Journal of Universal Computer Science, vol. 29, no. 10 (2023), 1139-1160
submitted: 16/9/2022, accepted: 21/6/2023, appeared: 28/10/2023 CC BY-ND 4.0

Survey on Integration of Consensus Mechanisms in IoT-based Blockchains

Anderson Melo de Morais
(Universidade Federal de Pernambuco, Recife, Brazil
https://orcid.org/0000-0001-7795-7183, amm6@cin.ufpe.br)

Fernando Antonio Aires Lins
(Universidade Federal Rural de Pernambuco, Recife, Brazil
https://orcid.org/0000-0002-4007-3891, fernandoaires@ufrpe.br)

Nelson Souto Rosa
(Universidade Federal de Pernambuco, Recife, Brazil
https://orcid.org/0000-0001-9374-6351, nsr@cin.ufpe.br)

Abstract: While IoT systems are increasingly present in different areas of society, ensuring their data's privacy, security, and inviolability becomes paramount. In this direction, Blockchain has been used to protect the security and immutability of data generated by IoT devices and sensors. At the heart of Blockchain solutions, consensus algorithms are crucial in ensuring the security of creating and writing data in new blocks. Choosing which consensus algorithms to utilise is critical because of a fundamental tradeoff between their security strength and response time. However, recent surveys of consensus mechanisms for IoT-based Blockchain focused on individually using and analysing these algorithms. Investigating the integration between these algorithms to address IoT-specific requirements better is a promising approach. In this context, this paper presents a literature review that explains and discusses consensus algorithms in IoT environments and their combinations. The review analyses eight dimensions that help understand existing proposals: ease of integration, scalability, latency, throughput, power consumption, configuration issues, integrated algorithms, and adversary tolerance. The final analysis also suggests and discusses open challenges in integrating multiple consensus algorithms considering the particularities of IoT systems.

Keywords: Internet of Things, Blockchain, Consensus Mechanisms, Information Security
Categories: H.3.1, H.3.2, H.3.3, H.3.7, H.5.1
DOI: 10.3897/jucs.94929

1 Introduction

The Internet of Things (IoT) has become increasingly present in society, transforming everyday devices into intelligent and autonomous ones [Huang et al. 2023]. IoT elements are now spread out through several areas. Examples of such areas include smart homes (to allow to automate and manage homes remotely), smart cities (to use better resources such as energy, transportation, and water), Industrial IoT (to optimise factory operations, increase efficiency, and reduce costs), and health care (to scan patient health, track remedy use), among several other applications.

IoT devices generate a large amount of data, and applications commonly handle users' data whose sensitivity raises issues about how this data is processed and stored and the security and privacy of users using such devices. In this direction, a technology that has been used to provide security to IoT environments is Blockchain, which utilises cryptographic methods and decentralised data recording to establish data reliability and security [Kamran et al. 2020].

Integrating IoT and Blockchain is difficult because IoT devices have computational resource limitations (e.g., memory, processing capacity, energy), making it challenging to implement the traditional encryption mechanisms used by classic Blockchains. A similar challenge occurs in deciding the consensus algorithm to be used. This algorithm validates new blocks before they are inserted into the chain and is critical to using Blockchain. Adopting suitable algorithms usually has a tradeoff between their security strength and response time.

Currently, approaches suggest integrating more than one consensus algorithm within the same solution to cover several IoT domains and use the most appropriate consensus algorithm in each situation. These integrations are very beneficial as they allow leverage of the strengths of each algorithm while reducing security vulnerabilities. For example, a home monitoring application needs information to be processed quickly and securely. A consensus algorithm that takes several minutes to record the occurrence would not be suitable in this scenario, even though it is very secure.

In this context, this paper surveys existing approaches to integrating consensus algorithms in IoT Blockchains. It presents advances to the state-of-the-art by performing a complete analysis of consensus algorithms, considering some dimensions, such as their ease of integration, scalability, latency, throughput, power consumption, configuration issues, integrated algorithms, and adversary tolerance.

The rest of this paper is organised as follows. Section 2 introduces the main concepts needed to understand the rest of this paper. Next, Section 3 presents existing surveys on using Blockchain for IoT. Section 4 describes this work's main contribution: a literature review on proposals for integrating consensus mechanisms. Section 5 describes the open research challenges of integrating Blockchain consensus mechanisms with IoT. Finally, Section 6 presents the final considerations of the work.

2 Background

This section presents the main concepts and definitions necessary to understand the contributions of this paper.

2.1 Blockchain

Blockchain consists of a mechanism for recording transactions distributed and shared by nodes of a distributed system organised as a peer-to-peer (P2P) network [Monrat et al. 2019]. Blockchain presents itself as a safe environment for recording transactions, as once a new block is added, it cannot be removed or modified without this being noticed by the other nodes throughout the chain.

Some nodes, called miners, perform block validation through a consensus algorithm to confirm transactions and produce new blocks for the chain. In the context of IoT, Blockchain can authenticate, authorise and audit the data generated by devices [Huang et al. 2023]. Due to its decentralised nature, there is no need to trust third parties, which reduces the risk of system failures [Kamran et al. 2020].

Each block has a header that records information relevant to block identification, such as the previous block's hash and the block identification hash. The hash is a numerical code that guarantees that the transaction is valid. Once found, the block can finally be added to the network [Monrat et al. 2019]. Also stored is the root of the Merkle tree in which the block is located. Merkle tree is a type of data structure containing a summary information tree about a larger piece of data [Yu et al. 2020]. The timestamp is also recorded, which records the exact time the block was created.

Figure 1 presents the main structure of Blockchain blocks. The transaction content is stored in the body of the block. Each block in the Blockchain records a reference to the previous one. Hence, the information stored in a block cannot be modified without impacting other blocks. A chained ledger is one of the factors that makes Blockchain networks secure and virtually tamper-proof. The first chain block, the genesis block, is encoded when the network is created and represents the system's initial state.

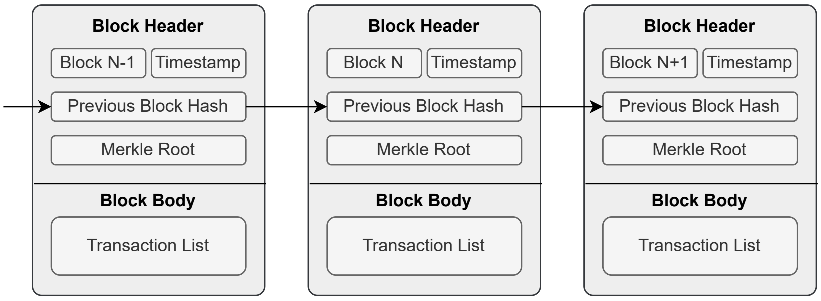

Figure 1: Basic structure of a Blockchain

Blockchain technology can be classified into two main groups: public or open access; and private or authorised access. In a public Blockchain, the access can be anonymous, applications have an open characteristic, and the network follows its rules. Private Blockchains provide access to identified, authenticated, and authorised users.

2.2 Consensus Mechanisms

Consensus mechanisms are techniques to ensure Blockchain security and reliability [Liao and Cheng 2023]. Blockchain technology was initially proposed for other scenarios, such as using cryptocurrencies. However, it was soon realised that a consensus mechanism could be used in different contexts, for example, in IoT, due to its security potential, for which there was a need to adapt existing consensus mechanisms to the context of the IoT.

