Blockchain Based Edge Information Systems Frameworks for Industrial IoT: A Novel Approach

M. Parimala Devi, Mani Deepak Choudhry, R. Nithiavathy, G. Boopathi Raja, and T. Sathya

1 Introduction

To bridge the gap between the physical and digital environment, an intellectual milieu is rendered for the different sector to reduce the cost of production by using IoT, which are capable of sensing and communicating over the Internet [1]. IoT can be habiliment, automated device growing in numbers; the immense volume of data is congregated, managed effectively. IoT is a networked device that communicates to progress the upcoming applications transversely in all domains. In IoT, security becomes a significant apprehension as it deals with huge data from various domains and services [2, 3]. Early the IoT was in data processing and storage in the cloud environment, it deployed in the healthcare sector, industries who were involved in manufacturing monitored [4]. There are security breaches and time sensitivity in the IoT data process as the number of systems interconnected. Lately, blockchain technology is advanced, which is capable of handling applications that may assimilate peer-to-peer distributed storage and encryption along with various technologies.

The main fundamental technology of block chaining is digital currency, such as Ethereum and Bitcoin [5]. The decentralized system is a prime solution of the trust among the nodes by consent and verification of nodes [6]. Blockchain includes

M. Parimala Devi (✉) · G. Boopathi Raja · T. Sathya
Department of ECE, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India

M. D. Choudhry
Assistant Professor, Department of Information Technology, KGiSL Institute of Technology, Coimbatore, Tamil Nadu, India

R. Nithiavathy
Department of Computer Science & Engineering, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

S. Misra, A. Kumar Tyagi (eds.), *Blockchain Applications in the Smart Era*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-89546-4_2

confidentiality in the transaction with security, suitability, invariance of data, and fault tolerance widely used in finance, transportation, and encryption technology, etc. [7–14]. The democratization of the network of things and the IoT system is emphasized in blockchain by some companies such as IBM [15–17]. There is no need for third party in IoT, where the blockchain by itself proposes storage distribution and generation of data that are recorded in an incontrovertible and certifiable manner [18].

All the action traced in the IoT network, which is triggered according to the timestamp decision to fulfill the governing acquiescence and operations in the system. The IoT transactions are secure in sharing the data, and the blockchain yields steady and trustworthy environment. Though the blockchain and IoT are emerging technologies, there are deficiencies in approaches which consider management of data, and its provision in the architectural design results in developing IoT blockchain system. The chapter flow in the next section describes the work carried out to understand different blockchain systems for industrial IoT. The following section of related work deals with an approach or framework that solves the current issues and challenges posed. The final section of the chapter deals with the experimental results and concluding remarks.

2 Related Works

With limited use of memory, battery resources, and computing proficiencies, sensors and actuators are the Internet of Things including mobiles, home appliances, and vehicles that are connected in the network of devices where the data are collected and exchanged for an application such as in the medical field, industries, transport, etc. [19–21].

For usage of a huge volume of data, they use cloud servers as a centralized system, which leads to high latency and bandwidth ingesting in the network. The data manipulation, e.g., altered and interfered by outsiders, in the cloud leads to a security breach of sensitive and vital information stored in the cloud storage [22].

The issue in the trust information system proposed by Satoshi Nakamoto [5] provides two perceptions: Bitcoin and blockchain. A bitcoin maintains value without the entity of financial centralized authority. The coin is held by a decentralized peer-to-peer network with actors where they validate. Blockchain is a mechanism that involves transaction monitored by actors. It holds an auditable ledger that is translucent, absolute, and protected. The blockchain protocol assemblies the data in a chain of blocks, where each one of the blocks holds a set of Bitcoin dealings completed at a specified time. Blocks are related and organized by a reference to the preceding block, creating a chain. To fund and activate the blockchain, system peers have to deliver the below functionality wallet services and mining routing technique and storage space [6].

Using the blockchain technology and the manufacturing controller system leads to lowering the cost of the process, resources supervision, and vigorous use, thereby avoiding threats and attacks. A peer-to-peer network is established by blockchain, which allows to share the maintainable cost by allocating the storage and computing needs in a centralized cloud. There is a problem in communication at a single point of a fiasco. This can be addressed by IoT working along with block chaining to maintain privacy using encryption algorithms. A tamperproof ledger [23] is used to resolve the dependability issue in the Internet of Things. Arisas et al. have highlight confidentiality, safekeeping, and performance issues in employing the blockchain technology in IoT [24].

For the cyber-physical social services, a cloud-based framework focuses on the trust mechanism and optimized performance by employing blockchain along with IoT applications [25]. A structured network that is heterogeneous allows data protection from information processing and communication protocol through sensors [25, 26]. There are some delay and issues in access control in a distributed manner to handle the classified information. To afford substantiation and secrecy, IPsec along with TLS is used, where it does not satisfy all requirements such as computing devices with limited resources and high cost. To the above problem, the solution is done by block validation along with the consent methods, but for complex blockchain it is difficult. They did, however, build on the constraints of recollection and computational features, power, and industrial Internet submission obligations to cloud computing in data layer management.

For example, we can take food safety guarantee by tracing the various food products which involve many members like a producer, nourishing, handling, circulation, etc., when there is an intruder or a break the chain in part of the blockchain leads to data leak results in slow down the process of finding out infected part may affect the lives of people, economical fall in markets in the circumstance of foodborne outburst [27]. A healthier regulator in these zones would surge food safety, cultivating the data distribution among contestants and dropping the exploration time in the case of a food-borne outbreak, which will save a lot of lives. The usage of blockchain technology and IoT deals with secure and reliable data. Together, the IoT and blockchain are implemented in smart cities, cars, etc. by adding new members in the environment and providing better-quality services and their adoption [28]. Scalability, confidentiality, and consistency problems related to the IoT paradigm can be tackled by blockchain technology. Combination of IoT and blockchain yields the following scalable decentralization, moving the central construction to P2P by eliminating the vital reason for failure and bottleneck [29]:

- **Uniqueness:** Using mutual blockchain system, members can recognize all solitary devices. Statistics provide and feed the scheme, which is absolute and uniquely classifies definite data that was provided by a device. Furthermore, blockchain can offer reliable circulated confirmation and agreement of devices for IoT applications [30].
- **Self-sufficiency:** Blockchain technology provides future application features, manufacture conceivable the growth of smart independent assets and hardware as a facility [29, 30].

- **Services:** The construction of an IoT network of facilities and data marketplaces can be hastened by blockchain, where communications among peers are plausible without authorities. Microservices can be simply positioned, and micro-payments can be made with full protection in a faithless environment [31–33]. Protected code positioning: enchanting the benefit of blockchain secure-immutable storage, encryption can provide security devices [27, 34].

The benefits of blockchain and the benefits of current IoT communications, such as fog computing, can be leveraged to balance the confines of blockchain and the IoT. For example, fog computing comprises rarer computational partial strategies such as gateways and where mining is done similarly as enterprises that employ IoT [35, 36].

