Secure BlockChain protocol for IOT Business Applications

Vikram Dhiman
Lyallpur Khalsa College of Technical Campus, Jalandhar, India

Bhavneet Singh
Global Group of Institute, Amritsar Punjab India

Sapinderjit Kaur
Global Group of Institute, Amritsar Punjab India
Corresponding author: Vikram Dhiman, Email: er.vikramdhiman@gmail.com

The Internet of Things (IoT) specifies the connection of physical items that, for the purpose of sharing data and of interacting with other devices or systems through the Internet, include software, sensors, and other technologies. IoT equipment shares the sensor data it gathers with an IoT gateway or another peripheral device in which data are either referred to the cloud for local analysis. The combination of IoT and BlockChain opens the door for new possible experiences that reduce inefficiencies, enhance safety and expand the vision of all involved parties while enabling safe machine-to-machine transactions. Coupling these technologies makes it possible to trace a physical asset from the time, for instance, the mining of raw materials and between every stage of the supply chain to the end customer Internet of Things (IoT) connects the devices, objects through the internet using wireless technology. The proposed hybrid BlockChain solution offers several sorts of characteristics, including improved and more effective failure tolerance, improved system dependability, scalability and cheaper operating expenses.

Keywords: IOT, Block chain, Hash function, Proof-of-work, DApp.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 25–35. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-4

1 Introduction

IoT technology is most identical with goods that are related to the notion of "smart home" and include equipment or appliances such as thermostats, lighting devices, home safety devices and cameras, and other home appliances that support one or more of these common ecosystems. An IoT ecosystem contains of web-enabled smart devices that use embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices exchange the collected sensor data by attaching it to an IoT gateway or another edge device that either directs the data to the cloud for locally analysis. These devices may connect with other related devices and use information they get from each other. Devices function mostly without human interaction, although individuals can engage with devices, for example to set up them, provide instructions or access to the data. The connection and networking protocols with web-enabled devices rely greatly on the individual IoT applications utilized. IoT may also utilize artificial intelligence (AI) and machine learning to make it easier and more dynamic to collect data. In early 2015, Bit coin, an experimental decentralized digital currency, was accessible to all 4,584 alumni of the Massachusetts Institute of Technology. As a unique aspect of the project, students who would usually accept the technology got access to many their classmates first and then had to select whether to continue to invest in or leave this digital currency. When a new transaction is transmitted from computer to computer, it is transferred until everybody has a copy of the transaction. A distributed system computer will add the newest transactions to the BlockChain and distribute the update with all the others on the network at around 10 minute's interval. However results imply that natural early adopters would more likely reject the technology when they are delayed relative to their peers. Transactions across a computer network before Bit coin could be relayed. The difficulty though is that contradictory transactions can be inserted into a computer network. For example, two different transactions can be created that use the same digital coin, and both transactions can be sent to the network simultaneously. That's called a "double spending. IoT helps to transfer, communicate, and share the data anywhere at any time via the internet [1]. It creates a remote environment for accessing the data and it has been used in many real-time applications such as smart cities, smart homes, smart energy, smart agriculture, smart industry, and smart living. IoT has its characteristics which include interconnectivity, safety, heterogeneity, enormous scale, dynamic changes, and connectivity. The IoT environment is specified in fig. 2. IoT is a combination of several technologies such as embedded systems, pervasive computing, Actuators, Ambient Intelligence, Sensors, Internet Technologies and communication technologies, etc., IoT is classified based on their functionalities [2]. It consists of three functionalities there are Things oriented, Semantic oriented, and Internet-oriented. IoT's primary objective is to facilitate operations, remote access control, settings and end-users. In addition to diverse networks, IoT offers seamless connection. Block chain technology is the missing link in the Internet of Things to address privacy and reliability problems. The silver bullet needed by the IoT sector may be a block chain technology. It may be used to track billions of linked devices that enable transactions to be processed and device coordination, which enables considerable savings for IoT manufacturers. This decentralized method would eliminate single failure points and provide the gadgets with a more robust environment. Block chains' usage of cryptographic methods would secure customer information. The leader is manipulative and cannot be influenced by bad actors as it is not present in any one place and human attacks cannot be carried out since there is nothing that can intercept a single communication thread. Block chain makes it possible to send messages without any confidence and by offering assured pair-to-peer payment services without the need for third parties' brokers in financial-services worldwide through crypto currencies like bit coin. IT solutions are based on the decentralized, autonomous, and untruthful capacities of the block chain as an optimal component. It is no wonder that IoT technologies from companies have been one of the early users of block chain technology.

