IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 January 2024, accepted 4 February 2024, date of publication 14 February 2024, date of current version 23 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3366492

RESEARCH ARTICLE

Blockchain-Based Privacy-Preserving Shop Floor Auditing Architecture

FATEMEH STODT[1,2], (Member, IEEE), MOHAMMED B. M. KAMEL[1,3,4], CHRISTOPH REICH[1], (Member, IEEE), FABRICE THEOLEYRE[2], (Senior Member, IEEE), AND PETER LIGETI[4]

[1]Institute for Data Science, Cloud Computing and IT Security (IDACUS), Furtwangen University, 78120 Furtwangen, Germany
[2]ICube Laboratory, CNRS/University of Strasbourg, 67400 Strasbourg, France
[3]Department of Computer Science, University of Kufa, Najaf 54001, Iraq
[4]Department of Computer Algebra, Eötvös Loránd University (ELTE), 1053 Budapest, Hungary

Corresponding author: Mohammed B. M. Kamel (mkamel@inf.elte.hu; mkamel@uokufa.edu.iq)

This work was supported in part by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund through the TKP2021-NVA Funding Scheme under Project TKP2021-NVA-29, in part by the European Research Council (ERC) Advanced Grant "ERMiD" and the Federal Ministry of Education and Research (BMBF) of Germany under Grant COSMIC-X 02J21D144, and in part by the Projektträger Karlsruhe (PTKA).

ABSTRACT In the rapidly evolving realm of the Industrial Internet of Things (IIoT), securing shop floor operations, especially in audit processes, is of critical importance. This paper confronts the challenge of ensuring data integrity and trust in IIoT systems by leveraging the capabilities of blockchain technology. The unique characteristics of blockchain, such as its immutable and decentralized ledger, establish a solid and transparent foundation for verifying shop floor transactions and activities. We introduce a privacy-centric approach, meticulously designed to comply with stringent data privacy regulations. This method allows auditors to authenticate both IIoT data and devices, ensuring confidentiality and adhering to regulatory standards. Our practical implementation strategy, tailored for shop floor environments, not only enhances the security of device and data integrity but also showcases robustness against specific adversarial threats, including network intrusion, data tampering, and unauthorized access. The findings indicate that our approach not only strengthens security protocols but also integrates effortlessly with existing IIoT infrastructures. It presents an efficient, scalable solution that elevates the safety and reliability of IIoT ecosystems, making it a significant step forward in the quest for secure and compliant industrial operations.

INDEX TERMS Attribute-based verification, blockchain, IIoT, Industry 4.0, privacy, shop floor.

I. INTRODUCTION

The manufacturing sector is undergoing a transformative evolution, propelled by Industry 4.0, which ushers in an era of intelligent, data-driven production [1]. This paradigm shift, characterized by the integration of Big Data analytics across the product lifecycle - from production to distribution, and after-sales support to retail - is reshaping how products are conceived, produced, and delivered [2]. Such integration significantly impacts the industry, revolutionizing traditional manufacturing processes.

The associate editor coordinating the review of this manuscript and approving it for publication was Stefano Scanzio.

However, this transition towards intelligent manufacturing brings forth significant challenges. A notable issue is the fragmentation of data within the manufacturing industry, as identified by Yu et al. [3]. This fragmentation acts as a barrier, impeding the efficient aggregation and analysis of vast data volumes, which is crucial for harnessing the full potential of Industry 4.0 [4]. Addressing this data fragmentation is key to enhancing the effectiveness and efficiency of production processes.

At the heart of this transformation is the shop floor, where raw materials are converted into finished goods. Here, the need for efficient coordination and real-time information sharing is more pronounced than ever. Any lapse in data

management or tracking can lead to significant operational disruptions, ultimately impacting the competitiveness of industrial entities [5].

In response to these challenges, blockchain technology emerges as a viable solution, offering a decentralized, transparent, and secure method for managing and tracking information on the shop floor [6]. This study explores the development and application of a blockchain solution tailored to the specific needs of shop floor operations within the context of Industry 4.0.

Our research is novel in its approach and contribution to the IIoT field, particularly in the following aspects:

1) We develop a unique blockchain-based framework specifically designed for the IIoT environment. This framework enhances data integrity and auditability on the shop floor, offering a more refined and practical solution compared to existing models.
2) We introduce a privacy-preserving verification process that allows auditors to authenticate IIoT data and devices without compromising sensitive information. This approach is aligned with current data privacy regulations, addressing a critical gap in existing research.
3) We provide empirical validation of our framework through real-world testing, demonstrating its effectiveness in improving operational efficiency and data security. This practical application distinguishes our study from others that primarily focus on theoretical aspects.

These contributions represent significant advancements in the application of blockchain technology within the IIoT domain, especially in enhancing secure and efficient audit processes on the shop floor.

The structure of the paper is organized as follows: Section II reviews related research in the field of industrial blockchain, emphasizing recent developments and advancements. Section IV provides background information on attribute-based authentication and industrial blockchain. Our proposed architecture is detailed in Section V, and an analysis of this architecture is presented in Section VI. In Section VII, we bring a practical use case to illustrate the application of our proposal. Finally, Section VIII concludes the paper with our findings.

II. RELATED WORKS

The combination of blockchain technology and the IIoT is revolutionizing manufacturing processes and fostering a synergistic effect that enhances efficiency, security, and transparency in the quickly changing Industry 4.0 landscape. While Bahga's [7] introduction establishes a framework for understanding blockchain in IIoT, it falls short in addressing specific implementation challenges in industrial environments, a gap this research aims to fill.

The digitization of industry necessitates the confidentiality and integrity of critical data. Blockchain technology is instrumental in securing shop floor data [8] and adds unprecedented transparency to manufacturing processes [9]. However, these studies primarily focus on theoretical aspects and lack practical implementation strategies, particularly in high-volume, fast-paced industrial settings, which our research directly addresses. In the following, the state of art of blockchain-based IIoT (II-A) and lightweight blockchain-based approaches (II-B) are discussed.

A. BLOCKCHAIN-BASED INDUSTRIAL INTERNET OF THINGS (BIIOT)

Blockchain-based Industrial Internet of Things (BIIoT) enhances interoperability across IIoT systems, as seen in the work by Kasten et al. [10]. However, these approaches often do not consider the unique security challenges of decentralized systems, especially in firmware upgrade procedures, which our study aims to address. Wan et al.'s [11] blockchain-based solution for firmware upgrades is innovative but lacks scalability and real-world applicability, aspects our research improves upon.

The centralized nature of systems is one of the major issues with the present IIoT infrastructure, and this is most noticeable in the firmware upgrade procedure. Conventional techniques entail the manual installation of firmware upgrades on IIoT nodes after obtaining them from a central server. This procedure adds possible security flaws in addition to being expensive and time-consuming. More recent techniques implement a kind of distributed repository of firmwares [12], where each node can provide certain versions to its neighbors. However, enforcing global security may be very challenging with these techniques.

A blockchain-based solution that uses smart contracts to automate and secure the firmware upgrade process throughout the industrial network is introduced in the work published in [11]. Using a decentralized approach improves the system's efficiency and security since nodes may independently evaluate and apply firmware changes.

