Blockchain: Research and Applications 7 (2026) 100369

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

Research Article

EcoChain: A novel forest-inspired blockchain network architecture

Robertas Damaševičius [a,*], Gintautas Mozgeris [a], Tomas Krilavičius [b], Rytis Maskeliūnas [a]

[a] Center of Real Time Computer Systems, Kaunas University of Technology, Kaunas 44001, Lithuania
[b] Center of Excellence Forest 4.0, Vytautas Magnus University, Akademija 53067, Lithuania

ARTICLE INFO

Keywords:
Blockchain
Sustainability
Resilience
Cloud computing
Edge computing
Forest-inspired computing

ABSTRACT

Background: Blockchain technology, serving as the backbone for various sectors, faces challenges in sustainability and resilience. Traditional blockchain mechanisms, while secure, are not environmentally sustainable due to high energy consumption. This study introduces EcoChain, a novel blockchain architecture inspired by forest ecosystems, with the aim of addressing these challenges. *Objective:* To develop a sustainable, resilient, and efficient blockchain architecture drawing inspiration from the self-sustaining, adaptive, and diverse nature of forests. *Methods:* EcoChain integrates principles from forest ecosystems, such as diversity, symbiosis, and natural selection, into blockchain technology. The mechanism encompasses energy accumulation that is similar to photosynthesis, decomposition for node removal, symbiotic relationships for resource sharing, natural predation for security, and adaptive mechanisms to respond to environmental changes. A mathematical model is provided along with a hierarchical node structure that includes a seed, a sapling, a mycelium network, and guardian nodes. *Results:* The experimental evaluation demonstrates that EcoChain enhances network performance, reduces transaction latency, and improves the overall resilience of the system against attacks and failures. *Conclusions:* EcoChain presents a novel approach to blockchain, merging forest-inspired ecological principles with digital technology to develop sustainable, resilient, and efficient blockchain systems.

1. Introduction

1.1. Context and background

Blockchain technology, often hailed as the backbone of the next-generation Internet, has attracted significant attention due to its potential to revolutionize various sectors, from finance [1] to supply chain management [2], healthcare [3], smart manufacturing [4], education [5,6], energy sector [7,8], communications [9], and beyond.

Blockchain technology, at its core, is a decentralized digital ledger that records transactions on a network of computers [10]. This ensures not only transparency but also immutability of records, thus fostering trust among participants without the need for a central authority. Innovation lies in its use of distributed consensus mechanisms that enable secure and verifiable transactions [11]. Each block in the chain contains a number of transactions; once a block is completed, it is linked to the previous block, forming a chain of blocks with fixed and tamper-resistant information. The decentralized nature of blockchain offers significant advantages in terms of security, privacy, and efficiency over traditional centralized systems [12]. Its applicability extends beyond cryptocurrencies to areas such as supply chain management, smart contracts, and identity verification, demonstrating its potential to revolutionize various sectors by ensuring integrity, transparency, and efficiency [13]. The integration of blockchain in various application areas, as discussed in Ref. [14], highlights its versatility and potential in diverse fields.

1.2. The need for sustainable and resilient systems

In the contemporary discourse surrounding blockchain technology [15], the emphasis has progressively shifted from mere functionality to the broader implications of these systems on social infrastructures and the environment [16,17]. This change underscores the paramount importance of sustainability and resilience in blockchain consensus mechanisms [18]. The environmental footprint of blockchain systems, particularly those that employ proof-of-work (PoW) consensus mechanisms, has been a topic of intense scrutiny. The computational intensity required by PoW, as exemplified by Bitcoin's energy consumption, has raised pertinent questions about the long-term viability of such systems. The International Energy Agency reported in 2021 that Bitcoin's energy consumption surpassed that of some nations, underscoring the

* Corresponding author.
E-mail addresses: robertas.damasevicius@ktu.lt (R. Damaševičius), gintautas.mozgeris@vdu.lt (G. Mozgeris), tomas.krilavicius@vdu.lt (T. Krilavičius), rytis.maskeliunas@ktu.lt (R. Maskeliūnas).

https://doi.org/10.1016/j.bcra.2025.100369
Received 4 March 2024; Received in revised form 13 October 2024; Accepted 21 May 2025

Available online 27 August 2025
2096-7209/© 2025 THE AUTHORS. Published by Elsevier B.V. on behalf of Zhejiang University Press. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

urgency for more sustainable alternatives. As global attention focuses on environmental conservation and carbon neutrality [19], the onus is on blockchain technologies to align with these objectives.

Beyond sustainability, the resilience of a blockchain system determines its robustness in the face of adversarial threats and systemic vulnerabilities. In a decentralized paradigm, where trust is distributed and is not anchored to a central authority, the system's ability to withstand attacks, adapt to evolving threats, and recover from potential failures becomes crucial [20]. Sustainability and resilience are not mutually exclusive, but rather intertwined. A truly sustainable system is not only environmentally conscious but also resilient to both internal and external perturbations. In contrast, a resilient system, due to its adaptive capabilities, can ensure its sustainable operation over long periods, even in the face of evolving challenges [21–23].

As blockchain technology matures and permeates diverse sectors, from finance to healthcare [24,25], supply chains [26,27], real estate [28], construction [29], education [30], drones [31], and beyond, the consensus mechanisms that underlie these systems must evolve. This evolution should address not only the immediate challenges of scalability and efficiency but also the overarching imperatives of sustainability and resilience. Such a holistic approach will ensure that blockchain technology remains a force of positive transformation in the digital age [32].

1.3. The need for new consensus mechanisms

At the heart of the functionality and security of the blockchain is its consensus mechanism [33], which ensures that all participants in the network agree on a single version of the truth. The concept of consensus in distributed systems is not new. However, blockchain brought it to the forefront due to the unique challenges it presented: achieving consensus in a decentralized, trustless environment where participants might have incentives to act maliciously [34]. In a blockchain, a consensus mechanism serves multiple purposes. Validation ensures that the transactions added to the block are valid and adhere to the network's rules. Consistency ensures that all participants in the network have a consistent view of the ledger. Security protects the network against malicious actors and potential attacks, such as the double-spending problem. Over the years, various consensus mechanisms have been proposed and implemented, each with its advantages and drawbacks:

- PoW is the first and most well-known consensus mechanism, used by Bitcoin. It requires participants (miners) to solve complex mathematical puzzles, which consumes significant computational power. It is secure but energy-intensive [35–43].
- Proof-of-stake (PoS) is a more energy-efficient alternative to PoW. Participants (validators) are chosen to create new blocks based on the number of coins they hold and are willing to "stake" or lock up as collateral [44–51].
- Delegated proof-of-stake (DPoS) is a variation of PoS in which coin holders vote for a small number of delegates, who then validate transactions and create new blocks.
- In proof-of-authority (PoA), transactions are validated by approved accounts, known as validators. It is faster than PoW but centralizes control to some extent.
- In proof-of-space/storage, participants prove that they have allocated a certain amount of storage space to the network.

Although blockchain consensus mechanisms have been instrumental in ensuring the security and functionality of decentralized networks, they are not without challenges. PoW, in particular, has been criticized for its environmental impact due to the vast amounts of energy it consumes. Some mechanisms, such as DPoS and PoA, can lead to centralization, where a few nodes or participants have disproportionate control over the network. As blockchain networks grow, ensuring fast transaction times while maintaining security becomes a challenge [52–55].

1.4. Novelty and contribution

This research introduces "EcoChain", a forest-inspired consensus mechanism that bridges this dichotomy by offering a novel approach to blockchain consensus. Drawing parallels from the intricate dynamics of forest ecosystems, EcoChain mimics principles of diversity, interdependence, growth, and decay, departing from traditional mathematical or game-theoretic models and providing a fresh perspective on consensus design. EcoChain's design inherently reduces computational and energy demands typically associated with blockchain validation processes, presenting a more sustainable alternative without compromising transactional performance or security. In addition, EcoChain features mechanisms that allow it to adapt to varying network conditions, much like a forest responding to environmental changes, ensuring optimal performance and resilience. Moreover, beyond mere transaction validation, EcoChain introduces symbiotic relationships and natural predation, enhancing network security and trustworthiness with a multifaceted security approach that addresses both internal and external threats, thereby ensuring robustness.

1.5. Structural organization

The paper is structured as follows: First, the article introduces the concept. Section 2 provides a review of the relevant work. Section 3 details EcoChain's core concept, drawing parallels between ecological principles and blockchain functionalities. Section 4 provides a comprehensive overview of EcoChain, covering its principles, node organization, and specific mechanisms. Section 5 offers architectural details, consensus mechanisms, security protocols, adaptation mechanisms, and integration interfaces. Section 6 assesses EcoChain's performance, analyzing network throughput, transaction latency, smart contract execution time, and block confirmation time. Finally, the paper is summarized by discussion and conclusions in Section 7.

2. Related work

Forest-related adaptations to blockchain networks are gaining attention for their potential to enhance transparency, traceability, and efficiency in managing forest ecosystems and resources, often to address specific environmental challenges such as deforestation, illegal logging, carbon emissions, and sustainable resource management [56]. The integration of blockchain with the Internet of Things (IoT) and advanced cryptographic protocols [57] is advancing the capacity of blockchain to monitor, manage, and conserve forest resources more effectively [58]. In this section, we examine how relevant research in blockchain technology specifically targets the challenges and opportunities in forest management, with an emphasis on improving operational efficiency.

2.1. IoT with blockchain systems and real-time forest monitoring

The integration of IoT sensors with blockchain systems represents a key advancement in forest management, as it allows for real-time monitoring of forest ecosystems [58]. IoT devices placed in forested areas can collect data on environmental conditions, such as tree growth, humidity, soil composition, and even the detection of illegal logging activities [59]. IoT devices can relay data directly to blockchain networks [60], where the information is securely recorded and made available to stakeholders. Research to improve the efficiency of these systems focuses on reducing the energy consumption of IoT devices while ensuring high reliability and speed in data transmission [61].

The use of blockchain with IoT provides efficiency gains in forest monitoring, as data from remote areas can be verified without requiring physical inspections [58]. The state-of-the-art in this domain includes the deployment of low-power, energy-efficient IoT devices combined with lightweight blockchain protocols to ensure sustainability [62]. Researchers are exploring the use of directed acyclic graph systems, such as

IOTA, which are designed to support high-frequency transactions from thousands of connected devices without the energy overhead of traditional blockchains. This approach minimizes the energy impact of data collection while ensuring that changes in forest ecosystems are recorded in an immutable, transparent ledger [63].

2.2. Tokenization of forest resources and carbon credits

One of the most notable research trends in this field is the tokenization of forest assets [64], such as carbon credits and timber resources, on blockchain networks. The tokenization process here involves the creation of digital assets that represent real-world entities such as forested land, carbon stocks, or harvested timber. The blockchain ensures that transactions related to these assets are transparent and immutable [65], offering a way to track resource use and prevent double-counting of environmental benefits, such as carbon offsets.

Researches pioneered the use of blockchain for issuing carbon credits [66,67] that represent verifiable emissions reductions from reforestation or forest conservation projects [68]. These credits are tokenized and traded on a decentralized marketplace, where the blockchain ensures the authenticity and uniqueness of each token. Tokenization not only adds greater transparency, but also introduces efficiency by automating the verification process [69,70]. Studies are exploring the potential of smart contracts to automatically trigger payments or rewards when predefined conditions are met, such as carbon sequestration goals, reducing the reliance on manual verification systems [71]. Current research also addresses the limitations of tokenization [72], particularly how to integrate remote sensing and satellite data to automatically verify changes in the forest cover and track carbon sequestration [73]. The purpose of the researchers is to streamline forest management by linking real-time environmental data with tokenized assets, offering a transparent and efficient means of overseeing reforestation and deforestation projects [74].

2.3. Decentralized and secure forest governance

Another area of research focuses on the use of blockchain for decentralized governance in forest management [75]. Forests are often managed by multiple stakeholders, including governments, indigenous communities, private companies, and conservation organizations. Blockchain-based decentralized autonomous organizations (DAOs) allow for a more equitable and transparent governance structure by allowing stakeholders to participate in decision-making processes through blockchain voting systems [76]. Recent research has examined how DAOs can be applied to forest management, particularly in cases where ownership and resource rights are contested [58]. Quadratic voting systems, which allow stakeholders to express the intensity of their preferences [77], have been explored as a way to ensure that smaller or marginalized communities can have a more proportional say in forest management decisions. Blockchain ensures that voting outcomes are transparent and immutable, reducing the potential for corruption or manipulation in the decision-making process [78].

Ensuring the privacy and security of forest data is a critical concern in blockchain applications, particularly in cases where sensitive information must be protected [79]. For example, data about specific logging patterns may need to be kept private to avoid exploitation. Current cryptography research explores methods such as zero-knowledge proofs (ZKPs) and homomorphic encryption to allow verification of environmental data without revealing the underlying information [80]. ZKPs are particularly promising for forest management applications [81]. ZKPs allow entities to prove that certain environmental actions [82], such as carbon sequestration or forest regeneration, have occurred without disclosing exact details such as geographical location or land ownership. ZKPs ensure that sensitive data remains secure [83], allowing transparent and verifiable potential tracking of forest management efforts on the blockchain.

2.4. Energy-efficient consensus and transaction mechanisms

Given the environmental focus of forest management applications and resulting in huge amounts of data to process, reducing the energy consumption of blockchain networks is a priority [84]. Traditional blockchain systems based on PoW algorithms consume substantial amounts of energy, which could negate the environmental benefits of blockchain-based forest conservation [85]. In response, research has shifted to more energy-efficient consensus mechanisms, such as PoS, DPoS, and PoA [86], which often can reduce the computational power needed for network validation [87], aligning with the sustainability goals of forest management projects.

Ethereum's transition to Ethereum 2.0 and PoS consensus is being studied as a model for blockchain systems designed for environmental concerns [88]. PoS drastically lowers energy requirements by allowing validators to stake tokens instead of performing energy-intensive calculations to add new blocks. Recent research in this area has focused on how PoS mechanisms can be optimized for forest-related use cases, ensuring that the energy efficiency of blockchain networks complements the environmental objectives of sustainable forest management [89].

PoA consensus models are also being examined in the context of management projects [90]. PoA relies on a limited set of trusted validators, making it particularly suitable for cases where centralized entities, such as government agencies or international non-governmental organizations (NGOs), are responsible for validating transactions related to forest conservation. PoA model offers rapid transaction finality and minimal energy consumption [87], further improving the efficiency of blockchain applications in forest ecosystems [89].

