EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Proof-of-resource: A resource-efficient consensus mechanism for IoT devices in blockchain networks

Mahmoud Abbasi[1], Javier Prieto[1,*], Marta Plaza-Hernández[1], and Juan Manuel Corchado[1,2]

[1]BISITE Research Group, University of Salamanca, Salamanca, Spain
[2]AIR Institute, IoT Digital Innovation Hub, Salamanca, Spain

Abstract

In this paper, we propose an innovative, lightweight, and energy-efficient consensus mechanism, Proof-of-Resource (PoR), custom-designed for Internet of Things (IoT) devices in blockchain networks. As IoT's integration with blockchain faces hurdles such as scalability, resource efficiency, and security, conventional blockchain consensus mechanisms prove unsuitable due to IoT devices' resource limitations. The PoR is a breakthrough that capitalizes on IoT device resources' inherent capabilities to achieve consensus, thus enabling secure and efficient data exchange while minimizing resource consumption. Our paper presents the comprehensive design of PoR, discussing aspects like initialization, resource verification, consensus protocol, validator selection, block validation, and rewards. Through a simulation involving fifteen IoT devices, we demonstrate that PoR effectively addresses key challenges in IoT-blockchain integration, signifying a significant step forward in enabling blockchain technology for IoT systems.

Received on 22 February 2024; accepted on 01 July 2024; published on 09 July 2024

Keywords: Blockchain, Consensus mechanism, IoT

doi:10.4108/eetiot.6565

1. Introduction

The rapid proliferation of Internet of Things (IoT) applications has facilitated the cooperation of a diverse range of lightweight smart devices to provide services, with or without human intervention [1]. With the increased prominence and deployment of these IoT-based applications, a significant amount of transaction data is generated by the interconnected smart IoT devices, thus highlighting the criticality of ensuring data security and privacy. Deployed in a distributed network environment, these IoT systems comprise numerous devices with varied characteristics and behavior [2]. A scalable, flexible, and lightweight system architecture is necessitated by the heterogeneity and resource limitations of these devices. The ideal architecture should support swift development and easy deployment across multiple application vendors, regardless of their adherence to standard development technologies. Furthermore, considering the geographical dispersion of these smart devices across network edges and the fact that they are managed by fragmented service providers enforcing different security policies, conventional security policies, which rely on centralized authority and are prone to performance issues and single points of failure, are found to be inadequate and inefficient in addressing the performance and security challenges prevalent in IoT systems [3].

Recently, the design of decentralized security mechanisms for distributed network applications has gained significant attention in academia and industry. Blockchain, the foundational protocol of Bitcoin [4], has demonstrated its potential to revolutionize information technology (IT) due to its appealing properties such as decentralization and transparency. Notably, blockchain-enabled security mechanisms for IoT-based applications have been reported in various domains, including smart surveillance systems, social security systems, space situation awareness, biometric imaging data processing, identification authentication, and access control [5]. The combination of blockchain and smart contracts holds promise in offering a decentralized security mechanism for IoT systems. In other words, the fusion of IoT and blockchain technology

*Corresponding author. Email: mahmoudabbasi@usal.es

has the power to reshape how we interact with and secure our increasingly connected world. It promises safer, more efficient supply chains, more resilient smart cities, and enhanced healthcare systems, among countless other possibilities.

However, integrating blockchain technologies into IoT systems presents critical challenges in designing scalable and lightweight blockchain protocols. Specifically, the performance of blockchain networks heavily relies on consensus mechanisms, which determine data consistency, the speed at which consensus is reached, resistance to malicious nodes, and network scalability. Unfortunately, existing blockchain protocols are not directly suitable for IoT scenarios. Most permissionless blockchain networks, such as Bitcoin, require solving computationally intensive hashing puzzles for block generation. While these hashing-intensive proof-of-work (PoW) consensus mechanisms ensure network scalability and mitigate Sybil attacks, they come at the cost of low throughput, high energy consumption, and ever-growing chain data [6]. On the other hand, classical Byzantine consensus protocols like Practical Byzantine Fault Tolerance (PBFT) [7] exhibit better performance in terms of high throughput, low latency, and limited overhead. However, they rely on identity authentication and have limited network scalability with regard to the number of nodes.

To overcome these obstacles in integrating blockchain technologies with IoT systems, a novel consensus mechanism called Proof-of-Resource (PoR) is introduced in this paper, which is specifically tailored to accommodate IoT devices with limited resources. The existing resources within IoT devices, such as processing power, memory, and energy, are utilized by the PoR consensus to establish consensus within the blockchain network. By tapping into the inherent capabilities of IoT device resources, a lightweight and energy-efficient consensus mechanism is provided by PoR, ensuring secure and reliable transactions without imposing excessive demands on resource-constrained devices.

