Noname manuscript No.
(will be inserted by the editor)

A Blockchain Scheme for Authentication, Data Sharing and Nonrepudiation to Secure Internet of Wireless Sensor Things

Asad Ullah Khan[1] · **Nadeem Javaid**[1,2,*] · **Muhammad Asghar Khan**[3] · **Insaf Ullah**[3]

the date of receipt and acceptance should be inserted later

Abstract A blockchain based scheme is proposed in the underlying work for performing registration, mutual authentication, data sharing and nonrepudiation in internet of wireless sensor things. The nodes are divided into three types in the proposed scheme: sensor nodes, cluster heads and coordinators. Moreover, a consortium blockchain, deployed on the coordinators, is employed for storing the legitimate nodes' identities. Furthermore, coordinators also help in the execution of smart contracts, which facilitate the sensor nodes in authentication, data sharing and nonrepudiation processes. Additionally, for storing the nodes' ambient data, artificial intelligence based interplanetary file system (IPFS) is used. Furthermore, to increase the transaction throughput and efficiency of the network, a stellar consensus protocol is used. From the simulation results, the transaction latency of the proposed model is approximately 81.82% lower than the proof of work based model. Moreover, the gas consumption of data request and provisioning is 0.10 US Dollars.

Keywords Mutual Authentication · Consortium Blockchain · Data Sharing · Data Nonrepudiation · Artificial Intelligence · Interplanetary File System · Internet of Wireless Sensor Things

[1]Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan.

[2]School of Computer Science, University of Technology Sydney, Ultimo, NSW, 2007, Australia.

[3]Hamdard Institute of Engineering and Technology, Hamdard University, Islamabad 44000, Pakistan.

*Correspondence:
nadeemjavaidqau@gmail.com; www.njavaid.com

1 Introduction

Over the past few years, Internet of Things (IoT) has emerged as a promising communication paradigm and is expected to transform the current operation of many industrial systems such as healthcare, transportation, and manufacturing systems [1]. It is the network of objects that are embedded with actuators and other technologies. These objects communicate and exchange data with other objects and systems without human interference over the Internet [2]. According to the predictions of Ericsson mobility report, the number of IoT connection will reach 26.9 billion by 2026 [3]. The integration of these devices with other technologies is a challenging task. IoT devices are used in agriculture domain as well [4]. Moreover, the Wireless Sensor Networks (WSNs) and communication technologies serve as the cornerstone of the IoT. The WSN consists of tiny sensors, which are self organized and have limited storage, energy and computational resources [5]. Moreover, WSNs are widely used in different areas, which include transportation, healthcare, manufacturing systems, environmental monitoring, military,, etc. The examples include vehicle movement tracking, surveillance in battlefield, forest fire detection, damage assessment in war, patient's data in telemonitoring, etc. Besides, distributed and centralized are two types of architectures followed for IoT network formation [6]. In former, the nodes communicate directly with other nodes of the network. Whereas, in the latter, the Cluster Heads (CHs) are used to forward aggregated data of all the nodes to the Base Stations (BSs).

Moreover, blockchain is an emerging technology and it eliminates the centralized control over a system. It is used to transform IoT into decentralized and distributed network. The blockchain technology is one of

Table 1: List of Abbreviations and Acronyms

Abbreviation	Full Form
BSs	Base Stations
CHs	Cluster Heads
DPoS	Delegated Proof of Stake
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ICN	Information-Centric Network
IoT	Internet of Things
IIoT	Industrial IoT
IPFS	InterPlanetary File System
KMC	Key Management Center
MAC	Media Access Control
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
SCP	Stellar Consensus Protocol
WSNs	Wireless Sensor Networks
$Contract_{dataSharing}$	Data sharing smart contract
$Contract_{arbitration}$	Arbitration smart contract
$Data_{hash}$	Hash of data
$ID_{coordinator}$	Unique ID of a coordinator
ID_{node}	Unique ID of a node
ID_{CH}	Unique ID of a CH
$Keycard_{node}$	Keycard of a node
$sign_{coordinator}$	Signing a message with coordinator's private key
$coordinatorID_P$	Coordinator ID of node P
ID_P	ID of node P
CH_P	CH ID of node P
ID_Q	ID of node Q
CH_Q	CH ID of node P
$Keycard_P$	$Keycard$ of node P
$Threshold_i$	Lower limit of a requested feature
$Threshold_j$	Upper limit of a requested feature

the emerging technologies. Satoshi Nakamoto introduced it in the peer-to-peer electronic currency system, called Bitcoin [7]. The blockchain is also known as a distributed ledger technology, which is a network of nodes connected in a peer-to-peer manner. These nodes preserve the state of the distributed ledger [8, 9]. This ledger contains blocks and preserves the accounts' states. A cryptographic hash is used to connect the current block with its previous block. Moreover, a set of transactions being validated by the miners is added to the new block. The nodes having high computational power are referred as miners. Moreover, a consensus algorithm is implemented for transactions' validation and new blocks' addition to the network. Blockchain provides immutability, auditability, security, decentralized control and transparency in different systems, e.g., supply chain, IoT, banking system, voting system, healthcare, etc. In [10], authors highlighted the challenges being faced by the IoT. The blockchain technology is one of the solutions to provide security, transparency, immutability and decentralization for resource constrained devices. The authors in [11] provide challenges being faced by the integration of blockchain and IoT. These challenges include the need of adaptive and low latency consensus protocols for real time application development. With the passage of time, some new features are introduced in the blockchain [12].

In the blockchain network, the smart contracts are introduced to add the feature of terms and conditions based transactions. The smart contract is executed as a decentralized program. It contains code script being executed in an autonomous manner when predefined conditions are fulfilled [13]. Moreover, smart contract is executed without centralized entity's intervention on the blockchain network. Furthermore, the dependency on centralized entity and service availability is removed.

In [6], the authors propose an identity authentication mechanism based on blockchain technology. Both the global and local blockchains are used to authenticate nodes. However, due to the deployment of multiple blockchains, high computational overhead on CHs is observed. As a result, the energy of CHs depletes rapidly, which leads to decrease in network lifetime. Moreover, a Delegated Proof of Stake (DPoS) and certificate-less cryptography based scheme for key management is proposed in [14]. However, DPoS is not decentralized and is vulnerable to 51% attack. Furthermore, in certificateless cryptography, the public key cannot be formed using the identity information only. As a result, a node can generate public keys repeatedly to perform a Sybil attack.

In [15], a nonrepudiation scheme is proposed for Industrial IoT (IIoT), which uses homomorphic hash and blockchain. However, due to resource constrained devices in IIoT, the homomorphic hashing is inappropriate. As a result, high computation and complex task cannot be efficiently executed on these devices. Therefore, an efficient scheme is required that provides mutual authentication of sensor nodes, data sharing and nonrepudiation. This paper is an extension of our conference paper [16]. Moreover, in [17], the authors provide a detailed survey of different consensus protocols used in blockchain technology. The authors suggest to use practical byzantine fault tolerance based consensus protocols for data sharing between lightweight devices.

A consensus mechanism, named DPoS, is proposed in [14], in which 51% attack can be performed because DPoS is not completely decentralized. To solve this issue, Stellar Consensus Protocol (SCP) is used in our network. This protocol is secured because the malicious node has to compromise 60% of network nodes to perform a malicious transaction. Moreover, the au-

thors in [6] propose an authentication mechanism for multi-WSNs. However, the energy of the whole network rapidly decreases due to the use of two blockchains (local and global). To solve this issue, we propose an authentication mechanism in which mutual authentication is performed between CHs and ordinary nodes. Furthermore, a blockchain based nonrepudiation mechanism is proposed in [15]. In this mechanism, the homomorphic hash is used to provide enough evidence that neither the service provider nor the client can repudiate its actions. However, this homomorphic hash requires a lot of computational capabilities, which is not suitable for resource constrained IIoTs. To solve this issue, we propose a smart contract based nonrepudiation mechanism in which nonrepudiation of both service provider and client is ensured by business rules written in the smart contract.

