Indonesian Journal of Electrical Engineering and Computer Science
Vol. 42, No. 2, May 2026, pp. 596~608
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v42.i2.pp596-608

A lightweight architecture for IoT based on blockchain, designed for constrained IoT devices

Yassin Elgountery, Mohamed Aghroud, Meryem Lasaad, Mohamed Oualla
Department of Computer Science, CVDIS team, CESTec laboratory, FST Errachidia, Moulay Ismail University, Errachidia, Morocco

Article Info

Article history:

Received Oct 22, 2025
Revised Feb 24, 2026
Accepted May 26, 2026

Keywords:

Blockchain
Delegated node
IoT
Lightweight architecture
PBFT

ABSTRACT

Blockchain is a technology that is evolving day by day, characterized by features such as security, decentralization, immutability, traceability, and privacy protection. These features make it a promising solution for internet of things (IoT) systems. However, the inherent constraints of IoT devices in terms of storage, computation, energy capacity, and other aspects present significant challenges to integrating blockchain into these systems. This emphasizes the necessity of developing a lightweight solution that considers these specific constraints. This conceptual article proposes a lightweight architecture based on delegated nodes, centered on blockchain technology, and an optimized practical byzantine fault tolerance (PBFT) consensus algorithm, to ensure scalability and reliability for IoT. Moreover, to reduce the storage overhead in the blockchain, an off-chain cloud-based storage solution is proposed in this article. The proposed architecture is designed to prevent direct IoT device-blockchain interactions. All system operations are defined in a single smart contract, which helps reduce the complexity and overhead of the system.

Corresponding Author:

Yassin Elgountery
Department of Computer Science, CVDIS team, CESTec laboratory, FST Errachidia
Moulay Ismail University
BP 509 Boutalamine, Errachidia 52000, Morocco
Email: y.elgountery@edu.umi.ac.ma

1. INTRODUCTION

The emergence of the internet of things (IoT) marks a fundamental evolution that drives advancements in various sectors such as healthcare, industry, and agriculture. It enables a wide variety of physical objects, such as sensors, actuators, and smart devices, to connect to the internet. This technological advancement has the potential to revolutionize various fields by simplifying processes such as real-time monitoring [1], intelligent control [2], and automation [3]. Recently, there has been a revolutionary deployment of a wide range of smart IoT applications, including smart grids [4], e-health [5], and smart cities [6]. Consequently, the total number of devices connected to the IoT has grown exponentially. However, the massive integration of IoT brings several critical challenges, such as data preservation, security, and interoperability [7]. To overcome these challenges regarding security, privacy, and interoperability, blockchain technology offers a promising solution. A blockchain is a decentralized ledger technology (DLT) that ensures data security through cryptographic methods and facilitates the storage and processing of information in a distributed manner [8]. Utilizing blockchain to develop IoT systems is becoming a viable solution to address key IoT challenges, such as access security [9], data sharing [10], and efficient identity management [11]. In other words, implementing blockchain technology can enhance the efficiency of IoT solutions for various reasons. It eliminates the limitations of traditional centralized IoT models, such as

availability, transparency, and security, by enabling distributed IoT architectures. Furthermore, it ensures data reliability, decentralized management, and activity traceability. Additionally, blockchain employs programs called smart contracts, which enable the automation of transactions, making them transparent, traceable, and verifiable without the need for intermediaries [12].

In IoT environments, blockchain technology offers vast potential to address various challenges, as demonstrated by several review studies. The efficiency of IoT systems can be significantly enhanced through the intrinsic features of blockchain, such as decentralization, smart contracts, built-in trust, peer-to-peer structure, transparency, and asymmetric encryption [13], [14]. In their study, Khalid *et al.* [15] proposed a decentralized authentication system for lightweight IoT devices, utilizing fog computing and a public blockchain, which can be applied in various scenarios. Experiments have demonstrated that this mechanism is more efficient compared to existing state-of-the-art systems [8]. Dorri *et al.* [16], a lightweight and scalable blockchain (LSB) is proposed for IoT, featuring an adapted consensus algorithm and a distributed trust system to verify blocks. This two-tier system consists of interconnected networks and efficient domestic networks. Trust between nodes in the overlay network, based on direct and indirect proofs, reduces the number of transactions to be validated in each new block [17]. According to a study from Vishwakarma and Das [18], an IoT authentication model using blockchain is proposed to ensure communication security by employing a hybrid cryptosystem with lightweight cryptographic features. In this system, IoT devices are organized into clusters that operate independently without interaction. However, this structure ensures secure communication between devices within the same cluster after authentication through the blockchain. Due to their energy consumption, blockchain technologies are not well-suited for low-power IoT devices. To address this issue, Huang *et al.* [19] implemented a lightweight consensus algorithm based on proof of work, utilizing credit. A detailed analysis demonstrated the effectiveness of this model for an IoT system [8]. Zhang *et al.* [20], IoT devices act as blockchain nodes, collecting information from sensors, encrypting it, and transmitting it to a cloud server. A searchable reference to the data is then integrated into the blockchain network. According to Gehlot *et al.* [21], the IoT architecture uses blockchain technology to ensure the security of data transmission, utilizing gateways that connect IoT devices to a cloud server. This cloud server manages the transmission of IoT data and connects the system to the blockchain network. The IoT architecture described in [22] uses blockchain technology to ensure the security of data transmission in an unstable environment. IoT devices establish direct communication with the blockchain, thereby ensuring security and identity verification, and can access the network in various ways, depending on their capabilities. According to the study presented in [23], an IoT data communication method relies on blockchain technology and uses homomorphic encryption. The information collected by IoT devices is first encrypted with fully homomorphic encryption on an edge server, then signed on a cloud server using a signature algorithm. Clients send computation requests to the cloud server to retrieve the data, which returns the encrypted texts required to recover the information stored on the blockchain. The smart contract used in the IoT data-sharing system described in [24] allows for the management of functions such as client registration, device identification, data storage, and task management. Blockchain is required for all elements of the network: IoT devices, servers, and clients, in order to interact directly with it. In the study from Lone and Naaz [25], it was also demonstrated that solutions using blockchain smart contracts can be used to manage aspects such as access control in IoT, authentication, integrity assurance, data protection, and secure key management. According to Rahman *et al.* [26], a study suggests an IoT solution that uses smart contracts to enable data sharing based on policies. Each IoT device owner benefits from a distinct smart contract, thus ensuring the security and privacy of the data.

