

Proof-of-Friendship Consensus Mechanism for Resilient Blockchain Technology

MARCHANG, Jims <<http://orcid.org/0000-0002-3700-6671>>, SRIKANTH, Rengaprasad, KEISHING, Solan and KASHYAP, Indranee

Available from Sheffield Hallam University Research Archive (SHURA) at:

<https://shura.shu.ac.uk/35165/>

This document is the Published Version [VoR]

Citation:


MARCHANG, Jims, SRIKANTH, Rengaprasad, KEISHING, Solan and KASHYAP, Indranee (2025). Proof-of-Friendship Consensus Mechanism for Resilient Blockchain Technology. *Electronics*, 14 (6): 1153. [Article]

Copyright and re-use policy

See <http://shura.shu.ac.uk/information.html>

Article

Proof-of-Friendship Consensus Mechanism for Resilient Blockchain Technology

Jims Marchang^{1,2,*}, Rengaprasad Srikanth³, Solan Keishing² and Indranee Kashyap²¹ Advanced Wellbeing Research Centre, Sheffield Hallam University, Sheffield S1 1WB, UK² School of Computing and Digital Technologies, Sheffield Hallam University, Sheffield S1 1WB, UK; s.keishing@shu.ac.uk (S.K.); indranee.kashyap@shu.ac.uk (I.K.)³ Supply Chain Security, BT Group, 1 Braham St, London E1 8EE, UK; rengaprasad.srikanth@bt.com

* Correspondence: jims.marchang@shu.ac.uk

Abstract: Traditional blockchain consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), face significant challenges related to the centralisation of validators and miners, environmental impact, and trustworthiness. While PoW is highly secure, it is energy-intensive, and PoS tends to favour wealthy stakeholders, leading to validator centralisation. Existing mechanisms lack fairness, and the aspect of sustainability is not considered. Moreover, it fails to address social trust dynamics within validator selection. To bridge this research gap, this paper proposes Proof of Friendship (PoF)—a novel consensus mechanism that leverages social trust by improving decentralisation, enhancing fairness and sustainability among the validators. Unlike traditional methods that rely solely on computational power or financial stakes, PoF integrates friendship-based trust scores with geo-location diversity, transaction reliability, and sustainable energy adoption. By incorporating a trust graph, where validators are selected based on their verified relationships within the network, PoF mitigates the risks of Sybil attacks, promotes community-driven decentralisation, and enhances the resilience of the blockchain against adversarial manipulation. This research introduces the formal model of PoF, evaluates its security, decentralisation, and sustainability trade-offs, and demonstrates its effectiveness compared to existing consensus mechanisms. Our investigation and results indicate that PoF achieves higher decentralisation, improved trustworthiness, reduced validator monopolisation, and enhanced sustainability while maintaining strong network security. This study opens new avenues for socially aware blockchain governance, making consensus mechanisms more equitable, efficient, and environmentally responsible. This consensus mechanism demonstrates a holistic approach to modern blockchain design, addressing key challenges in trust, performance, and sustainability. The mechanism is tested theoretically and experimentally to validate its robustness and functionality. Processing latency (PL), network latency (NL) [transaction size/network speed], synchronisation delays (SDs), and cumulative delay per transaction are 85 ms, 172 ms, 1802 ms, [PL + NL + SD] 2059 ms, respectively.

Keywords: blockchain technology; consensus; proof of work; proof of stake; cyber-attacks

Academic Editor: Antoni Morell

Received: 11 January 2025

Revised: 4 March 2025

Accepted: 6 March 2025

Published: 14 March 2025

Citation: Marchang, J.; Srikanth, R.; Keishing, S.; Kashyap, I.Proof-of-Friendship Consensus Mechanism for Resilient Blockchain Technology. *Electronics* **2025**, *14*, 1153. <https://doi.org/10.3390/electronics14061153>**Copyright:** © 2025 by the authors. Licensee MDPI, Basel, Switzerland.This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

A blockchain is a peer-to-peer distributed ledger technology that allows data to be securely stored, shared, and updated across a distributed network of computers. It operates on the principles of decentralisation, transparency, and immutability. The adoption of blockchain technologies has reached far and near across various industries from fintech and banking to supply chain, healthcare, energy and utilities, and beyond. *What makes*

blockchain technology so remarkable? Unlike traditional systems, blockchain networks operate without centralised governing authorities. They provide an innovative and highly secure mechanism for data storage, offering minimal opportunities for attackers to compromise the integrity of the stored information [1–3].

In a blockchain-distributed network, one of the key features it must possess is a consensus algorithm, and it is critical because it ensures that all nodes in the network agree on the validity and accuracy of the data stored on the blockchain [4–6]. This agreement is essential for maintaining the integrity, security, and functionality of a decentralised system. Here are the key reasons why consensus algorithms are important: they are crucial in maintaining trust among the decentralised nodes, preventing double spending, maintaining data integrity and security, preserving fault tolerance and resistance to attacks, and providing scalability. Consensus algorithms optimise the efficiency of transaction validation and block addition, balancing the need for security with the need for timely performance in the network [7].

Bitcoin [8] and Ethereum [9] are often considered pioneers of cryptocurrencies and digital tokens. There are two primary consensus mechanisms that most blockchains are based on: Proof of Work (PoW) and Proof of Stake (PoS). Most of the world’s largest blockchain networks fall into either of these two categories; however, in recent times, there has been a large influx of newer mechanisms that use different approaches to address security issues and make them more efficient. Such distributed systems must be sustainable and maintain trust across the distributed network. So, researchers are working on building sustainable blockchain solutions and making them scalable and energy-efficient to adopt [10–13]. To maintain trust and transparency in blockchain applications, various authors have explored and provided solutions for banking, green finance, economics, etc. [14–18], to ensure the safe adoption of such disruptive technology.

