Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2022 SCPE. Volume 23, Issues 4, pp. 457–472, DOI 10.12694/scpe.v23i4.2038

BLOCKCHAIN ENABLED ARCHITECTURE WITH SELECTIVE CONSENSUS MECHANISMS FOR IOT BASED SAFFRON-AGRI VALUE CHAIN

JAHANGEER ALI* AND SHABIR A. SOFI †

Abstract. The Internet of Things (IoT) is the backbone behind numerous smart and automated applications in the modern era by providing seamless connectivity and information retrieval among physical and virtual objects. IoT networks are resource constraint platforms hence prone to security and privacy challenges. Blockchain technology comes to the forefront to improvise security, privacy, and less dependency on third-party centralized servers. There exists a rich amount of work with numerous practical applications by fusing IoT and blockchain. In blockchain technology, the consensus mechanisms are considered to be the driving force in its implementation. In this paper, we propose a simplified Blockchain-based Internet of Things (BIoT) architecture for resource-constrained IoT devices with selective consensus mechanisms based on the scale of IoT networks. We have selectively highlighted some of the important consensus algorithms which are favorable for IoT networks. We have tailored the blockchain framework to suit resource-constrained IoT networks. We implemented a prototype leveraging the blockchain and IoT network to evaluate our design. The preliminary results suggest that the proposed system incorporating supply chain management of the Saffron-Agri value chain outperforms the existing systems. Furthermore, we have carried out a detailed case study on the cultivation and marketing strategies for maintaining originality and transparency starting from farmer to consumer in the Saffron-Agri value chain.

Key words: IoT, blockchain, security, BIoT architecture, consensus mechanism, SCM, BIoT applications

AMS subject classifications. 68M14

1. Introduction.

With the advancement in information communication technology, most of the real-world use cases are utilizing its benefits by connecting the smart objects accessible globally with unique addresses to create a smart ecosystem with on-demand services at any place [71]. IoT as a technology is growing enormously in fact having a direct role in the economy of any country [49]. The IoT-based networks mostly possess heterogeneous and inter-operable behavior which becomes a challenging task to maintain all operational standards in the network [21]. The IoT system is dependent on third party like cloud-based centralized services which cannot be trusted all the time [1]. The data generated by IoT devices can be manipulated by unauthorized users which are stored on these centralized servers. And these centralized servers will restrain the adoption of IoT technology due to the huge amount of data generated by IoT end devices. This leads to a single point of failure [5]. The IoT applications are spreading over vast fields like supply chain logistics [30], agriculture [71], healthcare, smart cities [55], smart grids, industries 4.0 [64]. Researchers work in different fields like inter-operable platforms, architectures, standardized protocols, and emerging technologies [71]. Considering the security and privacy of these networks which is of much importance as most of the human-related activities are been processed and shared globally [36]. The last research development is seen to maintain the security and privacy of IoT devices. One of the reasons for the fewer security mechanisms specific to IoT devices is that scarce resources lead to various security and trust-based issues [3].

Blockchain is a distributed ledger that maintains the data in form of blocks in a decentralized manner. The complete chain of blocks is linked together by using a cryptographic hash function in a peer-to-peer communication [5]. The participating nodes maintain identical copies of the complete ledger which makes it more transparent. Once the new block is added to the existing blockchain network after due consensus arrived between the participating parties no change can be made to the data block. At any instance time in history, actual

*Research Scholar, Department of Information Technology, National Institute of Technology Srinagar, J&K, India (jehangir_04phd18@nitsri.ac.in).

†Associate Professor, Department of Information Technology, National Institute of Technology Srinagar, J&K, India (shabir@nitsri.ac.in).

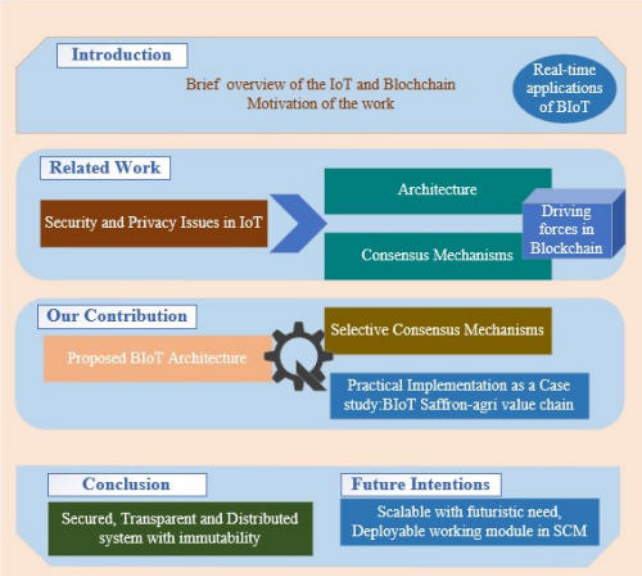

Fig. 1.1: Taxonomy of the article with distinctive highlights.

information can be retrieved from the blockchain network. Blockchain technology can monitor, communicate and perform transactions for large quantities of IoT devices without any intermediary [18]. Blockchain networks come in various variants depending on the complete access and restricted access to the participating peers in the network. In public blockchain networks, anyone can join the network. While in the case of a private blockchain, the owner can restrict limited access to the participating users. The integration of blockchain technology with IoT networks will definitely improve security, transparency, and immutability. Blockchain technology is adding new dimensions to the existing IoT networks with promising applications like supply chain logistics [35], smart agriculture [5], smart land records, System firmware updates [18], smart-grids [49], smart cities [10].

The paper motivates about the importance of integration of blockchain technology with IoT networks in maintaining security and transparency in a distributed architecture. To address the problem of a generalized Blockchain-based Internet of Things (BIoT) architecture, we propose a simplified BIoT architecture with a selective consensus mechanism for large and small-scale IoT applications. The proposed architecture uses inbuilt features of security and privacy to secure the data generated by the IoT devices in encrypted hash codes which are difficult to eavesdrop and all blocks are chained together with the hash codes of every previous block in the chain. And every main node maintains a complete copy of the ledger. Figure 1.1 provides a clear visualization of this article. The rest of the paper is organized as Section 2 discusses the work carried out in areas of interest like security and privacy issues, Real-time applications of BIoT, BIoT architectures, and various consensus mechanisms related to blockchain. Section 3 presents our proposed work like BIoT architecture with a provision for the selection of optimal consensus mechanism with respect to the scale of the IoT application area. Section 4 discusses the detailed use case-based novel study in integrating blockchain with IoT ecosystems. Section 5 concludes the paper and section 6 discusses the possible future perspectives for enhanced BIoT ecosystems.

The highlights of our proposed system are as under:

- We propose a BIoT architecture that comprises vast IoT application domains with customized consensus mechanism applicability.
- Although numerous consensus mechanisms are available in the literature but we have selected some distinctive consensus mechanisms specifically favorable for IoT applications only.
- Practical Implementation as a Case study: BIoT Saffron-Agri value chain.

