Indonesian Journal of Electrical Engineering and Computer Science
Vol. 41, No. 1, January 2026, pp. 439~452
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v41.i1.pp439-452

Towards adapting the consensus proof of authentication algorithm for IoT

Mohamed Aghroud, Yassin El gountery, Mohamed Oualla, Lahcen El Bermi
[1]Department of Computer Science, CVDIS teams, Faculty of Sciences and Technology (FST) Errachidia, Moualy Ismail University, Meknes, Morocco
[2]Department of Computer Science, GLISI teams, Faculty of Sciences and Technology (FST) Errachidia, Moualy Ismail University, Meknes, Morocco

Article Info

Article history:

Received Oct 30, 2025
Revised Dec 15, 2025
Accepted Dec 22, 2025

Keywords:

Blockchain
Consensus algorithm
IoT
PoAh

ABSTRACT

The Internet of Things (IoT) represents an increasingly sophisticated paradigm which interconnects heterogeneous devices, enabling continuous data exchange and automation. However, IoT systems face significant challenges related to scalability, limited device resources, and data security. Blockchain technology provides an effective foundation for addressing such challenges thanks to its decentralized structure and consensus algorithms. This work focuses on improving the blockchain consensus protocol or consensus algorithm referred to as proof of authentication (PoAh) for adaptation to IoT networks using smart contract. It also presents a comparison of various existing consensus algorithms and explores different blockchain open-source platforms and their adaptation to IoT. Although experimental validation remains part of future work, the conceptual design and theoretical analysis presented here lay the groundwork for the future implementation and evaluation of the improved PoAh within real IoT use cases.

Corresponding Author:

Mohamed Aghroud
Department of Computer Science, CVDIS teams, Faculty of Sciences and Technology (FST) Errachida
Moualy Ismail University
Meknes, Morocco
Email: mo.aghroud@edu.umi.ac.ma

1. INTRODUCTION

Internet of things (IoT) and blockchain are considered sophisticated technologies [1], that will have a transformative impact on various sectors [1], particularly in a variety of applications like smart homes [2], smart farms [2], [3], degree certification and electronic voting, though IoTs is considered effectively an interconnected system composed of devices which provide a variety of services for industry [4]. The IoT has the same characteristics:

- The variety within IoT devices and systems.
- This decentralization concerns their infrastructure.
- Network complexity.
- This heterogeneity regarding IoT datasets.

All of these characteristics bring issues such as the diversity in IoT architectures, insufficient compatibility limitations, resource restrictions of connected devices in IoT, and risks related to confidentiality and protection [4], [5].

This emergence related to technology offers the possibility of addressing the previousely mentioned issues associated with IoT. In essence, blockchain represents a decentralized ledger that spans the whole decentralized network. With decentralised consensus, blockchains enable transactions to be carried out and validated in a distributed system where mutual distrust prevails, with no intervention of an intermediary party [4]. as long as blockchain technology is an unhackable database that no one person controls but everyone can use and anyone can check. Additional blocks (or records) can be added to the old ones as long as every node on the network agrees to add them. Additionally, once blocks are written down, they cannot be changed or removed blockchain technology has the following key aspects: decentralization, immutability, non-repudiation, transparency, pseudonymity, traceability [4]. Integration of blockchain in IoT has the following merits: interoperability, traceability, reliability, autonomic interactions [4]. Several studies have demonstrated blockchain technology's ability in ensuring data authenticity as well as traceability in IoT environments. For instance, the Docschain framework introduces a blockchain-IoT based architecture designed to securely verify and authenticate academic documents [6].

The involvement of blockchain technology into the IoT raises various issues related to the adaptation of consensus algorithms to IoT networks, especially regarding computing power, latency, data storage as well as security [7], [8]. "Widely recognized proof of work (PoW) demands significant processing power and has a latency of several minutes, which is completely unsuitable for IoT networks" [9]. This vulnerability also affects other algorithms like proof of capacity (PoC), leased proof of stake (LPoS), proof of authority (PoA), Casper, proof of burn (PoB), ByzCoin, Definity, Algorand, RsCoin, and Elastico [8], [10], [11]. Other algorithms that are suitable to some extent for IoT networks include: delegated practical byzantine fault tolerance (dPBFT), Stellar, Ripple, Tendermint, Raft, OmniLedger, and RapidChain [8]. Several researchers [8] have attempted to address these concerns, for example by using the original proof of authentication (PoAh) algorithm. However, this algorithm has its own drawbacks, as described:

- Network nodes mix transactions to form the block without validation.
- Authentication only applies at the block level, which can compromise data security and integrity.

To ensure secure communication, there are blockchain consensus algorithms such as PoW, but the issue of energy consumption means that PoAh is an algorithm suited to IoT networks based on authentication instead of processing computationally intensive operations that require higher performance.

In other words, it seems clear that Blockchain is an ideal partner for IoT because of its enhanced, data confidentiality, protection, dependability, interoperability and system expansion. In the present article, we explore an improvement to the PoAh algorithm by integrating smart contracts in order to validate transactions before they are mixed into the block, meaning that the operation is performed directly on validated blocks. Smart contracts can improve PoAh by:

- Trust development automatically: smart contracts serve to define authorization rules and adjust trust scores. The distributed ledger stores the identity and power information for each device, and smart contracts identify authorized devices and penalize inactive or malicious devices by reducing their trust scores. This makes the selection of validators dynamic, based on battery power and behavior history.
- Ensuring fast latency with lower energy consumption: smart contracts automatically enforce access control and authentication policies. When a transaction is sent, the signature and trust score are verified, resulting in either acceptance or rejection, ensuring fast latency with lower energy consumption.

The other parts of the present are subsequently presented as detailed below: section 2 outlines the consensus algorithms, with a particular focus on the PoAh algorithm. Section 3 outlines the research problem and its challenges. Section 4 introduces the proposed solution, detailing a new consensus algorithm. Section 5 presents the perspectives of this paper, highlighting the future work dedicated to modeling, performance testing, and large-scale deployment of the PoAh mechanism. At the end, section 6 sums up the work through a recap of the important results and emphasizing the key inputs of both the original and improved PoAh algorithms to IoT-blockchain integration, as well as their potential for scalable and secure real-world applications.

2. OVERVIEW OF CONSENSUS ALGORITHMS AND POAH

The blockchain employs a variety of algorithms to help nodes to reach consensus on new blocks. Table 1 classifies these consensus algorithms. This section covers two major categories: validation algorithms and authentication algorithms. We first describe validation methods and assess their usefulness for blockchain-based IoT networks. Next, we compare the various consensus validation procedures described in Table 2. Algorithms that are either incompatible with IoT networks or reflect minor variations on current consensus mechanisms are briefly discussed [8]. Finally, we consider PoAh as an example of an authentication consensus algorithm.