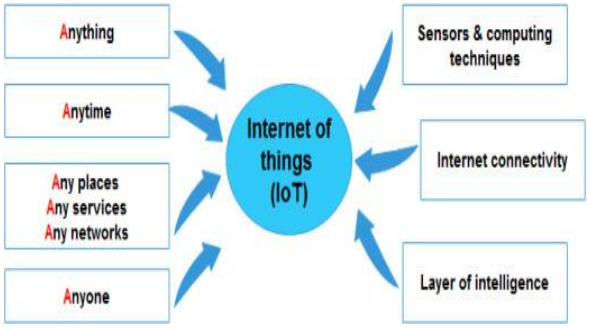

Fig. 1. IOT

The block chain may store the history of intelligent devices in an IoT network. This capability allows smart devices to work autonomously without centralization. The block chain therefore opens the door to a number of IoT scenarios which, without it, have been extraordinarily difficult or even impossible to carry out. The block chain is a database that keeps an increasing number of data records. It is dispersed in nature, which means that the chain does not have a master computer. Instead, the nodes involved have a copy of the chain. It is also increasing — only data files are added to the chain. There are two kinds of elements in a block chain: Transactions are measures developed by the system participants. These transactions are recorded by blocks and verified that they are in the right sequence and not manipulated.

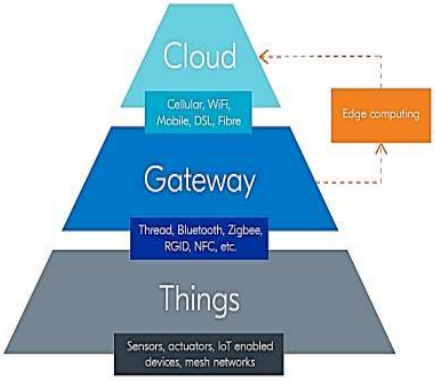

Fig. 2. IoT Environments

2 Literature Survey

In this paper, [3] an IoT security solution based on a block chain was suggested, where the immutable and decentralized characteristics of the block chain built trust. The distributed nature of the block chain makes the system stronger and more resistant from one single failure point. In their evaluation of genuine user presence in the valid IoT zone constantly, the authors suggested a technique for establishing continuous security in the systems. Each user transaction was saved in the block chain of

an IoT environment, and a number were an IoT trail for a user. For authorized user interactions a unique digital crypto-token is necessary. This token is used to prevent unwanted access to the system as an access control mechanism.

