Quorum-based Blockchain Network with IPFS to Improve Data Security in IoT Network

Sethuraman BALAKUMAR[1]*, Angamuthu Rajasekaran KAVITHA[2]

[1] Anna University, Chennai, India
elk.bala@gmail.com (**Corresponding author*)

[2] Department of CSE, SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India
arkavithabalaji@gmail.com

Abstract: The Internet of Things (IoT) is an emerging technology. It enables users and various IoT-enabled devices to be linked across the IoT network in order to exchange their data and resources, which would result in a more relaxed and connected lifestyle. There are still several challenges facing the new centralized IoT network. For illustrative purposes, the method for computing all connected nodes within the network relies on a centralized server. The centralized IoT model prompts a single point of failure when the central server is offline. The centralized IoT model is a clear target for privacy and security issues, as a centralized system completely handles all IoT data of several connected devices. The implementation of the Quorum Blockchain Network (QBN) with the InterPlanetary File System (IPFS) on the IoT network will solve these problems. It provides an unchangeable ledger that would ensure the reliability of transactions between linked nodes on a distributed blockchain network thereby replacing the central authority. This paper aims to propose a distributed IoT data store and a decentralized IoT network using a QBN model with an IPFS protocol.

Keywords: Internet of Things, Quorum Network, InterPlanetary File System, Privacy and Security, Blockchain.

1. Introduction

IoT (The Internet of Things) is a ground-breaking invention that allows nearly all people to be linked over the Internet. IoT makes it possible to detect the various sensors around us in the world by low-priced sensor devices. They are routinely linked and shared over the Internet with either a wireless or a wired networking system (Atlam et al., 2018a). The core aim of unified IoT architecture is to allow multiple devices to be interconnected anywhere by anybody who may use any service or network/path (Patel & Patel, 2016). While the IoT architecture offers various advantages across different domains, it deals with multiple problems accompanied by the existing centralized paradigm in the sense that entire IoT devices and artifacts are detected, validated, and managed by a centralized server. This server is faced with various hurdles. For example, this server handles entire computing activities and supervises entire nodes on the network, providing a single point of vulnerability where, in case the server goes down, the whole infrastructure would be unavailable (Atlam et al., 2018).

Security is also another problem for a centralized server, as all confidential information is processed at one position and below the rationale of a single server, making it a convenient aim for several types of servers. By comparison, data privacy security tends to be doubtful while real-time data from IoT devices is obtained and stored on a remote server outside the control of the users and only under a centralized server's supervision. Centralized architecture still causes a scalability problem since it only suits small companies, but it would be an unsustainable option for big corporations with multiple branches in various places worldwide (Fernández-Caramés & Fraga-Lamas, 2018).

In recent years, Distributed Ledger Technology (DLT) has obtained tremendous attention as a ground-breaking solution that offers a consistent and provable database of proceedings. In distributed, decentralized environment, DLT puts together a network of untrusted nodes. This DLT will offer some advantages too many government functions, including issuance of passports, tax collection, voting, and licensing. DLT delivers an unchallengeable ledger which can't be modified or changed and removes the requirement for a centralized, trustworthy 3rd party (Wu et al., 2017). With many drawbacks in the centralized IoT infrastructure, switching IoT to Blockchain Distributed Ledger Technology (DLT) with IPFS could be the right decision. Quorum Blockchain Network is a decentralized and distributed chain of proceedings which is able to manage a constantly increasing group of records. A collection of transactions are clustered together and allocated a ledger chain's block to blocks. Every individual block contains the time stamp and hash function of the last block. The hash function authenticates the consistency (subsection 3.7) and data non-repudiation within a node. Similarly, every

https://doi.org/10.24846/v30i3y202108

individual user preserves the duplicate of original ledger and whole nodes are updated and replicated with new updates to keep all blockchain network nodes updated.

The combination of IoT with Blockchain would have multiple benefits. For example, the implementation of a decentralized infrastructure for the IoT system will address several problems, specifically security and a single point of failure, because the Blockchain offers a distributed and decentralized ecosystem where there is no requirement for a central authority to accomplish the operation and control of announcement between the different network nodes. Fundamentally, it delivers a trusting ecosystem. In this ecosystem the contributed nodes are the only individuals to authorize or abandon their consent-based contract (Reyna et al., 2018). By comparison, the Blockchain offers improved protection for different IoT applications. To secure the data against the malicious attack Blockchain offers a tamper-proof and permanent database in which no data change or alteration is applied to the ledger unless the majority of contributed nodes validate it (Karafiloski & Mishev, 2017).

The remainder of this paper is structured as follows. Section 2 summarizes relevant work on the centralized IoT network and Blockchain in IoT. The proposed system model is presented in Section 3, with its complete explanation. The results of simulation are set forth with their discussion in Section 4. Section 5 discusses possible future work and concludes the paper.

2. Literature Review

This section includes a literature review on the centralized IoT system model, highlighting the limitations of the centralized IoT system and blockchain technology in IoT. The related work is summarized in Table 1.

2.1 Centralized IoT System Model

These days, the recent implementation of IoT is executed based on the centralized system for client-server where the devices incorporated with IoT and its sub-peripherals are evaluated through cloud-based servers. Moreover, the communication between the devices is carried out by the centralized servers. Based on Fernández-Caramés & Fraga-Lamas (2018) and Yin, Yueming & Li (2015), the unified IoT architecture consists of 3 primary layers: networking, sensing, and application layer. The primary layer of the IoT architecture consists of sensing layers involving Radio-frequency identification, actuators, different sensors, and wireless sensor networks (WSNs).