The twofold objective of this research is: (1) to develop a PoR consensus mechanism suitable for resource-constrained IoT devices and (2) to evaluate its performance and security characteristics. By addressing the limitations of existing consensus mechanisms, this research aims to offer a practical solution that enables the active participation of IoT devices in blockchain networks while minimizing resource consumption.

The rest of the paper is structured as follows: related papers are reviewed and discussed in Section 2. Section 3 provides the system design of the PoR mechanism. The system's performance evaluation is conducted in Section 5. Finally, our paper is concluded in Section 6.

2. Literature review: advancements in blockchain consensus mechanisms for IoT applications

In this section, we review the existing literature on the integration of blockchain technology in IoT systems, with a focus on consensus mechanisms and their limitations (see Table 1).

Li *et al.* [8] addressed the challenge of implementing blockchain technology in resource-constrained scenarios such as IoT and smart homes. They proposed a lightweight blockchain solution to overcome the limitations of computing, storage, and bandwidth resources. Their improved PBFT consensus mechanism, coupled with a reward and punishment strategy, enhances efficiency and reduces communication resources. Additionally, a storage optimization scheme based on RS erasure code is presented to minimize storage overhead while ensuring data recoverability. Experimental results validate the effectiveness of these strategies in reducing consensus delays, communication requirements, and the overall cost of blockchain storage. These findings contribute to the development of reliable and efficient security solutions for resource-constrained devices in IoT and smart home environments. The study have been conducted in [9] introduces Microchain, a hybrid consensus mechanism designed for lightweight distributed ledgers in IoT systems. Existing blockchain technologies like Bitcoin and Ethereum face challenges when integrating with resource-constrained IoT platforms due to power consumption and low throughput. To address this, Microchain proposes a hybrid Proof-of-Credit (PoC)-Voting-based Chain Finality (VCF) consensus protocol. The protocol utilizes a bias-resistant randomness protocol and cryptographic sortition algorithm to select a random subset of nodes as a final committee for consensus. The hybrid mechanism combines PoC, a pure Proof of Stake (PoS) protocol, to determine block proposers based on fair credit assignment. The voting-based chain finality protocol resolves conflicting checkpoints and selects a unique chain. Experimental results from a proof-of-conception prototype demonstrate that Microchain offers a partially decentralized, scalable, and lightweight distributed ledger protocol suitable for IoT applications. Liu *et al.* [10] proposed RAFT+, a DQN-based consensus mechanism for integrating blockchain into resource-constrained IoT networks. The aim is to ensure data security in IoT applications while addressing the limitations of IoT end devices. RAFT+ is built upon the distributed consensus algorithm called RAFT and introduces a new leader selection scheme. The scheme utilizes a deep Q-Network (DQN) to optimize leader selection based on various conditions, effectively managing system resources and balancing the load across multiple IoT end devices. Simulation results demonstrate that RAFT+ improves