Bitcoin adopts the Proof-of-Work (PoW) consensus mechanism, where all the miners on the network provide proof that they utilised computational power to reach a consensus. It is slower compared to the Proof-of-Stake (PoS) consensus approach adopted by, say, the Ethereum network. The power consumption in PoW is not comparable with that of PoS solutions, which is one of the main reasons for Ethereum moving from PoW to PoS solutions, as shown in Table 1 based on an analysis carried out by the University of Cambridge [19,20]. As of 31 December 2024, the average yearly power consumption for Bitcoin is 183.62 TWh, and that of Ethereum 2.0 is only a mere 5.72 GWh (PS: 1 TWh = 1000 GWh). Thus, the annual energy consumption of Ethereum is approximately less than 0.003% of the annual energy consumed by the Bitcoin network.

Table 1. Bitcoin and Ethereum power consumption [13,14].

Year	Bitcoin	Ethereum 1.0	Ethereum 2.0
2011	0.14 TWh	-	-
2012	0.10 TWh	-	-
2013	1.06 TWh	-	-
2014	4.73 TWh	-	-
2015	3.62 TWh	0.10 TWh	-
2016	5.73 TWh	0.20 TWh	-
2017	12.93 TWh	2.65 TWh	-
2018	43.32 TWh	8.98 TWh	-

Table 1. Cont.

Year	Bitcoin	Ethereum 1.0	Ethereum 2.0
2019	54.63 TWh	5.75 TWh	-
2020	67.14 TWh	6.69 TWh	-
2021	89.00 TWh	16.40 TWh	0.01 GWh
2022	95.53 TWh	17.58 TWh	2.33 GWh
2023	121.13 TWh	-	5.85 GWh
2024	183.62 TWh	-	5.72 GWh

Unlike PoW, the PoS algorithm selects validators for a transaction from a pool of pre-determined validators. In the crypto world, this system works based on the amount of cryptocurrency validators stake in their account. The idea is to ensure only responsible and accountable nodes take part in the validation process. It does not matter if the validators are from the same region or not. It does not even matter the success rates of the previous transactions or the types of energy sources it uses, and that is the area that this paper is exploring. The more coins staked, the higher your chance of being selected as a validator [21]. Such an approach might invite an opportunity for an over-reliance on some high-performing nodes, leading to unfairness and security risks.

The most popular blockchain network, i.e., the Bitcoin network, could suffer from a 51% attack, also known as a majority attack, whereby an attacker can reverse or manipulate the network by capturing more than 50% of the resources [22]. So, malicious actors should not be allowed to manage more than 50% of the resources in Proof-of-Work (PoW) blockchain networks like bitcoin. Otherwise, it will enable the malicious entity to tamper, alter, or modify the details of transactions. In a Proof-of-Stake (PoS) network, controlling 51% of the staked cryptocurrency is enough to carry out such an attack [21]; however, this is more challenging compared to PoW because attackers need to control 51% or more of the staked ETH tokens, i.e., those of the Ethereum network. If there is an evenly distributed approach to this “staking” among the network users, then the system can be influenced via blockchain forks [23]. Thus, blockchains are far from perfect; they face multiple challenges including security and efficiency issues, network centralisation due to the dependence on resource accumulation or the staking power of miners and validators, and un-scalable power-consumption concerns. So, this paper aimed to address some of the issues raised in PoW and PoS consensus solutions to make the validators more distributed over the globe, increase the reliance on trusted nodes, avoid 51% attacks, and encourage those who use renewable and green energy to make blockchain networks environmentally friendly. Thus, this novel multi-factor consensus mechanism based on friendship among multiple parameters aims to improve the security and trust in a blockchain network.

The mechanism proposed in this paper aims to address the following four objectives by incorporating geo-location, successful transaction rates of the participating validators, and the energy source used in the consensus mechanism of the validating process:

1. Enhancing decentralisation and fair validator selection.
2. Improving trust.
3. Promoting sustainable and energy-efficient consensus.
4. Strengthening resistance against 51% attacks and collusion.

The rest of the paper is organised as follows: Section 2 provides the background materials, Section 3 details the proposed PoF mechanism, and Section 4 covers the analysis and discussion. The last two sections, i.e., Sections 5 and 6, cover the limitations and future directions and the conclusion, respectively.

2. Background Materials

This section investigates the background literature of consensus algorithms with a special focus on the security challenges inherent in existing blockchain frameworks, thereby paving the way for proposing a novel system that addresses these issues; it also explores the power consumption challenges commonly associated with blockchain technologies [24]. Blockchain activity involves the following key steps: (1) Transaction Initiation: A user initiates a transaction, which is broadcast to the network. (2) Validation: The network nodes validate the transaction using the blockchain's consensus mechanism. (3) Block Creation: Valid transactions are grouped into a block and cryptographically linked to the previous block. (4) Addition to the Chain: The block is added to the blockchain, becoming a permanent and unchangeable part of the ledger. (5) Updates Across Nodes: The updated blockchain is distributed to all nodes in the network.