Tokens are regenerated using a user IoT trail in the block chain prediction model. The authors have secured, resilient and interoperable improved the system by utilizing BlockChain as a basic foundation in IoT environment and by means of the continuous security approach. In the paper [3] an initial milestone was made in creating hybrid architecture for IoT, the Hybrid-IoT BlockChain. In Hybrid-IoT, IoT subgroups make up PoW BlockChain called sub-block chains of PoW. Then, the link between the PoW substrates uses a BFT connector structure, such as Polkadot or the universe. The authors concentrated on the construction of PoW sub BlockChain, based on a set of dimensions, metrics and boundaries. We conduct a performance and security assessment to demonstrate the legitimacy of the method. This study author [4] looked at a key use of the CTNs (i.e. IoT) and proposed to use a BlockChain method for a safe Hybrid Industrial IoT framework. The authors have utilized a hybrid industrial architecture in several countries with various divisions of a firm. Although IoT devices are utilized and help to reduce manufacturing costs as well as improve quality, IoT devices caused by different hackers can pose many dangers. IoT devices may be affected by intruders in order to execute harmful actions. In order to ensure transparency between different users in different locations, authors have utilized BlockChain as a way to extract information from IoT devices and store extract records in the BlockChain. In addition, experiments have been undertaken using the proposed framework against Block Chain's internal communication, with IoT devices being affected by a number of invaders. The findings were analyzed against the traditional technique and confirmed with better simulated results, providing a success rate of 89 percent across user request time, falsified attack, black hole attack and BlockChain technology authentication scenarios. In the article author [5] et al. has mentioned that BlockChain fundamental algorithms for big IoT systems are not viable. The sophisticated consensus-based safety must be reduced in order to make it scalable for IoT. In this paper the authors presented a new lightweight proof of the consensus method of Block & Trade (PoBT) for IoT Block Chain and its inclusion architecture. This method allowed both trades and blocks with decreased time to be validated. The authors also introduced a ledger distribution technique in order to reduce IoT node memory needs. Security concerns, computational time, memory and bandwidth needs analysis and assessment reveal a substantial improvement in system efficiency. This paper outlines the new framework for monitoring critical patient indicators utilizing BlockChain based smart contracts, offered by Faisal Jami [6] et al. The system is created and developed utilizing hyper leader, the company's distributed BlockChain-based application management platform. This method provides patients with a number of benefits, including as a comprehensive, unchanging record and worldwide access at any time to medical information. To get physiological data, the Libelium e-Health toolbox is utilized. In terms of transaction per second, transaction latency, and use of the resources, the performance of the planned and constructed system is tested through a common benchmark tool called hyper-leaders. In order to monitor patient data, the method presented was shown to outperform the conventional system of health care. Prince Waqas Khan [7] et al. introduced ADL methods, a hybrid model based on recurring neural networks in this study (RNN). Therefore, as a prediction model and genetic algorithm (GA) optimization, we have utilized long-term memory (LSTM) and recurring gate units (GRUs). The authors chose GA's best training settings and cascaded LSTM with GRU. For a varied number of users, the performance of the proposed system was assessed. This article seeks to enhance the use of advanced technologies by supply chain practitioners, and to assist industry develop policy based on the ADL forecasts. Deepa Pavithran[8] et al. present the latest analyses of the IoT block chain literature in this study. In addition to design considerations and problems to consider while developing block chain architecture for IoT, they identified five important components. He also highlights shortcomings that prevent the establishment of a safe IoT block chain structure. The authors simulated two distinct forms of BlockChain execution and recognized the significantly superior output of device by device than

gateway-based executions. Alkhazaali[9] in this publication proposed (IoT) rely mostly on clouds processing and data storage. The amount and speed of the data produced by IoT cannot be handled in the clouds. IoT is sensitive to delay and has limited resources. Fog computing advocated endorsing the requirements of the internet of things (IoT). Fog Computing expands the network edges of the cloud computing service. Use of fog decreases reaction time and overhead of the network while preserving security issues. The inter-dependence of Isolation and OS accomplished by virtualization. Block chain suggested resolving fog computing safety and privacy. A decentralized, unchangeable leader is a block chain. Fog Block Chain Computing as an IoT infrastructure is presented. Fog computing employed in this suggested work with the lightweight block chain. This modification supports the requirements of IoT with limited resources for low reaction time. Researchers examined the applicability of the system with a focus on data protection and safety – the applicability of the model being developed in concentration by distinct IoT demands and limitations. Response times and use of rams in 1000 transactions in the suggested model did not interfere with 100 and 300MiB. One of the primary problems associated with the use of the block chain is the necessity for suitable applications that benefit from the integration of block chain technology. Over the course of many years the Internet of Things (IoT) has been connected to security issues and issues and experts and organizations are beginning to study the use of the IoT security block chains. A distributing BlockChain leader is defective, which reduces the need for confidence for the parties involved, said Andres Ricaurte, senior vice president, IT Services Company World Payment Manager. Therefore, no one organization controls the vast volume of IoT device-generated data. Altering current data records by BlockChain encryption is almost difficult for anyone. In order to avoid unwelcome intruders from obtaining network access, another security layer is provided by using BlockChain to store IoT data. In this section, several layers of BlockChain are covered. Due to the rapid expansion and advancement of BlockChain technology, various applications are likely to appear over time. Some were previously accomplished, while some newest BlockChain technology innovations are anticipated for the future.