1.1 Research Methodology

This research is carried out using the following steps.

- Firstly, the most relevant and recent articles are selected (see Table. 2).
- Secondly, the literature review of the selected articles are conducted (see section 2).
- Thirdly, a problem statement is identified from some of the selected articles (see section 3).
- A solution for the identified problem is proposed (see section 4).
- Extensive simulations are conducted to validate the proposed solution (see section 5).

1.2 Research Contributions

A blockchain based scheme is put forward in the underlying work for WSNs, which provides identity authentication of nodes, data sharing and nonrepudiation. The contributions that make this paper significant are given as:

- nodes mutually authenticate each other before transmitting data using blockchain,
- secure sharing of the data using smart contract and blockchain is ensured,
- a nonrepudiation scheme for IoT is proposed to provide secure and efficient data exchange between data requester and owner node, and
- the Stellar Consensus Protocol (SCP) is used in the proposed model to provide high transaction throughput.

The organization of remaining paper is given as: the related work is presented in section 2, while problem statement is given in section 3. Section 4 and section 5 describe the system model and simulation results, respectively. The conclusion of this paper is given in section 6.

2 Related Work

The literature review of related papers is presented in this section. The papers are categorized according to the limitations they addressed.

2.1 Identity Authentication and Access Management

The current identity authentication mechanisms for IoT rely on a trusted third party and are vulnerable to a single point of failure. Moreover, the traditional architectures proposed for access management of IoT devices are based on centralized models, which make it very hard to manage a large number of devices deployed globally. These architectures are heavyweight for IoT scenarios [6]. A centralized BS in dynamic WSN can be easily targeted by attackers during key management. Moreover, current cryptographic approaches have scalability, storage, high computational and communication overhead issues in WSN [14]. The IoT devices are lightweight in terms of computational power and cannot perform validation of access rights [18].

The IIoT relies on a centralized architecture, which leads to a single point of failure issue. The sensors and their collected data in IIoT need to be protected against different attacks [19]. The authors in [20] propose a data sharing and access control mechanism for IoT devices. Furthermore, the IoT devices are vulnerable to various security threats, e.g., confidentiality, integrity, availability, etc.

The lack of traceability and transparency during the process of data exchange between IoT devices is observed in [18]. The response of the miners to clients' requests makes the system more complex and results in high latency while fetching access control information from blockchain. The management hub in the proposed model is vulnerable to spoofing, information disclosure, denial of services, tampering, repudiation and elevation of privileges attacks. In [19], each access control contract implements a single access control method and is used between a single subject and object pair, which increases the complexity and deployment cost of the system. The misbehavior of a subject is evaluated on the basis of frequent resource access requests, which are insufficient to evaluate the behavior of a subject. Furthermore, a subject may repudiate that the file or provided service is not legitimate.

The sensor nodes in WSNs are resource constrained devices and can be easily controlled by an attacker. The use of a master key in [21] as an identifier for node or services leads to the security issues of the node. Furthermore, in the proposed model of [22], every node in the network needs to store identification data of all the nodes. The storage problem occurs in an IoT network when a lightweight node stores huge amount of data and the network contains millions of devices. In the process of authentication, a source node might be authentic. However, a malicious intermediary node adds incorrect data to the event, which results in the failure of authentication process. The mechanism for trust factor evaluation is not added in the proposed framework of [23]. Only the registration of users and sensors is done. If a node is registered, then it is trusted. The reputation of nodes needs to be considered in the evaluation mechanism to easily detect the malicious or misbehaving nodes after registration.

2.2 Trust Evaluation for Malicious Node Detection

WSN is a key technology in the development of IoT and supports its core functionality. However, the malicious node detection models for WSN and IoT do not assure impartiality and traceability of the detection process [24]. Furthermore, in traditional systems, centralized models are inefficient due to the high cost of computation, storage, single point of failure and latency. Moreover, the fog nodes in a distributed attack detection model need sufficient amount of data to efficiently detect attacks, which might be impossible due to the limited number of devices or privacy leakage of the connected devices [25].

The consensus mechanism used in the proposed scheme of [24] is Proof of Work (PoW), which requires high computational power and is unsuitable for consortium blockchain. The PoW is suitable for public blockchains to maintain a highly trusted environment. However, it consumes high energy and computing power. The default consensus mechanism used by Ethereum is PoW, which takes 5 to 10 minutes in transaction verification. Furthermore, the computational overhead, in [25], results in high response time. Moreover, the evidence against malicious node is not stored for traceability. The failure of fog node blocks the traffic from benign nodes. Similarly, many other authors work on promoting trust between nodes like [26].

2.3 Trust Evaluation for Secure Localization

The assurance of beacon nodes' credibility during localization process in a WSN is a challenging issue [27]. The range-free localization process in a WSN does not use any special hardware, which leads to errors due to malicious nodes' presence in the network. The malicious nodes provide wrong location information during the localization process. The traditional localization schemes for WSNs rely on a centralized entity, which leads to the single point of failure [28]. The trust evaluation based on Bayesian statistics, reinforcement learning and maximum likelihood estimation must be tested [27]. The blockchain is utilized for trust management. Furthermore, the parameters used to evaluate trust of the beacon nodes in [28] are very limited. Therefore, the behavior and data trust need to be used for the evaluation of final trust value.

2.4 Trusted and Secure Routing

The selfish behavior of upstream nodes during data transmission is not discussed in [29]. In [30], the authors propose a blockchain based service provisioning scheme and an incentive mechanism for lightweight clients. The consensus mechanism used in the proposed model of [31] is Proof of Authority (PoA), which makes the system somehow centralized. In the proposed routing protocol of [32], the gateway agent coordinates with sensor nodes and manages keys for nodes in a centralized manner. If gateway fails, the clusters connected to it go offline. Moreover, if a node does not receive acknowledgment message for a forwarded packet, it retransmits that packet. As a result, it causes early death of nodes and decreases the network lifetime. In a routing protocol of [33], the IoT network consists of resource constrained devices, which are unable to execute PoW consensus algorithm. In [34], the authors propose a reinforcement learning based resource allocation and optimization framework for heterogeneous vehicular networks. Moreover, in [35], the authors propose a maximization technique for energy efficiency of IoT. The authors use non-orthogonal multiple access with sensor communication to maximize the total energy efficiency.

2.5 Lightweight Blockchain for WSN

In WSNs, the participants of the network have limited resources, i.e., computation, power, storage, etc., [36]. Due to these constraints, the sensor nodes are unable to perform a resource intensive task, i.e., mining. All the nodes need to be connected according to the structure

of blockchain, which is impossible and causes storage issue. Moreover, blockchain technology requires high resources in terms of electricity, storage and computation [37]. Furthermore, the size of a ledger increases with time, which leads to the storage issue in the IIoT.

The issues of scalability, high latency, mobility, security, privacy, bandwidth and a single point of failure exist in the network architecture of a smart city [38]. The data in Information-Centric Network (ICN) based WSN need to be shared as much as possible. However, the identical data is vulnerable to privacy issues [39]. Moreover, an edge server acts as a centralized entity in the proposed architecture [38]. In case of edge server failure, the entire public infrastructure is disconnected from the core network. Furthermore, the transaction throughput of the proposed system is almost double to that of the Bitcoin, which is not suitable for applications where real time response is required.

