# The Amalgamation of Blockchain and IoT: A Survey


**Jignasha Dalal**

**Abstract** Blockchain, the form of Distributed Ledger Technology, is getting momentum. Data in the blockchain is in the form of transactions. Blockchains are transparent, immutable and auditable distributed ledgers with peer to peer connection, cryptography and consensus algorithm. All the parties involved have the same copy of data (transparency), data cannot be modified or deleted (immutability) and a full history of transactions is available (auditable). Based on history, future transactions are validated by all the parties (consensus). Internet of Things means connecting lightweight devices to share information among themselves and to enable some functionalities based on the shared information. This exchange of information among multiple devices must be secure as it contains sensitive and safety-critical data. Because of the scale and distributed nature of IoT, security and privacy are major concerns. Traditional security solutions are not suitable for IoT devices as they have limited resources in terms of memory and processing power. Blockchain can bridge the gap. The information exchange among these devices can be stored on the blockchain to increase transparency among the devices. This paper provides a review of literature in the area of IoT and blockchain.

**Keywords** IoT · Blockchain · Ethereum · Security · IOTA · Tangle

## 1 Introduction

A blockchain is a distributed, peer to peer, immutable, append-only ledger where all the transactions are visible to all the parties. Transactions can be in the form of currency, land records, patient records, Personal Identifiable Information (PII) and so on. The transactions are grouped into blocks and blocks are cryptographically linked. These chains of blocks grow continuously as the number of transactions grows. The Blockchain is stored on all the nodes and all nodes required to validate

J. Dalal (✉)
K. J. Somaiya Institute of Engineering and Information Technology, Mumbai University, Mumbai, India
e-mail: jignasha@somaiya.edu

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

P. K. Singh et al. (eds.), *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*, Lecture Notes in Networks and Systems 203,
https://doi.org/10.1007/978-981-16-0733-2_55

**Table 1** Distributed database versus distributed ledger

| Distributed database | Distributed ledger |
|---|---|
| Data can be deleted or modified by authorised parties | Data cannot be deleted, modified by any of the parties involved |
| Data can be added anywhere by the authorised party | Data can be appended only after verification by all the parties |
| Client–server architecture | Peer to peer architecture |

the transactions so that they can agree on a single global state. This is done through a Consensus algorithm. Blockchains also provide a way to store logic. This is done through Smart Contracts. Smart contracts are the executable program codes which are triggered by some events. They are similar to traditional contracts in the real world. There are three kinds of blockchains: (i) Public or Permissionless, where anyone can join the blockchain, (ii) Consortium or permissioned, where only authorised parties can join the blockchain and (iii) Private with centralized authority. The difference between Distributed ledger and Distributed database is shown in Table 1.

IoT is the seamless interconnection of heterogeneous devices to provide services in the sectors of social media, businesses, intelligent transports and smart cities. These connected devices generate a huge amount of data traffic. The sensitivity of the data depends on the application where IoT is used. The security of this data while in storage and in the transmission is very important. Blockchain provides immutability, transparency, auditability and decentralization. The security of the shared data among the devices can be significantly improved using Blockchain. Ferrag et al. [1] provided a detailed overview of Blockchain usage in various application areas of IoT. They have also shown when to use Blockchain model for IoT applications. When there is a peer to peer communication among the devices, synchronization is needed among the devices and no centralized server, then Blockchain technology can be incorporated with an IoT application. They also classified the IoT applications in different domains like the Internet of Vehicles, access management, Internet of cloud, SDN, Edge Computing, Distributed P2P applications, Data Storage, etc. and provided the overview of existing applications with Blockchain in these domains. They analysed vulnerabilities in Blockchain and how those vulnerabilities are applicable in Blockchain-IoT applications. They provided a detailed analysis of security and privacy for Blockchain-based IoT applications.