system performance while maintaining security even under high load conditions. Fu *et al.* [11] proposed an efficient and fault-tolerant blockchain consensus transform mechanism designed for IoT environments, named BCT. With the increasing number of IoT devices generating incremental data, there is a need for credible data sharing across different private domains controlled by data owners through edge devices. While existing solutions rely on blockchain for cross-domain IoT data sharing, the requirements of efficiency and Byzantine fault tolerance pose challenges. To address this, the paper proposes the BCT mechanism and presents two consensus algorithms: Detectable RAFT (DRAFT) and Double-Layer Parallel BFT (DPBFT). These algorithms enhance the efficiency and fault tolerance of the data sharing process. Extensive experiments are conducted to validate the efficiency and tolerance of the BCT mechanism, demonstrating its effectiveness in enabling efficient and reliable cross-domain IoT data sharing. The study in [12] introduces B-IoT, a blockchain-driven IoT system with a credit-based consensus mechanism. Blockchains are power-intensive and low-throughput, which poses challenges for power-constrained IoT devices. To address these challenges, the paper proposes a credit-based PoW mechanism specifically designed for IoT devices. This mechanism enhances security and transaction efficiency simultaneously. Additionally, to ensure the confidentiality of sensitive IoT data, a data authority management method is designed to regulate access to sensor data. The system is built on a directed acyclic graph (DAG)-structured blockchain, which offers greater efficiency compared to traditional blockchain structures. A prototype of B-IoT is implemented on Raspberry Pi, and a case study of a smart factory is conducted. Lao *et al.* [13] introduced G-PBFT, a location-based and scalable consensus protocol designed for IoT-blockchain applications. G-PBFT leverages fixed IoT devices with greater computational power and reduced likelihood of becoming malicious nodes. By utilizing geographic information and selecting loyal endorsers, G-PBFT achieves high consensus efficiency and low traffic intensity, mitigating Sybil attacks. The protocol also incorporates an era switch mechanism to handle IoT network dynamics. Experimental results demonstrate that G-PBFT significantly reduces consensus time, network overhead, and offers scalability for IoT applications. Biswas *et al.* [14] proposed a lightweight consensus algorithm designed for scalable IoT business blockchains, called PoBT. PoBT reduces computation time for block and trade validation and includes a ledger distribution mechanism to decrease memory requirements for IoT nodes. The algorithm improves overall system performance in terms of security, computation time, memory, and bandwidth requirements. PoBT offers a practical solution for leveraging blockchain in large-scale IoT business scenarios. The paper in [15] focuses on the implementation of blockchain technology in the data acquisition part of SCADA systems for smart grids and Industry 4.0. The paper introduces PoRCH (Proof of Random Count in Hashes), a novel consensus mechanism specifically designed for blockchain-enabled SCADA systems. The mechanism incorporates a customized mining node selection scheme. A small-scale prototype of a blockchain-enabled data acquisition system is developed, and its performance evaluation highlights the benefits of blockchain technology. This research addresses the need for efficient and easy-to-implement consensus mechanisms in the field of blockchain-enabled SCADA systems, emphasizing the potential of blockchain to enhance the security, resilience, and data integrity of future SCADA systems in smart grids and Industry 4.0.

3. System design of Proof-of-Resource

This section outlines the details of the PoR mechanism, specifically designed for IoT devices in the context of blockchain. The methodology comprises several key steps, including initialization, resource verification, reputation score update, consensus and validator selection, and block validation and rewards (see Fig. 1).

3.1. Initialization

The initialization step involves each IoT device committing a portion of its limited computational power, storage capacity, and energy resources to participate in the blockchain network. Each IoT device is assigned an initial reputation or resource score based on its committed resources. The initial score reflects the proportion of resources committed by each IoT device and establishes their starting reputation within the PoR mechanism.

Committed resources. Each IoT device $i \in \{1, 2, \ldots, N\}$ participating in the mechanism commits a set of resources denoted as $C(i) = \{r1, r2, ..., rM\}$. The committed resources can represent different aspects such as computational power, communication, and storage capacity. In our implementation, we consider computational, storage, and energy resources. Each resource type rj, where $j \in \{1, 2, \ldots, M\}$, has a specific value indicating the amount of that resource committed by the device. The total resources available in the system are calculated as the sum of the committed resources from all IoT devices: $T = \sum C(i), for\ i \in 1, 2, ..., N$.

Initial reputation score calculation. The initial reputation $S(i)$ for each IoT device i is determined based on the resources it has committed and the corresponding importance weight assigned to each resource. In other

Table 1. Comparison of blockchain consensus mechanisms for IoT applications

Reference	Consensus mechanism	Key features	Benefits	IoT application
Li *et al.* [8]	Improved PBFT	Reward/punishment strategy , RS erasure code	Reduces consensus delays, communication requirements , cost of storage	Smart home
Xu *et al.* [9]	PoC-VCF	Bias-resistant randomness protocol , cryptographic sortition	Scalable, lightweight, partially decentralized	Generic IoT
Liu *et al.* [10]	RAFT+	DQN-based leader selection	Optimizes resource management, maintains security under high load	Generic IoT
Fu *et al.* [11]	BCT	Efficient and fault-tolerant consensus mechanism	Enhances efficiency and fault tolerance of data sharing	Cross-domain IoT data sharing
Huang *et al.* [12]	Credit-based PoW	Data authority management method, DAG-structured blockchain	Enhances security, transaction efficiency, and confidentiality	Smart factory
Lao *et al.* [13]	G-PBFT	Location-based and scalable consensus protocol	Reduces consensus time, network overhead, mitigates Sybil attacks	Generic IoT
Biswas *et al.* [14]	PoBT	Lightweight consensus algorithm, ledger distribution mechanism	Improves security, computation time, memory, bandwidth	IoT business
Hossain *et al.* [15]	PoRCH	Consensus mechanism for blockchain-enabled SCADA systems	Enhances security, resilience, data integrity	Smart grids, Industry 4.0