Layer-2 solutions are also being explored as a way to improve the efficiency of blockchain systems in managing large volumes of transactions [91], including those related to agriculture and forest resources [92]. In forest management, multiple transactions may occur in rapid succession, such as the issuance of carbon credits, the trading of timber rights, or the allocation of conservation funds [93]. Processing these transactions on the main blockchain can be costly and time-consuming. Layer-2 solutions, such as sidechains, rollups, and state channels, allow off-chain or parallel processing of transactions, alleviating the load burden on the main blockchain [91].

3. The forest ecosystem: An inspiration

Forests, with their intricate web of life, have long been a source of fascination and study. Their ability to sustain diverse forms of life, recover from disturbances, and adapt to changing conditions, offers inspiration for the design of systems that are both resilient and sustainable, as the forest ecosystem provides a compelling blueprint [21,94,95]. This section focuses on the inherent attributes of the forest and extrapolates lessons for the blockchain domain.

3.1. Diversity and resilience in forests

Forests are a testament to the power of biodiversity. This diversity is not merely a collection of different species, but a complex interplay that confers numerous benefits. A diverse forest is less susceptible to disturbances such as diseases or pests that can decimate a single species [96–98]. Similarly, on a blockchain, a diverse network of nodes can prevent systemic failures or targeted attacks [99]. Different species in a forest have different resources and nutrition patterns, ensuring that resources are used efficiently without depletion [100,101]. This principle can be applied to blockchain systems to optimize resource allocation and consumption. A biodiverse forest can better adapt to changing environmental conditions, ensuring its survival through climatic changes [102–104]. In terms of blockchain, a diverse network can adapt to changing technological and threat landscapes.

Table 1
Comparison of forests and blockchain technology.

Criterion	Forests	Blockchain
Risk mitigation	A diverse forest is less susceptible to diseases or pests, ensuring resilience.	A diverse network of nodes enhances security against systemic failures or attacks.
Resource optimization	Species have varied needs and nutrition patterns, optimizing resource use without depletion.	Diverse node capabilities optimize resource allocation and consumption.
Adaptive capacity	Biodiversity enables forests to adapt to environmental changes, ensuring survival.	A diverse network can adapt to changing technologies and threats.
Growth and succession	Forests evolve from grasslands to old-growth forests, establishing stable ecosystems through succession.	Blockchains evolve with newer nodes and protocols, maintaining relevance and efficiency.
Decay and regeneration	The decay of plant matter provides nutrients for new growth, promoting regeneration.	Outdated or compromised nodes are replaced or updated to ensure network health.
Interdependence	Symbiotic relationships, such as those between fungi and tree roots, underscore collaboration for mutual benefit.	Nodes collaborate for enhanced security and efficiency, highlighting the importance of interdependence.

3.2. Growth, decay, and interdependence

Forests are dynamic systems characterized by cycles of growth, decay, and regeneration. This cyclical nature ensures sustainability and balance: Forests undergo successional stages, transitioning from grasslands or severe disturbances of stand replacement to old-growth forests over time [105]. This growth process allows the establishment of a stable ecosystem. Similarly, a blockchain can evolve, with newer nodes or protocols succeeding older ones, ensuring its continued relevance and efficiency. The decomposition of old or dead plants provides nutrients for new growth [106,107]. In the blockchain, outdated or compromised nodes can be replaced or updated, ensuring the health of the network. Symbiotic relationships in forests, such as those between fungi and tree roots, highlight the power of collaboration for mutual benefit [108–111]. Blockchain systems can foster inter-node collaborations for enhanced security and efficiency.

Similarly, the concept of a velvet fork in blockchain networks [112,113] mirrors these natural processes by introducing upgrades or modifications in a nondisruptive manner, ensuring the continuity of the system without rendering previous structures obsolete. In a velvet fork, both new and old nodes can co-exist and collaborate [112], much like how diverse species in a forest contribute to ecosystem resilience. Rather than forcing an abrupt transition, velvet forks enable a gradual adaptation, where nodes that adopt new protocols can still interact with older ones, maintaining the overall health of the blockchain network, particularly important in IoT-driven applications [114]. Such approaches, in principle, parallel the process of ecological succession, where new growth does not replace but builds upon the foundations of earlier ecosystems, ensuring long-term stability and adaptation to changing conditions. Furthermore, just as symbiotic relationships in forests support the thriving of different species, velvet forks facilitate interoperability and cooperation within the network, allowing it to evolve in a decentralized yet cohesive manner [115].

3.3. Lessons for blockchain systems

The forest ecosystem, with its millennia of evolution, offers a treasure trove of lessons to design resilient, sustainable, and efficient systems. By observing and emulating these natural processes, blockchain technology can achieve unprecedented levels of sustainability and resilience. Drawing parallels between forest ecosystems and blockchain networks offers several actionable lessons transferable to system design.

- Just as a diverse forest is more resilient, a diverse network of nodes, both in terms of geographic distribution and functional roles, can enhance the resilience of blockchain.
- Blockchain networks should prioritize sustainable growth, ensuring that resource consumption (like energy in PoW systems) does not outpace the network's capacity or harm the broader environment.
- Encouraging collaborative mechanisms, similar to symbiotic relationships in forests, can lead to a more secure and efficient blockchain system.
- Blockchain systems should have mechanisms for updates, replacements, and improvements, mirroring the decay and regeneration processes in forests.

The parallels between forests and blockchain networks are summarized in Table 1.

4. EcoChain: Overview

4.1. Principles underlying EcoChain

EcoChain is underpinned by several foundational principles, extrapolated from the forest ecosystem. Similar to a forest that thrives on the **diversity** of its inhabitants, EcoChain promotes a diverse network of nodes, ensuring resilience against targeted attacks and systemic vulnerabilities. EcoChain's consensus mechanism is designed to **optimize resource consumption**, ensuring that energy and computational demands do not escalate to unsustainable levels. The nodes in the EcoChain network are encouraged to form **symbiotic relationships**, pooling resources and sharing rewards, mirroring the mutualistic interactions observed in forests. EcoChain incorporates mechanisms that allow seamless **adaptation to updating** or replacement of nodes, ensuring that the network remains current and secure.

4.2. Formal description of EcoChain

Given the forest-inspired nature of EcoChain, we can represent the consensus mechanism using the following notations:

1. **Nodes representation**. Let N be the set of all nodes in the network, where $N = \{n_1, n_2, \ldots, n_k\}$. Each node n_i has an associated energy level $E(n_i)$ which is a function of the number of transactions it validates and the relationships it forms.
2. **Energy accumulation (photosynthesis mechanism)**. The energy accumulation for a node n_i over time t can be represented as

$$E(n_i, t) = \int_0^t v(n_i, \tau) d\tau \tag{1}$$

where $v(n_i, \tau)$ is the validation rate of node n_i at time τ. In practice, the energy rate $v(n, \tau)$ is integrated over the time interval between two blocks

$$\Delta E(n) = \int_{t_i}^{t_{i+1}} v(n, \tau) d\tau \tag{2}$$

where t_i and t_{i+1} are the timestamps of consecutive blocks.

3. **Decomposition mechanism**. If a node's energy drops below a certain threshold θ, it decays if

$$E(n_i, t) < \theta \tag{3}$$

then n_i is removed from N.

Symbiotic relationships. Let R be the set of all relationships in the network. A relationship between nodes n_i and n_j results in shared energy accumulation

$$\begin{aligned} E(n_i, t)' &\leftarrow E(n_i, t) - \alpha \cdot E(n_j, t) \\ E(n_j, t)' &\leftarrow E(n_j, t) + \alpha \cdot E(n_i, t) \end{aligned} \tag{4}$$

where $0 < \alpha < 1$ is the sharing factor, and $\alpha \cdot E(n_i, t)$ is energy transferred from node n_i to node n_j, ensuring that energy is conserved.

4. **Natural predation**. Let G be the set of guardian nodes. A guardian node $g \in G$ monitors nodes in N and isolates a node n_i if it detects malicious activity if g detects malicious activity in n_i then

$$E(n_i, t) = 0 \tag{5}$$

5. **Seasonal adjustments**. The validation difficulty $D(t)$ can be represented as a periodic function to simulate seasonal changes

$$D(t) = D_0 + D_1 \sin(\omega t + \phi) \tag{6}$$

where D_0 is the average difficulty, D_1 is the amplitude of the difficulty changes, ω is the frequency and ϕ is the phase shift. Our idea here is that such a periodic adjustment model mimics natural cycles, where seasons affect the availability of resources, allowing the network to dynamically adjust its operational parameters. The validation difficulty can be reduced during low-activity periods to make it easier for nodes to participate in consensus processes and prevents unnecessary energy consumption when fewer transactions are processed. This type of design choice in EcoChain allows for adjusting validation difficulty to align with the availability of energy resources, particularly in settings where renewable energy sources fluctuate seasonally. During times of higher energy availability, the network can operate at full capacity, while during energy-scarce periods, the difficulty can be lowered to conserve energy and avoid overloading the network.

4.3. Node structures in EcoChain

EcoChain, inspired by the intricate dynamics of forest ecosystems, introduces a hierarchical node structure that mirrors the growth and interdependence observed in forests. This structure ensures a balance between trust, decentralization, and efficiency.

4.3.1. Seed nodes

Seed nodes, analogous to the trees of previous generations in a forest, serve as the foundational pillars of the EcoChain network.

Let S be the set of all seed nodes in the network, where $S = \{s_1, s_2, \ldots, s_m\}$. Seed nodes primarily handle transaction validation and block proposal. Given their established trust, they play a crucial role in maintaining the integrity of the network. A node n becomes a seed node if

$$E(n, t) > \Theta \tag{7}$$

where $E(n, t)$ represents the energy accumulated by node n over time t and Θ is a predefined energy threshold for seed node status.

The seed nodes are responsible for

1. Validating and proposing blocks to maintain the integrity and trustworthiness of the blockchain by checking transactions for compliance with network rules and assembling them into blocks to be added to the blockchain.
2. Monitoring and mentoring sapling nodes. The seed nodes also oversee the growth and health of the sapling nodes, acting as mentors. They provide guidance and support to ensure that sapling nodes contribute effectively to the network, fostering a robust and resilient blockchain ecosystem.
3. Participating in consensus voting with higher voting power. These nodes have a significant influence on the network consensus mechanism. Given their higher voting power, seed nodes are pivotal in making decisions about block additions and other critical changes to the blockchain protocol, ensuring that consensus is reached in a secure and efficient manner.

4.3.2. Sapling nodes

The sapling nodes represent the intermediate layer of trust in the EcoChain network, analogous to the younger trees in a forest that are growing and establishing their presence.

Let P be the set of all the sapling nodes in the network, where $P = \{p_1, p_2, \ldots, p_n\}$. The sapling nodes assist the seed nodes in transaction validation and also relay transactions from the mycelium network. Sapling nodes are tasked with

1. Assisting in transaction validation as the sapling nodes contribute to the integrity of the network by participating in the verification process of transactions. Their role ensures that transactions are legitimate and conform to the network's rules, enhancing security and reliability.
2. Relay transactions and blocks, as these nodes act as intermediaries, facilitating the propagation of transactions and blocks across the network. This ensures a timely and efficient dissemination of information, which is crucial to maintaining the current and synchronized state of the blockchain.
3. Monitoring of mycelium network nodes. In the metaphor of a forest ecosystem, where the mycelium represents the underlying network that connects various entities, the sapling nodes monitor these connections for health and functionality. This involves checking the status of other nodes and the general health of the network, similar to how the mycelium in forests supports communication and nutrient distribution between trees.

4.3.3. Mycelium network nodes

The mycelium network, inspired by the vast underground fungal networks in forests, consists of the majority of nodes in the EcoChain system, providing foundational support.

Let M be the set of all nodes in the mycelium network, where $M = \{m_1, m_2, \ldots, m_k\}$. The nodes in the mycelium network primarily relay transactions to the seed and sapling nodes and participate in lightweight validation tasks. A mycelium node m can evolve into a sapling node if:

$$E(m, t) > \Phi \tag{8}$$

where Φ is a predefined energy threshold for the status of the sapling node, but less than Θ.

Mycelium nodes are responsible for

1. Relaying transactions to higher-tier nodes, where mycelium nodes facilitate the transfer of transaction data to more central or significant nodes in the network, ensuring efficient data flow and contributing to the speed and reliability of transaction processing.

2. Participating in lightweight consensus tasks, where these nodes engage in consensus mechanisms, but in a capacity that demands less computational power. This involvement is crucial for maintaining the network's decentralization and security while ensuring scalability.
3. Monitoring and reporting of malicious activities, where mycelium nodes act as watchdogs within the network, identifying and reporting suspicious or malicious activities. This proactive surveillance helps to maintain the overall security and integrity of the blockchain network.

4.3.4. Guardian nodes

Guardian nodes, as the name suggests, act as protectors of the EcoChain network. Let G be the set of all guardian nodes in the network, where $G = \{g_1, g_2, \ldots, g_l\}$. Guardian nodes ensure the security of the EcoChain network. The nodes are selected as guardian nodes based on their longevity, trustworthiness, and performance on the network. Formally, a node n becomes a guardian node if

$$\begin{aligned} E(n,t) &> \Theta_G \\ B(n,t) &> \Theta_B \end{aligned} \tag{9}$$

where Θ_G is a high energy threshold and Θ_B is a high behavior score threshold.

Guardian nodes are responsible for

1. Monitoring, as they continuously observe the activities of nodes in the network to detect anomalies or malicious behaviors.
2. In the detection of anomalies, using advanced algorithms and heuristics, guardian nodes can detect anomalies in transaction patterns, validation behaviors, and network communications. If a node n exhibits behavior that deviates from the norm by a factor F, it's flagged if

$$F(n,t) > \Theta_F \tag{10}$$

   then flag n, where Θ_F is a predefined anomaly threshold.
3. Reporting, as they flag suspicious nodes for further investigation or immediate action. Guardian nodes collaborate with each other, sharing insights and data to improve the accuracy of their detection mechanisms. If more than η guardian nodes flag a particular node, immediate action is taken.
4. Intervention, as in extreme cases, guardians' nodes have the authority to temporarily isolate a suspicious node from the network, preventing potential harm.
5. Network healing, as guardian nodes can redistribute the responsibilities of the isolated node among trustworthy peers, which ensures that the network's functionality remains uninterrupted.

4.3.5. Dynamic thresholding

The thresholds for switching roles (e.g., from mycelium to sapling or from sapling to seed nodes) depend on two factors:

- **Network size (N):** As the network grows, the number of nodes in each role must be balanced to prevent overpopulated roles. A larger network may require higher energy thresholds to become a seed node, ensuring that only a small, capable subset of nodes is promoted to the highest tier.
- **Transaction throughput (T_t):** During periods of high transaction volumes, the threshold for node promotion could be lowered to increase the number of validating nodes and increase network capacity. During low transaction periods, thresholds could be increased to maintain a leaner and more efficient set of higher-tier nodes.