Today's manipulators can necessitate many benefits using blockchain in several applications, i.e., using shared infrastructure while maintaining a level of security and privacy in a system. It makes blockchain unique, but creating blocks using the blockchain concept comes not easy; it requires a lot of mathematical and cryptographic operation [37–39]. It also requires a lot of time to compute such an operation. This is a disadvantage of this novel concept. Cybersecurity is also playing an important role in industrial IoT [40, 41], and the need for recent techniques for ICT was explained well [42].

3 Novel Tier-Based EIS Framework of Blockchain for Industrial IoT

Internet of Things (IoT) is a pioneering, novel, and groundbreaking computing model, which empowers every device (IoT) with communication, computation, and storage competence to link traditional Internet. IoT applications are found in various fields since it is a massive field. IoT devices in the healthcare sector reside on the patient interact straight to the healthcare organization through a communication network. These IoT devices unceasingly diffuse substantial information to the healthcare organization, such as blood pressure and heart rate. In the transportation domain, IoT is evolving as IoV (Internet of Vehicles), which is mainly responsible for safe traffic, less fuel consumption, and optimization of travel times. In a nutshell, IoT is an upsurging innovation that has an enormous impact on various stakeholders.

Blockchain (BC) is a technique initially planned for cryptocurrency, and the financial industry can be exploited within IoT-enabled networks to attain anticipated security and confidentiality. The key knowledge behind the BC is to extant a communal and public "open ledger," where every contributing node can get anticipated information without any necessity on a third party. So, a fully distributed method is espoused in BC, which, as a result, upsurges the effectiveness of the network in terms of security and transparency as identical update and precise and reliable evidence are comprised of every node.

In a BC network, solving complex consensus algorithm was carried out by miners, the nodes participating in the network which can add or modify data in BC. Many existing algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), etc., use consensus algorithms where nodes are allowed to access and modify information in BC only if it can solve the PoW algorithm. This is a huge challenge in the modern day of IoT-based framework design in industries.

Blockchain methodology assimilates consensus, distributed storage, encryption, peer-to-peer transmission, and other technologies. The key values of BC are attracting much research and development in a wide range of industrial Internet of Things (IIoT) and become an important topic of discussion among researchers. With limited storage, computing, and bandwidth, IoT smears to a large number of edge sensor devices. In the field of industrial Internet device, layer requires hundreds of data sources. The disseminated and enormous data traffic retorting to quality of service (QoS) requirements becomes tailbacks. Blockchain approach as the essential methodology of digital currency, such as Ethereum [35] and Bitcoin, resolves the delinquent trust-building among nodes of a devolved system through the substantiation and distributed node consensus method, thus effecting value transfer while disseminating information and comprehending the noteworthy conversion of current network architecture from “information Internet” to “value Internet.”

Generally, IIoT comprises edge computing devices that are resource inhibited. The minimum levels of computing power, battery capacity, and memory are the physiognomies of an edge computing IIoT. Thus, to balance computing and resource consumption, the system requires a trivial algorithm. It is tough to comprehend the valuable data interconnection because IIoT lacks operative data sharing method.

The overall organization of this chapter is structured and demonstrated as per guidelines in [42]. The contribution of this chapter is to propose a novel, efficient modified blockchain framework for industrial IoT and its edge applications. The framework can be explained by defining the three-tier architecture along with an improved consensus algorithm, and its performance results are compared with the existing approach.

3.1 Blockchain Architecture for Industrial IoT

In this section, we provide the layered architecture [43], which is found effective and efficient in many industrial applications. The architecture proposed in Fig. 1 consists of three distinct or unique domains:

1. ***IoT device domain:*** IoT device data transmission through a wireless channel is carried out through this domain. It will be helpful in the generation of useful information.
2. ***Communication domain:*** It acts as a message gateway between tiers 1 and 3. The relay nodes are important as it relays information to BS, which improves latency and delays.

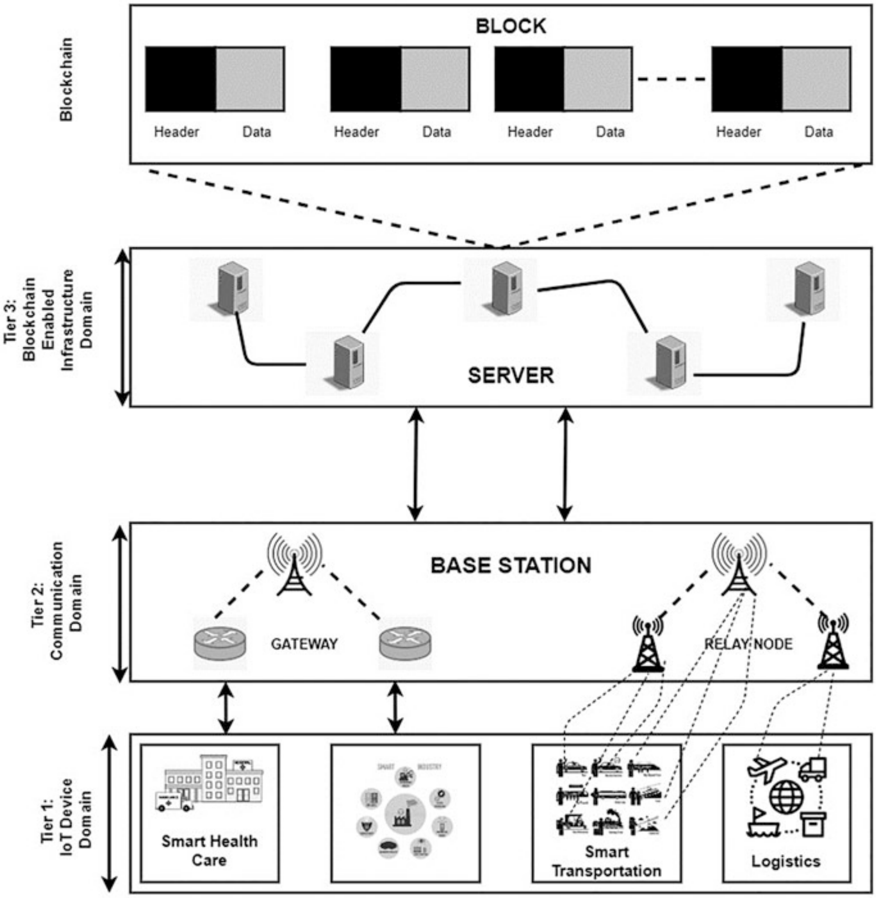


Fig. 1 Layered architecture of blockchain for industrial IoT

3. ***Blockchain-empowered infrastructure domain:*** Blockchains are in the layered architecture, which is represented by the back-end domain. The block has two major components: block header and block data, to validate the information and solve the PoW algorithm.

3.2 Operations in the Layered Blockchain IIoT Architecture

The main tedious process is linking IoT devices and blockchains. To mainly address this issue, the layered architectures of blockchain are proposed to provide connectivity. It operates in three parallel phases:

Phase 1: *Generation of information of IoT devices.*
Phase 2: *Dissemination of information.*
Phase 3: *Add or modify the record.*

The operation of layered architecture is thus straightforward, and various IoT applications are making use of it.

