

# IBchain: Internet of Things and Blockchain Integration Approach for Secure Communication in Smart Cities

Tanweer Alam

Faculty of Computer and Information Systems, Islamic University of Madinah

170, Prince Naif bin Abdulaziz road, Madinah, Saudi Arabia

Email: tanweer03@iu.edu.sa

**Keywords:** internet of things, blockchain, wireless communication, security, data transmission, smart cities

**Received:** June 1, 2021

*Introducing IBchain, a new blockchain architecture with the Internet of Things (IoT), could be an attractive framework regarding improvements in connectivity implementation through the smart cities. Instead of meriting innovation and security, the IoT links people, sites, and products and provides opportunities. Everything that transfers information to the IoT system is integrated by advanced microchips, sensors, and actuators in actual things. The analytical ability of the IoT converts observations into actions, impacting business advancements and significant ways of activity. IoT enables connected objects to transmit information to personal blockchain systems to create tamper-resistant transaction records. The information from sensors and microchips is progressing rapidly with blockchain ledgers, making them more portable and relevant for immediate conversations. In IBchain methodology, the smart objects are permissible to connect securely with other smart objects in diverse situations. IBchain creates an innovative blockchain-based processing configuration through the IoT. The IBchain could analyze blockchain to the main expertise or supports the IoT validation and trustworthiness. It reinforces blockchain and cloud to build an empowering IoT ubiquitous situation for secure communication among the smart devices.*

*Povzetek: Prispevek opisuje novo arhitekturo veriženja IBchain, ki uporablja internet stvari in verigo blokov za varno komunikacijo.*

## 1 Introduction

The IBchain is an approach for secure communications between physical objects using the integration of IoT and blockchains. This approach is useful for smart cities. The IBchain is becoming a revolutionary invention that operates on a decentralized, dispersed, open, and instantaneous network to collect IoT nodes' activities. Throughout fact, the blockchain is a sequence of blocks, every block is connected to the previous nodes [1]. Each block will have a public key, a preceding block hashing code, along with the metadata [2]. IBchain processes would be the specific sections that have been developed to convey data between IoT nodes [3]. Each IoT device appears to have been various types of potential but smart devices, including embedded sensors, cameras, networks, and the ability to communicate with various other IoT nodes [4]. IoT links individuals, sites, objects or resources for increased efficiency and security. Advanced devices, transceivers are integrated into physical things, every transferring information to the IoT devices. Then IoT analytical tools use this obtained information to transform ideas towards outcomes, improve workflows, and contribute to innovations. Smart cities will deliver the best facilities to promote residents' everyday lives in the areas of medicine, traffic, power use, and skills training. Interestingly, the idea of smart cities is emerging, and, considering its desired future, security measures are on the emergence. Blockchains can encourage the growth of

smart cities due to their positive characteristics like accountability, openness, flexibility as well as integration.

The function of IBchain will provide an approach to analysing secure transaction data by IoT nodes [5]. IBchain tends to be a comfortable place that may be used both publicly and privately [6]. The connectivity allows

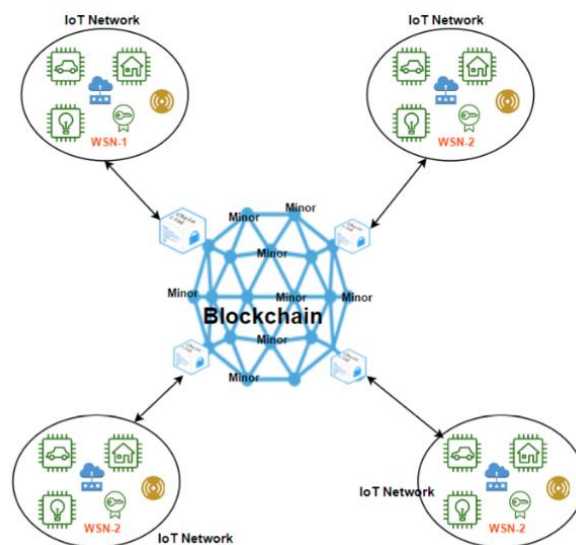


Figure 1: IoT network and Blockchain.

the devices to enable the cryptographic operations between IoT nodes under the complicated network [7].

The activities could be tracked and moved anywhere accessible to communicate in the IoT network [8]. The Blockchain tends to be a sequence of authenticated or cryptographical blocks controlled through a computer linked to the entire network [9]. Such blocks of data are stored digitally as well as sending data to a blockchain [10]. There are several remarkable possibilities for the integration approach. Figure 1 shows the IoT network connectivity with blockchains.

i) Building trust between the stakeholders: The IBchain approach will establish relationships between numerous wireless technologies due to its extensive additional functionality. Only verified devices can communicate with the framework since a miner would first verify each transaction block and then connect to the blockchain [11].

ii) IBchain technique may reduce costs because it works efficiently without a third-party vendor. This erases the entire third-party clusters among the transmitter and the recipient. Such an approach offers great conversation.

iii) IBchain helps in reducing a lot of time. Such an approach minimizes transaction time from hours to seconds.

iv) IBchain approach ensures privacy and security to devices and information.

v) IBchain approach provides connected networks for both social and community facilities. Connected devices can communicate with each other and share data.

vi) This approach can securely exchange money without the use of a third person. This offers rapid, secure, and economic details services. Also, this can reduce the transmission time and charge.

vii) This strategy performs a significant responsibility in investigating or eliminating the potential for loss of the asset or activity.

IBchain approach may face several challenges, such as scalability, storage, skill levels, and detection, etc.

1. It can be hanged due to the huge transaction volume. Expect that since IoT is integrated with Blockchain, the capacity would be stronger than that of the existing condition.

2. IoT node would maintain a digital transaction in IBchain. During most of the period, it will enhance its processing power, and it will be a difficult mission or turn out to be a huge burden on the linked devices or routers.