To implement dynamic thresholds, we define the threshold $\Theta(t)$ as a function of network size $N(t)$, transaction throughput $T_t(t)$, and total energy available in the network $E_{total}(t)$:

$$\Theta(t) = \Theta_0 + \beta_1 \cdot \frac{T_t(t)}{N(t)} + \beta_2 \cdot \frac{E_{total}(t)}{N(t)} \tag{11}$$

where Θ_0 is the base threshold value. β_1 and β_2 are scaling factors that determine the influence of transaction throughput and total energy on the threshold. $T_t(t)$ is the transaction throughput at time t. $E_{total}(t)$ is the total energy available in the network at time t. $N(t)$ is the total number of nodes at time t.

Dynamic thresholding allows the network to automatically adjust the criteria for node promotions, ensuring that the network performs optimally and remains resilient under varying conditions.

4.3.6. Architecture

Fig. 1 represents the structure and operational dynamics of EcoChain, reflecting its principles of bioinspired design and the hierarchical node architecture. The nodes are the primary entities, differentiated into seed nodes, sapling nodes, and mycelium nodes according to their roles and responsibilities within the ecosystem. Transactions are validated by seed nodes and assisted by sapling nodes, which capture the transaction validation and block proposal process. The blocks are proposed by the seed nodes, illustrating their pivotal role in adding new blocks to the blockchain. The relationships between nodes represent the symbiotic energy-sharing mechanism, inspired by forest ecosystems. Guardian nodes have a special role in monitoring the network for malicious activities, ensuring its health and integrity.

4.4. Mechanisms in EcoChain

EcoChain, inspired by the ecological dynamics of forests, incorporates several unique mechanisms to ensure network sustainability, security, and efficiency. One of the pivotal mechanisms is the "photosynthesis mechanism", which governs the energy dynamics and evolution of nodes within the network.

4.4.1. Photosynthesis mechanism

The photosynthesis mechanism in EcoChain is responsible for the energy dynamics of nodes and is inspired by the natural process of photosynthesis, where plants convert light into energy, which, in the context of EcoChain represents the trust, validation power, and overall status of a node within the network. Each node in the EcoChain network accumulates energy on the basis of its participation and contribution to the network's operations.

1. **Validation rate**, as nodes that validate more transactions accumulate energy faster.
2. **Network participation**, as active participation in consensus rounds, relaying transactions, and other activities in the network contribute to energy accumulation.
3. **Symbiotic relationships**, as nodes that form beneficial relationships with other nodes receive shared energy, improving their accumulation rate.

The energy rate function $\upsilon(n,t)$, which represents the rate of energy accumulation for node n at time t, can take both positive and negative values. A positive $\upsilon(n,t)$ indicates that the node is accumulating energy through network activities, while a negative $\upsilon(n,t)$ represents energy loss due to task execution, penalties, or natural energy decay. If the integral of $\upsilon(n,t)$ over time results in the node's energy falling below critical thresholds, the node may be demoted to a lower role.

Node evolution As nodes accumulate energy, they undergo evolutionary transitions, moving from one tier to another within the network hierarchy.

A mycelium node m evolves into a sapling node when

$$E(m,t) > \Phi \tag{12}$$

where Φ is the energy threshold for the sapling status.

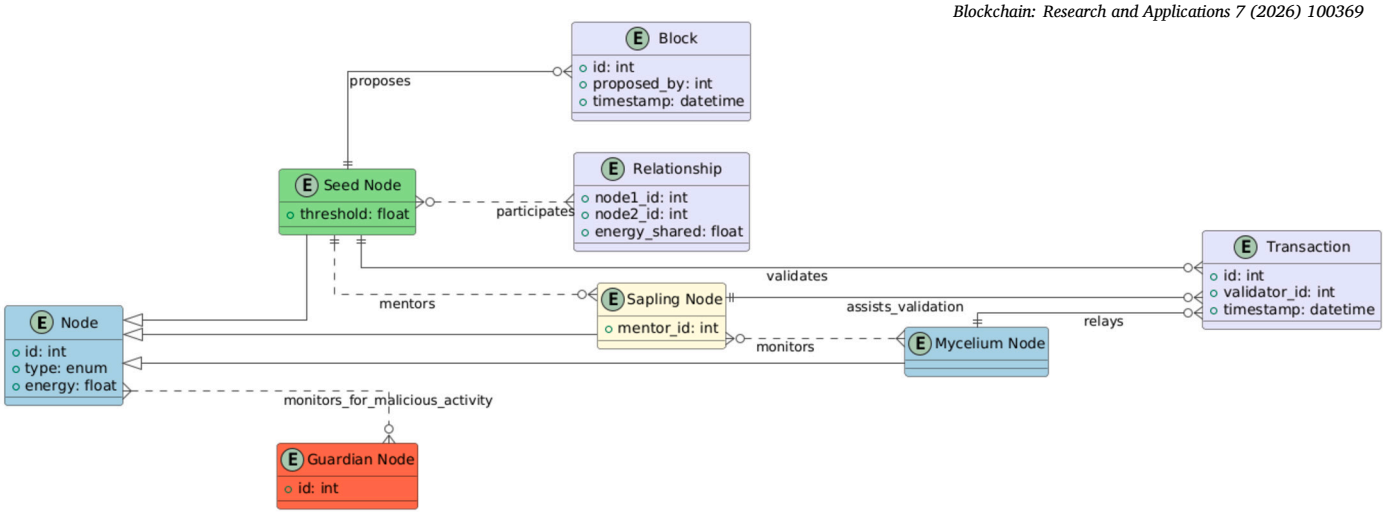


Fig. 1. EcoChain nodes and their relationships.

A sapling node p evolves into a seed node when

$$E(p,t) > \Theta \tag{13}$$

where Θ is the energy threshold for seed status and $\Theta > \Phi$.

Just as nodes can evolve, they can also be downgraded or removed if their energy drops below certain thresholds or if they exhibit malicious behavior. For example, a seed node s can be downgraded to a sapling node if

$$E(s,t) < \Theta' \tag{14}$$

where Θ' is a lower energy threshold to maintain seed status.

The photosynthesis mechanism ensures that nodes are rewarded for their positive contributions to the network and provides a dynamic, meritocratic structure that promotes active and beneficial participation.

4.4.2. Decomposition mechanism

Mirroring the natural process of decomposition in forests, where dead organic matter is broken down and recycled, the decomposition mechanism in EcoChain addresses nodes that are either malicious or no longer beneficial to the network's health and ensures the integrity and security of the network by actively monitoring and managing its constituent nodes. In EcoChain, this detection process is automated and collaborative.

Each node n has an associated behavior score $B(n,t)$ that quantifies its activities over time t. Anomalies or deviations from expected behavior can decrease this score

$$\Delta B(n,t) = -\alpha \times \text{AnomalyFactor}(n,t) \tag{15}$$

where α is a penalty coefficient and AnomalyFactor quantifies the detected anomaly's severity.

The network nodes can report suspicious activities of their peers. If a node n receives more than β reports within a time window δt, its behavior score is penalized

$$B(n,t)' = B(n,t) - \gamma \tag{16}$$

where γ is a predefined penalty for collaborative reports.

A node n is flagged as malicious if its behavior score drops below a certain threshold Θ_B, if

$$B(n,t) < \Theta_B \tag{17}$$

then n is malicious.

Once a node is detected as malicious, it undergoes a decay process, eventually leading to its removal from the network.

The malicious node n is first isolated from the network, preventing it from participating in any consensus rounds or transaction validations.

The node's energy $E(n,t)$ is drained at a rate ρ until it reaches zero

$$\frac{dE(n,t)}{dt} = -\rho \tag{18}$$

Once the node's energy is completely drained, it is removed from the network's active node set

$$N' = N \setminus \{n\} \tag{19}$$

where N' is the set of all active nodes in the network.

After removal, the network undergoes a healing process, redistributing the responsibilities and connections of the removed node among its neighbors. The EcoChain decomposition mechanism ensures that malicious nodes are quickly detected and removed, preserving the integrity and trustworthiness of the network.

4.4.3. Symbiotic relationships

Drawing inspiration from mutualistic interactions observed in forest ecosystems, the concept of symbiotic relationships in EcoChain introduces a collaborative paradigm between nodes, where relationships promote enhanced security, efficiency, and resilience within the network. The nodes in a symbiotic relationship can support each other during network adversities, improving overall resilience. Symbiotic nodes can vouch for each other, enhancing the trustworthiness of their operations within the network. Symbiotic relationships in EcoChain are formed on the basis of mutual benefits and trust between nodes.

Two nodes n_i and n_j form a symbiotic relationship R_{ij} if

$$\begin{aligned} B(n_i,t) &> \Theta_B \\ B(n_j,t) &> \Theta_B \end{aligned} \tag{20}$$

where $B(n,t)$ is the behavior score of a node and Θ_B is a threshold that ensures that only trustworthy nodes engage in symbiotic partnerships.

Once in a symbiotic relationship, nodes share a fraction α of their energy accumulation

$$\begin{aligned} E(n_i,t)' &= E(n_i,t) + \alpha \times E(n_j,t) \\ E(n_j,t)' &= E(n_j,t) + \alpha \times E(n_i,t) \end{aligned} \tag{21}$$

where $0 < \alpha < 1$ is the sharing factor.

4.4.4. Natural predation

In EcoChain, as in nature, there exists a mechanism of natural predation to maintain balance and health within the network. Guardian nodes play the role of these natural predators, ensuring that malicious or non-

performing nodes are kept in check, thereby preserving the integrity and security of the entire system.

The natural predation mechanism in EcoChain draws inspiration from ecological predation dynamics to manage the network's health and security. This mechanism is conceptualized as a way to identify and neutralize malicious nodes, similar to how predators control the population of certain species in a forest, thus maintaining ecological balance.

Each guardian node $g \in G$, where G is the set of all guardian nodes, continuously monitors the network for nodes n_i exhibiting behavior that deviates from the protocol or is considered harmful.

Upon detection of malicious activity by a node n_i, the guardian node takes action to "isolate" or remove the offending node from the network. This is represented as setting the energy level of the node to zero

$$E(n_i, t) = 0 \tag{22}$$

A node whose energy level is depleted (set to zero) is considered to be "predated" and is thus removed from the network, if

$$E(n_i, t) = 0 \tag{23}$$

then n_i is removed from N.

Depending on the specific rules of EcoChain, there might be mechanisms for a node to recover or for new nodes to be introduced into the network to replace those that have been removed. Such an approach ensures that the network remains healthy by preventing any single node or group of nodes from performing actions that could harm the integrity or performance of the network. It mimics the self-regulating processes of natural ecosystems, providing a dynamic and resilient approach to network security.

4.4.5. Adaptation mechanisms in EcoChain

EcoChain, inspired by the adaptive capabilities of forest ecosystems, incorporates mechanisms that allow the network to adjust and evolve in response to internal and external stimuli. This adaptability ensures that the network remains resilient, efficient, and relevant in a constantly changing environment. Just as forests undergo successional stages, the EcoChain network experiences different phases in its lifecycle.

The nascent stage of the network is characterized by

$$N_{\Phi_I} < \Theta_N \tag{24}$$

where N_{Φ_I} is the number of nodes in the initialization phase and Θ_N is a threshold. During this phase, the network focuses on attracting nodes, establishing basic consensus, and ensuring initial security.

As the network gains traction, it enters a phase of rapid expansion

$$\frac{dN}{dt} > \Theta_G \tag{25}$$

where $\frac{dN}{dt}$ is the rate of node addition and Θ_G is a growth rate threshold. Here, the emphasis is on scaling, optimizing transaction speeds and maintaining symbiotic relationships.

Once the network reaches stable size and operation, it focuses on optimization, security, and sustainability. This phase is identified when the growth rate stabilizes

$$\left|\frac{dN}{dt}\right| < \Theta_M \tag{26}$$

where Θ_M is a minimal growth rate threshold.

If the network faces significant challenges or disruptions, it might enter a phase of decay. However, built-in renewal mechanisms can rejuvenate the network, leading to a new growth or climax phase.

EcoChain's adaptability is not just internal, but also extends to external conditions, ensuring that the network remains robust in varied environments.

- As new technologies emerge, EcoChain can integrate them through modular updates. Let $T(t)$ represent the technological state of the network at time t. When a significant technological shift occurs, $T(t)$ undergoes a transformation to $T'(t)$.
- The network continuously monitors external threats and adjusts its security protocols accordingly. If a new threat Θ_T is detected, the security state of the network $S(t)$ evolves to $S'(t)$ to counteract it.
- EcoChain can adjust transaction fees, validation rewards, and other economic parameters in response to external economic conditions. If the external economic condition is represented by $E(t)$, the economic parameters of the network $P(t)$ can be adjusted to $P'(t)$ to maintain equilibrium.
- In line with its ecological inspiration, EcoChain can adapt its consensus mechanisms and node operations to be more energy efficient and environmentally friendly, especially in response to global environmental changes.

4.5. Examples of using EcoChain

4.5.1. Load balancing

Consider two nodes, n_a and n_b, where n_a experiences a sudden surge in transaction validation requests. Through their symbiotic relationship, n_b can assist in handling excess load, ensuring timely transaction validations, and maintaining network efficiency.

To visualize the symbiotic load balance process in EcoChain, focusing on the interaction between nodes n_a and n_b during a load surge, we present a UML sequence diagram. Fig. 2 shows how this approach n_b assists n_a in handling excess transaction validation requests, ensuring network efficiency and timely transaction validations. The load-balancing system (LBS) periodically checks the load on nodes within the EcoChain network. Node n_a reports a high load status due to a sudden surge in transaction validation requests. Currently, the LBS identifies node n_b as having a low load. This makes n_b a suitable candidate for assisting n_a with its excess load. The EcoChain state is updated to form a symbiotic pair between n_a and n_b, enabling them to share transaction validation responsibilities. Node n_a transfers its excess load to n_b, which confirms receipt and starts processing additional transactions.

Balancing complete: Once the load is successfully transferred and balanced between the nodes, the LBS updates the EcoChain state to reflect the new load statuses. The system then marks the load balancing operation as complete.

4.5.2. Attack mitigation

In an instance where node n_x is targeted by a distributed denial of service (DDoS) attack, its symbiotic partner n_y can temporarily take over its validation responsibilities, ensuring uninterrupted service and mitigating the effects of the attack.

