Digital Communications and Networks xxx (xxxx) xxx

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Lightweight consensus mechanisms in the Internet of Blockchained Things: Thorough analysis and research directions ☆

Somia Sahraoui [a], *, Abdelmalik Bachir [b]

[a] RLP Laboratory, Computer Science Department, University Mohamed Khider of Biskra, 07000, Algeria
[b] National Higher School of Artificial Intelligence, Algiers, 01600, Algeria

ARTICLE INFO

Keywords:
Blockchain
Internet of Things
Lightweight consensus

ABSTRACT

The Internet of Things (IoT) has gained substantial attention in both academic research and real-world applications. The proliferation of interconnected devices across various domains promises to deliver intelligent and advanced services. However, this rapid expansion also heightens the vulnerability of the IoT ecosystem to security threats. Consequently, innovative solutions capable of effectively mitigating risks while accommodating the unique constraints of IoT environments are urgently needed. Recently, the convergence of Blockchain technology and IoT has introduced a decentralized and robust framework for securing data and interactions, commonly referred to as the Internet of Blockchained Things (IoBT). Extensive research efforts have been devoted to adapting Blockchain technology to meet the specific requirements of IoT deployments. Within this context, consensus algorithms play a critical role in assessing the feasibility of integrating Blockchain into IoT ecosystems. The adoption of efficient and lightweight consensus mechanisms for block validation has become increasingly essential. This paper presents a comprehensive examination of lightweight, constraint-aware consensus algorithms tailored for IoBT. The study categorizes these consensus mechanisms based on their core operations, the security of the block validation process, the incorporation of AI techniques, and the specific applications they are designed to support.

1. Introduction

Nowadays, Artificial Intelligence, Internet of Things and Blockchain are considered as driving actors that are revolutionizing the technological landscape [1]. While the concept of connecting everything to a global network (commonly referred to as IoT) is well understood, and its benefits—such as enhanced human-context interactions, improved quality of service, and enriched user experiences—are becoming increasingly tangible, significant security risks persist. These risks pose a major challenge to the successful deployment of IoT and must be addressed effectively. The primary issue lies in the reliance on traditional countermeasures, which are generally based on centralized architectures and lack the robustness required for modern systems [2]. Indeed, securing widely distributed networks, like IoT, using centralized mechanisms has revealed several limitations, including weak fault tolerance and the vulnerability of single points of failure to potential security breaches.

Recently, serious research efforts have been carried out in order to transform the classical Internet services and applications from centralized to distributed models [3], [4]. In this transformative context, Blockchain has emerged as a groundbreaking technology, revolutionizing the way data and transactions are managed. This evolution extends to security management, removing the need to depend on centralized third parties whose trustworthiness must be pre-established. Blockchain technology [5] operates as a large distributed database, designed to store vast amounts of data securely. It integrates various advanced technologies, including asymmetric cryptography, hashing functions, and distributed algorithms for block validation. In recent years, numerous research studies have explored the applicability of Blockchain technology in distributed environments beyond its financial roots. One prominent area of interest is the Internet of Things, where Blockchain could play a transformative role. However, the limited capabilities and constrained resources of IoT devices present significant challenges, as Blockchain solutions are typically resource-intensive. Consequently, Blockchain functionalities must account for IoT's limitations to enable the successful integration of Blockchain into IoT infrastructures.

☆ Peer review under the responsibility of the Chongqing University of Posts and Telecommunications.

* Corresponding author.

E-mail addresses: s.sahraoui@univ-biskra.dz (S. Sahraoui), abdelmalik.bachir@ensia.edu.dz (A. Bachir).

https://doi.org/10.1016/j.dcan.2024.12.007
Received 8 August 2023; Received in revised form 21 December 2024; Accepted 24 December 2024

Available online 6 January 2025

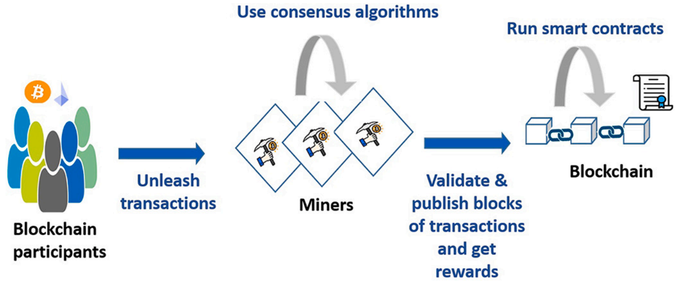

Fig. 1. Blockchain components.

In this paper, we are interested in the consensus algorithms proposed for the IoBT. Consensus algorithms are distributed mechanisms that are used for Block validation but they are known to be greedy in terms of resource consumption. In this context, we are particularly interested in lightweight consensus algorithms, exploring their types, operations, security considerations and smartness features. Additionally, we investigate lightweight application-driven consensus mechanisms. Each class of consensus mechanisms is analyzed, and the study concludes with a comparative table that highlights the advantages and disadvantages of the examined protocols. While numerous survey papers have addressed IoT-specific consensus mechanisms [6], [7], [8], [9], this is the first review to offer a comprehensive study and classification of lightweight consensus mechanisms designed for Blockchain-enabled IoT systems.

The rest of the paper is organized as follows: Section 2 presents an overview on Blockchain technology, its components and types. Section 3 highlights the concept of Internet of Blockchained Things and its related aspects. Section 4 is devoted to an in-depth study of the lightweight consensus mechanisms proposed for the Internet of Blockchained Things. Finally, section 5 concludes the study and outlines the open issues, as well as the potential research directions for developing consensus mechanisms in Blockchain-enabled IoT systems.

2. Overview on Blockchain technology

This section highlights the key aspects of blockchain technology. It begins with an overview of the anatomy of blockchain and then explores the various types of blockchain platforms.

2.1. Anatomy of Blockchain technology

Blockchain technology is a distributed ledger system that consists of several key components [10], including the chain of blocks, the pool of miners, the consensus algorithm, and optionally, smart contracts. Fig. 1 illustrates the structure and components of Blockchain technology.

The client (or participant) in a Blockchain system can initiate one or more transactions, typically representing the transfer of value between themselves and other participants within the same Blockchain platform. More broadly, transactions are designed to model interactions among Blockchain participants, which is a crucial feature that enables the integration of this technology with the Internet of Things.

Transactions cannot be directly stored on the Blockchain as they first need to be collected and validated. The entities responsible for validating blocks before they are appended to an existing Blockchain are known as miners or validators. The validation process depends on the consensus algorithm in use, which defines the rules determining how a miner establishes the validity of a block.

In addition to transactions, blocks contain additional information to ensure their security and facilitate their placement within the chain. Each block includes the hash value of the preceding block (except the first block, known as the genesis block) and its own hash value, which is also incorporated into the subsequent block. The hash value is computed over the entire content of the block, including the hash of the previous block. This mechanism guarantees the immutability of the Blockchain, as any modification to a block's content will automatically be detected in the altered block and all subsequent blocks. This is because the hash value generated for the modified block will no longer match.

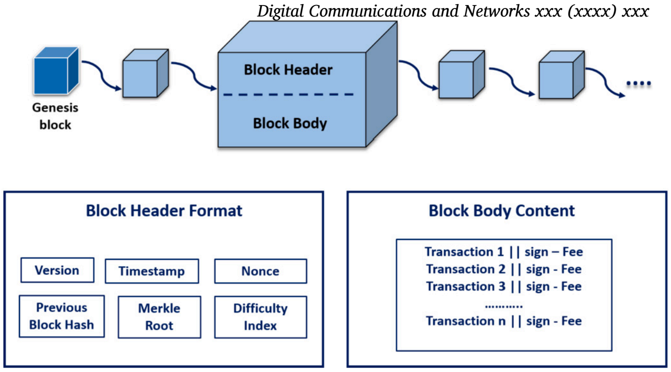

Fig. 2. Block structure.

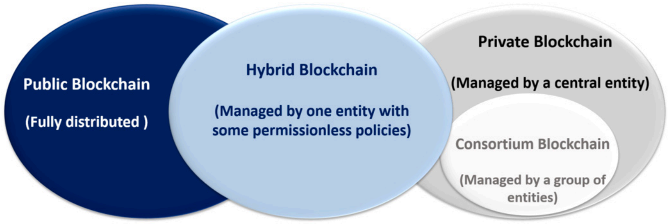
Public Blockchain
(Fully distributed)
Hybrid Blockchain
(Managed by one entity with some permissionless policies)
Private Blockchain
(Managed by a central entity)
Consortium Blockchain
(Managed by a group of entities)

Fig. 3. Types of Blockchains.

In terms of security, Blockchain technology ensures data integrity through the block hashing mechanism and employs asymmetric cryptography for transaction signing and encryption. The detailed block structure is illustrated in Fig. 2.

Block miners are entities that compete to generate new approved blocks of transactions. In fact, mining operations are time- and power-consuming tasks, but they can be highly profitable. Miners are rewarded for every successful block mined, with the reward value typically linked to the transaction fee, commonly known as the gas fee. The consensus algorithm is responsible for orchestrating the miners in a distributed manner. For example, miners independently attempt to solve complex cryptographic puzzles, or they may simply need to meet predefined criteria, such as holding a certain amount of tokens. In either case, the winning miner adds the new block to the blockchain and earns the associated gas fees.

Smart contracts [11] are a crucial software component of Blockchain technology. First introduced by Ethereum [12], they are programs written in the Solidity programming language and stored on the Blockchain. Smart contracts are specifically designed to be condition-oriented; that is, they are automatically executed once predefined conditions are met, without the need for third-party intervention. Additionally, they can be leveraged for purposes such as authorization and security management.

2.2. Types of Blockchain technology

Blockchain solutions can be classified as public, private, consortium, or hybrid [13] (Fig. 3). The core differences between these types lie in how the Blockchain is managed, how participants access and utilize its data, and the specific security considerations associated with each category.

- **Public Blockchain:** Also known as a permissionless Blockchain, a public Blockchain is fully open to any participant and entirely decentralized. All nodes have equal rights to mine and add new blocks of transactions. Bitcoin [14] and Ethereum [15] are among the most prominent examples of public Blockchain platforms. In these systems, participants do not require prior permission to mine cryptocurrency and earn fees for their computational contributions.

- **Private Blockchain:** Private Blockchains [16] are often adopted by companies seeking complete control over their Blockchain-based solutions. These organizations can define specific permissions to restrict access and participation in the consensus process. Permissioned or private Blockchains are inherently more secure, eliminating the need for highly complex cryptographic computations during block validation phases.
- **Consortium Blockchain:** Consortium blockchains [17] are a specialized type of private blockchain. Unlike private blockchains, which are typically managed by a single organization, consortium blockchains are governed by a group of organizations. These blockchains are commonly utilized in industries such as supply chain management and other collaborative sectors.
- **Hybrid Blockchain:** Both public and private blockchains have notable shortcomings. Public blockchains, for instance, often face significant delays in block validation, while private blockchains tend to be more centralized, making them more vulnerable to disruptive actions targeting their managing entities. To combine the advantages of both types of blockchains (public and private), hybrid blockchains have been developed [18].

3. The Internet of Blockchained Things (IoBT)

Besides the similar distributed natures of Blockchain and the Internet of Things (IoT), the integration of Blockchain technology into IoT environments has been realized through the consideration of communication acts and all interactions among IoT actors (devices and users) as transactions that need to be validated and stored on a secure and decentralized ledger (Fig. 4). Thus, Blockchain technology can be explored in multiple fields beyond its cryptocurrency-related use cases, such as logistics, distributed networking, cybersecurity, and more. In this context, IOTA [19] emerged in 2015 as an IoT-dedicated distributed ledger. IOTA is designed to handle Machine-to-Machine (M2M) monetary microtransactions among IoT devices and defines MIOTA as its crypto-token.

Like other Blockchain platforms, IOTA employs a rewarding system for its participants. However, this IoT-oriented distributed ledger has unique properties that distinguish it from other existing ledgers. Notably, IOTA does not have a block structure, miners, or transaction fees. Moreover, it uses a Directed Acyclic Graph (DAG) consensus mechanism named Tangle, which is specifically designed to meet IoT constraints, particularly the low computational power of nodes. With a DAG-based organization of the ledger, operations become more efficient, and issues such as forking are eliminated.

In this section, we discuss two critical aspects of integrating IoT and Blockchain technologies: security and storage. Additionally, we highlight the potential issues and challenges associated with the Internet of Blockchained Things.