2.6 Incentive Mechanisms for Data Storage and Crowdsensing

Data storage is one of the main constraints in WSN nodes [40]. When a node in WSN behaves selfishly and denies to store data, it affects the normal operations of network. Furthermore, the traditional IoT based monitoring systems for the quality of frozen shellfish rely on a centralized authority and the information about the quality of shellfish gets tampered [41]. Moreover, the traditional incentive mechanisms do not provide privacy protection mechanisms for users in crowdsensing networks [42]. A trusted third party is used in [40], which eliminates decentralization feature of blockchain. The storage of ordinary node is very limited, so it is very difficult to store a growing ledger of blockchain [41].

2.7 Nonrepudiation in Service Provisioning

The malicious service providers or users in IIoT repudiate from the provisioning or utilization of a service in an untrusted environment [15]. Moreover, the use of a trusted third party in traditional nonrepudiation schemes makes them ineffective and do not provide true fairness. The dispute resolution mechanisms in traditional nonrepudiation schemes are not effective and suffer from weak fairness, which as a result do not guarantee trust. When a client requests for a service, the crypto collectible tokens are transferred to the address of the service provider [15]. If the service provider is malicious, then the client loses these tokens. The credibility of service providers must be recorded based on clients' feedback, behavior and quality of service. Moreover, a homomorphic hash function is used in the proposed scheme, which is very slow.

3 Problem Statement

The authors in [14] propose a DPoS consensus based scheme for secure key management in dynamic WSN. The DPoS consensus mechanism is not fully decentralized and attackers can easily perform 51% attack. It is because few nodes control the network and vote in the selection of witnesses [43]. Moreover, the entire public key for a node cannot be formed using identity information in certificate-less cryptography. Furthermore, a malicious node generates public key repeatedly to perform a Sybil attack. In [6], authors propose a scheme based on blockchain to provide mutual authentication in multi-WSN. However, the workload on CHs is increased along with energy depletion owing the deployment of global and local blockchains. Moreover, in [15], authors propose a blockchain dependent nonrepudiation scheme and homomorphic hash for IIoT. However, the homomorphic hashing function is inappropriate for IIoT due to its computational overhead. Furthermore, an independent and secure channel is required to deliver digital signatures and hashes in the verification of information. The authors in [18] propose an access management architecture based on blockchain for IoT scenarios. The blockchain is used to store access control policies. However, there is a lack of traceability and transparency in the process of data exchange between IoT devices. Moreover, there is high latency while fetching access control information from blockchain.

4 System Model

Some logical assumptions along with a brief introduction of the proposed model's components are put forward in this part of the manuscript. Next, we explain the proposed mutual authentication, data sharing and nonrepudiation scheme.

4.1 Assumptions

The reasonable assumptions for the implementation of the proposed scheme are as follows:
– the coordinators are rich nodes in terms of computational, power and storage resources to deploy blockchain and smart contracts,
– a unique and permanent Media Access Control (MAC) address is used by each node,

Table 2: Summary of Related Work

Limitations already addressed	**Solutions already proposed**	**Limitations to be addressed**	**Validations already done**
Authentication of IoT nodes relies on trusted third party [6]. Single point of failure.	Hybrid blockchain based authentication mechanism is proposed.	BS acts as centralized entity. Use of hybrid blockchain increases computational overhead on CH.	Data integrity and availability, scalability. Message size of registration and authentication.
Centralized BS in dynamic WSNs [14].	Certificate-less cryptography. Key material aging.	DPoS is not fully decentralized. Inefficient malicious node detection mechanism.	Energy consumption, computing and storage overhead during cryptographic operations.
Traditional non-repudiation schemes for IIoTs rely on trusted third party [15]. The dispute resolution mechanisms in traditional non-repudiation schemes suffer from weak fairness.	Blockchain based non-repudiation scheme proposed for service provisioning. The homomorphic hashing technique is used for data validation and smart contract is used for dispute resolution.	Advance transfer of crypto collectible tokens to service provider. The credibility of service provider is not considered. Homomorphic hash function is slow and non-performant.	The cost of events in terms of gas consumption and average transaction latency and throughput of the PoW and PoA.
Traditional data access architectures based on centralized models [18].	Smart contract and blockchain are used to store and enforce access control policies.	Lack of traceability and transparency during data exchanged between IoT devices.	Effect of the management hub is evaluated. The performance of the IoT devices and management hub.
Traditional access control schemes for IoTs are centralized and IoT devices are unable to validate access control polices [19].	Smart contract based access control	Smart contract deployment for each subject object pair increases deployment cost. Misbehavior judgment mechanism is not efficient	Response of all smart contracts are shown.
The privacy and security of the exchanged data between nodes, identity authentication and trust management in WSNs nodes [21].	A blockchain based security and privacy, trust management and identity authentication model is proposed. HKT is used to maintain reputation and trust of a node.	Use of master key as an identifier may lead to the security issue of the node.	The restriction on malicious node in the system is used to validate the system.
The authentication protocols for IoTs are proposed to tackle specific attack or are weak and vulnerable to privacy attacks [22].	A sequence number based peer-to-peer authentication protocol is proposed.	Storage problem when a lightweight node stores identity information of nodes and a malicious intermediary may cause failure of authentication process.	The proposed system is validated using the multilevel node authentication.
Current IIoTs rely on the centralized architecture and leads to single point of failure and privacy issues [23].	Blockchain based security mechanism for smart sensors in IIoTs and trust factor for reliability of the sensor.	Only registered nodes are considered as trusted nodes.	Probability of attack success, falsification attack, authentication accuracy and false authentication.
Lack of traceability and transparency in malicious node detection [24].	Malicious node detection based on blockchain. Response time, forwarding rate and delayed transmission for malicious node detection.	PoW requires high computational power and is not compatible with consortium blockchain.	Reputation of all sensor nodes and location of sensors are depicted.
Centralized and distributed attack detection models are inefficient due to high cost of computation, storage cost, single point failure and latency [25].	Blockchain, cloud, fog and SDN controllers based attack detection model is proposed. SDN, fog and edge computing paradigm is utilized to provide fast response.	PoW decreases the response time of the system. Lack of evidence recording for later traceability.	The accuracy, DR, MCC, F1-score, AUC of the receiver operating characteristics and DT. Moreover, DDoS, TCP and ICMP flooding attacks are analyzed. Overhead with and without blockchain.
The beacon nodes' credibility during localization process [27].	Blockchain based trusted localization scheme. Feedback, behavioral and data trust are used for credibility evaluation.	Trust evaluation based on Bayesian statistics, reinforcement learning and maximum likelihood estimation to be tested.	True positive rate, true negative rate, detection accuracy, localization and average localization error. Energy consumption and probability to find true location.
Range-free localization process in WSNs prone to errors due to presence of malicious nodes in the network [28]. Reliance on centralized and trusted entity.	Range-free localization scheme for WSN using blockchain is proposed. Residual energy, mobility, neighbor node list and reputation are used for trust value evaluation.	Limited parameters are used for trust evaluation.	Average localization error, localization error variance and malicious nodes' detection ratio with simulation time. Security is analyzed against impersonation, spoofing and bad mouthing attacks.