The first Blockchain adopted Proof of Work (PoW) as a consensus algorithm. PoW has high power consumption and computational resources, such as memory and processing [Monrat et al. 2019]. Hence, other mechanisms have been developed, such as Proof of Stake (PoS), Delegated PoS (DPoS), and Proof of Burn (PoB), among others [Wu et al. 2019].

Over the years, the need arose to design more efficient consensus mechanisms that reduce memory and CPU usage [Hassija et al.2019]. The main consensus algorithms are [Wu et al. 2019] :

- **Proof of Work (PoW)**: Any node in the system can provide computational power to verify transactions. Through a competition mechanism, some nodes can solve a computational puzzle and obtain the reward through the process known as mining. The main disadvantage of PoW is that it has a generally low throughput and usually wastes a considerable amount of computing resources [Sadawi et al. 2021].

- **Proof of Stake (PoS)**: PoS seeks to ensure Blockchain security while reducing consumed resources and improving transaction throughput. PoS is a system in which any participant in the network with a sufficient amount of ”tokens” can use their cryptocurrencies for some time and validate the transactions [Dai et al. 2019].

Currently, there are several variants of PoW and PoS mechanisms [Ali et al. 2018][Lao et al. 2020]:

- **Delegated Proof of Stake (DPoS)**: New blocks are generated by delegate nodes, who sign them with their signature. Delegates are chosen through voting by Blockchain nodes. By selecting delegates, the DPoS algorithm eliminates the need for the transaction to wait for confirmation by all nodes. By reducing confirmation time, transaction speed is significantly improved.

- **Proof of Luck (PoL)**: PoL uses random number generation from a Trusted Execution Environment (TEE) platform to choose a consensus leader. The algorithm offers transaction validation with low latency, deterministic commit time, low power consumption, and equitably distributed mining.

- **Proof of Capacity (PoC)**: PoC uses available hard disk space instead of concurrent computing power. It means that the higher the hard disk space provided, the more likely the mining is to be successful.

- **Proof of Activity (PoA)**: PoA is a combination of PoW and PoS. The mining process starts with nodes looking for a valid hash to create a new block. At first, the process resembles PoW. Once the valid hash is found, it is transmitted to the network, which will verify the solution. The more coins a node has, the more likely it will be chosen to validate the inserted block.

- **Proof of Burn (PoB)**: PoB takes an alternative approach, ”burning” coins into the system instead of using computing resources. PoB works like virtual mining and burning virtual coins. Each miner can write blocks proportionately to the coins it is willing to burn. The more coins the miner burns, the more powerful the mining rigs and the greater the chances of finding a new block.

- **Proof of Importance (PoI):** It seeks to introduce the concept of importance to measure a miner’s ability to create a block. The miner’s number of coins and transactions made and received by that account determines its importance. PoI has efficient power consumption and a high transaction rate [Salimitari et al. 2020].

- **Proof of Elapsed Time (PoET)**: PoET is similar to PoW but with lower power consumption. Before creating a new block, each node receives a time, which is randomly determined. The node chosen to create the new block is the one whose timer expires first. Checking the correctness of timer execution is done using a trusted execution environment (TEE) like Intel’s software guard extension (SGX) [Salimitari et al. 2020].

Another family of consensus algorithms is those based on Byzantine Fault Tolerance and its variants. Byzantine failure occurs when one or more components fail, and there is no accurate information about whether a component has failed or the system information is correct [Qi and Guan 2022]. Therefore, it is necessary to implement strategies to bypass the failure and allow the system to continue working reliably. Hence, some Byzantine fault-tolerant Blockchain consensus algorithms emerged [Lao et al. 2020]:

- **Practical Byzantine Fault Tolerance (PBFT)**: It is considered the first consensus algorithm to handle Byzantine faults asynchronously. A node creates a request and sends it to the other nodes in the network, which forward it to others until a response can be returned after three verification rounds. Even if some node is faulty or malicious, the others continue to run through the verification process. The algorithm provides high throughput and low latency in node validation [Ali et al. 2018].
- **Tendermint**: It consists of a quasi-asynchronous BFT consensus protocol. Tendermint uses PBFT optimally and requires only two rounds of voting to reach a consensus. Tendermint participants are called validators, who take turns proposing transaction blocks and voting on them.
- **Raft**: A non-Byzantine voting-based fault tolerance algorithm is used. While similar to PBFT, it can only tolerate crash failures of up to 50% of nodes, while Byzantine algorithms can tolerate arbitrary corrupted nodes. Raft throughput is limited and has low-security vulnerabilities, so it may not be suitable for IoT networks.
- **Ripple**: The Ripple algorithm uses collectively trusted subnets within the more extensive network to reach a consensus on the Byzantine problem. Ripple transactions use less power than PoW systems, are confirmed in seconds, and cost little computing power.
- **Stellar**: Each node selects a set of trusted nodes in this algorithm. A transaction is sent for verification and will be considered approved if it is authenticated by all nodes that are part of that selected group [Wu et al. 2019]. Stellar is considered the first secure consensus mechanism that enjoys four main properties simultaneously: 1) decentralised control; 2) low latency; 3) flexible trust, and 4) asymptotic safety.

In IoT, consensus algorithms that demand many computational resources and high processing time for each block, such as PoW, may need to be more feasible.

3 Existing Research

Blockchain technology has been used for many applications, including being able to be adapted for use in IoT. Consensus mechanisms are critical components of Blockchains. Wen [Wen et al. 2020] presents systematic research on Blockchain consensus mechanisms in IoT. Initially, the requirements of consensus mechanisms in IoT networks are introduced to understand the connection between Blockchain and IoT consensus mechanisms. Next, Blockchain consensus mechanisms are divided into four categories: consensus mechanisms for security, consensus mechanisms for scalability, consensus mechanisms for energy savings, and consensus mechanisms for performance improvement.

Sadawi [Sadawi et al. 2021] discusses IoT systems' main challenges and the proposals for using Blockchain to solve them. The paper also examines the current integration stage of Blockchain networks with IoT environments. Furthermore, it discusses technical issues related to IoT-Blockchain integration. The research aims to benefit from Blockchain features and services to ensure decentralised data storage and processing and thus address security and anonymity challenges to achieve transparency and efficient authentication service, i.e., highly fault and intruder tolerant.

According to Lao [Lao et al. 2020], IoT security challenges can be solved using Blockchain. However, considering the associated performance challenges, this integration must be done efficiently. Therefore, the authors focus on the main IoT-Blockchain systems and analyse their architectures. The survey proposes a general IoT-Blockchain architecture and compares consensus algorithms and their strengths and weaknesses when applied to IoT. It analyses the current traffic models of P2P and Blockchain systems and proposes a traffic model for IoT-Blockchain systems.

In Blockchain technology, consensus mechanisms are essential in allowing cryptocurrencies such as Bitcoin to maintain consistency and reliability. For Nijsse and Litchfield [Nijsse and Litchfield 2020], to ensure the security and liveliness of a publicly accessible and verifiable Blockchain, fault tolerance must be robust. The authors present a classification of consensus methods applied to current Blockchains, intending to help researchers to consider the variations between them. Another critical topic addresses access control in IoT systems, which presents several challenges due to resource constraints, the small size of IoT devices, and the dynamic topology. Lone [Lone et al. 2020] presents a taxonomy of Blockchain-based access control systems, which seek to meet IoT access control requirements.