Fig. 3 illustrates how the EcoChain system takes advantage of its symbiotic relationships with its network to ensure resilience against attacks and maintain uninterrupted service. The EcoChain network detects a DDoS attack targeting a specific node (n_x). The attack node notifies the network of the detected attack. Upon detection of the attack, the network activates the symbiotic partner node (n_y) of the attacked node (n_x). The symbiotic partner temporarily takes over the validation responsibilities of n_x, ensuring that the network service remains uninterrupted. A guardian node is assigned to the node under attack for additional protection. This guardian node establishes a monitoring link with n_x and begins intensive monitoring of its activities to further mitigate the attack and prevent future events. After the attack is mitigated, the symbiotic partner node (n_y) restores the validation responsibilities back to n_x. The node under attack then notifies the network that the attack has been mitigated and normal operations have resumed.

4.5.3. Resource sharing

Nodes n_p and n_q have different peak activity times due to their geographical locations. Through their symbiotic relationship, they can share computational resources, ensuring that idle resources during off-peak times are utilized efficiently by the active partner.

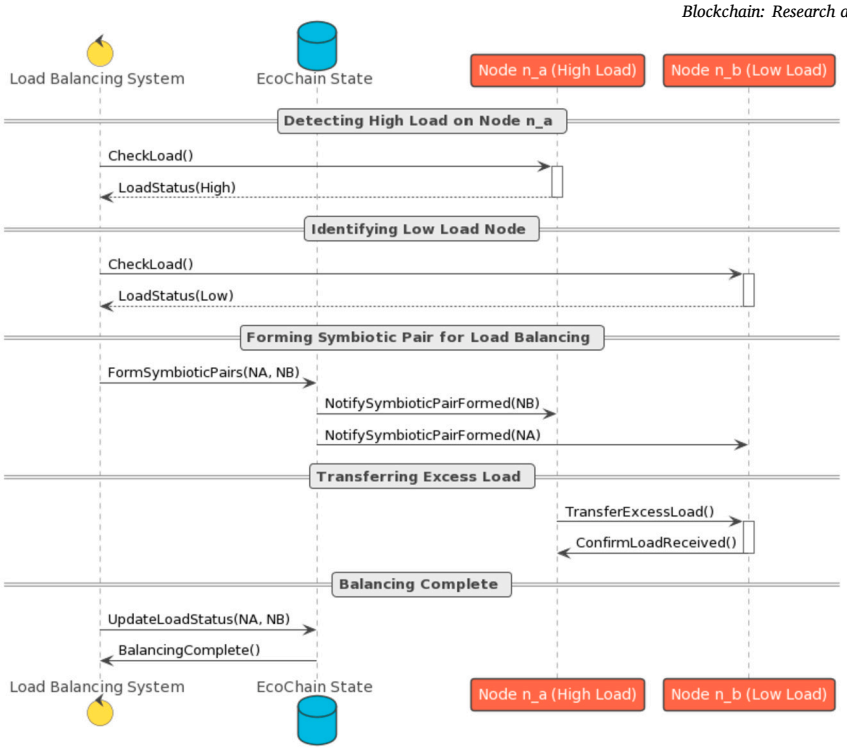


Fig. 2. Load balancing in EcoChain.

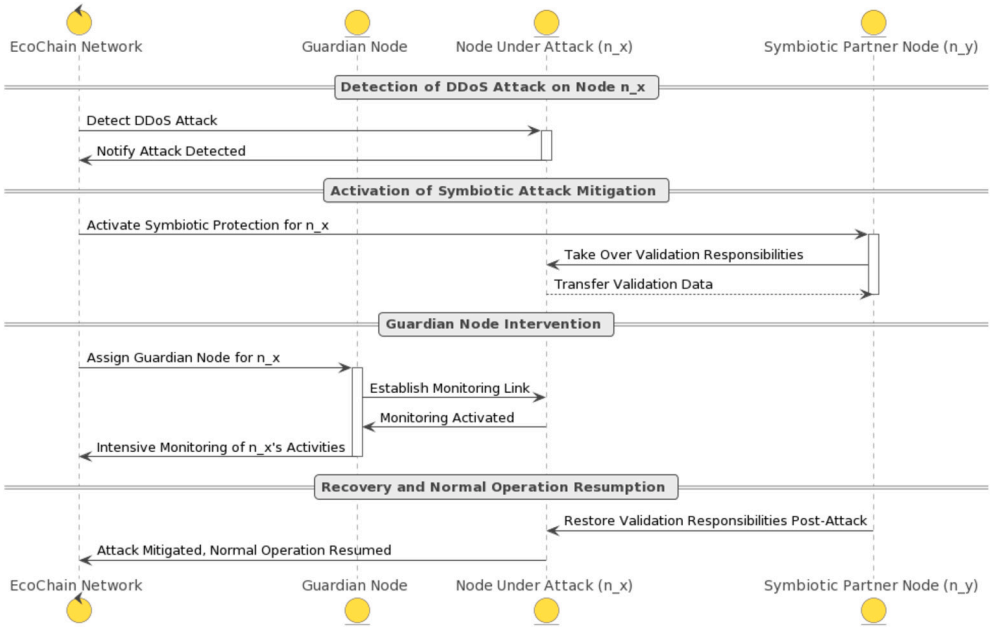


Fig. 3. Attack mitigation in EcoChain.

Fig. 4 describes the process within the EcoChain network where computational resources are shared between nodes with excess resources (Resource Rich Nodes) and those in need of more resources (Resource Scarce Nodes). The EcoChain network initiates the process by instructing the resource management system (RMS) to form symbiotic resource links between these nodes. For each resource-scarce node, the RMS identifies an optimal resource rich node to partner with. Once identified, the resource-rich node establishes a resource-sharing link with the scarce node, enabling the transfer of resources. These processes ensure efficient utilization of the network's overall resources by redistributing excess capacity where it is needed most, mirroring symbiotic relationships found in natural ecosystems.

5. Implementation of EcoChain

Implementing EcoChain requires a multifaceted approach, including the design of its unique node structures, the integration of its ecological mechanisms, and the establishment of protocols [116] to ensure network security and efficiency. The EcoChain network architecture is designed to embody the principles of efficiency, scalability, and environmental sustainability within the blockchain domain. This section

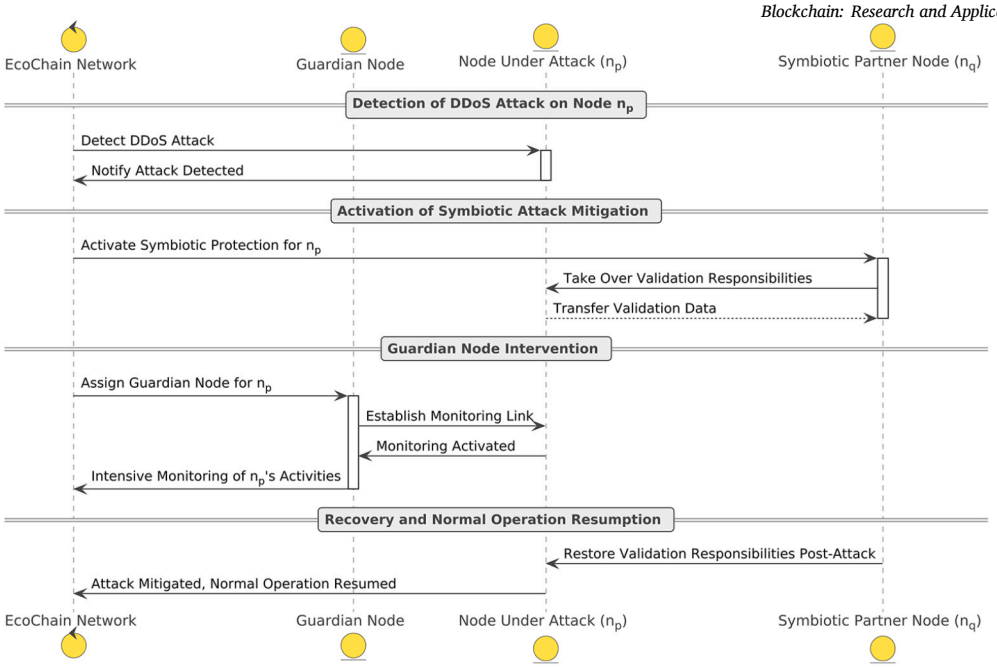


Fig. 4. Resource sharing between resource rich and resource scarce nodes in EcoChain.

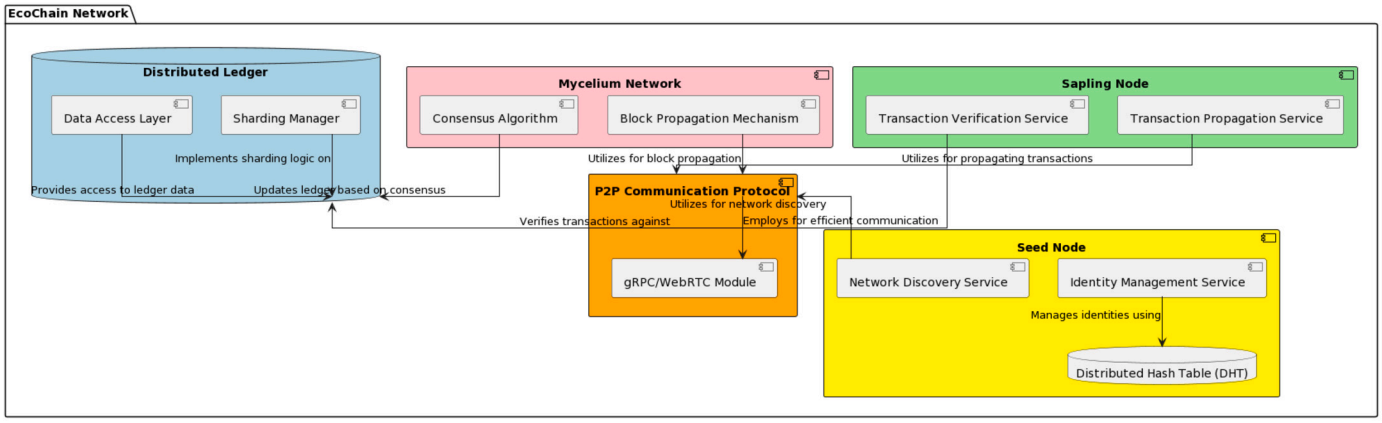


Fig. 5. EcoChain network architecture.

describes the engineering mechanisms and technologies that underpin the EcoChain network, namely node deployment, communication protocols, and data storage strategies.

5.1. EcoChain architecture

The EcoChain network architecture introduces a novel categorization of nodes, distinguishing them into distinct ecosystem components, namely seed nodes, sapling nodes, and the mycelium network. This taxonomy is instrumental in delineating the roles and responsibilities within the network, facilitating a structured and hierarchical approach to network management and operation. The seed nodes act as the primary entry points to EcoChain, offering robust connectivity and facilitating network discovery. Sapling nodes, similar to lightweight clients, participate in transaction verification and propagation without carrying the full load of ledger storage. The mycelium network, inspired by the intricate fungal networks found in nature, represents a dense, interconnected layer of nodes that underpins the network's resilience and distributed processing capabilities. A distributed hash table (DHT) is used to manage the identities of the nodes and their respective roles, using a decentralized mechanism for efficient data lookup and routing within the network.

The EcoChain leverages a peer-to-peer (P2P) communication protocol to ensure efficient and secure data exchange between nodes. This protocol is the backbone of network operations, facilitating transaction broadcasting, block propagation, and consensus messaging. Adaptations of established protocols such as gRPC or WebRTC are considered for this purpose, chosen for their reliability, low-latency characteristics, and support for bidirectional streaming. gRPC, with its foundation on HTTP/2, offers multiplexed streams that are ideal for the high-throughput requirements of blockchain networks. WebRTC, on the other hand, provides real-time communication capabilities that are beneficial for direct peer interactions, especially in scenarios requiring immediate consensus or data sharing.

At the core of the EcoChain network lies a distributed ledger, partitioned across nodes, designed to store transaction data with high integrity and availability. This ledger employs advanced data storage techniques, among which sharding is notable for its ability to enhance data retrieval speeds and manage storage efficiently. Sharding divides the blockchain into smaller, manageable segments (shards), each maintained by a subset of nodes. This division not only reduces the storage

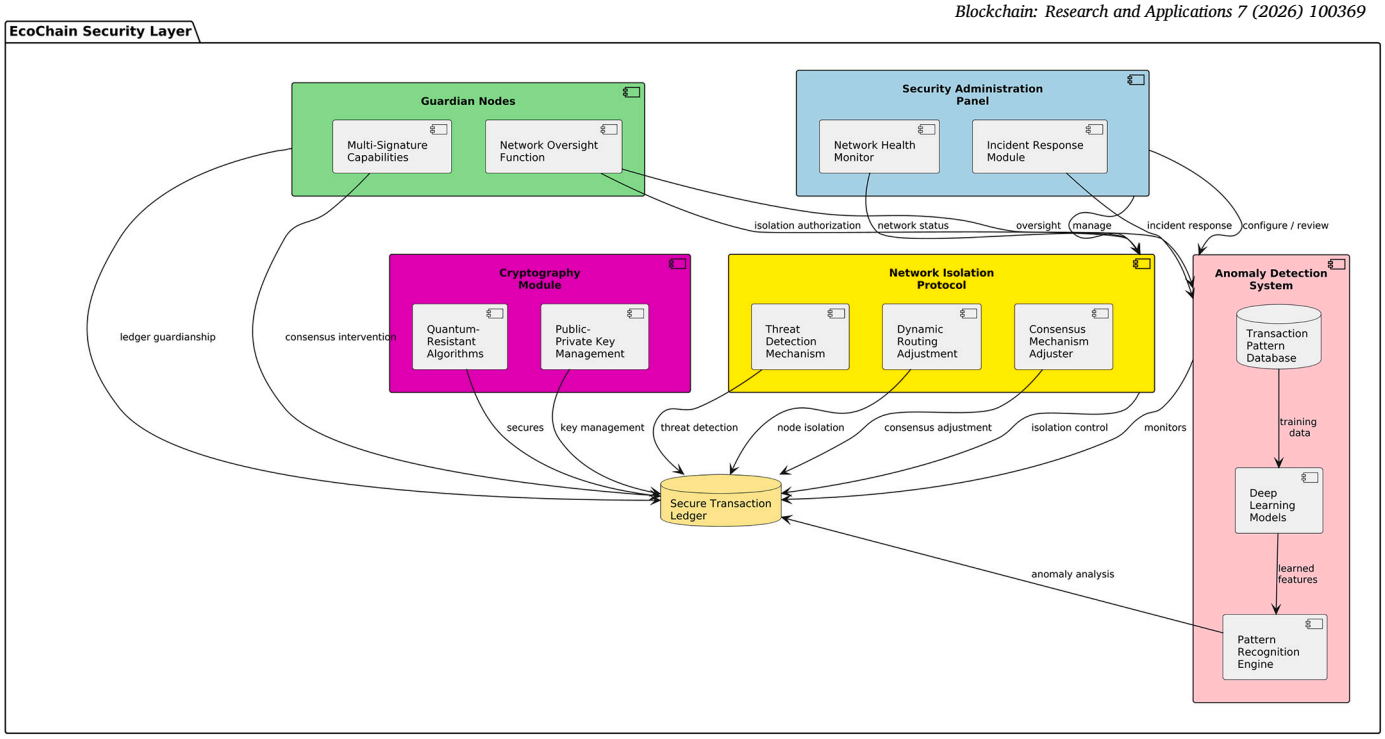


Fig. 6. Security infrastructure in EcoChain.

burden on individual nodes but also parallelizes transaction processing, significantly improving the network's scalability and performance. To ensure data consistency and prevent fragmentation issues, consensus algorithms are tailored to manage and synchronize shards across the network, thereby maintaining the ledger's integrity and cohesiveness.