In the existing IoT applications, most devices are connected through the central server. The central server becomes a single point of failure. Blockchain can bring decentralization and also can help in transferring the value of massive IoT data. Yu et al. [2] suggested a 3-layer distributed network architecture with PBFT-DPOC consensus algorithm. The Network architecture consists of DAPP layer, Blockchain layer and the intelligent device layer. To reduce the pressure on devices with limited resources they have used DPOC (Delegated Proof of Contribution) consensus algorithm. This algorithm shows better throughput than consensus algorithm used in

Bitcoin and Ethereum. Lo et al. [3] did a systematic literature review for incorporating Blockchain in IoT applications. They identified some challenges in the IoT domain. The challenges are:

- Lack of standards
- Limited bandwidth and computation capability
- The integrity of states of devices
- Interoperability among devices.

They analyzed different solutions addressing the above challenges and found some interesting insights:

- Most of the solutions were tested in the test net.
- During the testing, very few devices were connected.
- Some tests have used Ethereum test nets which are using Proof of Authority consensus algorithm.
- Public Blockchain like Ethereum is not suitable for IoT as latency is very high, throughput is less and also transaction fees are involved.
- Permissioned Blockchains with PBFT are more suitable for IoT.
- The performance should be analysed for the whole process starting from transaction submission to transaction confirmation.
- IOTA means "small". It is specifically designed for incorporating Blockchain concept in IoT applications. But it suffers from 33% attack. Bitcoin and Ethereum suffer from 51% attack.

Casino et al. [4] presented an in-depth analysis of applications using Blockchain technology. The IoT is a domain where the use of Blockchain can bring a revolution. For Blockchain to be used with IoT applications to make it more transparent and secure, Blockchains need to be scalable, privacy-preserving and must have low latency. Various consensus algorithms are developed to increase scalability. For IoT applications, it is also needed to reduce resource consumption. Kumar and Jain [5] have proposed a PoG (Proof of Game) consensus algorithm. Multi-round and Multi-bit challenges are more suitable for the devices with limited resources to confirm the Block in stipulated time.

The contributions of this paper are as follows:

1. This paper reviews different IoT domains where Blockchain can be incorporated. It also discusses the challenges associated with the implementation of Blockchain in these domains.
2. The paper also reviews the IOTA (means small), a DAG-based, fee less Blockchain architecture and how it is suitable for incorporating with IoT devices.

The paper is organized as follows: Sect. 2 reviews the research work in different IoT domains with Blockchain. The domains are Access Control, Blockchain, IoT and Machine learning, Data storage and sharing, Health, Supply Chain and VANETs. Section 3 provides Analysis and Summary of the literature review and Sect. 4 concludes the paper.

## 2 IoT Domains

### 2.1 Access Control

In IoT, devices need to share their resources with other IoT devices. They need to have the local policy which defines who can access their resources. But the devices have limited storage to define these access management policies. If the devices are static, they can be managed with a centralized server where access policies are stored and defined. In the case of dynamic IoT scenario, where IoT devices are mobile and joining and leaving any time, access management cannot be done with a centralized server. Novo [6] has suggested an access management system with Blockchain. In his system, IoT devices do not write any information on the blockchain, so high latency problem with Blockchain is not present here. Instead, IoT devices read access control information from the Blockchain. Read operation from Blockchain system is inexpensive as it does not require consensus. The set of IoT devices need to register with a manager who is responsible for interacting with Blockchain. The manager can be a single point of failure. The Ethereum Blockchain with a single smart contract is used for defining access control policies. The agent node is the node on the blockchain. A service provider can act as an agent node and the owner of IoT devices can act as a manager node. Then the system has been compared with existing centralized IoT access management systems. The proposed system provides good scalability.

IoT devices are needed to share data with external parties. These external parties must have proper authorisation to access the data. Traditional access control schemes do not work in constrained IoT environment. Attribute-based access control is more appropriate for IoT [7–10]. Fully decentralization systems are not possible, even with Blockchain. Permissioned Blockchain requires all the participants to be authenticated before joining the network. In the dynamic IoT environment, when IoT devices are joining and leaving the network any time, they need to get authenticated each time they connect to the network. The authentication of the participant is done by some central authority.