3.1. *Blockchain for the sake of IoT security*

Since traditional defensive countermeasures in IoT rely on a single point of failure, the convergence of Blockchain and IoT enables the latter to benefit from Blockchain's distributed security services, which can be summarized as follows [20]:

- **Immutability:** Transactions are tamper-resistant, and any modification of the blockchain content can be detected and tracked.
- **Confidentiality:** Transactions carrying sensitive data are encrypted (using symmetric or asymmetric encryption) to protect the privacy of the involved participants.
- **Authentication:** Digital signatures are used to associate data and transactions with their rightful owners.
- **Durability:** All data stored on the blockchain is permanently available.
- **Access control:** The use of smart contracts to manage access control is crucial in blockchain environments. Smart contracts can verify participants' membership, preventing malicious or unauthorized entities from accessing the blockchain.

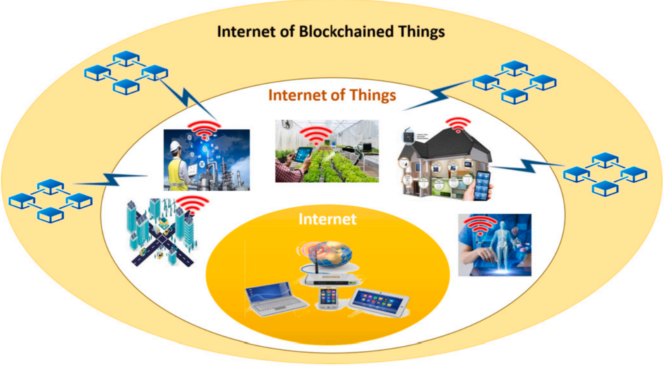

Fig. 4. Illustration of the concept of the Internet of Blockained Things.

Recently, several research studies have investigated the exploitation of Blockchain technology to enhance security in IoT and to transform its underlying infrastructures and services from centralized to distributed schemes (e.g., authentication servers, certification authorities, web servers, etc.). In [21], the authors propose using Blockchain and deep learning algorithms for collaborative intrusion detection in IoT networks. The solution consists of four modules: data collection, data management, analysis, and response. It is based on a permissioned Blockchain to secure communication among the intrusion detection agents. The solution defines three categories of agents: full communication agents that act as miners, light agents that hold only the block headers and verify the integrity of their respective agents' behavior, and a super-agent. The super-agent maintains the entire ledger and ensures that all other nodes in the detection module have a consistent copy of it. Reinforcement learning is further employed to enable the agents to analyze communication messages and detect potential attacks at the transport layer. A microchain-based intrusion detection system is proposed in [22] for detecting routing attacks in IoT networks.

The authors in [23] proposed using Blockchain to secure an intrusion detection system designed to mitigate Internet-originated threats and intrusions (e.g., viruses, malware, worms) targeting E-healthcare applications in the IoT. Beyond E-healthcare, Blockchain as a distributed security mechanism has been applied to numerous other domains, including industrial IoT [24], [25], [26], and smart grids [27], [28], [29]. Notably, the relationship between intrusion detection systems and Blockchain is bidirectional: Blockchain can enhance distributed intrusion detection through its immutability property, while intrusion detection systems, often employing machine learning techniques, can secure Blockchain by identifying threats, such as fraudulent transactions.

As for other security services, Blockchain has been widely proposed for authentication and access control security services [30], [31], [32]. Blockchain is also an effective platform through which participants can establish trusted commitments without needing a central third party. This makes it possible for each participant to verify data consistency and integrity. In [33], the authors proposed using Blockchain to establish end-to-end trust connections for trading over IoT. The authors in [34] were the first to explore Blockchain technology for IoT-connected LPWANs (Low Power Wide Area Networks), particularly LoRaWAN, for trust management between customers and network operators. In [35], the authors proposed TrustChain, an application of Blockchain technology for trust management in supply chains. The solution is based on a lightweight reputation model that evaluates the trustworthiness of participants and estimates the quality of commodities.

At this stage, it is important to mention that although Blockchain technology is considered an efficient security mechanism for IoT, both its software and hardware components (miners, consensus algorithms, smart contracts) must also be secured. Therefore, high trust levels cannot be achieved with Blockchain solutions unless the technology itself is secure and free from threats.

3.2. *Blockchain as a storage solution for the IoT*

With the advent of the Internet of Things (IoT), numerous storage options have emerged, all aiming to store and manage the vast amounts of data generated by IoT devices. Cloud and edge computing [36] have been the cornerstone of nearly all IoT-driven storage solutions. Recently, Blockchain-based solutions have gained significant attention. In [37], the authors proposed a distributed storage architecture based on Blockchain and edge computing for wireless sensor network data in IoT. The primary objective of the proposal is to ensure dynamic storage while minimizing the storage footprint within each Blockchain node. Similarly, the authors of [38] introduced ChainSplitter, a hierarchical storage solution focusing on Blockchain for the Industrial Internet of Things (IIoT). According to this solution, most of the proposed Blockchain system is hosted on the cloud. Additionally, newly generated blocks are stored in an overlay network. The authors claim that their solution can seamlessly link local IIoT networks, the Blockchain overlay network, and the cloud infrastructure.

To reduce the memory footprint associated with Blockchain storage requirements, particularly in constrained environments such as IoT, the authors in [39] propose adopting the Reed-Solomon erasure technique. IoT generates massive amounts of data that must be stored, processed, protected, and communicated. In this context, Blockchain appears to be a promising candidate to meet these requirements. However, the limited storage capacity of IoT devices poses challenges for their participation in Blockchain applications. This issue can be addressed by either augmenting the overall memory space with external, larger storage utilities or by adapting Blockchain systems to the constrained memory capacities of IoT devices. To address these challenges, a Blockchain compression technique for IoT data storage is proposed in [40], with the primary objective of accommodating IoT constraints and resource limitations, particularly storage capacity. Similarly, a Blockchain-based solution to store the location data of IoT devices is presented in [41]. To prevent network overburden, the solution recommends defining a reasonable number of transactions per block, relative to the network size.

3.3. *Potential issues and challenges related to the IoBT*

The issues and challenges associated with integrating Blockchain technology into the Internet of Things typically stem from the constraints of IoT devices, which must be carefully considered when adopting Blockchain solutions. The main concerns and challenges can be summarized as follows:

- **Scalability:** On one hand, the huge and ever-increasing number of IoT devices frequently generates transactions. On the other hand, Blockchain technology is known for being scalability-unfriendly since the memory footprint grows significantly as the number of transactions increases and the Blockchain scales up. Consequently, scalability risks being compromised, and the limited-memory constraints may not be met by IoT nodes that are required to store very large Blockchains. To address this issue, techniques like sharding [42] and hierarchical Blockchains [43] have been proposed. These techniques divide the entire Blockchain into smaller Blockchains, referred to as shards, where each shard manages its own data and maintains its uniqueness at the shard level.
- **Limited processing capabilities:** The use of highly complex consensus mechanisms in the IoBT is discouraged, despite their potential benefits from a security perspective. For this reason, the success of IoBT may strongly depend on balancing operational efficiency with the associated processing costs across all aspects of Blockchain, particularly consensus mechanisms.
- **Security and QoS-related issues:** Most of IoT applications require real time interactions among the involved parties and the handled data are often sensitive and/or privacy-tied. For this, QoS parameters (especially the latency) and data security should be seriously taken into consideration by the operational parts of the Blockchain, namely the consensus and smart contracts.
- **Smartness Challenge:** The convergence of the Internet of Things (IoT) and Artificial Intelligence (AI) has significantly enhanced the intelligence and effectiveness of IoT applications and services, leading to improved autonomy in smart devices. With the emergence of Blockchain-empowered IoT, the distributed security and data organization provided by Blockchain technology must align with the intelligence requirements to enable what can be termed Blockchained Artificial Intelligence of Things (BAIoT).

4. Overview on lightweight consensus algorithms in the IoBT

The successful integration of Blockchain technology within IoT environments depends on how well IoT constraints, such as limited energy, processing, and memory resources, are addressed. The consensus algorithms play a crucial role in determining the suitability of Blockchain technology for IoT. In other words, the feasibility of combining Blockchain and IoT largely hinges on the ability of consensus algorithms to account for the limitations of IoT devices. Unfortunately, most consensus algorithms are computationally intensive and significantly impact the storage footprint of the Blockchain, as they control the block validation throughput.

This section provides an in-depth analysis of the consensus algorithms proposed for the IoBT. The focus is specifically on lightweight consensus mechanisms. At this stage, it is important to highlight that a lightweight consensus mechanism not only ensures efficient block validation but also demonstrates a strong awareness of IoT constraints. Additionally, the study includes a classification of the reviewed solutions based on the dominant aspects of the proposed consensus mechanisms in the context of Blockchain-based IoT. Indeed, some consensus mechanisms introduce new operations to validate blocks or employ adaptation techniques to optimize existing consensus algorithms. Others focus on enhancing the security or intelligence of the block validation process. Furthermore, certain consensus mechanisms are specifically designed to address the unique requirements of IoT applications.

4.1. *Types of consensus algorithms according to the operation*

When it comes to the operation of consensus protocols, two main aspects are of concern: how miners are selected for the approval of new blocks, and how the approval process should be carried out by the miners. In this context, numerous consensus mechanisms have been proposed. Some were originally defined for the Ethereum and Bitcoin platforms and have since undergone adaptations to make them suitable for IoT constraints. Other consensus protocols have been directly proposed for integrated Blockchain and IoT applications.

4.1.1. *Proof of Work (PoW)-based consensus mechanisms*

PoW [44] is one of the oldest and most well-known consensus algorithms in the Blockchain domain, with Bitcoin being the first to utilize it. Its core concept revolves around solving a complex cryptographic puzzle, where the first participating node to successfully solve it is selected to mine the next block and earn the corresponding reward. In fact, the puzzle-solving process in Proof of Work consensus algorithms involves adding a random nonce to the block and then applying a hash function to all parts of the block (Equation (1)). The resulting hash value must meet a specific condition, which typically requires the hash to start with a certain number of leading zeroes. Consequently, the nonce is adjusted repeatedly until the condition is satisfied.

$$HashValue = h(block \parallel nonce) \tag{1}$$

PoW algorithms are fully distributed but highly resource-intensive in terms of the computational power required. Furthermore, the transaction and block validation speeds are relatively slow due to the high complexity of the cryptographic puzzles. Considering these factors, researchers widely agree that directly applying the PoW process to IoT is impractical. Consequently, numerous research efforts have emerged to address and mitigate the costs associated with PoW.

In [45], the authors propose using the Proof of Work (PoW) consensus algorithm in a non-monetary context. Their solution introduces a Lightweight Scalable Blockchain (LSB) tailored for enhancing security and privacy in automotive IoT systems. The proposed approach addresses the scalability issues inherent in conventional PoW-based blockchains, where all mined transaction blocks are broadcast to every node in the network. Moreover, it tackles the limited throughput of blockchains utilizing PoW consensus algorithms, which are constrained by the intensive computational requirements. For instance, Bitcoin's PoW allows for the generation of fewer than ten transactions per second. To overcome these limitations, LSB employs a scheduled block generation policy, reducing the computational overhead and thereby lightening processing demands. Additionally, the solution incorporates a Distributed Throughput Management (DTM) mechanism to dynamically adapt the blockchain throughput to match the processing capacity of the network nodes.

In [46], the authors propose a lightweight blockchain model incorporating an innovative Green Proof of Work (Green-PoW) consensus algorithm tailored to constrained environments, such as the Internet of Things (IoT). This approach is designed to outperform the traditional PoW mechanism in such contexts. Unlike the conventional PoW, the Green-PoW divides the block mining process into two distinct rounds. In the first round, miners compete in a fully decentralized manner to mine a block, during which a subset of miners is also selected to validate the next block. In the second round, which is more time- and energy-efficient, the next block is mined exclusively by the elected group of miners determined in the first round. Although the evaluation results demonstrate that Green-PoW achieves significant energy savings (up to 50% in the best cases) among the participating miners, the restriction on the number of miners involved may impact the decentralized nature of the original PoW consensus. Furthermore, the proposed solution does not account for the complexity introduced at the node level. Additionally, the security of the miner election policy is a critical concern that requires thorough validation.