The integration of blockchain with digital twins, as discussed by Sasikumar et al. [13], marks a significant advancement. However, their approach underestimates the complexity of real-time data synchronization in IIoT networks, an issue our framework tackles. Yang et al.'s EdgeShare [14] demonstrates the importance of edge computing in blockchain-IIoT integration but does not adequately address latency and privacy issues, which our architecture overcomes.

Stodt et al.'s [15] specialized blockchain-based Trust Management System (TMS) for IIoT is notable for its decentralized trust management. However, it lacks adaptability in dynamic industrial environments, an aspect our proposal significantly enhances.

B. LIGHTWEIGHT BLOCKCHAIN-BASED APPROACHES

Lightweight blockchain solutions, like Tikiri [16] and LightChain [17], are pivotal for resource-constrained Internet of Things (IoT) devices. These methods, while efficient,

do not fully address the balance between computational overhead and security robustness. AEchain [18] and Fusion Chain [19] focus on security and data privacy but their approaches to scalability and real-time processing are limited, issues our approach resolves.

The work by Selvarajan et al. [20] and Allouche et al. [21] offers significant insights into privacy preservation and load balancing, but they do not fully explore the integration of these technologies in industrial settings, a gap our research fills.

In summary, while existing literature lays a strong foundation for the integration of blockchain in IIoT, there remain significant gaps in practical implementation, security, scalability, and real-time data handling. Our research addresses these gaps, offering a comprehensive, scalable, and secure framework tailored for industrial IIoT environments.

III. BLOCKCHAIN-BASED IIOT CHALLENGES

The convergence of blockchain technology and the IIoT or BIIoT represents a paradigm shift towards an industrial ecosystem that is more transparent and safe. Nonetheless, this integration creates specific difficulties. To fully realize the potential of BIIoT, this subsection explores the open research issues and challenges that must be resolved.

1) PRIVACY LEAKAGE

Although blockchain technologies use a number of safeguards to protect transaction confidentiality, they are not infallible. For example, Bitcoin transactions use IP addresses to mask user identities, thereby offering some anonymity [22]. These precautions, however, are not always successful since transaction patterns can disclose user identities [23]. Moreover, confidentiality violations may result from the full storage of transaction data on the blockchain.

2) SECURITY VULNERABILITY

Security is improved by integrating blockchain with IIoT through the creation of signatures and cryptographic techniques. However, security risks associated with vulnerabilities in IIoT and blockchain systems are substantial [24]. Industrial wireless networks are vulnerable to security lapses like eavesdropping and jamming [25]. Furthermore, the viability of heavy encryption techniques is limited by the resource constraints of IIoT nodes [26], and it is difficult to manage cryptographic keys in decentralized environments. These security problems are made worse by smart contract vulnerabilities, as the DAO attack showed when it stole $50 million worth of Ethereum by taking advantage of these flaws [27].

3) RESOURCE CONSTRAINTS

IIoT nodes, which include RFID tags and sensors, are generally limited in terms of their processing power, storage capacity, and energy availability. The resource-intensive Proof ofWork (PoW) consensus algorithm used in blockchain technology may not be appropriate for low-energy IIoT nodes [28]. The deployment of blockchain data across IIoT nodes is complicated by its large size since these nodes frequently function in environments with erratic network connections [22].

4) SCALABILITY

One major obstacle to blockchain technology's use in large-scale IIoT networks is its scalability. The low transaction throughput of existing blockchain systems, such as Bitcoin, limits their applicability to IIoT applications with high transaction volumes [29]. Blockchain scalability improvements are necessary to handle the high volume of transactions and nodes in IIoT networks.

5) BIG DATA

The massive volumes of data generated by IIoT call for efficient big data analytics in order to glean insightful information. However, because blockchain data is encrypted and IIoT nodes have limited resources, traditional big data analytics systems are not appropriate for BIIoT [30]. Although cloud computing presents a viable solution, it also raises issues with latency and privacy.

In summary, while blockchain offers promising solutions for enhancing IIoT, addressing these challenges in Table 1 is crucial for its successful integration and adoption in industrial settings.

TABLE 1. Issues in blockchain-based IIoT.

Challenge	Description
Privacy Leakage	• User identities can be revealed through analysis • Complete transaction data storage leads to potential breaches
Security Vulnerability	• Resource constraints limit encryption techniques • Challenges in key management and smart contract vulnerabilities
Resource Constraints	• IIoT nodes are resource-constrained • Resource-intensive blockchain consensus algorithms are infeasible • Large blockchain data size and unstable network connections are challenging
Scalability	• Low transaction throughput in current systems • Not suitable for high-transaction IIoT applications • Need for enhanced blockchain scalability
Big Data	• Vast amounts of data generated by IIoT • Cloud computing offers solutions but introduces privacy and latency issues

IV. PRELIMINARIES

The foundations for the attribute verification protocol and industrial blockchain are intricately laid out, providing a solid framework for understanding the seamless integration of these technologies for the proposed architecture. In this section, the main building blocks of our solution have been discussed.

A. ATTRIBUTE VERIFICATION PROTOCOL

Attribute verification protocol [31] is a distributed protocol that can be utilised as a building block in a system to verify the participants based on their attributes in privacy-preserving approach. It has many applications as data validation [32] and network security [33]. Three roles with specific responsibilities exist:

- **Issuer**: The issuer acts as the authority and the responsible entity for attributes. An issuer is responsible for giving the verifier the public key of attributes and providing the attributes to the prover (user).
- **Verifier**: The verifier's role is to check and confirm the attributes of the prover (user). In a zero-knowledge scenario, the verifier challenges the prover for proof.
- **Prover**: The prover is the entity trying to prove that it possesses certain attributes. It first validates its ownership of the proven attributes with the issuer. Once a prover has confirmed possession of a claimed attribute, the issuer sends a secret key for that attribute to the user. Then, the prover will be able to respond to the challenges posed by the verifier.

The verifier in the attribute verification protocol decides which attributes will be used during the verification process. The protocol supports two main verification modes:

- *1-out-of-n verification mode*: In this mode, the verifier defines a set of attributes, and the verification process of the prover passes as long as at least one of its attributes is in the set of defined attributes by the verifier.
- *n-out-of-n verification mode*: this mode provides exhaustive verifications since the prover's verification process ensures that all defined attributes pass the verifier's tests.

It is noteworthy to mention that in the 1-out-of-n verification mode, the privacy of the prover is preserved as the prover does not need to reveal any of its attributes other than the fact that it has one of the defined attributes by the verifier.

B. INDUSTRIAL BLOCKCHAIN

The inherent decentralization and immutability of blockchain technology provide significant benefits for applications in the industrial sector. Assuring accuracy and confidence in data, a uniform ledger view is made available to all authorized network members, hence elevating transparency.

1) PROPERTIES

A fundamental change in the recording and sharing of information is brought about by blockchain technology. Blockchain is a distributed ledger that keeps an ever-expanding list of data records safe from alteration and manipulation. Every record, referred to as a block, has a timestamp and is connected to all other blocks in a chronological sequence [34].

Instead of being kept in one place, the ledger is duplicated and dispersed among a network of computers. All nodes in the network receive updates from the blockchain whenever a new block is added. The decentralized nature of the ledger enhances its transparency and reliability by enabling all network participants to verify, store, and transmit data.