Table 1. The categorization of blockchain consensus algorithms [8], [12], [13]

Validation consensus algorithms	Authentication consensus algorithms
Raft, PoI, PoB, dPBFT, Tendermint, PoS, Stellar, PoA, PoET, ByzCoin, DPoS, Ripple, Casper, PoW, Tangle, LPoS, PoC, Definity, PBFT, Algorand, RSCoin, Elastico, OmniLidger, RapidChain.	PoAh

2.1. Validation consensus algorithms

The principal blockchain consensus algorithms each offer distinct validation mechanisms and levels of suitability for IoT environments. PoW [10] relies on miners' computational power, while its variants such as PoC [10] and PoET [8] use storage and random waiting times respectively, though only PoET shows partial IoT adaptability due to low latency but suffers from hardware dependency [11]. PoS [10] and its derivatives, DpoS [11], LPoS [10], PoI, PoA, Casper, and PoB, select validators based on monetary stakes, making them energy-efficient but conceptually misaligned with IoT systems lacking currency-based incentives. BFT based algorithms, notably PBFT [10], effectively secure small private IoT networks, whereas extensions like dBFT [11], SCP, Ripple, Tendermint, and ByzCoin [11] incur higher latency and throughput constraints. Verifiable random function mechanisms [12], such as Algorand and Definity [12], enhance fairness through random committee selection but are hampered by significant latency. Sharding-based algorithms, RSCoin, Elastico, OmniLedger, and RapidChain, improve scalability via parallel processing yet demand high storage and introduce synchronization complexity [13]. Raft [12], derived from Paxos, achieves low latency through leader-based voting but risks single-node dependency. Finally, Tangle [11], used by IOTA, replaces traditional blocks with a directed acyclic graph (DAG) [14], allowing every transaction to confirm two others [14], thus offering a promising lightweight structure tailored for decentralized IoT ecosystems.

Table 2 elaborates on an examination contrasting the aformentioned validation-focused agreement mechanisms and their respective adjustments [15], relative to IoTs [15], [16]. The appropriate consensus algorithms for IoTs are indicated by ● [8], [15], partially adaptable consensus algorithms are symbolized by ◐ [8], [15], and not adaptable algorithms to IoTs are represented by ○ [8], [15].

Table 2. Analytical overview on different validation consensus algorithms [8], [16]-[18]

Consensus algorithm	Through-put	Latency	Storage overhead	Adaptation in IoT
Raft	HIGH	LOW	HIGH	◐
PBFT	HIGH	LOW	HIGH	●
PoS	LOW	MEDIUM	HIGH	◐
Algorand	MEDIUM	MEDIUM	HIGH	○
PoET	HIGH	LOW	HIGH	●
Stellar	HIGH	MEDIUM	HIGH	◐
PoA	LOW	MEDIUM	HIGH	○
PoI	HIGH	MEDIUM	HIGH	◐
ByzCoiin	HIGH	MEDIUM	HIGH	○
DPoS	HIGH	MEDIUM	HIGH	◐
Tendermint	HIGH	LOW	HIGH	◐
PoC	LOW	HIGH	VERY HIGH	○
PoW	LOW	HIGH	HIGH	○
Tangle	HIGH	LOW	LOW	●
LPoS	LOW	MEDIUM	HIGH	○
Definity	N/A (Not applicable)	MEDIUM	N/A (Not applicable)	○
PoB	LOW	HIGH	HIGH	○
RapidChain	HIGH	MEDIUM	LOW	◐
dPBFT	HIGH	MEDIUM	HIGH	◐
Casper	MEDIUM	MEDIUM	HIGH	○
RSCoin	HIGH	LOW	HIGH	○
OmniLedger	HIGH	MEDIUM	LOW	◐
Ripple	HIGH	MEDIUM	HIGH	◐
Elastico	LOW	HIGH	HIGH	○

2.2. Authentication consensus algorithms

The category of authentication algorithms includes PoAh, which focuses on authenticity verification. PoAh is a consensus mechanism which integrates an confirmation process during block

validation. In the actual section, we will investigate the PoAh consensus algorithm, which is proposed to create a flexible and sustainable blockchain tailored for devices with limited resources. This algorithm incorporates an authentication process during the block validated process, while adhering to traditional communication protocols for the remainder of the process.

Figures 1, and 2 give a study comparing the PoAh offered with the PoW. The participants within network environment create transactions (Trx) using data captured or collected to constitute a block. These are represented by B = {Trx1, Trx2, ..., Trxn} as illustrated in Figure 2. The blocks are propgated by nodes for supplementary evaluation and/or assurance in the network by trusted nodes. Figure 3 shows step by step the process involves in selecting a trusted node [16].

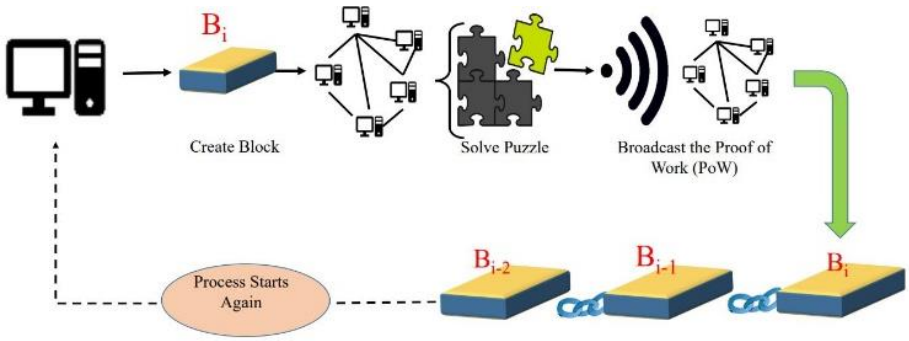

Figure 1. The machanism the consensus algorithm PoW [16]

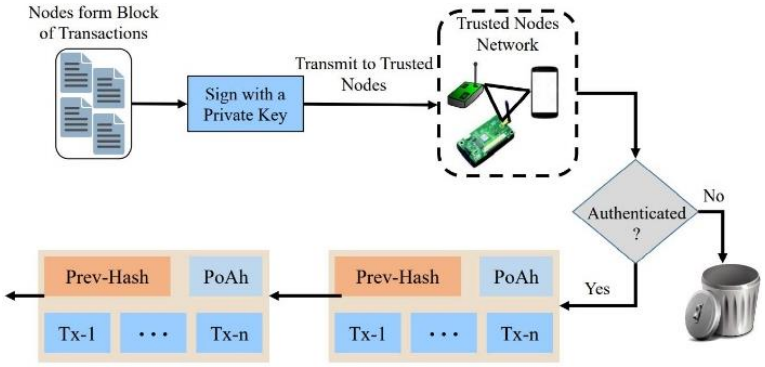

Figure 2. The original consensus algorithm PoAh [16]