As indicated by the aforementioned research, it is feasible to use blockchain technology to address the challenge of efficiently managing data communications within an IoT network. However, certain design constraints have been identified that could hinder the practical implementation of IoT. These constraints include the direct interactions of IoT devices with the blockchain, the need to integrate additional entities [20], [22], [24] and the limited support for local intra-cluster communications [18]. In addition, there is the increased complexity caused by cloud-based blockchain communication [21], the analysis and computation of encrypted data based on the cloud [23], and the deployment of multiple smart contracts [26]. It is clear that there is still significant potential for further research and development in this emerging field. The integration of blockchain into IoT systems requires IoT devices to maintain a copy of the blockchain and participate in transaction verification and validation. However, most IoT devices face limitations in terms of storage, energy, and computational power. Additionally, large IoT networks, comprising hundreds of devices, demand a sufficiently scalable security solution. Consequently, integrating blockchain into IoT systems is a challenging task.

The central objective of this conceptual article is to address all these limitations in order to develop a lightweight, efficient, and scalable blockchain-based IoT architecture. The proposed architecture is based on delegated nodes and is structured around the blockchain technology. IoT devices are not directly integrated into the blockchain, which enhances the usability of the proposed solution in various IoT scenarios

with limited capabilities. The system operates through a single smart contract, simplifying the entire process within the blockchain network and reducing communication costs between nodes.

The proposed architecture offers the following main contributions:

- Proposal of a lightweight, scalable, decentralized, and easy-to-manage architecture.
- Implementation of lightweight nodes that perform all tasks on behalf of IoT devices not directly integrated into the blockchain network. This approach aims to achieve high performance and reduce the computational complexity of the blockchain.
- Implementation of the optimized practical byzantine fault tolerance (PBFT) protocol in the main blockchain network of our architecture. This protocol is a highly scalable consensus mechanism well-suited for IoT.
- Deployment of a smart contract encompassing all system operations to ensure traceability, operational transparency, and the reduction of communication and processing overhead in the proposed architecture.

The rest of the article is organized as follows: section 2 provides a description of the proposed architecture. Section 3 details the interactions of the proposed system. Section 4 presents a hypothetical use case illustrating the application of a lightweight architecture. Finally, section 5 concludes the article and discusses future perspectives.

2. PROPOSED ARCHITECTURE

IoT devices often face constraints in terms of computing power, storage, and energy capacity. These limitations present a real challenge when integrating blockchain into the IoT network. To overcome these challenges and simplify the management of these devices, a lightweight architecture is proposed that incorporates delegated nodes to perform complex tasks such as data management, routing, and security for these devices.

The proposed architecture consists of several layers designed to provide an IoT data communication system based on blockchain technology. The main architectural layers of the system, as illustrated in Figure 1, include the perception layer, the management layer, the blockchain layer, and the storage layer. Additionally, the blockchain network incorporates a unique smart contract deployed within the system. The system defines two major categories of users: the system administrator and the end user. The system administrator is responsible for system control, granting access permissions to clients, maintaining the blockchain network, as well as deploying and updating the smart contract. Any remote user device can serve as a client, provided it can read and write data on the blockchain network. This subsection provides a functional description of each component.

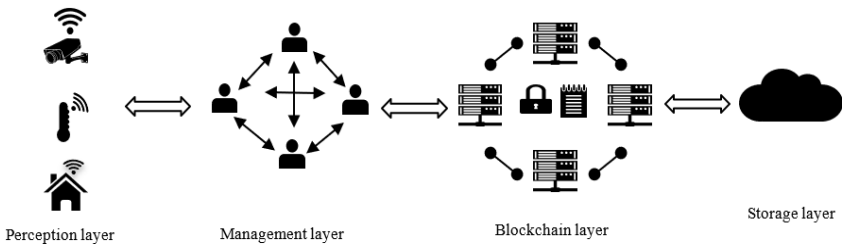

Figure 1. Proposed lightweight architecture

2.1. Perception layer

IoT devices (sensors and actuators) form the perception layer, which often faces limitations in terms of computing power, storage, and energy capacity. These limitations prevent them from interacting with the blockchain network. To simplify the management of these devices, delegated nodes are introduced into the architecture (management layer), which are often more powerful and reliable, to perform complex tasks such as data management, routing, and security. IoT devices are registered under the control of the delegated nodes. Each interaction of these devices with the blockchain network occurs through these nodes, which act as smart intermediaries and enable the execution of certain tasks on behalf of the IoT devices.

2.2. Management layer

The management layer consists of delegated nodes, which are multitasking devices serving as intelligent intermediaries between IoT devices and the blockchain. They are characterized by their unlimited

computing power, storage, and energy capacities. These delegated nodes manage the interaction between IoT devices and the blockchain, making it possible to transmit IoT data through the blockchain. They connect the IoT devices to each other and provide them with secure access to the blockchain network. Furthermore, they offer various other functionalities such as device registration, identity management, transaction verification for IoT devices, smart contract invocation, and encryption/decryption of information. The use of multiple distributed delegated nodes reduces the pressure compared to using a single node and prevents system failures caused by a single node crash. The replication of all information across all delegated nodes ensures a backup function in case of a single node failure.

2.3. Blockchain layer

For the sake of simplicity, the architecture proposed in this paper is based on a private blockchain network that can only be used by authorized users. This blockchain network operates as a distributed ledger, recording transactions and operations in an IoT context. By using a single smart contract, the delegated nodes have the ability to access and modify the ledger based on the requirements of the IoT devices. The logic of this contract is predefined, and the code is based on mathematical functions. By utilizing a smart contract, the delegated nodes can access the blockchain network, autonomously, without the intervention of a third party [27]. Due to the irreversible and immutable nature of blockchain smart contracts, it is extremely difficult for an unauthorized entity (hardware or otherwise) to alter the transactions recorded in the ledger [8], [28].

In the architecture proposed, the blockchain entity consists of four main modules as shown in Figure 2. The registration module links each IoT device to a unique identifier that corresponds to its blockchain address. The control module monitors node access to various system resources. The mining module manages blockchain transactions using mining nodes. Finally, the smart contract module simplifies the setup of a smart contract and manages all resulting events.