Fig. 5 provides a detailed view of the EcoChain network architecture, showcasing the specific functionalities and interactions that underpin this innovative blockchain system. This diagram illustrates the intricate components within the EcoChain network. Seed nodes hosts the DHT for identity management and a network discovery service for connecting with other nodes. The sapling nodes contain services for transaction verification and propagation, facilitating lightweight participation in the network. Mycelium network comprises the consensus algorithm for agreement on the ledger state and a block propagation mechanism to ensure network synchronicity. The distributed ledger encapsulates the sharding manager for efficient data management and a data access layer for interfacing with blockchain data. The P2P communication protocol etilizes a gRPC/WebRTC module for secure and efficient communication between nodes.

5.2. Consensus mechanism

At the heart of EcoChain's consensus model lies the photosynthesis mechanism, a novel adaptation inspired by the natural process of photosynthesis. In this context, nodes within the EcoChain network accumulate "energy" reflecting their contributions to the network's health and operations. This mechanism is ingeniously implemented through a variant of the PoS protocol, where the "stake" a node holds is directly proportional to its accumulated energy level. Such an approach incentivizes nodes to actively participate in network activities, including transaction validation and block creation, mirroring the energy accumulation observed in photosynthesis. The energy level of a node is determined by various factors, such as the accuracy of transaction validation, the frequency of block proposals, and general network support activities, thus fostering a sustainable and meritocratic network ecosystem.

Complementing the photosynthesis mechanism is the decomposition mechanism, which embodies the natural process of breaking down organic matter. Within the EcoChain network, this mechanism is implemented through the deployment of continuous monitoring scripts on each node. These scripts are designed to meticulously scan and analyze node behaviors, identifying and flagging nodes that exhibit anomalous or malicious patterns. Nodes that are determined to have behavior scores below a predefined threshold are subsequently isolated from participating in consensus-related activities. This mechanism serves as a natural cleansing process, removing or rehabilitating nodes that could potentially harm the network's integrity, thereby maintaining a healthy and robust ecosystem.

To further bolster network security and integrity, EcoChain introduces guardian nodes. These nodes possess elevated privileges and are equipped with multisignature capabilities, enabling them to perform critical interventions when network threats are detected. Guardian nodes act as overseers of the network, drawing inspiration from keystone species in a forest ecosystem that play a pivotal role in maintaining ecological balance. Their multisignature capabilities ensure that any intervention requires consensus among multiple guardian nodes, thereby preventing unilateral actions and ensuring decisions are made in the network's best interest. Guardian nodes are selected based on stringent criteria, including historical contributions, energy levels, and trust scores, ensuring that only the most reputable and reliable nodes assume this vital role.

5.3. EcoChain security protocols

EcoChain's security model is based on public-private key cryptography, ensuring secure and anonymous transactions. It goes beyond conventional methods by pioneering the adoption of quantum cryptography algorithms that are resilient against quantum computer attacks. Quantum-resistant algorithms such as lattice-based cryptography, hash-based cryptography, and multivariate polynomial cryptography safeguard transactions against future threats, ensuring long-term network security.

In case of detected threats, EcoChain swiftly implements protocols to contain incidents. This includes temporarily isolating affected network segments to stop the spread of malicious activities. Network isolation

is achieved through adjustments of the dynamic routing protocol and consensus mechanism, effectively quarantining compromised nodes or segments without disrupting overall network continuity. This containment strategy minimizes the impact of the attack, allowing controlled assessment and neutralization of the threat.

Fig. 6 provides a comprehensive view of the security architecture within the EcoChain network. This detailed diagram shows the intricate relationship between various components designed to ensure the integrity, confidentiality, and availability of the network. The cryptography module within EcoChain's security layer employs quantum-resistant algorithms to safeguard transactions and communications, ensuring the protection of digital assets and facilitating secure, anonymous interactions through its public-private key management system. Anomaly detection in EcoChain utilizes deep learning models trained with data from the transaction pattern database, continuously monitoring transaction patterns in real time to quickly identify irregularities signaling potential security threats or vulnerabilities. The network isolation protocol responds dynamically to detected threats by isolating affected network segments, utilizing its threat detection mechanism to engage components such as the dynamic routing adjustment and the consensus mechanism Adjuster, effectively mitigating risks and maintaining overall network health. Guardian nodes serve as a crucial security layer in EcoChain, equipped with multi-signature capabilities to oversee critical operations and directly engage in strategic responses to threats, ensuring prudent actions aligned with the network's best interests. The security administration panel offers network administrators tools for incident response and ongoing network health monitoring. It supervises the configuration of the anomaly detection system and manages the network isolation protocol, enabling the prompt resolution of identified security issues.

5.4. EcoChain adaptation mechanisms

EcoChain employs advanced adaptation mechanisms to ensure its resilience, scalability, and responsiveness to changing conditions, utilizing state-of-the-art technologies and methodologies. One key mechanism involves dynamic resource scaling through the Kubernetes container orchestration tool, which enables automated deployment, scaling, and management of containerized applications, allowing seamless adjustment of network nodes and services in response to transaction volume fluctuations. Containerized environments improve fault tolerance and load balancing, bolstering the network's robustness and scalability without manual intervention.

The integration of application programming interfaces (APIs) enables EcoChain to monitor external conditions such as technological, economic, and environmental changes, proactively adapting protocols and operations accordingly. For example, APIs from financial markets inform economic trends, prompting adjustments in transaction fees or incentives to maintain network stability. The APIs for environmental data align energy consumption strategies with renewable energy availability, supporting EcoChain's sustainability commitment.

Central to EcoChain's adaptive mechanisms are feedback loops powered by continuous-monitoring tools. Real-time data on network metrics such as transaction processing times, node performance, and security threats inform areas that need optimization, such as resource allocation, security protocols, or consensus mechanisms. Feedback loops enable dynamic self-optimization, enhancing efficiency, security, and user experience while swiftly addressing internal performance and external threat concerns, thereby upholding operational integrity and user trust.

Fig. 7 provides a detailed view of how EcoChain uses Kubernetes and other technologies to implement its adaptation mechanisms, ensuring that the network remains scalable, responsive, and secure. Kubernetes cluster serves as the backbone of EcoChain's infrastructure, orchestrating the deployment, scaling, and operation of network components. It includes

- API server is the central management entity for Kubernetes, handling cluster operations.
- Container runtime is responsible for running containerized applications.
- Pods are the smallest deployable units that can be created, scheduled, and managed.
- Service discovery allows pods to locate each other and communicate within the cluster.
- The load balancer distributes the incoming network traffic across multiple pods to ensure high availability and reliability.
- Dynamic scaling module utilizes the horizontal pod autoscaler to automatically scale the number of Pods in response to observed CPU utilization or custom metrics provided by the custom metrics server, ensuring EcoChain can dynamically adjust its resources.
- The external condition monitoring module integrates with external APIs to monitor conditions such as market trends, technological advancements, or environmental data. The condition analysis tool processes this data to inform dynamic adjustments within the EcoChain network.
- The feedback loop system comprises monitoring tools that collect real-time data on network performance, a performance analytics engine that analyzes these data to identify optimization opportunities, and a security threat detector that identifies potential security threats. This system ensures continuous adaptation and optimization of the network based on real-time performance and threat data.

5.5. Integration and APIs

A cornerstone of EcoChain's integration capabilities is its support for smart contracts, which are self-executing contracts with terms directly encoded into code. EcoChain utilizes platforms like Solidity, a statically typed programming language designed for smart contract development on the Ethereum virtual machine (EVM). Leveraging Solidity offers benefits such as maturity, a robust tooling ecosystem, and access to an extensive developer community. Smart contracts on EcoChain automate complex processes, enable decentralized applications (DApps), and execute agreements without relying on intermediaries. Compatibility with the EVM ensures that developers can create highly programmable and interoperable DApps effortlessly, leveraging existing development tools and libraries.

For seamless integration with third-party applications and services, EcoChain provides comprehensive API support via RESTful APIs and GraphQL endpoints. RESTful APIs offer a widely adopted method of interacting with web services, allowing applications to perform CRUD operations on blockchain data in a stateless manner. This approach is suitable for services that require straightforward action-based interactions with the EcoChain network. However, GraphQL endpoints offer a more flexible and efficient approach to working with EcoChain data. Clients can precisely query the data they need, reducing bandwidth usage and enhancing performance for complex applications, particularly beneficial for DApps requiring real-time data extraction and aggregation from the blockchain.

Both RESTful APIs and GraphQL endpoints are designed to support a wide range of interactions, from simple wallet operations to complex smart contract executions, allowing one to enhance the accessibility and utility of the EcoChain platform for developers and businesses, fostering innovation and collaboration within the ecosystem.

Fig. 8 outlines the infrastructure that supports EcoChain's integration capabilities and API services. At the core of the EcoChain network lies the EVM compatible node, providing an environment for executing solidity-based smart contracts. Within this node, the smart contract runtime component facilitates the deployment and execution of contracts, enabling programmable interactions on the blockchain. Serving as the primary access point for external integrations, the API gateway hosts both the RESTful API service and the GraphQL Service. These services enable seamless communication between client applications,

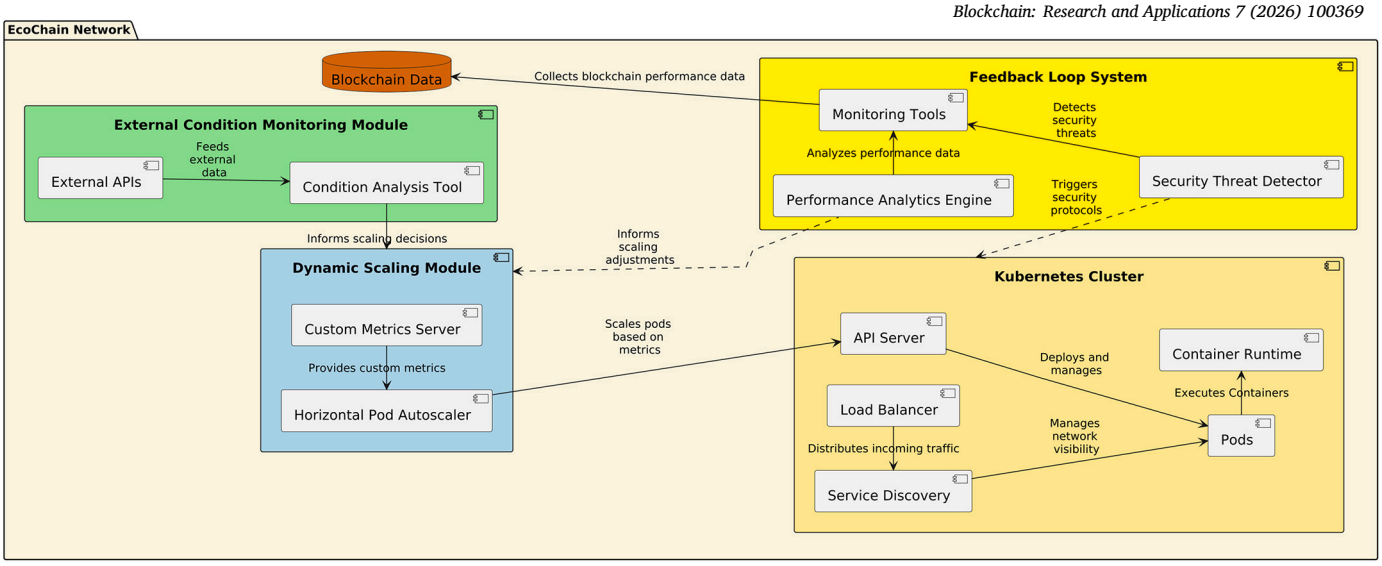


Fig. 7. Containerization using Kubernetes.

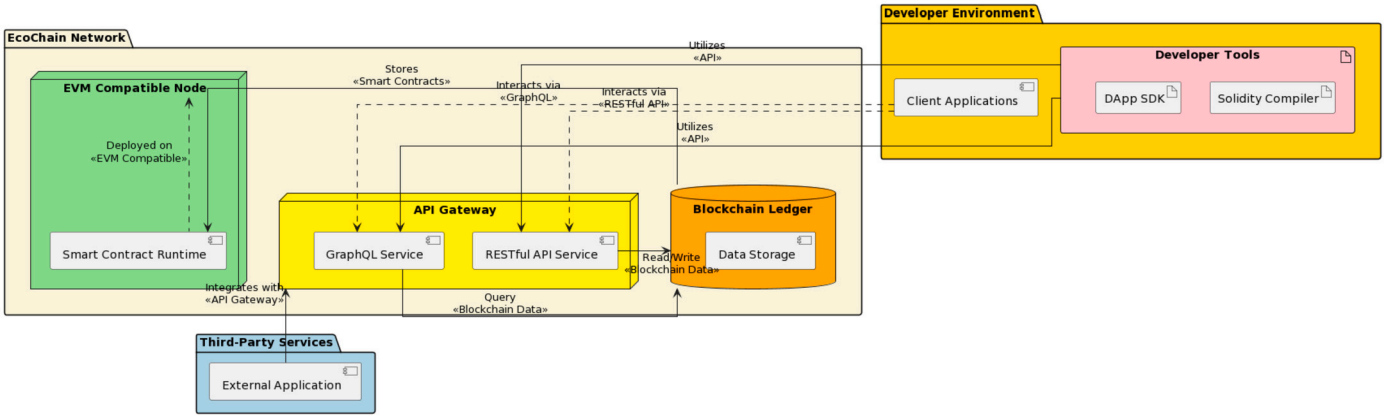


Fig. 8. Deployment of EcoChain and integration with third-party APIs.

third-party services, and the blockchain ledger, facilitating efficient data exchange and manipulation. The blockchain ledger acts as an immutable record of all transactions and smart contracts within the EcoChain network. It includes a Data Storage component that securely stores ledger data, accessible through the API Gateway. The developer environment is equipped with essential Developer Tools, including a Solidity compiler for smart contract development and a DApp SDK for building DApps. These tools enable developers to create, compile, and deploy smart contracts and applications on the EcoChain network. Client applications and third-party services are the end users of EcoChain APIs, integrating with the network to perform various operations such as transaction submissions, smart contract interactions, and data queries. They take advantage of the API gateway for efficient interaction with the blockchain ledger.