2. Related Work.

2.1. Security and privacy issues in IoT. With the adoption of more IoT application use cases, millions of devices are getting connected over the internet with huge data collection mostly dependent on centralized cloud services. Most of the IoT devices are resource constrained in nature which makes it difficult for existing security frameworks and protocols to safeguard and preserve the privacy and security of these devices [4]. Almost the least priority is given to security and privacy measures in IoT ecosystems mostly relying on wireless medium in a heterogeneous manner [36, 28]. There are various types of security and privacy attacks in IoT networks which include Denial of services(DoS) and Jamming attacks in which the attacker broadcasts radio signals in the shared wireless channels which badly affects the communication of IoT devices which can discharge the limited battery of IoT nodes and leads to node failure [64, 21, 54]. Distributed DoS leads to blocking of channels, memory and CPU utilization in 96% of IoT devices [31]. In a Sybil attack, the IoT devices are prone to fake identities created by the attacker which deteriorates the functioning of normal IoT nodes in the network [21]. The attacker node with multiple addresses captures most of the data within the compromised network [28]. In sleep denial attack, the IoT devices deployed in remote areas are mostly equipped with sleep-enabled modes in case of no data activity to conserve energy. The attacker can alter the infect the programming code of sleep mode and will make the node active all the time which will decrease the network lifetime of the node [2]. In a sinkhole attack, the sinkhole node compromises the existing IoT network and then acts as a promising sink node for all neighboring nodes. With the result, all nodes forward the data to the sinkhole node [54]. In a wormhole attack, the attacker creates a falsely high resource link which attracts the other nodes to forward their packets via wormhole node [54, 28]. Man-in-the-middle attack (MITM) is the major threat to the security and privacy of the end devices in the IoT ecosystem [31]. The attacker masquerades the communication between two IoT nodes which can monitor or modify the delicate data between comprised IoT nodes [54]. In malicious code injection, various types of malicious programs can be injected in the form of viruses, and trojans into IoT networks which can lead to loss of data or non-availability of resources in the network [2]. And in routing protocol for low power and lossy networks(RPL) attacks in IoT networks can easily be compromised by the attacker nodes which can increase the network latency and restrict the resource usage.

As IoT devices are facing serious challenges in securing the data shared within the IoT networks. There is a dearth of research on new enabling technologies that must be formulated or integrated with IoT networks in order to secure the information stored or transactions carried out in these systems. Thus collaborating blockchain technology with IoT networks in the distributed and decentralized with in-built security and privacy mechanisms[37, 60].

2.2. Real-time applications of blockchain-based IoT systems. IoT has a vast application area, the blockchain involvement as the backbone network will add more dimensions in a new era of application services. S. B. Rane et al.[47] focused on the future commitments of the supply chain towards a green economy. The main contribution of this article actively incorporates the involvement of stakeholders and using BIoT in achieving the goal. The authors have also proposed a BIoT architecture in a very simplified manner by involving the majority of the stakeholders. However this work does not present the practical implementation of the research findings in specific application use cases. Weijun Lin et al. [26] highlighted in detail the importance of BIoT in the field of agriculture systems and practices. The authors have done a thorough survey on the technical aspects like cryptographic security protocols, data structures, consensus mechanisms, smart contracts, blockchain-based agriculture applications, and the possible solutions for the problems faced. Q. Yung et al.[67] presented a smart blockchain scheme for the IoT enabled smart homes specifically focusing on transactive energy management by enhancing the overall performance of smart meters in reducing the power losses, privacy concerns, and safeguards for sudden failures due to centralized systems. Fernández-Caramés et al.[18] stressed applying blockchain technology in many use cases.

Blockchain technologies can be applied in different areas where IoT applications are involved like supply chain management (SCM), smart living, mobile crowdsensing, cyber law, and security in mission-critical scenarios. Blockchain can also be used in IoT agriculture applications. One working example of it is tracking Chinese agri-food supplies, where the main aim is to enhance food safety, and quality and reduce the logistic cost. Blockchain technology has also remarkable imprints in the field of healthcare mainly in clinical trials and precision medicine, smart grids, and smart cities. Aya Reyna et al.[49] mentioned blockchain applications mostly occurring in the field of online financial transactions where many cryptocurrencies are available like Bitcoin,

Litecoin, Namecoin, etc. Furthermore, blockchain technology can be an ideal solution for traceability applications. Many applications that use IoT devices to digitize the sensed data can be improved with blockchain technology. Blockchain can further make the smart city a reality by incorporating security and privacy-based smart contracts without any third-party centralized services [46]. Blockchain can also be incorporated into the Energy sector, Insurance, and Mortgage based IoT applications with the heterogeneous involvement of various stakeholders in a distributed manner [29]. Mainly addressing the important challenges in integrating blockchain technology with IoT applications will pave more directions for its feasible implementation with far better results. M. S. Ali et al. [5] have not restricted the use of blockchain technology only to online financial transactions but significant scientific research is carried out in the field of the Internet of Things.

Blockchain technology has shown promising imprints in several industries like smart insurance, smart grids, healthcare, SCM, smart home applications, and connected vehicle fleet network. The main motive of this survey is to make an attempt by bringing blockchain technology to its maturity in leveraging IoT by considering the challenges faced in its integration. Wang Xu et al.[64] discussed the IoT security challenges faced by centralized service mechanisms, as the IoT devices are data-centric, which generate huge amounts of data that can be easily compromised by potential attackers. Thus blockchain is considered to be an emerging technology that can be inquired with IoT networks to provide security, data integrity, and reliability. Blockchain show promising application areas with IoT in the field of smart grids, nuclear factory, SCM, and smart cities. The decentralized nature of blockchain makes it more feasible for IoT networks but there are underlying technological challenges in its integration, which need to be addressed for future large-scale high capacity IoT applications. Ali Dorri et al.[30] highlighted that enormous research and innovation were carried out in order to implement blockchain in IoT networks. Mostly the use cases take advantage of blockchain features like decentralized control, security, fault tolerance, data integrity, immutability, and the ability to run smart contracts. The applications of blockchain with IoT mainly discussed in this paper are autonomous decentralized peer-to-peer telemetry, secured smart cities, secure firmware updates for the devices to run securely on regular basis, smart home architecture, self-managed vehicle ad-hoc networks, and SCM. As these use cases are in discussion for example in the case of smart cities it's not clear which blockchain platform, consensus protocol, and transaction validation technique are to be implemented. Daniel et al.[35] have given more importance to the cryptographic security and decentralized nature of blockchain technology, for this reason, blockchain technology is resistant to false modifications of underlying information. Various applications have evolved because of their distinguished capabilities like trustworthy contracts between different participating parties, storing information securely, and transferring money safely without any third-party control. One more application mentioned is smart logistic management services in which trigger-based invoices pay themselves when a shipment is received by the user.

Blockchain can also be applicable in IoT environments for device configuration storing sensor data, and performing micro-payments [50]. supply chain provenance [22], software push to remote IoT devices [51]. Muneeb et al.[19] highlighted anonymity as the best to maintain privacy in IoT networks which led to the applications like electronic patient record management. In financial transaction management using blockchain must secure the personal information of the peers which means maintaining anonymity based on two strategies named ZeroCoin [34] and ZeroCash [52]. Application areas involving the trading of energy resources show promising results from the research perspective when leveraging the blockchain with IoT-based networks. In order to maintain the immutable transactional flow transparently throughout the supply chain from producer to consumer via smart contracts which can perform automatic billing invoices and micro-payments as well [23, 58, 41].

The blockchain-based IoT systems are still vulnerable to some privacy issues that need to be resolved before final implementation practically. Thomas B. et al.[8] presented a detailed use case of blockchain in the pharma SCM. Project-based on sensor devices in IoT considers environmental control parameters like temperature and humidity in the most critical use case of the medical supply chain to ensure quality control and company regulatory norms as per international standards. the sensor nodes attached continuously monitor the temperature of each shipment item, then the data is transferred to the blockchain based on smart contact's assessment decisions made to ensure the safety of the patients using the medicines. Ali Dorri et al.[15] considered the security and privacy of IoT networks as the prime attributes thus integrating the blockchain with the IoT systems mainly in the application area of smart homes. As blockchain is a decentralized network and uses

cryptographic hash functions to secure the data shared in the form of chained blocks to maintain security and privacy. As IoT devices are mostly resource-constrained in nature thus it will be impracticable to use the energy-consuming proof of work(PoW). Thus the blockchain-based smart home consists of three main entities: cloud storage, overlay, and smart home. The smart home is embedded with the high resource device called a miner which is responsible for handling the block's authentication and authorization into the blockchain. It has shown improving results. But there are still some overheads in terms of traffic, processing time, and energy consumption which needs proper justification to compromise a certain extent of these overheads with this proposed technology.