In [47], the authors propose a statistical approach for the proof of work consensus algorithm operating over Blockchain, utilized in cloud and fog computing. The solution is claimed to address the computational complexity of the standard PoW mechanism through a polynomial matrix factorization, which simplifies the puzzle-solving process for the participating miners. To tackle the significant processing complexity of the standard PoW consensus algorithm and adapt it for constrained IoT networks, a diversity-based PoW mechanism [48] has been proposed. This proposed PoW mechanism operates over consortium Blockchains, which are inherently better suited to meet security and privacy requirements. Specifically, the consortium Blockchain defines a set of admission rules for all nodes intending to mine blocks of transactions initiated by IoT devices and users. Before entering the block mining phase, each validator must select a random number, compute its hash value, and combine it with hash values of other relevant information, such as the timestamp. If the resulting value is below a predefined threshold, the node is accepted into the current round's set of miners and becomes eligible for the next block validation. Additionally, the transactions have consistent sizes (an average of 464 bits), which enhances mining efficiency and awareness of constraints. However, the solution does not specify the IoT applications that might benefit from its implementation. Furthermore, the number of miners allowed to perform block mining should not compromise mining throughput or safety. Hence, the heterogeneous capabilities of the miners, as well as their trustworthiness, should be carefully assessed.

A proof of work mechanism with a fair mining strategy is proposed in [49] for blockchains in IoT contexts. The solution is inspired by the concept of digital twins to implement a fairness-based policy among IoT miners running the PoW consensus algorithm while possessing heterogeneous processing resources. In this approach, the edge physical miners are represented as microservices, with their corresponding twins residing in the cloud to monitor the miners' functional behavior in real time. Notably, the solution introduces Proof of Behavior (PoB), which aims to reinforce the fair mining process by enabling the twins to detect misbehavior and penalize deceptive miners. Although the proposed solution appears promising, the authors highlight several challenges that need to be addressed before deployment in real IoT environments. Specifically, ensuring secure communication between the twins and miners is crucial, as is addressing the potential for compromise targeting both parties. Additionally, the management of mining fairness and its safety-related functionalities should have minimal overhead to enhance the solution's adaptability to IoT constraints and limitations.

To summarize, most adaptation attempts that aimed at making the PoW algorithm suitable for IoT limitations focus on reducing the number of miners rather than alleviating the processing-related tasks performed by each participating miner. While this approach offers significant advantages for global energy conservation, it comes with trade-offs. By reducing the number of participating miners, the distributed nature of the consensus mechanism is compromised, potentially increasing the vulnerability of the system to security risks. This includes threats from malicious miners that could monopolize the mining process.

4.1.2. Proof of Stake (PoS)-based consensus mechanisms

PoS [50] is another widely known consensus algorithm. Unlike Proof of Work, which is a competitive consensus mechanism, PoS operates on a cooperative mining strategy. In PoS, miners are referred to as validators, and a block is not considered validated until a group of validators approves it. Machines participating in the block validation process must lock up some of their coins (tokens) to qualify as validators, a process known as staking. The selection of validators for the next block of transactions is performed randomly. Validators are systematically rewarded after every successful block validation. This eliminates the need for machines with high computational capabilities, making PoS a viable alternative to PoW, especially for blockchains operating in resource-constrained IoT environments. However, PoS tends to favor nodes with higher coin holdings, as the probability of being selected as a validator increases with the amount of staked coins. This mechanism can lead to centralization, as entities with larger stakes are more likely to dominate the validation process, potentially monopolizing and compromising the system's integrity. To address these issues and improve PoS in terms of scalability and fairness, the Delegated Proof of Stake (DPoS) [51] was introduced. DPoS incorporates stakeholder voting to select the group of validators responsible for producing the next block. Currency holders vote for a set of validators, with the voting weight proportional to the voter's stake. The most highly voted entities serve as the current round's validators and block producers. These validators share a portion of their rewards with their voters, and the process repeats for the next round of block validation.

Considering the energy efficiency of PoS consensus algorithms, several research studies have explored their application in IoT environments. In [52], the authors propose a solution called Bazo: a PoS-based blockchain that employs sharding and transaction aggregation techniques to enhance the efficiency of the PoS mechanism, particularly in terms of scalability. Furthermore, the solution introduces an IoT-BC adaptation framework to facilitate the integration of IoT data into the blockchain. The proposal specifically targets the integration of data originating from LoRa-enabled devices. The solution has been evaluated using a small, fixed set of validators hosted on Google Cloud. However, the mechanism for staking among these validators of IoT-originated blocks is not clearly explained. A Randomized Delegated Proof of Stake (RD-PoS) algorithm is proposed in [53]. This solution aims to improve the resilience of the traditional Delegated PoS by incorporating randomness into the selection process for potential block producers from the most-voted validators. Additionally, it advocates for the use of modern, energy-efficient cryptographic primitives such as Elliptic Curve Digital Signature Algorithm (ECDSA) and Boneh–Lynn–Shacham (BLS) instead of classical ones within the blockchain-enabled IoT system. To address scalability requirements, RD-PoS proposes splitting the pool of potential block producers into multiple sub-pools. Each sub-pool can dynamically expand or contract based on the need for additional candidate validators. This approach endows the proposed consensus algorithm with an auto-scaling capability that better suits the requirements of IoT networks.

PoS consensus has even been adopted for blockchains serving specialized IoT networks, such as the Internet of Vehicles (IoV) and the Internet of Flying Things (IoFT). As mentioned earlier, in PoS consensus, nodes with higher stakes are more likely to be elected as validators. In [54], the authors proposed a PoS-based approach for blockchain-enabled IoV applications. Their solution introduces a voting mechanism as a mandatory step before potential validators are selected and proceed to the block approval phase. To promote fairness and prevent nodes with high stakes from dominating the consensus, voters are allocated a limited number of tokens. Furthermore, the solution classifies voters based on their behavior—whether faulty or well-intentioned—using a priority-based approach. These classifications are then utilized to define the priorities for access to the voting process. In [55], the integration of PoS in Unmanned Aerial Vehicle (UAV)-aided IoT systems is proposed. To ensure secure data gathering, the blockchain network of UAVs is organized into clusters, where a pool of stakes is constructed and maintained by active UAVs. Other UAV stakeholders within the clusters are incentive to contribute stakes and benefit from gain-sharing opportunities. The IoT data collected by the deployed UAVs are treated as block transactions, which are subsequently validated by the selected validators. The evaluation results of the proposed system indicate that with larger cluster sizes and a higher pool of stakes, the solution performs better, aligning with the authors' expectations. However, the quantification of QoS-related assessment parameters—such as energy consumption and latency induced by block validation per cluster, as well as block validation rates under the proposed framework—has not been provided.

4.1.3. *IOTA Tangle consensus*

Tangle is the first consensus mechanism proposed for IOTA, a promising blockchain-like and IoT-friendly distributed ledger. Validating micro-transactions is a straightforward task; each new transaction (referred to as a "tip") must validate two earlier transactions to join the Directed Acyclic Graph (DAG) network. The validation process ensures that transactions comply with all rules defined by Tangle. To mitigate spam and prevent flooding attacks, a lightweight Proof of Work (PoW) puzzle must be solved before submitting any transaction to the network. Furthermore, the weighted random walk algorithm [56] is commonly employed to facilitate the selection of the two transactions to validate. Once the validation rate for a transaction reaches a predefined threshold, the transaction is considered validated. As mentioned earlier, Tangle builds its validation network on a Directed Acyclic Graph structure, illustrated in Fig. 5.

Indeed, Tangle offers several significant advantages, including the fast and lightweight validation of transactions, which, in turn, enables high throughput in transaction validation. Additionally, Tangle capitalizes on the vast number of transactions generated by IoT devices to enhance scalability and increase transaction validation rates. In other words, the more IoT nodes generate transactions, the greater the likelihood of finding tips for validation. Considering these advantages, numerous solutions have adopted IOTA architectures and Tangle principles in implementing non-financial Blockchain-IoT applications [57], [58], [59], [60]. However, security challenges remain the primary drawback that upcoming versions of IOTA aim to address [61].

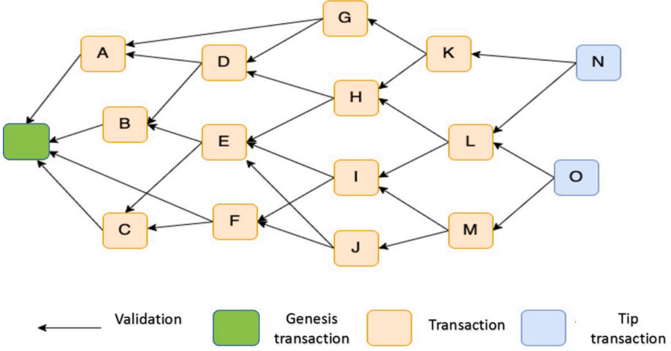

Fig. 5. DAG structured IOTA enabled by Tangle consensus mechanism.

4.1.4. *Other operation-based consensus algorithms*

In addition to the two prominent consensus algorithms, PoW and PoS, several other variants of consensus mechanisms have emerged in both the cryptocurrency domain and blockchain-based IoT systems. This section highlights these variants and discusses their applicability to IoT environments.

- **The Proof of Elapsed Time (PoET):** The objective of PoET [62] is to serve as a lightweight consensus mechanism while promoting fairness among participating validators. The core idea is based on ensuring that all validators have an equal opportunity to approve blocks. Initially, each validator waits for a randomly assigned time period before attaching proof of this waiting period to the block. The block with the shortest verified waiting time is approved, and the corresponding validator is declared the winner. To maintain fairness, the algorithm prevents validators from consistently generating the shortest waiting times, thereby avoiding domination in block validation.
- **Proof of Capacity (PoC):** Instead of investing time or currency, as in PoC [63], validators allocate hard disk space. The more space an entity dedicates, the greater its chances of validating blocks. The application of proof of capacity in IoT can be efficient when validators are hosted on the cloud or at the edge. However, adopting such a mechanism on memory-constrained end devices appears unfeasible.
- **Proof of Authority (PoA):** PoA is another consensus mechanism that could be a strong candidate for the Internet of Blockchained Things [64]. This mechanism establishes strict rules regarding the identities of the participating validators. Only entities with valid and reputable identities are allowed to become validators. The blocks created by approved validators can be directly accepted or verified by all (or the majority of) other participating validators. PoA does not require computational work or competition for block validation, making it an extremely lightweight consensus mechanism. However, PoA tends to be more suitable for private blockchains than public ones due to its mandatory identity verification process for all validating entities.
- **Proof of Elapsed Work and Luck (PoEWL):** A non-cooperative consensus for Blockchain applications in the Internet of Things, PoEWAL is specifically designed to accommodate the resource limitations of IoT devices while enabling them to execute the proof of work consensus algorithm and store the ledger [65]. The core concept of PoEWAL is to address a significant problem partially within a fixed time slot, rather than solving the entire problem over a variable period. Additionally, the mechanism provides a solution to the forking issue, ensuring that each new block is added by exactly one miner. Assessment results indicate that PoEWAL exhibits

Table 1
General comparison of the studied operation-based consensus algorithms.

Class of Operation-based consensus	Miner/validator selection criterion	Advantages	Drawbacks
Proof of Work	Solving complicated cryptographic puzzle	Fully distributed. Better security	Computationally heavy. Important latency. High energy -consumption
Proof of Stake	Staking coins and being among the most voted on entities.	Less energy consumption. Slight latency	Tends to be centralized. Limited security Weak fairness among participants.
Proof of Elapsed Time	The minimum time spent to validate a block	Low cost. Good fairness. Slight energy consumption	Risk of time tampering. Very intuitive; it might need to be combined with other techniques.
Proof of Capacity	The investment in storage resources (hard disk)	Well adapted for cloud/edge aided networks	Not suitable for constrained environments
Proof of Authority	Identity verification for the validators	Low computational overhead	May face scalability issues en applied on public environments, like IoT.
Proof of Elapsed Work and Luck	Partial solving of a cryptographic puzzle	More lightweight compared to the basic PoW. Better dealing with fork issues	Important consensus latency. Weak scalability. Important memory footprint.
Proof of Sincerity	The sincerity level of the miner	Lightweight block validation operation	Prone to 51% attack
Practical Byzantine Fault Tolerance	Cooperation between leader and backup entities	Good fault tolerance	Important network overhead. Does not support network scalability
IOTA Tangle	No specific miners	Lightweight validation. Important flexibility and QoS. IoT friendly	Weak security

low energy consumption. However, since IoT devices are responsible for both mining and storing the entire ledger, the scalability factor should also be evaluated.

- **Proof of Sincerity (PoSin):** PoSin [66] is based on the sincerity of each participant in the blockchain system. Sincerity is used to replace complex puzzles, thereby simplifying the consensus process while maintaining a fair level of competition among block miners. This consensus mechanism is particularly suited for mobile blockchains, where mobile participants can demonstrate their highest level of sincerity to engage in the mining process and receive rewards. However, PoSin is vulnerable to security-related issues, particularly the 51% attack.
- **Practical Byzantine Fault Tolerance (PBFT):** The Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm that is particularly suitable for blockchains operating over small, high-performance networks, due to its limited scalability, poor resiliency, and significant energy overhead. Its primary goal is to achieve high block validation rates while tolerating a certain number of faulty nodes. The model categorizes nodes into a single leader and several backup nodes, which exchange messages and utilize cryptographic tools to verify both the authenticity and integrity of the transmitted messages. Given the complexity of this consensus algorithm, only a few studies [67], [68], [69] have explored its feasibility for IoT networks.