2.1. Blockchain Components

Before delving into an in-depth analysis of blockchain mechanisms, it is essential to first understand the fundamental components of a blockchain. The blockchain node could consist of the elements listed in Figure 1, i.e., blockchain version, Merkle root, timestamp, nonce, transaction ID, Data, previous hash, current hash, and so on. These parameters are considered for this proposed system too. While the network is maintained by miners and validators. Other key terminologies of blockchain include the following:

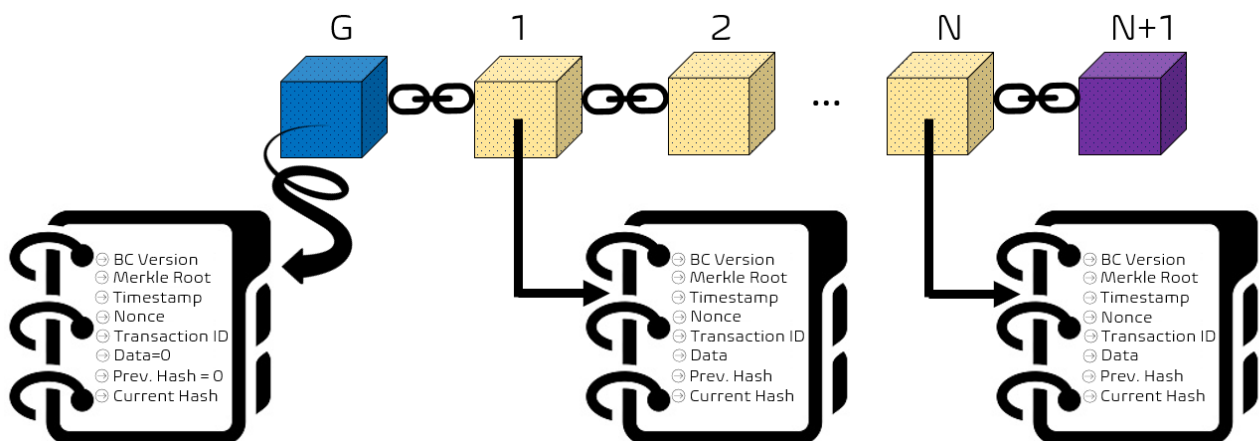


Figure 1. Blockchain Chain node (designed by authors).

Block time: This is the time taken to confirm a new block on the chain [25].

Transaction confirmation time: This refers to the time taken from the moment a transaction is announced to the moment it is appended to the blockchain [26].

Transactions per second (TPS): This is arguably the most important metric to compare network efficiency [27].

Block size: The size of a block is often fixed, and in the case of Bitcoin, it is 1 MB. The block size determines how many transactions can be stored in a block. This is usually in the range of 1000 s. The block size plays a role in efficiency [28].

Gas price: Gas price is also known as transaction price. This is the amount of money a user must pay to have their transaction verified on the blockchain. This is usually measured in Gwei. Gwei is a smaller denomination of Ether, where 1 Ether represents one billion Gwei [29].

Hashrate: This is another measure of network speed that is only relevant to Proof of Work; it refers to the rate at which computational power is used in the network. So, the measurement is denoted in hashes per second [30].

Network Difficulty: This is a parameter unique to Proof-of-Work blockchains. The difficulty of the hash calculations that the miners perform and compete over is variable. It fluctuates depending on the number of miners present on the network [31].

2.2. Blockchain Efficiency and Scalability (PoW vs. PoS)

Blockchain efficiency and security are influenced by numerous interconnected factors, often presenting a trade-off between these two paradigms [32]. Striking the right balance requires a nuanced understanding of these elements. A key metric in blockchain performance is latency, frequently misunderstood as being synonymous with TPS (transactions per second). While TPS measures a network's throughput—the number of transactions processed per second—latency refers to the time required to confirm and finalise a transaction [33]. Although a higher number of TPS often correlates with lower latency, the two are distinct parameters. TPS is significantly influenced by the block size and block time; increasing the block size or reducing the block time can enhance the transaction rate [34]. Scalability emerges as a critical consideration when adjusting the block size. For larger blockchains like Bitcoin, increasing the block size may reduce transaction fees by accommodating more data per block. However, a gradual increase could lead to blocks of gigabyte-scale size, creating barriers for average users due to higher bandwidth and hardware requirements [35]. These challenges are relevant to both Proof-of-Work (PoW) and Proof-of-Stake (PoS) mechanisms.

In PoW blockchains, the difficulty parameter—tied to the hashing mechanism—ensures consistent block times by adjusting according to network size. As network difficulty rises, scalability challenges grow, necessitating more powerful hardware for participation. In summary, PoW networks encounter scalability limitations due to fixed block sizes and increasing network difficulty, which makes participation challenging for casual users without advanced hardware. Off-chain solutions offer partial relief but are not large-scale remedies. However, PoS networks, which emphasise staked cryptocurrencies over hardware, are more efficient and accessible for new users, with fewer scalability constraints compared to PoW systems.

2.3. Blockchain Security (PoW vs. PoS)

Technologies leveraging zero-knowledge proofs enable the validation or verification of information without exposing the actual data itself [36]. Ideally, all Internet-based processes would adhere to this model. While that is not yet a universal reality, blockchains exemplify this concept effectively. This is particularly significant in decentralised systems, where no third-party authority exists to verify data. Consequently, blockchain technologies inherently prioritise data privacy and integrity. However, the decentralised nature of blockchain is also its greatest vulnerability. The absence of centralised regulatory authorities facilitates unethical and illegal activities to occur unchecked. Most blockchain security challenges arise not from direct system attacks but from the unreliability of nodes, miners, or validators. The decentralised structure, combined with the anonymity and accessibility it offers, creates an environment conducive to malicious activities. For instance, fraudulent practices like pump-and-dump schemes in the cryptocurrency domain exploit unsuspecting investors. The mechanism proposed in this research aims to address some of these security vulnerabilities.