3.3 System-Level Architecture Model

The system-level model in Fig. 2 gives a detailed view of the task or process involved in each domain of the layered architecture. It is a sectional architecture, where designers shall substitute or enhance any new component as each layer is dissociated from other layers without distressing the other parts of the system.

The physical layer of IoT system-level architecture model with the capabilities of communication, computing, and data storage embraces abundant linked devices. Self-organization is essential because physical devices don't have any common Internet protocols (IP), such that routing management is the key mechanism provided by the connectivity layer. The other functionalities, such as services, managing networks, security maintenance, and breaking of messages, are provided by this layer.

The final layer is all about servicing blockchain, to provide several mechanisms, such as blockchain mechanisms, managing identity, consensus, and peer-to-peer (P2P) communication, by establishing common services with all modules.

The participants of the BC network have a self-copy of the ledger, which is carried out by the distributed ledger, that is, the consensus of shared, harmonized, and replicated digital data that are widespread along with this network. To handle the configuration of devices and data detection of physical sensors, safe storage spaces are offered by this layer. The replication of any modification is done in all copies within seconds. The ledger can be either permission or permission less, concerning if a peer can be run to validate transactions by anybody or only authenticated members.

The system-level model contains big data analytics function which is a powerful method that empowers the BC for online storage of data. The transactional data is an impeccable source for further investigation, which is stored as an organized form of ledgers. The components involved are authenticated to access all details in a single network.

The smart contract is used to realize access and modifications in the ledger, which is instantiated by the client as a code and is installed in each peer network.

The module which manages the event directs it every time either to fulfill the precondition of a smart contract or when a ledger gets a new block. The accessibility and management of the network can be done through the BC network service provider as services are exposed by the API interface. The data from physical

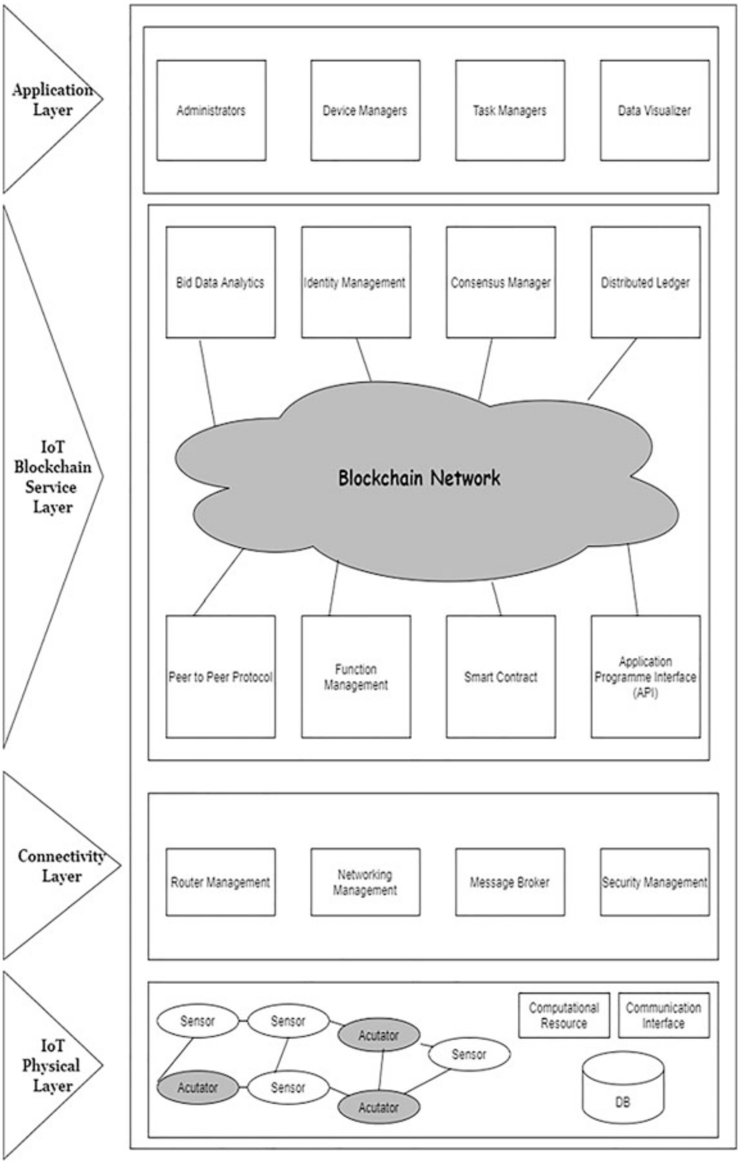


Fig. 2 System-level layered architecture for blockchain-based IoT framework

devices, controlling and deployment of the devices are foreseen by the application layer, which is the topmost layer of the model through various interfaces [43].

3.4 Interaction Model for the Proposed Layered Architecture for Blockchain-Based IoT Framework

The app client is used to deliver intense services, such as enrollment of the user, registration of the device, and generation of task services, and submit the proposals of transactions to the BC network through an instinctive. The registration is done before submitting a transaction where an explicit participant is provided with a certificate, which encompasses private keys to sign it is an essential part.

Figure 3 defines the workflow-based interaction diagram and gives a clear understanding of its components. It incorporates not just a user service outline but also a methodological setup, in which the smart contract and dispersed ledger are disclosed to the application.

The IoT server is responsible for generating a new job or device, which is carried out through the device owner. In turn, to achieve some secured operations, the BC network accepts the request from the server and processes it. In real time, the device that has acquired data that is sensed or the modification in the status can be sent back and also instruct to handle the job request from the client.

The individual owner who is related to the physical device is allowed to submit transactions right away to the BC network as the identity of the device owner is authentic.

The threshold defined by the smart contract compares the data which is detected or the status affixed in the ledger. The device owner is notified by generating a warning if the compared value exceeds the threshold defined.

3.5 Transaction Flow of BC Framework

The comprehensive transaction performance process of the BC network is illustrated in Fig. 4. To submit proposals of the transaction, the client application has to get the authorized permission for it. The permission can be obtained through credentials issued by the service which manages the identity.

