided [27].

Yunfa Li et al. consolidate the IoT with the BC, utilizing the benefits of BC decentralization, high dependability, and minimal cost to move and reserve image information of the users safely. Taking into account the security concerns, a secure transfer and stockpile option are proposed for detecting the image. First and foremost, this option brilliantly senses user image information, and partitions the detected information into intelligent blocks. Also, various blocks are encrypted and conveyed safely using encryption algorithms [28].

Jaspreet Kaur et al. created decentralized architecture utilized from Blockchain innovation combined with a centralized cloud setup which is client/servers setup with a basic BC at back end uphold with smart contract application. This architecture is implemented by the authors, and it was shown that how this design forestalls data misuse by utilizing the working of BC without any need to run a BC node by the IoT gadgets. For an end client experience, it will have all the earmarks of being the same as an ordinary web application and from the developer's point of view, the smart contract service will have equivalent software design to recent web applications along these lines permitting a simple change for both of centralized and decentralized techniques, while as yet holding the trust of decentralization [29].

5 Deployment of Blockchain with IoT

The implementation of BC in the IoT framework is certainly not a simple assignment. The initial and significant step is to pick the BC platform that will be embraced to blend the IoT with BC innovation [16]. Some well-recognized platforms can be used to implement the BC with IoT [10]. Table 1 shows the comparison of such platforms.

Table 1 Various platforms for blockchain

Platform	Type of blockchain	Smart contract	Consensus
Ethereum	Public and Permissioned	Yes	PoS
Hyperledger	Permissioned	Yes	PBTF
IOTA	-	Yes	-
Multichain	Permissioned	Yes	PBTF
Litecoin	Public	No	Scrypt
Lisk	Public and Permissioned	Yes	DPoS
HDAC	Permissioned	Yes	ePOW
Quorum	Permissioned	Yes	Multiple

5.1 Ethereum

This platform is used for BC, and it was reported in 2013. It creates an all-inclusive platform for different BC-driven applications. It was chiefly founded to implement smart contracts, preserved on the BC forever, and empower executing clients' requests. Even though Ethereum depends on smart contracts, the exchanges can keep various sorts of information.

This amplifies the probability for audibility and permits powerful extensions for different IoT services. The downside of this platform is that it requires somewhere in the range of 10 and 20 s to transfer a block. A few investigations used Ethereum to coordinate Blockchain with IoT [30].

5.2 Hyperledger

This platform is open-source, and it was intended to assist cross-industry BC innovations. It is overall open-source cooperation including pioneers from various ventures. It is a permission BC. However, most of the distributed records license opens deployment; this platform elevates and upgrades security to stay away from different kinds of attacks.

Before the usage of smart contracts in this platform is chiefly founded on chaincode usage, it gives quicker execution between peers in a few milliseconds. Along these lines, receiving chain-code smart contracts gives a powerful strategy to deploy BC in IoT services. Hyperledger fabric is among the most well-known and generally used structures.

5.3 IOTA

IOTA isn't treated as a BC platform as it principally relies upon Tangle, which is also a distributed ledger innovation. One can characterize this as a decentralized platform that encourages and measures different exchanges among interacting gadgets across the Internet. Essentially, IOTA executes an organized non-cyclic outline of transactions rather than chained blocks of various transactions. This gives a few advantages, for example, it gives a lightweight arrangement as the agreement doesn't need most interacting nodes to favor distinctive raised exchanges, instead, and two transactions can be checked by one node presenting an exchange themselves. This diminishes the exchange time and burden [21].

A few highlights of IOTA just as the utilization of facilitated non-cyclic graphs make the most versatile executions of a distributed log, forming it a productive alternative and platform for IoT services. Numerous scientists used IOTA to give a proficient platform to IoT services.

5.4 Multichain

Multichain permits the formation and implementation of private Blockchains. It utilizes an API, which scale-up the core of the actual Bitcoin API with new working, permitting the management of permissions, transactions, etc. Additionally, it gives a command-line tool to communicate with the network and various users that can communicate via JSON-RPC with the network such as Node.js, Java, C #, and Ruby.

5.5 Litecoin

This platform is technically similar to Bitcoin, yet provides quicker transaction confirmation times and enhanced storage capacity. It also provides the reduced generation time of a block and PoW. Moreover, the computational needs of Litecoin nodes are fewer, hence it is well-suited for IoT.

5.6 Lisk

It gives a platform that supports the concept of sub-blockchains that can be described with decentralized BC services and an option of cryptocurrencies to utilize. This platform also provides support to fabricate and implement decentralized services inside the platform used by the end clients directly. The services developed may utilize LSK currency or may produce custom tokens. This platform makes use of delegated proof of stake consensus.

5.7 Quorum

Quorum is fabricated to give the financial services industry permission implementation of Ethereum with support for transaction and contract privacy. It permits more than one consensus mechanism and attains data privacy via cryptography and segmentation. Quorum was being used by chronicled to build secure connections among physical assets and BC.

5.8 HDAC

This BC-based platform is an IoT contract and M2M transaction platform. The HDAC framework uses a mix of public and private Blockchains, and it assures security of these exchanges by using quantum random number generation. The HDAC cryptocurrency-enabled public BC can be proficiently utilized with multiple private Blockchains.