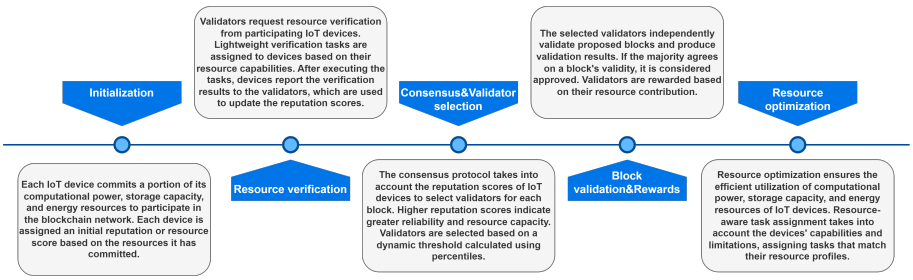

Figure 1. Enhancing resource efficiency and security: Our lightweight PoR mechanism ensures dependable transactions on constrained devices, outperforming current state-of-the-art approaches.

words, $S(i)$ refers to the sum of the committed resources of each type, multiplied by their respective weights, as follows.

$$S(i) = \textit{computational power weight} * \textit{computation power} + \textit{storage capacity weight} * \textit{storage capacity} + \textit{energy resource weight} * \textit{energy resource} \quad (1)$$

In our implementation, the weight assigned to computational power is 0.4, while storage and energy resource are assigned weights of 0.3 each. The initial reputation score provides a basis for evaluating the devices' resource contribution and establishing their starting reputation within the PoR mechanism.

3.2. Resource verification

The resource verification step involves validators requesting resource verification from participating IoT devices $i \in \{1, 2, \ldots, N\}$, assigning lightweight verification tasks $T(i)$, executing the tasks, reporting the results, and updating the reputation scores based on the verification outcomes. By periodically verifying the resources of participating devices, the mechanism ensures that devices fulfill their commitments and demonstrates their reliability and resource capacity. In the context of the PoR consensus mechanism, lightweight resource verification tasks refer to relatively simple and efficient operations that IoT devices can perform to contribute to the blockchain network, such as storage-related activities, computations, and cryptographic operations. These tasks are designed to be lightweight, considering the limited computational power, storage capacity, and energy constraints of IoT devices.

Let $V(i)$ be the set of verification results obtained by device i after executing its assigned tasks and R be the set of validators who initiate the verification process. Upon successful completion of the verification tasks, IoT device i reports the verification results $V(i)$ to the validators in R. The reported verification results $V(i)$ are used to update the reputation scores of the participating IoT devices. Note that the method for updating scores may vary depending on operational requirements and objectives. In our implementation, we increment the score by one unit following the successful verification of resources. In other words, successful completion of resource verification tasks leads to an increase in the device's reputation score, indicating its reliability and resource contribution to the network. The purpose of resource verification tasks is to assess the device's ability to fulfill its commitment and validate its suitability for participating in the blockchain network. The actual resources of the device, such as computational power, storage capacity, or energy resources, remain unchanged unless there are external factors or events that affect them. For example, if an IoT device experiences a hardware failure, a decrease in available storage capacity, or a change in its energy source, these events would result in a change in its resource levels. However, such changes are not inherent to the mechanism itself but rather external factors that may affect device resources.

3.3. Consensus protocol and validator selection

The consensus protocol and validator selection step involves the consensus protocol taking into account the reputation scores of IoT devices and selecting validators for each block based on their scores. By considering the scores, the mechanism aims to ensure fair and efficient participation in the consensus process. The selected validators collectively validate and agree on the contents of the proposed block, leading to its approval and addition to the blockchain. The consensus protocol governs how agreement is reached among the participating nodes (validators) in the blockchain network. Let B be the set of blocks to be added to the blockchain, and $L(b)$ be the set of validators selected for block $b \in B$.

During the validators selection process, higher reputation scores indicate greater reliability and resource capacity, making it more likely for devices with higher scores to be selected as validators. This approach encourages active and reliable participation in the network.