The clients who wish to join the network are validated by the identity manager that clasps user IDs. In the BC network, the client application sends transaction tenders to peers. The BC network and the client application between communications supervene the SDK of the application. The peers can be of two types: either endorses or committers. Endorsers can feign and sign transaction offers, retort to conceding, or repudiate endorsements; committers authenticate results of transaction and write the block of the transaction once to the ledger. Each peer of the endorser invokes the smart contract to receive and implement the offer of transaction in its simulated environment. The results of execution won't be reproduced in the ledger. The endorser peers record the read data from the present state at the time of simulation of transaction and write data after the execution of the transaction by simply apprehending the RW sets. For authorization review, ciphering of the RW

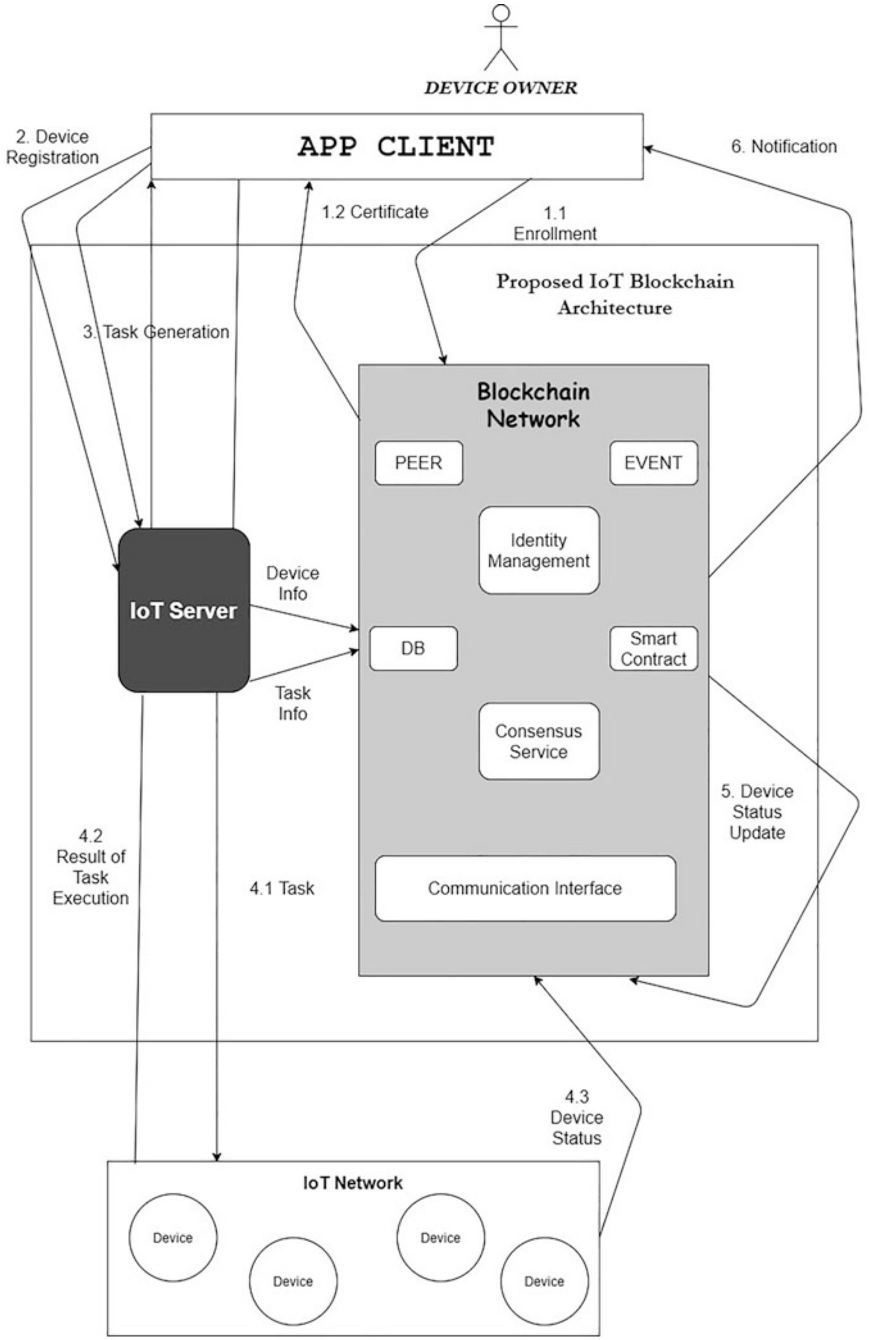


Fig. 3 Proposed IoT BC framework workflow diagram

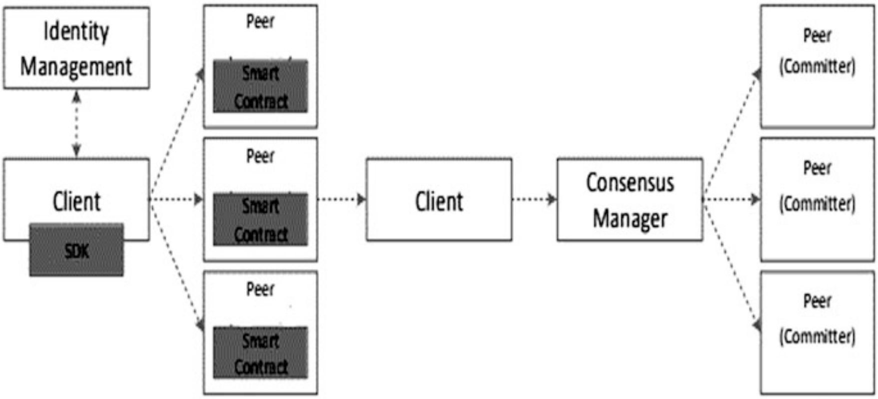


Fig. 4 Workflow implementation: a detailed diagram

sets and sending back the proposal rely on the client application was carried out by the peers of the endorser.

The signatures are to be approved by the client to validate and oversee if the stated endorsement policy has been fulfilled. The client packages the transaction along with the RW sets, and it is combined and submitted to the consensus manager. In parallel, with the help of signed transactions across the network, consensus occurs and RW sets are submitted, and peers of committer are distributed with the block of this order. The legalization of the transaction is carried out by each peer of the committer by comparing present state and RW sets to find if they are matching. If the simulation of the endorser results in the same as the present state, the data of reading is still available.

After the transaction is authorized by a peer of the committer, the state can be updated with the write data from RW set accordingly based on the transaction written to the ledger. Finally, the client application is notified at different times whether the transaction submitted is a success or failure by the peers of the committer asynchronously. Each peer of the committer notifies event occurrence to the client application which occurs when enrolled for events.

3.6 Improved Consensus Mechanism for Blockchain

Figure 5 demonstrates the PoW technique of the BC network, in which a PoW puzzle was created first by each miner. Secondly, broadcasting of the created puzzle was carried out by a node in BC, which is observable and reachable to each contributing node. But embracing, accessing, and modifying data in BC can be carried out only by the nodes which resolve the PoW mechanism.