One of the most immediate risks to blockchain security is presented by oracles. Oracles act as intermediaries between blockchains and external systems, enabling smart contracts and decentralised applications (DApps) to access off-chain data [37]. Oracles are categorised into five types: hardware, software, outbound, inbound, and consensus-based [38]. Their reliability, however, is often inconsistent, making them critical weak points in terms of data integrity. A compromised oracle can feed falsified data into the blockchain, which becomes immutable once added.

Beyond oracles, vulnerabilities in smart contracts can also pose significant risks. For instance, recursive functions within smart contracts can be exploited in “re-entrancy attacks”, enabling attackers to siphon funds repeatedly from a target contract. Such exploits are classified as “Middle Protocol Attacks” [39]. These vulnerabilities are particularly relevant to blockchains that support smart contracts. More commonly discussed blockchain attacks include 51% attacks and Distributed Denial of Service (DDoS) attacks. However, these are primarily feasible for smaller networks, as larger blockchains are generally resistant to such system-wide threats. The most effective attacks in the blockchain ecosystem tend to target individual users or nodes rather than the entire network. For example, Ethereum’s documentation [40] highlights “front-running” as a key risk. Front-running involves exploiting insider information, often using Maximal Extractable Value (MEV) bots. These bots scan unconfirmed transactions in the memory pool (mempool) and prioritise their transactions by paying higher fees, thereby manipulating market prices [41]. This exploit is more prevalent in Proof-of-Work (PoW) systems due to the delay between transaction initiation and confirmation. Although Proof-of-Stake (PoS) systems eliminate mempools, front-running remains a potential threat, even in Ethereum’s planned 2.0 upgrade. Mitigating these attacks would require advanced algorithms to counteract the bots’ speed and targeting strategies [42]. Sybil and Eclipse attacks, meanwhile, disrupt node communication within the blockchain network [43]. Sybil attacks involve creating a large number of malicious nodes to gain majority control, which is nearly impossible in modern blockchains due to computational and verification requirements enforced by consensus mechanisms [44]. Eclipse attacks, as shown in Figure 2, on the other hand, isolate an honest node by surrounding it with malicious nodes, severing its connection to the legitimate network [45]. These attack types are often interlinked, as a Sybil attack can lead to an Eclipse attack. The consequences of an Eclipse attack can be severe, enabling double-spending, DDoS attacks, and the disruption of honest mining efforts. Mitigating such risks requires robust communication path randomisation and other proactive security measures. Therefore, blockchain security is a multifaceted challenge rooted in its decentralised structure and the reliance on nodes and external components like oracles. While Proof-of-Work and Proof-of-Stake systems each face unique vulnerabilities, addressing these issues requires innovative mechanisms and protocols. This research aims to contribute to these solutions by identifying and mitigating key risks within the blockchain ecosystem by improving node distribution and allowing only highly trustable nodes in the validation process by considering the geo-location and success rates of the transaction validation.

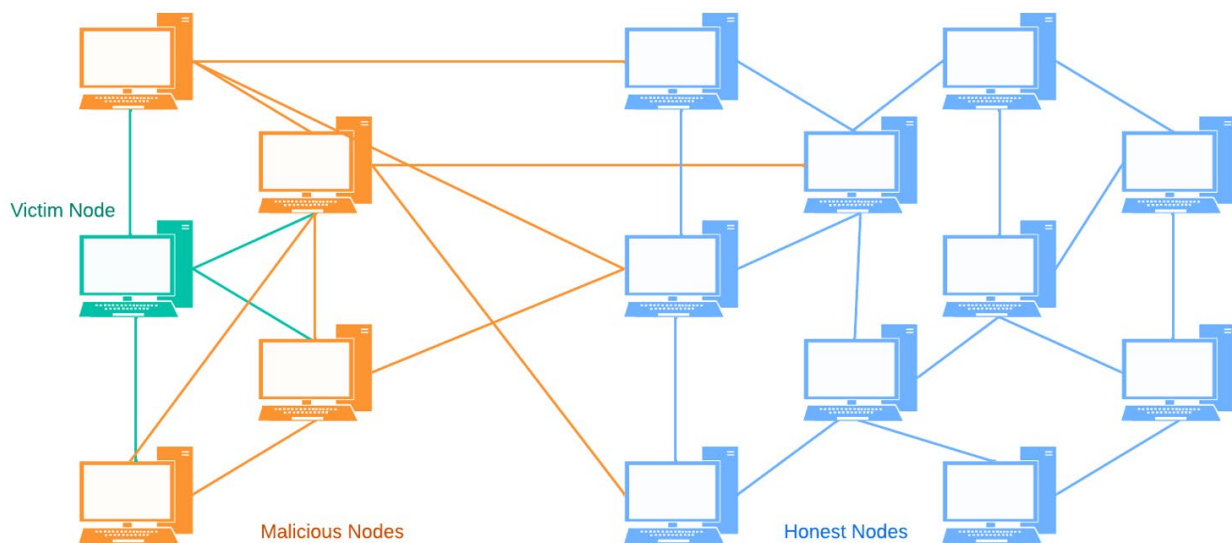


Figure 2. Eclipse attack through malicious Sybil nodes.