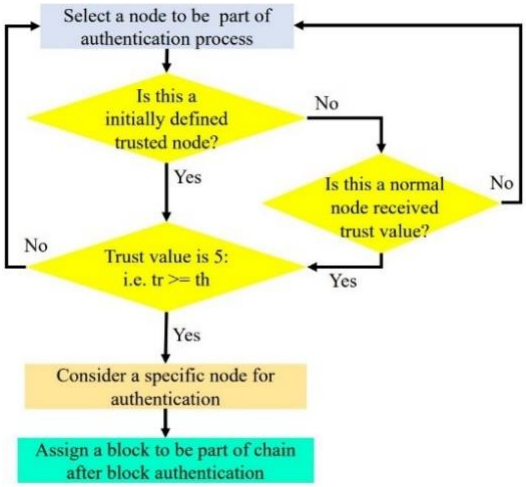

Figure 3. Process for selecting the authenticated node under PoAh [16]

The PoA consensus algorithm is designed for IoT networks to verify the authenticity of connected devices and achieve consensus on the network's state. An authentication mechanism is introduced by PoAh algorithm, contrasting with the validating process employed by different consensus algorithms. Authentication requires less energy and fewer resources compared to alternative mechanisms, making it particularly beneficial for resource-constrained environments like IoT architectures [16].

2.3. Analysis of PoAh

Practically, each device within the network is interconnected through either a wireless or cable-based network through a routing device. As a result, the devices's media access control (MAC) addresses serve as identifiers during the initiation of a transaction. Once this later is initiated, the the designated validator node obtains it and initiates the verification procedure [16]. Subsequently, this validator node [16], appends blocks into local blockchain and subsequently broadcasts it on the network [16]. Other participants will only add the block if it originates from the trusted nodes [16]. Upon receiving blocks from the trusted nodes, the nodes integrate these entries within their individual ledger maintained within the storage layer [16].

The PoAh consensus algorithm is distinguished by its resource-efficient block validation process [19]. In comparison to PoW, PoAh offers the benefit of faster execution while ensuring security. This approach enhances security thanks to decentralized blockchain-based solution of the IoTs. Furthermore, PoAh offers a more suitable for IoT applications than other blockchain consensus algorithms. These characteristics position PoAh as a promising solution, balancing efficiency, security, and flexibility for IoT environments. However, the PoAh algorithm does have certain limitations, especially regarding scalability, its capacity for large-scale implementation.

3. PROBLEMATIC STATEMENT

Blockchain and IoT are transformative developed technologies which could drastically transform various sectors as well as reshape societal structures. Blockchain enables decentralization by removing the need for intermediaries to validate transactions. However, this integration presents several research challenges for IoT, including diversity within IoT systems, network complexity [20], resource constraints of IoT devices [21], and privacy vulnerability [22].

In general, consensus algorithms in IoTs environments face several critical challenges. Foremost among these is data storage, as IoT devices typically have limited memory capacity. Ensuring the availability, integrity, and secure storage of data presents a significant hurdle. Latency is another key issue, where timely decision-making is crucial. Energy consumption poses additional concerns, given that many IoT devices are battery-powered and must operate efficiently to prolong battery life [8]. Moreover, the constrained computational ability of IoT devices can complicate the deployment of consensus protocols [8], necessitating resource-optimized solutions [8], [23].

Numerous studies have explored consensus algorithms in applications, offering a range of solutions. The use of the PoAh consensus method, which utilizes the MAC address of each network node to achieve consensus. Human networks are classified into three categories: sensor human networks, aggregator human networks, and trusted human networks, which function as miners. Experimental results indicate that the block validation process has a latency of 29 ms and an energy consumption of 44 mJ. Another proposal, discussed in [8], also uses the PoAh consensus algorithm but incorporates the EL GAMAL cryptography model along with an authentication mechanism. In this setup, trust chains authenticate transaction blocks before determining whether to accept or reject them for inclusion in the blockchain. The observed latency in this case, based on experimental results, is 3.34 seconds [16].

The primary challenge lies in identifying a consensus algorithm that is adaptable for IoTs. A comparative analysis for blockchain consensus algorithms and their applicability to IoT networks has been conducted in sources [8]. Additionally, a research study has identified several key parameters guiding selecting an agreement algorithm tailored for IoT [8], such as latency, computational power, data storage capacity, and security. Many consensus algorithms designed for cryptocurrency are not suitable for IoT applications. Therefore, the choice of a consensus method for IoT networks must consider several factors.

Based on the research projects and findings mentioned, the PoAh consensus algorithm emerges as the preferred choice due to its compatibility with IoT applications. PoAh was selected due to its authentication mechanism as well as energy efficiency, thus fitting for low-consumption IoT environments. Additionally, PoAh significantly reduces transaction latency, addressing common challenges faced by IoT applications. However, this method faces some challenges:

- Scalability: the authentication process can become a significant challenge for large-scale IoT networks, as each device must undergo unique authentication with a trust seal.

- Centralization: the PoAh algorithm depends on trust-based consensus for user authentication, which could limit decentralization and resistance to criticism—key attributes of blockchain systems.
- Susceptibility to attacks: the absence of trust within the system makes it vulnerable to cyberattacks, as malicious actors might exploit it to forge authentication credentials.

In this context IoT still encounter major issues concerning latency, network communication capacity, as well as scalability [24]. Recent research has introduced optimized multi-user communication models aimed at enhancing efficiency and minimizing transmission delay [24].

In the area of integrating blockchain technology into IoT [25], many researchers, as referenced in studies [16], [25], have proposed the PoAh consensus algorithm as a suitable and viable solution for IoT networks. However, PoAh presents several challenges within the IoT environment. First, network nodes combine transactions without conducting prior validation, which undermines the reliability of the data saved in the blocks. Additionally, there is a limit of the authentication process to the block level, leaving the data vulnerable to security and integrity risks. Finally, the authentication mechanism could become a significant bottleneck in large-scale IoT networks, as each device must be individually authenticated by a trusted node, potentially hindering performance.

The integration of the system of blockchain within IoT marks a major leap forward [26], "with the potential to transform the way connected devices communicate and exchange data" [27]. Blockchain offers a decentralized and secure framework, facilitating reliable transactions among IoT devices avoiding dependence on a central authority. Owing to the immutable and transparent features of blockchain, IoT-produced data sensors may be securely logged, establishing an indelible record.