The information on a blockchain is thought to be unchangeable. Network agreement is necessary because once a block's data is recorded, it cannot be changed without also changing all blocks that come after it. A fundamental component of the blockchain's security mechanisms is its immutability, which guarantees that once a transaction is entered, it cannot be removed or altered.

Consensus algorithms are the procedures used to arrive at a consensus on transactions. These techniques ensure that every copy of the distributed ledger is identical [35]. Two popular methods are PoW and Proof of Stake (PoS). PoW needs a lot of processing power to validate transactions and create new blocks, whereas PoS chooses validators based on how much Bitcoin they possess. Furthermore, trust in a distributed network is addressed by Practical Byzantine Fault Tolerance (PBFT), which enables the system to operate properly and establish consensus even in the event that some nodes malfunction or behave maliciously.

While not the main emphasis of every industrial blockchain, smart contracts offer the chance to further automate and optimize industrial processes where they are suitable.

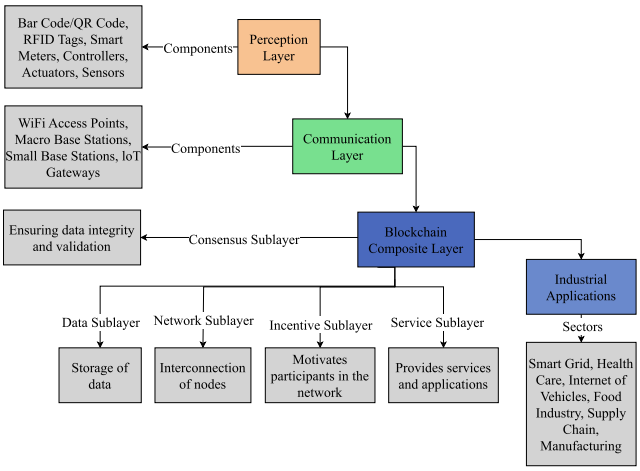


FIGURE 1. Industrial blockchain architecture and layers.

2) LAYERS OF AN INDUSTRIAL BLOCKCHAIN

Different from their public counterparts, industrial blockchain networks are usually permissioned, meaning that only authorized businesses are allowed to participate in the network. The integrity and dependability of information are vital in the industrial, energy, and supply chain management sectors, where this design decision is especially important for handling sensitive data and vital activities.

Fig. 1 provides a graphic representation of the complex multi-layered blockchain architecture that interfaces with the Internet of Things (IoT). By facilitating a safe and smooth information flow between various applications, this

integration makes sure that the digital and physical domains work together harmoniously.

At the base, the Perception Layer collects ambient data using sensors and actuators to act as a link between the physical and digital worlds. Accurate real-time data capturing is the job of this layer; the Communication Layer then securely transmits the data. To ensure data accuracy from the source to the Blockchain Composite Layer, this next layer uses a variety of communication protocols.

Anchoring the whole system, the Blockchain Composite Layer is the central component of the architecture. It is an intricate web of layers, each with a distinct function. The composite layer is where all of the blockchain's essential features come together. It is responsible for controlling data storage and retrieval, monitoring network connections, confirming transactions using strong consensus techniques, and encouraging network involvement.

Finally, the Industrial Applications Layer shows how blockchain is really being used in a variety of businesses. This layer covers the end-use applications, demonstrating the flexibility of the blockchain and its potential to transform industrial processes, whether it is optimizing energy distribution in smart grids, improving supply chain traceability, or guaranteeing the integrity of data in healthcare.

V. PROPOSED ARCHITECTURE

The architecture proposed in this study is designed to integrate blockchain technology within heterogeneous network environments of IIoT, focusing on operational speed, transparency, legal liability, accountability, and privacy. The architecture adopts a hierarchical approach, as depicted in Fig. 2, and introduces ''middle nodes'' to interconnect subnetworks isolated by VLANs. These nodes are pivotal for executing computational tasks and maintaining network efficiency.

A. EXPERIMENTAL RESEARCH METHODOLOGY

This study employs a comprehensive experimental research methodology to rigorously investigate and evaluate the effectiveness of the proposed blockchain-integrated architecture in heterogeneous network environments of Industrial Internet of Things (IIoT).

Experimental Setup: The experimental setup replicates a typical IIoT environment with simulated Local Nodes (LNs), Middle Nodes (MNs), and Full Nodes (FNs) interacting within a virtual network environment. This setup allows testing under various scenarios, including normal operation, high-load conditions, and simulated network attacks.

Data Collection and Analysis: Metrics such as operational speed, network efficiency, and security and privacy measures are systematically collected and analyzed using statistical tools.

Validation of Architecture Components: Each component of the architecture (LNs, MNs, and FNs) is tested in isolation and in combination to validate its functionality and performance, particularly under simulated real-world scenarios.

Limitations and Scope: While this approach provides insights into the architecture's performance, limitations exist due to the simulated nature of the environment. Future work includes testing in a live IIoT environment

B. ARCHITECTURE PRELIMINARIES

The architecture employs a multi-tiered network structure, each tier with distinct roles and responsibilities:

- **Local Nodes (LNs)**: These are devices like sensors and actuators with limited computational capacity. They perform data collection and actuation tasks and rely on Middle Nodes (MNs) for secure communication and data storage. The LNs are designed to operate under low-power conditions and have limited storage capacity, making them reliant on MNs for heavy computational tasks.
- **Middle Nodes (MNs)**: MNs act as facilitators within the network to optimize data processing and storage. They serve as bridges within subnetwork entities and perform the majority of processing operations. Equipped with Hardware Security Modules (HSMs), these nodes ensure the generation of cryptographic keys, maintaining the security and privacy of data transactions. The MNs are strategically placed to balance the load and optimize network traffic.
- **Full Nodes (FNs)**: FNs form the backbone of the blockchain, maintaining consensus and appending validated blocks to the chain. Positioned strategically across the network, FNs execute the Practical Byzantine Fault Tolerance (PBFT) algorithm to maintain consensus and ensure the integrity of the blockchain. The FNs are chosen based on their computational capability and reliability, ensuring robustness in the blockchain network.

C. ARCHITECTURE DESCRIPTION

The architecture facilitates a harmonious collaboration where LNs transmit data to MNs. At the core of our proposed system is a constellation of MNs that not only facilitate computation offloading but also act as local data custodians, significantly improving fault tolerance. The employment of a PBFT consensus mechanism by FNs ensures the reliability and security of transactions across this distributed architecture. FNs and MNs are strategically chosen based on criteria such as computational capability, network connectivity, and trust level of them based on historical performance.