To deliver consistent information about the surrounding physical world, this layer is employed for gathering entire applicable information about

Table 1. Summarized Literature Review

The Identified Problem	The Proposed Solution	The Technique	Results	Limitations
The computational power of lightweight clients (Alghamdi et al., 2019)	Fair payment scheme with secure service provisioning	Blockchain with Proof of Authentication	Service provisioning cost is reduced.	No security check on lightweight clients and service providers
Authentication of IoT (Swierczewski, 2012)	The attribute-based access control mechanism	The Blockchain-based access control mechanism	Secure access control policies achieved	User attribute revocation is not considered.
Credibility verification in IoT (Qu et al., 2018)	The Blockchain-based credibility verification method	Self-organization blockchain structure	Response time and storage capacity are optimized.	Complete decentralization is not achieved.
Security and authentication (Coeure, 2017).	The decentralized access control mechanism	Blockchain and Attribute-based access control	Scalability and robustness achieved	No real-time scenario is considered.
Secure data sharing scenario (Laurent et al., 2018)	Efficient access control and permission levels	Data chain and behavior chain is used for data sharing.	Security and privacy-preserving data sharing systems	Distributed System is limited.

the nearby environment. All objects and devices in the sensing layer have a centralized gateway and they are not connected directly (Atlam et al., 2018b). All IoT devices and objects are connected to the Internet by means of the network layer. This network layer consists of a gateway which plays a part as an interlayer communication point between the network layer and the sensing layer. For transporting data between application and sensing layer, various protocols and communication technologies are used. For example, ZigBee, 3G/4G, Bluetooth, Wi-Fi, and Broadband, are utilized to transport data. The application layer contains several IoT applications and it provides more benefits from the collected data. Sensors such as smart cities, smartparking, connected cars, and healthcare are used for collecting data.

Pan et al. (2018) designed the IoT framework called "EdgeChain" based on the blockchain model permission and the digital currency mechanism to deal with several IoT devices. Recent research in IoT blockchain network applications has mostly focused on ensuring data privacy and authentication for IoT sensors and devices. IoT's main research area is to examine whether data to be stored securely by various IoT-enabled distributed systems can be accessed by implementing smart contract-based access control. Shafagh et al. (2017) considered a time-series IoT data sharing system where data owners need to issue ACL policy transactions when data third party shares data, only the data owner can later amend that ACL policy. Also, Laurent et al. (2018) proposed a blockchain system to handle transactions between peers before permissions are granted, but how these transactions are completed is not addressed.

To manage a bunch of nodes the central server built the centralized system. This central server handles all requirements coming from various nodes and allocates the tasks to several network nodes. Generally, the communication between the central server and the various nodes is similar to the Transmission Control Protocol (TCP) connection, in the sense that when creating a link, the messages are delivered between the connected node and the central server. These messages might involve getting a node address and registering a node (Hugoson, 2018). The centralized system is faced with several challenges. For a case, if the server crashes, the whole system will be unavailable. This case is known as a single point of failure. Furthermore, to serve all network nodes, the hardware condition is required to be acceptable before the central server computing process is achieved; or else, the nodes might take a long time to do their job. The central system is also impossible to implement with various branches in several locations of the world (Tommasi & Weinschelbaum, 2007).

The centralized system is unprotected with regard to the exploitation of data. Gathering and storing real-time data from various devices simultaneously based on a centralized server authority can infringe on privacy of the data. The gathered data might cover confidential data about nodes, which is their passwords, financial accounts. Because this data is held in one location and it can track easily, this data could be changed or even deleted (Conoscenti et al., 2017). As such, privacy is one more problem in the centralized IoT structure that should be resolved.

All computing operations in centralized architecture are carried out via the central server; the hardware and software resources should be good enough to support all the nodes on the network.

There is a high amount of communication between nodes and a centralized server that needs to be managed, which requires a high processing power to support several nodes simultaneously. It also requires a large data storage capacity for storing data from various devices on the network. As IoT is concerned, there are high costs associated with the deployment and maintenance of centralized servers, which have risen with the growing number of IoT devices on the network (Rehman et al., 2019).

Security is a significant problem in the centralized system as all data is stored in a single location, and all operations are carried out via a central server, which makes it an easy target for various types of attacks, notably Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The considerable rise in the number of IoT devices in the world contributes to an increase in leveraging security vulnerabilities within IoT devices that are poorly protected. IoT devices (data source) and a centralized cloud server (data storage location) are, therefore, an easy target for security attacks (Atlam & Wills, 2019).

2.2 Blockchain in IoT

Tommasi & Weinschelbaum (2007) suggested an approach based on blockchain for the authentication of an IoT reputation. This work suggested a self-organizing blockchain architecture. The feasibility of the suggested method is measured by utilizing storage performance and reaction time. Though, the proposed approach failed to achieve full decentralization. Swierczewski (2012) suggested a method for data exchanging in a distributed environment with the help of the mechanism of the fine-grained access management. This work proposed a system of the distributed model that utilizes the Attribute-Based Encryption (ABE) and Ethereum Blockchain scheme to address the shortcomings of centralized infrastructure. The effectiveness of the device is evaluated using experimental analysis. However, the Access Control Policy is not considering the removal of the user attribute.

Lee (2017) suggested a new IoT control to access the protocol focused on attributes that ensured the method's robustness and scalability. The Proof of Work Consensus mechanism is not utilized by IoT applications that have greatly minimized overhead connectivity. The real-time situation, though, is not considered. (Zhang et al., 2018) presented a data-sharing mechanism based on Blockchain, which utilizes Artificial Intelligence (AI) and fine-grained control to access. Two blockchains are suggested for data-sharing mechanisms, and they are named Action Chain and Data Chain. Hyperledger Fabric is the foundation for the proposed system. The suggested effort, however, is limited in scope. As a result, the proposed work's economic impact is ignored.

Zhang & Wen (2017) suggested the IoT e-business model leveraging blockchain technologies. To utilize the blockchain technology the developers presented the Peer to Peer (P2P) paradigm. In the trading of P2P, the authors suggested Distributed Autonomous Corporation (DAC) with machine learning algorithm. The Person-to-Machine (P2M) technique was used by DAC in the proposed work. Alghamdi et al. (2019) suggested a lightweight client service provisioning system based on a consortium blockchain. The issue of these devices` limited computing capacity is addressed. An incentive system is suggested in the proposed work to motivate the participants. In the proposed work, the PoA consensus method is employed instead of the PoW consensus mechanism to save resources. A comparison of hashing algorithms is also carried out in order to determine which method performed better in the given model. In addition, the service provisioning is done at a lower cost.

3. Proposed System Model

The proposed system, an Ethereum-based Quorum Blockchain Network (QBN) with IPFS, is discussed in this section. The suggested model's goal is to secure data exchange among IoT-enabled devices through the use of a trusted service. The suggested solution allows IoT devices to communicate in a safe environment and addresses the problems that a centralized IoT system faces.