Figure 4 illustrates the workflow for generating, checking and adding blocks into the blockchain, as well as that associated difficulties. Once a transaction is issued, it is disseminated to the network nodes, where each participant maintains an instance or portion of the transactional registry on its device-level storage [18]. Node administrators determine either to retain a full ledger copy or just the most recent blocks, based on storage and processing needs. Nevertheless, the entire blockchain remains available on the miners' nodes. Miners then confirm each transaction and group them into a block for further processing [16].

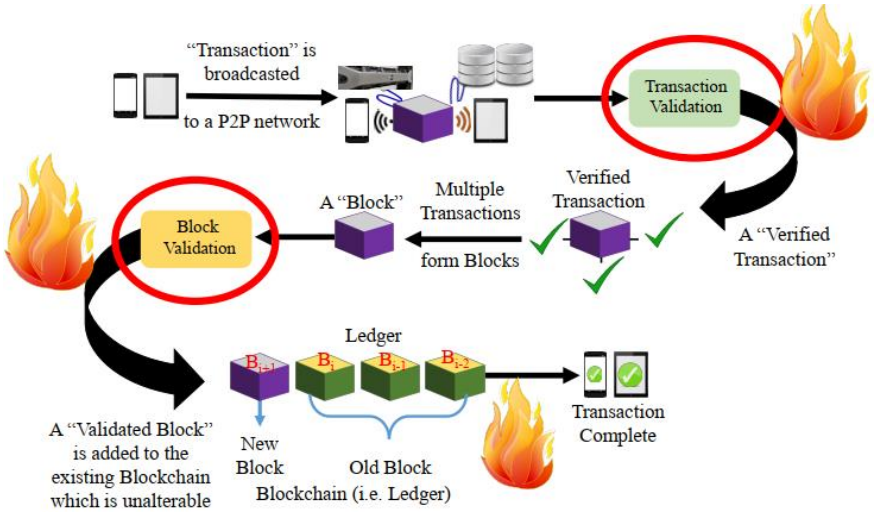

Figure 4. Procedure for forming a block and appending it to the ledger.
Visual flames are used to emphasize [16]

4. PROPOSED SOLUTION (NEW ALGORITHM)

The blockchain consensus algorithm designated by the abbreviation PoAh uses MAC addresses as identifiers for connected objects (interconnected devices). Initiated transactions are combined to form a block, and when trusted nodes receive the block, they verify the issuer's digital signature along with the device identifier (MAC address). After validation, the resulting unit becomes incorporated into a node-level ledger before being broadcast toward the remaining participants, which only add the block if it comes from a trusted node. Unlike PoW algorithm, which requires solving a costly hash puzzle (mathematical operations) (10 minutes per block), PoAh is based on lightweight operations (digital signature verification (private key (PrK) and public key (PuK)) and MAC address checking) [28], [29].

The theoretical and practical advantages are explained as follows [28], [30]:

- Energy efficiency: by eliminating intensive mining operations, PoAh reduces energy consumption.
- Fast execution: latency is in the sequence of milliseconds, that is suitable for IoT.
- Security: PoAh is based on digital signatures and limits 51% attacks by restricting validation to trusted nodes.

Despite the advantages mentioned, the original PoAh is highly dependent on trust nodes. If these fail (or are compromised), the system can become vulnerable. This means that the centralization inherent in this approach and the management of trust values pose challenges such as scalability and energy consumption.

Based on our comparative analysis regarding blockchain consensus algorithms along with their adaptability to IoT, we selected the PoAh consensus algorithm. Additionally, we proposed an improvement to enhance its suitability for IoT environments. The improved PoAh algorithm based on smart contracts which offers several notable characteristics, including:

- The improved PoAh verifies the transactions before they are intertwined in the block.
- The improved PoAh serves as a mechanism of cryptographic authentication designed for lightweight blockchain systems [30].

We present a novel architecture for improved PoAh, depicted in Figure 5, incorporating the enhancements described below:

When the transactions are released, they must be verified via the smart contracts that is using sophisticated conditions according to the specifities of the system. The rest of the process continues as in the original PoAh [16]. All of that is done to cater for:

- Data security and integrity: to strengthen data security and integrity during transaction validation, a novel approach incorporates the use of smart contracts. This method employs a conditional verification mechanism that rigorously checks each transaction before it is added to a block. The verification criteria rely on private and PuK, referencing a pre-registered list associated with each network node. If an attack attempt involving fraudulent transactions is detected, smart contracts automatically reject these transactions and flag the incident as malicious.
- Scalability: authentication should follow the verification of the transactions that constitute a block. The improved PoAh algorithm depends on an authentication process conducted by trusted nodes. However, this method faces significant scalability challenges. To overcome this, the proposed solution introduces a transparent network setup. This method guarantees that information such as the number of nodes, their list, and their MAC addresses are readily available to all participants. The goal of this transparency is to enhance transaction verification and minimize the potential for manipulation.
- Latency: continues to pose a major challenge in implementing blockchain technology in the IoT sector [31], primarily due to the requirement for real-time consensus validation times within milliseconds. One possible solution to this challenge is the integration of smart contracts. These contracts enable the definition of specific conditions for block validation or rejection, thus automating the validation process within a set timeframe. Enhancing the original PoAh algorithm involves establishing transparent network configurations, validating transactions prior to block creation, and incorporating smart contracts. These improvements aim to address current obstacles and improve the original PoAh algorithm's suitability for large-scale IoT applications.

4.1. An overview of blockchain open-source platforms

Several open source blockchain platforms offer varying degrees of suitability for IoT applications as illustrated in Table 3. Hyperledger Besu, which supports PoA and IBFT 2.0, moderately compatible with IoT due to its low computational requirements. Multichain provides a configurable framework for private blockchains emphasizing privacy, control, and throughput, supporting customizable consensus mechanisms such as PoA, yet its enterprise focus limits optimization for resource-constrained IoT environments [32], [33]. Go Ethereum (Geth), initially based on PoW and later PoS, is unsuitable for IoT because of its high resource demands, low scalability, and high transaction costs, despite supporting hybrid consensus. Substrate, developed by Parity Technologies, stands out for its modular and extensible architecture, enabling developers to design tailored blockchains with flexible consensus algorithms and interoperability across networks [34], [35]. Lastly, open Ethereum (formerly Parity Ethereum), written in rust, offers efficiency and configurability through PoA based private networks and hybrid consensus experimentation [34], [36].

The comparative analysis of blockchain platforms illustrated in Table 3 provides essential insights into their capabilities and development ecosystems for implementing the PoAh. By evaluating which is based on the implementation of the PoAh in IoT [37], indeed Substrate is the ideal choice for both IoT and PoAh use cases. Its highly modular and flexible framework allows developers to build custom consensus algorithms, including identity verification features required for PoAh, making it uniquely suited to identity based consensus models. Additionally, substrate's adaptability enables the creation of tailored solutions that

satisfy the specific needs of IoT environments [38], including lightweight and resource-efficient consensus mechanisms [38]. This combination of flexibility and customizability makes parity substrate exceptionally well-suited for both IoT and PoAh applications [16], [34].