Network latency and data delivery problems in existing routing schemes [29].	Intrusion prevention framework for mobile IoTs based on blockchain. Voronoi architecture is used to generate clusters. Uncertainty principle is used to select mobile CH nodes.	The selfish behavior of upstream nodes during data transmission. No mechanism is defined to avoid unnecessary routing requests.	Network lifetime, energy consumption, packet drop ratio, end-to-end delay and routing overhead.
No trustworthiness between routing nodes. Third party based trust management solutions in WSNs [31].	Blockchain and reinforcement learning based routing scheme for WSNs.	PoA consensus is a centralized system.	Average package delay when 25% and 50% of the nodes are malicious. Average transaction latency and gas consumption of PoW and PoA consensus mechanism.
The centralized and distributed data storage in underwater sensor networks are prone to single point of failure, and security and privacy issues [32].	A blockchain based lightweight routing and consensus protocol for IoUTs is proposed.	The gateway agents are working in a centralized manner.	The block generation time and energy consumption in 100 blocks' generation, the number of rounds with total remaining energy and reliability are used to validate the performance.
A centralized entity is required in traditional routing protocols to manage the identities and authenticate network participants [33].	Smart contract and blockchain based routing protocol is proposed.	A smart contract is created on each route request and PoW requires high computational power.	The PDR, throughput, routing overhead and RAL are used to validate the proposed system.
Sensor nodes are resource constrained and are unable to perform PoW [36]. Peer-to-peer connection is not possible in WSN nodes.	Blockchain is designed for resource constrained devices and partially connected nodes.	N/A	Probability of finding connected path between two nodes.
Blockchain requires high resources and PoW may lead to centralization [37].	Lightweight blockchain is proposed for IIoTs.	N/A	Block generation speed, computational cost, network hash quality, block cycle with storage cost and ledger data is performed.
Scalability issue in smart cities due to high latency, mobility, bandwidth, single point of failure, security and privacy [38].	A blockchain and SDN based hybrid network architecture for smart cities is proposed that contains centralized and decentralized features.	An edge server acts as a centralized entity. The critical applications in smart cities requires quick response and transaction throughput of PoW is very low.	Difficulty, hashing rate of mining, transaction throughput, latency and block generation time.
The in-network data in ICN based WSNs is vulnerable to privacy issues and no caching technique is proposed in ICN based WSNs to investigate the behavior of nodes in literature [39].	A secure caching scheme for ICN based blockchain is proposed. The public key cryptography and blockchain is used for identification and protection of caching ledger, respectively.	Data storage on blockchain is costly, and generation of public and private keys is responsibility of centralized entity.	The statistical model for data generation, received signal power, the packet length, difficulty of block and average processing and response time.
The selfish behavior of the sensor node during data storage in WSNs affect normal operation [40].	A trusted blockchain based incentive mechanism is proposed to encourage nodes for storing data. Access control is provided using DHT.	A trusted third party is used to verify blocks and sensor nodes have very limited storage resources.	A theoretical discussion about PDP mechanism is provided.
Single point of failure in traditional IoTs [41].	Blockchain and WSN based monitoring system for feature collection of frozen shellfish to maintain its quality.	N/A	One way ANOVA, MRE and RMSE are used for validation.
The traditional incentive mechanisms do not provide privacy protection for users in crowdsensing networks [42].	A privacy aware incentive mechanism is proposed for crowdsensing networks. Confusion mechanism is used to provide privacy.	N/A	The participation rate of participants for traditional and blockchain based privacy mechanism is used to validate the proposed system.

– the Key Management Center (KMC) is a reliable participant and
– InterPlanetary File System (IPFS) which is powered with the strong artificial intelligence based techniques, does not allow the modification and deletion of data once it is uploaded.

4.2 System Description

In this scheme, blockchain and smart contracts are used among multiple WSNs for authentication, sharing and nonrepudiation of data, as depicted in Fig. 1. A consortium blockchain is used to reduce the computational overhead of the CHs, that is deployed on CHs and coordinators. Moreover, for performing nodes' registration, nodes' authentication, data sharing and arbitration, 3 individual smart contracts are used in the underlying work. The smart contracts are deployed on the coordinators. Furthermore, coordinators are transaction mining nodes. When a node wants to join a network, a public-private key pair is generated by KMC using Elliptic Curve Cryptography (ECC). In the process of registration, it is mandatory for a sensor node to provide its CH's information and public key. The registration fails if any of the information is found invalid. Otherwise, the sensor node is registered. Moreover, during the communication of sensor nodes, they mutually authenticate each other. Furthermore, all WSNs (from WSN_1 to WSN_n) are connected to IPFS, which stores the environmental data being generated by the wireless sensor nodes.

In this scheme, the $contract_{dataSharing}$ smart contract provides data sharing between two sensor nodes. It is triggered each time when a node accesses data of any other node. In a data access request, it is mandatory for requesting node to send both crypto token and data request to $contract_{dataSharing}$. In the response to a data access request, the node having the desired data uploads it to the IPFS. It then transmits the address of data and location hashes with $contract_{dataSharing}$. The $contract_{dataSharing}$ transfers the tokens to the node's wallet upon finding that the exchanged data is valid. In case of a dispute between requester and owner node, the $contract_{dataSharing}$ sends the crypto tokens, address and hash of data to the $contract_{arbitration}$. The $contract_{arbitration}$ provides judgment and resolves the repudiation issue.

There are different consensus protocols, which are used to reach an agreement in a decentralized network. Both Bitcoin and Ethereum use PoW, which is computationally expensive. Moreover, Proof of Stake (PoS) and DPoS are alternative of PoW. However, both protocols are not fully decentralized and are vulnerable to 51% attack. The other consensus protocols implement some form of Byzantine Fault Tolerance (BFT). The BFT is faster and cheaper than PoW, however, it sacrifices the decentralization. In [44], the authors propose SCP as a decentralized consensus protocol that is alternative to the BFT. It is also known as Federated Byzantine Agreement (FBA). The SCP is an open membership consensus protocol, which means anyone can join and leave the consensus process. In SCP, each validator decides which other validators it trusts. The list of trusted validators is called a quorum slice. The quorum slices overlap to form a quorum or network-wide consensus for a transaction. The transaction latency of the SCP is very low as compared to PoW consensus protocol. Moreover, the SCP is more secured than PoW and is not vulnerable to 51% attack. While using PoW, the attackers with 51% of computing power in the network can control the mining process. However, in SCP, the messages are exchanged during consensus and the solving of cryptographic puzzle is not required. So, the attack using computing power is not possible. Additionally, 66.67% of nodes in the network needs to be agreed on the state of ledger. Furthermore, due to the high security, low latency and high throughput of SCP, it is used in the proposed model.

Below, the constituent entities of the smart model are discussed.

4.3 Consortium Blockchain

The consortium blockchain is used by the coordinators, which serve as miner nodes while smart contracts are used by the CHs to acquire data from the blockchain. Moreover, the blockchain contains records for all of the system model's entities. On the CHs and BSs, the local and global blockchains are deployed, respectively, in [6]. Using two blockchains limits network longevity and adds processing load. As a result, using consortium blockchain minimizes the processing overhead of CHs while increases network longevity. Besides, various primary characteristics of the consortium blockchain are provided: low transaction cost, high throughput, increased scalability and low energy consumption.

4.4 Key Management Center

During registration phase, KMC registers the sensor nodes, and stores their public keys and CHs' information. Moreover, KMC initializes identity information of all nodes. The public keys and nodes' identity information are housed in KMC, which in turn tackle the certificate-less cryptography related issues.