3.1 Architecture Overview

The proposed system mode allows for the creation of scattered IoT nodes efficiently. Figure 1 displays the proposed system model which is framed to address the specifications and complexities of the Unified IoT system. This figure illustrates two distinct types of nodes, namely: Quorum Blockchain Network (QBN) nodes and IPFS nodes. Quorum supports the confidentiality and privacy of smart contracts and transactions and crashes and Byzantine fault-tolerant consensus algorithms. In this model, a protocol named IPFS and peer-to-peer network are distributed to ensure reliable service delivery. The IPFS node requests a distributed infrastructure from the QBN nodes.

When a novel unrecognized participant node joins the network, a unique enode address is given to the participating node by QBN. Each participant node in the QBN has its individual enode address, which creates trust between the communication network participants. The Tessera transaction manager measures the confidence value that guarantees the integrity of the participating node. In particular, both IPFS nodes provide sensor information required by the participant node. Both IPFS nodes are linked in a P2P mode.

3.2 IPFS Node Model Overview

Sensory data is obtained from smart devices and stored in IPFS. Whenever an intelligent computer calls for service, IPFS nodes connect with Quorum nodes. There are computational assets of three types in each IPFS node such as processing, sensing, and data storage. Based

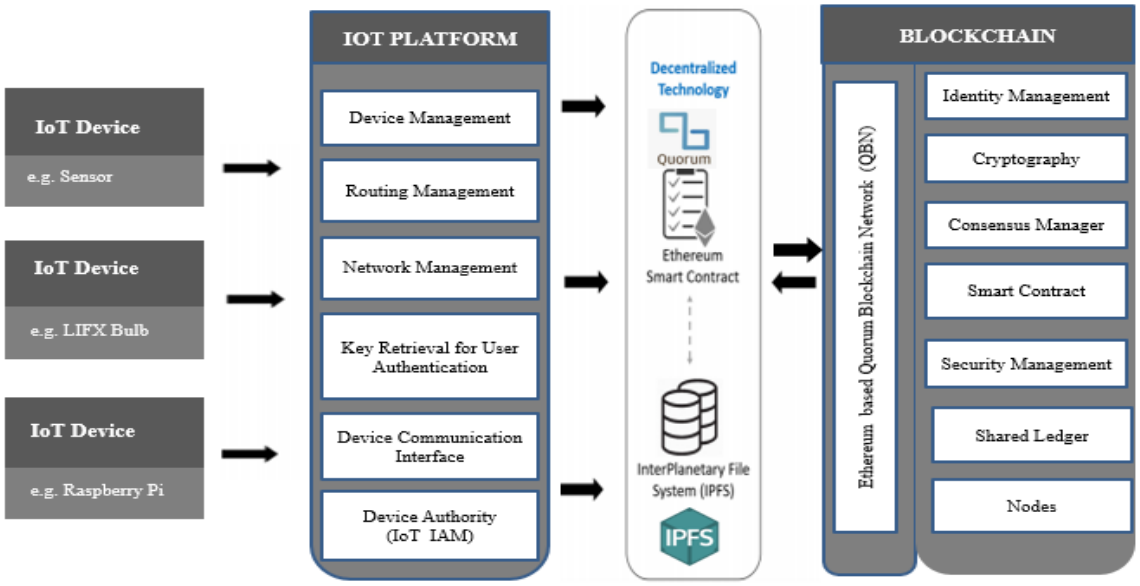

Figure 1. Proposed System Model

on these roperties, the IPFS nodes vary from the Quorum nodes. These IPFS nodes gather the system information from the IoT nodes and transfer it to the Quorum nodes that use IPFS to store it.

IPFS is used for distributed data management over centralized networks such as point loss and data loss (Huang et al., 2019). IPFS is referred to as a completely open file system on the Internet (Zhang & Lin., 2018).

IPFS is presently a subsystem of the Internet as a single peer-to-peer swarm that enables secure and open file sharing over the Internet. IPFS files can be addressed based on their content and their hashes can be defined. Therefore, IPFS is an ideal network for storing and sharing files to create a decentralized IoT model for access control.

3.3 Authentication of IoT Devices

Smart contracts are employed for authenticating the IoT devices placed in the blockchain network and for preventing malicious activities. In Smart Contract, unique hash IDs are allocated to each computer on the network used to identify it. Records for assigning hash IDs to various machines are also maintained in the IPFS node. Every time a fresh malicious node attempts to join the network, it is identified fast as malicious based on the lack of its hash ID. Additionally, each value of the system trust that is based on service sharing is determined by IPFS.

In the proposed system QBN, smart devices are registered using the hash ID given by the IPFS node. A registry of all registered devices is held on the planned blockchain network. The Internet of Things (IoT) interface connects with the IoT node for the resources needed. The IoT node then interacts with the Quorum nodes to accept the IPFS request and respond consequently. Both transportations on the blockchain network are ensured confidentiality by encryption. In the suggested model, the encryption is performed using the AES128 technique. IoT data trust values are determined using IPFS, which describes the behavior of the smart device. The information that smart devices send to IoT nodes using IPFS is stored, IPFS holds the information specified in the distributed hash table and generates the corresponding hash codes. And then a blockchain network stores those hashes. Instead of the PoW, the PoA Consensus mechanism is utilized to authenticate the devices. If the requested service is not available at IPFS, the device will be referred to with an invalid service message.

3.4 Proof-of-Authentication

Proof of authentication (PoA) is a blockchain method that uses a consensus process based on identification to provide reasonably quick transactions. IoT device owners should schedule when their devices contribute to mining during idle time.

For Bitcoin-like applications, blockchain consensus algorithms such as proof-of-work and proof-of-stake are added. The introduced proof-of-authentication follows the classical blockchain working model with lightweight block verification.

The first step of a miner in a network is to verify the block, followed by evaluating the hash value. At the same time, proof-of-authentication is meant to authenticate the blocks using the same blockchain transaction method. The miners should be trustworthy network nodes that are used for authentication. All network nodes must be synchronized and record on the same distributed ledger, and they must be able to track transaction data. The network's trusted nodes authenticate the blocks to be added to the distributed ledger. It takes two authentication steps: (1) authenticating the block and source of the block, and (2) upon validating the authenticated block by trusted nodes. All network nodes then update the distributed ledger. For energy-efficient distributed secure communications and computing in IoT, proof-of-authentication should prevent the inverse hash computation. Table 2 Compares and categorizes various blockchain consensus algorithms based on their properties.