For our case, the chosen platform was selected based on criteria such as compatibility with specific blockchain consensus algorithms like PoAh, which differs from PoA, and adaptability to IoT systems and networks. Based on these requirements, we chose parity substrate as it provides the flexibility to customize the consensus mechanism and is well suited for integration with IoT networks it contains pallets that allows to personalize and develop the consensus algorithm recommended [16], [39]. However, one can find other distributed-ledger systems like IOTA, Solana, Hyperledger Fabric, and Sawtooth [40].

Table 3. Adaptation of platforms for PoAh consensus algorithm and IoT [8], [10]

Platform	Features	Adaptation for PoAh	Programming language
Hyperledger Besu	Partially YES Supports various configurations, including PoAh for secure transactions. Allows for some customization of consensus algorithms but does not natively support PoAh.	Partially YES	JAVA
Multichain	NO Designed for enterprise use; can implement PoAh in private networks. Highly flexible; users can define their own consensus algorithms, including PoAh.	NO	C++
Go-Ethereum	NO Flexible enough to adapt PoAh for secure authentication in applications. Primarily supports PoW and is not designed for custom consensus algorithms like PoAh. Customization is limited in this context.	NO	RUST
Open Ethereum	NO Discontinued; lacks support and updates for PoAh implementation. Customization for PoAh is not straightforward and would require extensive modifications.	NO	GO
Parity Substrate	Highly modular; can be customized to implement PoAh as needed. Parity Substrate is highly modular and allows developers to implement custom consensus mechanisms, including PoAh. This flexibility makes it a strong candidate for projects requiring tailored authentication solutions.	YES	RUST

4.2. The proposed implementation of improved PoAh in IoT

Figure 5 shows the system architecture that describes how improved PoAh in IoT works. Combining transactions before verification is one of the problems encountered in the original PoAh, so we propose an improved version of PoAh by integrating smart contracts. In this case, when transactions are initiated and ready to be combined into a block, smart contracts intervene to verify them. Verification is performed according to the conditions to be processed. smart contracts operate as an automated enforcement layer that validates transactions against predefined operational constraints [28]. After verification, the valid transactions are combined into a block by the blockchain network nodes, signed with their PrK, and transmitted to trusted nodes. This prevents invalid transactions. Upon receipt of a block for validation [28], the trusted node performs signature verification by matching the sender's PuK against the signed data [41]. Once authentication is successful, the approved blocks are disseminated by authorized nodes carrying PoAh credential. Next, participating entities on the network check the PoAh related data before appending blocks to the ledger [16]. Once accepting a confirmed block [16], the participant calculates a cryptographic hash used to connect the subsequent block [16], and obtains the previous block's hash to record it in active block [16]. As illustrated in Figure 5, ledger continuity is maintained through the uniform application of this principle across all participating nodes [18]. The operational steps of the proposed procedure for improved PoAh consensus algorithm [42], are outlined within the proposed procedure as follows in Algorithm 1.

Algorithm 1. Proposed procedure for the improved PoAh [43]

- Inputs: Each node in the network employs SHA-256 cryptographic hashing, "every node is equipped with PrK and a PuK" [43].
- Outputs:
  Validated blocks added to the blockchain.
  Notation:
  Trx denotes a transaction.
  SC denotes a smart contract.
- (V_SC)(Trx): Verify transactions using smart contracts;

```
        /* Smart contracts validate transactions according to predefined, application-
specific conditions. */
-   (Trx+) → block;
        /* Nodes aggregate multiple transactions to form a block. */
-   (S_PrK)(block) → broadcast;
        /* "Each node generates a digital signature over the block using its PrK and
propagates the signed block throughout the network" [16]. */
-   (V_PuK)(block) → MAC verification [16];
        /* "Signature validation is performed by the trusted node through the sender's PuK"
[16]. */
-   If the trusted node completes block decryption successfully [16], then
                a. Authenticate the block;
                /* Block authentication is successful. /
                b. block ‖ PoAh(D) → broadcast [16];
                /* "The authenticated block is disseminated across the network by the
        trusted node" [16]. */
                c. H(block) [18] → append to blockchain [16];
                /* "Following confirmation from the trusted node, participating nodes
        integrate the block into their local blockchain ledger" [16]. */
-   Else
                a. Declare authentication failure;
                /* Block authentication is unsuccessful. */
                b. Reject the block;
-   Return to Step 1 for the next block.
```

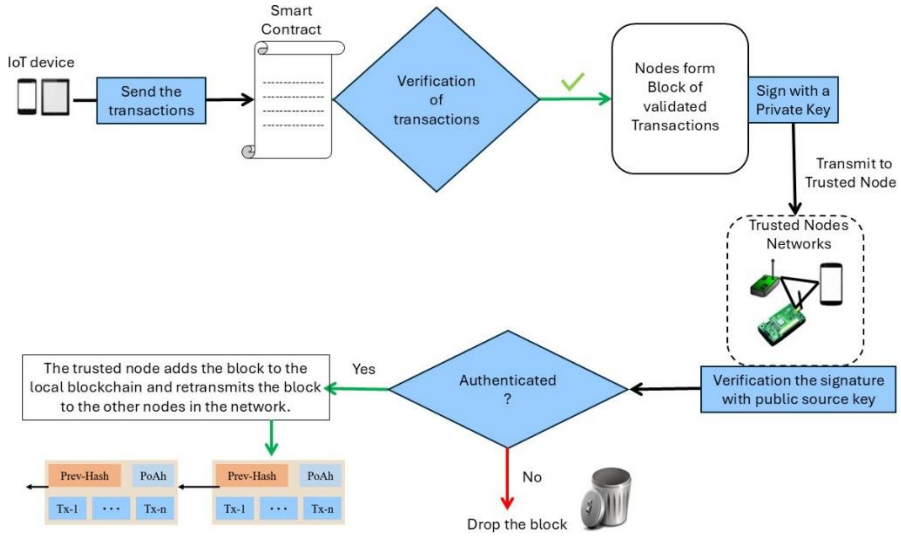

Figure 5. System architecture diagram of improved PoAh in IoT smart contract

4.3. Future simulation evaluation

The original and improved PoAh will be tested in an environment with programming languages such as Rust and JavaScript. The laptop is a trusted node where it runs the local blockchain network using a substrate node, and two Raspberry Pi devices act as IoT devices to interface with the local blockchain system as illustrated within Figure 6. This test will be based on latency calculation to measure latency. The original and improved PoAh.