For Tang [Tang et al. 2021], Blockchain performance largely depends on the consensus mechanism, but researchers rarely discuss IoT security from the perspective of the consensus mechanism. To meet the IoT security challenges, it is proposed to seek consensus optimisation from three perspectives: Blockchain node evaluation optimisation, Blockchain architecture optimisation, and Blockchain storage optimisation. The authors analyse the impact of the consensus mechanism on IoT security. IoT security issues are classified into three perspectives: data security, communication security, and application security. Finally, the work analyses the problems of Blockchain consensus in IoT security.

Most consensus algorithms are designed for computationally resource-intensive environments and may not be suitable for resource-constrained IoT devices. Given this, Khan [Khan et al. 2022] presents a systematic knowledge classification and explanation tool to structure research on Blockchain consensus algorithms for IoT. The authors developed an ontology for consensus algorithms. The proposed ontology is subdivided into two parts, namely CONB and CONIoT, representing the classification of generic consensus algorithms and those specific to IoT. The authors also present an analysis of the leading consensus algorithms and their adaptability for IoT.

The work of Panarello [Panarello et al. 2018] presents comprehensive research on integrating Blockchain and IoT. The survey aims to analyse research trends on using approaches and technologies related to Blockchain technology in an IoT context. The authors cover different application domains, organise the available literature according to this categorisation, introduce two usage patterns, namely device manipulation and data management, and report the development degree of solutions presented in the literature. The work also analyses researchers' challenges in integrating Blockchain and IoT and discusses the main open questions.

According to Salimitari [Salimitari et al. 2020], it is essential to use methods that guarantee the security of IoT data. However, Blockchain's classic consensus algorithms are unsuitable for IoT requirements. Therefore, the work investigates the various Blockchain consensus methods that apply to resource-constrained IoT devices and networks. The work discusses possible measures that can be taken to reduce computational power and convergence time for the underlying consensus methods. It also details alternatives to Public Blockchain, such as Private Blockchain, and its potential adoption on IoT networks.

Blockchain can address data security concerns in IoT networks. For Wang [Wang et al. 2019], inadequate data security and reliability in IoT limit its adoption. This paper presents a comprehensive survey of existing Blockchain technologies applied to IoT. It identifies possible adaptations and enhancements to Blockchain consensus protocols and data structures for suitability in this domain. The paper also presents the main challenges and benefits of Blockchain in IoT applications, the limitations of current Blockchain technologies for IoT applications, and potential future research directions.

According to Alfandi [Alfandi et al. 2021], it is critical to maintain security and robustness in authentication to ensure the secure exchange of critical data between users and IoT objects. The paper performs a comprehensive literature review addressing IoT's security and privacy challenges. According to the authors, Blockchain's secure decentralisation can overcome IoT environments' security and authentication limitations. In addition, the work highlights the challenges and privacy issues resulting from integrating Blockchain with IoT applications. Finally, the research proposes a structure of IoT security and privacy requirements when using Blockchain technology.

Despite the security features presented by Blockchain technology, scalability issues limit its ability to operate in services with multiple interactions, such as IoT. According to Fotia [Fotia et al. 2021], edge computing also faces administrative and decentralised security challenges. For the authors, combining edge computing and Blockchain in IoT environments can solve these challenges. Hence, the authors survey the integration between edge computing and IoT.

According to Fotia [Fotia et al. 2022], edge-based IoT systems face decentralised trust management challenges. This challenge is essential to getting reliable mining and data privacy and security. In this paper, the authors examine edge computing and IoT architectures and the layered architectures of edge-based IoT systems. A discussion is presented about the feasibility of integrating Blockchain technology and edge computing in IoT systems and the necessary adaptations to Blockchain to enable such integration. Finally, the authors collect and discuss performance parameters used in the literature to understand how an edge-based IoT system should be evaluated.

Table 1 shows an overview of related surveys. This overview contains the main topics covered in each work compared to what is being presented in this paper. The table indicates if the related work deals with integrating consensus algorithms, scalability, latency, and power consumption of Blockchain solutions for IoT. It also shows which Blockchain configuration is used and if the work deals with adversary tolerance.

	Int. of consensus algorithms	Scalability	Latency	Power Cons.	Blockchain Config.	Adversary Tolerance
[Wen et al. 2020]		✓		✓		✓
[Sadawi et al. 2021]		✓	✓		✓	
[Lao et al. 2020]		✓	✓	✓	✓	
[Panarello et al. 2018]		✓		✓		
[Salimitari et al. 2020]		✓	✓			
[Nijsse and Litchfield 2020]		✓		✓	✓	✓
[Tang et al. 2021]		✓				✓
[Khan et al. 2022]		✓	✓	✓		✓
[Lone et al. 2020]		✓			✓	
[Wang et al. 2019]		✓	✓	✓		
[Alfandi et al. 2021]		✓				✓
[Fotia et al.2021,2022]		✓	✓	✓		
This survey	✓	✓	✓	✓	✓	✓

Table 1: Comparison between related surveys

It is possible to notice in Table 1 that there is a recurring concern with the theme of scalability, reinforcing the idea that this theme is fundamental in this context since there is an increasing number of connected devices in IoT. However, the significant advance of this paper is its focus on integrating consensus algorithms.

This work advances the state of the art as it performs a more profound analysis of consensus algorithms for IoT, considering the requirements of scalability, latency, fault tolerance, power consumption, and Blockchain configuration used. In practice, existing surveys focus on integrations of Blockchain and IoT, while this survey concentrates on proposals for integration between possible consensus algorithms already existing in the literature.

4 Analysis of consensus algorithms and their integrations

This section analyses existing proposals for integrating consensus mechanisms. The initial phase of the research aimed to explore the area of Blockchain for the security of IoT devices. In this research phase, the search strings were applied to the scientific bases listed in Table 2, resulting in 127 papers.

Database	**No. of Papers**
IEEE Xplore	55
ACM Digital Library	7
Springer Link	5
Science Direct	25
Google Scholar	37
Total	**129**

Table 2: Existing solutions focusing on Blockchain for the security of IoT devices

After this first step, the papers were examined to identify open problems. This research resulted in some relevant topics: the performance of IoT systems connected to Blockchain, data privacy, and the choice of efficient consensus mechanisms in Blockchains for IoT.

Figure 2 presents the sequence of activities adopted in this research. Among the open challenges initially identified, the most relevant one was the consensus mechanisms. This topic is fundamental for the performance and security of the Blockchain and the guarantee of data privacy. Considering this fact, the focus on Blockchain consensus mechanisms for IoT yields 59 papers out of 129.

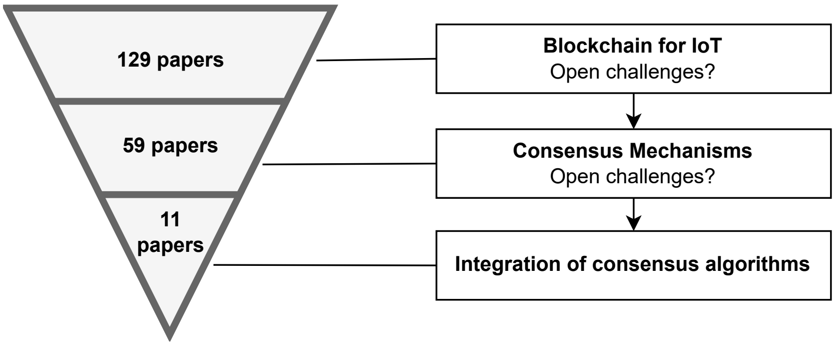

Figure 2: Sequence of activities adopted to carry out this survey

The next phase of the research aimed to evaluate the existence of open problems among the 59 papers dealing with consensus mechanisms for IoT. The most recurrent problem cited by the authors was that IoT devices have resource limitations, such as memory and processing, which makes it challenging to implement robust security strategies based on encryption [Andola et al. 2020]. As a result, devices may present security vulnerabilities. Table 3 shows the number of papers retrieved from each database in this search.