3.5 Decentralizing IoT Networks

A decentralized strategy to networking of IoT will overcome many of the issues encountered for the centralized IoT system. Implementing a standardized networking model of peer-to-peer communication to handle 100 trillion transfers between the devices would crucially minimize the costs of building and managing massive consolidated centers of data and spread the computing and storage requirements across the billions of devices that make up IoT networks. It would prohibit any single node on the network from taking the whole network to an uncertain breakdown.

However, the establishment of peer-to-peer communications would raise its collection of challenges, especially the problem of protection. The architecture of a decentralized IoT model is based on a peer-to-peer network among multiple nodes on a network without the necessity for a central server to control protocol make decisions and smart contract execution in aid of other nodes. Thus, each individual node makes an independent judgment on the basis of its own interests which are consistent with the objectives of the other node. Nodes can communicate and connect with each other to exchange data and provide numerous services to other nodes.

3.6 Block Validation Methods

The technique of verifying new block transactions by solving a cryptographic puzzle is known as "proof of work" (PoW). In the blockchain a new block is added with previous block by using hash key. Therefore, PoW consensus is an expensive computation and adds unwanted delay in IoT. Alternative Consensus Algorithm, 'Proof-of-Stake' (PoS) selects a validating node for block creation to their candidate block. The possibility of selecting a node is comparative to its network's share. The benefit of PoS is that it doesn't require huge IT resources to review new transactions and link those transactions to the blockchain. Although, PoS leaves the network exposed to 'nothing-at-stake' attacks (Financial Conduct Authority, 2017), in which nodes fastly can branch out into a chain without being part of the network and without investing in large amounts of computing resources. PoS offers the chance to investigate blockchains' feasibility in IoT further on, as low computing requirements are ideal for IoT networks.

3.7 Quorum Blockchain Network (QBN)

QBN is a decentralized and distributed chain of transactions which is utilized to control an ever-increasing volume of documents. Blockchain network's participating nodes should register and accept the approval to store a transaction in a ledger. The set of transactions is clustered together

Table 2. Comparison of different consensus blockchain algorithms

Task	Proof-of-Work (PoW)	Proof-of-Stake (PoS)	Proof-of-Authentication (PoA)
Energy consumption	High	High	Low
Computation requirements	High	High	Low
Latency	High	High	Low

and a ledger chain`s block is assigned to blocks. Each individual block includes the time stamp and hash function of the last block to bind together the blocks. The hash function authenticates the consistency and non-repudiation of the block data. Also, to keep all of the contributing blockchain network nodes up-to-date, each participant maintains the original ledger backup, and entire nodes are modified and synchronized and with new changes. Figure 2 shows the smart contract for IoT device Registration.

QBN provides a high degree of transparency by exchanging transaction information between entire nodes. In the world of blockchain, a third-party requirement that improves business usability ensures a secure workflow, and blockchain prevents a single point of failure that affects and impacts the whole framework. By comparison, blockchain has improved security by using a common key infrastructure for protection against malicious behavior. The participating blockchain nodes believe in the legitimacy and security of the consensus mechanism (Sultan et al., 2018).

QBN offers a worldwide data system by incorporating a non-trusted node group into a distributed atmosphere. It offers an immutable ledger that cannot be adjusted or changed and reduces the requirement for a centralized, reliable 3rd party. As a result, a centralized server is not necessary to handle processes and instead trust is maintained among the communicating parties; the distributed ledger is accountable for preserving trust by monitoring the multiple nodes' ownership (Majaski, 2018). There are five major components for the implementation of the Quorum Blockchain Network, as it is summarized in Figure 1, namely:

3.7.1 Shared Ledger

The entire transaction of the nodes is maintained through the centralized database in the network area. On the other hand, the ledger management process is executed from different locations, it is necessary to update and synchronize based on different ledger copies without noticeable latency.

3.7.2 Cryptography

The role of Cryptography in DLT is inevitable where nodes are approved through the authentication process, records-based validation, and enabling consensus on the ledger's updates.

```
pragma solidity >=0.4.25 <0.6.0;
contract DeviceContract {
    struct device { //device structure
        uint deviceId; // device ID
        bytes32 deviceName; //name of device
        bool verified;  // if device verified
        address deviceOwner; // device owner
        uint index;// device index
    }
    mapping (uint => device) private   devices;
    uint[] private  deviceIndex;
    event LogNewDevice   ( uint  indexed deviceId, uint index, bytes32 deviceName, address deviceOwner);
    //create a new device
    function AddDevice(uint deviceId,bytes32 deviceName,bool verified,address deviceOwner) public returns(uint index){
        if (IsDeviceExist(deviceId)){
            revert();
        }
        devices[deviceId].deviceId = deviceId;
        devices[deviceId].deviceName = deviceName;
        devices[deviceId].verified = verified;
        devices[deviceId].deviceOwner = deviceOwner;
        devices[deviceId].index = deviceIndex.push(deviceId)-1;
        emit LogNewDevice(deviceId,devices[deviceId].index,deviceName,deviceOwner);
        return deviceIndex.length-1;
     }
    function IsDeviceExist(uint deviceId) public view  returns(bool isIndeed)
    {
      if(deviceIndex.length == 0) return false;
      return (deviceIndex[devices[deviceId].index] == deviceId);
    }

    function Getdevice(uint deviceId) public view returns( bytes32 deviceName, bool verified, uint index)
     {
         if (!IsDeviceExist(deviceId)) {
            revert();
        }
       return(
         devices[deviceId].deviceName,
         devices[deviceId].verified,
         devices[deviceId].index);
     }
}
```

Figure 2. IoT Device Registration – Smart Contract

This process is executed based on auditing the transactions between two nodes which are secured, recoded, maintained by cryptography approach. In other words, each participating node has a cryptographic digital signature to authenticate itself before a transaction is added or changed (Financial Conduct Authority, 2017).

3.7.3 Consensus Mechanism

In the network environment, all the nodes are involved in the same processes where Ledger based validation process taken place. The Ledger Consensus contents are incorporated with validation phase and Ledger Update Agreement phase. Although the Consensus mechanisms are of many types, the most considerable types are Proof of Stake (PoS) and Proof of Work (PoW). Moreover, based on the delegate and reward transaction verification process, the consensus mechanisms differ from each other (Zhang & Lin., 2018).