In Proof-of-Work (PoW) systems, trust is ensured through redundancy, where multiple miners verify the same transaction competitively. However, this redundancy drives the notoriously high energy consumption of PoW blockchains. Proof of Stake (PoS), on the other hand, does not inherently ensure trust, as the required “stake” can often be purchased outright on exchanges. To address this limitation, alternative mechanisms such as Proof of Reputation have been developed, which evaluate a node or validator’s reliability and incorporate this factor into validator selection. Attacks on mining pools often aim to disrupt financial gains rather than direct theft. For example, selfish miners can withhold reporting processed blocks to the pool, creating forks in the blockchain [46]. These mining pool attacks are categorised into subtypes such as “block withholding”, “pool hopping”, and “fork after withdrawing (FAW)”. Withholding a mined block and revealing it later can overwrite the main blockchain, while pool hopping exploits the network’s difficulty metric. Attackers may temporarily contribute significant computing power to a pool to increase its difficulty before shifting to another network. Several countermeasures can mitigate mining pool attacks [39]:

- Implementing stricter revenue distribution systems.
- Modifying mining protocols to exclude recognition of partial proof of work.
- Establishing credit-verification systems to evaluate miner trustworthiness.
- Adopting dynamic algorithms to determine network difficulty, factoring in past transactions.

However, some of these solutions may resemble centralised financial systems, which critics argue contradict the fundamental principles of blockchain. Another financially driven attack type is the double-spending attack. In this scenario, an attacker exploits the system to use the same cryptocurrency more than once. This is especially effective against users or merchants accepting unconfirmed transactions. By sending a transaction and subsequently issuing another transaction that redirects the funds back to the attacker’s wallet, the attacker can outpace the verification process. Preventing double-spending attacks requires merchants to exercise caution and avoid accepting unconfirmed transactions. The discussion of blockchain security would be incomplete without addressing the role of cryptography. Hashing plays a crucial role in ensuring the integrity of blockchain systems: Hashes store transactional data on the blockchain, with each block containing the hash of the previous block. This structure ensures that altering one block would necessitate modifying all preceding blocks. In PoW, hashes determine network difficulty and computational requirements. Bitcoin utilises the SHA256 hashing algorithm, while Ethereum employs Keccak256 from the SHA3 family, offering enhanced encryption strength. The following table (Table 2) summarises the attack types and their targeted mechanisms for convenience. Note that this list covers only some of the relevant attack vectors, as many others fall outside the scope of this research.

Table 2. Cyber-attacks and mechanisms they primarily affect.

Attack Type	PoW	PoS	Description
51% attacks			These attacks target blockchain networks regardless of mechanism type. A 51% attack in blockchain refers to a situation where a single entity or group gains control of more than 50% of a blockchain network’s mining or computational power [22].
DoS attacks			A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of traffic or sending data in a way that the system cannot handle [47].

Table 2. Cont.

Attack Type	PoW	PoS	Description
Injection attacks			Injection attacks are a type of cyberattack where an attacker injects malicious code or commands into a vulnerable program, query, or system [48].
Double-spending			Double-spending in blockchain refers to a scenario where the same cryptocurrency or digital asset is spent more than once [49].
Oracle exploits			These kinds of attacks exploit vulnerabilities in smart contracts. An oracle is one of the parts of a smart contract that interacts with the external Internet, and naturally, it offers a trove of vulnerabilities [50].
Re-entrancy attacks			It is a vulnerability in smart contracts, particularly in Ethereum and other blockchain platforms that support programmable contracts [51].
Sybil and Eclipse attacks			Sybil and Eclipse attacks target inter-node communications and spoof nodes [52–54].
Transaction failure			The most common security flaw is that a user's transaction fee is taken even if a transaction fails [50,55].
Pool-hopping			Pool-hopping is a strategy used by miners in blockchain-based mining pools to maximise their rewards by switching between different mining pools based on their payout schemes and block discovery patterns [56]. It primarily affects PoW and less on PoS.
Fork After Withdrawing attacks			Fork After Withdrawing (FAW) attacks are a type of blockchain attack that exploits the possibility of creating a forked version of the blockchain after completing a transaction, typically withdrawing assets, to revert the transaction's effects on the original chain [39].
Block Withholding			Block withholding (BWH) is an attack in blockchain mining where a miner deliberately withholds valid blocks they discover instead of broadcasting them to the network [57].
Frontrunning			Frontrunning in a blockchain network refers to malicious or opportunistic behaviour where an entity (usually a miner, validator, or bot) exploits knowledge of pending transactions to gain a financial advantage by placing their transaction ahead of others in the blockchain transaction queue [58].

Yellow represents the mechanism that is unaffected by the said attack. Blue represents the mechanism that is affected by the said attack.

2.4. Background Study of the Next Generation of Blockchain Consensus Mechanisms

Consensus mechanisms have evolved to address specific challenges in previous systems, enabling innovative solutions in blockchain technology. Fundamentally, these mechanisms aim to create a trustworthy environment without requiring users to share personal or sensitive information. Their primary function is to provide Byzantine Fault Tolerance (BFT), addressing the Byzantine General Problem. This theoretical dilemma illustrates the difficulty generals face in reaching a consensus within a distributed network, particularly when some actors may act maliciously. The concept of the 51% attack arises from this problem. Similarly, most consensus mechanisms are developed to resolve specific limitations. For instance, one of the key motivations for creating the Proof-of-Stake (PoS) model was to significantly reduce energy consumption—a factor driving Ethereum's transition to this model.