3. Blockchain has become a radical revolutionary innovation with the IoT [12]. Some people worldwide know this technology

4. Discovering the nodes is a challenge across all smart devices in this strategy [13]. IoT can discover their connected nodes, but this task will be challenging when it integrates with the blockchain [14].

5. The ledger will be freely distributed through all connected nodes [15]. Each node may look at the blockchain activities. Therefore, privacy has been a big challenge in the integrated solution.

6. Blockchain may be either personal or public kind. Interoperability among public and private blockchains

[16] will thus be an obstacle under the integrated approach.

7. IBchain will operate globally and is thus faced with several regulations to execute the policy.

Blockchain can also contribute to reducing operational expenses by removing intermediaries or agents.

Blockchain is broader than the period of shared ledgers, which are based on Bitcoin's cryptocurrency capacity. The system is being utilized in fixed areas such as retailers to improve sales relaxation using supply chains and prescription medicines to assure the completeness of agreements, scientific investigations, and medicines. The finest product and service categories are closely watched with the integration in various areas. The major challenge for the constructions on the boundaries of the IoT, assuming the existing description, its protective structure, with the central authorities monitoring the end-user model allowing for detecting a single fault source. By enabling decisions in a network of shared devices, Blockchain addresses such issues. However, there are three big obstacles to consider while building IoT devices next to the blockchain ladder: One of the most challenging parts of the IoT method is the measuring of the enormous amount of information acquired through a huge variety of information that is acquired by the wide sensory networking to unambiguously lower speed or latency of the transactions. Creating a preliminary comprehensive knowledge model might save time when delivering a solution. In public blockchains, the privacy of transaction history for IoT devices is not simply possible in the shared blockchain network. This is because activity sequence checks may be utilized to assume that users or devices are identical behind authentication tokens.

The rest of the paper is structured as below. Section 2 represents the related works, section 3 represents the IBchain methodology and results, section 4 represents the IBchain for Smart Cities, section 5 represents the discussion and section 6 represents the conclusion.

## 2 Related works

The IoT is frequently associated with the exploitation of connected gadgets which include surveillance cameras, execute malicious actions, which is related to serious cyber assaults. To assist them, questions regarding the comfort of IoT's uninterrupted Internet-connected devices were raised in search of realistic solutions to address the security imbalance. This is the extremely creative technology blockchain, which assures that the agency has less danger of technical harm and improves the damage of IoT execution. It will constitutionally enable the security of IoT connections in various ways, including generating a human behaviour agreement that does not help to separate any nodes that may be misrepresented.

In 2016, Mayra Samaniego et.al. have presented the blockchains as a service. The blockchains is a public or shared repository containing linked blocks of data. In comparison to all various ledger strategies, blockchains ensure revocability evidence security of

authorized activities. according to the shared and distributed structure, blockchains have been used in IoT, – for example, to control network settings, storing device data, and allow multi-payments. It introduces the concept that uses blockchains as an IoT service which examines the efficiency of a blockchain-enabled execution [17].

In 2017, Ahmad Banafa has published an article on IoT and Blockchain Convergence. He has presented the integration of Blockchain and IoT in this article. Blockchains could be used to monitor billions of smart devices, allowing exchange management and collaboration among connected objects. It enables substantial benefits to IoT technology producers. Such a collaborative approach can remove specific failures, providing a more stable environment for gadgets to operate through. Cryptosystems used throughout blockchains will directly activate information more securely. Blockchains allow secure, peer-to-peer communication permissible and has shown their utility in the context of business transactions via digital currencies, offering assured peer-to-peer payments processing without third-party agents [18].

The primary objective of blockchains is to enable secure communications among parties via a peer-to-peer infrastructure utilizing a shared database. Its purpose is to remove all third - parties verification and replacement the trust of the central authority for verification of transactions for authentication evidence. although several blockchains app revolves around cryptocurrency, blockchains may be used in several other areas, like banking, storage systems, healthcare, robotics, and so on. The blockchains could be used to build distributed apps by building an accessible distributed system [19].

IoT and blockchains are rising in aspects of the advanced social system and are key consideration societies and cultures, whether individually or combined. Moreover, both techniques for health monitoring allow open transmission of information between the group members. The features of centrally consolidated and worldwide decentralized measurement are being accessed throughout this blockchain-IoT network by separating others into the base or edge platforms. The whole association improves efficiency and network performance. This same new plan was successful in the experiment of autonomy systems management and surveillance [20]. The blockchains-based trust platform for IoT devices is explained in the article [21].

The execution of IoT consists in a moving object of risk requiring authentication measures. Smart devices range from highly scalable situations to business-oriented frameworks. Extensive coverage of IoT protection is required, in particular for highly scalable situations, but related enterprise systems. A variety of security processes and strategies were introduced and used. Blockchains frameworks contribute to protecting several IoT-oriented technologies by being key to the success of a security matrix in the sense of a technique. The blockchain is a ledger that records all evidence activities [22]. Businesses must consider whether hybrids or blockchains better match their privacy requirements.

The integrity of IoT sensors may necessitate the destruction of the IoT sensor by interacting with the relevant process volume required to complete the transactions. A safe situation for information collection and transactions should be protected by measures to ensure IoT devices' dependability that cannot be changed by exterior manipulations. In summary, blockchain and IoT are two technologies with large potential, however, owing to technological and safety problems they currently need considerable acquisition.

### 3 IBchain methodology and results

There is a combination of two major forces: when the blockchain combines IoT, in the long term, the availability of IoT expanded considerably and connected numerous gadgets and networks with homes, offices, travel systems, or whole cities. The blockchain over the last decade will once again change the business model with its encrypted and transportable manual for annoying data and real-time statistics.