The above study summarizes the diversified application domains of both technologies and their integration will have a significant impact on real-time applications considering some challenges for further improvements. The blockchain approach needs to be augmented by robust and scalable architectures.

2.3. Blockchain Architectures. The commencing notability of blockchain technology in its inception with the existing technologies and applications was relying on its distributed architecture with security, transparency, immutability, and traceability. The IoT ecosystems face serious challenges in security and distributed architectural framework needs, which are mostly based on traditional centralized servers. Therefore, the need for the combination of IoT with blockchain technology will have satisfying results [63]. O. Nova [40] incorporated blockchain framework for IoT-based networks. The access control mechanism in the architecture is fully distributed which removes any dependence on single centralized servers. Syed T. Ali et al. [59] carried out a comparative analysis of blockchain technology to be incorporated into IoT. The inbuilt features like security, decentralization, immutability, transparency, and privacy in blockchain technology manage various IoT-based critical applications as a backbone network. H. Bai et al. [6] proposed a two-layer consensus-based architecture for IoT considering the resource constraints of the IoT devices. The paper lacks details about the selection of top-layer nodes as servers and storage of a complete chain of blocks in the network which further limits the decentralization. C. K. Pyoung et al. [44] proposed LiTiChain, a scalable and lightweight blockchain-based IoT architecture that is based on a finite lifetime of blocks in the network. Thus reducing the storage and scalable problem in massively deployed IoT networks. P.K. Sharma et al. [56] proposed a blockchain-based integration of cloud and fog services architecture for IoT applications. It comprises of three layers: the device layer of IoT devices, Fog-based distributed blockchain subnetworks, and the blockchain-based cloud layer. Wattana Viriyasitavat et al. [62] proposed an interoperable and trust-based blockchain framework for service-oriented IoT networks. Ali Dorri et al. [15] proposed a blockchain-based smart home architectural framework for secured communication and management of information remotely in device-to-device interactions. M. Pourvahab et al. [43] enhanced the security mechanisms of existing software-defined networking based IoT systems by using blockchain technology as the most promising peer-to-peer distributed framework. The blockchain-based layered architecture possesses various rules for the control and validation of blocks in the network. The Chain of Custody (CoC) consensus mechanism is specifically utilized for digital forensics as a use case. S. K. Singh et al. [57] proposed a state of art framework which includes technologies like blockchain, and artificial intelligence integrated with IoT systems. Blockchain enhances the security, trust, and transparency of existing intelligent IoT systems via decentralized architectures and removes the single point of failure in big data analysis. Y. Qian et al. [45] proposed a blockchain-based security management architecture for IoT devices. Blockchain helps in maintaining security services, operations, and software firmware updates throughout the life cycle of all IoT devices. Any type of threat carried in the system can be easily detected and traced. K. Prescilla et al. [24] focused on the resource-constrained nature of the IoT devices and centralized servers are prone to single-point failures in existing IoT networks. Considering the decentralized manner of blockchain technology proposed sliding window-based blockchain architecture for IoT applications uses the most complex PoW consensus mechanism for resource-constrained IoT devices.

Besides having numerous developments in the integration of blockchain-based IoT architectures. There is still a need for the most generalized BIoT architecture which will cater to security, privacy, and interoperability with the scale of the IoT devices. BIoT architectures are extended even further to the foundation of blockchain technology, and consensus procedures, which are covered in the following subsection.

2.4. Consensus Mechanisms. The core executing environment in blockchain technology is consensus mechanisms. They are predefined computational logics that come into the execution in peer-to-peer distributed

Table 2.1: Comparative analysis of distinctive areas in leveraging Blockchain and IoT

Research Domain	Paper [Year]	Contribution	Advantages	Limitations	Future Intentions
Real-Time BIoT Applications	[12] [2022]	BIoT	security and autonomy of smart object	Authentication of nodes	Improving computation of IoT devices using ML
	[48] [2021]	BIoT	storing, retrieving, managing Healthcare data	actual implementation missing	implementation of proposed model
	[20] [2020]	Blockchain based QR cheque system	Secure authentication scheme	Limited to cheque only feature in banks	complete bank solution
	[35] [2018]	BIoT	Security highlights	Implementation	Optimal deployment
	[27] [2021]	BIoT	Security solution areas	Practical implementation	smart contract driven solutions
	[68] [2021]	Fruit and vegetable SCM	on-off chain mechanisms	limited use-case approach	consensus mechanisms
BIoT Architectures	[40] [2018]	First BIoT architecture	constrained IoT specific, secured, and better scalability	public access	Application use case
	[44] [2020]	LiTiChain finite state based BIoT	better scalability	Cost overhead	permissionless version of erasable blockchains
	[57] [2019]	AI enabled BIoT	efficient mechanism in terms of security, Big-data analytics, and low latency	limited use	wider dimensions given
	[16] [2021]	BIoT	Architecture with elastic smart contract, Smart city	Addressing security concerns on deployment	machine learning and transaction cost
Consensus Mechanisms(CM)	[69] [2020]	CMs comparative analysis	CMs categorizes in probabilistic-finality, absolute-finality	no idea proposed	Fault tolerant based CM with applications
	[39] [2018]	Types of CMs	Proof, voting criteria	limited comparison	Not available
	[65] [2020]	CMs detailed survey with vulnerability analysis	Analysis of Performance metrics	application specific	Futuristic CM design
	[66] [2021]	Enhanced CM for D2D communication	Reliability and performance	Issue with limited Lightweight device	Further enhancing for generalized BC system

communication as an agreement between the participating nodes while maintaining security, privacy, transparency, and immutability throughout the life cycle of the network. S. Nakamoto [38] initially proposed the concept of using blockchain technology for creating virtual currency such as Bitcoin. They utilized Proof of Work (PoW) as the main consensus mechanism for the fulfillment of agreement and validation of peers. PoW uses most of the computational power and high latency thus is not feasible for IoT systems. Proof of Stake(PoS) [9] is an improvement over PoW with less computational cost [49, 5]. Practical Byzantine Fault Tolerance (PBFT) [11, 5, 13] is more efficient and applicable than PoW and PoS. Proof of Activity (PoA) [7] is another consensus protocol based on PoW and PoS. Delegated Proof-of-Stake (DPoS) is representative democratic while PoS was directly democratic. Delegates are selected for the creation and validation of new blocks. DPoS is not totally decentralized but block finality is faster as compared to PoS [70]. Stellar consensus protocol (SCP) [33] is a variant of Byzantine agreement protocol. SCP gives the participants a valid choice to select the participants from a group of trusted nodes[70]. The participating node takes a decision based on the consensus of