There are numerous variations of consensus mechanisms, many of which expand upon established models like Proof of Work (PoW) and PoS. Notable mechanisms include the following:

Proof of Work (PoW) [46]: It is the original blockchain consensus mechanism introduced by Bitcoin, where network participants solve complex mathematical problems to validate transactions and create new blocks. It ensures network security and decentralisation by making the validation process computationally intensive and expensive, thereby deterring malicious actors.

Proof of Stake (PoS) [46]: It is a consensus mechanism that selects validators based on the amount of cryptocurrency they hold and are willing to “stake” as collateral. It was developed as a more energy-efficient and scalable alternative to Proof of Work (PoW). Validators are incentivised to act honestly, as they risk losing their staked assets if they act maliciously.

Proof of Authority (PoA) [59]: Designed for private blockchains, PoA offers high transaction throughput. Unlike PoS, where validators stake cryptocurrency, PoA validators stake their identities. This mechanism is scalable, as it operates with a limited number of trustworthy validators selected at random.

Delegated Proof of Stake (DPoS) [60]: It is a consensus mechanism designed to enhance the scalability and efficiency of traditional Proof-of-Stake (PoS) systems. In DPoS, stakeholders vote to elect a smaller group of delegates (or witnesses) who are responsible for validating transactions and producing new blocks. This approach is faster and more energy-efficient, but it can raise concerns about centralisation and governance.

Leased Proof of Stake (LPoS) [61]: It is a variation of Proof of Stake (PoS) that allows users to lease their tokens to a validator or “node”, enhancing their staking power. Validators use the combined stake to participate in block validation, while lessors (those who lease their tokens) share in the rewards earned. This mechanism provides an opportunity for token holders to contribute to network security and earn rewards without running their nodes.

Proof of Burn (PoB) [62]: It is a unique blockchain consensus mechanism where participants “burn” a certain amount of cryptocurrency by sending it to an irretrievable address (a burn address) to gain the right to validate transactions or mine new blocks. This mechanism ensures that validators have invested resources into the network, aligning their incentives with its long-term health.

Proof of Capacity (PoC) [63]: It is also known as *Proof of Space (PoSpace)*, it is a blockchain consensus mechanism that utilises unused hard drive storage space for mining. Participants allocate storage space to solve cryptographic challenges, and the probability of mining a block depends on the amount of disk space dedicated. Unlike Proof of Work (PoW), PoC minimises energy consumption by reducing reliance on computational power.

Proof of Elapsed Time (PoET) [64,65]: It is a blockchain consensus mechanism designed to ensure fair and random leader selection while maintaining energy efficiency. It leverages trusted execution environments (TEEs), such as Intel’s Software Guard Extensions (SGXs), to generate random wait times for nodes. The node with the shortest wait time wins the right to produce the next block.

Proof of Space and Time (PoST) [66]: It is a blockchain consensus mechanism that combines Proof of Space (PoS or PoSpace) and Proof of Time to achieve a secure, energy-efficient, and fair process for mining blocks. This approach was popularised by the Chia Network, which integrates these two elements to balance scalability, decentralisation, and environmental sustainability.

Proof of Importance (PoI) [67]: It is a blockchain consensus mechanism designed to reward active network participation and foster community engagement. It goes beyond

simply relying on stake (as in Proof of Stake) by incorporating additional metrics such as transaction activity, network contributions, and the amount of cryptocurrency held.

The diverse mechanisms outlined above highlight how consensus models are tailored to address specific challenges within blockchain systems. A comparative study of different types of consensus algorithms is shown in Table 3. This research aimed to identify issues within larger consensus mechanisms and propose a novel solution. One challenge with new consensus models is the varying degrees of centralisation or decentralisation they embody. Blockchain purists often criticise these systems, extending their scrutiny to users and crypto exchanges. PoS requires validators to stake coins, with many PoS blockchains imposing minimum staking requirements. Certain exchanges further centralise this process by acting as validators on behalf of users purchasing coins through their platforms. This introduces an element of centralisation, which some sources equate to an oligarchy. Thus, this paper proposes a novel approach that is secure and has a holistic approach to modern blockchain design, addressing key challenges like trust, performance, and sustainability.

Table 3. Comparison of Popular consensus algorithms and techniques.

Consensus Algorithm	Security	Decentralisation	Energy Consumption	Fairness	Scalability	Resilience
Proof of Work [46]	High (strong against attacks, costly to compromise)	High	Very High	Low	Low	High
Proof of Stake [46]	High (with risk of stake centralisation)	Medium to Low	Low	Medium to Low	High	Medium to High
Proof of Authority [59]	Medium (validator trust required)	Low	Low	Low	Very High	Medium
Delegated Proof of Stake [60]	Medium to high (dependent on delegate integrity and voter participation)	Low	Low	Medium	Very High	Medium
Leased Proof of Stake [61]	Medium to high (pooled stakes enhance security but risk centralisation)	Medium	Low	Medium	High	Medium
Proof of Burn [62]	Medium to high (economic disincentives for attacks; risks from wealth concentration)	Medium	Low	Medium	High	Medium to High
Poof of Capacity [63]	Medium to high (dependent on storage distribution and diversity)	Medium	Low	Medium	High	Medium to High
Proof of Elapsed time [64,65]	Medium to high (relies on trusted hardware)	Medium	Low	High	High	Medium to High
Proof of Space and Time [66]	Medium to high (combines storage and time for robust defence mechanisms)	Low	Medium	Medium to High	High	High
Proof of Importance [67]	High (ensures secure participation)	High	Low	Medium	High	Medium to High