Figure 6 illustrates an applied example of the system architecture for performing a practical simulation of improved PoAh. This figure represents a localized blockchain-based IoT network composed of a PC node and two Raspberry Pi devices interconnected within the same local network. The PC functions as the validator node, hosting and maintaining the blockchain through a Substrate-based environment where the PoAh operates. Meanwhile, the Raspberry Pi devices act as IoT data sources, each responsible for collecting and transmitting specific sensor information. Raspberry Pi 1 continuously measures and sends the CPU frequency, whereas Raspberry Pi 2 monitors and transmits the processor temperature. These data packets are formatted as blockchain transactions and transmitted to the validator node (the PC) for processing and validation.

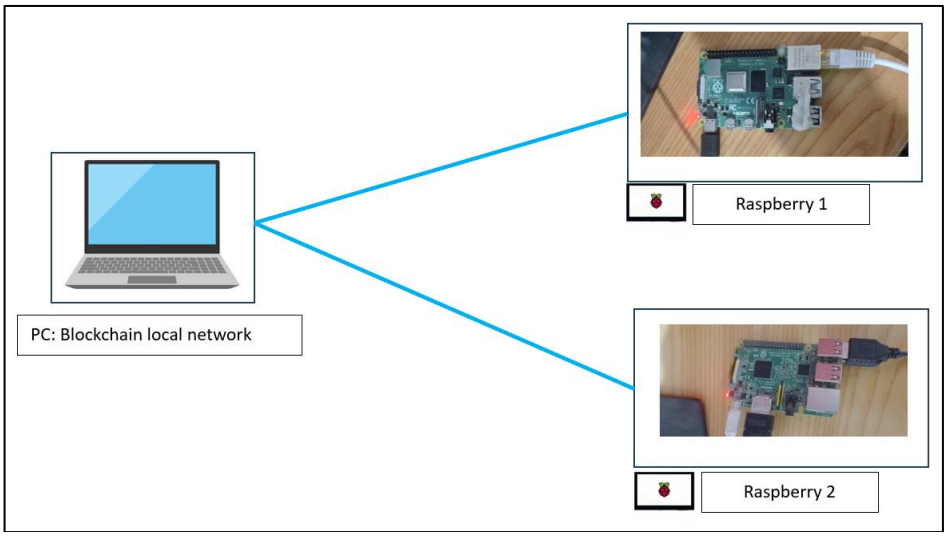

Figure 6. Case study for the proposed architecture for implementing the improved PoAh in the IoT

The improved PoAh (Figure 5) algorithm enhances the original consensus model by introducing a smart contract layer that automates transaction verification before block formation. As shown in the proposed procedure, "every node in the IoT-blockchain network employs SHA-256 hashing for cryptographic integrity, with each node owning a PrK and a PuK for secure authentication" [44]. When an IoT device initiates a transaction (Trx), the smart contract automatically checks whether the predefined conditions, such as threshold limits, sensor data consistency, or device authorization are met. This automatic validation (V_SC) significantly reduces manual verification overhead, thereby improving trust, consistency, and adaptability to application-specific rules. After validation, the authenticated transactions (Trx^{+}) are grouped into blocks, signed by the nodes using their PrK, and distributed to "the network for verification by trusted nodes" [16].

"At the validation stage, the trust node decrypts the received block using the sender's PuK to verify authenticity and confirm the source's MAC address" [45]. If the verification is successful [46], the trust node disseminates the authenticated block and adds it to the blockchain [46], ensuring integrity, immutability, and transparency. Otherwise, the block is rejected to maintain data reliability. Compared to the original PoAh, this improved PoAh with smart contracts achieves lower latency due to automated verification, enhanced security through dual-layer validation (cryptographic and conditional logic), and optimized storage since only validated and relevant data are stored on-chain. This hybridization makes it highly efficient for IoT applications requiring dynamic trust management and real-time data validation.

The comparative analysis between the original PoAh and the improved PoAh enhanced with smart contract integration demonstrates a notable evolution with respect to latency [46], throughput, security level [46], as well as storage optimization [46], all associated with which are critical parameters in IoT-blockchain systems. Both algorithms share the same foundational principles of lightweight authentication through digital signatures and trusted validation, but the improved version integrates programmable smart contracts to automate decision-making and enhance transaction verification efficiency.

The comparison between the original PoAh and the improved PoAh integrated with smart contracts clearly reveals a substantial improvement in the performance as well as adaptability within blockchain systems designed for IoT environments. Both algorithms rely on lightweight authentication using cryptographic key pairs to validate transactions and ensure data integrity, but the improved PoAh introduces a smart contract layer that automates transaction verification before block formation. This innovation reduces manual validator workload and ensures that only transactions meeting specific pre-defined conditions are processed, resulting in faster validation and greater consistency.

Overall, these findings highlight the enhanced performance delivered by the improved PoAh. The combination related to smart contract automation and cryptographic authentication leads to lower latency, higher throughput, stronger security, and optimized storage usage, thereby rendering it more apt for extensive IoT environments.

A hybrid approach integrating blockchain with edge computing has demonstrated the ability to lower processing latency while strengthening security in distributed IoT systems [7]. This aligns directly with the objective of enhancing PoAh performance in our proposed work.

5. PERSPECTIVES

The current study has established the theoretical and conceptual foundations of the consensus mechanism within blockchain technology. However, the next phase of work will primarily focus on the practical implementation of the original and improved PoAh consensus algorithm. This algorithms. The testbed for evluation for performance will focus on characteristics in terms of latency, security, and scalability, but we will start with latency.

The implementation process of this algorithm will involve several critical steps:

- Original and improved PoAh algorithm modeling: the first phase will involve translating theoretical concepts into a computational model capable of managing transaction validation within the network. This will include developing a robust authentication protocol to ensure the reliability of participating nodes.
- Performance testing: once the algorithm is modeled, extensive tests will be conducted to assess its performance under various conditions, particularly in terms of latency, fault tolerance, and security. These tests will help optimize the algorithm's parameters to enhance its efficiency.
- Comparison between original and improved PoAh algorithms: to measure the advantages of improved PoAh over original PoAh consensus mechanism. This will quantify improvements in energy efficiency, speed, and security.
- Simulation and evaluation: will be tested in an environment using a laptop that is a trust node running the local blockchain network using a Substrate node, and two Raspberry Pi devices acting as IoT devices to interact with the local as depicted in Figure 6 of the blockchain network. The programming languages used are Rust and JavaScript.
- Large-scale application: after validation, the algorithm will be tested on a simulated blockchain network to observe its behavior on a larger scale. This test will be crucial in evaluating the feasibility of its deployment in real-world distributed networks.