Table 2.2: Selective IoT-based Consensus mechanisms

Consensus Mechanism	Scalability(IoT Networks)	Latency	Throughput	Computational Cost	Network Overhead
PBFT	Small Scale IoT	Low	High	Low	High
DPoS	Large Scale IoT	Low	High	Low	Low
PoET	Large Scale IoT	Low	High	Low	Low
PoI	Large Scale IoT	Low	High	Low	Low
SCP	Large Scale IoT	Low	High	Low	High
Ripple	Large Scale IoT	Low	High	Low	High
Tendermint	Large Scale IoT	Low	High	Low	Low
SDTE	Small Scale IoT	High	Low	High	High
PLEDGE	Small Scale IoT	Low	High	Low	Low

its trusted circle. Delegated Byzantine Fault Tolerance (DBFT) is a proxy voting-based consensus mechanism. Some nodes are chosen as delegates or bookkeepers, which maintain the digital ledger after a valid agreement is achieved to add a new block [30, 42]. Ripple [53] is a consensus mechanism that organizes the nodes in the form of trusted clusters within the larger network. There are two types of nodes in the network, a server for carrying the consensus process and a client for only transferring funds. Every cluster server stores a Unique Node List (UNL). In order to write a new block in the ledger, the nodes in UNL with almost 80 % majority agreement are mandatory for adding a new block in the ledger which reduces the chances of attacker nodes. Ripple is more scalable, thus favorable for IoT devices that only store the previous and new balance with no monetary rewards. Tendermint [25, 30, 5, 70] a variant of BFT consensus mechanism. It utilizes some features of PoS and PBFT to enhance high throughput, security, and less block finality time. Block is initiated by a proposer. The proposer node is in turn selected by round robin procedure by dedicated validators without any mining process. Nodes need to deposit their coins to act as validators which increases the security by punishing the dishonest nodes. Secure blockchain-based Data Trading Ecosystem (SDTE) [14] is a new consensus mechanism for data trading e-markets. In SDTE protocol, the broker and the buyer can interact with limited analysis mostly restricted to the personal data of the seller. It runs a three-way trusted secured communication protocol between the seller, buyer, and the trusted nodes. The SDTE is more secure against malicious contracts and prevents data theft and fraud. Proof of Honesty (PLEDGE) [32] is a secured consensus protocol having low transaction latency and computational cost. PLEDGE reduces the reputations and contribution of malicious and non-performing nodes in the consensus mechanism.

In Table 2.2, we have selected some of the promising consensus protocols feasible for IoT-based networks considering the scalable nature of the devices with highlights of performance metrics in terms of latency, throughput, computational cost, and network overhead of these protocols.

From the above discussion, we concluded that there are different numbers of consensus mechanisms in the literature applied to blockchain applications. Most of the consensus mechanisms are more economical for financial services. Relation to the usage of blockchain in IoT applications should fulfill some additional constraints already present in IoT systems. IoT devices are mostly connected in a distributed way and have limited commuting and communicating capabilities. The most promising consensus algorithms which are presently used in blockchain-based applications are impractical for IoT networks. However, in relation to blockchain architectures for IoT systems, some consensus algorithms may be effective in comparison to others. The reason stems from the intrinsic characteristics of blockchain architectures. In Table 2.1, we have highlighted some recent research papers based on the criteria of contribution, advantages, limitations, and future intentions in the research domains of applications, architectures, and consensus mechanisms. The next section presents our proposed blockchain architecture and also discusses the effectiveness of some consensus mechanisms in the proposed architecture.

3. Proposed Work. In this section, we will discuss about our detailed work including various dimensional attributes in leveraging blockchain with IoT-based system applications. Initially, we proposed a BIoT architecture for generalized real-time application use cases. Secondly, we summarized customized consensus mechanisms

specifically feasible for IoT-based applications. And lastly, we have discussed the real-time application use in focusing on SCM(India).

3.1. Proposed BIoT architecture. Our proposed novel blockchain-based IoT architecture (BIoT) addresses the security, failure, resilience, and many more issues associated with existing state-of-the-art IoT systems. The proposed architecture is a fusion of blockchain technology with IoT systems. In this novel architecture, the blockchain acts as the main backbone of the IoT systems, implementing security, transparency, immutability, auditability, and fault tolerance in a distributed fashion. Our architecture also incorporates the provision for the optimized consensus mechanisms for the different IoT-based applications depending on the number of IoT devices deployed in the whole network. Let us discuss the proposed architecture in detail. Figure 3.1 shows our proposed architecture in detail. The 3-tier architecture comprises of IoT device layer, the blockchain (BC) layer, and the application layer. These three layers are briefly discussed as follows.

The IoT device layer comprises the actual IoT devices which are deployed for the application-specific operation. IoT devices are mostly limited in resources. As these devices have to deal with the BC framework, a cluster of resource-efficient edge gateways will handle the computation and communication workloads of the distributed peer-to-peer network. IoT end devices are incapable of retaining the complete block of information from the blockchain ledger. However, IoT devices will store the block header information in order to maintain transparency and traceability throughout the communication network. The edge gateways are responsible enough to act as participating peers in the blockchain network. These edge gateways directly take part in the consensus mechanisms as miners or coordinators for achieving the agreement between the participating peer nodes in the distributed blockchain network. After the selection by the consensus mechanism and authorization by the certificate agency mostly government-based (eGov). The edge gateway acting as a miner also will broadcast it to the neighboring IoT nodes in the cluster. The IoT nodes will acknowledge the corresponding edge gateway as their cluster head and forward all the data directly to acknowledged cluster heads.

The blockchain layer logically comprises the main peer-to-peer BC framework and the BC access control layer. Since there is no central authority in the blockchain network, all the nodes are eligible in taking part in joining the network. The edge gateways from the IoT layer are capable of handling the computation and communication costs in the distributed BC network. The edge gateways are considered as main peer nodes in the making of a blockchain network. We have also proposed a consensus selector mechanism to select the optimal consensus mechanism which is explored in the next section. In the case of the private blockchain application security and privacy is maintained as only the specified parties are allowed to participate and carry transactions with the existing network. In our approach, some portion of the information excluding personal data in the form of analytical patterns, graphs, etc. can be uploaded to a cloud data store for business research analysis. The BC access control layer manages the creation and deployment of smart contracts, government approved certificate authority which maintains the authentication and authorization of all the participating parties in a decentralized manner. The certificate authority generates tokens as digital signatures which are further associated with the nodes for their validity in adding blocks to the distributed ledger. This layer also manages role-based policy for nodes on the basis of computing and communication capabilities and is differentiated as light IoT nodes and full nodes.

The application layer directly represents the information retrieval mechanism via different interfaces like web portals, dashboards, and decentralized applications (DApps). These are numerous IoT application uses cases with blockchain technology where transparency, security, and immutability are in a distributed manner without any third party.

The key features of the proposed BIoT architecture:

- Our model extends the existing 3-tier generalized IoT architecture with blockchain integration in a simplified manner highlighting some promising application use cases for its early adoption.
- The IoT device layer takes care of the constrained-IoT devices which simply capture the data and forward it to their corresponding Intelligent edge gateway. The information is stored in the blockchain network via full nodes by preserving the security and privacy of all nodes in a distributed and transparent manner.
- The BC layer controls the main logic of the entire system model by invoking the pluggable consensus mechanism with autonomous smart contracts among the stakeholders in agreed predefined business pro-

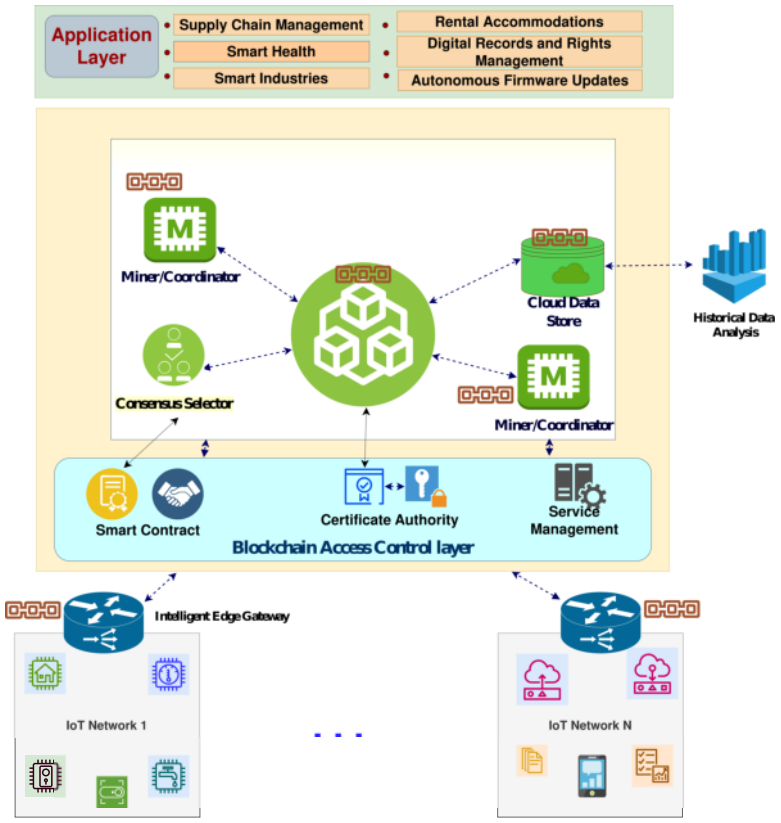

Fig. 3.1: Proposed BIoT architecture.

cedures. The distinctive feature of this layer includes the certified agency for verifying the authenticity of the registrants in the network.