3. Proposed Consensus Method

In PoS systems, the verification of transactions is performed through validators, instead of miners. In a standard PoS blockchain, validators are chosen at random from a pool based on certain conditions. In this proposed Proof-of-Friendship mechanism, validators are also selected from a pool, but certain special conditions and statistics are taken into consideration to (1) set the transaction fees, (2) conduct identity verification, and (3) perform validator selection. To make the system sustainable and trustworthy, factors like the geo-location of the validators, success rate of transaction validation, and verified eco-energy source are considered among the distributed network validators as elaborated below:

- Geo-location (G_i): Incorporating geo-location as a factor in selecting validators can help address socio-political challenges and avoid monopoly and control by certain influential validators of a particular region. On a global scale, validators from different regions as the transactors often carry a higher level of perceived trustworthiness, fostering greater confidence in the network when the same agreement is reached across the network.
- Trust based on the success rate of transactions (S_i): Transaction failure leads to a waste of network gas fees. It means that even if the transaction is not successful, the gas fee is taken by the network validators. So, failure to complete the transaction is expensive and the network is not trustable. Thus, the higher a validator's success rate, the higher should be the chance of being nominated by the consensus mechanism. Therefore, the transaction success rate is key to maintaining the validator's trust. So, in this proposed system, S_i is directly proportional to the selection of the validators for the consensus mechanism.
- Verified eco-energy source (E_i): Selecting the right network validators to improve efficiency is one thing, but it is also critical to promote clean validators because of the challenges faced by net-carbon zero, so the use and promotion of clean re-renewable energy during the mining and validation process is vital to make the blockchain solution scalable and sustainable. So, in this proposed system, a novel idea of encouraging the network to use renewable energy is taken into account in the process of selecting the validators. Thus, validators who have a verified renewable power source will be rewarded with a higher chance of selection in the consensus process to make the network scalable and sustainable. This is one of the ways to promote clean mining and validation processes and to make blockchains eco-friendly.

The information needed to certify validators, e.g., knowing the region in which it operates, its transaction success rate, and its energy sources, requires the use of a third-party verification process, but this needs to be conducted while preserving the validator's privacy, and sometimes it may exceed certain boundaries of anonymity e.g., exposing the region or name of the country of the validator. Such a system may be seen as more centralised, so it may work best in a permissioned environment. However, such actions are necessary to make the system more safe, trustable, and adoptable in real-life applications. The idealistic application of Proof of Friendship is in private blockchains where participants will be identified but anonymised by administrators and might need to provide extra data to prove their credibility.

Coming now to transactors, a user who wishes to make a transaction can select from two types of validators:

- A. **Trusted Validator:** This will be a validator who has once validated one of the user's transactions already and meets the criteria in terms of geo-location, transaction success rate, and energy sources; they will be included in the 'friend list'. Depending on the diversity of geographical location, transaction success rates and use of green energy the trust factor of the same node varies over time. Regardless, its trust value is higher than that of a New Validator.
- B. **New Validator:** A New Validator meeting a validator's prerequisites regarding system resources, network requirements, and bandwidth can take part as an initial factor of selection.

Any user/validator has a list of "friends" who have previously validated their transactions successfully and meet all the validator's requirements. The friend list will be dependent on the network size because at least 70% of the validators will be considered in taking part in the validation process to maintain a high security level, and a successful validation of transactions of at least 51% will be considered to ensure correctness. If the number of friends on a translator's friend list is 'n', the same set of validators will not be used; rather, a New Validator will be considered and rotated to guarantee fairness among the validators that meet the validating criteria. The oldest validator on the list will be knocked out if it goes above the required number of validators, and the newest validator that meets the validating criteria will be given a fair opportunity to take part in the validation process. This system is explained in more detail in the following sections.

Transactions validated from the same geo-location are to be given a choice with a lower preference compared to the ones from different locations. But it will be allowed to join the validation, if the number of required validators is not reached or it is met with a lower preference. However, during the trust factor calculation, a geo-location's uniqueness is not the only factor taken into account; the two other factors, i.e., the transaction success rate and the source of energy used for validation, will also be taken into account. New Validators will be allowed to join the initial validation network to maintain fairness.

Proposed Choosing Validators

Just like in PoS, there is a pool of validators from which one is chosen to validate the transaction by considering the following three parameters:

- Trust factor;
- Geo-location;
- Energy source.

The flowchart of the validator selection process is shown in Figure 3. The detailed elaboration of the geo-location diversity, transaction success rate, and energy source check is given below, and the pseudo-code for the validation selection process is elaborated upon in Algorithm 1.