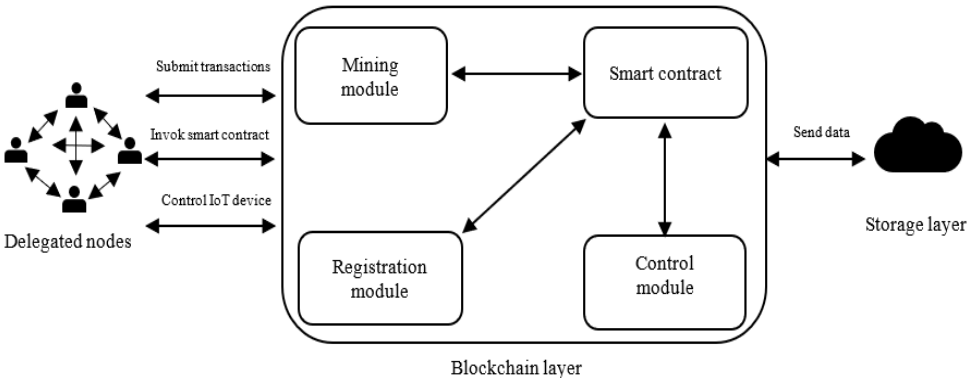

Figure 2. Modules of blockchain entity

As shown in Figure 2, miner nodes are essential for executing smart contracts. They verify and execute the contract instructions when conditions are met. They also validate the triggered transactions before adding them to a block, while ensuring everything complies with the network's rules. The smart contract operates autonomously and securely with the registration module, which manages device identities. It automates data management and updates the registration module according to predefined rules. It ensures transparency and traceability, allowing all participants to verify the registration module, thereby strengthening trust in the data.

The triggering of an action by the smart contract begins when an event on the blockchain, such as a transaction or validation, activates the execution of the contract. The smart contract then sends a request to a cloud API via an oracle [29], a service that connects the blockchain to external systems. The cloud service receives the request and executes the requested action, such as storing data or launching a computation. Once the action is completed, the results are sent back to the blockchain to be recorded or to trigger other actions, ensuring an automated, transparent, and secure process between the blockchain and the cloud. The smart contract plays a central role in the secure and autonomous management of access, whether for IoT devices or data stored in the cloud. It defines precise access rules for IoT devices, limiting interactions to specific users or devices based on predefined criteria. Additionally, it automates authorization processes for cloud data, for example by dynamically generating an access key after authentication on the blockchain, ensuring transparent, secure, and reliable permission management.

2.4. Storage layer

The storage layer is based on two types of storage: raw data storage and the storage of hashes of that data. Blockchain is used to record immutable and secure transactions. However, blockchain has limited storage capacity, which makes it unsuitable for storing large amounts of data (e.g., video streams, raw sensor, and data). Off-chain storage thus overcomes this limitation by leveraging the cloud, which stores the raw data received from the network of delegated nodes. The data can be made publicly accessible, ensuring transparency of information, or it can be restricted to preserve the privacy of the entities involved. Each delegated node allocates a cloud space for each IoT device. Once the cloud space is allocated, the delegated node provides the IoT device with secure access information, such as a token or an authentication key, enabling access to the cloud. The IoT device uses this information to encrypt, transfer, or retrieve data. Each allocated cloud space is associated with a cloud public key (CPk) [30]. This process ensures that the data is transmitted appropriately and that the source is traceable. To summarize, blockchain is used to store the hashes of the off-chain stored data, ensuring the integrity, traceability, and authenticity of this data.

3. INTERACTION BETWEEN THE LAYERS OF THE ARCHITECTURE

The interaction process between the delegated nodes and IoT devices relies on a decentralized architecture, where the delegated nodes play a crucial role in managing, securing, and ensuring the efficiency of communications between the IoT devices and the blockchain network. The section below explains the interactions between the delegated nodes and the IoT devices on one side, and those between the delegated nodes and the blockchain nodes on the other side.

3.1. Interaction process between IoT devices and delegated nodes

Figures 3 and 4 illustrate the interactions within our system. The process begins with the initialization of a smart contract and the registration of authorized clients. IoT devices register with delegated nodes, which validate their registration through the blockchain. These devices collect environmental data and transmit it to the delegated nodes, where the data is secured through encryption and hashing. The raw data is then sent to the cloud for processing, while the hash is transmitted to the blockchain to ensure its integrity.

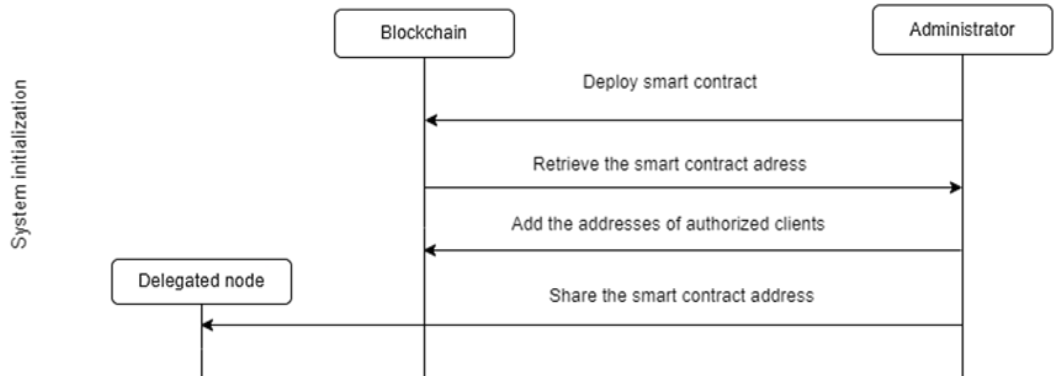

Figure 3. System initialization

3.1.1. System initialization

During the initialization phase, as shown in Figure 3, a smart contract must be created and deployed by the administrator on the blockchain network. The local addresses of authorized clients are also added by the administrator. This allows the system to manage client access and restrict system resource access to authorized users only. New clients can be added, and existing clients can be removed by the administrator as needed. The simplicity of this process is maintained to minimize system complexity while ensuring flexibility for integrating additional authentication and authorization mechanisms.

Once the smart contract is deployed and accepted in the blockchain network, the administrator receives the address of the smart contract. This address is used to identify the smart contract within the system, and other components of the blockchain network require the contract's address in order to interact with it.