Database	**No. of Papers**
IEEE Xplore	29
ACM Digital Library	5
Springer Link	2
Science Direct	8
Google Scholar	15
Total	**59**

Table 3: Existing solutions focusing on consensus mechanisms in IoT

According to Tapwal [Tapwal et al. 2021], the consensus mechanisms commonly used in Blockchains are unsuitable for IoT, as they demand considerable computational resources, such as memory, processing, and power consumption. Many authors [Tsang et al. 2019], [Huang et al. 2019], [Zilnieks 2021] propose improvements in consensus algorithms to make them more suitable for IoT. Others [Lao et al. 2020a], [Alrubei et al.

2021], [Makhdoom et al. 2020], [Puthal et al. 2020] propose the creation of new algorithms. Finally, there are also several suggestions for integrating consensus algorithms [Xu et al. 2019], [Bai et al. 2019], [Tapwal et al. 2021], [Zhipeng 2019], [Rasolroveicy and Fokaefs 2020].

According to Alrubei [Alrubei et al. 2021], integrating consensus algorithms is promising, as it allows using already-known algorithms with proven efficiency. Thus, combinations between them will increase performance, security, and effectiveness in using Blockchain in the IoT context. However, according to Lunardi [Lunardi et al. 2019], choosing which consensus mechanism to use in each IoT context is an open challenge. Therefore, it was decided to deepen the studies on possible cases of integration between consensus algorithms already proposed in the literature, resulting in 11 papers.

Table 4 shows the databases from which the papers were selected for the analysis of this research.

Database	**No. of Papers**
IEEE Xplore	3
ACM Digital Library	2
Springer Link	0
Science Direct	2
Google Scholar	4
Total	**11**

Table 4: Existing solutions focusing on the integration of consensus mechanisms in IoT

Eight dimensions were defined to investigate the selected works. These dimensions were chosen based on their relevance to the study of Blockchain-based solutions:

- **Scalability**: It indicates the system's ability to handle increasing IoT nodes uniformly and without performance losses.
- **Latency**: It corresponds to the processing speed of transactions by the nodes to create new blocks.
- **Throughput**: It consists of the transaction rate per second concerning the number of IoT nodes and workloads processed concurrently.
- **Power consumption**: This dimension assesses whether the consensus engine performs a considerable amount of computational effort, consuming much energy, or if the process uses low-power mechanisms.
- **Integrated Algorithms and complexity**: It identifies the consensus algorithms being integrated and measures whether the characteristics of algorithms allow them to operate together efficiently after integration.
- **Blockchain configuration**: This dimension analyzes how consensus algorithms are used in Blockchain solutions for IoT and how nodes operate in this context.
- **Adversary tolerance**: This dimension assesses the ability of each consensus mechanism to withstand and recover from adversarial attacks.

4.1 Scalability

In Blockchain, scalability indicates the system's ability to handle increasing IoT node connections uniformly without performance losses. The scalability of current Blockchains limits their implementation in large-scale IoT applications. Specifically, IoT devices generate gigabytes of data in real-time, while Blockchain is not designed to store this massive amount of data [Sadawi et al. 2021].

According to the Trilemma of Scalability, Blockchain-based systems can only have two of the following three properties: security, decentralisation, and scalability [Monte et al. 2020]. This trilemma establishes that a Blockchain architecture must balance the three properties in its application according to its use.

According to Bai [Bai et al. 2019], the efficient integration of IoT devices with Blockchain is an open challenge due to the need for scalability and computational power. This work presents a two-layer consensus-based Blockchain architecture optimised for IoT (using the combined PoW and PoS consensus algorithms). At the top layer, a Blockchain of particular nodes that run a non-Byzantine fault-tolerance algorithm is implemented to determine consensus. In the lower layer, devices with scarce computational resources are used. According to the authors, their proposal presents a consensus with better fault tolerance and increases scalability.

Those potentially serving millions of users are classified as ”High” among the main consensus algorithms. Ones supporting hundreds or thousands of users are classified as ”Low”.

All algorithms are classified as ”High” except PBFT. PBFT has high throughput, low latency, and low computational overhead – all desirable for the IoT context. However, its high network overhead makes it not scalable to large networks, so it can only be applied to small IoT networks. In PBFT, all nodes need to participate in voting and creating a new node, which limits its scalability in a broader scenario.

4.2 Latency

In the Blockchain context, latency is the time to process transactions, create new blocks, and add them to the chain. In an environment with several smart devices connected, processing and recording the data in the blocks must be rapid. Bitcoin's 10-minute block generation rate is unsuitable for an IoT environment [Bai et al. 2019]. The challenge of reducing the latency has a significant impact on application security and consistency.

According to Alrubei [Alrubei et al. 2021], IoT devices are vulnerable to attacks. Blockchain technology can solve many security problems due to its decentralised and reliable nature. Still, not all Blockchain is suitable for IoT due to the limitations of the device's computing resources. Therefore, the authors propose a new consensus mechanism based on Proof of Authority (PoA) and Proof of Work (PoW). The security advantages of PoW were utilised, and its long confirmation time can be mitigated by combining it with PoA in a single mechanism called Honesty-based Distributed Proof of Authority (HDPoA) [Alrubei et al. 2022]. This integration's main advantage is obtaining a lightweight consensus algorithm, which does not require considerable power consumption to mine a block and has lower latency than using the algorithms separately.

Xu [Xu et al. 2019] considers that IoT devices have limited resources, so efficient security mechanisms must protect them. Therefore, the authors present Microchain, a hybrid Proof-of-Credit (PoC) and Voting-based Chain Finality (VCF) consensus protocol. The proposal selects a random subset of nodes to perform the consensus protocol. The hybrid consensus mechanism is based on PoC (an algorithm derived from PoS). The voting-based chain termination protocol is responsible for terminating a history of blocks by resolving conflicting checkpoints and selecting a unique chain. The objective of the integration, when using a consensus algorithm based on voting, is to obtain a reduction in the latency rate.

Algorithms having a latency of minutes/seconds/milliseconds are classified as ”High”, ”Medium”, and ”Low”, respectively. Due to the high data flow and the need for real-time responses of most IoT applications, the more suitable algorithms are those with low latency.

The integration proposals found in the literature use algorithms with low latency [Salimitari et al. 2020] [Lao et al. 2020]. The algorithms that have low latency are Proof of Luck (PoL), Proof of Elapsed Time (PoET), Practical Byzantine Fault Tolerance (PBFT), Tendermint, and Raft. Other algorithms (medium latency or even high latency like PoW) are integrated to meet other essential requirements besides latency, such as security and adversarial tolerance.