3.2. Selective Consensus Mechanisms for IoT. The consensus mechanism is the core of blockchain technology in its integration of IoT ecosystems. Consensus mechanisms make the blockchain a resilient distributed and transparent mode of data storage and communication in real-time. As from the literature, there is a number of consensus mechanisms followed at different blockchain networks in varied applications. In the case of IoT-based applications, the limit of using consensus mechanisms is restricted because of resource constraints in terms of computation and communication capabilities.

Our idea of designing a customized container of optimal consensus mechanisms for the integration of blockchain-based IoT applications is motivated by the complexity of choosing among numerous consensus protocols available in the field of blockchain technology for finance, cryptocurrency, and other application services. Since IoT networks are densely deployed with IoT end devices. The scale of the number of devices varies in IoT-based applications. Thus there must be a simplified mechanism for selecting among the feasible consensus mechanisms in the framework specifically meant for IoT networks with optimal parameters like scalability, latency, throughput, computational cost, and network overhead.

The key attributes in our algorithm comprise of Z = (threshold value of the max range for small IoT network), IoT subsystems = IoT_n, I_n = number of IoT nodes in the IoT subsystem, S[x] = contains small scale consensus mechanisms, L[y] = contains large scale consensus mechanisms and selected-CM = final consensus mechanism selected. In a blockchain network, the participating peers engage in distributed peer-to-peer communication fashion. The edge gateways will act as participating peers in order to be part of the network and add their corresponding blocks in the immutable distributed ledger of blockchain after successful computational

operations. Depending on the feasible parameters required by the particular IoT-based application, the most favorable consensus mechanism will be selected and finally implemented in order to maintain the prerequisite properties of the main blockchain network. Then accordingly the edge gateways will act as miners or coordinators in different consensus mechanisms. The IoT nodes will simply follow a hierarchical tree form topology, where the edge gate will act as a cluster head for the particular IoT subsystem. Since all the IoT devices rely on cluster head gateway for their further data communication. Most of the IoT nodes will be reluctant in taking part in the mining process of the blocks, thus local copies of the block ledger will be maintained only at the level of edge gateways. With the help of this enabled procedure in the BIoT architectural framework, the work will become easier in distributed communication with resilient features of security, transparency, and high throughput in the majority of IoT applications.

Algorithm 1: Selective Consensus mechanism for IoT network

Input: Z, S[x], L[y]
Output: Selected CM
initialization;
while $IoT_n! = 0$ **do**
  check for the scale of IoT network;
  if $n^* \sum I_n >= Z$ **then**
    L[y] = [DPos, PoET, PoI, SCP, Ripple, Tendermint];
    selected-CM = L[y];
  else
    S[x] = L[y] $\bigcup$ [PBFT, SDTE, PLEDGE] ;
    selected-CM = S[x] ;
  end
end

4. Case study: Blockchain based Saffron Agri-Value Chain. Since agriculture sector is the backbone of the Indian economy, as it comprises the main pillar of India's GDP (Gross Domestic Product). We focused on ways to improvise agriculture and its allied service sectors. Supply Chain Management (SCM) is the streamlined flow of products and their data exchanges throughout the communication link between various parties in the network. The main objective of the enhancement in terms of innovation and technology in the field of SCM in the Indian agricultural sector is to maintain a transparent processing and distribution system of generating value for all starting from farmers to consumers. BC technology's integration with SCM has sufficed to maintain prerequisite features like security without any third party, transparency, data integrity, minimal risk, cost reduction, immutability, and traceability. Blockchain technology improvises the social sustainable development in SCM [17, 61]. The COVID-19 pandemic drastically highlighted the loopholes in existing SCM throughout the world and even the World Economic Forum report highlighted the need for integration of distributed and transparent technology like blockchain technology in SCM for smooth transparency and traceability with negligible reliance on third-party servers.

To understand the importance of BC in SCM in the agriculture sector. We tried to integrate the various stakeholders involved in the agriculture SCM. The main motive for integrating IoT; which will monitor real-time data via IoT devices and BC technology; acting as the backbone network which will preserve the transparency, provenance, and security of the data received by the IoT device in a permanent distributed leader. Let us take the case of saffron marketing from production, processing, and distribution. Saffron is considered to be the costliest spice grown in the world and cultivated in the northern region of India, particularly in Pampore, Jammu and Kashmir. The real challenge which the cultivators, as well as the consumers, are facing in its distribution and consumption is the availability of fake and adulterated variants of saffron in the market. Integrating the BC technology with the existing saffron marketing strategies helps in maintaining transparency and traceability throughout the saffron distribution life cycle in the whole ecosystem.