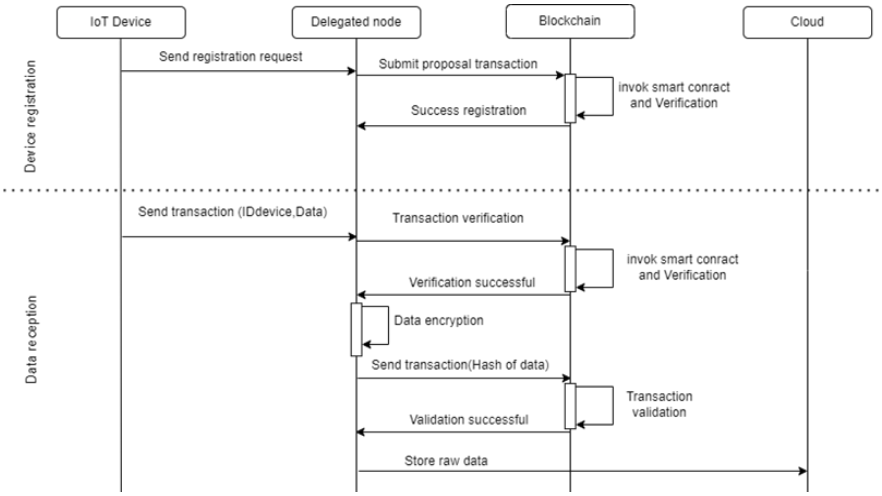

Figure 4. Device registration and data reception

3.1.2. Device registration

In the proposed scheme, the perception layer consists of various IoT devices such as sensors, surveillance cameras, and many others. Before a device can transmit the observed data, it must first register with a unique identifier under the control of a delegated node. The device sends a registration request to a delegated node in the management layer, as shown in Figure 4.

The delegated node handles the device's registration request and submits it to the blockchain node as a transaction proposal. The smart contract confirms the device's identifier and performs the transaction on the blockchain network. After completing the PBFT process [31], a new block is generated and distributed to all blockchain nodes. The node then receives the registration confirmation. All devices are registered under the control of delegated nodes with a unique identifier, following the same process, as illustrated in Figure 5.

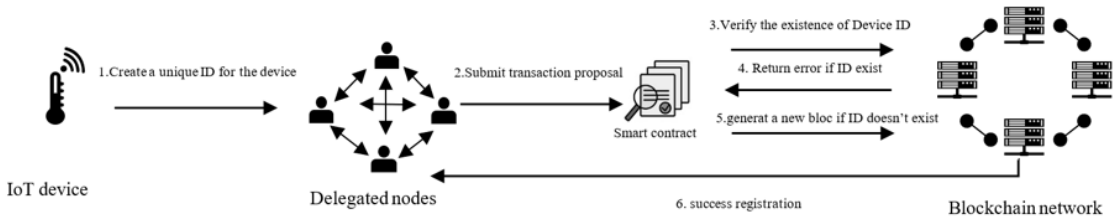

Figure 5. Device registration process

3.1.3. Data collection

IoT devices (e.g., sensors) capture environmental information such as temperature, pressure, or wind speed. This data is then sent to their delegated node via lightweight communication protocols such as message queuing telemetry transport (MQTT) and constrained application protocol (CoAP) [32]. These protocols are detailed in section 6.

3.1.4. Data reception

At the stage of data reception, as shown in Figure 4, the delegated nodes receive data from the IoT devices after verifying their authenticity. They can temporarily store the data to prevent network overload. The delegated nodes implement security protocols to ensure that the IoT devices communicating are properly authenticated. They use encryption mechanisms or digital signatures to ensure the integrity and confidentiality of the exchanged data. Afterward, they perform local analysis to process or filter the raw data and apply the hashing algorithm. The raw data is then transmitted to the cloud server, and the hash of this data is sent to the blockchain nodes. The process works as follows:

Hashing the data: the delegated node applies the SHA-256 hashing algorithm [33] to the collected data to generate cryptographic digests. This allows for verifying the integrity of the transmitted data without

having to send the raw data to the blockchain network. Hashing is a security step that ensures the data has not been altered between the source and the destination.

Sending raw data to the cloud server: after hashing and verifying the data, the delegated node sends the raw data (or, in some cases, the hashed summaries) to the cloud server for further processing, storage, or analysis. The cloud provides greater processing capacity and allows for centralizing data for more complex operations (data analysis and machine learning). The delegated node selects optimal communication paths and may retransmit the data to other delegated nodes if needed.

3.2. Interactions with the blockchain

The delegated node is directly connected to a blockchain node, such as a miner. Multiple sensor networks can be connected to a delegated node, and multiple delegated nodes can be connected to the same blockchain node. IoT devices can only request access to blockchain information through a delegated node. For simplicity, the information of the nearest miners is manually defined in each delegated node.

Figure 6 illustrates the interactions between the delegated nodes and the blockchain network. Once a delegated node generates a new block, this block must be sent to the associated blockchain node to be validated by validators before being added to the blockchain. Block validation involves verifying the data transactions by checking the public keys of the data sources and their signatures in the transactions.

The delegated node sends the received transactions to the associated blockchain miner node. The miner node receives transactions from the delegated node, with each transaction containing <IDdevice, IDnode, Hash of data>. The miner node forms a block of transactions after verifying them. Then, the miner node broadcasts the block to the blockchain network. After executing the PBFT consensus, the miner nodes validate the block. Upon validation, the block is broadcasted throughout the blockchain network.

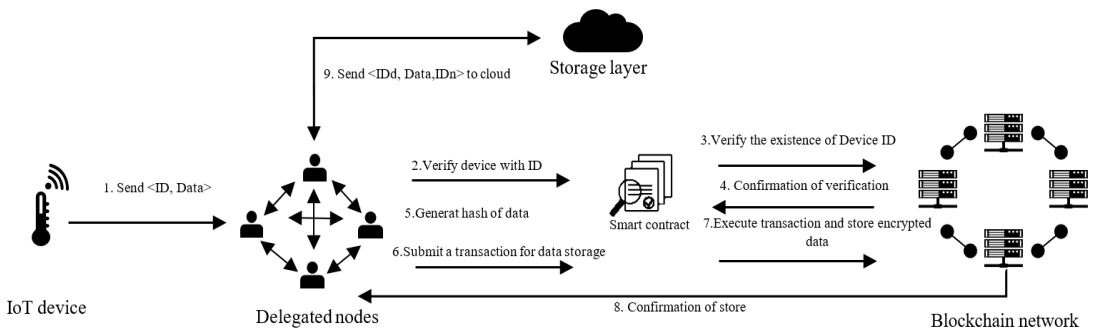

Figure 6. Data storage process

A delegated node can freely request information from any IoT device and obtain the result almost instantly from the blockchain node. On the other hand, the query operation is not stored in the blockchain, as the delegated node does not use a transaction to retrieve information from the blockchain. The information is directly extracted from the blockchain store in the blockchain node. Querying information from the blockchain incurs no fees or delays.