4.3 Throughput

Blockchain throughput consists of the number of transactions per second and concurrent workloads, IoT nodes can process that. As the number of connected IoT devices increases, the consensus algorithm must adapt its throughput to ensure that transaction confirmation times remain acceptable according to the requirements of each application [Alrubei et al. 2022].

Blockchain throughput is limited, and the number of transactions uploaded per time unit is much less than the number of transactions generated by users. Although Blockchains like Bitcoin have high scalability due to PoW consensus characteristics, it has performance losses such as high latency and low throughput. Byzantine consensus protocols such as PBFT exhibit better performance with high throughput, lower latency, and limited overhead. However, they rely on identity authentication and support limited network scalability regarding the number of nodes [Zhipeng 2019].

An alternative for improving consensus algorithms' limited throughput without compromising scalability features is combining a scalable permissionless consensus algorithm (e.g., PoW) with a high throughput consensus algorithm (e.g., PBFT). For this, Zhipeng [Zhipeng 2019] seeks to integrate the PBFT consensus algorithm with PoW. The algorithm combines PBFT and PoW to solve the decentralisation and performance problems. PoW nodes select PBFT nodes, and any node can participate and become a PoW node to ensure the decentralisation and security of the consensus algorithm. The experimental results shown in this work indicate that the hybrid consensus algorithm is better in terms of throughput and latency.

For comparison purposes, a throughput of up to 100 TPS (transactions per second) is rated ”Low”; those having a throughput between 100 and 1.000 TPS are ”Medium”, and ones having a throughput higher than 1,000 TPS are ”High”. For IoT-integrated Blockchain applications, the consensus algorithms used must have a high capacity to process transactions, as it is assumed that IoT devices and sensors generate a large flow of data.

Some algorithms have low throughput. These are the ones that demand more computational resources (e.g., memory, processing, power consumption), such as PoW and PoS, and those directly derived from them, i.e., ones with similar characteristics, such as PoC and PoB, and PoA.

4.4 Power Consumption

This dimension explores the power consumption of existing consensus algorithms.

Blockchain-based solutions are becoming common in scenarios where there is a need for data security while satisfying both transparency and immutability. However, classical consensus algorithms must be improved for managing heterogeneous IoT data, primarily because of their implicit constraints.

Algorithms like PBFT are ideal for an authorised Blockchain because they consume less energy than others like PoW [Alrubei et al. 2022]. Algorithms like PoS are efficient regarding power consumption but have reduced scalability [Tapwal et al. 2021]. Thus, while PoW provides unavoidable security and is highly distributive, it has low scalability and requires high power consumption.

Tapwal [Tapwal et al. 2021] proposes a dynamic Blockchain system (A-Blocks) for Industrial IoT (IIoT). The A-Blocks system exploits the resources of available consensus algorithms. It dynamically selects the most appropriate one in real time, considering the data type that will be processed. The system operates in two phases: 1) Categorising data into groups based on their characteristics; and 2) Selecting the appropriate consensus algorithm among PoW, PoS, and PBFT. According to the authors, PoW is used because of its security; PoS is utilised because it is efficient in power consumption despite its reduced scalability; and PBFT is suitable for more rapid processing and contributes to efficient power consumption.

Similarly, Rasolroveicy and Fokaefs [Rasolroveicy and Fokaefs 2020] design a self-adaptive mechanism that dynamically chooses the most appropriate consensus algorithm (among Raft, PoET, and PBFT) for the IoT Blockchain network. The proposed solution manages and changes the consensus algorithms to make them suitable for IoT data on the Blockchain. The paper's main objective is to manage network cost, performance, and security and reduce energy consumption by making consensus more efficient. Furthermore, it can dynamically reconfigure the properties of the consensus protocol, including multiple validation nodes and validation time.

Proof of Stake is an alternative to PoW to reduce power consumption and is classified as a ”Medium”. Similarly, algorithms derived from PoS and PoW, such as Delegated Proof of Stake (dPoS), Proof of Activity (PoA), and the Proof of Burn (PoB), belong to the same category. Consensus algorithms that demand a higher power consumption have a ”High” classification. Only the Proof of Work belongs to this class.

In the IoT context, there is a need for consensus algorithms that present low power consumption. Voting-based algorithms such as PBFT and dPBFT are more efficient regarding power consumption because only a few nodes create new nodes. The other algorithms are classified as ”Low” as they were designed for situations that require higher efficiency and resource savings.

4.5 Integrated Algorithms and complexity

Integrating consensus algorithms may be complex, depending on each algorithm's characteristics and the IoT environment's requirements. Those algorithms requiring high computational cost (e.g., memory or CPU usage), or even those requiring tokens or cryptocurrencies to reach a consensus, are classified as having a ”High” degree of integration complexity. Algorithms with higher performance and low computational cost are classified with integration complexity ”Low”. The cases of integration between a computationally more expensive algorithm (like PoW) and a light one are classified as ”Medium”.

In Alrubei [Alrubei et al. 2021], the PoW and PoA algorithms were integrated. This integration aimed to take advantage of the security of PoW and the high execution speed of PoA, which reduces the transaction confirmation time.

Table 5 summarises existing integration proposals. The integration proposed by Alrubei [Alrubei et al. 2021][Alrubei et al. 2022] is classified with a ”High” degree of integration complexity, as they integrate two algorithms with high execution costs.

Authors	Integration proposal	Integration Complexity
[Alrubei et al. 2021]	PoW, PoA	High
[Bai et al. 2019]	PoW, PoS	High
[Tapwal et al. 2021]	PoW, PoS, PBFT	High
[Lunardi et al. 2019]	PBFT, WBC	Low
[Rasolroveicy and Fokaefs 2020]	PoET, Raft, PBFT	Low
[Zhipeng 2019]	PoW, PBFT	Medium
[Xu et al. 2019]	PoC, VCF	Low
[Wang et al. 2020]	DPoS, PoP	Low
[Alrubei et al. 2022]	PoW, PoA	High
[Luo et al. 2023]	RAFT, PBFT	Low
[Huang et al. 2023]	DPoS, PBFT	Low

Table 5: Integration proposals

Bai et al. [Bai et al. 2019] integrate PoW and PoS to create a solution with a high-security level and good scalability due to the use of PoW and PoS, respectively. As these algorithms demand high computational costs, the complexity of integration is ”High”.

Tapwal et al. [Tapwal et al. 2021] integrate PoW, PoS, and PBFT algorithms. According to the authors, PoW is used because of its security, PoS is used because of its efficient power consumption despite having reduced scalability, and PBFT is suitable for faster processing and contributes to efficient power consumption. The complexity of this integration is also rated ”High”. This integration was proposed for use in Industrial IoT (IIoT).

Lunardi et al. [Lunardi et al. 2019] propose a Blockchain structure to support different consensus algorithms through a modular design. The authors integrate the PBF and a Consensus Based on Witnesses (WBC) to reduce the latency rate and throughput. As they are consensus algorithms that consume few computational resources, the complexity of integration was classified as ”Low”.

The paper of Rasolroveicy and Fokaefs [Rasolroveicy and Fokaefs 2020] designs a self-adaptive mechanism that dynamically chooses the consensus algorithm for the IoT Blockchain network. Raft, PoET, and PBFT algorithms are integrated to manage the network’s cost, performance, and security and reduce power consumption. The degree of complexity in integrating this solution can be classified as ”Low” because all algorithms used in the solution consume few computational resources in their execution.