In our implementation of the PoR mechanism, we establish a threshold. If a device's reputation score is equal to or greater than the threshold, that device is selected as a validator. In this approach, we calculate the threshold based on statistical properties of the reputation scores, specifically using percentiles. This dynamic calculation allows us to adjust the threshold based on the distribution of reputation scores in the network. The threshold is defined as following:

$$P = (n/100) * N \tag{2}$$

where N represents the total number of values in the reputation score list, P denotes the desired percentile, and n corresponds to the ordinal rank of a specific value within the sorted list of values, where the values are arranged in ascending order. In other words, the percentile of x indicates the relative position of x within a set of values, expressed as a proportion of values below x multiplied by 100, relative to the total number of values. In our implementation, we consider the value of P as 75, which corresponds to the 75th percentile of the reputation score distribution. By selecting this percentile, we aim to strike a balance between inclusiveness and selectiveness when choosing validators. By utilizing the 75th percentile, we ensure that validators with relatively higher reputation scores are chosen, indicating a stronger level of trust and reliability. This approach helps to mitigate the risk of including validators with lower reputation scores that may compromise the overall security and integrity of the network. Moreover, considering a percentile-based threshold calculation allows us to adapt to changes in the reputation score distribution over time. As the network evolves and new reputation scores are generated, the threshold dynamically adjusts to maintain the desired level of selectiveness based on the statistical properties of the scores. This approach provides flexibility in adapting to varying network conditions, ensuring that the validator selection process remains robust and efficient while promoting a high level of consensus and security within the blockchain network.

3.4. Block validation and rewards

The block validation and rewards step involves the validation of approved blocks by the selected validators in the network to ensure consensus and integrity. Once a sufficient number of validators have independently validated the proposed block and agreed on its validity, the block is considered approved. More specifically, if a majority of the validators agree on the validity of the block, the consensus is reached, and the block is considered valid. Each validator independently performs the verification process by checking various aspects of the block. This includes verifying the correctness of the transactions, validating the block's structure and format, ensuring the previous block's hash matches, and verifying the digital signatures or cryptographic hashes. After performing the verification, each validator produces a validation result, indicating whether the block is valid or not.

The validators participating in the validation process are rewarded for their contribution to the network, with the rewards being proportional to their resource contribution (see Equation 3). In this formula, k represents a constant or coefficient that determines the reward rate. The value of k can be adjusted based on the desired ratio of reward to resource contribution. In our implementation, we distribute 100 reward units among validators as the reward rate.

This step reinforces the integrity of the blockchain network and encourages active participation by validators and nodes. By rewarding validators based on their resource contribution, we reinforce the integrity of the blockchain network. Validators are motivated to allocate their resources efficiently and honestly, as their rewards depend on their level of participation and the resources they commit. This block validation and rewards mechanism encourages both validators and nodes to actively participate in the network, fostering a collaborative and robust ecosystem. The combined efforts of validators and nodes contribute to the overall security and stability of the blockchain network, ultimately benefiting all participants involved.

$$R = K * Validator.reputation.score \tag{3}$$

3.5. Resource optimization

Resource optimization is a crucial aspect of the PoR mechanism for IoT devices participating in the blockchain network. The mechanism aims to maximize the utilization of limited computational power, storage capacity, and energy resources while ensuring the efficient operation of IoT devices. One of the key considerations for resource optimization is resource-aware task assignment. When assigning resource verification tasks to IoT devices, the mechanism takes into account their resource capabilities and limitations. The tasks are designed to be lightweight and tailored to the devices' computational power, storage capacity, and energy constraints. By considering the devices' resource profiles, the mechanism avoids overburdening them with tasks that exceed their capabilities and ensures that they can efficiently complete the assigned tasks within their resource constraints. Algorithm 1 provides an algorithmic description of the PoR mechanism.

Algorithm 1 Proof-of-Resource Mechanism

Step1: Initialization
for $i = 1$ to N **do**
  Commit resources: $C(i) = r_1, r_2, ..., r_M$ {Computational power, storage capacity, and energy resources}
  Calculate initial reputation score: $S(i) = 0.4 \cdot$ computational power $+ 0.3 \cdot$ storage capacity $+$ $0.3 \cdot$ energy resource
end for
Step2: Resource Verification
Validators assign verification tasks $T(i)$ to IoT devices i
for $i = 1$ to N **do**
  IoT device i executes verification tasks and reports results $V(i)$
  if verification is successful **then**
    Increment reputation score: $S(i)$ += 1
  end if
end for
Step3: Consensus Protocol and Validator Selection
Calculate threshold: threshold $= (0.75/100) \cdot N$ {75th percentile}
Select validators based on reputation scores: $L(b) = \{i \mid S(i) \geq \text{threshold}\}$ {For each block b}
Step4: Block Validation and Rewards
Validators independently validate proposed blocks and produce results
If majority agrees on block's validity, consensus is reached
Distribute rewards to validators: $R = K \cdot$ Validator.reputation.score {Reward rate}
Step5: Resource Optimization
Assign resource verification tasks considering device capabilities and limitations
Design lightweight tasks tailored to computational power, storage capacity, and energy constraints

4. Implementation details

In this section, we provide a detailed overview of the implementation aspects of the PoR mechanism for IoT devices in the context of blockchain. We discuss key components, algorithms, and considerations involved in realizing the PoR mechanism.