3.7.4 Nodes

The network is associated with several nodes which are nothing but the participants in a particular network. These nodes execute several transactions including validating, auditing, administrating, asset issuing, and also act as proponents. Therefore, they play a significant part in enabling certain management transactions. By comparison, the activity of the asset issuer is to authorize the issue of newly generated assets.

3.7.5 Smart Contract

As it is shown in Figure 3, the smart Contract has various features that allow users to connect with the ledger, combining the state database and the Blockchain. 'Smart contracts' add programmability to the Blockchain, in the sense that they allow the execution of transactions while agreeing with the terms of the Contracts. Smart contracts are implemented in a blockchain with unique addresses, which means that transactions are signed off by nodes and addressed to smart contracts themselves to invoke a feature written in a smart contract. The block contains the transaction hash value and the hash value of the previous block to ensure the ledger's data consistency. If the ledger hosted by one peer is tampered with, it would not convince all the other peers because the ledger is distributed across the network. The transaction is appended to the block, and the state of the ledger is updated. In the end, the update result for the ledger is returned as a response to the question.

4. Results and Discussion

The effects of the simulation of the proposed model are discussed in detail in this section.

4.1 Simulation Environment

For the proposed system, the Quorum network is used to execute simulations. Quorum has an easy-to-use environment similar to Ethereum and Bitcoin. Quorum helps Decentralized Applications (DApps) in the blockchain world. Quorum is more effective than the Bitcoin network in terms of the number of transactions authenticated in a second. The Turing-complete

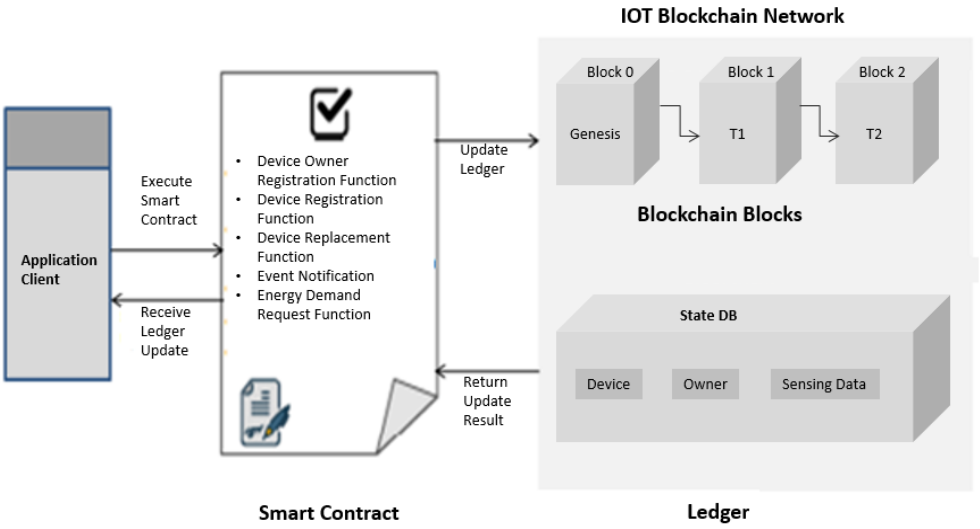

Figure 3. Smart contract network interactions

scripting language, known as Solidity, is utilized for the smart contract submission.

4.1.1 Remix IDE

Remix IDE is employed to simulate smart contracts based on the Solidity language. The implementation, and executions of smart contracts are promoted by a web browser-based programming environment.

4.1.2 Truffle

Truffle is a blockchain-based platform that provides authentic identifiers for smart contract execution. A unique address is stored in Truffle for each account. It also executes the method of mining by which the transaction is authenticated on the Blockchain network. In each account, predefined numbers of simulated ethers are deposited. These ethers are used in a blockchain setting as a cryptocurrency.

4.1.3 MetaMask

Metamask is a browser extension used for the Truffle and Remix link. It additionally offers networking services to local hosts and other blockchain networks, for example Rinkeby and Ropsten.

4.1.4 System Specification

The system specifications employed for network simulations are: Intel Core i5-8500 @ 3.00GHz, 8GB RAM, operating system Ubuntu Linux 18.04 LTS, Ethereum (Web3J), v4.5.5, Quorum v2.2.5, Truffle 5.1.58 and CLI Tool Geth

4.2 Results and Discussions

In this subsection, the proposed framework's average performance is presented. The execution and transaction costs are calculated based on gas. Several activities performed in the Quorum setting shall be deemed to be a transaction. During every purchase, a predefined quantity of gas usage is charged. This amount of predefined gas dispersion is denoted in Ethereum yellow paper (Samaniego et al., 2016).

The cost of enforcing Smart Contracts relies on a variety of factors. There is a set fee for executing the Contract and expenses for transaction computing and block storage.

Gas Spent for device Registration Contract

$= 435035$

Gas Price $= 20$ Gwei

Total Cost for device Registration Contract

$= 435035 * 20$
$= 8700700$ Gwei
$= 0.0087$ Eth

Gas Spent for IoT Data Storage Contract

$= 505437$

Gas Price $= 20$ Gwei

Total Cost for IoT Data Storage Contract

$= 505437 * 20$
$= 10108740$ Gwei
$= 0.0101$ Eth

Total Cost for Contract Deployment

$= 0.0087 + 0.0101$
$= 0.0188$ Eth

The proposed system has spent 20 Gwei of gas per device to mount the Smart Contract machine on the private Quorum Blockchain network. This cost is spent on the Test Quorum network, but this will change if one wants to deploy the same system contract on the main Quorum network. The total cost of 0.0188 Eth was paid on the Quorum Test Network before the launch of smart device contracts. At the time of smart contract deployment, the Eth to Dollar conversion rate was 270.54, close to the $5.08 cost.

Figure 4 estimates the overall gas consumption based on two separate consensus processes. One is QBN with IPFS, and the additional one is QBN without IPFS. The trial investigation concluded that the PoA consensus process is more effective than the PoW for gas consumption. In PoW, two miners are required in a dynamic mathematical puzzle-solving method that is time-consuming and uses too much energy. Simulation outcomes reveal that PoA is helpful for devices with limited resources.