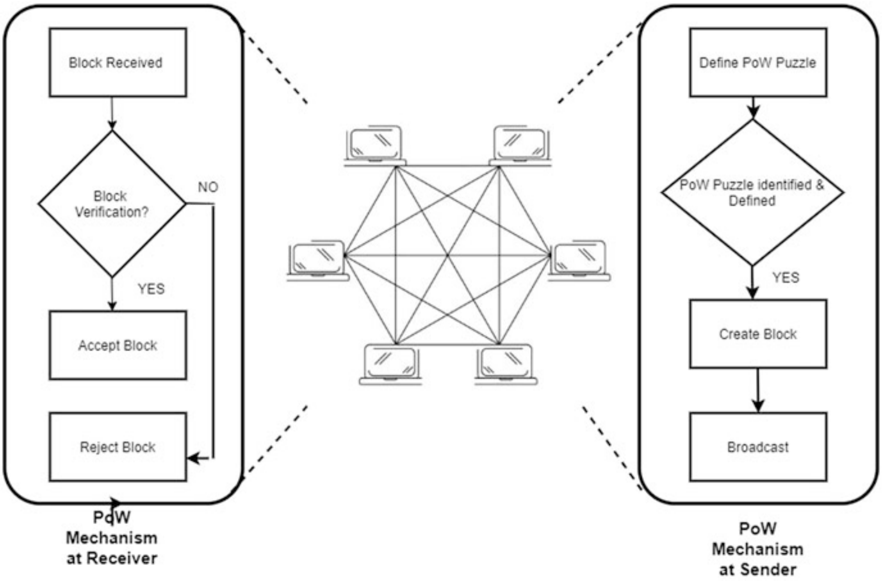


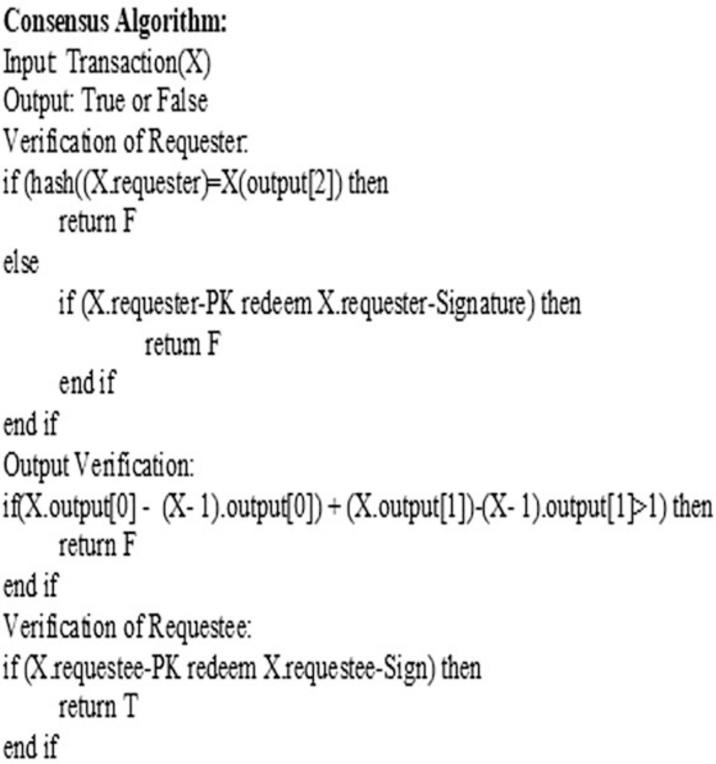
Fig. 5 Consensus mechanism for blockchain

The central administration doesn't have BC. Network miners independently generate the blocks. The same inference is reached and fabricated the identical common record of each node, thus attaining global consensus by a single node that uses information that is transmitted through the apprehensive connection. The whole chain of blocks was managed by the nodes that are complete, which validate it. In the main chain, if numerous nodes have identical blocks, then it can be concluded that consensus had reached.

The steps involved in the consensus technique are block authentication and the most widespread chain assortment. The node achieves these steps autonomously. In the network, firstly, the blocks are broadcasted, and when a new block is acquired by each node, it retransmits to the neighboring nodes. To ensure that only legal blocks are broadcasted, the blocks perform block authorization before this retransmission. The following is the explicit checklist to be followed:

(i). Block design (structure).
(ii). Verifying hash of header with difficulty established (met or not).
(iii). Limit of block size.
(iv). All transaction verification.
(v). Timestamp validation.

BC defines one parent for one block, but, in some circumstances, at a single point in time, miners produce new blocks, leading to have one parent with many children. This divergence resulted in the chain. Selecting blocks to be part of the main chain while rejecting others is the final step.The communication domain



```
Consensus Algorithm:
Input Transaction(X)
Output: True or False
Verification of Requester:
if (hash((X.requester)=X(output[2]) then
      return F
else
      if (X.requester-PK redeem X.requester-Signature) then
            retum F
      end if
end if
Output Verification:
if(X.output[0] -  (X- 1).output[0]) + (X.output[1])-(X- 1).output[1]>1) then
      return F
end if
Verification of Requestee:
if (X.requestee-PK redeem X.requestee-Sign) then
      return T
end if
```

Fig. 6 Algorithm for consensus

produces transient communication in IoT devices, which is the main feature of the IoT networks. In constrained time the delicate information which might proliferate must be shared among nodes. Thus, data can be made accessible for other nodes at a particular point in time by providing an optimized consensus algorithm in miners. So, improved consensus mechanism was deployed in the architecture, which helps applications with resource-constrained environments.

A time reliability algorithm is proposed to eliminate the problems faced by the old mean exhaustive procedure. The block creator is arbitrarily nominated for this procedure. In each block the CH waits for T time randomly before producing a new block. The block generations carry over a while, and when the number of blocks exceeds the threshold (based on the environment of the network and performance necessities), the CH will discard the blocks. So, to verify the block before attaching it to the chain, Fig. 6 shows the improved consensus algorithm, which will do the process:

The requester hash is compared with output transaction by CH, and if the requester agrees, output [0] will increase to 1 or else output [1] will be improved to 1.

In the transaction verification process, CH checks for output [0] fruitful transaction or failure transaction output [1]. Then, the requested signature is verified.

4 Experimental Simulation

In this section, the performance of the Lightweight Acquired Blockchain Framework (LABF) blocks is assessed to examine the viability of IIoT BC platforms. 20 nodes CH is the default arrangement for simulation. So, to assess the feasibility, different nodes were installed on different platforms. The framework proposed the cluster node as responsible for block generation, verification, and consensus because CH nodes have the authority to generate blocks. According to the data rate of sensor and delay of data gathering and block production, fine-tuning can be done in the gateway block production time. In Fig. 7 the comparison of results with the typical starting point based on the single simulation, which took 120 s and competed ten times, is illustrated. The left axis signifies the CH block verification time, and the right axis denotes the percentage of the transactions authenticated (PTA).

Due to the ungainly common trust by CH, the indulgence time of the two approaches was the same when LABF block substantiation starts. Unreliable trust was established between CH as many blocks were generated and validated by Resource Constrained Layer Block Chain (RCLBC). The processing time was reduced by LABF in comparison to baseline as LABF requires only a small communication part in the block, which is a newly generated block. Additionally, there are increases in a subsidiary conviction of CH and in block verification and a progressive reduction in transaction volume.