The PoR mechanism is programmed in Python using the Spyder IDE. All functionalities related to the hash function are implemented using the standard Python hashlib library.
A simulation involving fifteen IoT devices is conducted to participate in the blockchain network. For each IoT device, resource commitments such as computing power, storage capacity, and energy are generated using a random function. In addition, the blockchain network maintains a list of validators and records the validated blocks that are added to the chain.
In the context of resource verification, we have established three lightweight storage-related tasks. These tasks encompass data retrieval, data validation, and data processing. Furthermore, we determine the resource requirements for performing these tasks by utilizing a random function. Then, we have defined the `"get_suitable_devices"` function, which checks whether a given device is suitable for performing each of these tasks or not. This determination is based on considering the device's available resources and comparing them with the resource requirements of the task.
To create a new block, the first step is to instantiate a new block object from the related class. Next, we populate the block with transactions, data, and other relevant information, including a timestamp and the hash of the previous block. To achieve this, we define the structure of transactions using a Transaction class. Subsequently, we add these transactions to a transaction pool or mempool as pending transactions. This allows us to keep track of all the transactions that are awaiting verification and inclusion in the blockchain.
During the block verification process, we incorporate a cryptographic challenge by generating a hash challenge using SHA-256 and requesting validators to solve it before doing the validation. This challenge serves as an additional step to ensure the integrity and security of the blockchain network.
At the end of the block validation process, if the majority of the selected validators determine the new block to be valid, the block will be added to the validated blocks. This ensures that only blocks deemed valid by a majority of validators are added to the blockchain.

5. Performance evaluation

The performance evaluation serves as a crucial stage in gauging the effectiveness and efficiency of the proposed PoR mechanism within the context of IoT devices. In this section, we establish the performance criteria based on which the PoR mechanism is evaluated. We examine the system's performance through several key indicators, namely security, fairness, and a comparative analysis with existing mechanisms.

5.1. Security discussions

We assess the mechanism's capacity to uphold the security and integrity of the blockchain network. Specifically, we delve into the effectiveness of the resource verification tasks in thwarting malicious activities and guaranteeing data validity. Furthermore, we analyze the resilience of the consensus protocol against attacks and evaluate the robustness of the validator selection process. Through these evaluations, we gain insights into the mechanism's ability to maintain a secure and trustworthy blockchain network. The PoR consensus mechanism exhibits several security strengths that contribute to the overall robustness and integrity of the blockchain network. These strengths address specific security challenges faced by IoT devices and enhance the security of the consensus process.

- *Resource-driven consensus:* The primary strength of the PoR mechanism lies in its resource-driven approach to consensus. By leveraging the available resources of IoT devices, such as computational power, storage capacity, and energy, this mechanism aligns the consensus process with the underlying physical capabilities of the devices. This alignment enhances the resistance against resource-based attacks and ensures that the consensus is achieved through legitimate resource contributions.

- *Sybil attack resistance:* The PoR mechanism provides inherent resistance against Sybil attacks. Sybil attacks involve adversaries creating multiple identities or nodes to gain control or disrupt the network. Since IoT devices participating in the mechanism need to provide verifiable proof of their resources, the creation of multiple identities becomes challenging for adversaries. The resource verification process acts as a barrier against Sybil attacks, as each device must demonstrate genuine resource capabilities.

- *Transparent and auditable:* The PoR mechanism provides transparency and auditability, which are essential for ensuring the trustworthiness of the consensus process. By requiring IoT devices to provide verifiable proof of their resources, the mechanism enables anyone to independently verify the legitimacy of resource contributions. This transparency enhances trust among participants and allows for effective detection of malicious activities or attempts to manipulate the consensus.

- *Consensus diversity:* The PoR mechanism promotes consensus diversity by considering various resource types and their combinations. By allowing IoT devices to contribute different resources,

such as CPU cycles, storage space, or network bandwidth, the mechanism avoids concentration of power in a specific resource domain. This diversity enhances the decentralization and resilience of the consensus process, making it more robust against resource-specific attacks or monopolistic behavior.