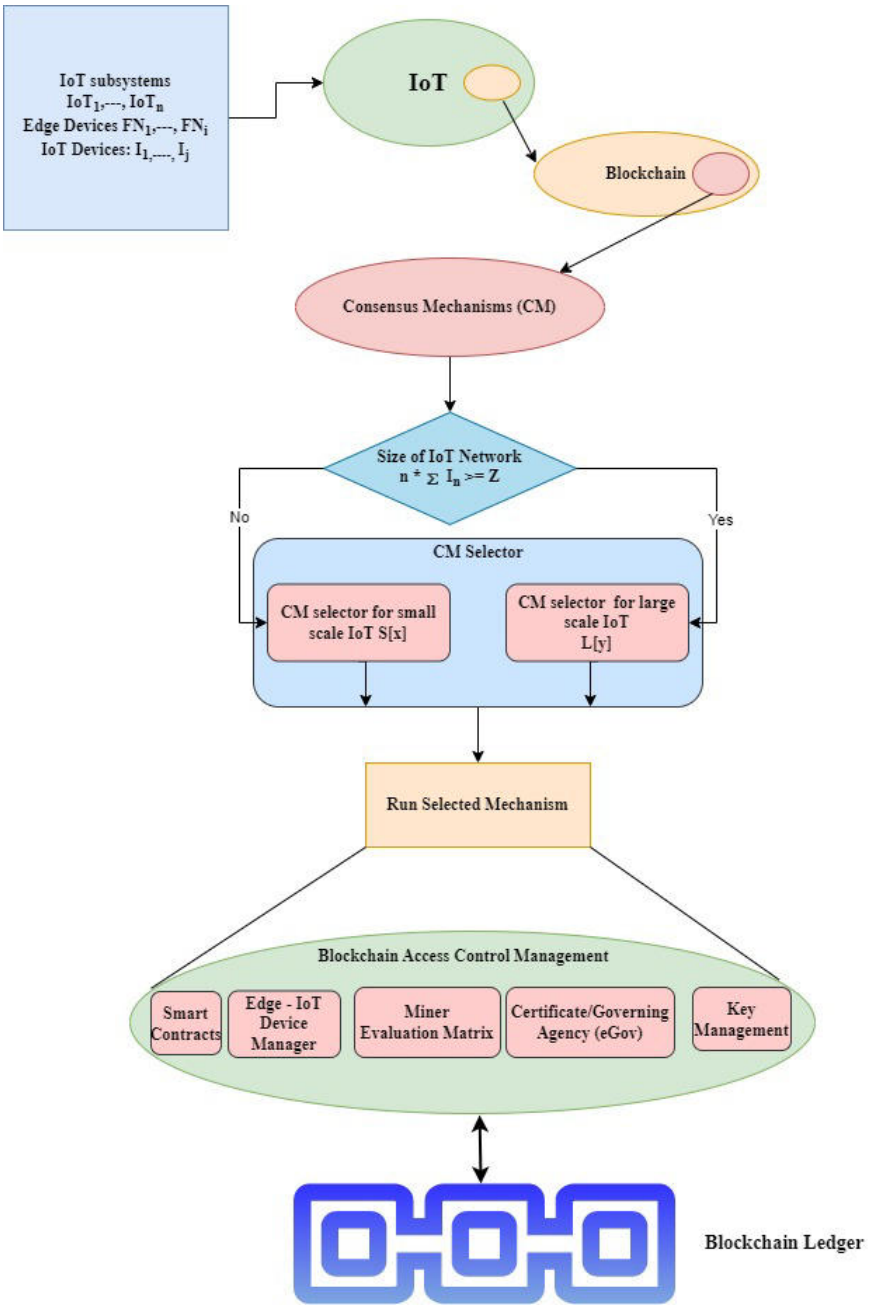

Fig. 3.2: Proposed Selective Consensus Mechanisms for BIoT Application.

Assumptions in the system model

1. BC type: Permissioned BC.
2. Light-weight IoT objects like sensors, Arduino, and Raspberry pi.
3. Full nodes- Edge gateways, Laptop, PC, Workstations.

4.1. Work Flow in Saffron-Agri Value Chain. A detailed graphical model is proposed as depicted in figure 4.1. The system model comprises real-world entities: raw material suppliers, saffron growers, government

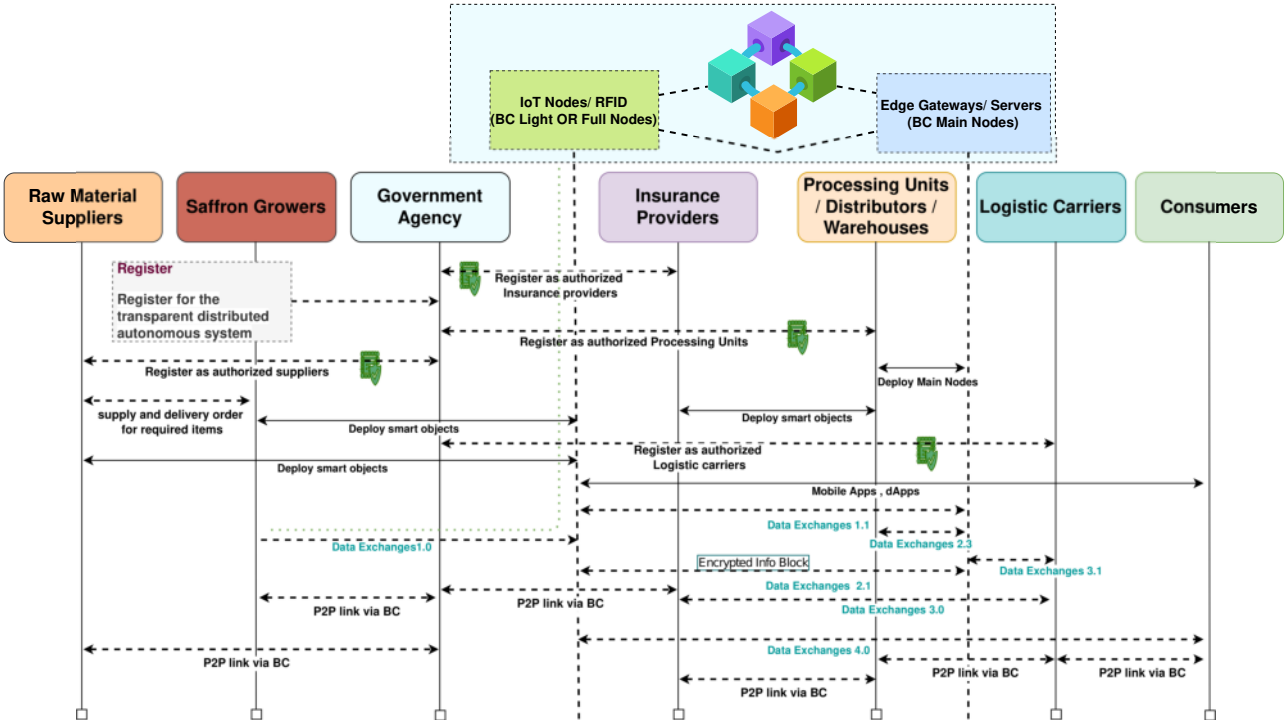

Fig. 4.1: Graphical representation of BIoT enabled Saffron-Agri Value Supply Chain in J&K, India.

market agencies, logistic carriers, insurance companies, processing units, warehouses, distributors, and end-user consumers. And the virtual objects from a technological perspective include Lightweight IoT nodes, RFID tags, and full nodes comprised of desktops, laptops, Raspberry Pi nodes, routers, and switches. The IoT networks seamlessly monitor the SCM from the farmer to the end consumer but with less security and transparency due to the main dependency on third-party services. The blockchain transaction process is based on mutual consensus in a peer-to-peer fashion and data blocks are cryptographically hashed with the previous data exchanges within the network. BC acts as the main source of proof for actual status and information throughout the network life-cycle in a transparent way. The transactional flow of data exchanges between different subsidiaries in the SCM of saffron farming initiates from the cultivating field of saffron. The saffron grower initially registers with the government agriculture department for authentication and future communication. The farmer will arrange the required raw material from government-approved suppliers. The data interactions at the actual saffron field will be captured by IoT objects and forwarded to the edge gateways. The edge gateways will act as main nodes to store the complete copy of the blockchain in their local memory. The participating parties in the system will perform autonomous transactions based on the access control management roles assigned to different peers in the network. The peers perform transactions based on the consensus mechanism implemented in the blockchain framework network. The autonomous programmable codes are created and deployed as smart contracts in BC. We focus on using the PBFT algorithm for the mutual consensus to be achieved between all participating peers in a decentralized manner. PBFT algorithm is highly efficient than PoW, PoS, and its other variants. PBFT algorithm was successfully implemented in the Hyperledger Fabric BC framework.

After authentication and authorization, any peer node can add its block to the existing ledger of transactional blocks in the blockchain network. Once the blocks are added to the chain of blocks, it is impossible to change the data block even not by the creator of the data block. As a result, all the data exchanges that are to be carried from the farmer to the consumer will be preserved efficiently and transparently.

Fig. 4.2: Prototype of test-bed network of BIoT setup

Table 4.1: Comparative analysis of existing SCM and proposed BIoT-based SCM

Index	Existing SCM	BIoT based SCM	Impact
Network Service	Centralized	Distributed	No third party
Fault Tolerance	Single point of failure	High	Replicas at multiple peers
Transparency	Low	High	Data Availability in the SC
Government agency	Least involvement	Active involvement	Report for any fraud etc
Reliability	Low	High	P2P interactions via smart contracts
Immutability	Low	High	Immutable transactions
Security	Low priority	Inbuilt hashing	Trust-less behaviour
Scalability	Low	High	IoT specific CMs
Time Saving	Low	High	Stakeholders are connected in P2P way
Cost Reduction	Low	High	Negligible monopoly of third party

4.2. Analogy of result metrics considering proposed system. The performance of the proposed BIoT architecture with selective consensus protocols in the Saffron-Agri value chain is based on our laboratory experimental simulation with limited IoT devices as light nodes and edge nodes as the full nodes. We have chosen Hyperledger Fabric, a permissioned private blockchain most favorable for our application use case. There are no transaction fees involved on any block to be added to the ledger. Any stakeholder entity needs to get registered with a government agency (eGov), which acts as the main certifying authority in the network.