The operation of the architecture may be comprehended in the following steps:

1) **Data Acquisition:** Real-time data capture and forwarding to corresponding MNs is done by LNs.
2) **Secure Storage:** MNs store the incoming data in their own databases. The type of data to be saved can determine whether it should be stored directly or as a

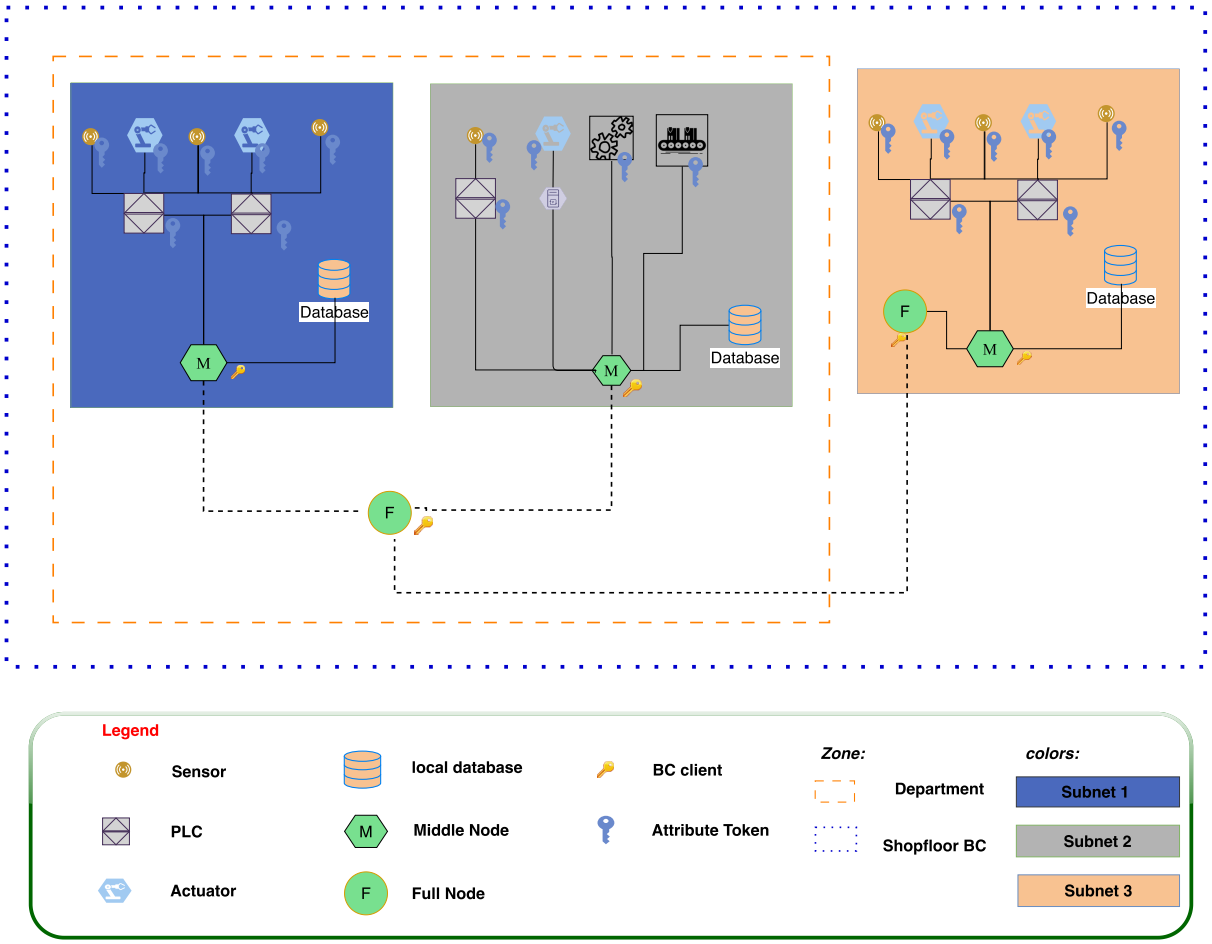


FIGURE 2. Shop floor blockchain architecture.

cryptographic hash, which guarantees data secrecy and integrity. Examples of this type of data include machine operational hours and threshold-based indicators like temperature.

3) **Transaction Lifecycle:** To ensure redundancy and data availability, middle nodes synthesize transactions from this data, sign them cryptographically, and then propagate them to other MNs inside the subnetwork.
4) **Candidate Block Formation:** The transactions are compiled by MNs in a subnetwork, creating candidate blocks that are prepared for network-wide verification.
5) **Network-wide Verification:** The candidate blocks go through PBFT verification after being broadcast to all FNs, ensuring consensus and preventing any data manipulation.
6) **Blockchain Append:** FNs combine the candidate blocks after verification and add them to the blockchain as new blocks, which makes the data permanent and unchangeable.

Even the LNs, such as simple sensors, may transfer data safely and reliably because of this complex design. The MNs in between serve as buffers, which are especially important when the network is unstable. They guarantee that data is never lost and is constantly prepared for blockchain integration.

D. ARCHITECTURE WORKFLOW

Our proposed architecture has been designed considering the privacy of the participants. Privacy within the network is ensured through the utilized attribute verification protocol that operates in conjunction with the blockchain in 4 phases: 1) Setup Phase, 2) Registration Phase, 3) Generation Phase, and 4) Validation Phase as described in the next sections. MNs handle the encryption of data using keys generated by Hardware Security Module (HSM)s, ensuring secure transaction initiation. LNs participate by providing hashed data to MNs, adding another layer of privacy. But before participating in the subnetwork, it is needed to pass the preregistration step.

1) SETUP PHASE

The setup phase is a very critical pre-registration step in network configuration, during which an IIoT node is identified and integrated into the network. In this phase, and

during registering a new node, the responsible LN assigns a *unique identifier* to guarantee its unique location inside the network. This is a dual-faced unique ID (ID_n) derived from the node's serial number (Sn) and MAC address (MAC) as in Equation 1. Whereas the MAC address is unique and identifiable in the digital world, the serial number is like an unchangeable imprint from genesis.

$$ID_n = H(Sn \parallel MAC) \tag{1}$$

Here, H represents a cryptographic hash function and $\parallel$ denotes concatenation. MAC, inherently unique and recognizable in the digital realm, serves as a reliable hardware-based identifier. In contrast, Sn acts like an immutable tag assigned at the time of manufacture. This dual-component approach to node identification enhances security, as it couples a physically unalterable attribute Sn with a digitally unique identifier MAC. The setup phase (see Algorithm 1)

Algorithm 1 Setup Phase

```
function SetupPhase(node)
    ID_n ← HashFunction(node.Sn ‖ node.MAC)
    node.unique_ID ← ID_n
    return node
end function
```

is rigorously conducted only once for each node to maintain the integrity of these identifiers. The MAC and Sn data is retrieved from the newly joined node during this phase during the identifier generation process. Since the generated identifiers are unique and immutable, they play a pivotal role in the network's overall security architecture. These components work together to provide a strong identification system, which is essential for safe and effective network operations.

2) REGISTRATION PHASE

Following the identity assignment in the setup phase, nodes are further characterized by a set of configurable attributes. These attributes play a crucial role in dictating their operational behavior and interaction within the network. Without loss of generality, we discuss four primary attributes as follows:

- **Logical Network Sector (SEC)**: This attribute defines the operational scope of a node within the network topology. It determines the node's functional area and its interaction with other segments of the network, aiding in effective network segmentation and management.
- **Installer Signature (INS)**: This records the entity responsible for commissioning and configuring the node. The INS is pivotal for traceability and accountability, ensuring that any modifications or installations are reliably logged.
- **Power Consumption (POW)**: This metric reflects the energy usage of the Local Node (LN), which is essential for evaluating the network's sustainability and efficiency. Monitoring POW helps in optimizing energy consumption and managing the environmental footprint of network operations.
- **Transmission Pattern (TRA)**: Describes the data communication behavior of the node, which is crucial for managing network traffic, load balancing, and optimizing bandwidth usage. The TRA helps in predicting and shaping the network's data flow, enhancing overall performance.