Zhipeng [Zhipeng 2019] integrates the consensus algorithms PBFT and PoW. In this proposal, the consensus process is partially performed by PoW to ensure a high level of security and partially by PBFT to reduce throughput and latency rates. Then, the solution presents better decentralisation and performance than using the algorithms separately. The complexity of this integration is ”Medium” due to the need to manage the demand for computational resources of PoW.

The paper developed by Xu et al. [Xu et al. 2019] introduces a hybrid Proof-of-Credit (PoC) and Voting-based Chain Finality (VCF) consensus protocol. When using an algorithm based on voting, the objective of this integration is to obtain a reduced latency integrated with the PoC that consists of an algorithm of low computational cost. Thus, the integration complexity of this proposal is classified as ”Low”.

In the paper of Wang et al. [Wang et al. 2020], a hybrid consensus algorithm based on modified Proof of Probability (PoP) and Delegated Proof of Participation (dPoS) is presented. As they are two algorithms with good performance, the complexity of integration is ”Low”. The proposal seeks to compensate for the security deficiencies of PoP with the efficiency of dPoS to avoid malicious behaviour.

The paper of Luo et al. [Luo et al. 2023] proposes integrating the RAFT and PBFT consensus algorithms for use in electric vehicle charging environments. The authors perform a theoretical analysis and simulation of the integration. According to the paper, these two consensus algorithms have high scalability, low communication complexity, low storage overhead, high throughput, and low latency. As the integrated algorithms have good performance, their integration complexity is classified as ”Low”. Furthermore, integration with RAFT can avoid the risk of the Byzantine leader being a malicious node.

The paper developed by Huang et al.[Huang et al. 2023] presents an integration between DPoS and PBFT algorithms. Combining these consensus algorithms makes it possible to use DPoS characteristics to improve efficiency in generating new blocks. Also, the PBFT features can be used to solve the data consistency problem with minimal resource consumption. The integration complexity is classified as ”Low” because they are two algorithms with good performance.

4.6 Blockchain Configuration

This dimension assesses how Blockchains are configured to use consensus mechanisms in IoT contexts.

Most projects use Gateways to manage the communication between devices and the Blockchain. The only consensus algorithms whose devices are used as nodes are Ripple and Stellar, which are utilised in payment mechanisms.

In Blockchain for IoT, two configurations are commonly used to integrate devices and the Blockchain. The first configuration, and most adopted, uses management devices like Gateways to mediate the communication between IoT data and Blockchain nodes [Dorri et al. 2019]. The second configuration uses the devices themselves as nodes.

Lunardi [Lunardi et al. 2019] reinforces the importance of integrating consensus algorithms to ensure the security of IoT data. The authors propose to improve a Blockchain whose architecture uses Gateways to support different consensus algorithms through a modular design. This work uses two algorithms: PBFT and Consensus Based on Witnesses (WBC). According to the authors, the decision on the most appropriate consensus algorithm is left open in the literature, depending on the application domain.

4.7 Adversary Tolerance

The ability of each consensus mechanism to tolerate and recover from attacks by adversaries is evaluated in this dimension.

According to Sengupta [Sengupta et al. 2020], the decentralisation presented by Blockchain technology allows nodes to participate in transactions without needing a trusted third party. This fact eliminates the bottleneck of a single point of failure, which increases fault tolerance. Blockchain nodes maintain identical replicas of all records, so there is a more outstanding guarantee of fault tolerance. This property helps maintain the data integrity and resilience of the network.

Different requirements must be met to implement a practical Blockchain-based application. Key characteristics to consider are network accessibility, degree of decentralisation, scalability, latency, throughput, adversary tolerance, computational overhead, network overhead, and storage overhead. Depending on the application, some of these characteristics become essential [Salimitari et al. 2020].

Wang et al. [Wang et al. 2020] present a hybrid consensus algorithm based on modified Proof-of-Probability (PoP) and Delegated Proof-of-Stake (dPoS). The efficiency of dPoS compensates for the security deficiencies of PoP. The probability-based behaviour of PoP weakens the ability of dPoS supernodes to prevent malicious behaviour. Combining the two algorithms makes the system perform better in terms of security and more tolerant of attacks from malicious adversaries.

The ability to tolerate faults against malicious attacks is essential to maintain consistency and reliability in a Blockchain. When choosing a specific consensus algorithm for IoT, it is necessary to consider its ability to opponent tolerance [Salimitari et al. 2020].

Table 6 compares the main consensus mechanisms and their characteristics according to the dimensions evaluated in this survey. Four dimensions inherent to the algorithms analysed: scalability, latency, throughput, and power consumption. Furthermore, four dimensions related to using Blockchain consensus mechanisms for IoT are also considered: integrated algorithms, integration complexity, Blockchain configuration, and adversary tolerance.

The consensus algorithms most indicated for use in the context of IoT, due to their characteristics, are Proof of Luck (PoL), Proof of Elapsed Time (PoET), and Practical Byzantine Fault Tolerance (PBFT).

Other consensus algorithms, which demand more computational resources, can be considered unfeasible because, in their classic form, they have characteristics unsuitable for IoT. Hence, the literature has adaptation proposals to use in this context. These include Proof of Stake (PoS), Delegated Proof of Stake (dPoS), Proof of Importance (PoI), dPBFT, Tendermint, and Raft.

Consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) have high latency, low throughput, and high power consumption, making them unsuitable for IoT environments.

Consensus Mechanisms for Blockchains Applied to IoT								
Family of Consensus Algorithms	**Scalability**	**Latency**	**Throughput**	**Power Consumption**	**Integrated Algorithms**	**Integration Complexity**	**Blockchain Configuration**	**Adversary Tolerance**
Proof of Work (PoW)	High	High	Low	High	(PoW, PoA), (PoW, PoS), (PoW, PBFT), (PoW, PoA)	High	1	<50%
Proof of Stake (PoS)	High	Medium	Low	Medium	(PoS, PoW)	High	1	<51%
Delegated Proof of Stake (dPoS)	High	Medium	High	Medium	(dPoS, PoP)	Low	1	<51%
Proof of Luck (PoL)	High	Low	High	Low	-	-	1	<50%
Proof of Capacity/ Space (PoC)	High	High	Low	Low	(PoC, VCF)	Low	1	<50%
Proof of Activity (PoA)	High	Medium	Low	Medium	(PoA, PoW)	High	1	51%
Proof of Burn (PoB)	High	High	Low	Medium	-	-	1	<25%
Proof of Importance (PoI)	High	Medium	High	Low	-	-	1	<51%
Proof of Elapsed Time (PoET)	High	Low	High	Low	(PoET, Raft), (PoET, PBFT)	Low	1	N/A
Practical Byzantine Fault Tolerance (PBFT)	Low	Low	High	Low	(PBFT, PoW), (PBFT, WBC), (PBFT, Raft), (PBFT, PoET)	Medium	1	<33%
dPBFT	High	Medium	High	Low	-	-	1	<33%
Tendermint	High	Low	High	Low	-	-	1	<33%
Raft	High	Low	High	Low	(Raft, PoET), (Raft, PBFT)	Low	1	<50%
Ripple	High	Medium	High	Low	-	-	2	20%
Stellar	High	Medium	High	Low	-	-	2	Variable

Table 6: Comparison between the main consensus algorithms

Most IoT devices have computational resource limitations, such as processing, memory, and battery. Specific IoT non-functional requirements must be met for the system's security and performance. IoT-integrated Blockchain can satisfy security requirements, ensuring system reliability and fault tolerance, but not all Blockchain consensus mechanisms can be IoT-integrated efficiently. Hence, it is possible to verify that for a consensus algorithm to be suitable for IoT, it must have the following characteristics:

- **High scalability**: It is necessary to support the fast adoption of IoT technology and increase users.
- **Low latency**: For better efficiency and security of the application, the consensus algorithm must have low latency.
- **High throughput**: In the IoT context, it is common to have an increased flow of information almost constantly, so a Blockchain-based solution must process numerous transactions to maintain environment consistency.
- **Efficient power consumption**: In most situations, IoT devices have resource limitations, such as memory and processing, or are battery-dependent. The consensus algorithm must be efficient in power consumption and maintaining security.