In Table 1, we provide a general comparison of all the studied classes of operation-based consensus algorithms and highlight the common advantages and disadvantages associated with each class. Table 2 presents a detailed comparison of the studied operation-based lightweight consensus mechanisms in the IoBT.

4.2. Secure consensus mechanisms in the IoBT

Although Blockchain is considered a modern distributed security mechanism attracting exponential interest across various technological fields, particularly in future computer networks and the IoT, it faces several security challenges that must be effectively addressed. Without such measures, Blockchain will be unable to fulfill its intended purpose. As discussed in earlier sections, all components of Blockchain technology must be secure, with a particular emphasis on consensus algorithms, which are crucial for ensuring the safe block validation process and providing resilience against potential threats. Indeed, numerous Blockchain-related threats [70] have emerged alongside the widespread adoption of Blockchain technology. These include the participation of unauthorized validators in permissioned blockchains, the injection of malicious content into validating blocks, the selfish behavior of participating nodes in cooperative consensus mechanisms, and more. Additionally, Blockchain networks, especially public ones, are susceptible to severe cyber-attacks, such as DDoS attacks, perpetrated by malicious participants.

The 51% attack [71] is a well-known example of such attacks, where a group of malicious miners controls more than 50% of the overall network's hash or validation rate. Once the 51% attack succeeds, the attackers can disrupt the entire ledger either by excluding transactions from being incorporated into new blocks or by preventing legitimate miners from participating in the validation process. The adversaries may even double-spend coins by validating blocks that contain reversed transactions. Despite the critical importance of security in the block validation process, only a few research studies have addressed this issue. Stake bleeding [72] is another emerging type of harmful attack targeting PoS-based blockchains. This attack exploits the "longest chain" property in flat blockchains to dominate block validation by controlling the staking process and creating a forked chain. The attackers then empower this forked chain by adding numerous newly produced blocks, making the deviating chain appear longer than the legitimate one.

The proposed solutions in this context can be categorized into two classes: solutions that aim to secure existing consensus mechanisms, such as PoW and PoS, which are free from built-in security, or those that add an additional security layer operating above them. The second category, on the other hand, proposes new consensus algorithms where security is an integral component.

4.2.1. Security of the existing consensus algorithms

The authors in [73] propose a combination of both PoS and PoW consensus algorithms to mitigate the 51% attack. The core principle of the solution is to make it more difficult for an adversary to control the majority of the network's computational power by forcing them to meet the mining requirements of both consensus systems: PoW and PoS. According to the proposed solution, the computational difficulty of PoW is adjusted, and coin staking is subject to interval-dependent regulations. Thus, the combined PoW-PoS system is designed to operate on each mining entity. Initially, the miner enters the PoW loop to find the appropriate nonce that satisfies the block hashing conditions. Afterward, the miner proceeds to the PoS loop to verify if the staking-related time

Table 2
Detailed comparison of the operation-based lightweight consensus mechanisms.

Solution	Category of consensus	Main technique	Suitability to IoT networks	Energy consumption	Scalability	Validation rate	Validation latency	Security	Fairness
A. Dorri et al. [45]	PoW	Scheduled block generation and distributed throughput management	Good	Low	Good	High	Medium	Good	Good
N. Lasla et al. [46]	PoW	Block mining process is split into two rounds	Good	High	Bad	Medium	Medium	Not secure	Bad
G. Kumar et al. [47]	PoW	Use of polynomial matrix factorization to simplify puzzle solving	Good	Low	Good	Medium	Low	Weak	Bad
C.P. Jayabal et al. [48]	PoW	Random selection of private miners with reduced transaction sizes	Good	Low	Medium	Medium	Medium	Good	Good
Q. Qu et al. [49]	PoW	Heterogeneous network and digital twins	Medium	Medium	Good	Medium	Low	Not secure	Good
M. Snider et al. [50]	PoS	Voting capacity of the stakeholders to select the group of validators that will produce the next block	Good	Low	Good	Medium	Medium	Weak	Good
S.R. Niya et al. [52]	PoS	Sharding and transactions aggregation	Very good	Low	Medium	High	Medium	Weak	Good
X. Fan et al. [53]	PoS	Random selection of the most voted block validators with the use of modern cryptographic techniques	Good	Low	Good	High	Low	Good	Good
J. Misic et al. [54]	PoS	Adding the voting mechanism as a mandatory step and priority-based classification of the voters	Good	Low	Good	Medium	Medium	Good	Medium
X. Tang et al. [55]	PoS	Clustering and intra-cluster staking	Good	Medium	Good	Medium	Medium	Good	Medium
M.A. Kumar et al. [62]	PoET	Backoff-like technique	Good	Low	Good	High	Medium	Weak	Very good
M. Salimitari et al. [63]	PoC	Devoting hard disk space	Bad	Low	Good	Medium	Medium	Weak	Bad
M.A.s Manolache 2022 [64]	PoA	Account/identity verification of the validators	Good	Low	Bad	Good	Low	Good	Good
N. Andola et al. [65]	PoEWL	Revolving complicated puzzle partially	Good	Medium	Bad	Low	Medium	Weak	Medium
Z. Zhang et al. [67]	PBFT	Cooperative Block validation	Bad	High	Bad	Medium	Medium	Weak	Good
M.U. Zaman et al. [66]	PoSin	Assign sincerity levels of the participating miners and ask them to resolve a slight puzzle	Good	Low	Good	High	Low	Not secure	Good
IOTA Tangle-based solutions [57], [58], [59], [60]	Tangle	Validation of two previous tips	Very good	Low	Very good	High	Low	Weak	Very good

interval and conditions are met. If the miner successfully passes the requirements of both consensus algorithms, they can mine the new block. While the solution significantly reduces the likelihood of an attacker gaining control of the mining process by requiring them to meet the mining criteria set by both consensus algorithms (PoW and PoS), it may affect mining latency and block validation throughput. Nevertheless, the regulated difficulty of the PoW consensus mechanism can facilitate the adoption of this solution in blockchain-based IoT networks.

In [74], the authors propose a Secure and Low-latency Proof of Work (SLPoW) protocol for Blockchain in green IoT networks. SLPoW introduces a hash function to enhance the security of the PoW consensus and, to make it more IoT-friendly, suggests running all security primitives and puzzle-solving operations on an Field-Programmable Gate Array (FPGA) platform for accelerated and energy-efficient processing. The solution's security strategy primarily focuses on hash-based protection. Additionally, it is claimed that the solution can protect the Blockchain network against attacks, such as the addition of fake transaction blocks and transaction alteration or dropping attacks, particularly in cases where an adversary controls the entire blockchain-based IoT network (e.g., the IoT network of a smart home). Unlike standard PoW, and for security reasons, the solution proposes controlling the participation of miners in IoT-integrated Blockchain systems. It achieves this by granting authorization only to IoT entities that hold the genesis transaction.

In [75], another secure consensus algorithm based on Proof of Work (PoW) in combined IoT and Blockchain environments is proposed. The proposed algorithm is named the Credit-Based Proof of Work Consensus, and it primarily addresses security issues in blockchains organized as Directed Acyclic Graphs (DAGs). The introduced credit system aims to balance security and energy costs within the PoW mechanism. To achieve this, each sensor node is assigned a dynamic credit, the value of which is directly influenced by the node's behavior. Specifically, good behavior is associated with the activity of a node and the weight of the block it has validated. In other words, the more blocks a node validates and the more other nodes approve the blocks it has generated, the greater its positive credit. Conversely, lazy nodes and any nodes that act maliciously (e.g., double spending) will be penalized by increasing their negative credit. To prevent malicious nodes from participating in mining, the credit system suggests that nodes with high negative credits will face increased PoW complexity (Equation (2)).

$$Credit = \frac{1}{Difficulty} \tag{2}$$

In this way, honest nodes will consume less energy, as the computational difficulties assigned to them are significantly lower. At this point, it is important to recall that the PoW difficulty is proportional to the required length of the zero prefix in the block hash value. Although the proposed security management mechanism appears to be efficient and applicable to Blockchain-enabled IoT, the credit calculation for all IoT nodes could become a time-consuming task as the network size increases.

As previously mentioned, PoS consensus mechanisms outperform traditional PoW algorithms in terms of computational efficiency. However, when it comes to security considerations, PoS-based protocols face several vulnerabilities, including 51% attacks and stake bleeding attacks. The authors in [76] propose two security protocols for PoS systems, aiming to protect the consensus mechanism against potential threats, such as the longest chain attack and account compromises. The first protocol employs a digital signature scheme to track the identities of validators, ensuring that each participant can generate only one block at each blockchain height. The second protocol utilizes Trusted Execution Environments (TEEs) to regulate block generation frequencies by entities. Although blockchain is typically considered a fully distributed solution, eliminating the need for trusted third parties, the proposed protocol justifies the adoption of TEEs by noting that their use can be tolerated within permissioned blockchains. Additionally, it has been observed that both security protocols may introduce additional overhead during the block validation phase, which could compromise IoT's Quality of Service (QoS) requirements.

On the other hand, IOTA Tangle-based security solutions offer an alternative approach. The authors in [77] propose a fair and confidence-aware Tangle called G-IOTA. This proposal focuses on protecting orphan tips and presents a fair tip selection mechanism that maximizes the number of confirmed transactions. In the standard IOTA, transaction fairness is defined as the percentage of validations a transaction receives from new tips on the Tangle. G-IOTA improves the weighted random walk algorithm used by IOTA to enhance transaction fairness, which in turn reduces the number of left-behind tips. The same authors demonstrate in [78] that the security and even the fairness of G-IOTA can be significantly improved by using variable tip selection parameters, such as varying high, mean, and low cumulative weights in the weighted walk algorithm. This technique, referred to as E-IOTA (Efficient IOTA), provides resilience against double-spending and various disruptive Tangle attacks.

In another study addressing a similar research problem, the authors of [79] focus on optimizing the factors that influence the number of left-behind tips. In [80], a cryptographic protocol is presented to secure IoT data exchange in IOTA-based blockchain networks. The solution is mindful of the stringent constraints of IoT devices and is built on two security solutions already provided by the IOTA Foundation: STREAM and MAM (Masked Authenticated Messaging). The STREAM protocol [81] ensures immutable publish/subscribe messaging, while the MAM protocol guarantees that only authorized IoT devices can publish and access transactions. L2Sec, the proposed solution, is a lightweight security mechanism that ensures most of the security objectives for data exchanged over constrained IoT devices running the IOTA Tangle. To improve performance, the solution encourages the use of Hardware Secure Elements (HSE) that natively integrate basic cryptographic primitives into devices.

The authors in [82] highlight a significant vulnerability in the IOTA Tangle: the ability of adversaries to create fake branches in the DAG, which can lead to double-spending issues. Their solution initially estimates the probability of such a vulnerability, then establishes a threshold security level to detect malicious branches. Another promising security strategy is proposed in [83], which focuses on detecting intrusions in the IOTA DAG and identifying malicious participation in the Tangle process. This approach uses a private IOTA DAG to facilitate network control and employs a sliding window that considers several dynamic properties (e.g., memory properties, input data averages, etc.). The resulting data is then transferred to a Machine Learning (ML) module for dynamic classification into various DoS threat indexes. Evaluation results demonstrate the solution's good performance, with low costs and accurate anomaly detection.

4.2.2. New secure consensus algorithms

The authors in [84] proposed a lightweight Proof of Authentication (PoA) consensus mechanism for Blockchain applications in the IoT. PoA is specifically designed to ensure secure and authenticated block validation by edge IoT nodes, while being more efficient than traditional consensus algorithms in terms of energy consumption and validation latency. According to the network model, three categories of nodes are defined: sensor nodes, aggregator nodes, and trusted nodes. Trusted nodes are indirectly connected to sensor nodes through aggregator entities, which are responsible for collecting data from sensor nodes via low-power communication links (e.g., LoRa connections). The aggregators also handle block construction and store the Blockchain alongside the trusted nodes. In fact, trusted nodes maintain a list of the MAC addresses of all authorized sensor nodes. This list is loaded onto the trusted nodes prior to network deployment and is used during the block validation process. Accordingly, blocks containing transactions from legitimate nodes (whose MAC addresses are registered in the list) will be validated and added to the Blockchain. As a result, validation-related energy consumption and delays are significantly reduced. However, the solution may face scalability issues, as the adopted authentication policy is not well-suited for dynamic and dense IoT networks. Moreover, the security scheme focuses on a set of trusted parties, which contradicts Blockchain's decentralized nature and principles. In [85], the authors introduced the concept of Proof of Reputation (PoR), where the behavior of participating nodes is assessed and classified into different trust levels. Highly trusted nodes are selected as block validators, while the remaining nodes are incentivized through reputation and reward-based mechanisms to actively participate in the voting process. The main goal is to enhance block-validation security while ensuring adaptability in constrained IoT-like environments. Evaluation results show that the solution effectively punishes and isolates malicious and selfish nodes attempting to either compromise the consensus or manipulate the voting process.