3 I Need A BlockChain, But Which One?

People argue which BlockChain variant is appropriate for certain applications, for e.g. permitted or unauthorized, public or private, hybrid or side Chain. It looks like all the hustle and bustle over "allowed vs. permission less" distracts us from a profound study of business challenges and solutions. Members in the community must choose sides. We're talking about technology - there's nothing like "good" or "bad," only use cases. Therefore, I thought about identifying criteria for building some type of BlockChain idea. The user's anonymity is not a criteria but a function. Even though validators are recognized and monitored, you can have anonymous users. Existing financial system clearly indicates that Confidence in a validator is something that links and cannot be considered globally with a certain user and validator. We conclude that the concept of an ecosystem and a BlockChain requires only 2 criteria:

1) Validators' level of anonymity (i.e. do we know their identity)
2) Confidence in validators ("since penalty for misconductivity is unavoidable")

The top-left quadrant tends to drift to full anonymity, Bit coin as a network threatens to become a simple multi-axis between large mining pools since they often control mining equipment too. Use security deposits and an election process to enhance reputation models on the top right, proof of stake is a good example. Such systems tend to develop into slightly decentralized, but quite fast federated networks. Use security deposits and an election process to enhance reputation models on the top right proof of stake is a good example. Such systems tend to become slightly decentralized, but quite fast, and connected, dozens of extremely strong nodes. In the lower left quadrant is utilized for building

national or cross-country BlockChain. Good overview of problems to scalability for various methods. Under the right quadrant, corporate systems will change and "BlockChain" will not be a point of sale at all. Traceability, flexibility, effective management and crypto-API for digital assets are what it means. The left top quadrant is for public BlockChain without authorization. Only work evidence may be applied here, as something outside of the system. To participate in the consensus process simply a computer required to be examined in past years

Table 1. A comparison of Technologies

	Traditional	**IOT**	**BlockChain + IOT**
Decentralized	centralized	centralized	decentralized
Reliability	Very Low	Low	High
Interoperability	Low	Low	High
Confidentiality	Low	Low	High
Storage	Low	Low	High
Immutable	Not immutable immutable	Not	Fully immutable

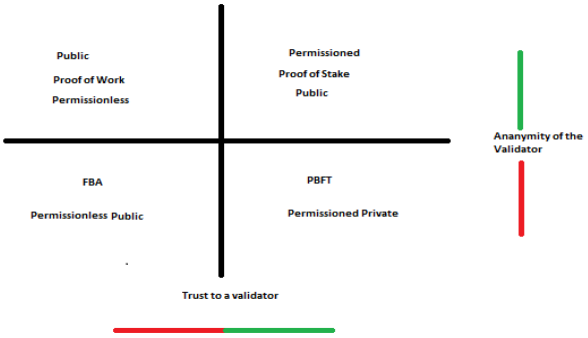

Fig. 3. BlockChain environment

4 Consensus Algorithm for BlockChain in IoT

In this paper, the consensus authentication proof methods were discussed which are especially suited for IoT devices. However, because of the unforeseen issues with IoT (IoT) devices utilized in this study, one method is substantially quicker than the other cannot be fairly compared. To function as a decentralized network, BlockChain systems need a consensus algorithm. An algorithm of consensus is a method used for device coordination in dispersed contexts. The machinery involved in the BlockChain network must agree on a single source of truth, which may be done through consensus. The transactions that are put into a block are immutable. The whole BlockChain integrity is threatened by a single fraudulent or incorrect trade. In this section we demonstrate our consensus method in an IoT context for corporate BlockChain. The plan is to do so as the technology of BlockChain evolves quickly and progresses various applications will evolve over time. But some have already materialized while others can be imagined