The success of this research is the development of the Integration system for smart objects using cloud and blockchains on the IoT. The whole structure is mainly designed for applications where information is accurately conveyed to smart objects at IoT platforms [23], [24]. Also, it is using a re-transmit method, participants' width, or congested traffic problems to strengthen the present framework. The implementation plan for this research is being described. Throughout able to develop content on the internet, the IBchain system must be designed to communicate securely among IoT-connected systems [25]. Figure 2 shows the transaction processing in IBchain. The last one is expected to give verified and accessible monitoring approaches for devices and processes, according to the previous, as IoT and blockchain operate jointly. Blockchain operates as an extensible text where numbers or subtitles are taken and several times is produced when more entries, also known as blocks, are introduced. All done by a digital signature becomes viewed and can never be changed or deleted. In essence, the blockchain may protect the IoT nodes from an environment where incorrect information can be suppressed and the public environment disrupted, whether a smart or intelligent automotive unit. This entire analysis will be carried out as a 3-layer architecture, with these layers being clouds, Blockchain, and IoT. Such a study proves data transmission in terms of developing an IBchain framework among several smart devices. This architecture has the key sections: a) IoT Nodes b) Internet

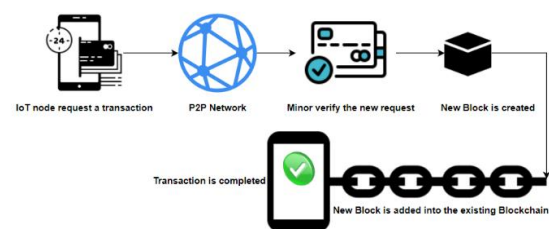


Figure 2: Transactions in IBchain.

c) Technology tools d) Blockchains [26]. It creates a basis for accessing secure data documents through IoT nodes.

Blockchain exchanges can be controlled or approved by another node confirmed to communicate with the IoT network [27]. IBchain can improve communication protection. The main advantages of IBchain are:

- 1) Communication between IoT devices or minimizing the chance of confrontations.
- 2) To minimize operating costs by having conversations without a third - party.
- 3) accelerating transaction data.

Many transactions are issued in the permitted blockchain-based file via simulation services, service providers, or cloud holders. The IoT nodes find smart contacts from inside the approved blockchain-based archive [28]. This approved blockchain-based archive creates the token for IoT nodes. This IoT node demands its key in the development tools from the remote system and guides the request key [29]. The main system authenticates the tokens from an authorized blockchain archive or generates a key per IoT node and system reaction [30]. An IoT node is enabled to collect data on the network. IoT is becoming an innovation of significant impact throughout many market sectors. Most IoT systems are designed to have worldwide coverage through thousands of easy and often embedded systems. Also, the limited capacities of many IoT devices, and the existing communications systems focused on centralized frameworks, are posing major issues in the IoT environment [31]. The blockchain has gained popularity in the IoT environment [32]. A business entity has indeed created the activewear platform for the internet bedding element [33]. Considered as the first and only one of such types, the solutions aimed to deal with the major IoT assaults with more participants and structural breakups than conventional aspects [34]. The research facility is aimed to further enhance the development and distribution of technology and its ability to change IoT. Blockchain on IoT is booming but does not have a few blocks.

In the experiment, three devices are considered to evaluate the method, however, in the future, we can enhance it for several IoT nodes [35]. After generating the session, the IoT nodes can communicate directly. Consider the D1, D2 and D3 are three IoT devices, connected in IBchain network with the shared hash code H. The Encryption key for D1 is D1E and the Decryption key for D1 is D1D. Consider D1 device is sending information to D2 and D3. IoT nodes D1, D2, and D3 are used in the challenges (ch)D1, (ch)D2, and (ch)D3 for confirming the secret hash code H generated by the blockchain. In the end, the IoT nodes will generate the final session key  $S = (SA, SB, SC)$  and distribute it to all connected nodes in the network. The following procedure will perform.

- (1)  $D1 \rightarrow D2: A, C(D1E),$   
 $D1 \rightarrow D3: A, C(D1E)$  and so on.
- (2)  $D2 \rightarrow D1: C(D1E (ACK, SD2)),$   
 $D3 \rightarrow D1: C(D1E (ACK, SD3)).$
- (3)  $D1 \rightarrow D2, D3: ACK(SD1).$
- (4)  $D1 \rightarrow D2, D3: K(SD1, h(SD1, SD2, SD3)).$

In (4), D1 is the sender, and D2, D3 are the receivers.

- (5)  $D2 \rightarrow D1: K(SD2, h(SD1, SD2, SD3))$   
 $D3 \rightarrow D1: K(SD3, h(SD1, SD2, SD3)).$

In (5), D2, D3 are senders and D1 is the receiver.

Data packets are distributed in the cloud by using IoT devices. All blocks have their cryptographic hash, the previous hash block code, and its information in Blockchain. Blockchain does have a link to the sharing of data. Respectively data holds numerous blocks including the prior hashing with block information. Those blocks have been interconnected through authentication via cryptographic algorithms. Blockchain is like the linked node in the linked list. Its blocks are distributed in a decentralized structure to use a P2P topology framework. Adding a novel block jumps to the system, visits each node associated with the network, and confirms the security.

Information transmission between the IoT devices in the network could pass information from IoT-gateways (IG), cloud gateways (CW), blockchain gateways (BG), or other gateways (OG). OG is the sequence of specific gateways other than the IG. IG is the compilation of accesses between the IoT nodes. Imagine that the interaction wait between IoT nodes is wonder about inconsequential. Think About  $t_1, t_2, t_3,$  and  $t_4$  are the communications deferral functions between the IoT gadgets and OG, OG and IG, IG and CG, and CG and BG.  $L_1, L_2, L_3,$  and  $L_4$  are the latencies of OG, IG, CG, and BG. Therefore, it implied broadcast latency could be achieved through the next method.

$$\sigma = (t_1\mu + t_2\theta + t_3\tau + t_4\epsilon) + (L_1\mu + L_2\theta + L_3\tau + L_4\epsilon) \tag{2}$$

Here  $\mu, \theta, \tau$  and  $\epsilon$  ( $\mu > \theta > \tau > \epsilon$ ) are the overall information packets delivered by IoT nodes, OG, IG, and CG. The information is conveyed from IoT nodes to the OG and OG to the IG then it needs power utilization.