### 2.2 Blockchain, IoT and Machine Learning

Combination of Blockchain, IoT and Machine learning can be a great solution to Industrial IoT. Liu et al. [11] suggested the use of Deep Reinforcement Learning (DRL) and private Ethereum blockchain for Industrial IoT data storage and sharing. The smart portable mobile terminals (MTs) include smartphones, UAVs with sensors, cameras, gyroscope and GPS. The system is suggested for Industrial IoT environment like a manufacturing plant. The deep learning technology is used for efficient collection of data and Blockchain is used for securely storing and sharing the data. The MTs move around the plant and collect data and they submit this data to the

Blockchain node in the form of transactions. To prevent the malicious behaviour of MTs, a Certificate Authority (CA) is used to verify the authenticity of MTs and data submitted by them. The system is tested against malicious behaviour of MTs, Eclipse attack and majority attacks. The system provides better security than a traditional centralized database.

The system is not fully decentralized as it is using the CA. the private Ethereum network is set up, but the roles of a network user are not specified. DRL is a combination of traditional reinforcement learning and deep learning. Smart cities are using IoT in the areas of transportation, energy distribution, security, manufacturing and agriculture. These IoT systems generate a huge amount of data and processing this huge amount of data efficiently and fruitfully is a big challenge. Machine learning can help with the classification of data. One of the classification methods is SVM (Support Vector Machine). This classifier needs training data for the classification. As the size of the training data grows, the accuracy of classification increases. It is difficult to get such a huge training data from one entity. The solution is to combine the data from multiple entities. The entities are reluctant to share data because of privacy (in health care), ownership and trust. Shen et al. [12] suggested SVM based training on Blockchain-based encrypted data. IoT data providers encrypt the data collected from the IoT devices and store it on the Blockchain. The analyst process and analyse encrypted data. The Paillier cryptographic system is used for this purpose. It is an additive homomorphic encryption technique which works on encrypted data. The security and efficiency of the system were evaluated using different experiments. The system can be extended for other classification models.

The combination of IoT, Blockchain and ML makes it possible to analyse and perform an audit of the IoT data.

## *2.3 Data Storage and Sharing*

Zhou et al. [13] suggested a Blockchain-based threshold IoT system Beekeeper. The system consists of servers, devices and a leader. Devices send encrypted data to the server,the server will perform homomorphic computations on encrypted data and sends back the results. The leader will have the decryption key and will be able to decrypt the result. All the communication among the participants is done through Blockchain. The record nodes manage the Blockchain. The beekeeper was tested on Ethereum Blockchain. In this system, IoT devices need to perform cryptographic computations and it is not feasible. So, Edge Computing/fog computing is introduced to reduce the computational load on IoT devices [14–18]. Hyperledger Fabric and Ethereum were used as Blockchain platform. Edge devices are placed in the same network as IoT devices. They help IoT devices to perform cryptographic computations.

Wang et al. [16] proposed a hierarchical Blockchain architecture called CHAIN SPLITTER. The old blocks are stored on the cloud and only a few recent blocks are

stored on the IoT devices. A centralized database is used in the local IoT network to store all the data in the local network.

Data storage and sharing of IoT data on Blockchain can provide transparency, immutability and auditability. It also provides decentralization, so there is no single point of failure. Full Decentralization is not possible, somewhere you will have some kind of central authority to verify the authenticity of the devices and validity of the data.

IoT devices generate a huge amount of data at very high speed. Cloud computing is the solution to process this large amount of data as IoT devices have limited storage and computational abilities. Transmitting such large data to centralized cloud servers at very high speed through the Internet is expensive and not secure. Sharma et al. [19] proposed a software-defined fog node based distributed cloud architecture to solve the cost and security issue with centralized cloud-based architecture. The fog node is a collection of SDN controllers with Blockchain. This architecture ensures high security, real-time deliveries, High scalability and low latency. The performance of the system is better than the traditional centralized cloud architecture.

Pan et al. [20] suggested an architecture EDGECHAIN which combines IoT, edge computing and Blockchain. A permissioned Blockchain is used for resource allocation to IoT devices from the Edge computing resources. All the IoT devices transactions and activities are stored on the Blockchain, which will help to analyse and audit the behaviour of IoT devices. Edge chain is placed between centralized cloud services and IoT devices. It does resource management for IoT devices as they are resource-constrained. Edge chain processes the massive data generated from IoT devices and only processed output is sent to the cloud servers.