5 Smart Contract

A smart contract is a code collection and data collection that is used on a BlockChain; future transactions transmitted to the BlockChain can then send data to the smart contract's public methods. With the user's data supplied to conduct a service, the contract implements the relevant method. A smart contract can calculate, retain information, and transmit cash to other accounts automatically. It doesn't even have a financial purpose to execute. For instance, this document built intelligent contracts which publicly provide reliable random integers. BlockChain offers an intelligent contract platform. These are self-automated programmers residing on the BlockChain which incorporate business logic and code to perform a needed function when specific circumstances are fulfilled. This is a revolutionary aspect of BlockChain since it provides flexibility, programmability and much greater control of activities that BlockChain users have to carry out in accordance with their business requirements. Some of the main features of a smart agreement are:

1. Self-reliance
2. Decentralized
3. Automatic adequacy

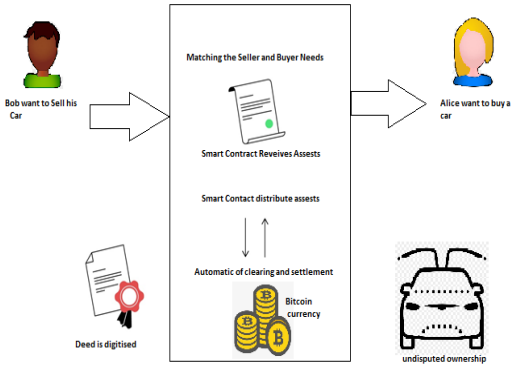

Fig. 4. Smart Contracts for the exchange of products and currency

A smart contract often includes some business logic and a small quantity of data. These smart contracts are used by BlockChain or participants. Alternatively they execute independently on the network's behalf participants. These mini-programs are stored on the BlockChain. If certain conditions are satisfied, business logic is executed.

6 Transaction Layout

Below is a generic block chain processing pipeline. A block chain is formed when a transaction occurs in a node. Every owner transfers the currency to the following one by digitally signing the previous transaction hash and adding the next owner's public key to the coin's end. A payee can check the signatures to check the ownership chain.

- All nodes will get new transactions. Hence new transactions are collected in one block by each node. Then each node uses its block consensus algorithm (often, node processing and electric power usage are costly).

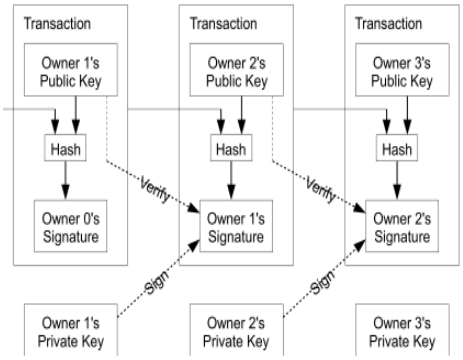

Fig. 5. Ownership Chain [10]

- When a node finishes processing the consensus method, it broadcasts the block and the processing results to all nodes. (In Bit coin, compensation is a transaction fee that the bit coin miner has processed and received.) Only if all transactions inside are legitimate, nodes will accept a block.
- Nodes indicate their approval of the block by utilizing the hash of the accepted block as the previous hash to create the new block. In the IoT environment, devices may be set to use the contract addresses of block chain to communicate with smart contracts. These gadgets can then enter into mutual transactions.