A trust-driven consensus mechanism, named Proof of Trust (PoT) [86], is proposed for the application of blockchain in IoT environments. In PoT, the mining entities are selected based on their behavior during block validation participation. The solution defines two trust computation phases that involve all participating nodes. In the first round of trust estimation, nodes are assigned credits calculated based on their past communication actions. In the second round, the trust credits calculated in the first round are reviewed by other nodes for confirmation or potential redefinition. Both the initial and recommended trust values are published on the blockchain, allowing all network nodes to view and evaluate their neighbors' trust values in an autonomous and distributed manner. It is important to note that the solution performs better with isolated malicious nodes. However, when a group of malicious miners generates corrupted trust values for legitimate nodes, the entire trust decision-making process can be compromised. In a similar context, a novel cryptographic consensus mechanism is proposed in [87]. This proposed consensus algorithm uses the Verifiable Random Function (VRF) to select the block miner for each block validation round. The VRF approach requires each participating node to have a pair of public and private keys. The private key, along with several initial shared credentials (including the current round time), is used to generate a hash value, while the public key is used for hash verification. If the hash value meets certain criteria, the node that calculates it is chosen to validate the block for the current round. However, the VRF function does not guarantee that only one miner will be selected in a round, making chain-forking a potential issue with this consensus. Furthermore, the computational complexity of the proposed consensus appears to shift to the miner selection phase, rather than being concentrated at the block validation level, as is the case with PoW.

Table 3 compares the secure consensus algorithms studied and proposed for the Blockchained Internet of Things (Table 4).

In conclusion, existing secure consensus algorithms often rely on the participation of authenticated parties, making them more suitable for private (permissioned) blockchains. Alternatively, some solutions adopt public (permissionless) blockchains while strengthening the consensus mechanisms to prevent malicious entities from dominating the block validation process. However, neither approach fully meets the requirements of IoT environments, which demand both a broad openness to all potential users and participants and an awareness of the resource constraints of the devices involved. Therefore, developing secure consensus algorithms that address these challenges and satisfy all the aforementioned conditions is of critical importance.

4.3. Smart consensus mechanisms

AI-enabled blockchain is still considered a relatively new concept but holds significant promise. Research has demonstrated that AI and blockchain share a bidirectional relationship, with each capable of benefiting the other. On the one hand, blockchain technology can enhance the security of artificial intelligence systems, particularly in the domain of machine learning [88], [89], [90]. On the other hand, recent studies have explored the integration of AI into various components of blockchain technology. In this section, we focus specifically on how AI can contribute to the block validation (consensus) process in the Internet of Blockchained Things. We also examine some of the proposed solutions in this area.

In [91], the authors proposed a consensus mechanism based on Machine Learning (ML) for blockchains operating on peer-to-peer networks. This proposed solution, called Proof of Machine Learning (PoML), employs ML competitions for block validation. In addition to the validators, the solution involves two other types of entities: suppliers and trainers. Initially, the suppliers deliver tasks and propose machine learning competitions, while the trainers focus on training models for the existing tasks. Finally, the validators evaluate the trained models using data (transactions). The solution appears to be too complex to be effectively supported by IoT devices. Moreover, it suffers from other challenges, such as high block validation latency and insufficient security measures. To address these issues, [92] introduced a lightweight, AI-based consensus mechanism specifically designed for IoT edge devices. This proposed approach eliminates the need for nonces and complex puzzles used in classical blockchains. Instead, it equips each IoT edge node with an ML-based classifier, which includes a dataset and a machine learning algorithm for the training phase. The solution proposes deploying a diverse set of classifiers (e.g., Support Vector Machine, Naive Bayes, Decision Tree, and Nearest Centroid) across edge nodes to prevent intruders from compromising the entire mechanism. Edge nodes are responsible for collecting and aggregating data generated by sensor nodes. The aggregated data is then integrated into blocks, which the classifier processes to determine whether the data is safe or malicious. Blocks that successfully pass the classification phase are validated, achieving consensus with low costs. Although assessment results demonstrate that the proposed framework delivers good Quality of Service (QoS), it seems that the AI-related aspects primarily focus on the classification of sensor data rather than on the consensus operation itself.

In [93], the authors propose employing AI for block validation node selection in highly mobile, blockchain-enabled IoT networks. The solution considers a clustered IoT network and presents an intelligent approach to determine the optimal set of mobile block validators. To achieve this, Artificial Neural Network (ANN) technology is utilized to assign reputation values to mobile consensus nodes (validators). The input layer of the ANN incorporates three reputation parameters: node age, node stability, and the rate of successful block validations. These reputation values, which are dynamic, are used to evaluate the honesty of the nodes. Notably, minimum and maximum reputation thresholds are locally defined within each cluster to enhance security and improve blockchain performance. In [94], the authors propose leveraging Tangle for validating updates in decentralized federated learning within IoT environments. The primary goal is to ensure high performance while protecting the model from corruption and poisoning attempts. The solution adopts the standard Tangle architecture with a mandatory adaptation of transaction content, which henceforth includes a set of parameters related to the machine learning model. Machine learning models are typically trained on edge entities to reduce the computational load on constrained IoT nodes in traditional setups. However, since Tangle requires transactions to be approved by IoT devices, it is unclear how IoT devices in the proposed solution will additionally manage machine learning mechanisms. Furthermore, the costs associated with the added "smartness" are not evaluated in the proposed Tangle-enabled ML mechanism.

In [95], the authors propose a lightweight and intelligent consensus mechanism in Blockchain-as-a-Service (BaaS) for the Internet of Things (IoT). The proposed mechanism, referred to as the Proof of Evolutionary Model (PoEM), departs from traditional rule-based protocols by leveraging machine learning to iteratively train a model for achieving consensus. This approach enhances efficiency and facilitates the participation of low-performance IoT devices. Furthermore, PoEM incorporates mechanisms to adapt to dynamically changing IoT environments. Analytical and experimental results validate PoEM's effectiveness in improving consensus efficiency and security in the IoBT. In [96], another lightweight and intelligent consensus algorithm, named Q-learning Improved Delegated Proof of Stake (QV-DPoS), is introduced to address the energy consumption and complexity challenges associated with blockchain consensus mechanisms. The proposed framework is implemented on Ethereum to develop a blockchain-based IoT prototype system. Experimental results demonstrate the platform's efficacy in managing trust, authenticating identities and behaviors, and improving transaction success rates, all while significantly reducing energy consumption compared to traditional algorithms.

To conclude the study of AI-enabled consensus algorithms in the Internet of Blockchained Things, it is evident that integrating AI techniques with consensus mechanisms remains a largely unexplored area. The few existing solutions are insufficient for a deeper understanding of the relationship between these two concepts. Specifically, leveraging AI's potential for validator selection and transaction or tip classification is crucial to achieving efficient smart block validation. However, it is imperative to ensure that the constraints of IoT systems are respected.

Table 3
Comparison of the studied secure and lightweight consensus mechanisms (1).

Solution	Based on existing consensus algorithm	New secure consensus	Addressed issue	Type of Blockchain	Main security policy	Authent. of participants	Protection against DoS attacks	Security-related overhead	Block validation latency
K.D. Gupta et al. [73]	PoW and PoS	/	Protection against 51% attack	Public	Forcing miners to satisfy the mining conditions of PoW and PoS with regulated difficulty of PoW	Not mentioned	Good	Medium	High
A. Yazdinejad et al. [74]	PoW	/	Protection against 51% attack and Make PoW more IoT-friendly	Public	New hash function to promote the security and accelerated and energy effective processing with FPGA platform	Ensured and it is based on verifying the ownership of the genesis transaction	Very good	Low	Medium
J. Huang et al. [75]	PoW	/	Malicious behavior monitoring	Public	Positive and negative credits for miners and PoW difficulty is adjusted according to the node's credit	Not mentioned	Good	Low	Low
W. Li et al. [76]	PoS	/	Protect the consensus mechanism against potential threats like longest chain and accounts tampering	Private	Limit the block generation frequency at every height with the use of the TEEs	Not mentioned	Good	High	Medium
S. Maitra et al. [84]	/	PoA	Trusted and authentic block validation	Private	Trusted nodes carry a list of MAC addresses of legitimate IoT nodes and only transaction originated from trusted nodes are validated.	Ensured	Good	Low	Low
E.K. Wang et al [85]	/	PoR	Trusted and authentic block validation with punishment and isolation of selfish validators.	Public	The behavior of the participating nodes is assessed through voting. Highly ranked nodes are selected as block validators	Ensured	Not mentioned	Low	Low
J. Zou et al. [86]	/	PoT	Trusted consensus	More practical for private ledgers	Collaborative trust computation for all participating nodes	Ensured	Not mentioned	High	Medium
Y. Wu et al. [87]	/	Crypto consensus	Secure selection of block validators	Public	Use of the Verifiable Random Function along with cryptographic credentials to generate hah values prior to validator selection	Ensured	Good	Medium	Medium
G. Bu et al. [77]	IOTA Tangle	/	Fair and confidence aware Tangle	Public	The protection of the orphan tips	Not mentioned	Not mentioned	Medium	Low

Table 4
Comparison of the studied secure and lightweight consensus mechanisms (2).

Solution	Based on existing consensus algorithm	New secure consensus	Addressed issue	Type of Blockchain	Main security policy	Authent. of participants	Protection against DoS attacks	Security-related overhead	Block validation latency
G. Bu et al. [78]	IOTA Tangle	/	Secure and efficient IOTA and G-IOTA	Public	Variable tip selection parameters	Not mentioned	Good	Low	Low
A. Carelli et al. [80]	IOTA Tangle	/	Securing IoT data exchange in IOTA-based blockchain	Public	Cryptographic IOTA-Tangle with the adoption of Hardware Secure Element	Ensured by the Masked Authenticated Messaging protocol	Good	Medium	Medium
Y. Chen et al. [82]	IOTA Tangle	/	Tangle security against fake branches and double spending problems in the DAG	Public	Estimation of the probability of the vulnerability with the detection of malicious branches with threshold security technique.	Not mentioned	Medium	Low	Low
S.A.P. Kumar et al. [83]	IOTA Tangle	/	Intrusions in Tangle process	Private	Machine learning-based intrusion detection system to classify IOTA DAG's data	Ensured	Good	Low	Not mentioned

4.4. Application-specific consensus mechanisms

From an application perspective, researchers have developed specialized consensus algorithms to adapt Blockchain technology to specific application domains within the IoT. The primary goal of these application-specific consensus mechanisms is to account for the unique requirements and challenges of particular applications during the block validation process. In this section, we examine the existing application-aware consensus mechanisms proposed for Blockchain-enabled IoT systems.

4.4.1. E-health-driven consensus mechanisms

E-health is one of the most significant IoT applications, generating vast amounts of sensitive data that must be handled and aggregated securely while protecting the privacy of data owners. Therefore, the consensus mechanisms proposed for Blockchain-enabled medical IoT should address these requirements. Additionally, they must ensure the trustworthiness and authentication of the participating consensus nodes (validators). An E-health-oriented consensus algorithm is proposed in [97]. This mechanism is built on private or consortium Blockchains specifically deployed to securely manage medical data. In this context, a lightweight proof of conformance consensus is proposed, where the core operation involves accepting only blocks generated by authorized doctors and patients. This consensus can also be achieved by creating a secure token for each registered user of the E-health application. Another consensus mechanism tailored for E-health applications in the IoBT is presented in [98]. This mechanism, referred to as the Rampant Smoothing Algorithm, is designed for deployment on private Blockchains. The core operation of the proposed consensus mechanism enables validators to collaborate through a judgment system that evaluates the communication of Blockchained medical data. Consensus is reached when the overall judgments made by the participating validators are positive. It is claimed that this medical consensus mechanism enhances the QoS parameters of the block validation process, particularly those related to validation throughput and energy consumption.