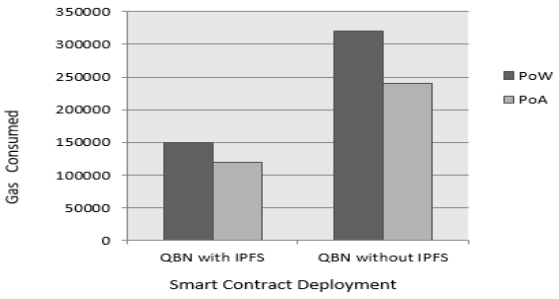

Figure 4. The Smart Contract Deployment Cost

Figure 5 designates the gas usage for the IPFS key functions. It can be seen that the Add Data characteristic consumes more gas when compared with Data Sharing and based on the size of the file to be uploaded and the conditions of the network. The gas consumption is not too high, which indicates the security of the device. A modular contract-based structure with a reduced effect of attacks was proposed.

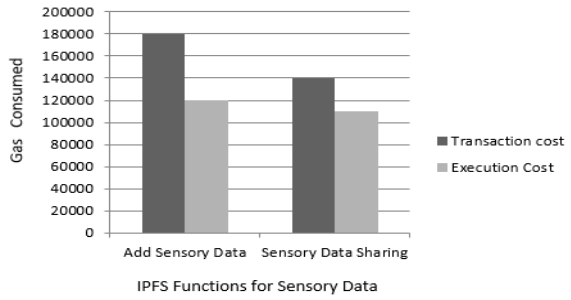

Figure 5. The Gas Consumption for Sensory Data in IPFS Functions

The gas usage of the numerous IPFS phases, such as Sensory Data Return Hash, Device Registration, and Participant Registration is presented in Figure 6. Based on the simulation outcomes, it can be concluded that gas supply is not too important for these functions. The proposed solution is efficient and scalable for devices with limited resources. The difference between the two costs is noticed when the execution cost is often lower than the cost of transaction. The explanation is that the implementation cost is the cost of performing a precise task. The effects of the simulation show that the total number of active transactions increases utility. The higher the confidence score, the higher the reliability of the systems. As a consequence, network contact reduces the risk of malicious behaviour/attacks.

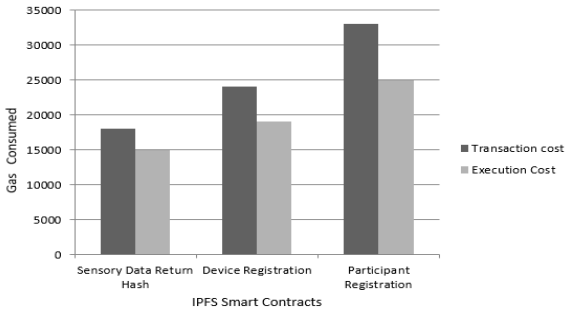

Figure 6. The Gas Consumption for IPFS Smart Contracts

4.2.1 Performance Metrics

Optimization using IPFS Protocol is checked with a range of performance metrics, including packet transmission ratio, end-to-end average delay, uniform routing payload, and IoT and Light sensor nodes' network life. The feasibility of the suggested approach is verified in TPS (transactions per second) and Time Taken (ms).

In Figure 7, the write-and-read-time performance metrics for 10k transactions are compared using Quorum Blockchain Network with/out IPFS.

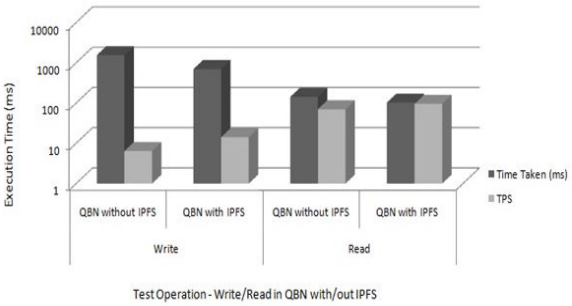

Figure 7. Read/Write Time Performance Metrics for 10k transactions

Table 3 displays the metrics reported during writing/reading experiments for 10k transactions on the proposed device with IoT Raspberry PI and the data transaction time recorded. Transaction times were calculated in terms of seconds, while the transaction expense is measured in Ether. These experiments were carried out over an IPFS-free Ethereum network and an Ethereum-based Quorum blockchain network with IPFS protocol.

Table 3. Results for reading/writing tests for 10k transactions

Test Operation	Test for 10k records	Time Taken (ms)	TPS	Cost(Eth)
Write	QBN without IPFS	1552	6.44	0.00029
	QBN with IPFS	702	14.22	0.00016
Read	QBN without IPFS	142	70.2	Nil
	QBN with IPFS	103	96.5	Nil

4.3 Storing and Retrieving Data from IPFS

Figure 8 shows the IoT data collected from the LIFX Cloud APIs connected to the light sensor, produces a small payload, encrypts it, and then stores the payload in a distributed IPFS system. The file hash is returned directly after the payload is stored in IPFS, and the returned file hash is sent to the Smart Contract to be mined and stored in the Quorum Blockchain network. The device retrieves the file hash from QBN using the Smart Contract and then retrieves the payload associated with the file hash, decrypts the payload, and controls the LIFX LED bulb Raspberry Pi device.

Figure 8. IPFS - Storing and Retrieving Data

Figure 9 shows the current block number, number of Quorum Active Nodes, Block details, and Transaction details.

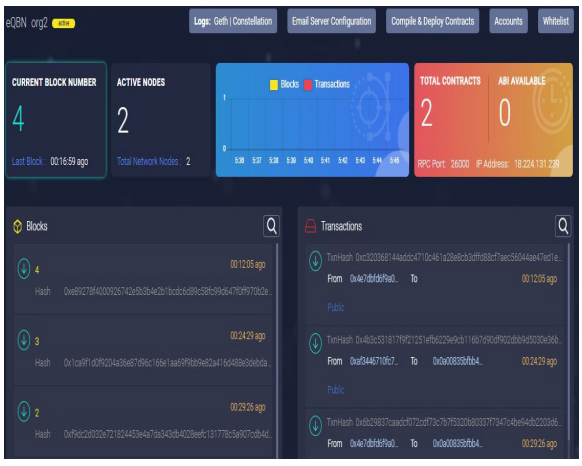

Figure 9. Blocks and Transactions on System

Figure 10 shows the smart contract lists, which are all deployed on the Quorum Blockchain network.