The effectiveness of the suggested method is analyzed via a variety of experimentation. Initially, hundreds of blocks of stable amount using an open-source package (Node.js) are designed and IoT system, linked to the amazon cloud, and create the blockchains network.

IBchain uses smart devices on the network edge of blockchain networks to interact, transfer, and distribute data between IoT nodes. Exchanges in the proposed work have been transmitted to the p2p network. Many special IoT nodes are referred to as Miners in the network. It is typically used in the verification of blockchain networks. If the transactions are processed in such a way that they

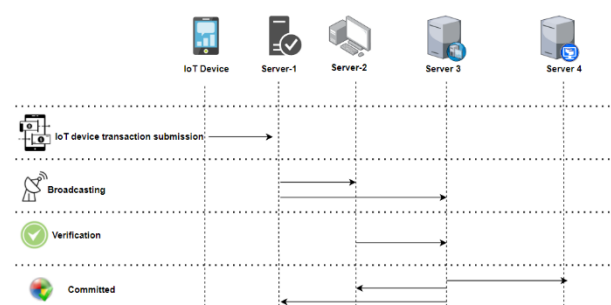


Figure 3: The Sumeragi in Hyperledger IROHA method.

are converted into blocks or agreed to connect to the current blockchains or transferred to the internet.

The miners have a critical role to play in integrating the development of a new block in the blockchains. The hashing technique is designed using the Hyperledger IROHA method. Figure 3 shows the IROHA method.

Stage 1. Transmission: verify, organize, or register transactions or submit information to the program.

Stage 2: verification and sign-up: this validates, queries, or signs transactions or distributes the verified IoT node of the P2P platform.

Stage 3: linked to the having signed.

In the case of system failure, the automatic program leads to a step called error tracking. Throughout fact, the technique performs with the current server to detect discrepancies. Study researchers compared the efficiency of 5 and 10 IoT nodes using investigations. Figure 4 shows the performance of 1 to 20 IoT devices with comparison analysis for discovering, choosing, and analyzing techniques.

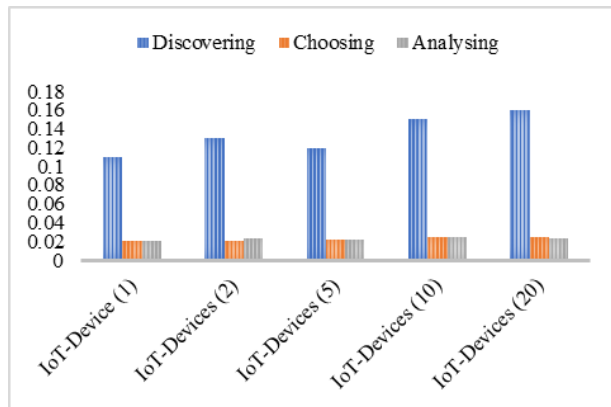


Figure 4: discovering, choosing, and analyzing 1 to 20 IoT devices.

Considering the 5 IoT devices linked to the 500, 1000, 300, 700, and 1500 mining power P2P services. The devices are in a position to carry out exchanges within the suggested technique. The header size 100 bytes and the transaction size 500 bytes are assumed. There are five IoT devices in the network.

IBchain system is evaluated with 5 IoT nearby devices and 2 distanced IoT devices. The blockchain-retrieved information in the cloud of a technology named the OPENSIFT framework. The FogSim technology is being applied to link the IoT devices to the network. The cloud is provided through the Amazon server. Figure 5 shows the execution factors in the IBchain.

IBchain requires miners in the blockchains network for a result of a study conducted. Initially, two miners were chosen with fixed exchanges (assume 5) as well as establish the nebula specifications with miners. Secondly, three miners of specific transactions (assumes 5) or established the nebula specifications for miners. Unless the cloud market is rising, the probability of mines the miner's block is stronger. Modeling criteria like the use of a processor, use of storage in blockchains compared with cloud, and edge are tested. I realized that its use processors in blockchains were smaller than cloud and

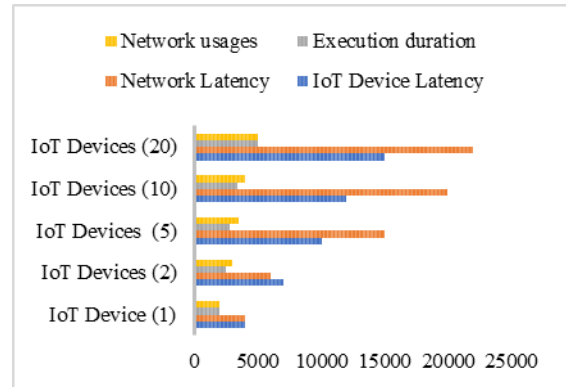


Figure 5: The execution factors in the IBchain.

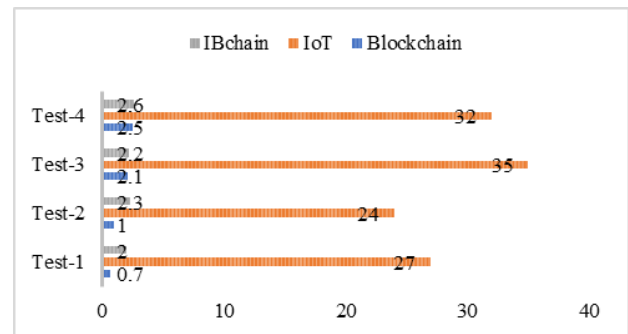


Figure 6: The Transmission delay in IBchain.