In [99], the Proof of Epidemiology-of-Interest (PoEoI) mechanism is proposed to support IoT-connected medical applications. This mechanism designates each hospital as a trusted consensus node, with its computing infrastructure responsible for gathering medical information and constructing blockchain blocks. Block validation is performed based on an epidemiological data dissemination policy, where each validator verifies the signatures within a newly created block. Upon successful validation, the block is broadcast to the other trusted nodes (validators) deployed across participating hospitals. It is noteworthy that the trusted nodes mutually evaluate their credibility, and the entire system employs a consortium blockchain to prevent unauthorized users from accessing the blockchain. In the same context, the authors of [100] proposed a consensus mechanism tailored for healthcare applications. Their proposed consensus mechanism ensures transaction approval alongside smart classification using Neural Networks (NN). Specifically, the transactions are systematically generated from medical records produced by various WBAN (Wireless Body Area Network) sensors. Although the solution appears promising due to its integration of AI into the consensus process, it lacks sufficient details about the entities that act as block miners or validators. Additionally, it remains unclear whether these entities should be located within hospitals, near the patients, or at an intermediary point.

Considering the nature of the application and the sensitivity of the data it processes, consortium or private blockchains appear to be the most suitable choice. These blockchain solutions provide acceptable levels of inherent security and address scalability concerns effectively. However, this approach should not become a universal standard for e-health applications. Blockchains can be selectively opened to contextual participants, enabling better integration with IoT environments while maintaining security and privacy requirements. Moreover, consensus mechanisms, whether operation-driven or based on IOTA's Tangle, can be tailored to meet the specific needs of IoBT-enabled healthcare applications [101], [102], [103].

4.4.2. Industrial applications-driven consensus mechanisms

In [104], a consensus mechanism for Blockchain-enabled Industrial Internet of Things (IIoT) applications is presented. The researchers propose using a permissioned (private) Blockchain for such applications and introduce a consensus mechanism that automatically discards malicious production transactions, approving only the legitimate ones. Since the Blockchain is private, the block validation process is restricted to authorized entities. Moreover, the proposed consensus has been trained on several relevant datasets, and the evaluation results demonstrate the mechanism's ability to accept and validate only legitimate transactions. An adaptation of the Delegated Proof of Stake (DPoS) consensus mechanism for Blockchained IIoT is presented in [105]. Trade nodes generate transactions, while consensus nodes construct and validate blocks. In addition to ordinary voting nodes, the solution introduces a second type of voting node: honor nodes, which have special voting priorities and can even replace ordinary nodes in the event of failure or poor performance. Consensus is achieved when the consensus node (either ordinary or honor) with the highest stake and votes is selected to validate the current block. As noted earlier, Proof of Stake (PoS) is recognized for being resource-efficient despite its drawbacks. Furthermore, the proposed improvement to the consensus mechanism has resulted in reduced block validation latency.

In [106], the authors propose a lightweight Proof of Chance (PoCh) mechanism tailored for the Industrial Internet of Things (IIoT). It uses chance rather than cryptographic puzzles, and the operation is divided into rounds. In each round, only one miner is selected based on randomized conditions. PoCh offers the advantage of being highly scalable, with strong fault tolerance, making it well-suited for industrial environments. The authors in [107] and [108] also explore the Tangle's Directed Acyclic Graph (DAG)-based consensus for permissioned (private) Blockchain-enabled IIoT systems. Their findings indicate that using such a consensus mechanism in IIoT ecosystems ensures lightweight and real-time block validation. Additionally, another work [109] proposes a green consensus mechanism specifically designed for the IIoT. Unlike most existing consensus mechanisms for IIoT, the proposed solution is based on a public Blockchain and is open to all IIoT devices. The block validation strategy is both collaborative and incentive. Each participating miner is assigned a collaboration index, which reflects their block mining activities.

4.4.3. Smart agriculture-driven consensus mechanisms

Smart agriculture (or smart farming) is a promising IoT application where blockchain technology is being successfully implemented. In fact, blockchain applications in the smart agriculture domain have two main use cases: food tracking/traceability and goods trading. In [110], the authors propose a platform for a permissionless (public) blockchain-based marketplace, where the block validation process is carried out using the PoW consensus. Authors in [111] have studied the applicability of existing consensus algorithms, such as PoW, PoS, PoA, PoC, etc., for smart farming-oriented blockchains. However, the study does not discuss how consensus mechanisms operating over other distributed ledgers (e.g., IOTA's DAG-based Tangle consensus) could be applied in smart agriculture environments. In [112], the authors propose the use of a cloud-powered PoW consensus to approve blocks of agricultural transactions generated by deployed IoT devices.

Authors in [113] have conducted a study on the suitability of consensus mechanisms for blockchain-enabled smart agriculture. They found that PoW and PoS-based consensus schemes are suitable for permissionless blockchains, while the Raft consensus [114] is more recommended for permissioned agriculture-oriented blockchains. Raft is a leader-follower consensus mechanism initially designed for classical distributed systems that promotes fault tolerance and enhances transaction validation rates. Consensus is achieved in Raft when a group of members, governed by a single cluster leader, agree on the validity of transactions. In general, the study favors permissioned blockchains over permissionless ones, as smart agriculture applications often require rapid validation of sensitive data. Unlike most IOTA-based solutions that are permissionless, the authors in [115] propose using Tangle consensus in permissioned IOTA-based smart farming ecosystems for a secure, lightweight, and energy-efficient block approval process.

4.4.4. Smart city-driven consensus mechanisms

A smart city is a unique application of IoT, where a large number of devices are interconnected through complex and pervasive communication technologies that must primarily support network scalability, real-time communications, high mobility of end users, and strong privacy protection. In this context, centralized solutions and infrastructures may not meet these requirements. Consequently, fully distributed, blockchain-based, and IoT-enabled smart city applications are likely to achieve significant success. In this section, we examine several relevant consensus mechanisms driven by smart city needs.

Authors in [116] proposed a post-quantum Proof of Work (PoW) consensus mechanism to meet the security requirements of smart city applications. Unlike the standard PoW, which relies on Secure Hash Algorithms (SHA) that are relatively weak and vulnerable to powerful quantum attacks targeting the block validation process, the proposed variant utilizes problems such as solving multivariate quadratic equations, which are more complex and resistant to quantum-based attacks. Additionally, the solution employs identity-based signatures for lightweight security of transactions. It is important to note that the complexity of the mining operation is unsuitable for IoT devices. However, this issue is mitigated in the proposed solution, as the blockchain type is public, and participating miners can leverage powerful entities to solve the intricate mining puzzles. In [117], a new consensus algorithm called Proof of Witness Presence is proposed. This algorithm is designed for smart city applications, aiming to improve secure, tamper-proof, and automated decision-making by citizens, particularly in political contexts. The proposed consensus is claimed to provide real-time, privacy-preserving block validation over a fully distributed blockchain, which aligns well with the requirements of smart city applications. The solution also leverages crowdsensing in a smart city for transaction processing and social proof mining.

In [118], the authors present a selective consensus mechanism for smart monitoring in smart city applications. In this solution, a central entity (a gateway) hosted on the fog network selects miners based on performance-related criteria. The solution adopts a PoW-like consensus, except that the block construction is performed by the gateway entity, which gathers smart city monitoring transactions from the deployed IoT sensors and sends the newly constructed block to the selected miner. The miner computes and appends the appropriate block hash and disseminates the newly validated block to the blockchain network. Note that the miners can be any participating hosts with sufficiently powerful capabilities. The assessment results show that the solution outperforms the standard PoW process, especially when the gateway assigns one block to a group of miners at a time for parallelized validation. Despite the potential advantages introduced by a central gateway that controls block construction and miner selection in specific smart city applications, the concept still carries the risk of reviving traditional problems associated with centralized architectures, particularly those related to security.

Another promising solution is proposed in [119]. The introduced consensus mechanism takes into account important aspects of smart city applications, such as transaction priority and transaction fees for mining. Validators are organized into clusters, where the leader and its followers cooperate to validate blocks. Cluster leaders are selected based on a machine learning-based model. Unlike most consensus mechanisms designed for smart cities, which tend to be permissionless, this solution suggests the use of permissioned blockchains due to their security-related benefits. The authors in [120] introduce a set of lightweight consensus protocols tailored for vehicular social networks. These protocols eliminate the need for puzzle-solving and cryptocurrency systems. The solution addresses different scenarios, considering communication reliability and static vehicle grouping. The consensus problem is resolved through private and public chains, with a seamless bridging scheme between them.

Besides these classes of application-aware consensus mechanisms for IoT, a few consensus mechanisms have been proposed for blockchain-dedicated applications, as seen in [121], [122], [123], and [124].

In Table 5, we present a general comparison of the classes of application-oriented consensus mechanisms proposed for the IoBT.

Table 5
General comparison of the classes of application-driven consensus solutions in the Internet of Blockchained Things.

IoT application	Dominant Blockchain type	Consensus operation	Miners/Validators
E-health	Permissioned	Check whether the Block transactions are generated by the authorized hospitals and/or application actors (doctors and patients).	Hospital's computing entities
Industry	Permissioned	Adaptation of PoS, voting and incentive-based consensus mechanisms.	Industry's computing entities.
Smart agriculture	Permissioned and permissionless	Adoption of PoW and PoS consensus mechanisms. Farm's computing entities or IoT nodes.	
Smart city	Permissionless	Improved or PoW-like consensus mechanisms. Novel Proof-based consensus or cooperative and clustered consensus mechanisms	Any powerful participating hosts.

5. Conclusion and open issues

Blockchain technology has recently emerged as a groundbreaking security solution for IoT networks and applications. This concept seeks to replace traditional security architectures that depend on trusted servers and third parties. While blockchain technology may not solve all IoT challenges, it offers a fully distributed security alternative to the centralized or semi-centralized solutions that dominate the current Internet and IoT landscape. The consensus process is particularly significant, as it is regarded as a key element for the successful integration of blockchain into IoT platforms. Consequently, developing mechanisms that efficiently address constraints-awareness and QoS provisioning, while validating the transactions generated by IoT devices, represents a critical area of research.

Throughout this review paper, we have presented a comprehensive analysis of consensus mechanisms designed for the Internet of Blockchained Things (IoBT). The study began with an in-depth exploration of consensus mechanisms, categorized based on their operational principles and constraint-awareness. Given the critical need for Blockchain technology to remain secure against potential threats, particularly those targeting the consensus process, the review also examined existing secure consensus mechanisms and the specific attacks they are designed to mitigate. Furthermore, the study included an analysis of AI-empowered block evaluation, despite the fact that smart consensus mechanisms are not yet fully mature. Lastly, we discussed consensus mechanisms that have been specifically designed or adapted to address the unique requirements of IoT applications.

Despite significant adaptation efforts to enable the use of traditional, constraint-agnostic consensus mechanisms in IoT environments, tailored consensus mechanisms designed specifically for the Internet of Blockchained Things (e.g., IOTA's Tangle consensus) appear to be far more suitable for IoT applications. However, the issues raised—particularly those related to security—must be effectively addressed. Moreover, while most existing application-oriented consensus mechanisms are private, which aligns with many security considerations, this approach may conflict with the inherently public nature of IoT, as well as its federated standards and infrastructures. Ultimately, the development of IoBT-specific consensus mechanisms that effectively address constraint awareness, QoS and smartness requirements, security challenges, and application-specific needs is strongly recommended.