Delegated nodes can also send commands to IoT devices in response to analyses performed or queries from central servers. For example, after processing temperature data, a delegated node can instruct an IoT device (such as a thermostat) to adjust the temperature in a building.

3.3. Consensus algorithm

In the context of the IoT, consensus algorithms play a crucial role in coordinating connected devices, particularly in decentralized systems such as sensor networks or cloud computing. However, IoT devices often have limited resources (energy, computation, and memory), making it essential to develop optimized consensus algorithms that address these constraints.

3.3.1. Analysis of the PBFT blockchain consensus mechanism

The PBFT consensus algorithm, as shown in Figure 7, is commonly used in the blockchain domain. It relies on state replication to ensure the consistency of transmitted information. PBFT achieves consensus in three distinct steps: preparation, pre-commitment, and finalization. This algorithm guarantees fault tolerance of $(N - 1)/3$, where N is the total number of nodes, ensuring the protection and longevity of the system [34].

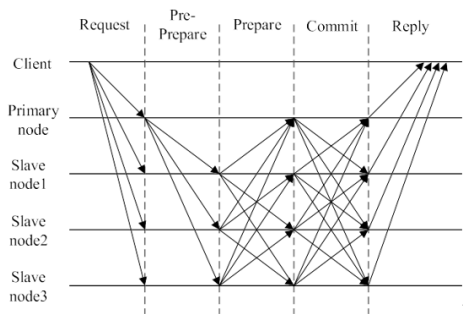

Figure 2. PBFT consensus algorithm [33]

PBFT guarantees satisfactory performance on the blockchain as long as the number of faulty nodes does not exceed one-third of the total nodes. However, with a communication complexity of $O(n^2)$, this algorithm requires a significant amount of communication resources. In the case of a simplified blockchain, where devices have limited bandwidth capabilities, the high resource requirements of PBFT make it unsuitable for contexts with constrained resources. Additionally, PBFT requires a high level of trust between nodes to maintain consistent and reliable operation. As a result, the presence of unusual or untrusted nodes seriously jeopardizes its efficiency.

3.3.2. PBFT optimization

The PBFT algorithm, designed to withstand Byzantine faults, is generally too resource-intensive for IoT contexts. This is why optimized versions are often preferred, as they consume less energy and require fewer messages. Recent studies [35]-[37] have also reduced the communication overhead associated with PBFT by streamlining the consensus process and identifying key points for achieving consensus more efficiently.

To adapt PBFT to IoT contexts, simplified versions incorporate several improvements. They reduce the interactions between replicas, thereby decreasing communication costs [35]. Criteria such as computing capacity or remaining independence are used to determine the leader, aiming to accommodate nodes with limited resources. Allowing for acceptance of delays facilitates information gathering, thus reducing the volume of interactions and energy consumption. Finally, a partial quorum can be used for certain decisions, tailored to the level of security required [37].

The simplified PBFT reduces energy consumption by minimizing the number of messages and offering a flexible quorum. Thus, even in its simplified version, PBFT remains resilient to faults and malicious behaviors. However, the lightweight PBFT is still more complex than basic algorithms like proof of authority (PoA) [38]. Furthermore, a reduction in the quorum and communications could slightly lower security, making the system more vulnerable to attacks.

3.4. Protocols of communication

In the proposed architecture, the perception layer consists of a wireless network of IoT devices, which are limited in terms of processing power, memory, and/or energy availability. IoT devices are characterized by their heterogeneity, as they are manufactured by different companies with varying specifications and communication protocols [39].

To address this issue, in the proposed architecture, delegated nodes can support different communication protocols to manage communications with various sensors. This flexibility is essential for heterogeneous networks where different devices may have distinct capabilities and communication requirements. Delegated nodes can convert messages from one protocol to another, allowing devices based on different technologies (such as CoAP, MQTT, and hypertext transfer protocol (HTTP)) [32] to communicate with each other. For instance, a sensor using CoAP to transmit data could be interpreted by a delegated node, which then retransmits the information in MQTT format to another part of the network. Devices use different protocols depending on their capabilities and specific needs. For example, the CoAP protocol is often adopted for resource-constrained sensors, MQTT is preferred for real-time communication in a publish-subscribe mode, while HTTP is used by more powerful devices that require connectivity with web services.

In a smart home use case, an IoT network monitors the house using various sensors for temperature, presence, and air quality. The temperature sensors, which have limited resources, use the CoAP protocol to transmit their data. Presence sensors use MQTT to instantly notify status changes, while more powerful air quality sensors periodically send their data to a delegated node via HTTP. In this architecture, a multi-

protocol delegated node that supports CoAP, MQTT, and HTTP centralizes the data from each sensor, processes it if necessary, and transmits it in a unified format to a cloud server or the blockchain network, ensuring smooth integration of the information.

Multi-protocol delegated nodes are crucial in IoT architectures because they promote interoperability among diverse devices, ensure scalability without disrupting the infrastructure, and reduce complexity by managing multiple protocols. This makes IoT networks more resilient, flexible, scalable, and easier to manage.

4. HYPOTHETICAL SCENARIO: APPLICATION OF THE PROPOSED ARCHITECTURE

This section presents a hypothetical use case illustrating the application of a lightweight architecture integrating the Hyperledger Fabric blockchain and the IoT for environmental monitoring of the supply chain.

4.1. Context

The IoT has become a key enabler in the digital transformation of supply chains, providing continuous product traceability, particularly in critical sectors such as agri-food and pharmaceuticals. However, the direct coupling of blockchain technologies with resource-constrained IoT devices introduces substantial challenges due to limitations in computational power, storage capacity, and energy efficiency. Consequently, the deployment of lightweight sensors, such as the DHT22, for monitoring essential environmental parameters necessitates an intermediate architecture that ensures scalability, traceability, data integrity, and overall technical viability.

4.2. The proposed lightweight architecture

The proposed architecture is based on a layered strategy comprising the IoT layer, an intermediate layer, the blockchain layer, and a storage layer. as illustrated in the Figure 8.