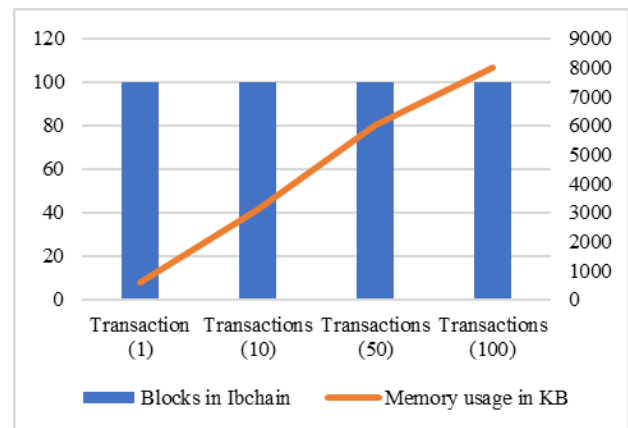


Figure 7: Usage of Memory and blocks in IBchain.

Nodes	Delay in ms	Duration time	Power consumption in KJ
5	146.5	288	5.2
5	12.3	703	5.2
5	99	905	5.5
10	15.1	225	12
10	12.4	499	15.9
10	53.2	293	11.7

Table 1: Power Consumption using different nodes.

IoT. Using storage based on the number of blocks with the volume of data. When the block size increase, storage use may also enhance. Likewise, as the number of transactions increases, storage use would therefore rise. Figure 6 shows the transmission delay in IBchain.

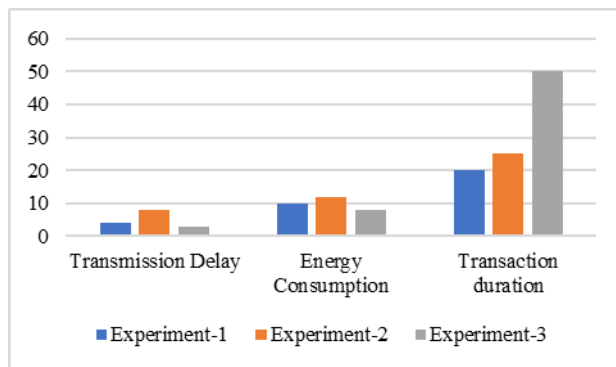


Figure 8: Performing on 10 IoT devices in IBchain.

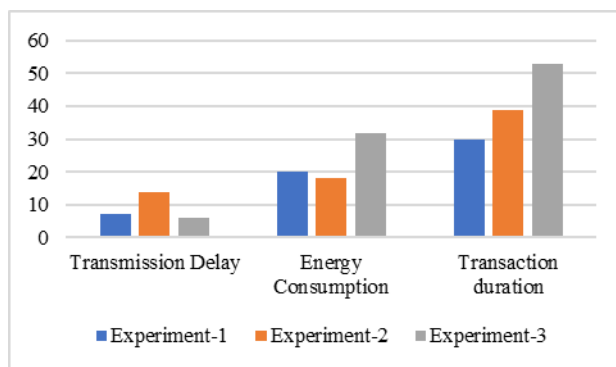


Figure 9: Performing on 20 IoT devices in IBchain.

Figure 7 shows the memory usage and number of blocks. Figure 8 and 9 shows the performance of 10 and 20 IoT nodes with three experiments. Table 1 represents the power consumption using different IoT nodes.

The author is implemented as an interface in JavaScript that assists the IoT devices to link with the IBchain system. This framework applies the web3 JavaScript libraries towards connecting through Ethereum domains via RPC requests and the CoAP JS APIblockchain-based-CoAP 5 to access sensor nodes.

## 4 IBchain for smart cities

Smart cities are being built and people can be recognized as smart residents pretty soon. Human lives will be exchanged and there are many advantages: smooth, processed public transport operations and vacated traffic, reduced crime rates, automated scheduling, service growth, and beyond.

### 4.1 Data collection blockchain

Current scientific requirements in the city involve the selection of sensors for data collection. It may be non-driving, delivery drones, city tracking cameras, automated lights, and any other calculating equipment. This makes it necessary to gather personal data, and it is thus essential to store the information. Gathering the personal realities and maintaining them gives the lives of all human beings an opportunity. Smart city solutions developers should provide evident client confidentiality, privacy, and security information. That is why blockchain technology offers all participants of this sort of system the possibility

to gather and exchange their information with a very high level of authenticity and security without the participation of one regulator or intermediary.

### 4.2 Smart cities thrive through blockchain

In future cities, there are several possibilities using blockchain integration. Smart contracts, for instance. Such contracts could be concluded autonomously if pre-mounted circumstances (for example, a person, an object, or gadget with other smart aspects) are satisfied among various occurrences. Due to its security and technological versatility, Blockchain maintains smart contracts. A cloud-enabled parking system is required for assigned vehicle storage. Blockchain chronology may be utilized to make a cloud analog convenient and secure, which ensures responsibility and transparency. Asset management responses and budget management may enhance efficiency and assure visibility by eliminating inefficient verification actions via the use of blockchain generation at the city level. All online-based sensors can identify and transmit data and perform operations in smart cities. Data from city sensors may be transformed into commercial units because of blockchain usage. Consider that the parking sensor generates data on whether it belongs or not at the moment. These statistics are acquired by the parking searches operator in the smart city. The non-public profession of engaging in sensors and restoring nerves chips could be focused on such possibilities. This technology enables a combination of a range of network and robotic offers, prevents safety violations, and guarantees that transactions go uninterrupted.

### 4.3 Present smart city blockchain software

Developers of smart cities frequently respond to ethical problems, technological integration difficulties, and regulatory restrictions, etc. several intriguing initiatives are excited about IoT integration. For individuals who have strong market positions: IoTA and robonomics. They worked endlessly and transparently and built integration solutions for various areas of smart cities. These are all based on over five years ago. These are both open-ended technologies that enable developers to promote improvements and to construct new projects based mainly on applications. When you think about 2015, IoTA was present and found the solutions by pursuing the "internet of things." This framework involves the authority to transmit important information and data between people and machines. Security violations also lead to insecurity of IoTA by 2020, amongst other deficiencies. It was one of the top five currencies before hacking. Its market value at the time was conserved for more than \$13 billion. Robonomics is an open IoT supply chain moderate platform. Professionals strive to create the notion of "robotic industry," in the actual global economic system, using robots and different computer systems as full-service agents. Intelligent devices may choose their storage independently, pay for electricity, and so on. Furthermore, robonomics improves the natural functions of tracking air quality with the assistance of drone sensors and water pollution processes.