7 Communication Model

Every transaction is recorded on the BlockChain (BC), which enables cross-border general distributed trust. Trusted Third Party systems or central location-based services can be tainted or hacked on a regular basis. When transactions are approved by consensus in BC, the block data becomes acceptable to everybody. The BC can be built as a (1) permissioned network, which is often a private network, or (2) permission-less network, which is typically a public network. Permissioned BC provides enhanced privacy and access features. The BC is capable of handling these sorts of obstacles with ease, strength, and competence. The communication model specifies how to deploy block chain programmers directly on IoT nodes and/or clouds with APIs to the IoT nodes. In the image above, every IoT device houses the ledger and may be involved in block chain transactions, including mine transactions. Each device has a private key or has capabilities to internally create a private key for network transactions. A consensus algorithm is a computer science method that is used to obtain agreement amongst dispersed processes or systems on a single data value. Proof of stake (PoS) is a way to reach a distributed consensus by use of the Bit coin BlockChain network. Evidence for stake requires users to prove the money (their "stake" in the currency) to the owner of the ship. A chunk of data that must be considerably calculated. In Bit coin, a numerical solution to the SHA256 algorithm must be found that fulfills a network-wide goal - the challenge target. A Peer to Pair Electronic Cash System" by Satoshi Nakamoto, published. Satoshi Nakamoto has merged numerous previous innovations, such as b-money and Hash Cash, to develop an electronic cash system which is entirely de-centralized and is not reliant on the central monetary or settlement authority and the verification of transactions. There would be roughly 80 bytes of a block header without transactions. If we assume that every block is created Ten minutes, 80 bytes * 6 * 24 * 365 = 4.2 million pounds annually. For computer systems that sell 2GB of RAM since 2008, and for Moore's law, which foresees current growth of 1.2GB per year, storage should

not be an issue, even when block headers need to be stored in the memory. Moore's law concerns Moore's' perspective that every two years, although the cost of computers is halved, the number of transistors on a microchip doubles. Moore's law says that every couple of years we may expect to enhance the speed and capacity of our computers and will cost less for them. To validate the digital signature, Bit coin employs public key cryptography. Each user may have one or many wallet addresses, but each address always has a few secret and public keys. For instance Alice begins a transaction with a specific quantity of Alice's address. The amount that I did not write here suggests it might be about 20 bit coins. Alice wishes to conduct a transaction with Bob of 20 bitcoins, and we know that the hash value of the respective addresses comes from the hash value. The concern now is how Bob will make sure the transaction was truly made by Alice. So that if the transaction was truly from Alice and this is not a force transaction, Bob can spend 20 bit coins on a different transaction.

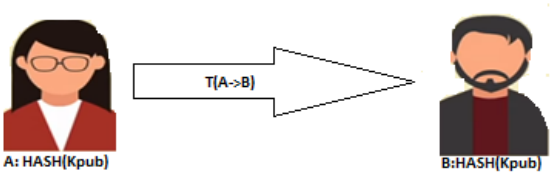

Fig. 6. Transactions

So what we have said numerous times previously, as with the transaction, we include the public key of Alice, two additional factors. K^A pub, this is Alice's public key and Alice's signature is also included. These two items have now been included in the deal, because we are aware that only Alice can hold its private key based on the digital signature method.