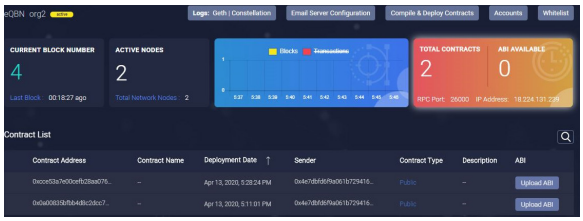

Figure 10. Deployed List of Total Smart Contracts

4.4 Quorum Blockchain Network Traffic Overhead

In blockchain applications, network traffic congestion arises from network nodes participating in a consensus algorithm. As the traffic congestion of the Ethereum and Quorum networks shows with the number of nodes in the consortium, the Ethereum traffic is significantly lower than the congestion of the traffic overhead of Monax.

The high network overhead in Monax is due to the fact that the Tendermint consensus engine transfers out empty blocks to verify if a peer is up. Monax was established for business purposes and was not meant to be employed in a scalable public network. This study measured network traffic on different numbers of consortium network nodes and different numbers of inbound access transaction requests per minute. Figures 11 and 12 illustrate the measurements collected from this research.

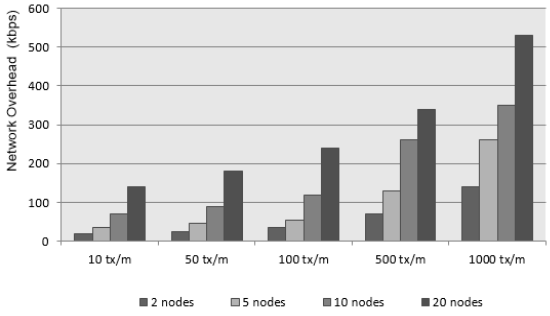

Figure 11. Network Traffic Overhead in QBN without IPFS

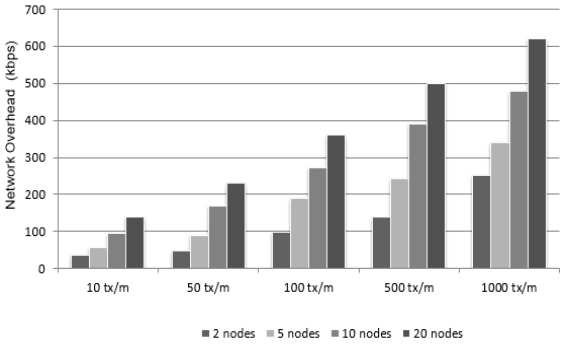

Figure 12. Network Traffic Overhead in QBN with IPFS

4.5 Characteristics of the Proposed Method

The characteristics of the proposed method are provided in this subsection. A description of the IoT problems and how the integration of QBN with IoT will address these concerns are presented in Table 4.

4.5.1 Data Integrity

It refers to the symmetric key encryption which encrypts the data generated over IoT devices. The data is stored in a distributed file system, viz. IPFS, which returns a hash of the stored data. This hash is stored on a blockchain, which guarantees the integrity of the data as it cannot be changed.

4.5.2 Decentralization

In the proposed system, a mutual ledger enables all contributing nodes to keep an authenticated copy of the leader with no requirement for a single central authority for IoT device and data management. It encourages all nodes to associate with each other and perform honestly. All of this is translated into lower costs, greater scalability, and a shorter time to perform and validate the transaction.

4.5.3 Privacy Preservation

The proposed system uses a hash identifier to enable communication between IoT devices. The actual device identification number is not used as an identifier as it leads to information leakage issues. The confidentiality of the proposed system is thus preserved due to the use of a hash code. All transactions in the Quorum nodes are encrypted, which guarantees data confidentiality. Thus, this model preserves data privacy and user identity.

4.5.4 Availability

In the proposed method, the information is stored and distributed in IPFS. A distributed hash table is supported for data stored in IPFS. If certain data is needed, a data request is sent to the particular node where it is hosted. Distributed data warehousing assures data availability with high system throughput at the same time. IPFS acts as a P2P network to defeat a single point of failure.

4.5.5 Immutability and Verifiability

The main advantage of QBN is keeping the legitimacy of transactions by keeping records unchanged and confirmable. By comparison, data stored in DLT can only be changed if this is accepted by most of the network nodes (Zheng et al., 2017).

5. Conclusions and Future Work

This work proposes an IPFS-based Quorum Blockchain Network that would ensure privacy and IoT confidentiality. The distributed file storage system is known as IPFS. It is considered to fix the issue of a centralized storage scheme. The key contribution of this article is the overview of Smart contracts, peer-to-peer file storage, and Quorum Blockchain Network, the control of IoT

Table 4. How QBN can address the challenges of IoT

IoT challenge	QBN can address the challenges of IoT
Security	QBN offers an immutable and stable platform for different types of IoT devices. It also guarantees data confidentiality as any update should be checked by most of the nodes involved in the blockchain network (Halpin & Piekarska, 2017).
Point of failure	QBN uses decentralized and asynchronous networking between participating nodes in the network, avoiding a single point of failure.
Ownership and identity	QBN can provide secure, approved identity registration, ownership tracking, and monitoring. Successfully used for controlling and recording items, commodities, and assets (Khan & Salah, 2018).
Data Integrity	QBN offers a permanent and tamper-proof database that cannot be updated until most participating nodes give their permission and validate the update.
Authentication and access control	QBN Smart Contracts can provide decentralized authentication rules and logic to allow sufficient authentication of IoT devices.
Costs and capacity constraints	As there is no need for a centralized server in the Blockchain, IoT devices can connect anonymously, share data, and operate automatically by smart contracts (Reyna et al., 2018).

devices over their data, and the reduction of the need for centralized IoT data processing. QBN uses a decentralized and distributed ledger for exploiting all participating nodes' computational resources in the Blockchain network, while eliminating latency and preventing a single point of failure. The simulation outcomes show that the planned classification model's gas ingestion is reduced to nearly 15% - 20% by PoA. In the future, the aim is to follow complex IoT nodes in a real-time computational paradigm with separate P2P networks to define the computing capabilities of the Quorum distributed Blockchain Network. Further work will also be considered with a view to maintaining a data stream with legitimate IPFS requests and blockchain pruning for tackling any increase in block processing time and saving storage space on block validator nodes.