The configuration of the main node comprises (CPU:i7 @3.2GHz, RAM:16GB, Storage:512GB) and one main distributed network kit with five nodes (Main Node: Quad-core @1.2GHz, RAM:2GB, OS: Ubuntu MATE 16.04 and 4 Sub-Nodes Quad-core @1.6GHz, RAM:1GB, OS: Debian 8). Light nodes comprise Arduino Uno integrated with limited sensors. Repeated tests were carried out in which the light nodes only capture data and forward it to the nearby edge nodes. The edge nodes take active participation in the block generation and storing in its database. The prototype of the test-bed network is shown in Figure 4.2. In Table 4.1 we have evaluated the comparison of our proposed scheme against the traditional approaches for different IoT-specific parameters. Our approach outperforms the traditional approach in almost all the comparison indices.

5. Conclusion. This paper focuses on enhancing security and transparency in the much-highlighted technology of the present industrial revolution i.e IoT by integrating with blockchain technology. We proposed a

BIoT architecture to incorporate BC and IoT together with a simplified access control mechanism. We have also designed a strategy for the selection of consensus mechanisms for the various IoT network applications based on determining factors like scalability, latency, throughput, computational cost, and network overhead. Our proposed model is based on a permissioned blockchain network. The advantage of using permissioned blockchain maintains limited access controls for unknown users and provides certain checks for the usage of information for different participating peers in the network. We have also discussed the case study of the proposed model in the area of the agriculture sector specifically for maintaining the transparency and traceability of the Saffron crops throughout the supply chain from farmer to the end-user. Integrating BC technology in the agricultural sector of the Saffron value chain cultivated in J&K, India, will certainly enhance provenance for the end consumers throughout the chain. It also improvises updating autonomously in various enabled services like licensing, products, and firmwares. We have implemented an initial prototype integrating blockchain with IoT devices. The preliminary results suggest that the proposed scheme implemented on SCM in the Saffron-Agri value chain outperforms the existing systems in SCM.

6. Future Perspectives. The work can be extended to other valued Agri- chain systems with modifications in their production and processing. The work can be enhanced with certain modifications for enhanced real-time track and trace other than Agri-value chain systems like handicrafts, etc.

REFERENCES

[1] R. Agrawal, P. Verma, R. Sonanis, U. Goel, A. De, S. A. Kondaveeti, and S. Shekhar, *Continuous security in iot using blockchain*, in 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, pp. 6423–6427.

[2] M. M. Ahemd, M. A. Shah, and A. Wahid, *Iot security: A layered approach for attacks & defenses*, in 2017 International Conference on Communication Technologies (ComTech), IEEE, 2017, pp. 104–110.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, *Internet of things: A survey on enabling technologies, protocols, and applications*, IEEE communications surveys & tutorials, 17 (2015), pp. 2347–2376.

[4] J. Ali and S. Sofi, *Ensuring security and transparency in distributed communication in iot ecosystems using blockchain technology: Protocols, applications and challenges*, International Journal of Computing and Digital System, (2021).

[5] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, *Applications of blockchains in the internet of things: A comprehensive survey*, IEEE Communications Surveys Tutorials, 21 (2019), pp. 1676–1717.

[6] H. Bai, G. Xia, and S. Fu, *A two-layer-consensus based blockchain architecture for iot*, in 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2019, pp. 1–6.

[7] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, *Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y*, ACM SIGMETRICS Performance Evaluation Review, 42 (2014), pp. 34–37.

[8] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, *Blockchains everywhere-a use-case of blockchains in the pharma supply-chain*, in 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), IEEE, 2017, pp. 772–777.

[9] V. Buterin, *What proof of stake is and why it matters*, Bitcoin Magazine, 26 (2013).

[10] R. Casado-Vara, J. Prieto, F. De la Prieta, and J. M. Corchado, *How blockchain improves the supply chain: Case study alimentary supply chain*, Procedia computer science, 134 (2018), pp. 393–398.

[11] M. Castro, B. Liskov, et al., *Practical byzantine fault tolerance*, in OSDI, vol. 99, 1999, pp. 173–186.

[12] E. Corradini, S. Nicolazzo, A. Nocera, D. Ursino, and L. Virgili, *A two-tier blockchain framework to increase protection and autonomy of smart objects in the iot*, Computer Communications, 181 (2022), pp. 338–356.

[13] L. Da Xu and W. Viriyasitavat, *Application of blockchain in collaborative internet-of-things services*, IEEE Transactions on Computational Social Systems, 6 (2019), pp. 1295–1305.

[14] W. Dai, C. Dai, K.-K. R. Choo, C. Cui, D. Zou, and H. Jin, *Sdte: A secure blockchain-based data trading ecosystem*, IEEE Transactions on Information Forensics and Security, 15 (2020), pp. 725–737.

[15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, *Blockchain for iot security and privacy: The case study of a smart home*, in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, 2017, pp. 618–623.

[16] S. Dustdar, P. Fernández, J. M. García, and A. Ruiz-Cortés, *Elastic smart contracts in blockchains*, IEEE/CAA Journal of Automatica Sinica, 8 (2021), pp. 1901–1912.

[17] B. Esmaeilian, J. Sarkis, K. Lewis, and S. Behdad, *Blockchain for the future of sustainable supply chain management in industry 4.0*, Resources, Conservation and Recycling, 163 (2020), p. 105064.

[18] T. M. Fernández-Caramés and P. Fraga-Lamas, *A review on the use of blockchain for the internet of things*, IEEE Access, 6 (2018), pp. 32979–33001.

[19] M. U. Hassan, M. H. Rehmani, and J. Chen, *Privacy preservation in blockchain based iot systems: Integration issues, prospects, challenges, and future research directions*, Future Generation Computer Systems, (2019).