Peña and Fernández [21] suggested an IoT architecture SAT-IOT consisting of different entities to manage data flow from IoT devices. In the case of dynamic IoT environment, the topology management entity will manage the topology of the IoT devices. The IoT visualization entity is incorporated to get the visual of the IoT system. The concept "Edge-Cloud Computing Location transparency" lets computation nodes, in an IoT network topology change dynamically (without administrator intervention) to fulfil the efficiency criteria defined for the IoT system. The "IoT Computing Topology Management" concept integrates the hybrid networks (cloud, edge, devices and their wireless or wired links) as part of the IoT Platforms. This gives an IoT system global view, from the hardware and communication infrastructures to the software deployed on them. The Embedded IoT Visualization System concept offers a mechanism to check the deployment of the new IoT system in the platform.

Guo et al. [22] have suggested a Blockchain-based Edge computing system to improve the efficiency of authentication in the IoT system. An optimized PBFT algorithm is designed and used in the Blockchain. A distributed authentication system based on name resolution strategy and Elliptic curve cryptography is used. To reduce delay a caching mechanism is introduced. The 3-layer architecture consists of the Physical layer, Blockchain edge layer and Blockchain node layer. In optimized PBFT algorithm, there is one speaker and other peers are congressmen. Speaker runs the consensus process for other peers. Each round a speaker is selected by the peers.

Speaker sends pre-prepare messages to the congressmen and if congressmen agree, they send prepare messages to the speaker. If the speaker receives prepare messages from $2f + 1$ peer, where $f = \mid (N - 1) /3 \mid$, the speaker sends commit messages to all the peers. When it receives the response from the $f + 1$ peer, the consensus is achieved. Caching strategy minimizes the download latency.

Lei et al. [23] have proposed GROUP CHAIN—a 2 level chain to enhance the performance of Blockchain in IoT architecture. There is a group chain and vice chain. The group chain contains the leaders who can generate vice blocks without PoW. Miners compete for membership in the leader group using PoW. Once the leaders are selected, they can generate any number of vice blocks without PoW, which is added to the Vice chain after getting a signature from all the leaders. This enhances the Bitcoin mining mechanism. The leader is required to deposit some amount, if it behaves honestly during an inspection period, the deposit will be refunded. This will prevent the leader from signing invalid transactions and creating a denial-of-service attack by generating vice blocks continuously.

IoT devices are resource-constrained. They generate massive data which need to be processed and analysed. The processing and transmission of data need an infrastructure along with IoT devices. This infrastructure can be a centralized cloud computing architecture, where the data from IoT devices are stored and processed. But transmitting data to the centralized data servers through the internet is expensive and makes data vulnerable. The data generated by IoT devices contain sensitive information most of the time. So, the concept of fog computing/edge computing is being used where the processing and computation devices are at the edge of the IoT devices' network. These edge devices form an edge network and they facilitate IoT devices with authentication, access control, information sharing, and passing the processed information or computation to cloud servers. It is possible to use Blockchain in edge computing layer and even in cloud computing layer to make the processing, computing and sharing of the data more transparently and securely. Most of the research has used permissioned Blockchain. This combination of edge computing and blockchain with IoT can help in developing many real-life applications for smart cities and industries.

## *2.4 Health*

Kumar et al. [24, 25] proposed a smart health care system based on Ethereum Blockchain. The authors have given a comprehensive review of existing healthcare systems with blockchain. There are separate Blockchains for Doctor, supplier, patient, hospital, staff and insurance. These Blockchains are integrated into one smart healthcare blockchain. It is a full-fledged and comprehensive healthcare system. Kumar et al. [24, 25]] have proposed three PoG based consensus algorithms for wearable kidney devices. The authors also reviewed the existing consensus algorithms and their limitations for using them in implementation of IoT based application with Blockchain.