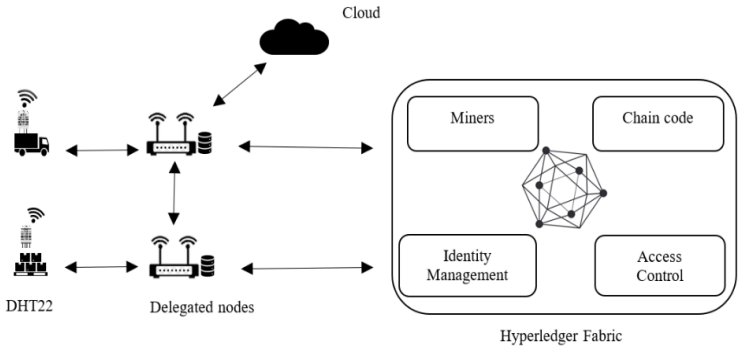

Figure 8. Proposed lightweight architecture for supply chain

The IoT layer is equipped with DHT22 sensors for temperature and humidity monitoring, deployed throughout the supply chain to periodically collect essential environmental data. However, a direct connection to the blockchain is not feasible due to the resource constraints of these devices. An intermediate layer, built on delegated nodes implemented using Node-RED and associated with the various supply chain stakeholders, ensures interoperability by handling data collection, aggregation, and preprocessing, environmental threshold verification, IoT device authentication, and the transformation of data into signed blockchain transactions. The blockchain layer, based on Hyperledger Fabric, immutably records cryptographic fingerprints (hashes) of validated data following the execution of an optimized PBFT consensus mechanism. Hyperledger Fabric relies on smart contracts to automate compliance verification, critical event logging, and responsibility traceability, while ensuring confidentiality and auditability through its permissioned model. Finally, the storage layer is responsible for preserving the raw data.

4.3. Architecture operation

Within the context of the studied agri-food supply chain scenario, DHT22 sensors are deployed to continuously monitor temperature and humidity during the transportation and storage phases of products. The collected data are transmitted via the MQTT protocol to an MQTT broker, which ensures reliable message management and distribution. These data streams are subsequently consumed by Node-RED, acting as a

delegated node for data processing tasks, including validation, timestamping, and aggregation of measurements. The raw data are stored in an off-chain storage system to optimize performance and storage capacity. In parallel, Node-RED generates a cryptographic hash for each data batch, which is recorded on the Hyperledger Fabric blockchain through the execution of a smart contract. This mechanism ensures data integrity, traceability, and non-repudiation, while preventing blockchain network overload.

4.4. Discussion

Conventional IoT–Blockchain architectures generally rely on the direct integration of IoT devices with the blockchain, whereby each device or gateway acts as a blockchain client capable of signing and submitting transactions. While this approach ensures a high level of decentralization and trust, it proves poorly suited to supply chain environments employing resource-constrained sensors such as the DHT22. Indeed, cryptographic key management, the execution of blockchain network stacks, and participation in consensus mechanisms far exceed the hardware capabilities of such devices.

In contrast, the proposed lightweight architecture adopts a clear functional separation between the IoT data collection layer and the blockchain layer. Unlike conventional models in which sensors are directly exposed to blockchain complexity, delegated Node-RED nodes act as intelligent intermediaries. This delegation significantly reduces the computational and energy burden on sensors while preserving integrity guarantees through the anchoring of cryptographic hashes on the Hyperledger Fabric blockchain.

From a data management perspective, traditional IoT–blockchain architectures tend to store a significant portion of data directly on-chain or to generate a large number of transactions, which leads to scalability, latency, and operational cost issues. In contrast, the proposed hybrid off-chain/on-chain approach restricts blockchain usage to cryptographic fingerprints, thereby enabling improved scalability and a natural adaptation to the massive data streams generated by IoT-based supply chain systems.

From a governance and access control standpoint, conventional architectures based on public or semi-public blockchains provide high transparency but limited control over participant identities. The use of Hyperledger Fabric in the proposed architecture enables a permissioned network that is more closely aligned with industrial supply chain requirements, where stakeholders are known and governed by contractual agreements. This characteristic represents a significant advantage over generic IoT–blockchain architectures, which are often designed for open environments.

However, this delegated approach introduces a trade-off between decentralization and efficiency. Unlike fully decentralized classical architectures, the presence of Node-RED delegated nodes may introduce additional points of trust. Nevertheless, this compromise is considered acceptable in an industrial context, where priority is given to performance, regulatory compliance, and ease of deployment rather than absolute decentralization.

Moreover, compared to traditional IoT–Blockchain architectures, the proposed lightweight architecture is distinguished by its integration flexibility. Node-RED facilitates interoperability with existing systems, including enterprise resource planning (ERP), warehouse management system (WMS), and cloud platforms, which often remains challenging in classical architectures tightly coupled with the blockchain. Therefore, within the context of the supply chain, the delegated approach represents a pragmatic solution that balances the theoretical requirements of blockchain with the operational constraints of real-world environments.

4.5. Limitations

Despite its advantages, this architecture presents certain limitations. Reliance on a delegated node introduces a potential point of failure or compromise, necessitating additional redundancy and security mechanisms. Furthermore, the management of off-chain storage raises challenges related to data availability, confidentiality, and synchronization with the hashes recorded on the blockchain. Finally, the latency introduced by intermediate processing at the Node-RED level may affect applications that require strict real-time decision-making.

5. CONCLUSION

This conceptual work proposed a lightweight architecture based on delegated nodes and centered around blockchain, aimed at addressing the constraints of resource-limited IoT devices. By establishing a clear functional separation between the IoT data collection layer and the blockchain layer, this approach enhances the efficiency, security, and overall performance of IoT networks while preserving the fundamental properties of the blockchain. Delegated nodes serve as intelligent intermediaries, capable of handling complex, resource-intensive tasks and optimizing data flows within large and heterogeneous networks.

Through a hypothetical scenario applied to environmental monitoring of supply chains, the study highlighted the relevance of the proposed architecture in reconciling the limitations of lightweight sensors

with industrial requirements for traceability, data integrity, and governance. The use of Node-RED–based delegated nodes significantly reduces the computational, energy, and storage burdens on IoT devices, while the hybrid off-chain/on-chain approach improves system scalability and adapts to the large volumes of data generated in real-world supply chain environments. Moreover, the integration of Hyperledger Fabric enhances access control, confidentiality, and auditability, which are critical in regulated industrial contexts.