5.2. Fairness evaluation

Fairness in the blockchain network is an important aspect to ensure equitable participation and rewards distribution among the network participants. In this section, we introduce the fairness Gini Index as a metric to evaluate the fairness of the reward distribution mechanism.

The Gini coefficient is a widely used measure of income inequality in economics and can be adapted to measure fairness in blockchain networks. In our context, we define the Fairness Gini Index (FGI) to assess the distribution of rewards among validators and non-validators in the network [16]. The FGI ranges from 0 to 1, where 0 indicates perfect fairness (all participants receive an equal share of rewards) and 1 represents maximum unfairness (one participant receives all the rewards). The formula for calculating the FGI is as follows:

$$FGI = 1 - ((V^2 + NV^2)/R^2) \tag{4}$$

where V is the proportion of rewards earned by validators, NV is the proportion of rewards earned by non-validators, and R is the total reputation of all devices (validators and non-validators) in the network.

To evaluate the fairness of our proposed PoR mechanism, we measured the FGI after each block validation process. We collected the reputation scores of all devices in the network and calculated the rewards earned by validators and non-validators. For each block, we calculated the V and NV values using the reputation scores and rewards earned by validators and non-validators, respectively. We then computed the FGI using the formula mentioned above. After conducting simulations and validating 100 blocks within our network, we proceeded to analyze the fairness of reward distribution by employing the FGI. Throughout multiple runs, we observed diverse results ranging from 0.056 to 0.061. The relatively low FGI values indicate a fair distribution of rewards among validators and non-validators. However, further investigations are required to analyze the impact of different parameters, such as reputation scores and reward calculation methods, on the fairness of the network.

5.3. Comparative analysis with other consensus mechanisms

Consensus mechanisms play a vital role in blockchain and distributed ledger technologies by ensuring agreement and validity of transactions across a decentralized network. When evaluating different consensus mechanisms, scalability and throughput are crucial factors to consider. Scalability refers to the ability of a system to handle an increasing number of participants or transactions without compromising performance. Throughput, on the other hand, refers to the rate at which transactions can be processed and confirmed within a given time frame. Our comparative analysis of different consensus mechanisms reveals important insights regarding their scalability and throughput characteristics. PoW demonstrates limitations in scalability as the network size increases due to the computational requirements for mining. Similarly, PoW exhibits limited throughput due to the computational complexity involved in the mining process. PoS offers improved scalability compared to PoW but still faces challenges with larger network sizes. The throughput of PoS depends on the block creation and validation process, affecting its overall performance.

PBFT demonstrates scalability for smaller networks, but scalability decreases as the number of participating nodes increases. It offers high throughput for small to medium-sized networks, but this throughput decreases when dealing with a larger number of participants. DPoS showcases scalability due to the delegation of block creation to a limited number of trusted nodes. DPoS also exhibits high throughput, thanks to its efficient block creation and validation process.

PoET demonstrates scalability due to its low computational requirements and the parallel processing capabilities of IoT devices. Its high throughput is facilitated by the asynchronous and parallel execution of tasks on multiple IoT devices. PoA shows scalability by allowing multiple transactions to occur simultaneously across the network. PoA has the potential for high throughput due to the parallel processing of multiple transactions across the DAG network.

Hybrid consensus mechanisms exhibit varying levels of scalability and throughput, depending on the specific combination of consensus mechanisms employed. The scalability and throughput of these hybrid approaches depend on the efficiency of the individual mechanisms in block validation and transaction processing. PoR demonstrates scalability dependent on the available resources in the network and efficient load balancing. It has the potential for high scalability as resources can be dynamically allocated based on network demands.

6. Concluding remarks and future directions

In this paper, the integration challenges of blockchain technology with IoT have been addressed, and a lightweight, energy-efficient consensus mechanism known as PoR has been proposed, specifically designed for resource-constrained IoT devices. The inherent capabilities of IoT device resources have been leveraged by PoR, offering an effective solution for establishing consensus in IoT environments. The feasibility and effectiveness of PoR have been demonstrated through simulation using IoT devices. The results have shown that PoR enables secure and efficient data exchange among IoT devices while minimizing resource consumption, making PoR an ideal consensus mechanism for IoT applications where energy efficiency and scalability are crucial.

Several advantages over traditional consensus mechanisms in terms of resource efficiency and security are offered by the proposed PoR mechanism. By using IoT device resources as a basis for consensus, the need for computationally intensive tasks has been eliminated by PoR, thereby reducing the energy consumption and computational overhead associated with blockchain operations on IoT devices. This research contributes to the advancement of blockchain integration with IoT by addressing the challenges of scalability, resource efficiency, and security.