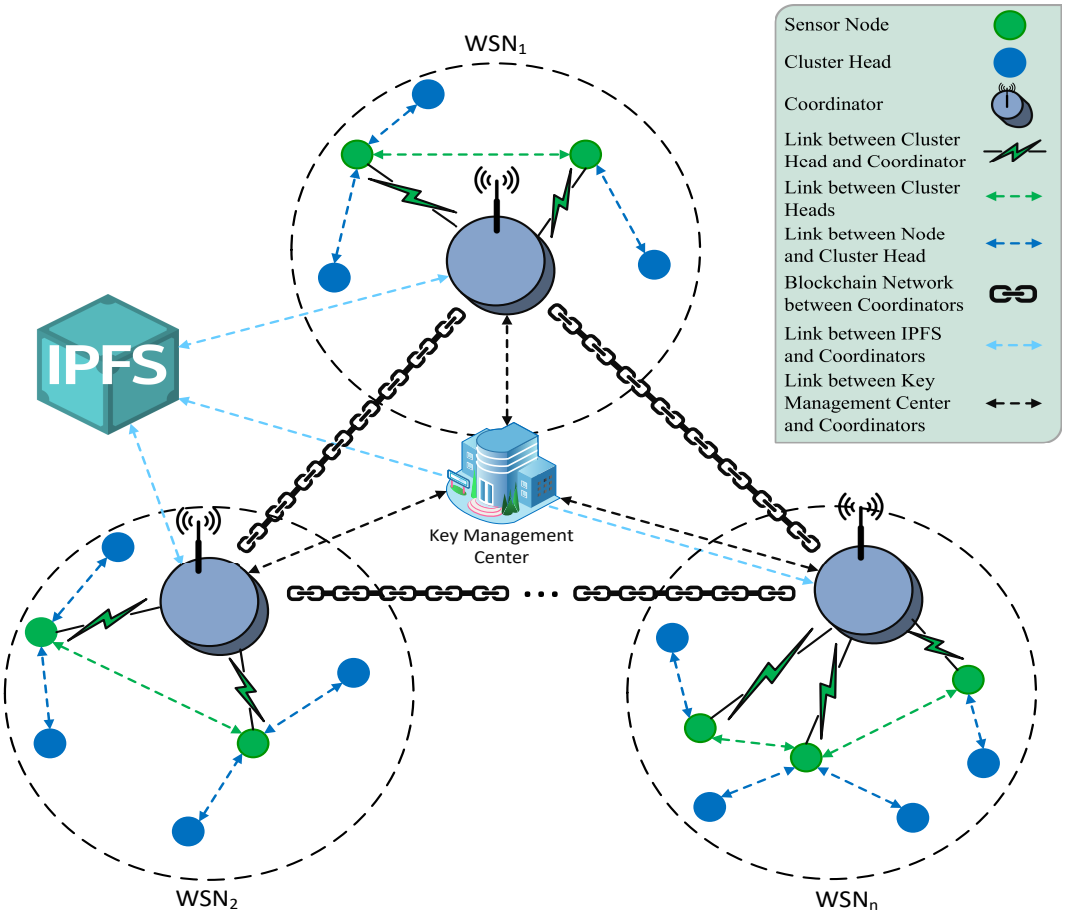

Fig. 1: Proposed System Model

4.5 Coordinator

The computationally enriched node of the network where the consortium blockchain and smart contracts are installed serves as a coordinator. The coordinators function as miners, and verify transactions using SCP. As a result, the coordinators regularly monitor the KMC's activities in order to avoid any malicious conduct. If an already registered node's public key is tried to be added by the KMC, it is restricted. The restriction is performed by the registration smart contract.

4.6 Cluster Heads

Owing high amount of residual energy, CHs are selected. On behalf of their cluster members, they seek blockchain for sensor node authentication. They are also unable to engage in the mining process. Furthermore, CHs trust the sensor nodes in a cluster. As the sensor nodes have limited resources, they send the registration request to KMC via their CH.

4.7 InterPlanetary File System

The IPFS is used to store data generated by sensor nodes in a distributed manner. Using IPFS in the proposed system, the reduction in blockchain's storage overhead is observed. Moreover, the issue of single point of failure is tackled. Furthermore, the reduction in network bandwidth consumption is observed because the data is efficiently stored without duplication.

4.8 Registration and Mutual Authentication

The KMC is responsible for initializing the nodes' identity information. The pair of public and private keys, denoted as Pub_{node} and Sk_{node}, is generated using ECC. The node sends Pub_{node} to the KMC. The KMC then performs hashing of the MAC address to generate a node's unique identity, given as $ID_{node} = keccak(MAC)$. Moreover, while performing nodes' registration and authentication, the verification of message integrity is performed. Furthermore, ID_{node}, $ID_{coordinator}$ and signed message $sign_{coordinator}(keccak(ID_{coordinator} \,||ID_{node}))$

Table 3: Mapping Table of Identified Limitations, Proposed Solutions and Validations

Limitations Identified	Proposed Solutions	Validations
L1: Increased computational overhead on CH with the usage of public and private blockchains [6]	S1: Consortium blockchain is used	V1: During registration and authentication processes, message size and execution time are observed (Figs. 3a, 3b)
L2: DPoS is not fully decentralized and is vulnerable to 51% attack [14]	S2: SCP is used	V2: Transaction latency of SCP is observed (Figs. 5a, 5b)
L3: High latency while fetching data access policies from blockchain [18]	S3: Smart contract provides data sharing between nodes	
L4: Public key does not map to the identity in certificate-less cryptography [14]	S4: Identity based cryptography is used	V3: Message size of registration and authentication is observed (Figs. 3a)
L5: Homomorphic hashing is slow and requires high computational power [15]	S5: Smart contracts and IPFS are used for data exchange and nonrepudiation	V4: Response time of IPFS and transaction latency of PoW and SCP are observed (Figs. 4a, 5a)

are the components of the $Keycard$. In addition, ID_{node} and $ID_{coordinator}$ gives a node's unique identity and a coordinator's unique identity, respectively. For message signing, the Elliptic Curve Digital Signature Algorithm (ECDSA) is employed.

Algorithm 1: Node's Registration Process

Input: $ID_{coordinator}$, ID_{node}, ID_{CH}, $Keycard_{node}$
Output: Successful registration message

if $isExist(ID_{node}) == True$ **then**
  ($False$, $error\ exists$) is returned;
else if $isVerified(ID_{coordinator}) == False$ **then**
  ($False$, $error\ exists$) is returned;
else if $isVerified(ID_{CH}) == False$ **then**
  ($False$, $error\ exists$) is returned;
else if $isVerified(Keycard_{node}) == False$ **then**
  ($False$, $error\ exists$) is returned;
else
  ($True$, $Node\ is\ successfully\ registered$) is returned;
end

The smart contract designed for CH registration is provided with $ID_{coordinator}$, ID_{CH} and $Keycard$. The verification of CH's data and the presence of node's identity is checked via a smart contract. After performing all the required verification, the CH is registered. The registration process is given in Algorithm 1.

For communicating between a node P and a node Q, an interaction request is sent through a CH via a secure channel to the $contract_{dataSharing}$. The request includes $coordinatorID_P$, ID_P, CH_P, ID_Q, CH_Q and $Keycard_P$. The authentication request is sent by both the nodes using a smart contract, which verifies the identity information being exchanged. If both the nodes belong to different clusters, then authentication request is sent to different CHs. Else, a secure connection is established. The mutual authentication process is given in Algorithm 2.