These stages lay the groundwork for future efforts, with the goal of integrating improved PoAh into concrete blockchain environments. This will pave the way for new applications and strengthen the capabilities of distributed networks in terms of authentication and security.

6. CONCLUSION

The original PoAh mechanism has proven to be a lightweight, efficient, and secure alternative to traditional consensus models such as PoW and PoS, which are not suited to resource-constrained IoT environments. By relying on cryptographic authentication through public and PrK, PoAh effectively guarantees the consistency, authenticity along with trustworthiness of information exchanged among IoT nodes, while maintaining a low computational load and minimal storage requirements. However, the combination of transactions without verification remains a problem. This study therefore aims to propose an improved PoAh by integrating smart contracts for the verification of transactions before they are combined into a block.

However, the introduction of improved PoAh through smart contracts marks a significant advance within blockchain-enabled IoT environments. This integration related to a smart contract layer automates transaction verification according to predefined rules, minimising latency and increasing throughput. In conclusion, future experimental validations will aim to confirm that the improved PoAh enables faster transaction verification and enhanced double-layer security, while maintaining low storage consumption. These optimisations should make improved PoAh both scalable and highly adaptable to dynamic IoT environments that require real-time decision-making, automated control and reliable data exchange. However, the challenge of implementing improved PoAh lies in its large-scale implementation, i.e., in an environment with a large number of trusted nodes.

In conclusion, the improved PoAh algorithm closes the divide between the safety needs regarding blockchain along with the efficiency requirements linked to IoT by providing a trust-based low-latency, energy-efficient consensus model suitable for smart, decentralised applications such as smart agriculture, industrial monitoring and supply chain traceability.

ACKNOWLEDGMENTS

We extend our sincere thanks to Mr. Jakimi Abdesslam, Head of the Computer Science Department at the Faculty of Sciences and Technology in Errachidia, for providing the logistical and pedagogical resources that made this work possible. His support and commitment were instrumental in the successful completion of this study

FUNDING INFORMATION

The authors declare that no funding 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
Mohamed Aghroud	✓	✓	✓	✓	✓	✓		✓	✓	✓				
Yassin El Gountery	✓	✓	✓	✓	✓	✓		✓		✓				
Mohamed Oualla		✓			✓		✓			✓	✓	✓	✓	
Lahcen El Bermi							✓				✓	✓	✓	

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 paper as no new data were created or analyzed in this study

REFERENCES

[1] S. Maitra, V. P. Yanambaka, D. Puthal, A. Abdelgawad, and K. Yelamarthi, "Integration of Internet of Things and blockchain toward portability and low-energy consumption," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, Jun. 2021, doi: 10.1002/ett.4103.

[2] S. Khan, W. K. Lee, and S. O. Hwang, "AEchain: a lightweight blockchain for IoT applications," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 64–76, Mar. 2022, doi: 10.1109/MCE.2021.3060373.

[3] Y. Wu, H. Huang, C.-X. Wang, and Y. Pan, *5G-Enabled Internet of Things*. CRC Press, 2019.

[4] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[5] M. Kamran, H. U. Khan, W. Nisar, M. Farooq, and S. U. Rehman, "Blockchain and Internet of Things: a bibliometric study," *Computers and Electrical Engineering*, vol. 81, p. 106525, Jan. 2020, doi: 10.1016/j.compeleceng.2019.106525.

[6] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, S. Mumtaz, and Z. U. Qayyum, "Docschain: Blockchain-Based IoT solution for verification of degree documents," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 3, pp. 827–837, Jun. 2020, doi: 10.1109/TCSS.2020.2973710.

[7] H. Liao *et al.*, "Blockchain and semi-distributed learning-based secure and low-latency computation offloading in space-air-ground-integrated power IoT," *IEEE Journal on Selected Topics in Signal Processing*, vol. 16, no. 3, pp. 381–394, Apr. 2022, doi: 10.1109/JSTSP.2021.3135751.

[8] M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in blockchain for resource-constrained IoT networks," *Internet of Things (Netherlands)*, vol. 11, p. 100212, Sep. 2020, doi: 10.1016/j.iot.2020.100212.

[9] C. Laroiya, D. Saxena, and C. Komalavalli, "Applications of blockchain technology," in *Handbook of Research on Blockchain Technology*, Elsevier, 2020, pp. 213–243.

[10] J. Debus, "Consensus methods in blockchain systems," *Frankfurt School of Finance & Management, Blockchain Center*, 2017.

[11] Z. Auhl, N. Chilamkurti, R. Alhadad, and W. Heyne, "A comparative study of consensus mechanisms in blockchain for IoT networks," *Electronics*, vol. 11, no. 17, p. 2694, Aug. 2022, doi: 10.3390/electronics11172694.

[12] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021, doi: 10.1109/ACCESS.2021.3065880.

[13] M. Zamani, M. Movahedi, and M. Raykova, "RapidChain: scaling blockchain via full sharding," in *Proceedings of the ACM Conference on Computer and Communications Security*, Oct. 2018, pp. 931–948, doi: 10.1145/3243734.3243853.

[14] "Publications – Laboratoire Informatique d'Avignon," 2025. https://lia.univ-avignon.fr/publications-en/ (accessed Dec. 13, 2025).

[15] A. Idrissi, *Modern Artificial Intelligence and Data Science, Tools, Techniques and Systems*, vol. 1102. Cham: Springer Nature Switzerland, 2023.

[16] D. Puthal, S. P. Mohanty, V. P. Yanambaka, and E. Kougianos, "PoAh: a novel consensus algorithm for fast scalable private blockchain for large-scale IoT frameworks," *arXiv: arXiv:2001.07297*, 2020, [Online]. Available: http://arxiv.org/abs/2001.07297.

[17] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "Ethereum for secure authentication of IoT using pre-shared keys (PSKs)," in *Proceedings - 2019 International Conference on Wireless Networks and Mobile Communications, WINCOM 2019*, Oct. 2019, pp. 1–7, doi: 10.1109/WINCOM47513.2019.8942487.