However, several challenges and open questions have also been highlighted by our analysis that warrant further investigation:

- Scalability challenges: Achieving scalability in large-scale networks with a significant number of participating nodes is a primary challenge. Some consensus mechanisms have shown promise in smaller networks, but their scalability is diminished as the network size increases. Innovative approaches to improve scalability in such scenarios should be explored in future research.

- Throughput optimization: Room for future research in the optimization of throughput in consensus mechanisms exists. Even though some mechanisms demonstrate high throughput, the efficiency of block creation, validation, and transaction processing can be significantly enhanced, thereby boosting the overall throughput of a consensus mechanism.

- Security considerations: Security remains a critical concern in consensus mechanisms. The security implications of different mechanisms should be evaluated in future research, and approaches to enhance resistance against various attacks and vulnerabilities should be explored.

Acknowledgement. This work was supported by the IoTalentum project within the framework of Marie Sklodowska-Curie Actions Innovative Training Networks-European Training Networks (ITN-ETN) (grant number 953442) which is funded by the European Union Horizon 2020 research and innovation program.

References

[1] Kök, İ., Okay, F.Y., Muyanlı, Ö., Özdemir, S.: Explainable artificial intelligence (xai) for internet of things: a survey. IEEE Internet of Things Journal (2023)

[2] Qiu, T., Chen, N., Li, K., Atiquzzaman, M., Zhao, W.: How can heterogeneous internet of things build our future: A survey. IEEE Communications Surveys & Tutorials **20**(3) (2018) 2011–2027

[3] Abbasi, M., Plaza-Hernández, M., Prieto, J., Corchado, J.M.: Security in the internet of things application layer: Requirements, threats, and solutions. IEEE Access **10** (2022) 97197–97216

[4] Mezquita, Y., Plaza-Hernández, M., Abbasi, M., Prieto, J.: Cryptocurrencies, systematic literature review on their current context and challenges. In: International Congress on Blockchain and Applications, Springer (2023) 162–172

[5] Majeed, U., Khan, L.U., Yaqoob, I., Kazmi, S.A., Salah, K., Hong, C.S.: Blockchain for iot-based smart cities: Recent advances, requirements, and future challenges. Journal of Network and Computer Applications **181** (2021) 103007

[6] Platt, M., Sedlmeir, J., Platt, D., Xu, J., Tasca, P., Vadgama, N., Ibañez, J.I.: The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In: 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C), IEEE (2021) 1135–1144

[7] Jiang, W., Wu, X., Song, M., Qin, J., Jia, Z.: A scalable byzantine fault tolerance algorithm based on a tree topology network. IEEE Access **11** (2023) 33509–33519

[8] Lao, L., Dai, X., Xiao, B., Guo, S.: G-pbft: a location-based and scalable consensus protocol for iot-blockchain applications. In: 2020 IEEE international parallel and distributed processing symposium (IPDPS), IEEE (2020) 664–673

[9] 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)

[10] Liu, Z., Hou, L., Zheng, K., Zhou, Q., Mao, S.: A dqn-based consensus mechanism for blockchain in iot networks. IEEE Internet of Things Journal **9**(14) (2021) 11962–11973

[11] Fu, J., Zhang, L., Wang, L., Li, F.: Bct: An efficient and fault tolerance blockchain consensus transform mechanism for iot. IEEE Internet of Things Journal (2021)

[12] Huang, J., Kong, L., Chen, G., Cheng, L., Wu, K., Liu, X.: B-iot: Blockchain driven internet of things with credit-based consensus mechanism. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), IEEE (2019) 1348–1357

[13] Li, C., Zhang, J., Yang, X., Youlong, L.: Lightweight blockchain consensus mechanism and storage optimization for resource-constrained iot devices. Information Processing & Management **58**(4) (2021) 102602
[14] Biswas, S., Sharif, K., Li, F., Maharjan, S., Mohanty, S.P., Wang, Y.: Pobt: A lightweight consensus algorithm for scalable iot business blockchain. IEEE Internet of Things Journal **7**(3) (2019) 2343–2355
[15] Hossain, M.T., Badsha, S., Shen, H.: Porch: A novel consensus mechanism for blockchain-enabled future scada systems in smart grids and industry 4.0. In: 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE (2020) 1–7
[16] Türk, U., Östh, J.: Introducing a spatially explicit gini measure for spatial segregation. Journal of Geographical Systems (2023) 1–20