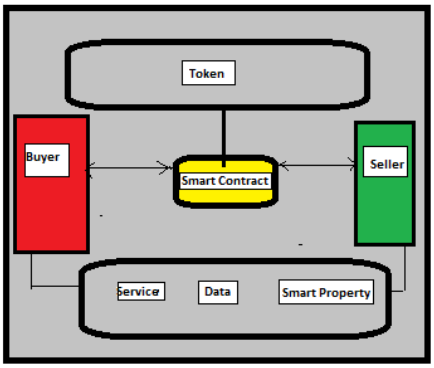

Fig. 7. Smart contract

So what we have usually said numerous times previously, as with the transaction, is that two other parameters one is Alice's public key. Both of these elements are now included in the transaction as we know that only Alice has its own private key based on the digital signature method. The private key of Alice and this specific signature was created with those private keys, and if you can use this public key for the public key of Alice, you may check the signature. Bob can therefore verify that signature, and Bob can make confident that that transaction was indeed made by Alice. Bit coin protocol operates on TCP port 8333, an ad-hoc network with unpredictable topology. The Bit coin network treats all nodes (users) equally. New nodes can be added at any time, nodes are deleted after 3 hours. Next we get to the Bit coin peer idea for peer networks. So, as we stated before, Bit coin is working in a fully decentralized way on top of peer to peer network design.

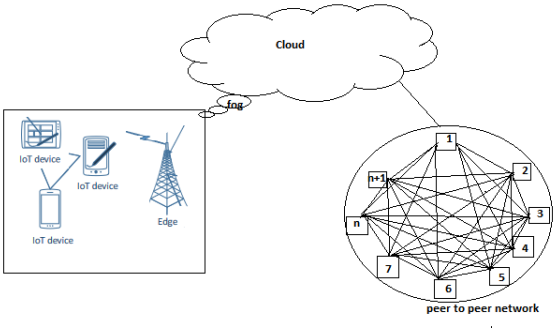

Fig. 8. Communication Model

8 Conclusions

IoT is a new technology that is being introduced to create a smart environment. Security is a major problem in such a widespread setting. This article also discusses how BlockChain may be used to improve IoT security. BlockChain, being a distributed technology, plays an important role in IoT security. The Internet of Things (IoT) network depends largely on efficient and intelligent business processes, where end-to-end optimization is crucial to the overall performance of ecosystems. We are proposing a mechanism ledger distribution to drastically reduce IoT node memory needs. Analysis and assessment of safety issues, time, storage and bandwidth needs reveal a considerable increase in overall system performance.

References

[1] T. Yashiro, S. Kobayashi, N. Koshizuka and K. Sakamura, "An Internet of Things (IoT) architecture for embedded appliances", in the *IEEE Reg. 10 Humanit. Technol. Conf.*, 2013, pp. 314–319.

[2] M. M. Rathore, A. Ahmad and A. Paul, "IoT-based smart city development using big data analytical approach", in the *IEEE Int. Conf. Autom.*, 2016, pp. 1-8.

[3] G. Sagirlar et al., "Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things-PoW Sub-Blockchains", in *IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree.*, 2018, pp. 1007–1016.

[4] G. Rathee, A. Sharma, R. Kumar and R. Iqbal, "A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology", *Ad Hoc Networks*, vol. 94, p. 101933, 2019.

[5] S. Biswas et al., "PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343–2355, 2020.

[6] F. Jamil, S. Ahmad, N. Iqbal and D. H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based BlockChain integrity management platforms in smart hospitals", *Sensors,* vol. 20, no. 8, 2195, 2020.

[7] P. W. Khan, Y. C. Byun and N. Park, "IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning", *Sensors,* vol. 20, no. 10, pp. 1–24, 2020.

[8] D. Pavithran, K. Shaalan, J. N. Al-Karaki and A. Gawanmeh, "Towards building a blockchain framework for IoT", *Cluster Comput.*, vol. 23, no. 3, pp. 2089–2103, 2020.

[9] A. H. Alkhazaali and O. Ata, "Lightweight fog based solution for privacy-preserving in IoT using blockchain", in the *2nd Int. Cong. Human-Computer Interact. Optim. Robot. Appl.*, 2020, pp. 1-10.

[10] V. Dhiman, Himakshi, A. Kaur and M. Kumar, "Pragmatic approach to conquer security perturbation in cloud computing using level classification", in the *2nd Int. Conf. for Conver. in Tech.*, 2017, pp. 192-197.

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *https://bitcoin.org/bitcoin.pdf*.