Xu et al. [26] have suggested HEALTHCHAIN, a Blockchain-based healthcare data privacy-preserving scheme. In the scheme, the patient medical data is encrypted. Patients have the right to revoke or grant access to their medical data. It is not advisable to store the full patient's health data on the Blockchain. So, the patients' health data is stored on the Interplanetary File System (IPFS) in encrypted form. It does not have a central server. The file is stored on different peers in parts. A unique hash string is associated with each file. This hash is stored on the Blockchain. There are two chains involved, Userchain and Doc chain. Userchain is a public Blockchain and Docchain is consortium Blockchain. Encryption keys and encrypted data are separated to achieve flexibility in key management.

Miners in the Blockchain need continuous power for mining. Mobile IoT devices request microgrids to supply power to them. Miners also can request nearby MECs to compute the hash for the mining. These MECS need the power to compute the hash on behalf of miners. Microgrids can provide efficient energy allocation. Li et al. [14, 15] proposed a microgrid based energy supply system for powering IoT mobile devices for mining computation. The microgrids provide real-time scheduling and decision making based on the energy consumption of miner. The energy allocation is formed as a Stackelberg game to optimize the profit for microgrids and cost-effectiveness for miners.

## *2.5 Supply Chain*

There are multiple participants involved in supply chain management. Blockchain can bring transparency and create trust among these participants. Tsang et al. [27] have proposed a Blockchain-based IoT system with fuzzy logic to ensure the Traceability and quality of food by assessing the shelf life of perishable food. The system combined cloud technology and blockchain technology and fuzzy logic. They are using the concept of Blockchain vaporization to increase the efficiency of the system. For a particular batch of food, batch id, container id and IoT id are stored on the Blockchain. One the batch of food reaches the endpoint or deal is completed, this data will be removed and stored on the cloud for future reference. The data from the blockchain is used as input to the fuzzy evaluation technique for quality assessment.

## *2.6 VANETS (Vehicular Adhoc Networks)*

The modern transportation system is intelligent as it incorporates IoT devices with internet connectivity. 5G technology will reduce latency and increase throughput. SDN (Software Defined Network) simplifies the management of IoT devices in the vehicle and also of VANETS. Security and privacy are very important for VANETS. Incorporating Blockchain in VANET will help to achieve the security and privacy in VANET. Xie et al. [28] have proposed a 5G-SDN enabled Blockchain base system for

VANETS. All vehicles and base stations are involved in maintaining the Blockchain. Each vehicle is assigned an ID. The vehicle is required to collect the videos and images of road conditions and broadcast it to other vehicles and base stations. This data will help the SDN controller to monitor the position of the vehicle and also helps in traffic management. SDN controller is the centralized system which is responsible for all kinds of policies. The message sharing among the vehicles is maintained on the Blockchain to detect malicious nodes. It is not possible to avoid malicious nodes. To detect them is the only solution. In case of an accident, the transactions on the Blockchain can be checked and originated vehicle ID can be identified. Vehicle Id does not reveal any information about the vehicle owner. The mapping between Vehicle ID and Vehicle Number is stored in the DMV database.

Zhang et al. [29] have proposed architecture of VANET using blockchain and Mobile Edge Computing (MEC). It has three layers-Service layer, Perception layer and Edge computing layer. The blockchain is used in Perception layer and Service layer to ensure the security of data transmission and security of data respectively. All vehicles will run wallets and Perception layer will perform the tasks of blockchain. All vehicles will be able to communicate with the blockchain in Perception layer.

## 3 Analysis and Summary

The paper has provided a detailed literature review of recent research in IoT and Blockchain. The Summary of IoT domains with Blockchain Technology is shown in Table 2. The major challenges in incorporating IoT systems in daily life and industry are:

(i) Massive data generation by IoT.
(ii) Storage and security of the data.
(iii) Configuration and management of IoT data.
(iv) Detection of malicious Behaviour.
(v) Defining and applying Access control policies for inter-device communication and external request.

Incorporation of Blockchain with IoT has great advantages. It can provide decentralization, improve the performance and increase the security of IoT system. Massive data storage problem can be solved by using cloud storage, but centralized cloud storage is inefficient in terms of transmission, processing of data and real-time delivery of data. It is also a single point of failure. Edge computing along with cloud storage is a better solution. Blockchain can be incorporated in the Edge computing layer to record the data exchange between cloud and IoT devices as well as the sharing of the data with other devices or external entity.