#### 4.4 The industry 4.0

The fourth revolution in commerce has arrived in humanity; reproduction is an important part of our life. Building intelligent cities are unavoidable. It is therefore vital for the aesthetic appearance and privacy of the user to expand their timely responses. This estimate could assist with blockchain latency and address various behavioral issues.

### 5 Discussion

Blockchain is a shared ledger idea that combines with IoT to allow device-to-device interactions. It employs data activities stored in a database which are validated through several resources and included in a standard ledger distributed throughout each node. The combination of IoT and blockchain gives the advantages of distinct technologies and enables an intelligent tool to function autonomously without a central authority. IoT devices employ smart contracts to enable data transmission that resolve the settlement between the two parties [36]. This option allows smart devices to run independently without a central authority. Blockchain can assist to minimize IoT and IoT-related safety problems by a ledger is concerning evidence on a blockchain device, which eliminates the need to rely on the many parties involved. No organization can manage a considerable number of statistics created by IoT devices [37]. Additional security layers, that hackers can breakthrough, may need to be loaded with the usage of a blockchain to maintain IoT data. Blockchain gives a further degree of coding, which does not prevent the bypassing of known information [38]. Blockchain enables transparency, by enabling any authorized individual to access the community through previous content. It could give a safe approach to recognize and undertake brief corrections for a successful move for any verifiable disclosure. Blockchain could enable transactions and communications between billions of connected devices to be processed more quickly. The shared production of the text provides a valuable approach to aid with the largest transactions with the growing range of connected gadgets. By establishing a method for enhancing the confidence of stakeholders, IoT companies may decrease costs by removing high-level processes. Users are strong smart devices with tremendous capabilities to disseminate safety improvements, which will certainly assist safeguard the most susceptible devices [39][40][41]. Blockchain and IoT are also anticipated to endure regulatory problems. For example, for companies, multi-source transactions may be managed in a consistent and visible document, which tracks records and physical assets during the transaction time. A blockchain report should be able to determine the moment – say tool or sensor – when anything has gone wrong during incorrect selection or overloading of a device, and businesses may take a rapid turnaround. IoT enables users to transmit information to blockchains public ledger for participation in public transactions with databases. The Blockchains allow the business participants to connect and distribute IoT data and no need for centralized controlling. The agreement

should be checked to avoid conflicts and to ensuring that each participant is kept responsible for certain specific activities. Construct a trustworthy and productive business among individuals and organizations which are working collectively. IoT nodes could engage in exchanges as a decentralized group. Its undeniable activities from devices recorded on the blockchain offer evidence of collaboration between companies and individuals. Improve efficiency for the design, management, and compliance of agreements by exchanging data between different groups. The participant in Hyperledger is the IoT device. The agreement is allowed to consent to the status of a distributed public blockchain network [42][43][44]. Generate a continuous or indelible database provided by the business and industry policies. Enhance exchanges to make it easier for customers and allow emerging technologies. Smart cities will deliver the best services to improve residents' everyday lives in the areas of medical care, mobility, power usage, and learning. Moreover, the idea of smart cities is still emerging, and, considering its desired future, privacy concerns have been on the emergence. distributed ledger provides the opportunity to facilitate the growth of smart cities due to its positive characteristics like accountability, efficiency, flexibility, and distribution. IoT is shaping the direction of businesses by the utilization of sensor nodes as well as other motion-connected technologies. It is a significant strategic initiative that needs to preserve knowledge at all stages of the IoT network. For the number of sensors emerging annually, information security is becoming highly complicated. Blockchains can tackle security risks in the embedded network. Blockchains and IoT are integrating throughout all sectors, involving banks, finance, manufacturing, and agricultural sectors. Also, in smart homes, suppliers, transportation, and agreements. Agreements connect blockchains to IoT systems to immediately enforce each transaction after certain tasks have been completed. The use of these blockchains helps businesses to process the information on sensor nodes in an IoT environment, decreasing the cost related to mobile device improvement and secure communication. This eliminates the risk of information management since there is no centrally controlled repository of information. In addition to safety, the blockchain gives clever city inhabitants the opportunity of earning more funds, secure agreements, machine communication, and other possibilities. The sophisticated technology in the market and use of IoT and robotics offer solutions for the interconnection of connected devices, their integration into the human economic system as contributors, transparent and convenient records administration, and much more. In keeping with the global financial forum research, efforts to create blockchain solutions for smart cities retain the best market potential

### 6 Conclusion

This research approach is developed and constructed using IoT, clouds, and blockchains. It is an integration of IoT and Blockchains. Blockchains technology is used to generate a highly distributed public realistic database for

transaction processing. Analysis has created an entirely new possibility throughout this field. A methodology is designed and evaluated to use a wide variety of IoT devices. This research could be a useful tool for improving the efficiency of the IoT system in an interconnected context. The method is designed to provide interaction security where big data are exchanged in a complex context in the long run. Researchers have evaluated the system in several situations, like memory and storage use in the integrated system and its effect on the secure operation. Researchers find that the suggested method improves the performance and removes the direct relation between IoT devices, making this method further reliable. Its research findings set out an innovative IoT framework with blockchains.