5 Open Challenges

This section presents open challenges to integrating consensus mechanisms of Blockchains in IoT environments.

- **Scalability evaluation.** A considerable number of existing approaches are only in conceptual or prototype phases. Hence, the performance and scalability tests may not represent the actual behaviour of a Blockchain in IoT. Therefore, an open challenge is evaluating the scalability of new solutions in actual setups to assess their efficiency and reliability.
- **Resource consumption evaluation.** Using a Blockchain-based solution for IoT has associated costs that most solutions ignore. An open research question is to assess essential requirements such as power consumption, computing power, and network bandwidth consumption, among others.
- **Propose and evaluate new integrations.** Integrating consensus algorithms for IoT is a relatively new area of research. Hence, there are still many possible integrations to be performed. An open research challenge is testing and evaluating possible efficiency, scalability, latency, throughput and adversarial tolerance integrations.

  To define the most possible Blockchain configuration. A relevant research challenge is to point out a strategy to assist in the decision-making for developers and companies about which configuration is more feasible for use in different situations, in which case to use a public or private Blockchain, which mechanism(s) of consensus to use or integrate, and the cost that each of these decisions would entail for the organisation.
- **Adversary tolerance.** Researchers often need access to many devices or a large IoT environment. Most existing solutions use simulation, and some carry out tests

with real devices, but in a limited way. Over the years, simulation methods and tools have made many advances and today have a high level of reliability. However, it is a research challenge to carry out tolerance tests on adversaries using real-world environments, where errors and failures related to human and environmental factors can arise, which are impossible to predict in a simulation. With this, the reliability of the solution will become more significant.

6 Conclusions and Future Work

The Internet of Things is gaining more and more popularity. It is present in different areas of society, but it is necessary to adopt strategies that guarantee the security of user data. Blockchain technology has the potential to solve IoT security problems. However, integrating the two areas still presents many challenges, as classic Blockchain consensus algorithms need to meet IoT requirements.

Therefore, this paper analyses existing approaches for integrating consensus algorithms for using Blockchains in IoT environments. A literature review was conducted, where works were studied to identify open problems and challenges in the area.

This paper analysed surveys in the literature on integrating consensus algorithms. The need to better evaluate factors such as performance, latency, and scalability of IoT solutions, which integrate Blockchain consensus algorithms, was identified. As in Blockchain, edge computing is presented as an alternative that can be used to reduce the overhead of cloud computing. Edge computing consists of offloading tasks from remote cloud servers, such as Blockchain nodes, to devices closest to users, reducing latency and making systems more efficient.

The main scientific contribution of this paper is the analysis of the state of the art and identification of open research challenges on the integration of consensus algorithms in IoT-based Blockchains. The overview presented in Table 6 shows the characteristics of each algorithm. It can later serve as a basis for other researchers in Blockchain for IoT.

For future work, it is relevant to study the costs of implementing blockchain-based solutions for IoT. Many factors must be considered, such as performance evaluation, energy consumption, memory, and computational complexity. It is also necessary to consider the adoption of incentive and reward mechanisms to be used by miners in environments where consensus algorithm integration occurs. Studying optimisation approaches for consensus mechanisms in IoT is also an interesting future research. Finally, it is also relevant to define strategies that help choose which Blockchain/consensus mechanism to use in each IoT context.

References

[Alfandi et al. 2021] Alfandi, O., Khanji, S., Ahmad, L. & Khattak, A. A survey on boosting IoT security and privacy through Blockchain. Cluster Computing. 24, 37-55 (2021).

[Andola et al. 2020] Andola, N., Venkatesan, S., Verma, S. & Others PoEWAL: A lightweight consensus mechanism for Blockchain in IoT. Pervasive And Mobile Computing. 69 pp. 101291 (2020).

[Ali et al. 2018] Ali, M., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F. & Rehmani, M. ”Applications of Blockchains in the Internet of Things: A comprehensive survey”. IEEE Communications Surveys & Tutorials. 21, 1676-1717 (2018).

[Alrubei et al. 2021] Alrubei, S., Ball, E. & Rigelsford, J. ”Securing IoT-Blockchain Applications Through Honesty-Based Distributed Proof of Authority Consensus Algorithm”. 2021 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA). pp. 1-7 (2021).

[Alrubei et al. 2022] Alrubei, S., Ball, E. & Rigelsford, J. ”Hdpoa: Honesty-Based Distributed Proof of Authority Via Scalable Work Consensus Protocol for Iot-Blockchain Applications”. Available At SSRN 3999127.

[Bai et al. 2019] Bai, H., Xia, G. & Fu, S. ”A two-layer-consensus based Blockchain architecture for IoT”. 2019 IEEE 9th International Conference On Electronics Information And Emergency Communication (ICEIEC). pp. 1-6 (2019).

[Dai et al. 2019] Dai, H., Zheng, Z. & Zhang, Y. ”Blockchain for Internet of Things: A survey”. IEEE Internet Of Things Journal. 6, 8076-8094 (2019).

[Dorri et al. 2019] Dorri, A., Kanhere, S., Jurdak, R. & Gauravaram, P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. Journal Of Parallel And Distributed Computing. 134 pp. 180-197 (2019)

[Fotia et al. 2021] Fotia, L., Delicato, F. & Fortino, G. Integrating Blockchain and Edge Computing in Internet of Things: Brief Review and Open Issues. 2021 International Conference On Cyber-Physical Social Intelligence (ICCSI). pp. 1-6 (2021).

[Fotia et al. 2022] Fotia, L., Delicato, F. & Fortino, G. Trust in Edge-based Internet of Things architectures: State of the Art and Research Challenges. ACM Computing Surveys (CSUR). (2022).

[Hassija et al.2019] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. & Sikdar, B. ”A survey on IoT security: application areas, security threats, and solution architectures”. IEEE Access. 7 pp. 82721-82743 (2019).

[Huang et al. 2019] Huang, J., Kong, L., Chen, G., Wu, M., Liu, X. & Zeng, P. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions On Industrial Informatics. 15, 3680-3689 (2019).

[Huang et al. 2023] Huang, R., Yang, X. & Ajay, P. Consensus mechanism for software-defined blockchain in the Internet of things. Internet Of Things And Cyber-Physical Systems. 3 pp. 52-60 (2023).

[Khan et al. 2022] Khan, M., Hartog, F. & Hu, J. A Survey and Ontology of Blockchain Consensus Algorithms for Resource-Constrained IoT Systems. Sensors. 22, 8188 (2022).

[Kamran et al. 2020] Kamran, M., Khan, H., Nisar, W., Farooq, M. & Rehman. Blockchain and Internet of Things: A bibliometric study. Computers & Electrical Engineering. 81 pp. 106525 (2020).