It is seen from Table 2 that a High throughput and low latency Blockchain platform is needed to make the real implementation of IoT with Blockchain. All proposed systems are developed on Ethereum and Hyperledger Fabric. Hyperledger Fabric

**Table 2** IoT Domains and Proposed Systems using Blockchain

| IoT domain | Requirements | Proposed systems |
|---|---|---|
| Access control | Low read latency | ACL is stored on the blockchain, the device only needs to read ACL |
| Blockchain, IoT and machine learning | Data storage, high throughput, low write latency | Blockchains are not designed to store data. Use ethereum and hyperledger fabric |
| Data storage and sharing | Low read latency, high throughput | Edge devices are used to reduce computational load on IoT devices |
| Health | Data storage, high throughput, Low write latency, scalability | PoG based consensus algorithms are used. Multibit and Multi round challenges are more suitable for IoT devices. IPFS is used for storing private data |
| Supply chain | Low read and write latency, high throughput, Scalability | Hyperledger fabric and ethereum are used |
| VANETS | Low read and write latency, High throughput, scalability, data storage | Involves real-time transactions |

uses PBFT (Practical Byzantine Fault Tolerance) consensus algorithm, which is not scalable. For VANETs, a high throughput and low latency blockchain is must as they involve real time transactions and high latency transactions may have serious consequences. For small scale IoT system, Hyperledger Fabric is suitable. But for industry level IoT system, a scalable Blockchain platform is needed.

Ethereum is a public Blockchain and transaction fees are involved [9, 10, 30]. Transactions are grouped into the block and blocks are added by the miners. Confirmation of transaction takes at least six-block times and it consumes a lot of energy as Proof of Work algorithm is used. These problems can be solved by using DAG-based blockchain architecture. IOTA is DAG-based Blockchain. Transactions are arranged as the vertices of DAG and each new transaction needs to approve two old transactions [31]. It is a feeless architecture. The latency is very low and throughput is high compared to Ethereum. It is a public Blockchain and Highly scalable.

## 4 Conclusion

Combining IoT and Blockchain is rewarding in terms of transparency, privacy and security. But real-time implementation has many challenges. Most of the proposals, models and architectures suggested are Proof of Concept. They are not tested in the

real environment. Majority of implementations are based on Ethereum and Hyperledger fabric. Hyperledger Fabric is suitable for small scale IoT system. To increase the efficiency and performance of the IoT system new Blockchain architectures need to be examined. DAG-based architecture IOTA can be an alternative to Ethereum for IoT implementation.