REFERENCES

Alghamdi, T. A., Ali, I., Javaid, N. & Shafiq, M. (2019). Secure Service Provisioning Scheme for Lightweight IoT Devices with a Fair Payment System and an Incentive Mechanism based on Blockchain, *IEEE Access*, *8*, 1048-1061.

Atlam, H. F., Alenezi, A, Alassafi, M. O. & Wills, G. (2018). Blockchain with Internet of Things: benefits, challenges, and future directions, *International Journal of Intelligent Systems and Applications*, *10*(6), 40-48.

Atlam, H. F., Walters, R. J. & Wills, G. (2018a). Internet of things: state-of-the-art, challenges, applications, and open issues, *International Journal of Intelligent Computing Research (IJICR), 9(3), 928-938.*

Atlam, H. F., Walters, R. J. & Wills, G. (2018b). Internet of nano things: security issues and applications. In *2018 2nd International Conference on Cloud and Big Data Computing* (pp. 71-77).

Atlam, H. F. & Wills G. B. (2019). IoT security, privacy, safety, and ethics, *Digital Twin Technologies and Smart Cities, 123-149.* Springer International Publishing.

Coeure, B. (2017). *Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework*. Available at: <https://www.bis.org/cpmi/publ/d157.pdf>>, last accessed: 12 Jul. 2019.

Conoscenti, M., Vetrò, A. & De Martin, J. C. (2017). Peer to peer for privacy and decentralization in the Internet of Things. In *2017 IEEE/ACM 39th IEEE International Conference on Software Engineering Companion Peer (pp. 288 -290).*

Fernández-Caramés, T. M. & Fraga-Lamas, P. (2018). A review on the use of Blockchain for the Internet of things, *IEEE Access, 6, 32979-33001.*

Financial Conduct Authority (2017). *Discussion Paper on Distributed Ledger Technology, Discussion Paper DP17/3*. Available at: <https://www.fca.org.uk/publication/discussion/dp17-03.pdf>, last accessed: 15 Oct. 2018.

Halpin, H. & Piekarska, M. (2017). Introduction to security and privacy on the Blockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* (pp. 1 - 3).

Huang, J., Kong, L., Chen, G., Wu, M., Liu, X. & Zeng, P. (2019). Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism, *IEEE Transactions on Industrial Informatics, 15(6), 3680-3689.*

Hugoson, M.-Å. (2008), Centralized versus decentralized information systems: a historical flashback, *IFIP Advances in Information and Communication Technology*, *303*, 106-115.

Karafiloski, E. & Mishev, A. (2017). Blockchain solutions for big data challenges: A literature review. In *Proceedings of 17th International Conference on Smart Technologies, IEEE EUROCON 2017 (pp. 763-768).*

Khan, M. A. & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges, *Future Generation Computer Systems, 82, 395-411.*

Laurent, M., Kaaniche, N., Le, C. & Plaetse, M. V. (2018). *An access control scheme based on blockchain technology*. Available at: <https://pdfs.semanticscholar.org/5659/945a50a79e5f28e72ef0e68faa12595985d8.pdf>, last accessed: 12 Apr. 2019.

Lee, I. (2017). *Advantages and Disadvantages of Distributed Systems. Available at: <https://www.cis.upenn.edu/~lee/07cis505/Lec/lec-ch1-DistSys-v4.pdf />, last accessed: 12 June 2019.*

Majaski, C. (2018). Distributed Ledger Technology, Investopedia. Available at: <https://www.investopedia.com/terms/d/distributed-ledgers.asp>, last accessed: 12 Oct. 2019.

Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y. & Zhao, Y. (2018). EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts, *IEEE Internet of Things Journal, 6(3), 471 -4732.*

Patel, K. & Patel, S. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, *International Journal of Engineering Science and Computing, 6(5), 6122-6131.*

Qu, C., Tao, M., Zhang, J., Hong, X. & Yuan, R., (2018). Blockchain Based Credibility Verification Method for IoT Entities, Security and Communication Networks. Available at: <https://www.hindawi.com/journals/scn/2018/7817614/>.

Rehman, M., Javaid, N., Awais, M., Imran, M. & Naseer, N. (2019). Cloud-based Secure Service Providing for IoTs using Blockchain. In *Proceedings of the IEEE Global Communications Conference (GLOBCOM 2019), (pp. 9-13).*

Reyna, A., Martín, C., Chen, J., Soler, E. & Díaz, M.

(2018). on blockchain and its integration with IoT. Challenges and opportunities, *Future Generation Computer Systems, 88*, 173-190.

Samaniego, M., Jamsrandorj, U. & Deters, R. (2016). Blockchain as a Service for IoT. In *IEEE International Conference on iThings and GreenCom and CPSCom and Smart Data* (pp. 433-436).

Shafagh, H., Burkhalter, L., Hithnawi, A. & Duquennoy, S. (2017). Towards blockchain-based auditable storage and sharing of IoT data, Available at: https://arxiv.org/pdf/1705.08230.pdf

Sultan, K., Ruhi, U. & Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & Applications. In *11th IADIS International Conference Information Systems* (pp. 49-57).

Swierczewski, L. (2012). *The Distributed Computing Model Based on the Capabilities of the Internet. Available at: <https://arxiv.org/abs/1210.1593>, last accessed: 19 Dec 2018.*

Tommasi, M. & Weinschelbaum, F. (2007). Centralization vs. decentralization: a principal-agent analysis, *Journal of Public Economic Theory 9(2), 369-389.*

Wu, H., Li, Z., King, B., Ben Miled, Z., Wassick, J. & Tazelaar, J. (2017). A Distributed Ledger for Supply Chain Physical Distribution Visibility, Information, 8(4), 137.

Yin, S., Yueming, L. & Li, Y. (2015). Design and implementation of IoT centralized management model with linkage policy. In *Third International Conference on Cyberspace Technology (CCT 2015)*, 2015 (pp. 5-9).

Zhang, Y. & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications, 10, 983-994.*

Zhang, A. & Lin, X. (2018). Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain, *Journal of Medical Systems, 42*, 140.

Zhang, G., Li, T., Li, Y., Hui, P. & Jin, D. (2018). Blockchain-based data sharing system for AI-powered network operations, *Journal of Communications and Information Networks*, *3*(3), 1-8.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, (2017). An overview of blockchain technology: architecture, consensus, and future trends. In *2017 IEEE 6th International Congress on Big Data (pp. 557-564).*