## References

- [1] Alam, Tanweer. "IoT-Fog-Blockchain Framework: Opportunities and Challenges." *International Journal of Fog Computing (IJFC)* 3.2 (2020): 1-20. DOI: <https://doi.org/10.4018/IJFC.2020070101>
- [2] Wang, Xu, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Xinxin Niu, and Kangfeng Zheng. "Survey on blockchain for Internet of Things." *Computer Communications* 136 (2019): 10-29. DOI: <https://doi.org/10.1016/j.comcom.2019.01.006>
- [3] Conoscenti, Marco, Antonio Vetro, and Juan Carlos De Martin. Blockchain for the Internet of Things: A systematic literature review. In 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-6). IEEE. (2016). DOI: <https://doi.org/10.1109/AICCSA.2016.7945805>
- [4] Alam, Tanweer. "Design a blockchain-based middleware layer in the Internet of Things Architecture." *JOIV: International Journal on Informatics Visualization* 4, no. 1 (2020): 28-31. DOI: <http://dx.doi.org/10.30630/joiv.4.1.334>
- [5] Alam, Tanweer, and Mohammed Aljohani. "An approach to secure communication in mobile ad-hoc networks of Android devices." In 2015 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), pp. 371-375. IEEE, 2015. DOI: <http://dx.doi.org/10.1109/ICIIBMS.2015.7439466>
- [6] Alphand, Olivier, Michele Amoretti, Timothy Claeys, Simone Dall'Asta, Andrzej Duda, Gianluigi Ferrari, Franck Rousseau, Bernard Tourancheau, Luca Veltri, and Francesco Zanichelli. "IoTChain: A blockchain security architecture for the Internet of Things." In 2018 IEEE wireless communications and networking conference (WCNC), pp. 1-6. IEEE, 2018. DOI: <http://dx.doi.org/10.1109/WCNC.2018.8377385>
- [7] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." *Ieee Access* 4 (2016): 2292-2303. DOI: <http://dx.doi.org/10.1109/ACCESS.2016.2566339>
- [8] Jiang, Tigang, Hua Fang, and Honggang Wang. "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis." *IEEE Internet of Things Journal* 6, no. 3 (2018): 4640-4649. DOI: <http://dx.doi.org/10.1109/JIOT.2018.2874398>
- [9] Alam, Tanweer. IoT-Fog: A communication framework using blockchain in the internet of things. *International Journal of Recent Technology and Engineering (IJRTE)*. Vol. 7(6), 2019. DOI: <http://dx.doi.org/10.22541/au.159164762.24316077>
- [10] Alam, Tanweer, and Mohamed Benaida. The role of cloud-MANET framework in the internet of things (IoT). *International Journal of Online Engineering* 14, no. 12 (2018). DOI: <http://dx.doi.org/10.3991/ijoe.v14i12.8338>
- [11] Teslya, Nikolay, and Igor Ryabchikov. "Blockchain-based platform architecture for industrial IoT." In 2017 21st Conference of Open Innovations Association (FRUCT), pp. 321-329. IEEE, 2017. DOI: <http://dx.doi.org/10.23919/FRUCT.2017.8250199>
- [12] Alam, Tanweer. "Blockchain cities: the futuristic cities driven by Blockchain, big data and internet of things." *GeoJournal* (2021): 1-30. DOI: <https://doi.org/10.1007/s10708-021-10508-0>
- [13] Yang, Yanhan, Yaming Yang, Jinlian Chen, and Mingzhe Liu. "Application of blockchain in internet of things." In *International Conference on Cloud Computing and Security*, pp. 73-82. Springer, Cham, 2018. DOI: [https://doi.org/10.1007/978-3-030-00018-9\\_7](https://doi.org/10.1007/978-3-030-00018-9_7)
- [14] Mo, Bing, Kuiren Su, Songjie Wei, Cai Liu, and Jianping Guo. "A solution for internet of things based on blockchain technology." In 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 112-117. IEEE, 2018. DOI: <https://doi.org/10.1109/SOLI.2018.8476777>
- [15] Alam, Tanweer, and Mohamed Benaida. CICS: Cloud-Internet Communication Security Framework for the Internet of Smart Devices., *International Journal of Interactive Mobile Technologies (iJIM)* 12, no. 6 (2018). DOI: <https://doi.org/10.3991/ijim.v12i6.6776>
- [16] Alam, Tanweer, and Mohamed Benaida. "Blockchain and Internet of Things in Higher Education." *Universal Journal of Educational Research* 8 (2020): 2164-2174. DOI: <https://doi.org/10.13189/ujer.2020.080556>
- [17] Samaniego, Mayra, Uurtsaikh Jamsrandorj, and Ralph Deters. "Blockchain as a Service for IoT." In 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData), pp. 433-436. IEEE, 2016. DOI: <https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102>
- [18] Banafa, Ahmed. "IoT and blockchain convergence: benefits and challenges." *IEEE Internet of Things* (2017).
- [19] Florea, Bogdan Cristian. "Blockchain and Internet of Things data provider for smart applications." In 2018