Algorithm 2: Mutual Authentication Process between Sensor Nodes

Input: $coordinatorID_P$, ID_P, CH_P, ID_Q, CH_Q, $Keycard_P$
Output: Authentication message sent to CH_P and CH_Q

if $isExist(ID_P) == False$ **then**
  ($False$, $error\ exists$) is returned;
else if $isExists(ID_Q) == False$ **then**
  ($False$, $error\ exists$) is returned;
else if $isAlive(ID_P) == False$ **then**
  ($False$, $error\ exists$) is returned;
else if $isAlive(ID_Q) == False$ **then**
  ($False$, $error\ exists$) is returned;
else if $CH_P == CH_Q$ **then**
  Secure interaction between nodes P and Q;
else
  Authentication message sent to the CH_P and CH_Q;
end

4.9 Data Sharing and Nonrepudiation

The process of data sharing and nonrepudiation is shown in Fig. 2. Moreover, the ECDSA based digital signatures of the requesting node and data owner are recorded on the blockchain in each transaction. The digital signatures make it impossible for either requester or owner to deny any of their actions. The digital evidences of each step are recorded on the blockchain to achieve transperancy and fairness in the nonrepudiation process. Fig. 2 shows the steps of data sharing and nonrepudiation. The details of these steps are as follows.

Step 1: The data requesting node sends request to the $contract_{dataSharing}$ for accessing a particular node's

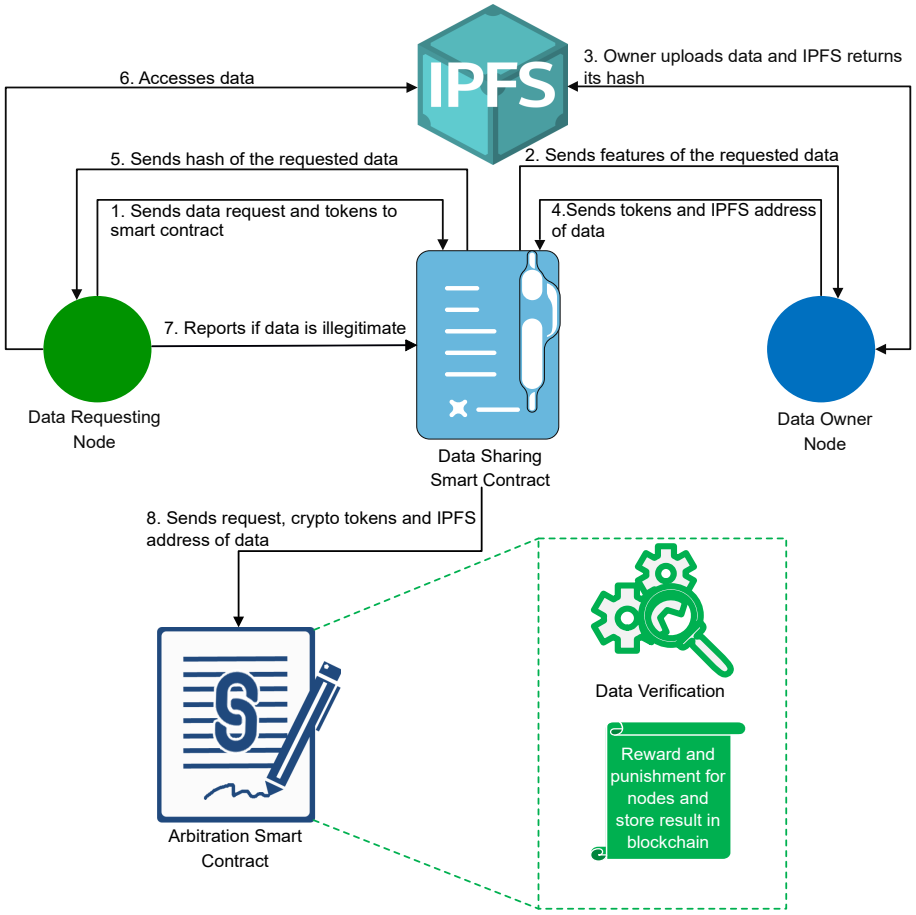

Fig. 2: Data Sharing and Nonrepudiation Process

data. A transaction is recorded on the blockchain for this request, which contains the digital signature of the requesting node. The request message contains the features of data required by the sensor node, the identity information of the owner node and crypto tokens. The crypto tokens are deposited to the $contract_{dataSharing}$ address for security purpose.

Step 2: The $contract_{dataSharing}$ first checks for the existence of data requester and owner nodes in the network. If the nodes are found to be unregistered, data access request is being rejected. Otherwise, the $contract_{dataSharing}$ sends features of the requested data to the owner.

Step 3: The requested data is uploaded to the IPFS by the owner, who gets the hash in return by the IPFS. This address is later used to access the data from IPFS.

Step 4: The data owner node sends the data hash, address and crypto tokens to the $contract_{dataSharing}$. The tokens of data owner are deposited to the smart contract to create a trusted, secure and reliable environment for data exchange. Moreover, the data owner's response is recorded on the blockchain as a transaction with digital signature of owner.

Step 5: The $contract_{dataSharing}$ sends the IPFS address and hash of the data to requesting sensor node.

Step 6: In this step, the requesting node accesses the data from IPFS using its address. The data accessing node confirms legitimacy of data; If data is found illegitimate, steps 7 and 8 are executed.

Step 7: In case of illegitimate data, the requesting node reports to the $contract_{dataSharing}$. Two possibilities exist here: either the requesting node denies that the exchanged data is not legitimate or the data owner shared illegitimate data.

Step 8: In this step, the $contract_{dataSharing}$ invokes the $contract_{arbitration}$. It shares the requesting node information, owner information, crypto tokens and IPFS address of the data with $contract_{arbitration}$. The smart contract $contract_{arbitration}$ checks the features of data requested by the requesting node and the data uploaded by the owner on the IPFS and makes a decision regarding the dispute. At the end, either the data owner or the requesting node is punished and the crypto tokens are transferred to the honest node. Moreover, the de-

cision of the arbitration is recorded on the blockchain and a malicious node is blocked from the network for a specific time.
The $contract_{arbitration}$ is invoked when a dispute occurs

Algorithm 3: Data Sharing and Nonrepudiation

Input: *Request*, *Tokens*
Output: Transfer tokens to the Owner
Requester sends *Request* and tokens to the $contract_{dataSharing}$;
if $isExist(ID_{node}) == True$ **then**
  $Contract_{dataSharing}$ sends features to *Owner*;
  Owner uploads data to *IPFS*;
  IPFS returns the hash;
  Owner sends hash and tokens to $contract_{dataSharing}$;
  Requester accesses data from *IPFS*;
  if *Data is illegitimate* **then**
    Requester reports $contract_{dataSharing}$;
    $Contract_{dataSharing}$ sends *Request*, tokens and $Data_{hash}$ to $Contract_{arbitration}$;
  else
    $Contract_{dataSharing}$ sends tokens to the *Owner*;
  end
else
  (*False*, *error exists*) is returned;
end

between the data requesting and the owner node. The $contract_{arbitration}$ as shown in Algorithm 4 checks the data uploaded to the IPFS with the features requested by the data requester. The $contract_{arbitration}$ checks if the data is within a given threshold or not. The owner is punished and the tokens are transferred to the requester's wallet address when the data is illegitimate. Otherwise, the requester is punished and the crypto tokens are transferred to the owner's wallet address.