CRediT authorship contribution statement

Somia Sahraoui: Writing – review & editing, Writing – original draft. **Abdelmalik Bachir:** Writing – review & editing, Writing – original draft, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H.-N. Dai, Z. Zheng, Y. Zhang, Blockchain for internet of things: a survey, IEEE Internet Things J. 6 (5) (2019) 8076–8094.
[2] A. Hameed, A. Alomary, Security issues in iot: a survey, in: 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies, 3ICT, IEEE, 2019, pp. 1–5.
[3] R. Rudman, R. Bruwer, Defining web 3.0: opportunities and challenges, Electron. Libr. 34 (1) (2016) 132–154.
[4] B. Rababah, T. Alam, R. Eskicioglu, The next generation internet of things architecture towards distributed intelligence: reviews, applications, and research challenges, J. Telecommun. Electron. Comput. Eng. 12 (2) (2020).
[5] M. Di Pierro, What is the blockchain?, Comput. Sci. Eng. 19 (5) (2017) 92–95.
[6] Q. He, N. Guan, M. Lv, W. Yi, On the consensus mechanisms of blockchain/dlt for internet of things, in: 2018 IEEE 13th International Symposium on Industrial Embedded Systems, SIES, IEEE, 2018, pp. 1–10.
[7] M. Salimitari, M. Chatterjee, A survey on consensus protocols in blockchain for iot networks, arXiv preprint, arXiv:1809.05613.
[8] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, Y. Yang, A survey of iot applications in blockchain systems: architecture, consensus, and traffic modeling, ACM Comput. Surv. 53 (1) (2020) 1–32.
[9] A.M. de Morais, F.A.A. Lins, N.S. Rosa, Survey on integration of consensus mechanisms in iot-based blockchains, J. Univers. Comput. Sci. 29 (10) (2023) 1139.
[10] M. Nofer, P. Gomber, O. Hinz, D. Schiereck, Blockchain, Bus. Inf. Syst. Eng. 59 (2017) 183–187.
[11] M. Wohrer, U. Zdun, Smart contracts: security patterns in the ethereum ecosystem and solidity, in: 2018 International Workshop on Blockchain Oriented Software Engineering, IWBOSE, IEEE, 2018, pp. 2–8.
[12] S. Tikhomirov, Ethereum: state of knowledge and research perspectives, in: Foundations and Practice of Security: 10th International Symposium, FPS 2017, Nancy, France, October 23–25, 2017, in: Revised Selected Papers, vol. 10, Springer, 2018, pp. 206–221.
[13] A. Arooj, M.S. Farooq, T. Umer, Unfolding the blockchain era: timeline, evolution, types and real-world applications, J. Netw. Comput. Appl. 207 (2022) 103511.
[14] H. Vranken, Sustainability of bitcoin and blockchains, Curr. Opin. Environ. Sustain. 28 (2017) 1–9.
[15] S. Ferretti, G. D'Angelo, On the ethereum blockchain structure: a complex networks theory perspective, Concurr. Comput. 32 (12) (2020) e5493.
[16] S. Pongnumkul, C. Siripanpornchana, S. Thajchayapong, Performance analysis of private blockchain platforms in varying workloads, in: 2017 26th International Conference on Computer Communication and Networks, ICCCN, IEEE, 2017, pp. 1–6.
[17] O. Dib, K.-L. Brousmiche, A. Durand, E. Thea, E.B. Hamida, Consortium blockchains: overview, applications and challenges, Int. J. Adv. Telecommun. 11 (1) (2018) 51–64.
[18] A. Alkhateeb, C. Catal, G. Kar, A. Mishra, Hybrid blockchain platforms for the internet of things (iot): a systematic literature review, Sensors 22 (4) (2022) 1304.
[19] M. Alshaikhli, T. Elfouly, O. Elharrouss, A. Mohamed, N. Ottakath, Evolution of internet of things from blockchain to iota: a survey, IEEE Access 10 (2021) 844–866.
[20] A.A. Khan, A.A. Laghari, Z.A. Shaikh, Z. Dacko-Pikiewicz, S. Kot, Internet of things (iot) security with blockchain technology: a state-of-the-art review, IEEE Access (2022).
[21] C. Liang, B. Shanmugam, S. Azam, A. Karim, A. Islam, M. Zamani, S. Kavianpour, N.B. Idris, Intrusion detection system for the internet of things based on blockchain and multi-agent systems, Electronics 9 (7) (2020) 1120.
[22] H.B. Patel, D.C. Jinwala, 6mid: mircochain based intrusion detection for 6lowpan based iot networks, Proc. Comput. Sci. 184 (2021) 929–934.
[23] S. Mishra, A.K. Tyagi, Intrusion detection in internet of things (iots) based applications using blockchain technology, in: 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC, IEEE, 2019, pp. 123–128.
[24] S.S. Mathew, K. Hayawi, N.A. Dawit, I. Taleb, Z. Trabelsi, Integration of blockchain and collaborative intrusion detection for secure data transactions in industrial iot: a survey, Clust. Comput. 25 (6) (2022) 4129–4149.

[25] R.F. Mansour, Blockchain assisted clustering with intrusion detection system for industrial internet of things environment, Expert Syst. Appl. 207 (2022) 117995.

[26] S. He, W. Ren, T. Zhu, K.-K.R. Choo, Bosmos: a blockchain-based status monitoring system for defending against unauthorized software updating in industrial internet of things, IEEE Internet Things J. 7 (2) (2019) 948–959.

[27] S. Mishra, Blockchain-based security in smart grid network, Int. J. Commun. Netw. Distrib. Syst. 28 (4) (2022) 365–388.

[28] B. Hu, C. Zhou, Y.-C. Tian, Y. Qin, X. Junping, A collaborative intrusion detection approach using blockchain for multimicrogrid systems, IEEE Trans. Syst. Man Cybern. Syst. 49 (8) (2019) 1720–1730.

[29] A.M. Alkhiari, S. Mishra, M. AlShehri, Blockchain-based sqkd and ids in edge enabled smart grid network, Comput. Mater. Continua 70 (2) (2022).

[30] A.Z. Ourad, B. Belgacem, K. Salah, Using blockchain for iot access control and authentication management, in: Internet of Things—ICIOT 2018: Third International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25–30, 2018, in: Proceedings, vol. 3, Springer, 2018, pp. 150–164.

[31] D. Li, W. Peng, W. Deng, F. Gai, A blockchain-based authentication and security mechanism for iot, in: 2018 27th International Conference on Computer Communication and Networks, ICCCN, IEEE, 2018, pp. 1–6.

[32] U. Khalid, M. Asim, T. Baker, P.C. Hung, M.A. Tariq, L. Rafferty, A decentralized lightweight blockchain-based authentication mechanism for iot systems, Clust. Comput. 23 (3) (2020) 2067–2087.

[33] B. Yu, J.K. Liu, A. Sakzad, S. Nepal, R. Steinfeld, P. Rimba, M.H. Au, Platform-independent secure blockchain-based voting system, in: Information Security: 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, in: Proceedings, vol. 21, Springer, 2018, pp. 369–386.

[34] J. Lin, Z. Shen, C. Miao, Using blockchain technology to build trust in sharing lorawan iot, in: Proceedings of the 2nd International Conference on Crowd Science and Engineering, 2017, pp. 38–43.

[35] S. Malik, V. Dedeoglu, S.S. Kanhere, R. Jurdak, Trustchain: trust management in blockchain and iot supported supply chains, in: 2019 IEEE International Conference on Blockchain, Blockchain, IEEE, 2019, pp. 184–193.

[36] J. Pan, J. McElhannon, Future edge cloud and edge computing for internet of things applications, IEEE Internet Things J. 5 (1) (2017) 439–449.

[37] O.I. Khalaf, G.M. Abdulsahib, Optimized dynamic storage of data (odsd) in iot based on blockchain for wireless sensor networks, Peer-to-Peer Netw. Appl. 14 (2021) 2858–2873.

[38] G. Wang, Z. Shi, M. Nixon, S. Han, Chainsplitter: towards blockchain-based industrial iot architecture for supporting hierarchical storage, in: 2019 IEEE International Conference on Blockchain, Blockchain, IEEE, 2019, pp. 166–175.

[39] C. Li, J. Zhang, X. Yang, L. Youlong, Lightweight blockchain consensus mechanism and storage optimization for resource-constrained iot devices, Inf. Process. Manag. 58 (4) (2021) 102602.

[40] T. Kim, J. Noh, S. Cho, Scc: storage compression consensus for blockchain in lightweight iot network, in: 2019 IEEE International Conference on Consumer Electronics, ICCE, IEEE, 2019, pp. 1–4.

[41] D. Li, Y. Hu, M. Lan, Iot device location information storage system based on blockchain, Future Gener. Comput. Syst. 109 (2020) 95–102.

[42] Y. Li, J. Wang, H. Zhang, A survey of state-of-the-art sharding blockchains: models, components, and attack surfaces, J. Netw. Comput. Appl. (2023) 103686.

[43] H. Chai, S. Leng, Y. Chen, K. Zhang, A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles, IEEE Trans. Intell. Transp. Syst. 22 (7) (2020) 3975–3986.

[44] A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of work blockchains, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 3–16.

[45] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Lsb: a lightweight scalable blockchain for iot security and anonymity, J. Parallel Distrib. Comput. 134 (2019) 180–197.

[46] N. Lasla, L. Al-Sahan, M. Abdallah, M. Younis, Green-pow: an energy-efficient blockchain proof-of-work consensus algorithm, Comput. Netw. 214 (2022) 109118.

[47] G. Kumar, R. Saha, M.K. Rai, R. Thomas, T.-H. Kim, Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics, IEEE Internet Things J. 6 (4) (2019) 6835–6842.

[48] C.P. Jayabal, P.R. Sathia Bhama, Performance analysis on diversity mining-based proof of work in bifolded consortium blockchain for internet of things consensus, Concurr. Comput. 33 (16) (2021) e6285.

[49] Q. Qu, R. Xu, Y. Chen, E. Blasch, A. Aved, Enable fair proof-of-work (pow) consensus for blockchains in iot by miner twins (mint), Future Internet 13 (11) (2021) 291.

[50] C.T. Nguyen, D.T. Hoang, D.N. Nguyen, D. Niyato, H.T. Nguyen, E. Dutkiewicz, Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities, IEEE Access 7 (2019) 85727–85745.

[51] M. Snider, K. Samani, T. Jain, Delegated proof of stake: features & tradeoffs, Multicoin Cap. 19 (2018) 1–19.

[52] S.R. Niya, E. Schiller, I. Cepilov, F. Maddaloni, K. Aydinli, T. Surbeck, T. Bocek, B. Stiller, Adaptation of proof-of-stake-based blockchains for iot data streams, in: 2019 IEEE International Conference on Blockchain and Cryptocurrency, ICBC, IEEE, 2019, pp. 15–16.

[53] X. Fan, Q. Chai, Roll-dpos: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems, in: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2018, pp. 482–484.

[54] J. Mišić, V.B. Mišić, X. Chang, Optimal multi-tier clustering of permissioned blockchain systems for iot, IEEE Trans. Veh. Technol. 71 (3) (2022) 2293–2304.

[55] X. Tang, X. Lan, L. Li, Y. Zhang, Z. Han, Incentivizing proof-of-stake blockchain for secured data collection in uav-assisted iot: a multi-agent reinforcement learning approach, IEEE J. Sel. Areas Commun. 40 (12) (2022) 3470–3484.

[56] S. Hassan, R. Mihalcea, C. Banea, Random walk term weighting for improved text classification, Int. J. Semant. Comput. 1 (04) (2007) 421–439.

[57] M. Bhandary, M. Parmar, D. Ambawade, A blockchain solution based on directed acyclic graph for iot data security using iota tangle, in: 2020 5th International Conference on Communication and Electronics Systems, ICCES, IEEE, 2020, pp. 827–832.

[58] B. Shabandri, P. Maheshwari, Enhancing iot security and privacy using distributed ledgers with iota and the tangle, in: 2019 6th International Conference on Signal Processing and Integrated Networks, SPIN, IEEE, 2019, pp. 1069–1075.

[59] S. Rochman, J.E. Istiyanto, A. Dharmawan, V. Handika, S.R. Purnama, Optimization of tips selection on the iota tangle for securing blockchain-based iot transactions, Proc. Comput. Sci. 216 (2023) 230–236.

[60] R. Soltani, L. Saxena, R. Joshi, S. Sampalli, Protecting routing data in wsns with use of iota tangle, Proc. Comput. Sci. 203 (2022) 197–204.

[61] https://v2.iota.org/, 2023. (Accessed 30 July 2023).

[62] M.A. Kumar, V. Radhesyam, B. SrinivasaRao, Front-end iot application for the bitcoin based on proof of elapsed time (poet), in: 2019 Third International Conference on Inventive Systems and Control, ICISC, IEEE, 2019, pp. 646–649.

[63] M. Salimitari, M. Chatterjee, Y.P. Fallah, A survey on consensus methods in blockchain for resource-constrained iot networks, Internet of Things 11 (2020) 100212.

[64] M.A. Manolache, S. Manolache, N. Tapus, Decision making using the blockchain proof of authority consensus, Proc. Comput. Sci. 199 (2022) 580–588.

[65] N. Andola, S. Venkatesan, S. Verma, et al., Poewal: a lightweight consensus mechanism for blockchain in iot, Pervasive Mob. Comput. 69 (2020) 101291.

[66] M.U. Zaman, T. Shen, M. Min, Proof of sincerity: a new lightweight consensus approach for mobile blockchains, in: 2019 16th IEEE Annual Consumer Communications & Networking Conference, CCNC, IEEE, 2019, pp. 1–4.

[67] Z. Zhang, D. Zhu, W. Fan, Qpbft: practical byzantine fault tolerance consensus algorithm based on quantified-role, in: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom, IEEE, 2020, pp. 991–997.