[Lao et al. 2020] Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S. & Yang, Y. ”A survey of IoT applications in Blockchain systems: Architecture, consensus, and traffic modeling”. ACM Computing Surveys (CSUR). 53, 1-32 (2020).

[Lao et al. 2020a] Lao, L., Dai, X., Xiao, B. & Guo, S. G-PBFT: a location-based and scalable consensus protocol for IOT-Blockchain applications. 2020 IEEE International Parallel And Distributed Processing Symposium (IPDPS). pp. 664-673 (2020).

[Liao and Cheng 2023] Liao, Z. & Cheng, S. RVC: A reputation and voting based blockchain consensus mechanism for edge computing-enabled IoT systems. Journal Of Network And Computer Applications. 209 pp. 103510 (2023).

[Lone et al. 2020] Lone, A., Dar, A. & Naaz, R. Taxonomy of Blockchain Driven Access Control Frameworks, Models and Schemes for IoT. Proceedings Of 2nd International Workshop On Blockchain Technologies For Robotic Systems. (2020).

[Luo et al. 2023] Luo, H., Yu, H. & Luo, J. PRAFT and RPBFT: A class of blockchain consensus algorithm and their applications in electric vehicles charging scenarios for V2G networks. Internet Of Things And Cyber-Physical Systems. 3 pp. 61-70 (2023).

[Lunardi et al. 2019] Lunardi, R., Michelin, R., Neu, C., Nunes, H., Zorzo, A. & Kanhere, S. ”Impact of consensus on appendable-block Blockchain for IoT”. Proceedings Of The 16th EAI International Conference On Mobile And Ubiquitous Systems: Computing, Networking And Services. pp. 228-237 (2019).

[Makhdoom et al. 2020] Makhdoom, I., Tofigh, F., Zhou, I., Abolhasan, M. & Lipman, J. PLEDGE: An IoT-oriented Proof-of-Honesty based Blockchain Consensus Protocol. 2020 IEEE 45th Conference On Local Computer Networks (LCN). pp. 54-64 (2020).

[Monte et al. 2020] Monte, G., Pennino, D. & Pizzonia, M. Scaling blockchains without giving up decentralisation and security: A solution to the blockchain scalability trilemma. Proceedings Of The 3rd Workshop On Cryptocurrencies And Blockchains For Distributed Systems. pp. 71-76 (2020).

[Monrat et al. 2019] Monrat, A., Schelén, O. & Andersson, K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access. 7 pp. 117134-117151 (2019).

[Nijsse and Litchfield 2020] Nijsse, J. & Litchfield, A. A taxonomy of Blockchain consensus methods. Cryptography. 4, 32 (2020).

[Panarello et al. 2018] Panarello, A., Tapas, N., Merlino, G., Longo, F. & Puliafito, A. Blockchain and IoT integration: A systematic survey. Sensors. 18, 2575 (2018).

[Puthal et al. 2020] Puthal, D., Mohanty, S., Yanambaka, V. & Kougianos, E. PoAh: A novel consensus algorithm for fast scalable private Blockchain for large-scale IoT frameworks. ArXiv Preprint ArXiv:2001.07297. (2020).

[Qi and Guan 2022] Qi, J. & Guan, Y. Practical Byzantine fault tolerance consensus based on comprehensive reputation. Peer-to-Peer Networking And Applications. pp. 1-11 (2022).

[Rasolroveicy and Fokaefs 2020] Rasolroveicy, M. & Fokaefs, M. ”Dynamic reconfiguration of consensus protocol for IoT data registry on Blockchain”. in Proceedings Of The 30th Annual International Conference On Computer Science And Software Engineering. pp. 227-236 (2020).

[Sadawi et al. 2021] Al Sadawi, A., Hassan, M. & Ndiaye, M. ”A survey on the integration of Blockchain with IoT to enhance performance and eliminate challenges”. IEEE Access. 9 pp. 54478-54497 (2021).

[Salimitari et al. 2020] Salimitari, M., Chatterjee, M. & Fallah, Y. ”A survey on consensus methods in Blockchain for resource-constrained IoT networks”. Internet Of Things. 11 pp. 100212 (2020).

[Sengupta et al. 2020] Sengupta, J., Ruj, S. & Bit, S. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal Of Network And Computer Applications. 149 pp. 102481 (2020).

[Tang et al. 2021] Tang, X., Hu, G., Yuan, Y., Li, H., Zhang, Y., Li, Y., Li, M. & Cheng, J. Survey: Research on Blockchain Consensus Mechanism in IoT Security. Advances In Artificial Intelligence And Security: 7th International Conference, ICAIS 2021, Dublin, Ireland, July 19-23, 2021, Proceedings, Part III 7. pp. 573-584 (2021).

[Tapwal et al. 2021] Tapwal, R., Deb, P., Misra, S. & Pal, S. ”Amaurotic Entity-Based Consensus Selection in Blockchain-Enabled Industrial IoT”. IEEE Internet Of Things Journal. (2021).

[Tsang et al. 2019] Tsang, Y., Choy, K., Wu, C., Ho, G. & Lam, H. Blockchain-driven IoT for food traceability with an integrated consensus mechanism. IEEE Access. 7 pp. 129000-129017 (2019).

[Wang et al. 2019] Wang, X., Zha, X., Ni, W., Liu, R., Guo, Y., Niu, X. & Zheng, K. Survey on Blockchain for Internet of Things. Computer Communications. 136 pp. 10-29 (2019).

[Wang et al. 2020] Wang, B., Li, Z. & Li, H. ”Hybrid consensus algorithm based on modified proof-of-probability and DPoS”. Future Internet. 12, 122 (2020).

[Wen et al. 2020] Wen, Y., Lu, F., Liu, Y., Cong, P. & Huang, X. Blockchain Consensus Mechanisms and Their Applications in IoT: A Literature Survey. Algorithms And Architectures For Parallel Processing: 20th International Conference, ICA3PP 2020, New York City, NY, USA, October 2–4, 2020, Proceedings, Part III 20. pp. 564-579 (2020).

[Wu et al. 2019] Wu, M., Wang, K., Cai, X., Guo, S., Guo, M. & Rong, C. ”A comprehensive survey of Blockchain: From theory to IoT applications and beyond”. IEEE Internet Of Things Journal. 6, 8114-8154 (2019).

[Xu et al. 2019] Xu, R., Chen, Y., Blasch, E. & Chen, G. ”Microchain: A hybrid consensus mechanism for lightweight distributed ledger for IoT”. ArXiv Preprint ArXiv:1909.10948. (2019).

[Yu et al. 2020] Yu, M., Sahraei, S., Li, S., Avestimehr, S., Kannan, S. & Viswanath, P. Coded merkle tree: Solving data availability attacks in blockchains. International Conference On Financial Cryptography And Data Security. pp. 114-134 (2020).

[Zhipeng 2019] Zhipeng, F. ”Research on Blockchain Hybrid Consensus Algorithm Based on Internet of Things”. International Journal of Internet of Things and Big Data (2019).

[Zilnieks 2021] Zilnieks, V. Choosing a Consensus Mechanism for a Blockchain-Based P2P Instant Transaction System Integrated with IoT. 2021 International Conference On Communication, Control And Information Sciences (ICCISc). 1 pp. 1-6 (2021).