It is noteworthy that these attributes are not static. They can be updated or expanded upon during the lifecycle of the system by the Main Nodes (MNs). This dynamic adaptability is crucial in a network environment that may evolve or require adjustments in response to new operational demands or technological advancements. We have adopted the *n-out-of-n* verification mode, as described in Section IV-A. The process of validation and tokenization of nodes based on their attributes is described as follows.

1) **Attribute Verification Function:** we can represent the verification process of a node's attributes by the Main Nodes (MNs) as follows:

$$V_{attr}(LN) = \begin{cases} 1 & \text{if } SEC, INS, POW \text{ is valid} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

where $V_{attr}(LN)$ represents the verification function for the LN attributes. The function returns 1 if all the attributes (SEC, INS, POW, TRA) are successfully verified by the MNs, and 0 otherwise.

2) **Token Issuance Function:** After the verification, tokens are issued to certify the readiness of the LNs for network participation.

$$T_{issue}(LN) = \begin{cases} \text{Token} & \text{if } V_{attr}(LN) = 1 \\ \text{No Token} & \text{if } V_{attr}(LN) = 0 \end{cases} \tag{3}$$

In equation 3, $T_{issue}(LN)$ represents the token issuance function. A token is issued if the verification function $V_{attr}(LN)$ returns 1, indicating successful verification of the node's attributes.

3) **Dynamic Attribute Update Function:** we can model the ability of MNs to update the attributes of LNs over time:

$$U_{attr}(LN, new\_attr) = \begin{cases} \text{Updated Attr} & \text{if update} \\ \text{Unchanged Attr} & \text{otherwise} \end{cases} \tag{4}$$

Here, $U_{attr}(LN, new\_attr)$ denotes the attribute update function, where LN, new_attr represents the new attributes to be assigned to the LN. This function reflects the dynamic adaptability of the network's attributes.

Moreover, these attributes, once verified and tokenized, enable more granular control over the network. They allow network administrators to implement policies based on specific node characteristics, enhance security protocols, and

optimize network performance. The registration phase (see Algorithm 2), therefore, is not just a procedural step but a critical component in establishing a robust, efficient, and secure network infrastructure.

Algorithm 2 Registration Phase

```
function RegistrationPhase(node)
    Define node.attributes ← {"SEC": None, "INS": None, "POW": None, "TRA": None}
    UpdateNodeAttributes(node)
    return node
end function
function UpdateNodeAttributes(node)        ▷ Update attributes based on network policies
end function
```

3) GENERATION PHASE

The Generation Phase is a pivotal process in the lifecycle of blockchain data management. It encompasses the creation and preparation of data for entry into the blockchain. This phase consists of several sequential steps to ensure data integrity and security, as described below:

1) **Data Generation**: Initially, raw data is generated by LNs. This data could represent transactions, sensor outputs, user actions, or any relevant information that needs to be recorded on the blockchain.

$$D = \text{GenerateData}(\text{Raw Inputs}) \tag{5}$$

where D denotes the generated data from raw inputs.

2) **Data Digest Creation**: Each piece of data D is then processed to create a cryptographic hash digest. This digest serves as a unique fingerprint of the data.

$$H(D) = \text{Hash}(D) \tag{6}$$

Here, $H(D)$ is the hash digest of data D.

3) **Attribute Digest Generation**: Concurrently, all relevant attributes of the data are hashed to ensure that every characteristic is accounted for and secured.

$$H(A) = \text{Hash}(A_1, A_2, \ldots, A_n) \tag{7}$$

With $H(A)$ representing the combined hash of attributes $A_1, A_2, \ldots, A_n$.

4) **Double Hash Formation**: To further enhance security, a double hash is formed, which is the hash of the hash digest and the attribute digest.

$$H_2(D, A) = \text{Hash}(H(D) \parallel H(A)) \tag{8}$$

$H_2(D, A)$ symbolizes the double hash, where $||$ denotes concatenation.

5) **Commit to Public Blockchain**: The final step is committing the double hash to the public blockchain. This action immutably records the data and its attributes, ensuring traceability and verifiability.

$$B = \text{CommitToBlockchain}(H_2(D, A)) \tag{9}$$

where B is the blockchain record containing the double hash $H_2(D, A)$.

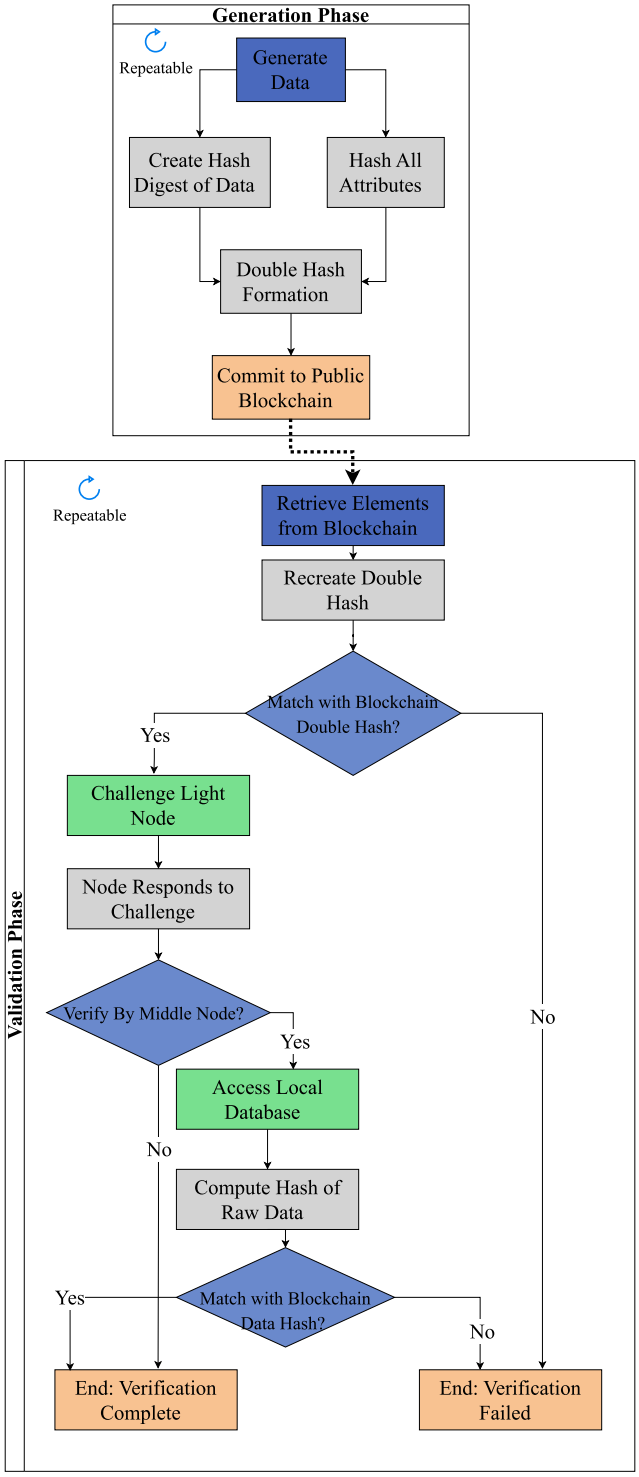


FIGURE 3. Generation and validation phases.