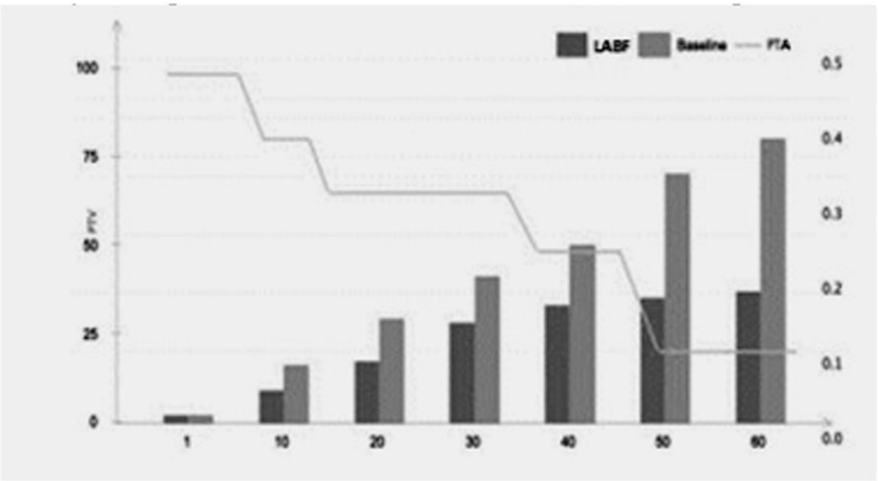


Fig. 7 Block verification performance evaluation

The integration of trust mechanism with block substantiation scheme accomplished by CH reputation module enhanced the authentication process.

Through the above experiment, the intricacy and network overload of this algorithm are analyzed. The analyzed results of the experiment show that there is an increase in the effectiveness of BC with network scale. Data flow and transaction flow are separated by the BC system. The transmission dormancy and lower packet outlay were taken care of by LABF. When there is an increase in CH, package outlay increases. Mutual trust is established between the blocks when CH produces more blocks as time goes by. Inversely, when the validation of blocks increases, the transaction validation of numbers decreases. Thus, there will be fixed processing time and verification of several transactions to be carried out.

To provide a complete solution, numerous investigational tests were carried out with the help of different performances.

$$\begin{aligned}\text{Service Execution Time} &= \text{Transaction Appeal Time for transmitting}\\ &\quad + \text{length of ack acquired by Web Client} \qquad (1)\end{aligned}$$

As per Eq. 1, it is understood that the execution time of service is the total appeal time of the transaction for transmission plus Web client acknowledgment length. Figure 8 illustrates the analyzed cost of service execution time on registration of device, which is the first study. To undergo this study, devices are segregated into four groups as 50, 150, 200, and 250, and their information is given to the proposed framework. Through Hyperledger Caliper [38], implementation was carried out. With the help of indicators, set users are permitted to configure particular execution of BC use case script. The implementation time was recorded as Min, Avg, and Max to perform this transaction in the proposed BC platform. The four groups of devices recorded different min, max, and average times. The group which has 50 devices shows 2262 ms as the minimum time, 2286 ms as the average time, and 2375 ms as the maximum time. The second group which has 150 devices recorded the min time as 2257 ms, the avg. time as 2335 ms, and the max time as 2801 ms. The third group of 250 devices delivered execution time as 2254 ms for the min time, 2585 ms for the avg. time, and 3004 ms for the max time. Finally, the fourth group, which has 500 devices, recorded the transaction execution time as 2267 ms for the min time, 2923 ms for the avg. time, and 4013 ms for the max time.

The next study is carried out to evaluate the execution time of service in storing data that are sensed in the BC network. The devices can appeal to Representational State Transfer (REST) server for API Sensor Reading as they have HTTP Client. REST server drew the implementation results from the BC network and sends them back to the device when sensed data is added to the BC. Figure 9 shows the estimation results of the execution time on accomplishing sensor reading transactions.

In the third study, evaluation of the BC network system performance is carried out when records that are sensed are stored in the distributed ledger. In Fig. 10 querying of data records in BC and their implementation time is measured. The min,

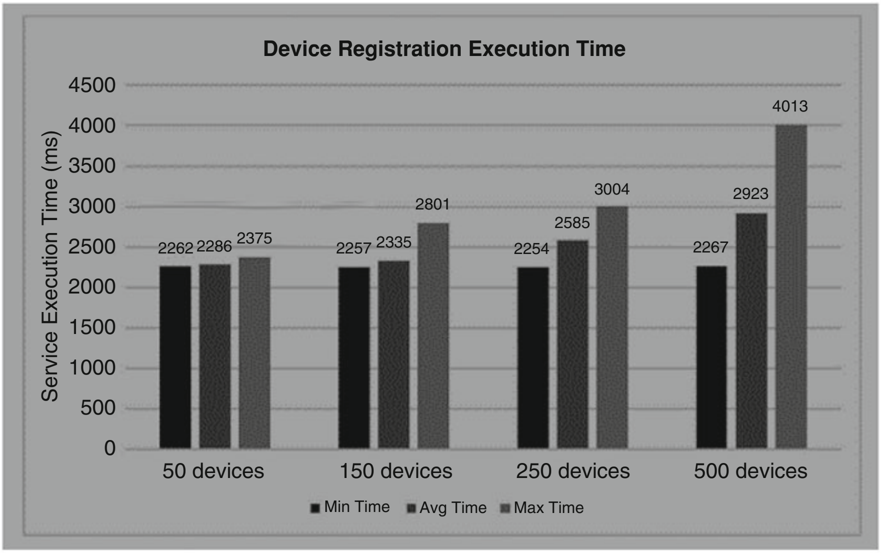


Fig. 8 Device generation performance study graph

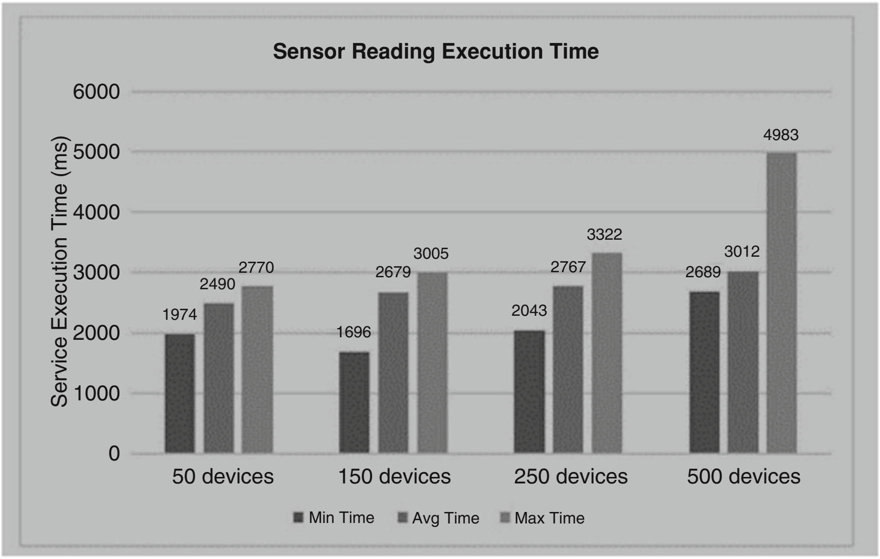


Fig. 9 Graph for sensor reading performance study

avg., and max delay times in ms taken by the proposed framework to repossess the sensing records were noted down ten times at arbitrarily selected system resource consumption levels.