[68] O. Onireti, L. Zhang, M.A. Imran, On the viable area of wireless practical byzantine fault tolerance (pbft) blockchain networks, in: 2019 IEEE Global Communications Conference, GLOBECOM, IEEE, 2019, pp. 1–6.

[69] O. Alfandi, S. Otoum, Y. Jararweh, Blockchain solution for iot-based critical infrastructures: Byzantine fault tolerance, in: NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2020, pp. 1–4.

[70] R. Zhang, R. Xue, L. Liu, Security and privacy on blockchain, ACM Comput. Surv. 52 (3) (2019) 1–34.

[71] F.A. Aponte-Novoa, A.L.S. Orozco, R. Villanueva-Polanco, P. Wightman, The 51% attack on blockchains: a mining behavior study, IEEE Access 9 (2021) 140549–140564.

[72] P. Gaži, A. Kiayias, A. Russell, Stake-bleeding attacks on proof-of-stake blockchains, in: 2018 Crypto Valley Conference on Blockchain Technology, CVCBT, IEEE, 2018, pp. 85–92.

[73] K.D. Gupta, A. Rahman, S. Poudyal, M.N. Huda, M.P. Mahmud, A hybrid pow-pos implementation against 51 percent attack in cryptocurrency system, in: 2019 IEEE International Conference on Cloud Computing Technology and Science, CloudCom, IEEE, 2019, pp. 396–403.

[74] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, H. Karimipour, S.R. Karizno, Slpow: secure and low latency proof of work protocol for blockchain in green iot networks, in: 2020 IEEE 91st Vehicular Technology Conference, VTC2020-Spring, IEEE, 2020, pp. 1–5.

[75] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, P. Zeng, Towards secure industrial iot: blockchain system with credit-based consensus mechanism, IEEE Trans. Ind. Inform. 15 (6) (2019) 3680–3689.

[76] W. Li, S. Andreina, J.-M. Bohli, G. Karame, Securing proof-of-stake blockchain protocols, in: Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT DPM 2017 and CBT 2017, Oslo, Norway, September 14–15, 2017, in: Proceedings, Springer, 2017, pp. 297–315.

[77] G. Bu, Ö. Gürcan, M. Potop-Butucaru, G-iota: fair and confidence aware tangle, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, IEEE, 2019, pp. 644–649.

[78] G. Bu, W. Hana, M. Potop-Butucaru, E-iota: an efficient and fast metamorphism for iota, in: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services, BRAINS, IEEE, 2020, pp. 9–16.

[79] Q. Bramas, Efficient and secure tsa for the tangle, in: International Conference on Networked Systems, Springer, 2021, pp. 161–166.

[80] A. Carelli, A. Palmieri, A. Vilei, F. Castanier, A. Vesco, Enabling secure data exchange through the iota tangle for iot constrained devices, Sensors 22 (4) (2022) 1384.

[81] P. Gangwani, A. Perez-Pons, T. Bhardwaj, H. Upadhyay, S. Joshi, L. Lagos, Securing environmental iot data using masked authentication messaging protocol in a dag-based blockchain: IOTA tangle, Future Internet 13 (12) (2021) 312.

[82] Y. Chen, Y. Guo, Y. Wang, R. Bie, Toward prevention of parasite chain attack in iota blockchain networks by using evolutionary game model, Mathematics 10 (7) (2022) 1108.

[83] S.A. Kumar, N. Ahmed, A. Bikos, Swiota: anomaly detection for distributed ledger technology-based internet of things (iota) using sliding window (sw) technique, in: IFIP International Internet of Things Conference, Springer, 2022, pp. 177–194.

[84] S. Maitra, V.P. Yanambaka, D. Puthal, A. Abdelgawad, K. Yelamarthi, Integration of internet of things and blockchain toward portability and low-energy consumption, Trans. Emerg. Telecommun. Technol. 32 (6) (2021) e4103.

[85] E.K. Wang, Z. Liang, C.-M. Chen, S. Kumari, M.K. Khan, Porx: a reputation incentive scheme for blockchain consensus of iiot, Future Gener. Comput. Syst. 102 (2020) 140–151.

[86] J. Zou, B. Ye, L. Qu, Y. Wang, M.A. Orgun, L. Li, A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services, IEEE Trans. Serv. Comput. 12 (3) (2018) 429–445.

[87] Y. Wu, L. Song, L. Liu, J. Li, X. Li, L. Zhou, Consensus mechanism of iot based on blockchain technology, Shock Vib. 2020 (2020) 1–9.

[88] F.O. Olowononi, D.B. Rawat, C. Liu, Resilient machine learning for networked cyber physical systems: a survey for machine learning security to securing machine learning for cps, IEEE Commun. Surv. Tutor. 23 (1) (2020) 524–552.

[89] A. Qayyum, J. Qadir, M. Bilal, A. Al-Fuqaha, Secure and robust machine learning for healthcare: a survey, IEEE Rev. Biomed. Eng. 14 (2020) 156–180.

[90] C.L. Stergiou, A.P. Plageras, K.E. Psannis, B.B. Gupta, Secure machine learning scenario from big data in cloud computing via internet of things network, in: Handbook of Computer Networks and Cyber Security: Principles and Paradigms, 2020, pp. 525–554.

[91] F. Bravo-Marquez, S. Reeves, M. Ugarte, Proof-of-learning: a blockchain consensus mechanism based on machine learning competitions, in: 2019 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPCON, IEEE, 2019, pp. 119–124.

[92] T. Abhiroop, S. Babu, B. Manoj, A machine learning consensus based light-weight blockchain architecture for internet of things, in: 2022 14th International Conference on COMmunication Systems & NETworkS, COMSNETS, IEEE, 2022, pp. 1–6.

[93] K. Saadat, N. Wang, R. Tafazolli, Ai-enabled blockchain consensus node selection in cluster-based vehicular networks, IEEE Netw. Lett. (2023).

[94] R. Schmid, B. Pfitzner, J. Beilharz, B. Arnrich, A. Polze, Tangle ledger for decentralized learning, in: 2020 IEEE International Parallel and Distributed Processing Symposium Workshops, IPDPSW, IEEE, 2020, pp. 852–859.

[95] Y. Zhao, Y. Qu, Y. Xiang, Y. Zhang, L. Gao, A lightweight model-based evolutionary consensus protocol in blockchain as a service for iot, IEEE Trans. Serv. Comput. (2023).

[96] W. Li, Q. Zhang, S. Deng, B. Zhou, B. Wang, J. Cao, Q-learning improved lightweight consensus algorithm for blockchain-structured internet of things, IEEE Internet Things J. (2023).

[97] S. Zhang, J.-H. Lee, Analysis of the main consensus protocols of blockchain, ICT Express 6 (2) (2020) 93–97.

[98] U. Tariq, Rampant smoothing (rts) algorithm: an optimized consensus mechanism for private blockchain enabled technologies, EURASIP J. Wirel. Commun. Netw. 2022 (1) (2022) 1–22.

[99] O. Samuel, A.B. Omojo, S.M. Mohsin, P. Tiwari, D. Gupta, S.S. Band, An anonymous iot-based e-health monitoring system using blockchain technology, IEEE Syst. J. (2022).

[100] I. Benkhaddra, A. Kumar, M.A. Setitra, L. Hang, Design and development of consensus activation function enabled neural network-based smart healthcare using biot, Wirel. Pers. Commun. 130 (3) (2023) 1549–1574.

[101] E.S. Rydningen, E. Åsberg, L. Jaccheri, J. Li, Advantages and opportunities of the iota tangle for health data management: a systematic mapping study, in: Proceedings of the 5th International Workshop on Emerging Trends in Software Engineering for Blockchain, 2022, pp. 9–16.

[102] J.P. Dias, H. Sereno Ferreira, Â. Martins, A blockchain-based scheme for access control in e-health scenarios, in: Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition, SoCPaR 2018, vol. 10, Springer, 2020, pp. 238–247.

[103] R. Zou, X. Lv, J. Zhao, Spchain: blockchain-based medical data sharing and privacy-preserving ehealth system, Inf. Process. Manag. 58 (4) (2021) 102604.

[104] M. Arifeen, T. Ghosh, R. Islam, A. Ashiquzzaman, J. Yoon, J. Kim, Autoencoder based consensus mechanism for blockchain-enabled industrial internet of things, Internet of Things 19 (2022) 100575.

[105] A. Sasikumar, L. Ravi, K. Kotecha, J.R. Saini, V. Varadarajan, V. Subramaniyaswamy, Sustainable smart industry: a secure and energy efficient consensus mechanism for artificial intelligence enabled industrial internet of things, Comput. Intell. Neurosci. (2022).

[106] M. Kara, A. Laouid, M. Hammoudeh, M. AlShaikh, A. Bounceur, Proof of chance: a lightweight consensus algorithm for the internet of things, IEEE Trans. Ind. Inform. 18 (11) (2022) 8336–8345.

[107] A. Sasikumar, N. Senthilkumar, V. Subramaniyaswamy, K. Kotecha, V. Indragandhi, L. Ravi, An efficient, provably-secure dag based consensus mechanism for industrial internet of things, Int. J. Interact. Des. Manuf. (2022) 1–11.

[108] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, K. Xu, An efficient and compacted dag-based blockchain protocol for industrial internet of things, IEEE Trans. Ind. Inform. 16 (6) (2019) 4134–4145.

[109] Y. Liu, K. Wang, Y. Lin, W. Xu, Lightchain: a lightweight blockchain system for industrial internet of things, IEEE Trans. Ind. Inform. 15 (6) (2019) 3571–3581.

[110] G. Leduc, S. Kubler, J.-P. Georges, Innovative blockchain-based farming marketplace and smart contract performance evaluation, J. Clean. Prod. 306 (2021) 127055.

[111] M.A. Ferrag, L. Shu, X. Yang, A. Derhab, L. Maglaras, Security and privacy for green iot-based agriculture: review, blockchain solutions, and challenges, IEEE Access 8 (2020) 32031–32053.

[112] R. Chaganti, V. Varadarajan, V.S. Gorantla, T.R. Gadekallu, V. Ravi, Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture, Future Internet 14 (9) (2022) 250.

[113] K. Dey, U. Shekhawat, Blockchain for sustainable e-agriculture: literature review, architecture for data management, and implications, J. Clean. Prod. 316 (2021) 128254.

[114] Y. Li, Y. Fan, L. Zhang, J. Crowcroft, Raft consensus reliability in wireless networks: probabilistic analysis, IEEE Internet Things J. (2023).

[115] A.K. Bapatla, S.P. Mohanty, E. Kougianos, sfarm: a distributed ledger based remote crop monitoring system for smart farming, in: IFIP International Internet of Things Conference, Springer, 2021, pp. 13–31.

[116] J. Chen, W. Gan, M. Hu, C.-M. Chen, On the construction of a post-quantum blockchain for smart city, J. Inf. Secur. Appl. 58 (2021) 102780.

[117] E. Pournaras, Proof of witness presence: blockchain consensus for augmented democracy in smart cities, J. Parallel Distrib. Comput. 145 (2020) 160–175.

[118] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, An efficient selective miner consensus protocol in blockchain oriented iot smart monitoring, in: 2019 IEEE International Conference on Industrial Technology, ICIT, IEEE, 2019, pp. 1135–1142.

[119] S.V. Sanghami, J.J. Lee, Q. Hu, Machine-learning-enhanced blockchain consensus with transaction prioritization for smart cities, IEEE Internet Things J. 10 (8) (2022) 6661–6672.

[120] Z. Zheng, J. Pan, L. Cai, Lightweight blockchain consensus protocols for vehicular social networks, IEEE Trans. Veh. Technol. 69 (6) (2020) 5736–5748.

[121] R. Huang, X. Yang, P. Ajay, Consensus mechanism for software-defined blockchain in internet of things, Internet Things Cyber-Phys. Syst. 3 (2023) 52–60.

[122] S. Biswas, K. Sharif, F. Li, S. Maharjan, S.P. Mohanty, Y. Wang, Pobt: a lightweight consensus algorithm for scalable iot business blockchain, IEEE Internet Things J. 7 (3) (2019) 2343–2355.

[123] A.K. Vishwakarma, H. Zhong, Y.N. Singh, Consensus mechanism for peer-to-peer energy trading, in: Recent Trends in Electronics and Communication: Select Proceedings of VCAS 2020, Springer, 2022, pp. 355–364.

[124] S. Chen, H. Mi, J. Ping, Z. Yan, Z. Shen, X. Liu, N. Zhang, Q. Xia, C. Kang, A blockchain consensus mechanism that uses proof of solution to optimize energy dispatch and trading, Nat. Energy 7 (6) (2022) 495–502.