Each step in the Generation Phase (see Algorithm 3) is designed to be repeatable and scalable, ensuring that as data generation increases, the system can handle the additional

load without compromising on security or integrity. The process also emphasizes the importance of repeatability, allowing for consistent data generation and recording in an efficient and secure manner. By Generation Phase, the

Algorithm 3 Generation Phase

```
function GenerationPhase(LN)
    D ← GenerateData(LN.raw_inputs)
    hash_digest ← HashFunction(D)
    attribute_hash ← HashFunction(LN.attributes)
    double_hash ← HashFunction(hash_digest, attribute_hash)
    B ← CommitToBlockchain(double_hash)
    return B
end function
```

blockchain system fortifies the data against tampering and unauthorized alterations, thus upholding the principles of decentralization and trust that are central to blockchain technology.

4) VALIDATION PHASE

The Validation Phase in a blockchain-based network is a critical multi-tiered process that ensures data integrity, privacy, and compliance with network protocols. This phase involves several key steps:

1) **Initial Verification by MNs:** The MNs first verify LNs properties against their pre-registered attributes. This verification is essential to ensure that each LN adheres to the network's standards and policies. The process can be represented as follows:

$$V_{MN}(LN) = \begin{cases} 1 & \text{match pre-registered values} \\ 0 & \text{otherwise} \end{cases} \tag{10}$$

where $V_{MN}(LN)$ is the validation function performed by the MNs on the LNs.

2) **Consensus Process by FNs:** FNs, utilizing the PBFT consensus mechanism, further scrutinize the blocks containing encrypted data. This step is crucial to maintain the integrity and trustworthiness of the data in the blockchain. The consensus can be represented as:

$$C_{PBFT}(Block) = \frac{\sum_{i=1}^{n} V_{FN_i}(Block)}{n} \tag{11}$$

where $C_{PBFT}(Block)$ is the consensus function, $V_{FN_i}(Block)$ is the validation function performed by each FN on the block, and n is the total number of FNs participating in the consensus process.

3) **Random Audits for Data Integrity and Privacy:** Post-verification, independent auditors conduct random checks to assure data integrity and validate the effectiveness of privacy-preserving measures (cf. Fig. 3). This layer adds an additional level of security and compliance verification.

By integrating privacy protocols with an efficient blockchain architecture, the system achieves a robust privacy framework that does not compromise the network's speed and efficiency. This balanced approach is critical for blockchain adoption in sensitive and high-stakes environments, such as IIoT networks, where data privacy and rapid processing are paramount. The Validation Phase algorithm (see Algorithm 4) is defined as:

Algorithm 4 Validation Phase

```
function ValidationPhase(LN, MNs, FNs, auditors)
    if not Verify(MNs, LN) then
        return False
    end if
    block ← LN.generate_block()
    if not PBFTConsensus(FNs, block) then
        return False
    end if
    if not RandomAudit(auditors, LN) then
        return False
    end if
    return True
end function
function PBFTConsensus(FNs, block)        ▷ Implement PBFT consensus mechanism
    return True or False
end function
```

VI. ANALYSIS

The effectiveness, security, and performance of the proposed architecture were evaluated using an experimental research method. In this section, the extensive analysis of the proposed architecture have been provided.

A. IMPLEMENTATION AND EVALUATION OVERVIEW

The implementation and evaluation involved setting up a test environment with one middle node and seven local nodes, each equipped with a 1.8 GHz processing unit, as illustrated in Figure 4. The implementation utilized the Charm framework [36] for the attribute verification protocol. The evaluation focused on the registration, generation, and validation phases, with an emphasis on measuring efficiency under varying conditions and examining the resilience of the system against potential security threats. As mentioned earlier, during the registration phase we assumed that a single MN is responsible for the four available attributes in the system, namely SEC, INS, POW, and TRA. Therefore, each of the LNs will get four tokens from the MN, to be used later during the validation phase. The attributes have been set as follows:

- Logical Network Sector (SEC=xxx)
- Installer Signature (SEC=xxx,INS=xxx)
- Power Consumption (SEC=xxx,POW=xxx)
- Transmission Pattern (SEC=xxx,TRA=xxx)

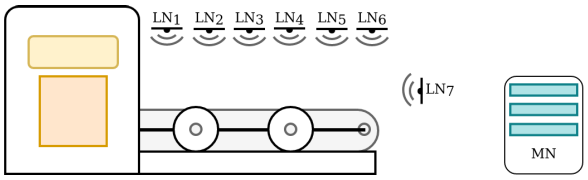


FIGURE 4. Implementation of the proposed framework.

TABLE 2. Implementation time.

Phases	No. of devices	Time (ms)
Registration	7 LNs	138
Generation	1 LN	0.65
Validation - challenge	1 LN	38
Validation - response	1 LN	29

B. IMPLEMENTATION DETAILS

The implementation specifics are as follows:

- Attribute Settings: Attributes for the nodes were set as Logical Network Sector (SEC), Installer Signature (INS), Power Consumption (POW), and Transmission Pattern (TRA).
- Hashing Process: During the generation, the SHA-1 hash function has been utilized.
- Token Issuance in Registration Phase: In the registration phase, each Local Node (LN) received four tokens from the Middle Node (MN), corresponding to the four attributes (SEC, INS, POW, and TRA), which were later used during the validation phase.
- Performance Metrics: Key metrics, such as time taken for registration, generation, and validation phases, were measured to assess the efficiency of the system (Table 2).

C. SECURITY ANALYSIS

Our approach addresses privacy leakage, security flaws, and resource limitations of IIoT devices. The architecture is designed to withstand a range of adversarial assaults, such as network intrusion, data tampering, and unauthorized access. Advanced encryption techniques were used to protect user identities and transaction data. The system's design inherently reduces the risk of data breaches, as it does not require the storage of all transaction data. Strong key management techniques and smart contract security measures further reinforce the framework.

The resilience of the system against adversarial threats includes protections against passive assaults aimed at data interception and active attacks like Denial of Service (DoS). The architecture anticipates such attacks and implements redundancy and resilience techniques to maintain network functionality even in the event of intermediate node failures.

D. PERFORMANCE ANALYSIS

Consensus mechanisms play a crucial role in balancing transaction speed, energy consumption, and system security in IIoT applications. We conducted a comparative study of Proof of Work (PoW) [37], Proof of Stake (PoS) [38], and Practical Byzantine Fault Tolerance (PBFT) [39]. Our proposed system, optimized for IIoT contexts, redefines the role of resource-limited local nodes, allowing them to safely generate data while not being directly involved in the consensus process.

TABLE 3. Comparative analysis of consensus mechanisms.