6. Experimental evaluation and results

6.1. Experimental setup

The experimental apparatus was centralized on a single server configuration to maintain consistency across all tests. Specifically, the server was equipped with an Intel Core i7-10710U CPU and 16GB of RAM, operating under the Ubuntu 20.04 64-bit operating system. This hardware setup was chosen for its balance between performance and availability, ensuring that the results are accessible to a broad spectrum of researchers and practitioners. For the blockchain infrastructure, Ganache-CLI v6.12.2 was used, serving as an Ethereum emulation network. This choice was dictated by the need for a controlled yet realistic blockchain environment in which variables could be manipulated with precision. The network was initialized with ten nodes, a configuration that provides a balance between simplicity and the complexity necessary to simulate real-world blockchain network interactions.

The experimental framework was further enhanced by the use of Solidity 0.8.11 for smart contract development, a choice that aligns with industry standards for Ethereum-based applications. This ensures that the findings are relevant and applicable to current blockchain development practices. The index and system logic were encapsulated within a Java-based architecture, leveraging the robustness and portability of the Java platform. The interaction between the experimental system and the blockchain was facilitated through Web3j 4.8.7, a widely recognized middleware in the Ethereum ecosystem. This component was critical in bridging the gap between the high-level system functionalities and the low-level blockchain operations, ensuring seamless communication and data exchange across the different layers of the experimental setup.

6.2. Set values for EcoChain constants

The set values for the constants in EcoChain (see Table 2) were determined based on the need to balance the resilience of the network, energy efficiency, and security. For example, the energy thresholds Θ and Φ for the evolution of the nodes ensure that only the nodes with significant

Table 2
Set values of constants in EcoChain.

Constant	Value	Description
Θ	0.8	Energy threshold for node evolution from sapling to seed node.
Φ	0.5	Energy threshold for node evolution from mycelium to sapling node.
α	0.3	Sharing factor in symbiotic relationships between nodes.
θ	0.2	Minimum energy required for a node to stay active before being decomposed.
ρ	0.1	Rate of energy decay for decomposing nodes.
γ	0.2	Penalty for collaborative reports on a node's suspicious activity.
Θ_G	0.9	Energy threshold for a node to be promoted to a guardian node.
Θ_B	0.3	Behavior score threshold for identifying a malicious node.
ω	1.0	Frequency of validation difficulty changes (for seasonal adjustments).

contributions to the network can advance, maintaining a stable and reliable node hierarchy. The sharing factor α is kept moderate at 0.3 to facilitate resource distribution in symbiotic relationships without overburdening any single node. The energy decay rate ρ and the penalty coefficient γ are relatively low to allow for gradual punishment and removal of malicious or inactive nodes, ensuring fairness while maintaining security. The thresholds for behavior scores Θ_B and energy for guardianship Θ_G are set to ensure that only trusted and high-performing nodes gain influential roles, while the frequency of difficulty adjustments ω accounts for the need to adapt the network dynamically to fluctuating conditions without introducing excessive instability. These values were empirically selected to reach a stable and adaptable configuration for our experimental blockchain system; however, further tuning may be necessary based on real-world deployments or additional simulations.

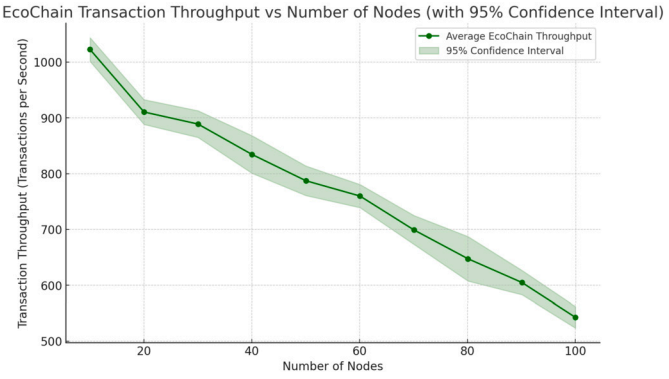


Fig. 9. Network throughput.

6.3. Network throughput

Fig. 9 illustrates the relationship between the number of nodes in the EcoChain network and its average transaction throughput in 10 simulations, with a focus on demonstrating the statistical reliability of these measurements by depicting the confidence intervals of 95%. The average transaction throughput decreases as the number of nodes increases. This trend suggests that adding more nodes to the network may introduce additional complexity and communication overhead, leading to a decrease in the efficiency with which transactions are processed. The shaded area that represents the confidence interval 95% around the average performance indicates the variability in the simulation results. As the number of nodes increases, the confidence interval narrows slightly, implying increased variability in throughput performance between simulations. This variability could be attributed to factors such as network latency, differences in node performance, and the stochastic nature of transaction arrivals and processing times. The narrower confidence intervals at lower node counts show higher reliability and less variability in throughput performance. In contrast, slightly wider intervals at higher node counts indicate a greater degree of uncertainty, reflecting the challenges of maintaining consistent performance as the network scales.

The observed decrease in throughput with increasing node counts highlights scalability as a critical concern for EcoChain. Although adding nodes improves the decentralization and fault tolerance of the network, it also poses challenges for maintaining high transaction processing efficiency. The results underscore the importance of optimizing network protocols and consensus mechanisms to mitigate the impact of added nodes on throughput. Strategies such as sharding, efficient consensus algorithms, and network optimization can be critical to addressing these scalability challenges.

6.4. Transaction latency

Fig. 10 shows the relationship between the number of nodes in a blockchain network and the average transaction latency, based on data from 10 simulations. The solid red line indicates the average transaction latency, while the shaded area represents the 95% confidence intervals around these averages, highlighting the variability and statistical reliability of the latency measurements. The average transaction latency increases as the number of nodes in the network increases. This trend suggests that a larger network size contributes to longer transaction processing times, likely due to the increased complexity of achieving consensus and the higher communication overhead across a more extensive network. The shaded area around the average latency line indicates the presence of variability in transaction latency in simulations. This variability could be attributed to factors such as network conditions, variations in node performance, and the stochastic nature of transaction processing.

The observed increase in transaction latency with network size underscores the importance of careful network design and optimization efforts. Techniques to reduce latency, such as optimizing consensus mechanisms or employing more efficient communication protocols, are crucial to maintain acceptable performance levels in larger blockchain networks. The findings highlight scalability as a pivotal challenge for blockchain networks, with transaction latency serving as a key metric to evaluate network performance. Addressing the challenge of scalability is essential for blockchain networks that want to support high volumes of transactions without significant delays.

6.5. Smart contract execution time

Fig. 11 illustrates the relationship between block size and the average execution time of smart contracts in the EcoChain network, incorporating data from 10 simulations to provide a statistically grounded analysis. The solid purple line represents the average execution time of smart contracts as the size of the block increases, while the shaded area denotes the 95% confidence intervals, highlighting the variability and statistical reliability of these measurements. The average execution time of the smart contract exhibits a logarithmic increase with block size, indicating that larger blocks lead to significantly longer execution times. This trend underscores the computational complexity associated with processing larger blocks, which can contain more transactions and, consequently, more smart contract invocations. The presence of the shaded

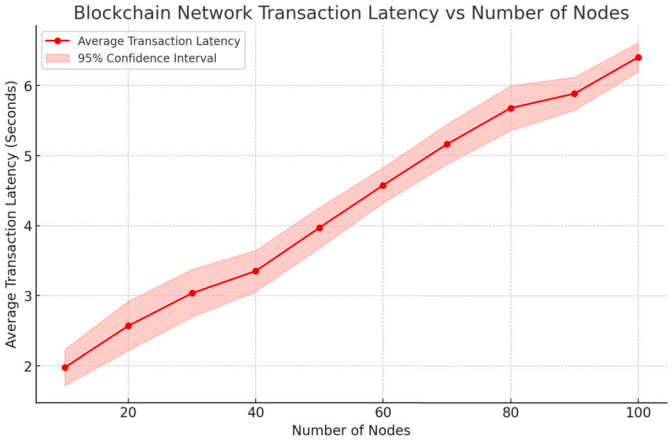


Fig. 10. Network latency.

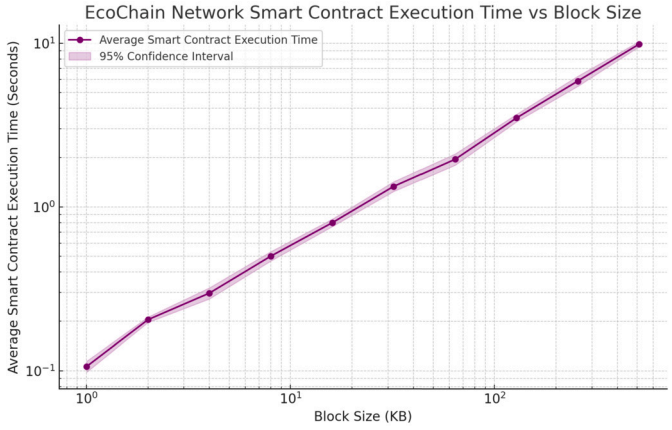


Fig. 11. Smart contract execution time.

area, which represents 95% confidence intervals, reveals the variability in execution time between different simulations. This variability is expected due to factors such as differences in smart contract complexity, variations in network load, and the stochastic nature of blockchain operation.

The measurements highlight the importance of optimizing smart contract code and blockchain infrastructure to effectively manage the computational demands of larger blocks. Techniques such as gas optimization, efficient data storage, and parallel processing could be critical in reducing execution time.

The findings illustrate the trade-offs between block size and network performance, especially with respect to smart contract execution. Blockchain architects and developers must carefully consider these trade-offs when designing and configuring the EcoChain network to balance scalability, efficiency, and transaction throughput.

6.6. Block confirmation time

Fig. 12 shows the relationship between block size and average block confirmation time in the EcoChain network, based on data from 10 simulations. The average confirmation time, represented by the solid orange line, shows how it varies as the block size increases. The shaded area around this line, which shows the confidence intervals of 95%, illustrates the variability in the confirmation time between simulations and provides a measure of statistical reliability. Unlike the smart contract execution time, the block confirmation time exhibits a more linear increase with increasing block size. This suggests that as the blocks become larger and contain more transactions, the time required for their confirmation by the network increases at a steady rate. This pattern reflects the additional computational and network resources needed to validate and propagate larger blocks across the network. The variability in confirmation times, as indicated by 95% confidence intervals, highlights fluctuations that can occur due to network conditions, node performance, and other operational factors. Despite these variations, the relatively narrow confidence intervals suggest that average confirmation times are statistically robust and reliable indicators of network performance under varying block sizes. They indicate the expected range within which the true average times are likely to fall, offering a solid basis for evaluating the network's scalability and efficiency in processing transactions encapsulated within blocks of varying sizes. The observed an increase in block confirmation time with block size underscores the scalability challenges faced by blockchain networks and highlights the need for efficient block validation and propagation mechanisms to maintain network performance as the demand for transaction processing capacity grows.

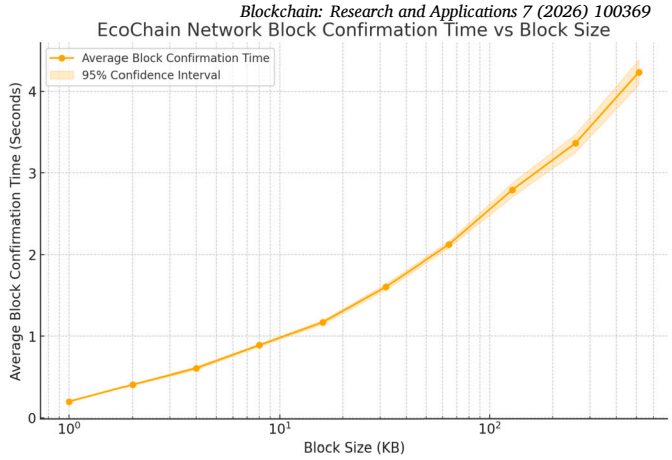


Fig. 12. Block confirmation time.

7. Discussion and conclusions

The study introduces a novel blockchain architecture inspired by forest ecosystems with the aim of efficiency, scalability, and environmental sustainability. Unique node structures, ecological mechanisms, and security protocols are designed to achieve this goal. The EcoChain network architecture categorizes nodes into seed nodes, sampling nodes, and the mycelium network, each having a distinguishing function. Seed nodes act as entry points, providing connectivity and network discovery, while the sapling nodes handle transaction verification and propagation without full ledger storage. The mycelium network, inspired by natural fungal networks, ensures network resilience and distributed processing capabilities.

EcoChain utilizes a DHT for efficient data lookup and routing, managing node identities and roles in a decentralized manner. A P2P communication protocol based on gRPC or WebRTC adaptations enables secure data exchange, transaction broadcasting, block propagation, and consensus messaging, supporting high-throughput and real-time interactions crucial for network coherence.

The core of EcoChain features a distributed ledger using sharding to improve data retrieval speeds and storage efficiency. Sharding divides the blockchain into smaller segments maintained by node subsets, reducing individual node burdens and parallelizing transaction processing, significantly enhancing scalability and performance. Tailored consensus algorithms synchronize shards across the network, ensuring data consistency and preventing fragmentation issues.

EcoChain's implementation integrates ecological inspiration with blockchain technology to create a robust, efficient, and environmentally sustainable network. Its unique node categorization, advanced communication protocols, and data storage strategies offer a scalable and secure blockchain solution.

Critical areas for future exploration include optimizing network architecture, consensus algorithms, and block propagation protocols to enhance scalability, efficiency, and overall performance. Scalability is identified as a key concern, emphasizing the importance of strategic network design and optimization to mitigate latency in larger blockchain networks.