[20] N. Kabra, P. Bhattacharya, S. Tanwar, and S. Tyagi, *Mudrachain: Blockchain-based framework for automated cheque clearance in financial institutions*, Future Generation Computer Systems, 102 (2020), pp. 574–587.
[21] M. A. Khan and K. Salah, *Iot security: Review, blockchain solutions, and open challenges*, Future Generation Computer Systems, 82 (2018), pp. 395–411.
[22] H. M. Kim and M. Laskowski, *Toward an ontology-driven blockchain design for supply-chain provenance*, Intelligent Systems in Accounting, Finance and Management, 25 (2018), pp. 18–27.
[23] D. Kirli, B. Couraud, V. Robu, M. Salgado-Bravo, S. Norbu, M. Andoni, I. Antonopoulos, M. Negrete-Pincetic, D. Flynn, and A. Kiprakis, *Smart contracts in energy systems: A systematic review of fundamental approaches and implementations*, Renewable and Sustainable Energy Reviews, 158 (2022), p. 112013.
[24] P. Koshy, S. Babu, and B. Manoj, *Sliding window blockchain architecture for internet of things*, IEEE Internet of Things Journal, 7 (2020), pp. 3338–3348.
[25] J. Kwon, *Tendermint: Consensus without mining*, Draft v. 0.6, fall, 1 (2014).
[26] W. Lin, X. Huang, H. Fang, V. Wang, Y. Hua, J. Wang, H. Yin, D. Yi, and L. Yau, *Blockchain technology in current agricultural systems: from techniques to applications*, IEEE Access, 8 (2020), pp. 143920–143937.
[27] A. H. Lone and R. Naaz, *Applicability of blockchain smart contracts in securing internet and iot: a systematic literature review*, Computer Science Review, 39 (2021), p. 100360.
[28] K. Lounis and M. Zulkernine, *Attacks and defenses in short-range wireless technologies for iot*, IEEE Access, 8 (2020), pp. 88892–88932.
[29] Q. Luo, R. Liao, J. Li, X. Ye, and S. Chen, *Blockchain enabled credibility applications: Extant issues, frameworks and cases*, IEEE Access, 10 (2022), pp. 45759–45771.
[30] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, *Blockchain's adoption in iot: The challenges, and a way forward*, Journal of Network and Computer Applications, (2018).
[31] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, *Anatomy of threats to the internet of things*, IEEE Communications Surveys Tutorials, 21 (2019), pp. 1636–1675.
[32] I. Makhdoom, F. Tofigh, I. Zhou, M. Abolhasan, and J. Lipman, *Pledge: A proof-of-honesty based consensus protocol for blockchain-based iot systems*, in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1–3.
[33] D. Mazieres, *The stellar consensus protocol (whitepaper2015)," 11 2015.*
[34] I. Miers, C. Garman, M. Green, and A. D. Rubin, *"zerocoin: Anony- mous distributed e-cash from bitcoin, " in IEEE Symposium on Security and Privacy (SP)*, (2013), p. 397–411.
[35] D. Minoli and B. Occhiogrosso, *Blockchain mechanisms for iot security*, Internet of Things, 1 (2018), pp. 1–13.
[36] N. Mishra and S. Pandya, *Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review*, IEEE Access, 9 (2021), pp. 59353–59377.
[37] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, *Addressing security and privacy issues of iot using blockchain technology*, IEEE Internet of Things Journal, 8 (2020), pp. 881–888.
[38] S. Nakamoto et al., *Bitcoin: A peer-to-peer electronic cash system*, (2008).
[39] G.-T. Nguyen and K. Kim, *A survey about consensus algorithms used in blockchain.*, Journal of Information processing systems, 14 (2018).
[40] O. Novo, *Blockchain meets iot: An architecture for scalable access management in iot*, IEEE Internet of Things Journal, 5 (2018), pp. 1184–1195.
[41] S.-V. Oprea, A. Bâra, and A. I. Andreescu, *Two novel blockchain-based market settlement mechanisms embedded into smart contracts for securely trading renewable energy*, IEEE access, 8 (2020), pp. 212548–212556.
[42] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, *Blockchain and iot integration: A systematic survey*, Sensors, 18 (2018), p. 2575.
[43] M. Pourvahab and G. Ekbatanifard, *An efficient forensics architecture in software-defined networking-iot using blockchain technology*, IEEE Access, 7 (2019), pp. 99573–99588.
[44] C. K. Pyoung and S. J. Baek, *Blockchain of finite-lifetime blocks with applications to edge-based iot*, IEEE Internet of Things Journal, 7 (2020), pp. 2102–2116.
[45] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustišek, *Towards decentralized iot security enhancement: A blockchain approach*, Computers & Electrical Engineering, 72 (2018), pp. 266 – 273.
[46] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, and M. Guizani, *Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city*, IEEE Access, 7 (2019), pp. 18611–18621.
[47] S. B. Rane, S. V. Thakker, and R. Kant, *Stakeholders' involvement in green supply chain: a perspective of blockchain iot-integrated architecture*, Management of Environmental Quality: An International Journal, (2020).
[48] P. P. Ray, D. Dash, K. Salah, and N. Kumar, *Blockchain for iot-based healthcare: Background, consensus, platforms, and use cases*, IEEE Systems Journal, 15 (2021), pp. 85–94.
[49] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, *On blockchain and its integration with iot. challenges and opportunities*, Future Generation Computer Systems, 88 (2018), pp. 173–190.
[50] M. Samaniego and R. Deters, *Blockchain as a service for iot*, in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 433–436.
[51] M. Samaniego and R. Deters, *Using blockchain to push software-defined IoT components onto edge hosts*, in: Proceedings of the International Conference on Big Data and Advanced Wireless Technologies BDAW '16, Blagoevgrad, Bulgaria, 58 (2016).
[52] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, *"zerocash: Decentralized anonymous*

payments from bitcoin, " in IEEE Symposium on Security and Privacy (SP), (2014), p. 459–474.
[53] D. Schwartz, N. Youngs, A. Britto, et al., *The ripple protocol consensus algorithm*, Ripple Labs Inc White Paper, 5 (2014).
[54] J. Sengupta, S. Ruj, and S. D. Bit, *A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot*, Journal of Network and Computer Applications, (2019), p. 102481.
[55] P. Sethi and S. R. Sarangi, *Internet of things: architectures, protocols, and applications*, Journal of Electrical and Computer Engineering, 2017 (2017).
[56] P. K. Sharma, M.-Y. Chen, and J. H. Park, *A software defined fog node based distributed blockchain cloud architecture for iot*, IEEE Access, 6 (2018), pp. 115–124.
[57] S. K. Singh, S. Rathore, and J. H. Park, *Blockiotintelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence*, Future Generation Computer Systems, 110 (2020), pp. 721–743.
[58] J. G. Song, E. S. Kang, H. W. Shin, and J. W. Jang, *A smart contract-based p2p energy trading system with dynamic pricing on ethereum blockchain*, Sensors, 21 (2021), p. 1985.
[59] T. A. Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, *A comparative analysis of blockchain architecture and its applications: Problems and recommendations*, IEEE Access, 7 (2019), pp. 176838–176869.
[60] P. Urien, *Blockchain iot (biot): A new direction for solving internet of things security and trust issues*, in 2018 3rd Cloudification of the Internet of Things (CIoT), IEEE, 2018, pp. 1–4.
[61] V. Venkatesh, K. Kang, B. Wang, R. Y. Zhong, and A. Zhang, *System architecture for blockchain based transparency of supply chain social sustainability*, Robotics and Computer-Integrated Manufacturing, 63 (2020), p. 101896.
[62] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, *New blockchain-based architecture for service interoperations in internet of things*, IEEE Transactions on Computational Social Systems, 6 (2019), pp. 739–748.
[63] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, *Blockchain-enabled smart contracts: Architecture, applications, and future trends*, IEEE Transactions on Systems, Man, and Cybernetics: Systems, (2019).
[64] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, *Survey on blockchain for internet of things*, Computer Communications, (2019).
[65] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, *A survey of distributed consensus protocols for blockchain networks*, IEEE Communications Surveys & Tutorials, 22 (2020), pp. 1432–1465.
[66] D. Yang, S. Yoo, I. Doh, and K. Chae, *Selective blockchain system for secure and efficient d2d communication*, Journal of Network and Computer Applications, 173 (2021), p. 102817.
[67] Q. Yang and H. Wang, *Privacy-preserving transactive energy management for iot-aided smart homes via blockchain*, IEEE Internet of Things Journal, 8 (2021), pp. 11463–11475.
[68] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, *A trusted blockchain-based traceability system for fruit and vegetable agricultural products*, IEEE Access, 9 (2021), pp. 36282–36293.
[69] S. Zhang and J.-H. Lee, *Analysis of the main consensus protocols of blockchain*, ICT express, 6 (2020), pp. 93–97.
[70] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, *Blockchain challenges and opportunities: A survey*, International Journal of Web and Grid Services, 14 (2018), pp. 352–375.
[71] A. Čolaković and M. Hadžialić, *Internet of things (iot): A review of enabling technologies, challenges, and open research issues*, Computer Networks, 144 (2018), pp. 17 – 39.

Edited by: Katarzyna Wasielewska
Received: Jul 27, 2022
Accepted: Nov 2, 2022