Mechanism	Throughput	Block Time	Energy	Security
PoW	Low	10 min	High	Very High
PoS	Med-High	Var	Low	Med-High
PBFT	High	Secs	Mod	Low-High
Our Proposal	High	Secs	Mod	High / ABS

By redefining the function of resource-limited local nodes, our proposed system addresses these issues and improves efficiency (cf. Table. 3). These nodes safely generate data, which enhances network security even if they are not directly involved in the consensus process. The full nodes are responsible for creating blocks by consensus; they include the safely stored information from the local nodes into the candidate blocks. Thus, the suggested system can both accommodate the resource constraints seen in IIoT contexts and preserve the high throughput and low latency features of PBFT.

The performance of our proposed architecture was thoroughly analyzed, with particular emphasis on the consensus mechanisms employed. While our approach utilizes the Practical Byzantine Fault Tolerance (PBFT) model, it's tailored to enhance the process of candidate block formation by Middle Nodes (MNs). In this refined model, MNs preprocess higher-level information, which is then consolidated by Full Nodes (FNs) during the block creation process.

This modification ensures that the information incorporated into candidate blocks by FNs has already undergone a preliminary layer of verification and secure storage by MNs, thereby making the process both more secure and efficient. Such a design is particularly advantageous in IIoT contexts, where resource constraints are common. It maintains the high throughput and low latency characteristics of traditional PBFT, yet optimizes it for the specific demands and limitations of IIoT environments. This nuanced approach to consensus ensures swift and secure transaction validation, aligning with the operational needs of IIoT systems.

In summary, the analysis section provides a comprehensive evaluation of the proposed blockchain-based IIoT architecture. It details the implementation setup, offers a thorough security analysis, and presents an in-depth performance analysis, thereby convincingly demonstrating the system's effectiveness, security, and efficiency.

VII. CASE STUDY: IMPLEMENTING BLOCKCHAIN ON A HYDRAULIC MACHINE SHOP FLOOR

This case study looks at how the suggested blockchain architecture might work in an actual setting, i.e., a shop

floor with large hydraulic machinery. Because hydraulic machines can provide enormous quantities of power for diverse operations, they are indispensable in many industrial applications. They do, however, also have to deal with issues like operating efficiency, energy usage optimization, and maintenance schedule.

A. PROBLEM STATEMENT

The absence of a strong data management system and unplanned maintenance caused a large amount of downtime for the chosen shop floor. The unpredictability of equipment breakdowns resulted in higher expenses and lower productivity. To improve operational efficiency and predictive maintenance capabilities, a system that could deliver secure, immutable, and real-time data was obviously needed.

B. IMPLEMENTATION OF PROPOSED ARCHITECTURE

There was no interruption to the shop floor's current infrastructure throughout the integration of the blockchain-based architecture. In order to monitor performance metrics, middle nodes were created to act as a link between the full nodes and the local nodes that were integrated into the hydraulic equipment. A new degree of communication between the machines and the management system was made possible by this network arrangement. Every hydraulic device had a special identification that connected to its local node within the blockchain. This identification guaranteed traceability and security in data transactions. Each node had parameters pre-registered for things like sector code, installer signature, power consumption, and transmission pattern, which helped to tailor the network to the unique requirements of a high-power-demand environment. Pressure, temperature, and fluid level data were gathered by the local nodes; these characteristics were essential for the hydraulic machinery to function. After that, the intermediary nodes safely received the data, processed it at first, and temporarily stored it. Middle nodes combined the data into transactions, which were subsequently signed and sent to complete nodes. In order to reach a consensus, the full nodes carried out the PBFT protocol. They then added the validated transactions to the blockchain, guaranteeing that the data was unchangeable and easily accessible for examination.

VIII. CONCLUSION

In this paper we proposed a privacy preserving approach to secure the shop floor auditing process, utilizing the attribute verification protocol as the main building block and the Blockchain technology. The proposed approach provides two main services: First, it provides a mechanism for an auditor to verify that the stored data in the Blockchain has been generated by a valid IIoT node in the sytem. Secondly, it allows an auditor to verify a set of given data has been previously generated by a specific IIoT node withing the system. The provided case study shows how the proposed approach can be implemented on an hydraulic machine shop floor to improve the operational efficiency and security.

The proposed approach exhibits several open problems. As the proposed approach involves heavy computations that requires relatively powerful devices, the future research directions include proposing approaches that can be directly implemented on resource-constrained devices. Additionally, the implementation of the adopted attribute verification protocol on IIoT devices can be further analyzed.

REFERENCES

[1] X. Yao and Y. Lin, "Emerging manufacturing paradigm shifts for the incoming industrial revolution," *Int. J. Adv. Manuf. Technol.*, vol. 85, nos. 5–8, pp. 1665–1676, Jul. 2016.

[2] T. Zheng, M. Ardolino, A. Bacchetti, and M. Perona, "The applications of industry 4.0 technologies in manufacturing context: A systematic literature review," *Int. J. Prod. Res.*, vol. 59, no. 6, pp. 1922–1954, Mar. 2021.

[3] B. Yu, J. Wright, S. Nepal, L. Zhu, J. Liu, and R. Ranjan, "IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain," *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 12–23, Aug. 2018.

[4] G. Culot, G. Orzes, M. Sartor, and G. Nassimbeni, "The future of manufacturing: A delphi-based scenario analysis on Industry 4.0," *Technol. Forecasting Social Change*, vol. 157, Aug. 2020, Art. no. 120092.

[5] T. Pulikottil, L. A. Estrada-Jimenez, J. J. P. Abadía, A. Carrera-Rivera, A. Torayev, H. U. Rehman, F. Mo, S. Nikghadam-Hojjati, and J. Barata, "Big data life cycle in shop-floor–trends and challenges," *IEEE Access*, vol. 11, pp. 30008–30026, 2023.

[6] A. Vatankhah Barenji, Z. Li, and W. M. Wang, "Blockchain cloud manufacturing: Shop floor and machine level," in *Proc. Eur. Conf. Smart Objects, Syst. Technol.*, Jun. 2018, pp. 1–6.

[7] A. Bahga, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, Oct. 2016.

[8] J. Stodt, D. Schönle, C. Reich, F. Ghovanlooy Ghajar, D. Welte, and A. Sikora, "Security audit of a blockchain-based industrial application platform," *Algorithms*, vol. 14, no. 4, p. 121, Apr. 2021.

[9] D. Mishra, P. Singh, and N. Singh, "Role of blockchain in achieving solutions in ambiguous supply chain operations," in *Blockchain Volatile-Uncertain-Complex-Ambiguous World*. Amsterdam, The Netherlands: Elsevier, 2023, pp. 57–73.

[10] J. E. Kasten, "Engineering and manufacturing on the blockchain: A systematic review," *IEEE Eng. Manag. Rev.*, vol. 48, no. 1, pp. 31–47, 1st Quart., 2020.

[11] J. Wan, J. Li, M. Imran, D. Li, and Fazal-E-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3652–3660, Jun. 2019.

[12] K. Arakadakis, P. Charalampidis, A. Makrogiannakis, and A. Fragkiadakis, "Firmware over-the-air programming techniques for IoT networks—A survey," *ACM Comput. Surveys*, vol. 54, no. 9, pp. 1–36, Oct. 2021, doi: 10.1145/3472292.

[13] S. Vairavasundaram, K. Kotecha, L. Ravi, G. Selvachandran, and A. Abraham, "Blockchain-based trust mechanism for digital twin empowered industrial Internet of Things," *Future Gener. Comput. Syst.*, vol. 141, pp. 16–27, Apr. 2023.