CRediT authorship contribution statement

Robertas Damaševičius: Conceptualization, Investigation, Validation, Writing – original draft, Formal analysis, Methodology, Visualization. **Gintautas Mozgeris:** Validation, Formal analysis. **Tomas Krilavičius:** Project administration, Validation, Funding acquisition, Resources. **Rytis Maskeliūnas:** Formal analysis, Writing – review & editing, Conceptualization, Validation.

Funding

This research paper has received funding from Horizon Europe Framework Programme (HORIZON), call Teaming for Excellence (HORIZON-WIDERA-2022-ACCESS-01-two-stage) - Creation of the centre of excellence in smart forestry “Forest 4.0” No. 101059985.

Declaration of competing interest

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

References

[1] G. Caldarelli, J. Ellul, The blockchain oracle problem in decentralized finance—A multivocal approach, Appl. Sci. 11 (16) (2021) 7572, https://doi.org/10.3390/app11167572.

[2] A. Kaur, G. Singh, V. Kukreja, et al., Adaptation of IoT with blockchain in food supply chain management: An analysis-based review in development, benefits and potential applications, Sensors 22 (21) (2022) 8174, https://doi.org/10.3390/s22218174.

[3] B. Aslan, K. Ataşen, Covid-19 information sharing with blockchain, Inf. Technol. Control 50 (4) (2021) 674–685, https://doi.org/10.5755/j01.itc.50.4.29064.

[4] X. Guo, G. Zhang, Y. Zhang, A comprehensive review of blockchain technology-enabled smart manufacturing: A framework, challenges and future research directions, Sensors 23 (1) (2023) 155, https://doi.org/10.3390/s23010155.

[5] C. Delgado-Von-eitzen, L. Anido-Rifón, M.J. Fernández-Iglesias, Blockchain applications in education: A systematic literature review, Appl. Sci. 11 (24) (2021) 11811, https://doi.org/10.3390/app112411811.

[6] P. Ocheja, F.J. Agbo, S.S. Oyelere, et al., Blockchain in education: A systematic review and practical case studies, IEEE Access 10 (2022) 99525–99540, https://doi.org/10.1109/ACCESS.2022.3206791.

[7] Y. Baashar, G. Alkawsi, A.A. Alkahtani, et al., Toward blockchain technology in the energy environment, Sustainability 13 (16) (2021) 9008, https://doi.org/10.3390/su13169008.

[8] Q. Wang, R. Li, L. Zhan, Blockchain technology in the energy sector: From basic research to real world applications, Comput. Sci. Rev. 39 (2021) 100362, https://doi.org/10.1016/j.cosrev.2021.100362.

[9] T. Zhang, B. Li, Y. Zhu, et al., Covert channels in blockchain and blockchain based covert communication: Overview, state-of-the-art, and future directions, Comput. Commun. 205 (2023) 136–146, https://doi.org/10.1016/j.comcom.2023.04.001.

[10] J. Yli-Huumo, D. Ko, S. Choi, et al., Where is current research on blockchain technology?—A systematic review, PLoS ONE 11 (10) (2016) e0163477, https://doi.org/10.1371/journal.pone.0163477.

[11] S. Zhang, J.-H. Lee, Analysis of the main consensus protocols of blockchain, ICT Express 6 (2) (2020) 93–97, https://doi.org/10.1016/J.ICTE.2019.08.001.

[12] A.A. Monrat, O. Schelén, K. Andersson, A survey of blockchain from the perspectives of applications, challenges, and opportunities, IEEE Access 7 (2019) 117134–117151, https://doi.org/10.1109/ACCESS.2019.2936094.

[13] Y. Yuan, F. Wang, Blockchain and cryptocurrencies: Model, techniques, and applications, IEEE Trans. Syst. Man Cybern. Syst. 48 (9) (2018) 1421–1428, https://doi.org/10.1109/TSMC.2018.2854904.

[14] R.O. Ogundokun, S. Misra, R. Maskeliunas, et al., A review on federated learning and machine learning approaches: Categorization, application areas, and blockchain technology, Information 13 (5) (2022) 263, https://doi.org/10.3390/info13050263.

[15] M.H. Tabatabaei, R. Vitenberg, N.R. Veeraragavan, Understanding blockchain: Definitions, architecture, design, and system comparison, Comput. Sci. Rev. 50 (2023) 100575, https://doi.org/10.1016/j.cosrev.2023.100575.

[16] Y. Himeur, A. Sayed, A. Alsalemi, et al., Blockchain-based recommender systems: Applications, challenges and future opportunities, Comput. Sci. Rev. 43 (2022) 100439, https://doi.org/10.1016/j.cosrev.2021.100439.

[17] M.N.M. Bhutta, A.A. Khwaja, A. Nadeem, et al., A survey on blockchain technology: Evolution, architecture and security, IEEE Access 9 (2021) 61048–61073, https://doi.org/10.1109/ACCESS.2021.3072849.

[18] B. Lashkari, P. Musilek, A comprehensive review of blockchain consensus mechanisms, IEEE Access 9 (2021) 43620–43652, https://doi.org/10.1109/ACCESS.2021.3065880.

[19] A. Vilkov, G. Tian, Blockchain’s scope and purpose in carbon markets: A systematic literature review, Sustainability 15 (11) (2023) 8495, https://doi.org/10.3390/su15118495.

[20] J. Lohmer, N. Bugert, R. Lasch, Analysis of resilience strategies and ripple effect in blockchain-coordinated supply chains: An agent-based simulation study, Int. J. Prod. Econ. 228 (2020) 107882, https://doi.org/10.1016/j.ijpe.2020.107882.

[21] S. Saberi, M. Kouhizadeh, J. Sarkis, et al., Blockchain technology and its relationships to sustainable supply chain management, Int. J. Prod. Res. 57 (7) (2019) 2117–2135, https://doi.org/10.1080/00207543.2018.1533261.

[22] M. Kouhizadeh, S. Saberi, J. Sarkis, Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers, Int. J. Prod. Econ. 231 (2021) 107831, https://doi.org/10.1016/j.ijpe.2020.107831.

[23] R.W. Scholz, Digital threat and vulnerability management: The SVIDT method, Sustainability 9 (4) (2017) 554, https://doi.org/10.3390/SU9040554.

[24] S. Sai, V. Chamola, K.-K.R. Choo, et al., Confluence of blockchain and artificial intelligence technologies for secure and scalable healthcare solutions: A review, IEEE Internet Things J. 10 (7) (2023) 5873–5897, https://doi.org/10.1109/JIOT.2022.3232793.

[25] D. Singh, S. Monga, S. Tanwar, et al., Adoption of blockchain technology in healthcare: Challenges, solutions, and comparisons, Appl. Sci. 13 (4) (2023) 2380, https://doi.org/10.3390/app13042380.

[26] B. Liu, X. Si, H. Kang, A literature review of blockchain-based applications in supply chain, Sustainability 14 (22) (2022) 15210, https://doi.org/10.3390/su142215210.

[27] M. Uddin, S. Selvarajan, M. Obaidat, et al., From hype to reality: Unveiling the promises, challenges and opportunities of blockchain in supply chain systems, Sustainability 15 (16) (2023) 12193, https://doi.org/10.3390/su151612193.

[28] A. Saari, S. Junnila, J. Vimpari, Blockchain’s grand promise for the real estate sector: A systematic review, Appl. Sci. 12 (23) (2022) 11940, https://doi.org/10.3390/app122311940.

[29] A. Mohammed, A. Almousa, A. Ghaithan, et al., The role of blockchain in improving the processes and workflows in construction projects, Appl. Sci. 11 (19) (2021) 8835, https://doi.org/10.3390/app11198835.

[30] Y. Wang, X. Cong, L. Zi, et al., Blockchain for credibility in educational development: Key technology, application potential, and performance evaluation, Secur. Commun. Netw. 2023 (2023) 5614241, https://doi.org/10.1155/2023/5614241.

[31] A. Kumar, N.J. Ahuja, M. Thapliyal, et al., Blockchain for unmanned underwater drones: Research issues, challenges, trends and future directions, J. Netw. Comput. Appl. 215 (2023) 103649, https://doi.org/10.1016/j.jnca.2023.103649.

[32] A. Gurzhii, A.K.M.N. Islam, A.K.M.B. Haque, et al., Blockchain enabled digital transformation: A systematic literature review, IEEE Access 10 (2022) 79584–79605, https://doi.org/10.1109/ACCESS.2022.3194004.

[33] S. Kaur, S. Chaturvedi, A. Sharma, et al., A research survey on applications of consensus protocols in blockchain, Secur. Commun. Netw. 2021 (2021) 6693731, https://doi.org/10.1155/2021/6693731.

[34] X. Sun, F.R. Yu, P. Zhang, et al., A survey on zero-knowledge proof in blockchain, IEEE Netw. 35 (4) (2021) 198–205, https://doi.org/10.1109/MNET.011.2000473.

[35] Z.G.T. Cooper, The deep time of bitcoin: Excavating the “work” in proof-of-work cryptocurrency systems, in: AoIR Selected Papers of Internet Research, AoIR, 2021, https://doi.org/10.5210/spir.v2021i0.11887.

[36] B.R. Sutherland, Blockchain’s first consensus implementation is unsustainable, Joule 3 (4) (2019) 917–919, https://doi.org/10.1016/j.joule.2019.04.001.

[37] R. Bezuidenhout, W. Nel, A. Burger, Nonlinear proof-of-work: Improving the energy efficiency of bitcoin mining, J. Constr. Proj. Manag. Innov. 10 (1) (2020) 20–32, https://doi.org/10.36615/jcpmi.v10i1.351.

[38] M. Bondarev, Energy consumption of bitcoin mining, Int. J. Energy Econ. Policy 10 (4) (2020) 525–529, https://doi.org/10.32479/ijeep.9276.

[39] S. Talukder, R. Vaughn, A template for alternative proof of work for cryptocurrencies, in: Proceedings of the 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), IEEE, 2021, pp. 1–6, https://doi.org/10.1109/SMARTGENCON51891.2021.9645773.

[40] D. Drusinsky, On the high-energy consumption of bitcoin mining, Computer 55 (1) (2022) 88–93, https://doi.org/10.1109/MC.2021.3123781.

[41] A. de Vries, Bitcoin boom: What rising prices mean for the network’s energy consumption, Joule 5 (3) (2021) 509–513, https://doi.org/10.1016/j.joule.2021.02.006.

[42] J. Ullrich, N. Stifter, A. Judmayer, et al., Proof-of-blackouts? How proof-of-work cryptocurrencies could affect power grids, in: M. Bailey, T. Holz, M. Stamatogian-

nakis, et al. (Eds.), Research in Attacks, Intrusions, and Defenses, Springer, Cham, 2018, pp. 184–203, https://doi.org/10.1007/978-3-030-00470-5_9.

[43] H. Vranken, Sustainability of bitcoin and blockchains, Curr. Opin. Environ. Sustain. 28 (2017) 1–9, https://doi.org/10.1016/j.cosust.2017.04.011.

[44] K. Košťál, T. Krupa, M. Gembec, et al., On transition between PoW and PoS, in: Proceedings of the 2018 International Symposium ELMAR, IEEE, 2018, pp. 207–210, https://doi.org/10.23919/ELMAR.2018.8534642.

[45] K. Stevenson, O. Skoglund, M. Raikwar, et al., Efficient novel privacy preserving pos protocol proof-of-concept with algorand, in: Proceedings of the 2021 3rd Blockchain and Internet of Things Conference, ACM, 2021, pp. 44–52, https://doi.org/10.1145/3475992.3475999.

[46] N. Sheth, P. Prajapati, A. Shaikh, et al., Casper: Modification of bitcoin using proof of stake, in: S. Satapathy, A. Joshi (Eds.), Information and Communication Technology for Intelligent Systems, Springer, Singapore, 2019, pp. 79–85, https://doi.org/10.1007/978-981-13-1742-2_8.

[47] V. Bachani, A. Bhattacharjya, Preferential delegated proof of stake (PDPoS)—Mmodified DPoS with two layers towards scalability and higher TPS, Symmetry 15 (1) (2023) 4, https://doi.org/10.3390/sym15010004.

[48] X. Li, J. Xu, X. Fan, et al., Puncturable signatures and applications in proof-of-stake blockchain protocols, IEEE Trans. Inf. Forensics Secur. 15 (2020) 3872–3885, https://doi.org/10.1109/TIFS.2020.3001738.

[49] M. Saad, Z. Qin, K. Ren, et al., e-PoS: Making proof-of-stake decentralized and fair, IEEE Trans. Parallel Distrib. Syst. 32 (8) (2021) 1961–1973, https://doi.org/10.1109/tpds.2020.3048853.

[50] V. Bagaria, A. Dembo, S. Kannan, et al., Proof-of-stake longest chain protocols: Security vs Predictability, in: Proceedings of the 2022 ACM Workshop on Developments in Consensus, IEEE, 2022, pp. 29–42, https://doi.org/10.1145/3560829.3563559.

[51] A. Li, X. Wei, Z. He, Robust proof of stake: A new consensus protocol for sustainable blockchain systems, Sustainability 12 (7) (2020) 2824, https://doi.org/10.3390/su12072824.

[52] F. Yang, W. Zhou, Q. Wu, et al., Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism, IEEE Access 7 (2019) 118541–118555, https://doi.org/10.1109/ACCESS.2019.2935149.

[53] M. Kaur, M.Z. Khan, S. Gupta, et al., MBCP: Performance analysis of large scale mainstream blockchain consensus protocols, IEEE Access 9 (2021) 80931–80944, https://doi.org/10.1109/ACCESS.2021.3085187.

[54] Y. Xu, X. Yang, J. Zhang, et al., Proof of engagement: A flexible blockchain consensus mechanism, Wirel. Commun. Mob. Comput. 2021 (2021) 6185910, https://doi.org/10.1155/2021/6185910.

[55] B. Cao, Y. Li, L. Zhang, et al., When Internet of Things meets blockchain: Challenges in distributed consensus, IEEE Netw. 33 (6) (2019) 133–139, https://doi.org/10.1109/MNET.2019.1900002.

[56] R. Damaševičius, R. Maskeliūnas, Leveraging entangled quantum states to develop consensus mechanisms in blockchain networks for smart forestry applications, in: Proceedings of the 2024 6th International Conference on Computing and Informatics (ICCI), IEEE, 2024, pp. 356–360, https://doi.org/10.1109/ICCI61671.2024.10485031.