6 Conclusion

The study offers a remedy for IoT data security using Blockchain technology. Security challenges will continuously be increasing, so there is an urgent requirement for a decentralized and secure innovation to overcome these hurdles. Both IoT and Blockchain technology change ideas and make additional opportunities, each in their separate situations and it is possible to make applications that can possess the attributes of both. The BC innovation promises the security of data, and the intruder is not able to control or feed false data without breaking the chain. This paper also discusses the implementation of Blockchain with IoT. The study presented some use cases where both the technologies were integrated to preserve data integrity and privacy, and also discuss various platforms that provide a solution for various security breaches.

References

1. Husamuddin MD, Qayyum M (2017) Internet of things: a study on security and privacy threats. In: IEEE conference paper
2. Vignesh R, Samydurai A (2017) Security on the internet of things (IoT) with challenges and countermeasures. Int J Eng Develop Res 5(1):417–423
3. Lo'ai Tawalbeh et al (2020) IoT privacy and security: challenges and solutions. MDPI Appl Sci 10:4102
4. Jari Porras et al (2018) Security in the internet of things–a systematic mapping study. In: Proceedings of the 51st Hawaii international conference on system sciences, pp 3750–3759

5. Chandra U et al (2020) Internet of things (IoT) in agriculture. Inf Stud 7(2):32–36
6. Kaur R et al (2020) Internet of things: architecture, applications, and security concerns. J Comput Theor Nanosci 17:2469–2475
7. Kaur R (2020) Blockchain based technique for improving data security on IOT server platform. J Interdiscip Cycle Res XII(IV):334–344
8. Fernández-Caramés TM, Fraga-lamas P (2018) A review on the use of blockchain for the internet of things. IEEE Access 6:32979–33001
9. Kshetri N (2017) Can blockchain strengthen the internet of things? IEEE IT Prof (19)4:68–72,
10. Kumar M, Kumar P (2018) Blockchain technology for security issues and challenges in IoT. In: International conference on computational intelligence and data science, pp 1815–1823
11. Zheng Z et al (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: IEEE 6th international congress on big data 2017, pp 558–564
12. Panarello A et al (2018) Blockchain, and IoT integration: a systematic survey. MDPI
13. Banerjee M et al (2018) A blockchain future for the internet of things security: a position paper. Digital CommunNetw 4:149–160
14. Reyna A et al (2018) On blockchain and its integration with IoT. Challenges and opportunities C. Future Gener Comput Syst 88:173–190 (Elsevier)
15. Sharma D et al (2020) Securing IOT communication using blockchain technology. Int J Adv Sci Technol 29(8):767–773
16. Pavithran D et al (2020) Towards building a blockchain framework for IoT, cluster computing. Springer Science+Business Media, LLC, part of Springer Nature 2020
17. Ahmad M et al (2018) IoT security: review, blockchain solutions, and open challenges. Elsevier Future Gener Comput Syst 82:395–411
18. WHunter G, Xu JC, Biaggi-Labiosa AM, Laskowski D, Dutta PK, Mondal SP, Ward BJ, Makel DB, Liu CC, Chang CW, Dweik RA (2011) Smart sensor systems for human health breath monitoring applications. J Breath Res 5:037111 (11pp)
19. Research article blockchain technology: is it a good candidate for securing IoT sensitive medical data? Article ID 9763937, Wiley Hindawi. Wireless Commun Mobile Comput 2018
20. Samaniego M et al (2016) Blockchain as a service for IoT cloud versus fog, In: IEEE international conference on internet of things and ieee green computing and communications and IEEE cyber, physical and social computing and IEEE smart data, pp 433–436
21. Atlam HF et al (2020) A review of blockchain in internet of things and AI, MDPI. Big Data Cogn Comput 4:28
22. Nguyen DC et al (2020) Integration of blockchain and cloud of things: architecture, applications, and challenges. IEEE Commun Surveys Tutor
23. Yaga D, Mell P, Roby N, Scrfone K (2018) Blockchain technology overview. National Institute of Standards and Technology Internal Report 8202
24. Novo O (2018) Blockchain meets IoT: an architecture for scalable access management in IoT. J Internet Things Class Files 14(8)
25. Dorri A et al (2017) Towards an optimized blockchain for IoT. In: IoTDI 2017, Pittsburgh, PA USA
26. Hang L, Kim D-H (2019) Design and implementation of an integrated IoT blockchain platform for sensing data integrity. MDPI Sensors 19:2228
27. Ouaddah A (2017) Towards a novel privacy-preserving access control model based on blockchain technology in IoT. Springer International Publishing, pp 523–533
28. Li Y et al (2020) A security transmission and storage solution about sensing image for blockchain in the internet of things. MDPI Sensors 20:916
29. Kaur J et al (2020) A blockchain-based solution for securing data of IoT devices. In: Yangui S et al (eds) ICSOC 2019 Workshops, LNCS 12019. Springer Nature Switzerland AG, pp 122–129
30. Xiang W, Atkinson I (2017) Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access