[14] L. Yang, W. Zou, J. Wang, and Z. Tang, "EdgeShare: A blockchain-based edge data-sharing framework for industrial Internet of Things," *Neurocomputing*, vol. 485, pp. 219–232, May 2022.

[15] F. Stodt, C. Reich, A. Sikora, and D. Welte, "Trust management system for hybrid industrial blockchains," in *Proc. IEEE 21st Int. Conf. Ind. Informat. (INDIN)*, Jul. 2023, pp. 1–6.

[16] E. Bandara, D. Tosh, P. Foytik, S. Shetty, N. Ranasinghe, and K. De Zoysa, "Tikiri—Towards a lightweight blockchain for IoT," *Future Gener. Comput. Syst.*, vol. 119, pp. 154–165, Jun. 2021.

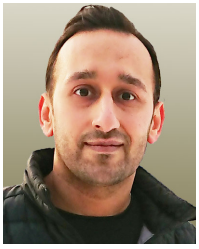
[17] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: A lightweight blockchain system for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3571–3581, Jun. 2019, doi: 10.1109/TII.2019.2904049.

[18] S. Khan, W.-K. Lee, and S. O. Hwang, "AEchain: A lightweight blockchain for IoT applications," *IEEE Consum. Electron. Mag.*, vol. 11, no. 2, pp. 64–76, Mar. 2022.

[19] D. Na and S. Park, "Fusion chain: A decentralized lightweight blockchain for IoT security and privacy," *Electronics*, vol. 10, no. 4, p. 391, Feb. 2021.

[20] S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, and J. C.-W. Lin, "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems," *J. Cloud Comput.*, vol. 12, no. 1, p. 38, Mar. 2023, doi: 10.1186/s13677-023-00412-y.
[21] M. Allouche, T. Frikha, M. Mitrea, G. Memmi, and F. Chaabane, "Lightweight blockchain processing. Case study: Scanned document tracking on Tezos blockchain," *Appl. Sci.*, vol. 11, no. 15, p. 7169, Aug. 2021, doi: 10.3390/app11157169.
[22] G. Rathee, S. D. Gupta, and N. Jaglan, "A review on blockchain and its necessitate in industrial IoT," in *Proc. Innov. Comput. Sci. Eng. 7th (ICICSE)*, 2020, pp. 207–214.
[23] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[24] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *Proc. IEEE World Congr. Services*, Jun. 2017, pp. 90–93.
[25] H. Derhamy, J. Eliasson, and J. Delsing, "IoT interoperability—On-demand and low latency transparent multiprotocol translator," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1754–1763, Oct. 2017, doi: 10.1109/JIOT.2017.2697718.
[26] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[27] N. Teslya and I. Ryabchikov, "Blockchain platforms overview for industrial IoT purposes," in *Proc. 22nd Conf. Open Innov. Assoc. (FRUCT)*, May 2018, pp. 250–256.
[28] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Performance optimization for blockchain-enabled Industrial Internet of Things (IIoT) systems: A deep reinforcement learning approach," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3559–3570, Jun. 2019.
[29] T. B. D. Silva, E. S. D. Morais, L. F. F. D. Almeida, R. D. R. Righi, and A. M. Alberti, "Blockchain and industry 4.0: Overview, convergence, and analysis," *Blockchain Technol. Ind. 4.0 Secure, Decentralized, Distrib. Trusted Ind. Environ.*, pp. 27–58, Jan. 2020, doi: 10.1007/978-981-15-1137-0_2.
[30] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.
[31] M. B. M. Kamel, Y. Yan, P. Ligeti, and C. Reich, "Attribute verifier for Internet of Things," in *Proc. 32nd Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2022, pp. 1–3.
[32] M. B. Kamel, P. Ligeti, and C. Reich, "D3vn: Decentralized abe-based distributed data validation network," in *Proc. 7th Int. Congr. Inf. Commun. Technol. ICICT*, vol. 4. Springer, 2022, pp. 653–661.
[33] M. B. Kamel, W. D. Abdullah, A. K. Hamoud, D. C. Valadares, A. Shareiyat, and P. Ligeti, "3l-aodv: Three layer security protocol for grayhole attack mitigation in manet," in *Proc. Int. Congr. Inf. Commun. Technol.* Springer, 2023, pp. 813–823.
[34] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Mar. 2017, doi: 10.1007/s12599-017-0467-3.
[35] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst. Man, Cybern. (SMC)*, Oct. 2017, pp. 2567–2572.
[36] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, "Charm: A framework for rapidly prototyping cryptosystems," *J. Cryptograph. Eng.*, vol. 3, no. 2, pp. 111–128, 2013.
[37] J. Yun, Y. Goh, and J.-M. Chung, "Analysis of mining performance based on mathmatical approach of PoW," in *Proc. Int. Conf. Electron., Inf., Commun. (ICEIC)*, 2019, pp. 1–2.
[38] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of PoW, PoS and DAG based blockchains," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 480–485, Nov. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864819301476
[39] H. Sukhwani, J. Martínez, X. Chang, K. Trivedi, and A. Rindos, "Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric)," in *Proc. IEEE 36th Symp. Reliable Distrib. Systems. (SRDS)*, Sep. 2017, pp. 253–255.

FATEMEH STODT (Member, IEEE) is currently pursuing the joint Ph.D. degree with the University of Strasburg and Furtwangen University, with a focus on blockchain technology, cybersecurity, and industrial Internet of Things (IoT). She is a Researcher with the University of Strasburg and Furtwangen University.



MOHAMMED B. M. KAMEL received the Ph.D. degree in computer science from Eötvös Loránd University and Furtwangen University. He is currently a Senior Researcher and a Certified Cybersecurity Consultant. He was a part of several projects as a cybersecurity researcher that have been accomplished. His research interest includes designing distributed secure protocols. He was a Gold and Bronze Award Winner from EIT, a body of the European Union.

CHRISTOPH REICH (Member, IEEE) received the Ph.D. degree in computer science from De Montfort University, U.K. He is currently a Professor with Furtwangen University and the Head of the Institute of Data Science, Cloud Computing, and IT Security (IDACUS), Furtwangen University. He has authored more than 180 research articles. His research interests include machine learning, distributed systems, and cybersecurity.

FABRICE THEOLEYRE (Senior Member, IEEE) received the Ph.D. degree in computer science from INSA, Lyon, France, in 2006. He is currently a Senior Researcher with CNRS. After having two years of experience with the Grenoble Informatics Laboratory, France, he has been a part of the ICube Laboratory, Strasbourg, France, since 2009. He held several visiting positions with the University of Waterloo, Canada; Inje University, South Korea; and Jiaotong University, China. His research interests include distributed algorithms and experimental design for the Internet of Things.

PETER LIGETI received the Ph.D. degree in mathematics and computer science from Eötvös Loránd University (ELTE), in 2008. He is currently a Habilitated Associate Professor with the Department of Computer Algebra, ELTE. He has authored more than 50 research articles and participated in more than ten research projects. His research interests include combinatorics and cryptography, especially combinatorial optimization, secret sharing, and secure communication protocols.