Algorithm 4: Arbitration Smart Contract

Input: *Request*, *Tokens*, $Data_{hash}$
Output: Arbitration Result
if $Data \geq Threshold_i$ ***AND*** $Data \leq Threshold_j$ **then**
  Punishes *Requester* and sends token to *Owner*;
  Blocks *Requester* from getting services;
else
  Punishes *Owner* and sends token to *Requester*;
  Blocks *Owner* from service provisioning;
end

5 Discussion of Simulations' Results

This section presents the results of simulations used to validate the proposed model's performance. Simulations are carried out using a laptop equipped with Intel Core-i5 housing RAM of size 6 GB and a 2.5 GHz processor. Smart contracts are built in Solidity while simulations are run on the Ethereum network. Users (requester or owner) communicate with smart contracts using the *web3.py* library, while *ipfshttpclient* stores files on IPFS. With respect to transaction latency, time taken by IPFS to respond, gas consumption, size of message, and execution time, the proposed system model's efficiency is assessed. Fig. 3a depicts the message size during the registration and authentication phases of sensor nodes and CHs. The duration of a sensor node and the network lifetime are determined by the size of the message being transmitted within the network. Message transmission and reception consume a certain amount of energy. The sensor nodes' message size is smaller than the CH nodes' message size. The interaction of sensor nodes only with a CH is the reason for small message size. While, communication of CH with both the sensor nodes and coordinators leads to large message size.

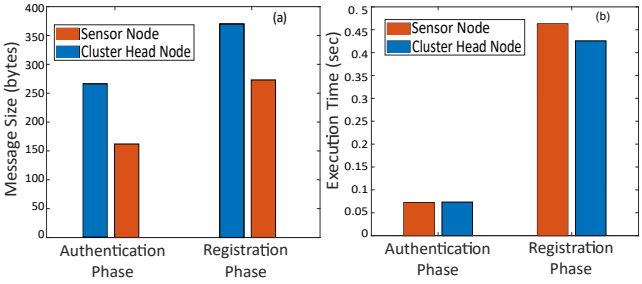

Fig. 3: Registration and Authentication. (a) Message Size. (b) Execution Time.

The execution time for authentication and registration of sensor nodes and CHs is shown in Fig. 3b. The registration time of sensor nodes is high because the identities of both CH and coordinator are validated. However, in the registration of CHs, the identities of these CHs are validated only. Moreover, the execution time for authentication of CHs and sensor nodes is almost equal as it requires node identity for verification. Fig. 4a depicts the time consumed by the IPFS during data upload and retrieval. The data files of 5 MB to 35 MB are uploaded to the IPFS. The response time of IPFS increases with the increase in data. Moreover, the response time during data retrieval from IPFS also increases with the increase in file size. The data is stored

in chunks on different IPFS nodes and data retrieval from these nodes requires large time. The response time of data uploading is high as compared to data retrieval because of the content hashing.

In an Ethereum environment, for performing transactions or executing smart contracts, some price or fee is incurred, which is given in the form of gas consumption. The gas consumed during data requesting and provisioning is depicted in Fig. 4b. In the system using PoW as a consensus mechanism, the cost of data request and data provisioning is found to be 45756 and 46002, in terms of Gwei, respectively. While, both functions' executional cost is 0.10 US Dollars. (1 US Dollar $\approx 3.6 * 10^{-4}$ Ethers).

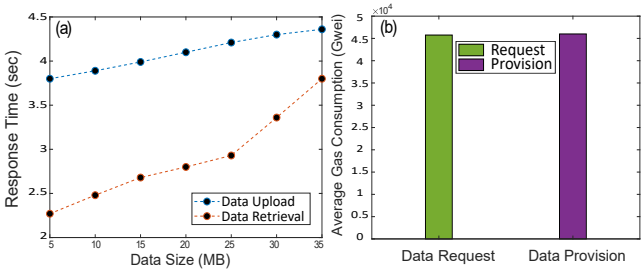

Fig. 4: (a) Response Time of IPFS. (b) Average Gas Consumption on Data Request and Provision

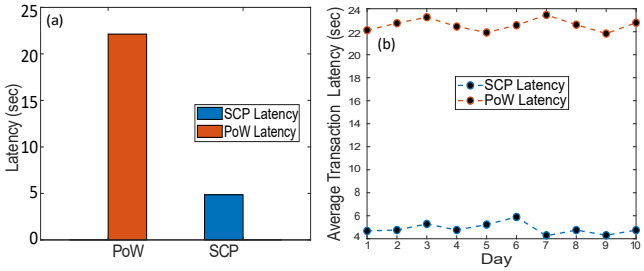

Fig. 5: PoW versus SCP. (a) Transaction Latency. (b) Average Transaction Latency

The transaction latency in blockchain network is referred to the time taken from the submission of a transaction to its addition to a block. The average transaction latency of PoW and SCP based systems as shown in Fig. 5a and 5b are approximately 22 sec and 4 sec, respectively. The proposed SCP based scheme is approximately 81.82% more efficient than PoW based scheme in terms of transaction latency. The transaction latency of the proposed model based on consortium blockchain with SCP consensus mechanism is stable in both data provisioning and arbitration processes.

6 Conclusion

The registration and authentication technique for sensor nodes based on blockchain is proposed in this study. The transactions are stored on the consortium blockchain, which is deployed on coordinators. In the proposed system, identity identification, data exchange, nonrepudiation and arbitration are provided through smart contracts. The presence of a large number of nodes generates a big amount of data in general. Furthermore, the IPFS stores the data collected by sensor nodes. Besides, the nonrepudiation of data kept on the IPFS is ensured. Furthermore, the arbitration contract is activated in the event of a disagreement between the data requester and the data owner. The contract determines the dispute outcome and penalizes the owner or requestor. Furthermore, the SCP is utilized to reach agreement among coordinators. In terms of message size and execution time during registration and authentication, average transaction latency, average gas consumption, and IPFS response time, the proposed model's efficiency is proven. In comparison to PoW-based systems, the proposed paradigm has an 81.82% percent reduced transaction latency. Furthermore, the data request and data provisioning consume 0.10 US Dollars of gas, which is consistent and cost-effective. We intend to reduce transaction latency in the future. Furthermore, scalability and decentralization are mutually exclusive, which means there exists a trade-off between both. We intend to efficiently tackle this trade-off in the future as well.

Author Contributions

The contributions of the authors in this paper are as follows. AK: Conceptualization, Methodology, Simulation Analysis and Writing Original Draft, NJ and MK: Conceptualization, Give Responses to Reviewers' Comments, Manuscript Proofreading and Revision, MK and IU: Writing Reviews and Editing.

Declarations

Conflict of Interest: The authors declare that they have no conflict of interest.
Data Availability Statement: No data were used to support this study.
Ethical Statement: This study does not involve any human participants and/or animal.