[18] M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for IoT networks," June 19, 2019, arXiv: arXiv:1809.05613. doi: 10.48550/arXiv.1809.05613.
[19] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: using blockchain to protect personal data," in *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, May 2015, pp. 180–184, doi: 10.1109/SPW.2015.27.
[20] H. N. Dai, H. Wang, G. Xu, J. Wan, and M. Imran, "Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies," *Enterprise Information Systems*, vol. 14, no. 9–10, pp. 1279–1303, Nov. 2020, doi: 10.1080/17517575.2019.1633689.
[21] J. H. Khor, M. Sidorov, and P. Y. Woon, "Public blockchains for resource-constrained IoT devices - a state-of-the-art survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11960–11982, Aug. 2021, doi: 10.1109/JIOT.2021.3069120.
[22] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, Jan. 2017, doi: 10.1109/MCOM.2017.1600363CM.
[23] T. A. Adep and V. S. Dhongde, "Implementation towards blockchain for security and maintenance of educational documents," Int. J. Innov. Res. Comput. Commun. Eng., vol. 11, no. 6, pp. 8667–8674, June 2023.
[24] N. Agrawal, A. Bansal, K. Singh, C. P. Li, and S. Mumtaz, "Finite block length analysis of RIS-assisted UAV-based multiuser IoT communication system with non-linear EH," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3542–3557, May 2022, doi: 10.1109/TCOMM.2022.3162249.
[25] D. Puthal, C. Y. Yeun, E. Damiani, A. K. Mishra, K. Yelamarthi, and B. Pradhan, "Blockchain data structures and integrated adaptive learning: features and futures," *IEEE Consumer Electronics Magazine*, vol. 13, no. 2, pp. 72–80, Mar. 2024, doi: 10.1109/MCE.2023.3268827.
[26] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: a systematic literature review," in *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, Nov. 2016, vol. 0, pp. 1–6, doi: 10.1109/AICCSA.2016.7945805.
[27] V. Pathak, R. J. Pandya, V. Bhatia, and O. A. Lopez, "Qualitative survey on artificial intelligence integrated blockchain approach for 6G and beyond," *IEEE Access*, vol. 11, pp. 105935–105981, 2023, doi: 10.1109/ACCESS.2023.3319083.
[28] S. Asaithambi, S. Nallusamy, J. Yang, S. Prajapat, G. Kumar, and P. S. Rathore, "A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things," *Scientific Reports*, vol. 15, no. 1, p. 15410, May 2025, doi: 10.1038/s41598-025-00337-3.
[29] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, Jan. 2019, doi: 10.1109/MPOT.2018.2850541.
[30] S. Maitra, V. P. Yanambaka, A. Abdelgawad, D. Puthal, and K. Yelamarthi, "Proof-of-authentication consensus algorithm: blockchain-based IoT implementation," in *IEEE World Forum on Internet of Things, WF-IoT 2020 - Symposium Proceedings*, Jun. 2020, pp. 1–2, doi: 10.1109/WF-IoT48130.2020.9221187.
[31] S. Namasudra and K. Akkaya, *Blockchain and its Applications in Industry 4.0*, vol. 119. Singapore: Springer Nature Singapore, 2023.
[32] S. Ismail, H. Reza, H. K. Zadeh, and F. Vasefi, "A blockchain-based IoT security solution using multichain," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023*, Mar. 2023, pp. 1105–1111, doi: 10.1109/CCWC57344.2023.10099128.
[33] S. M. Umran, S. F. Lu, Z. A. Abduljabbar, and V. O. Nyangaresi, "Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry," *Internet of Things (Netherlands)*, vol. 24, p. 100969, Dec. 2023, doi: 10.1016/j.iot.2023.100969.
[34] C. Connors and D. Sarkar, "Comparative study of blockchain development platforms: features and applications," *arXiv: arXiv:2210.01913*, 2022, [Online]. Available: http://arxiv.org/abs/2210.01913.
[35] C. N. Samuel, F. Verdier, S. Glock, and P. Guitton-Ouhamou, "A fair crowd-sourced automotive data monetization approach using substrate hybrid consensus blockchain," *Future Internet*, vol. 16, no. 5, p. 156, Apr. 2024, doi: 10.3390/fi16050156.
[36] I. Michail, "Blockchain ethereum private network," Master's Thesis, University of Piraeus, 2018. https://dione.lib.unipi.gr/xmlui/handle/unipi/11209 (accessed: Nov. 23, 2024).
[37] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment," *IEEE Access*, vol. 10, pp. 36978–36994, 2022, doi: 10.1109/ACCESS.2022.3164081.
[38] A. Mewada, N. Singh, M. A. Ansari, and A. S. Yadav, *Applications of Blockchain Technology*. Boca Raton: Chapman and Hall/CRC, 2025.
[39] X. Xu, I. Weber, and M. Staples, "Existing blockchain platforms," in *Architecture for Blockchain Applications*, Cham: Springer International Publishing, 2019, pp. 27–44.
[40] A. I. Abdi, F. E. Eassa, K. Jambi, K. Almarhabi, and A. S. A. M. Al-Ghamdi, "Blockchain platforms and access control classification for iot systems," *Symmetry*, vol. 12, no. 10, pp. 1–17, Oct. 2020, doi: 10.3390/sym12101663.
[41] Y. J. Chen, L. C. Wang, and S. Wang, "Stochastic blockchain for IoT data integrity," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 373–384, Jan. 2020, doi: 10.1109/TNSE.2018.2887236.
[42] E. Siemens, "Proceedings of the 7th International Conference on Applied Innovations in IT, ICAIIT 2019," *Proceedings of International Conference on Applied Innovation in IT*, vol. 7, no. 2, 2019.
[43] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-authentication for scalable blockchain in resource-constrained distributed systems," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Jan. 2019, pp. 1–5, doi: 10.1109/ICCE.2019.8662009.
[44] S. Eslamian and F. Eslamian, *Blockchain Technology for Water and Environmental Systems*. Boca Raton: CRC Press, 2025.
[45] S. T. Saeidi, H. R. Shahriari, and M. Nikooghadam, "Protecting metadata privacy in blockchain-based EHR systems: a group addressing structure," *Journal of Information Security and Applications*, vol. 94, 2025, doi: 10.1016/j.jisa.2025.104236.
[46] W. Zhao, M. Patibandla, and J. Ding, "An approach for ensuring the privacy in smart contracts," in *Proceedings - 2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security Companion, QRS-C 2023*, Oct. 2023, pp. 320–329, doi: 10.1109/QRS-C60940.2023.00046.

BIOGRAPHIES OF AUTHORS

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). He can be contacted at email: mo.aghroud@edu.umi.ac.ma.

Yassin El Gountery holded a Master 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 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 and Web3, and artificial intelligence (AI). His research interests include software engineering, blockchain, IoT, AI, and cloud computing. He can be contacted at email: m.oualla@umi.ac.ma.

Lahcen El Bermi is currently a professor of computer science and engineering in the Department of Computer Science at the Faculty of Sciences and Technology of Errachidia, Moulay Ismail University. He also served as head of the computer science department from 1994 to 2020. He is a member of several scientific associations and has served steering and program committees for numerous international conferences, workshops, and symposia. He has been teaching in the fields of software engineering and information systems since 1994. His research focuses on statistics and probability, software engineering, artificial intelligence, data visualization, blockchain, IoT, and smart applications. He can be contacted at email: l.elbermi@umi.ac.ma.