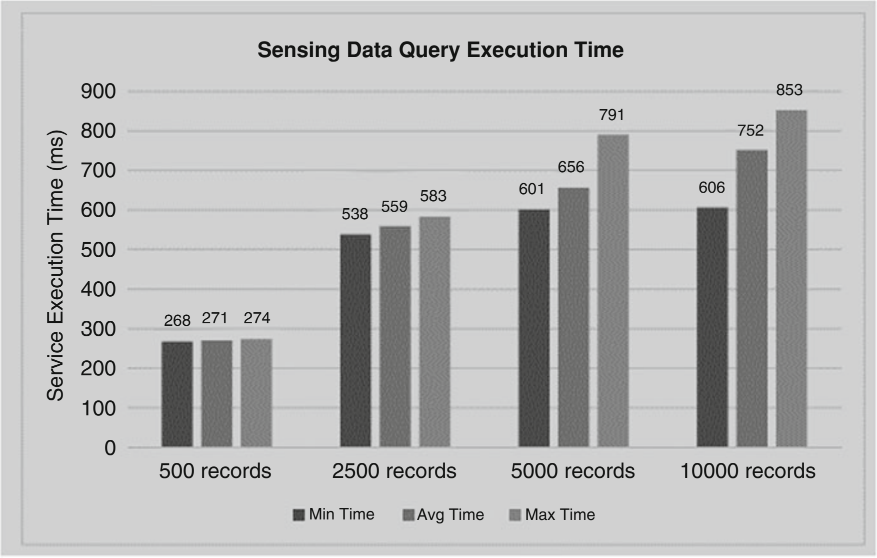


Fig. 10 Sensing data query performance graph

The proposed approach shows BC platform performance is significantly highlighted by the properties that play an essential role are considered for this study to compare the overfed platforms.

The selected system [39] setup was utilized for the analysis of this study. Through 50 peers, simulation was run for 60s during which 950 transactions were executed. Figure 11 illustrates processing overhead evaluation. As depicted in the graph, when compared to selected system processing overhead, processing time is reduced by 18% by changing the number of blocks from 10 to 60.

Permission-less BC network allows anyone to participate who is unidentified, through which most systems are developed. This depicts that there is neither privacy in contract nor privacy in a transaction that is produced. These systems issue their tokens to incent exclusive mining or to trigger the execution of smart contracts to alleviate nonexistence privacy. The transaction rate and rapidity can be significantly affected by undesirable links with cryptocurrencies.

In addition, as the token used in both systems must be unified, the BC network hinders the interaction with other distributed systems. In contrast, the proposed system lessens the peril of malicious code presentation through a smart contract intentionally by a participant where it is built on a permission network. All the activities of the participants are recorded on the BC in terms of affirmation policy given for the network and type of transaction as participants are known to each other. Additionally, in IoT devices, many systems simply deploy the full nodes to attain time-consuming mining as they are lagging in resource-constrained IoT devices. The consensus algorithm is limited to work with constraints, so the IoT resource-

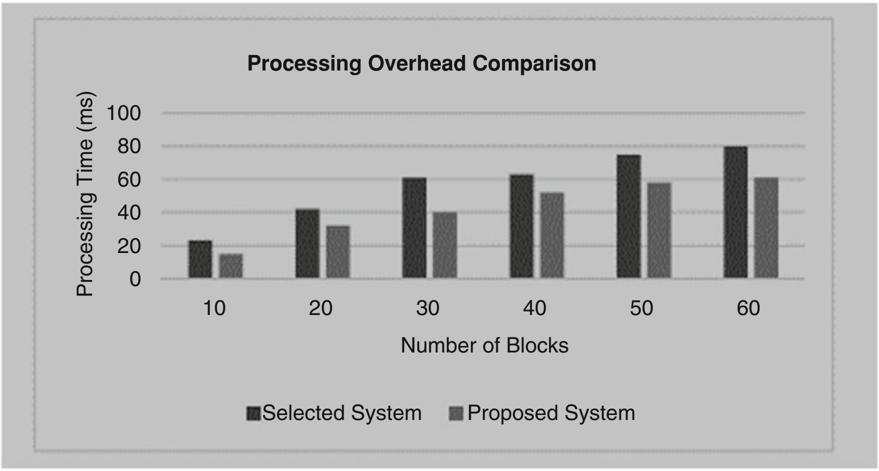


Fig. 11 Comparison of processing overhead and its performance analysis graph

constrained architecture has always been the chief interference in assimilating IoT with the blockchain. But present works deploy such huge algorithms on other devices, which are part of IoT-like gateways. However, these have limited storage space.

To authenticate transactions and block full nodes with the whole BC should be deployed on the gateway but many BC frameworks don't provide these requirements. If this is provided, gateways act as self-reliant targets and stand as the first line of defense as they link between the Internet and device. An Light Weight (LW) solution neglects the integration of the BC platform into IoT devices, and no modification is required and is proposed.

In the proposed model, the BC acts as a peripheral service to make the network provide secure storage, which is consistent. In addition, without extracting the whole BC, legalization of transactions produced by IoT devices is carried out. With limited capabilities, the proposed solution can be utilized in a wide range of IoT scenarios. Additionally, through Web service API BC network communicates with IoT devices, thus permitting cross-platform communication, which helps in the integration of the proposed and existing systems.

To prove the feasibility of the system proposed, a real-life smart space case study was implemented in the experiment. The proposed platform can be easily prolonged to numerous domains as it is built on a modular architecture.

The IoT sensors can be consigned to someone as it is linked to any product with remotely sensed data. Each party of a supply chain is allowed to access the ledger as it is made for sharing, such that recording of all the processing steps and storing it on the BC, including audit certificates, test evaluation results, and digital compliance documentation, can be carried out. This chapter aims to solve all the mentioned problems, and the demand for such IoT BC applications increased due to its various offers, such as permissioned network, user-friendly API, flexibility in architecture, and the latency of transaction is low, while the throughput of the transaction is high.

5 Conclusion

In this chapter LABF for edge computing-based IIoT applications was proposed. With a variety of resource capabilities, the BC operation is designed for edge devices. A time reliability algorithm is designed for limiting the generation of different blocks in the consensus cycle and also to diminish the asynchronous block operation in network delay. Accumulation of other node evidence is done by each node based on the generation of original blocks. To evaluate the effectiveness of BC, a high-throughput administration method is proposed. The highlight is the integration of BC with IoT, which is not an easy task that requires more attention from all directions.

Universal challenges are faced by IoT as millions and millions of devices are available online. Factors and manufacturers are always different from connected devices as they are diverse. Thus, in a secure way, uniqueness and interoperability are to be ensured. To enable IoT devices to have trusted interoperability for data and e-commerce, the BC platform gives innovative infrastructure and protocol for security. This paper provides an intuitive approach to address uniqueness and challenges in the data security of BC networks by delivering a decentralized IoT platform.

In the future adaptive block verification scheme can be implemented to verify and diminish the calculation cost of the block authentication process, thus improving the scalability and trust architecture delay. Furthermore, the blockchain architecture can be implemented through Resource Constrained Layer (RCL), Resource Extended Layer (REL), and cloud layers for expanding the areas, and quantitative researches can be formalized for investigation of functioning competence.