References

1. Da Xu, L., He, W. and Li, S., 2014. Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10(4), pp.2233-2243.
2. S. Gillis, Alexander. 2020. "Internet Of Things (IoT)". Techtarget. https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Accessed 6 March 2021].
3. Bugel, J., John, S. and Schwartz, S., 2020. "Ericsson Mobility Report." Available at: https://www.ericsson.com/4adc87/assets/local/mobility-report/documents/2020/november-2020-ericsson-mobility-report.pdf. [Accessed 6 March 2021].
4. Javaid, N., 2021. "Integration of context awareness in Internet of Agricultural Things." ICT Express. doi:10.1016/j.icte.2021.09.004.
5. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E., 2002. "Wireless sensor networks: a survey." Computer networks, 38(4), pp.393-422.
6. Cui, Z., Fei, X.U.E., Zhang, S., Cai, X., Cao, Y., Zhang, W. and Chen, J., 2020. "A hybrid blockchain-based identity authentication scheme for multi-WSN." IEEE Transactions on Services Computing, 13(2), pp.241-251.
7. Nakamoto, S. and Bitcoin, A., 2008. "A peer-to-peer electronic cash system." Bitcoin.–URL: https://bitcoin.org/bitcoin. pdf, 4.
8. En.wikipedia.org. 2021. "Blockchain". [online] Available at: https://en.wikipedia.org/wiki/Blockchain. [Accessed 7 March 2021].
9. Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 2018. "On blockchain and its integration with IoT. Challenges and opportunities." Future generation computer systems, 88, pp.173-190, doi:10.1016/j.future.2018.05.046.
10. Al Sadawi, A., Hassan, M.S. and Ndiaye, M., 2021. "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges." IEEE Access, 9, pp.54478-54497.
11. Majeed, U., Khan, L.U., Yaqoob, I., Kazmi, S.A., Salah, K. and Hong, C.S., 2021. "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges." Journal of Network and Computer Applications, 181, p.103007.
12. Tripathi, G., Ahad, M.A. and Paiva, S., 2020, March. "S2HS-A blockchain based approach for smart healthcare system". In Healthcare (Vol. 8, No. 1, p. 100391). Elsevier.
13. Zou, W., Lo, D., Kochhar, P.S., Le, X.B.D., Xia, X., Feng, Y., Chen, Z. and Xu, B., 2019. "Smart contract development: Challenges and opportunities." IEEE Transactions on Software Engineering, doi: 10.1109/TSE.2019.2942301.
14. Tian, Y., Wang, Z., Xiong, J. and Ma, J., 2020. "A blockchain-based secure key management scheme with trustworthiness in DWSNs". IEEE Transactions on Industrial Informatics, 16(9), pp.6193-6202.
15. Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J. and Zhang, Y., 2019. "A blockchain-based nonrepudiation network computing service scheme for industrial IoT." IEEE Transactions on Industrial Informatics, 15(6), pp.3632-3641.
16. Khan, A.U., Javaid, N. and Othman, J.B., 2021, September. "A Secure Authentication and Data Sharing Scheme for Wireless Sensor Networks based on Blockchain." In 2021 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-5). IEEE.
17. Fu, X., Wang, H. and Shi, P., 2021. "A survey of Blockchain consensus algorithms: mechanism, design and applications." Science China Information Sciences, 64(2), pp.1-15.
18. Novo, O., 2018. "Blockchain meets IoT: An architecture for scalable access management in IoT." IEEE internet of things journal, 5(2), pp.1184-1195.
19. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X. and Wan, J., 2018. "Smart contract-based access control for the internet of things." IEEE Internet of Things Journal, 6(2), pp.1594-1605.
20. Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I. and Javaid, N., 2020. "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices." Applied Sciences, 10(2), p.488.
21. Moinet, A., Darties, B. and Baril, J.L., 2017. "Blockchain based trust & authentication for decentralized sensor networks." arXiv preprint arXiv:1706.01730.
22. Hong, S., 2020. "P2P networking based internet of things (IoT) sensor node authentication by Blockchain." Peer-to-Peer Networking and Applications, 13(2), pp.579-589, doi: 10.1007/s12083-019-00739-x.
23. Rathee, G., Balasaraswathi, M., Chandran, K.P., Gupta, S.D. and Boopathi, C.S., 2020. "A secure IoT sensors communication in industry 4.0 using blockchain technology." Journal of Ambient Intelligence and Humanized Computing, pp.1-13, doi:10.1007/s12652-020-02017-8.
24. She, W., Liu, Q., Tian, Z., Chen, J.S., Wang, B. and Liu, W., 2019. Blockchain trust model for malicious node detection in wireless sensor networks. IEEE Access, 7, pp.38947-38956.
25. Rathore, S., Kwon, B.W. and Park, J.H., 2019. "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network". Journal of Network and Computer Applications, 143, pp.167-177.
26. Javaid, N., 2022. "A Secure and Efficient Trust Model for Wireless Sensor IoTs using Blockchain." IEEE Access, 10, pp. 4568-4579.
27. Kim, T.H., Goyat, R., Rai, M.K., Kumar, G., Buchanan, W.J., Saha, R. and Thomas, R., 2019. "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks." IEEE access, 7, pp.184133-184144.
28. Goyat, R., Kumar, G., Rai, M.K., Saha, R., Thomas, R. and Kim, T.H., 2020. "Blockchain powered secure range-free localization in wireless sensor networks." Arabian Journal for Science and Engineering, 45(8), pp.6139-6155, doi: 10.1007/s13369-020-04493-8.
29. Haseeb, K., Islam, N., Almogren, A. and Din, I.U., 2019. Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. Ieee Access, 7, pp.185496-185505.
30. Alghamdi, T.A., Ali, I., Javaid, N. and 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, pp.1048-1061.
31. Yang, J., He, S., Xu, Y., Chen, L. and Ren, J., 2019. A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. Sensors, 19(4), p.970.
32. Uddin, M.A., Stranieri, A., Gondal, I. and Balasurbramanian, V., 2019. "A lightweight blockchain based framework for underwater IoT." Electronics, 8(12), p.1552, doi: 10.3390/electronics8121552.
33. Ramezan, G. and Leung, C., 2018. "A blockchain-based contractual routing protocol for the internet of things using smart contracts." Wireless Communications and Mobile Computing, 2018, doi: 10.1155/2018/4029591.

34. Khan, W.U., Nguyen, T.N., , F., Jamshed, M.A., Pervaiz, H., Javed, M.A. and Jäntti, R., 2021. "Learning-Based Resource Allocation for Backscatter-Aided Vehicular Networks." IEEE Transactions on Intelligent Transportation Systems.
35. Ahmed, M., Khan, W.U., Ihsan, A., Li, X., Li, J. and Tsiftsis, T.A., 2021. "Backscatter Sensors Communication for 6G Low-powered NOMA-enabled IoT Networks under Imperfect SIC." arXiv preprint arXiv:2109.12711.
36. Sergii, K. and Prieto-Castrillo, F., 2018. "A rolling blockchain for a dynamic WSNs in a smart city." arXiv preprint arXiv:1806.11399.
37. Liu, Y., Wang, K., Lin, Y. and Xu, W., 2019. "LightChain: A lightweight blockchain system for industrial internet of things." IEEE Transactions on Industrial Informatics, 15(6), pp.3571-3581, doi: 10.1109/TII.2019.2904049.
38. Sharma, P.K. and Park, J.H., 2018. "Blockchain based hybrid network architecture for the smart city." Future Generation Computer Systems, 86, pp.650-655, doi: 10.1016/j.future.2018.04.060.
39. Mori, S., 2018. "Secure caching scheme by using blockchain for information-centric network-based wireless sensor networks." Journal of Signal Processing, 22(3), pp.97-108, doi: 10.2299/jsp.22.97.
40. Ren, Y., Liu, Y., Ji, S., Sangaiah, A.K. and Wang, J., 2018. "Incentive mechanism of data storage based on blockchain for wireless sensor networks." Mobile Information Systems, doi:10.1155/2018/6874158.
41. Feng, H., Wang, W., Chen, B. and Zhang, X., 2020. "Evaluation on frozen shellfish quality by blockchain based multi-sensors monitoring and SVM algorithm during cold storage." IEEE Access, 8, pp.54361-54370, doi: 10.1109/ACCESS.2020.2977723.
42. Jia, B., Zhou, T., Li, W., Liu, Z. and Zhang, J., 2018. "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks." Sensors, 18(11), p.3894, doi: 10.3390/s18113894.
43. Maxie, E., 2018. "Pros and Cons of the Delegated Proof-of-Stake Consensus Model." [online] Verypossible.com. Available at: https://www.verypossible.com/insights/pros-and-cons-of-the-delegated-proof-of-stake-consensus-model. [Accessed 6 March 2021].
44. Mazieres, D., 2015. "The stellar consensus protocol: A federated model for internet-level consensus." Stellar Development Foundation, 32, pp.1-45.