Future research directions include exploring mechanisms for decentralizing delegated nodes, for instance through Node-RED clusters or multi-gateway approaches. The integration of advanced encryption techniques for off-chain storage, as well as the automation of compliance audits via more sophisticated smart contracts, also represents a promising avenue. Finally, large-scale experimental evaluation, including performance, scalability, and energy consumption metrics, will be necessary to validate the relevance of this architecture in real industrial environments.

ACKNOWLEDGMENTS

We would like to express our sincere gratitude to Mr. Jakimi, head of the Department of Computer Science at the Faculty of Sciences and Techniques of Errachidia, for his constant support and for providing the logistical and educational resources necessary to carry out this study. His assistance contributed significantly to the smooth progress and successful completion of this work.

FUNDING INFORMATION

The authors declare that no financial support was received for the conduct of this study.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Yassin Elgountery	✓	✓	✓		✓	✓	✓	✓	✓		✓			✓
Mohamed Aghroud	✓	✓	✓		✓	✓	✓	✓	✓		✓			✓
Meryem Lasaad	✓			✓	✓					✓	✓	✓	✓	✓
Mohamed Oualla	✓			✓	✓					✓	✓	✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this article, as no new data were generated or analyzed in the course of this study.

REFERENCES

[1] T. P. da Costa *et al.*, "A Systematic Review of Real-Time Monitoring Technologies and Its Potential Application to Reduce Food Loss and Waste: Key Elements of Food Supply Chains and IoT Technologies," *Sustainability*, vol. 15, no. 1, p. 614, Dec. 2022, doi: 10.3390/su15010614.

[2] M. Salhaoui, A. Guerrero-González, M. Arioua, F. Ortiz, A. El Oualkadi, and C. Torregrosa, "Smart Industrial IoT Monitoring and Control System Based on UAV and Cloud Computing Applied to a Concrete Plant," *Sensors*, vol. 19, no. 15, p. 3316, Jul. 2019, doi: 10.3390/s19153316.

[3] W.-S. Kim, W.-S. Lee, and Y.-J. Kim, "A Review of the Applications of the Internet of Things (IoT) for Agricultural Automation," *Journal of Biosystems Engineering*, vol. 45, no. 4, pp. 385–400, Dec. 2020, doi: 10.1007/s42853-020-00078-3.

[4] R. Pal *et al*., "A comprehensive review on IoT-based infrastructure for smart grid applications," *IET Renewable Power Generation*, vol. 15, no. 16, pp. 3761–3776, Dec. 2021, doi: 10.1049/rpg2.12272.

[5] M. Al-rawashdeh, P. Keikhosrokiani, B. Belaton, M. Alawida, and A. Zwiri, "IoT Adoption and Application for Smart Healthcare: A Systematic Review," *Sensors*, vol. 22, no. 14, p. 5377, Jul. 2022, doi: 10.3390/s22145377.
[6] N. Gavrilović and A. Mishra, "Software architecture of the internet of things (IoT) for smart city, healthcare and agriculture: analysis and improvement directions," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 1, pp. 1315–1336, Jan. 2021, doi: 10.1007/s12652-020-02197-3.
[7] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," *Internet of Things*, vol. 15, p. 100420, Sep. 2021, doi: 10.1016/j.iot.2021.100420.
[8] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things," *J. Ind. Inf. Integr.*, vol. 21, p. 100190, Mar. 2021, doi: 10.1016/j.jii.2020.100190.
[9] S. Pal, A. Dorri, and R. Jurdak, "Blockchain for IoT access control: Recent trends and future research directions," *Journal of Network and Computer Applications*, vol. 203, p. 103371, Jul. 2022, doi: 10.1016/j.jnca.2022.103371.
[10] T. Li, H. Wang, D. He, and J. Yu, "Blockchain-Based Privacy-Preserving and Rewarding Private Data Sharing for IoT," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 15138–15149, Aug. 2022, doi: 10.1109/JIOT.2022.3147925.
[11] P. R. Sousa, J. S. Resende, R. Martins, and L. Antunes, "The case for blockchain in IoT identity management," *Journal of Enterprise Information Management*, vol. 35, no. 6, pp. 1477–1505, Nov. 2022, doi: 10.1108/JEIM-07-2018-0148.
[12] A. S. Albulayhi and I. S. Alsukayti, "A Blockchain-Centric IoT Architecture for Effective Smart Contract-Based Management of IoT Data Communications," *Electronics (Basel).*, vol. 12, no. 12, p. 2564, Jun. 2023, doi: 10.3390/electronics12122564.
[13] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet of Things*, vol. 10, p. 100081, Jun. 2020, doi: 10.1016/j.iot.2019.100081.
[14] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges," *IEEE Access*, vol. 9, pp. 54478–54497, 2021, doi: 10.1109/ACCESS.2021.3070555.
[15] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Comput.*, vol. 23, no. 3, 2020, doi: 10.1007/s10586-020-03058-6.
[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019, doi: 10.1016/j.jpdc.2019.08.005.
[17] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "A trust architecture for blockchain in IoT," in *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, New York, NY, USA: ACM, Nov. 2019, pp. 190–199. doi: 10.1145/3360774.3360822.
[18] L. Vishwakarma and D. Das, "SCAB - IoTA: Secure communication and authentication for IoT applications using blockchain," *J. Parallel Distrib. Comput.*, vol. 154, pp. 94–105, Aug. 2021, doi: 10.1016/j.jpdc.2021.04.003.
[19] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism," *IEEE Trans. Industr. Inform.*, vol. 15, no. 6, pp. 3680–3689, 2019, doi: 10.1109/TII.2019.2903342.
[20] H. Zhang, X. Zhang, Z. Guo, H. Wang, D. Cui, and Q. Wen, "Secure and Efficiently Searchable IoT Communication Data Management Model: Using Blockchain as a New Tool," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 11985–11999, Jul. 2023, doi: 10.1109/JIOT.2021.3121482.
[21] A. Gehlot, P. K. Malik, R. Singh, S. V. Akram, and T. Alsuwian, "Dairy 4.0: Intelligent Communication Ecosystem for the Cattle Animal Welfare with Blockchain and IoT Enabled Technologies," *Applied Sciences*, vol. 12, no. 14, p. 7316, Jul. 2022, doi: 10.3390/app12147316.
[22] H. Qiu, M. Qiu, G. Memmi, Z. Ming, and M. Liu, "A Dynamic Scalable Blockchain Based Communication Architecture for IoT," 2018, pp. 159–166. doi: 10.1007/978-3-030-05764-0_17.
[23] S. Sun, R. Du, and S. Chen, "A Secure and Computable Blockchain-Based Data Sharing Scheme in IoT System," *Information*, vol. 12, no. 2, p. 47, Jan. 2021, doi: 10.3390/info12020047.
[24] A. Manzoor, M. Liyanage, A. Braeke, S. S. Kanhere, and M. Ylianttila, "Blockchain based Proxy Re-Encryption Scheme for Secure IoT Data Sharing," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, May 2019, pp. 99–103. doi: 10.1109/BLOC.2019.8751336.
[25] A. H. Lone and R. Naaz, "Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review," *Comput. Sci. Rev.*, vol. 39, p. 100360, Feb. 2021, doi: 10.1016/j.cosrev.2020.100360.
[26] M. Ur Rahman, F. Baiardi, and L. Ricci, "Blockchain Smart Contract for Scalable Data Sharing in IoT: A Case Study of Smart Agriculture," in *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*, IEEE, Dec. 2020, pp. 1–7. doi: 10.1109/GCAIoT51063.2020.9345874.
[27] N. Teslya and I. Ryabchikov, "Blockchain Platforms Overview for Industrial IoT Purposes," in *2018 22nd Conference of Open Innovations Association (FRUCT)*, IEEE, May 2018, pp. 250–256. doi: 10.23919/FRUCT.2018.8468276.
[28] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making Smart Contracts Smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Oct. 2016, pp. 254–269. doi: 10.1145/2976749.2978309.
[29] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania, "Astraea: A Decentralized Blockchain Oracle," in *2018 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)*, IEEE, Jul. 2018, pp. 1145–1152. doi: 10.1109/Cybermatics_2018.2018.00207.
[30] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, IEEE, Sep. 2019, pp. 1–6. doi: 10.1109/PIMRC.2019.8904404.
[31] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.
[32] M. Joshi and B. Pal Kaur, "CoAP Protocol for Constrained Networks," *International Journal of Wireless and Microwave Technologies*, vol. 5, no. 6, pp. 1–10, Nov. 2015, doi: 10.5815/ijwmt.2015.06.01.
[33] M. Kammoun, M. Elleuchi, M. Abid, and A. M. Obeid, "HW/SW Architecture Exploration for an Efficient Implementation of the Secure Hash Algorithm SHA-256," *Journal of Communications Software and Systems*, vol. 17, no. 2, pp. 87–96, 2021, doi: 10.24138/jcomss-2021-0006.
[34] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, Nov. 2002, doi: 10.1145/571637.571640.
[35] Y. Li *et al.*, "An Extensible Consensus Algorithm Based on PBFT," in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, IEEE, Oct. 2019, pp. 17–23. doi: 10.1109/CyberC.2019.00013.