[57] Y.I. Alzoubi, A. Al-Ahmad, H. Kahtan, et al., Internet of Things and blockchain integration: Security, privacy, technical, and design challenges, Future Internet 14 (7) (2022) 216, https://doi.org/10.3390/fi14070216.

[58] J. Henriques, W. Westerlund, Digitalization of forest management: Next generation unsupervised monitoring using Internet of Things and blockchain, MS Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2020.

[59] R. Singh, A. Gehlot, S.V. Akram, et al., Forest 4.0: Digitalization of forest using the Internet of Things (IoT), J. King Saud. Univ. Comput. Inf. Sci. 34 (2022) 5587–5601, https://doi.org/10.1016/j.jksuci.2021.02.009.

[60] S. Liu, J. Wu, C. Long, IoT meets blockchain: Parallel distributed architecture for data storage and sharing, in: Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2018, pp. 1355–1360, https://doi.org/10.1109/Cybermatics_2018.2018.00233.

[61] W. Liang, M. Tang, J. Long, et al., A secure Fabric blockchain-based data transmission technique for industrial Internet-of-Things, IEEE Trans. Ind. Inform. 15 (6) (2019) 3582–3592, https://doi.org/10.1109/TII.2019.2907092.

[62] S. Abed, R. Jaffal, B.J. Mohd, A review on blockchain and IoT integration from energy, security and hardware perspectives, Wirel. Pers. Commun. 129 (3) (2023) 2079–2122, https://doi.org/10.1007/s11277-023-10226-5.

[63] C.P. Igiri, D. Bhargava, C. Udanor, et al., Blockchain versus IOTA tangle for Internet of Things: The best architecture, Blockchain Technology (2022) 259–278, https://doi.org/10.1201/9781003138082-16.

[64] C. Gómez Mont, S. Persson, C Buenadicha Sánchez, Digital tokens for climate action and nature-based solutions: Exploration of opportunities and considerations, https://doi.org/10.18235/0004834, 2023. (Accessed 26 October 2026).

[65] B. Vagadia, Data integrity, control and tokenization, in: Digital Disruption. Future of Business and Finance, Springer, Cham, 2020, pp. 107–176, https://doi.org/10.1007/978-3-030-54494-2_5.

[66] G. Kotsialou, K. Kuralbayeva, T. Laing, Blockchain's potential in forest offsets, the voluntary carbon markets and REDD+, Environ. Conserv. 49 (3) (2022) 137–145, https://doi.org/10.1017/S0376892922000157.

[67] S. Saraji, M. Borowczak, A blockchain-based carbon credit ecosystem, arXiv preprint, arXiv:2107.00185, 2021.

[68] G. Kotsialou, K. Kuralbayeva, T. Laing, et al., Forest carbon offsets over a smart ledger, SSRN preprint, https://doi.org/10.31235/osf.io/mk7fw, 2021.

[69] O. Bodemer, Transforming the insurance industry with blockchain and smart contracts: Enhancing efficiency, transparency, and trust, TechRxiv, https://doi.org/10.36227/techrxiv.24006237.v1, 2023.

[70] A. Galenovich, S. Lonshakov, A. Shadrin, Chapter 17 - Blockchain ecosystem for carbon markets, environmental assets, rights, and liabilities: Concept design and implementation, in: A. Marke (Ed.), Transforming Climate Finance and Green Investment with Blockchains, Academic Press, New York, NY, 2018, pp. 229–242, https://doi.org/10.1016/B978-0-12-814447-3.00017-3.

[71] G.E. Marchant, Z. Cooper, P. Gough-Stone, Bringing technological transparency to tenebrous markets: The case for using blockchain to validate carbon credit trading markets, Nat. Res. J. 62 (2022) 159, https://digitalrepository.unm.edu/nrj/vol62/iss2/2/.

[72] Y. Zhao, Y. Ban, J. Sullivan, Tokenized time-series in satellite image segmentation with transformer network for active fire detection, IEEE Trans. Geosci. Remote Sens. 61 (2023) 1–13, https://doi.org/10.1109/TGRS.2023.3287498.

[73] A. Alonso-Robisco, J. Manuel Carbo, E. Kormanyos, et al., Houston, we have a problem: Can satellite information bridge the climate-related data gap?, LAJCB 7 (1) (2026) 100173, https://doi.org/10.1016/j.latcb.2025.100173.

[74] P. Howson, S. Oakes, Z. Baynham-Herd, et al., Cryptocarbon: The promises and pitfalls of forest protection on a blockchain, Geoforum 100 (2019) 1–9, https://doi.org/10.1016/j.geoforum.2019.02.011.

[75] Y. Peng, W. Huang, Using blockchain technology and sharing culture to promote sustainable forest management in tribal communities, J. Environ. Public Health 2022 (2022) 1529407, https://doi.org/10.1155/2022/1529407.

[76] E. Tan, S. Mahula, J. Crompvoets, Blockchain governance in the public sector: A conceptual framework for public management, Gov. Inf. Q. 39 (1) (2022) 101625, https://doi.org/10.1016/j.giq.2021.101625.

[77] D. Helbing, S. Mahajan, R.H. Fricker, et al., Democracy by design: Perspectives for digitally assisted, participatory upgrades of society, J. Comput. Sci. 71 (2023) 102061, https://doi.org/10.1016/j.jocs.2023.102061.

[78] M.M. Ibrahimy, A. Norta, P. Normak, Blockchain-based governance models supporting corruption-transparency: A systematic literature review, Blockchain: Res Appl 5 (2) (2024) 100186, https://doi.org/10.1016/j.bcra.2023.100186.

[79] M. Ebrahim, A. Hafid, E. Elie, Blockchain as privacy and security solution for smart environments: A survey, arXiv preprint, arXiv:2203.08901, 2022.

[80] P.-W. Chi, Y.-H. Lu, A. Guan, A privacy-preserving zero-knowledge proof for blockchain, IEEE Access 11 (2023) 85108–85117, https://doi.org/10.1109/ACCESS.2023.3302691.

[81] R. Lavin, X. Liu, H. Mohanty, et al., A survey on the applications of zero-knowledge proofs, arXiv preprint, arXiv:2408.00243, 2024.

[82] J. Heiss, T. Oegel, M. Shakeri, et al., Verifiable carbon accounting in supply chains, IEEE Trans. Serv. Comput. 17 (4) (2024) 1861–1874, https://doi.org/10.1109/TSC.2023.3332831.

[83] T. Feng, P. Yang, C. Liu, et al., Blockchain data privacy protection and sharing scheme based on zero-knowledge proof, Wirel. Commun. Mob. Comput. 2022 (2022) 1040662, https://doi.org/10.1155/2022/1040662.

[84] A. Alofi, M.A. Bokhari, R. Bahsoon, et al., Optimizing the energy consumption of blockchain-based systems using evolutionary algorithms: A new problem formulation, IEEE Trans. Sustain. Comput. 7 (4) (2022) 910–922, https://doi.org/10.1109/TSUSC.2022.3160491.

[85] A.L.C. Merlo, D.S. Mendonça, J. Santos, et al., Blockchain for the carbon market: A literature review, Discov. Environ. 3 (1) (2025) 68, https://doi.org/10.1007/s44274-025-00260-4.

[86] A. Sharma, Consensus mechanisms in blockchain networks: Analyzing various consensus mechanisms such as proof of work (PoW), proof of stake (PoS), and practical Byzantine fault tolerance (PBFT), Blockchain Tech. & Distributed Sys. 1 (1) (2021) 1–11.

[87] S. Fahim, S.K. Rahman, S. Mahmood, Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV, Int. J. Math. Sci. Comput. 9 (3) (2023) 46–57, https://doi.org/10.5815/ijmsc.2023.03.04.

[88] M. Wendl, M.H. Doan, R. Sassen, The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review, J. Environ. Manag. 326 (2023) 116530, https://doi.org/10.1016/j.jenvman.2022.116530.

[89] S.W. Sheng, S. Wicha, Blockchain-based traceability for teak identity: A transformational approach, J. Mob. Multimed. 20 (2) (2024) 267–306, https://doi.org/10.13052/jmm1550-4646.2022.

[90] P. Rani, P. Sharma, I. Gupta, Toward a greener future: A survey on sustainable blockchain applications and impact, J. Environ. Manag. 354 (2024) 120273, https://doi.org/10.1016/j.jenvman.2024.120273.

[91] C. Sguanci, R. Spatafora, A.M. Vergani, Layer 2 blockchain scaling: A survey, arXiv preprint, arXiv:2107.10881, 2021.

[92] M.A. Ferrag, L. Shu, X. Yang, et al., Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges, IEEE Access 8 (2020) 32031–32053, https://doi.org/10.1109/ACCESS.2020.2973178.

[93] C. Pan, A. Shrestha, J.L. Innes, et al., Key challenges and approaches to addressing barriers in forest carbon offset projects, J. For. Res. 33 (2022) 1109–1122, https://doi.org/10.1007/s11676-022-01488-z.

[94] A.S. Mori, K.P. Lertzman, L. Gustafsson, Biodiversity and ecosystem services in forest ecosystems: A research agenda for applied forest ecology, J. Appl. Ecol. 54 (2017) 12–27, https://doi.org/10.1111/1365-2664.12669.

[95] S.A. Nitoslawski, K. Wong-Stevens, J.W.N. Steenberg, et al., The digital forest: Mapping a decade of knowledge on technological applications for forest ecosystems, Earth's Future 9 (2021) e2021EF002123, https://doi.org/10.1029/2021EF002123.

[96] I. Thompson, B. Mackey, S. McNulty, et al., Forest resilience, biodiversity, and climate change. A synthesis of the biodiversity/resilience/stability relationship in forest ecosystems, https://www.uncclearn.org/wp-content/uploads/library/cbd-ts-43-en.pdf, 2009. (Accessed 23 October 2026).

[97] E.E. Cleland, Biodiversity and ecosystem stability, Nat. Educ. Knowledge 3 (10) (2011) 14.

[98] P. Balvanera, A.B. Pfisterer, N. Buchmann, et al., Quantifying the evidence for biodiversity effects on ecosystem functioning and services, Ecol. Lett. 9 (10) (2006) 1146–1156, https://doi.org/10.1111/j.1461-0248.2006.00963.x.

[99] A. Guru, B.K. Mohanta, H. Mohapatra, et al., A survey on consensus protocols and attacks on blockchain technology, Appl. Sci. 13 (4) (2023) 2604, https://doi.org/10.3390/app13042604.

[100] A.E. Richards, D.I. Forrester, J. Bauhus, et al., The influence of mixed tree plantations on the nutrition of individual species: A review, Tree Physiol. 30 (9) (2010) 1192–1208, https://doi.org/10.1093/treephys/tpq035.

[101] D. Tilman, D. Wedin, J. Knops, Productivity and sustainability influenced by biodiversity in grassland ecosystems, Nature 379 (1996) 718–720, https://doi.org/10.1038/379718a0.

[102] S. Naeem, Species redundancy and ecosystem reliability, Conserv. Biol. 12 (1) (1998) 39–45, https://doi.org/10.1111/j.1523-1739.1998.96379.x.

[103] G. Peterson, C.R. Allen, C.S. Holling, Ecological resilience, biodiversity, and scale, Ecosystems 1 (1998) 6–18, https://doi.org/10.1007/s100219900002.

[104] J. Bengtsson, S.G. Nilsson, A. Franc, et al., Biodiversity, disturbances, ecosystem function and management of European forests, For. Ecol. Manag. 132 (1) (2000) 39–50, https://doi.org/10.1016/S0378-1127(00)00378-9.

[105] P. Angelstam, T. Kuuluvainen, Boreal forest disturbance regimes, successional dynamics and landscape structures: A European perspective, Ecol. Bull. 51 (2004) 117–136.

[106] M.E. Harmon, K.J. Nadelhoffer, J.M. Blair, Measuring decomposition, nutrient turnover, and stores in plant litter, in: G.P. Robertson, D.C. Coleman, C.S. Bledsoe, et al. (Eds.), Standard Soil Methods for Long-Term Ecological Research, Oxford Academic, New York, NY, 1999, pp. 202–240, https://doi.org/10.1093/oso/9780195120837.003.0011.

[107] B. Berg, Litter decomposition and organic matter turnover in northern forest soils, For. Ecol. Manag. 133 (1) (2000) 13–22, https://doi.org/10.1016/S0378-1127(99)00294-7.

[108] E. Terhonen, K. Blumenstein, A. Kovalchuk, et al., Forest tree microbiomes and associated fungal endophytes: Functional roles and impact on forest health, Forests 10 (1) (2019) 42, https://doi.org/10.3390/f10010042.

[109] D.S. Guttman, A.C. McHardy, P. Schulze-Lefert, Microbial genome-enabled insights into plant – microorganism interactions, Nat. Rev. Genet. 15 (2014) 797–813, https://doi.org/10.1038/nrg3748.

[110] P.R. Hardoim, L.S. van Overbeek, G. Berg, et al., The hidden world within plants: Ecological and evolutionary considerations for defining functioning of microbial endophytes, Microbiol. Mol. Biol. Rev. 79 (3) (2015) 293–320, https://doi.org/10.1128/mmbr.00050-14.

[111] H. Toju, P.R. Guimarães, J.M. Olesen, et al., Assembly of complex plant–fungus networks, Nat. Commun. 5 (2014) 5273, https://doi.org/10.1038/ncomms6273.

[112] A. Kiayias, A. Polydouri, D. Zindros, The velvet path to superlight blockchain clients, in: Proceedings of the 3rd ACM Conference on Advances in Financial Technologies, ACM, 2021, pp. 205–218, https://doi.org/10.1145/3479722.3480999.

[113] T. Nemoz, A. Zamyatin, On the deployment of FlyClient as a velvet fork: Chainsewing attacks and countermeasures, IACR Cryptol. ePrint Arch. 2021 (2021) 782.

[114] P. Perazzo, R. Xefraj, SmartFly: Fork-free super-light Ethereum classic clients for the Internet of Things, IEEE Internet Things J. 11 (9) (2024) 15348–15358, https://doi.org/10.1109/JIOT.2024.3350333.

[115] R. Matzutt, M. Henze, D. Müllmann, et al., Illicit blockchain content: Its different shapes, consequences, and remedies, in: S. Ruj, S.S. Kanhere, M. Conti (Eds.), Blockchains. Advances in Information Security, Springer, Cham, 2024, pp. 301–336, https://doi.org/10.1007/978-3-031-32146-7_10.

[116] A. Gangwal, H.R. Gangavalli, A. Thirupathi, A survey of Layer-two blockchain protocols, J. Netw. Comput. Appl. 209 (2023) 103539, https://doi.org/10.1016/j.jnca.2022.103539.