## References


1. Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H (2019) Blockchain technologies for the internet of things: research issues and challenges. IEEE Internet Things J 6(2):2188–2204
2. Yu S, Lv K, Shao Z, Guo Y, Zou J, Zhang B (2018) A high performance blockchain platform for intelligent devices. In 2018 1st IEEE international conference on hot information-centric networking (HotICN), pp 260–261. IEEE
3. Lo SK, Liu Y, Chia SY, Xu X, Lu Q, Zhu L, Ning H (2019) Analysis of blockchain solutions for IoT: a systematic literature review. IEEE Access 7:58822–58835
4. Casino F, Dasaklis TK, Patsakis C (2019) A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Inform 36:55–81
5. Kumar A, Jain S (2019) Proof of Game (PoG): a game theory based consensus model. International conference on sustainable communication networks and application. Springer, Cham, pp 755–764
6. Novo O (2019) Scalable access management in IoT using blockchain: a performance evaluation. IEEE Internet of Things J 6(3):4694–4701
7. Ding S, Cao J, Li C, Fan K, Li H (2019) A novel attribute-based access control scheme using blockchain for IoT. IEEE Access 7:38431–38441
8. Islam MA, Madria S (2019) A permissioned blockchain based access control system for IOT. In: 2019 IEEE international conference on blockchain (blockchain). IEEE, pp 469–476
9. Liu H, Han D, Li D (2020) Fabric-IOT: a blockchain-based access control system in IoT. IEEE Access 8:18207–18218
10. Liu Y, Hei Y, Xu T, Liu J (2020) An evaluation of uncle block mechanism effect on ethereum selfish and stubborn mining combined with an eclipse attack. IEEE Access 8:17489–17499
11. Liu CH, Lin Q, Wen S (2019) Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning. IEEE Trans Ind Inform 15(6):3516–3526
12. Shen M, Tang X, Zhu L, Du X, Guizani M (2019) Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. IEEE Internet of Things J 6(5):7702–7712
13. Zhou L, Wang L, Sun Y, Lv P (2018) Beekeeper: a blockchain-based iot system with secure storage and homomorphic computation. IEEE Access 6:43472–43488
14. Li R, Song T, Mei B, Li H, Cheng X, Sun L (2019a) Blockchain for large-scale internet of things data storage and protection. IEEE Trans Serv Comput 12(5):762–771
15. Li J, Zhou Z, Wu J, Li J, Mumtaz S, Lin X, Gacanin H, Alotaibi S (2019) Decentralized on-demand energy supply for blockchain in internet of things: a microgrids approach. IEEE Trans Comput Soc Syst 6(6):1395–1406
16. Wang G, Shi Z, Nixon M, Han S (2019) Chainsplitter: towards blockchain-based industrial iot architecture for supporting hierarchical storage. In: 2019 IEEE international conference on blockchain (blockchain). IEEE, pp 166–175
17. Truong HTT, Almeida M, Karame G, Soriente C (2019) Towards secure and decentralized sharing of IoT data. In 2019 IEEE international conference on blockchain (blockchain). IEEE, pp 176–183

18. Bajoudah S, Dong C, Missier P (2019) Toward a decentralized, trust-less marketplace for brokered IoT data trading using blockchain. In: 2019 IEEE international conference on blockchain (blockchain). IEEE, pp 339–346
19. Sharma PK, Chen MY, Park JH (2017) A software defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access 6:115–124
20. Pan J, Wang J, Hester A, AlQerm I, Liu Y, Zhao Y (2019) EdgeChain: an edge-iot framework and prototype based on blockchain and smart contracts. IEEE Internet of Things J 6(3):4719–4732
21. Peña MAL, Fernández IM (2019) SAT-IoT: an architectural model for a high-performance fog/edge/cloud IoT platform. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, pp 633–638
22. Guo S, Hu X, Guo S, Qiu X, Qi F (2019) Blockchain meets edge computing: a distributed and trusted authentication system. IEEE Trans Ind Inf
23. Lei K, Du M, Huang J, Jin T (2020) Groupchain: towards a scalable public blockchain in Fog computing of IoT services computing. IEEE Trans Serv Comput 13(2):252–262
24. Kumar A, Krishnamurthi R, Nayyar A, Sharma K, Grover V, Hossain E (2020a) A novel smart healthcare design, simulation, and implementation using Healthcare 4.0 processes. IEEE Access 8:118433–118471
25. Kumar A, Kumar Sharma D, Nayyar A, Singh S, Yoon B (2020b) Lightweight Proof of Game (LPoG): A Proof of Work (PoW)'s extended lightweight consensus algorithm for wearable kidneys. Sensors 20(10):2868
26. Xu J, Xue K, Li S, Tian H, Hong J, Hong P, Yu N (2019) Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things J 6(5):8770–8781
27. Tsang YP, Choy KL, Wu CH, Ho GTS, Lam HY (2019) Blockchain-driven IoT for food traceability with an integrated consensus mechanism. IEEE Access 7:129000–129017
28. Xie L, Ding Y, Yang H, Wang X (2019) Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs. IEEE Access 7:56656–56666
29. Zhang X, Li R, Cui B (2018) A security architecture of VANET based on blockchain and mobile edge computing. In: 2018 1st IEEE international conference on Hot Information-Centric Networking (HotICN). IEEE, pp 258–259
30. Wood G (2014). Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151(2014):1–32
31. Gal A (2018) The tangle: an illustrated introduction. Retrieved from https://blog.iota.org/the-tangle-an-illustrated-introduction-4d5eae6fe8d4