[36] M. M. Jalalzai and C. Busch, "Window based BFT blockchain consensus," in *Proc. 2018 IEEE Int. Conf. Internet Things (iThings), GreenCom, CPSCom, and SmartData*, Halifax, NS, Canada, 2018, pp. 971–979, doi: 10.1109/Cybermatics_2018.2018.00184.
[37] C. Li, J. Zhang, X. Yang, and L. Youlong, "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices," *Inf. Process. Manag.*, vol. 58, no. 4, p. 102602, Jul. 2021, doi: 10.1016/j.ipm.2021.102602.
[38] S. Alrubei, E. Ball, and J. Rigelsford, "Securing IoT-Blockchain Applications Through Honesty-Based Distributed Proof of Authority Consensus Algorithm," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, IEEE, Jun. 2021, pp. 1–7. doi: 10.1109/CyberSA52016.2021.9478257.
[39] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *2012 10th International Conference on Frontiers of Information Technology*, IEEE, Dec. 2012, pp. 257–260. doi: 10.1109/FIT.2012.53.

BIOGRAPHIES OF AUTHORS

Yassin Elgountery holded a master's degree in Science and Technology (MST) in Software Engineering and Information Systems (ILSI) from the Faculty of Science and Technology (FST) in 2021 (Morocco), along with a CAPES in computer science from the National Higher School of Technical Education in Mohammedia (2011). His academic journey includes a Bachelor's degree in Science and Technology (LST) specializing in Software Engineering (2010), a University Diploma in Technical Studies (DEUST) in Mathematics, Computer Science, and Physics (2009), and a Baccalaureate in Experimental Sciences (2007). Professionally, he has worked on projects such as a cryptographic application, an e-Learning platform, and a study on blockchain and IoT in education. His research focuses on information systems, blockchain, IoT, and cryptographic applications. He is passionate about leveraging technology to develop advanced software solutions and enhance educational systems. He can be contacted at email: y.elgountery@edu.umi.ac.ma.

Mohamed Aghroud received the Master's degree in software engineering and information systems from the Faculty of Sciences and Technology of Errachidia, Moulay Ismail University, Meknes, Morocco, in 2020. He is currently pursuing a Ph.D. degree with the CVDIS Team at the same university. He also teaches at the middle school level within the Ministry of National Education in Morocco. His research interests focus on blockchain and the Internet of Things, particularly on adapting blockchain consensus algorithms for IoT networks. His academic background also includes a bachelor's degree in science and technology (LST) specializing in Software Engineering (2014), a University Diploma in Technical Studies (DEUST) in Mathematics, Computer Science, and Physics (2010), and a Baccalaureate in Experimental Sciences (2007). The author is available for contact via email at email: mo.aghroud@edu.umi.ac.ma.

Meryem Lasaad holds a Master's degree in Decision Support Systems and Imaging from the Faculty of Sciences and Techniques (FST), Errachidia, Morocco. She is a member of the ILSI research team at FST Errachidia. Her research interests focus on blockchain technologies and their applications in smart tourism and smart city systems. She can be contacted at: me.lasaad@edu.umi.ac.ma.

Dr. Mohamed Oualla obtained his Ph.D. in Computer Science from the Faculty of Sciences, Ibn Tofaïl University, in July 2017. He is currently an associate professor at the Faculty of Sciences and Technology of Errachidia, Department of Computer Science, Moulay Ismail University. He also serves as the coordinator of an engineering program and the treasurer of the Scientific Association of Academic Researchers (ASCA). He teaches in the fields of software development, blockchain & Web3, and artificial intelligence. His research interests include software engineering, blockchain, IoT, artificial intelligence, and cloud computing. He can be contacted at: m.oualla@umi.ac.ma.