References

1. Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications, 67*, 99–117.
2. Fan, L., et al., (2018). *Investigating blockchain as a data management tool for IoT devices in smart city initiatives*. In Proceedings of the 19th annual international conference on digital government research: Governance in the data age, 2018, p. 100.
3. Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (Feb. 2016). Middleware for internet of things: A survey. *IEEE Internet of Things Journal, 3*(1), 70–95.
4. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (Mar. 2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems, 56*, 684–700.

5. Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system*. Available online: https://bitcoin.org/bitcoin.pdf.
6. Antonopoulos, A. M. (2014). *Mastering bitcoin: Unlocking digital crypto-currencies*. O'Reilly Media, Inc..
7. Huang, X., Xu, C., & Wang, P. (2018). LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. *IEEE Access, 6*, 13565–13574.
8. Dorri, A., Steger, M., & Kanhere, S. S. (2017). BlockChain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine, 12*, 119–125.
9. Lei, A., Cruickshank, H., & Cao, Y. (1832–1843). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet Things, 2017*, 6.
10. Kang, J., Yu, R., & Huang, X. (2017). Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium Blockchains. *IEEE Transactions on Industrial Informatics, 6*, 3154–3164.
11. Li, L., et al. (2018). CreditCoin: A privacy-preserving Blockchain-based incentive announcement network for Communications of Smart Vehicles. *IEEE Transactions on Intelligent Transportation Systems, 19*, 2204–2220.
12. Yang, Z.; Zheng, K.; Yang, K.; Leung, V. (2017). *A blockchain-based reputation system for data credibility assessment in vehicular networks*. In Proceedings of the 2017 IEEE 28th annual international symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 8–13 October 2017.
13. Wang, J., et al. (2018). A Blockchain based privacy-preserving incentive mechanism in Crowdsensing applications. *IEEE Access, 6*, 17545–17556.
14. Tian, F. (2016). *An agri-food supply chain traceability system for China based on RFID & blockchain technology*. In Proceedings of the IEEE 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016.
15. Abayomi-Zannu, T. P., Odun-Ayo, I., Tatama, B. F., & Misra, S. (2020). Implementing a mobile voting system utilizing Blockchain technology and two-factor authentication in Nigeria. In *Proceedings of first international conference on computing, communications, and cyber-security (IC4S 2019)* (pp. 857–872). Springer.
16. Lu, Z., et al. (2018). A privacy-preserving trust model based on Blockchain for VANETs. *IEEE Access*.
17. Brody, P., & Pureswaran, V. (2014). *Device democracy: Saving the future of the internet of things*. IBM.
18. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *IEEE international congress on Big Data (BigData Congress)* (pp. 557–564).
19. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805.
20. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
21. Hammoudi, S., Aliouat, Z., & Harous, S. (2018). Challenges and research directions for internet of things. *Telecommunication Systems, 67*(2), 367–385.
22. Atzori, M. (2017). *Blockchain-based architectures for the internet of things: A survey*. University College of London.
23. Gao, J., Asamoah, K. O., Sifah, E. B., Smahi, A., & Xia, Q. (2018). Grid monitoring: Secured sovereign blockchain based monitoring on smart grid. *IEEE Access, 6*, 9917–9925.
24. Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*, 99–109.
25. Wang, X., Yang, L. T., Xie, X., & Jin, J. R. (2017). A cloud-edge computing framework for cyber-physical-social services. *IEEE Communications Magazine, 55*, 80–85.
26. Zhang, G., Gao, Y., Luo, H., Sha, N., Wang, S., & Xu, K. (2019). Security performance analysis for relay selection in cooperative communication system under Nakagami-m fading channel. *IEICE Transactions on Communications, E102-B*, 603–612.

27. Buzby, J. C., & Roberts, T. (2009). The economics of enteric infections: Human foodborne disease costs. *Gastroenterology, 136*(6), 1851–1862.
28. Malviya, H. (2016). *How Blockchain will defend IOT*. Available online: https://ssrn.com/abstract=2883711.
29. Veena, P., Panikkar, S., Nair, S., & Brody, P. (2015). Empowering the edge-practical insights on a decentralized internet of things. In *Empowering the edge practical insights on a decentralized Internet of Things* (Vol. 17). IBM Institute for Business Value.
30. Gan, S. (2017). *An IoT simulator in NS3 and a key-based authentication architecture for IoT devices using Blockchain*, Indian Institute of Technology Kanpur.
31. Chain of things. (2017). Available online: https://www.blockchainofthings.com/. Accessed 1 Feb 2018.
32. Filament. (2017). Available online: https://filament.com/. Accessed 1 Feb 2018.
33. LO3ENERGY. (2017). Available online: https://lo3energy.com/. Accessed 1 February 2018.
34. Aigang. (2017). Available online: https://aigang.network/. Accessed 1 Feb 2018.
35. My bit. (2017). Available online: https://mybit.io/. Accessed 1 Feb 2018.
36. Samaniego, M., & Deters, R. (2016). Hosting virtual IoT resources on edge-hosts with blockchain. In *2016 IEEE international conference on Computer and Information Technology (CIT)* (pp. 116–119). IEEE.
37. Ethembedded. (2017). Available online: http://ethembedded.com/. Accessed 1 Feb 2018.
38. Raspnode. (2017). Available online: http://raspnode.com/. Accessed 1 Feb 2018.
39. Sawal, N., Yadav, A. Tyagi, A. K., Sreenath, N., & Rekha, G. (2019). *Necessity of Blockchain for building trust in today's applications: An useful explanation from user's perspective* (May 15, 2019). Available at SSRN: https://ssrn.com/abstract=3388558 or https://doi.org/10.2139/ssrn.3388558.
40. Hyperledger Caliper (2019) Available online https://www.hyperledger.org/projects/caliper. Accessed on 15 Jan 2019
41. Awotunde, J. B., Ogundokun, R. O., Jimoh, R. G., Misra, S., & Aro, T. O. (2021). Machine learning algorithm for cryptocurrencies Price prediction. In S. Misra & A. Kumar Tyagi (Eds.), *Artificial intelligence for cyber security: Methods, issues, and possible horizons or opportunities* (Studies in computational intelligence) (Vol. 972). Springer. https://doi.org/10.1007/978-3-030-72236-4_17
42. Misra, S. (2021). A step by step guide for choosing project topics and writing research papers in ICT related disciplines. In S. Misra & B. Muhammad-Bello (Eds.), *ICTA 2020, CCIS 1350* (pp. 727–744). Springer Nature. https://doi.org/10.1007/978-3-030-69143-1_55
43. Parimala Devi, M., Choudhry, M. D., Boopathi Raja, G., & Sathya, T. (2022). A roadmap towards robust IoT-enabled cyber-physical systems in cyber industrial 4.0. In *Handbook of research of internet of things and cyber-physical systems: An integrative approach to an interconnected future*. Apple Academic Press. [In Press].