- 7th Mediterranean Conference on Embedded Computing (MECO), pp. 1-4. IEEE, 2018. DOI: <https://doi.org/10.1109/MECO.2018.8406041>
- [20] Jo, Byung Wan, Rana Muhammad Asad Khan, and Yun-Sung Lee. "Hybrid blockchain and internet-of-things network for underground structure health monitoring." *Sensors* 18, no. 12 (2018): 4268. DOI: <https://doi.org/10.3390/s18124268>
- [21] Di Pietro, Roberto, Xavier Salleras, Matteo Signorini, and Erez Waisbard. "A blockchain-based trust system for the internet of things." In *Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies*, pp. 77-83. 2018. DOI: <https://doi.org/10.1145/3205977.3205993>
- [22] Minoli, Daniel, and Benedict Occhiogrosso. "Blockchain mechanisms for IoT security." *Internet of Things* 1 (2018): 1-13. DOI: <https://doi.org/10.1016/j.iot.2018.05.002>
- [23] Zhao, Shanshan, Shancang Li, and Yufeng Yao. "Blockchain enabled industrial Internet of Things technology." *IEEE Transactions on Computational Social Systems* 6, no. 6 (2019): 1442-1453. DOI: <https://doi.org/10.1109/TCSS.2019.2924054>
- [24] Casado-Vara, Roberto, Fernando de la Prieta, Javier Prieto, and Juan M. Corchado. "Blockchain framework for IoT data quality via edge computing." In *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*, pp. 19-24. 2018. DOI: <https://doi.org/10.1145/3282278.3282282>
- [25] Rakovic, Valentin, Jovan Karamachoski, Vladimir Atanasovski, and Liljana Gavrilovska. "Blockchain paradigm and Internet of Things." *Wireless Personal Communications* 106, no. 1 (2019): 219-235. DOI: <https://doi.org/10.1007/s11277-019-06270-9>
- [26] Choudhary T., Virmani C., Juneja D. Convergence of Blockchain and IoT: An Edge Over Technologies. In: Hassanien A., Bhatnagar R., Khalifa N., Taha M. (eds) *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*. Studies in Computational Intelligence, vol 846. Springer, Cham. 2020. DOI: [https://doi.org/10.1007/978-3-030-24513-9\\_17](https://doi.org/10.1007/978-3-030-24513-9_17)
- [27] Alam, Tanweer. "Blockchain and its Role in the Internet of Things (IoT)." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 5, no. 1 (2019). DOI: <https://doi.org/10.32628/cseit195137>
- [28] Alam, Tanweer. Middleware implementation in cloud-MANET mobility model for internet of smart devices. *International Journal of Computer Science and Network Security*, 17(5), 2017. Pp. 86-94. DOI: <http://dx.doi.org/10.2139/ssrn.3638980>
- [29] Urmila, M. S., Balaji Hariharan, and Rekha Prabha. "Enabling Internet of Things (IoT) Security via Blockchain Framework." In *Innovations in Computer Science and Engineering*, pp. 575-582. Springer, Singapore, 2020. DOI: [https://doi.org/10.1007/978-981-15-2043-3\\_62](https://doi.org/10.1007/978-981-15-2043-3_62)
- [30] Pavithran, Deepa, Khaled Shaalan, Jamal N. Al-Karaki, and Amjad Gawanmeh. "Towards building a blockchain framework for IoT." *Cluster Computing* 23, no. 3 (2020): 2089-2103. DOI: <https://doi.org/10.1007/s10586-020-03059-5>
- [31] Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." *IEEE Internet of Things Journal* 5, no. 2 (2018): 1184-1195. DOI: <https://doi.org/10.1109/JIOT.2018.2812239>
- [32] Dai, Hong-Ning, Zibin Zheng, and Yan Zhang. "Blockchain for Internet of Things: A survey." *IEEE Internet of Things Journal* 6, no. 5 (2019): 8076-8094. DOI: <https://doi.org/10.1109/JIOT.2019.2920987>
- [33] Alam, Tanweer. "Blockchain-based big data integrity service framework for IoT devices data processing in smart cities." *Mindanao Journal of Science and Technology* (2021). DOI: <http://dx.doi.org/10.2139/ssrn.3869042>
- [34] Uddin, Md Ashraf, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. "A survey on the adoption of blockchain in iot: Challenges and solutions." *Blockchain: Research and Applications* (2021): 100006. DOI: <https://doi.org/10.1016/j.bcra.2021.100006>
- [35] Mahbub, Mobasshir. "Blockchain Technologies for Securing IoT Infrastructure: IoT-Blockchain Architectonics." In *Blockchain Applications in IoT Ecosystem*, pp. 187-202. Springer, Cham, 2021. DOI: [https://doi.org/10.1007/978-3-030-65691-1\\_13](https://doi.org/10.1007/978-3-030-65691-1_13)
- [36] Latif, Shahid, Zeba Idrees, Jawad Ahmad, Lirong Zheng, and Zhuo Zou. "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things." *Journal of Industrial Information Integration* 21 (2021): 100190. DOI: <https://doi.org/10.1016/j.jii.2020.100190>
- [37] Maitra, Sudip, Venkata P. Yanambaka, Deepak Puthal, Ahmed Abdelgawad, and Kumar Yelamarthi. "Integration of Internet of Things and blockchain toward portability and low-energy consumption." *Transactions on Emerging Telecommunications Technologies* 32, no. 6 (2021): e4103. DOI: <https://doi.org/10.1002/ett.4103>
- [38] Wu, Xu, and Junbin Liang. "A blockchain-based trust management method for Internet of Things." *Pervasive and Mobile Computing* 72 (2021): 101330. DOI: <https://doi.org/10.1016/j.pmcj.2021.101330>
- [39] Li, Yuyao, and Ashutosh Sharma. "Regional Network Education Information Collection Platform for Smart Classrooms based on Big Data Technology." *Informatica* 45, no. 5 (2021). DOI: <https://doi.org/10.31449/inf.v45i5.3555>
- [40] Veselov, Gennady, Alexey Tselykh, Ashutosh Sharma, and Ruihang Huang. "Applications of Artificial Intelligence in Evolution of Smart Cities and Societies." *Informatica* 45, no. 5 (2021). DOI: <https://doi.org/10.31449/inf.v45i5.3600>
- [41] Tran, Hai Anh, Duc Tran, Linh Giang Nguyen, Quoc Trung Ha, Van Tong, and Abdelhamid Mellouk. "SHIOT: a novel SDN-based framework for the heterogeneous internet of things." *Informatica* 42, no. 3 (2018). DOI: <https://doi.org/10.31449/inf.v42i3.2245>
- [42] Maurya, Sudhanshu, and Kuntal Mukherjee. "An energy efficient architecture of IoT based on service

- oriented architecture (SOA)." *Informatica* 43, no. 1 (2019). DOI: <https://doi.org/10.31449/inf.v43i1.1790>
- [43] Alam, Tanweer. "Cloud-Based IoT Applications and Their Roles in Smart Cities." *Smart Cities* 4, no. 3 (2021): 1196-1219. DOI: <https://doi.org/10.3390/smartcities4030064>
- [44] Alam, Tanweer, Abdirahman Ahmed Hadi, and Rayyan Qari Shahabuddin Najam. "Designing and implementing the people tracking system in the crowded environment using mobile application for smart cities." *International Journal of System Assurance Engineering and Management* (2021): 1-23. DOI: <https://doi.org/10.1007/s13198-021-01277-7>