Algorithm 1 The pseudo code for the validator selection in PoF

```

Initialised: MIN_GEO_DIVERSITY = 51, MIN_SUCCESS_RATE = 90, GREEN_ENERGY_WEIGHT = 1.0,
NUCLEAR_ENERGY_WEIGHT = 0.75, BIOFUEL_ENERGY_WEIGHT = 0.5
//Function: Screening Potential Validator Based on Success Rate
function add_validator(validator_address, country, success_rate, energy_source):
    if success_rate >= MIN_SUCCESS_RATE:
        new_validator = Validator(validator_address, country, success_rate, energy_source)
        candidate_validators.append(new_validator)
        Output: "Validator Added", validator_address, country
    else:
        "Validator does not meet minimum success rate"
//Assign validators based on energy source
selected_validators = []
for validator in trusted_validators:
    if validator.energy_source == "green":
        chance = GREEN_ENERGY_WEIGHT
    elif validator.energy_source == "nuclear":
        chance = NUCLEAR_ENERGY_WEIGHT
    elif validator.energy_source == "biofuel":
        chance = BIOFUEL_ENERGY_WEIGHT
    else:
        chance = 0 # Exclude validators with other energy sources
    calculate  $P_i$ : Probability of selecting the  $i$ th validator by using Equation (1).
//Step 4: Calculate geo-location diversity
function calculate_geo_diversity():
    unique_countries = count_unique_keys_in_dictionary(country_count)
    return (unique_countries * 100)/total_validators
//Function: Select validators
function select_validators():
    selected_validators.clear()
    country_count.clear()
    total_validators = 0
//Iterate through candidate validators
for each candidate in candidate_validators:
    Calculate (Trust Factor:  $T_i$ ) by using Equation (2).
    current_geo_diversity = calculate_geo_diversity()
    if current_geo_diversity >= MIN_GEO_DIVERSITY or country_count[candidate.country] == 0:
        selected_validators.append(candidate)
        country_count[candidate.country] += 1
        total_validators += 1
        Output: "Validator Selected", candidate.validator_address, candidate.country
        if total_validators >= MAX_VALIDATORS:
            break
        elif calculate_geo_diversity() < MIN_GEO_DIVERSITY:
            continue
return selected_validators (friend[list])

```

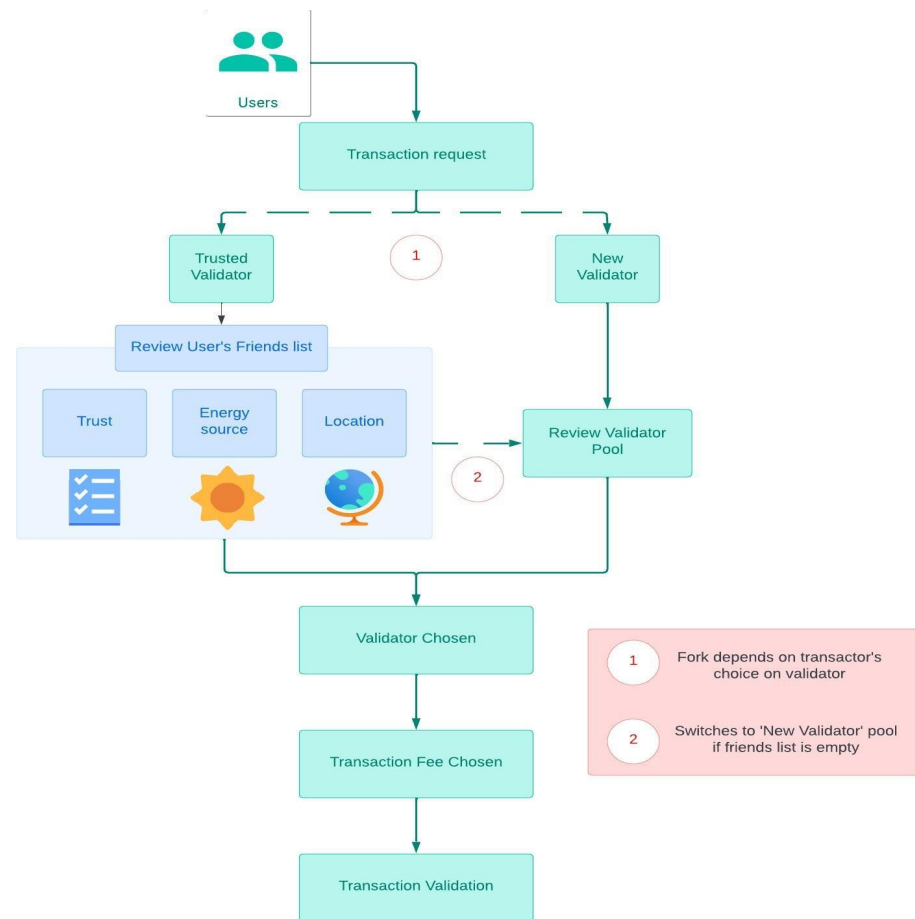


Figure 3. Proof-of-Friendship mechanism.

Firstly, calculate the percentage of unique geo-locations among candidate validators. Ensure a minimum of 51% diversity to improve the real network node distribution. In this model, validators with a transaction success rate of 90% or higher are considered for consensus participation. This ensures reliability and trustworthiness. Transaction failure and network congestion have a negative impact on the blockchain network, and in recent times, the Solana network hit around a 75% transaction failure due to bots and memecoins [55]. So, in this proposed system, to accommodate such network failure, a node with a transaction success rate of 90% or higher is considered. It will become impractical to enforce nodes to maintain 100% successful network transaction rates. No network can guarantee successful transactions at all times. The transaction success rate score (S_i) is between 0 and 1, where $S_i = R_i/100$, and R_i is the success rate in percentage. Energy Source Weighting: Assign a 100% selection probability for validators using green energy. Assign 75% for nuclear energy sources, 50% selection probability for validators using biofuel, and exclude validators using other types of non-renewable energy sources (chance = 0). Equation (1) shows the calculation of the probability of selecting the i th validator based on the energy source.

n : Total number of validators;

W_i : Weight of the i th validator based on the energy source;

P_i : Probability of selecting the i th validator.

$$P_i = \frac{W_i}{\sum_{j=1}^n W_j} \tag{1}$$

where $\sum_{j=1}^n W_j$ is the total weight of all the validators.

$$\text{Trust factor } (T_i) = w_g \cdot G_i + w_s \cdot S_i + w_e \cdot E_i \quad (2)$$

where the following are defined:

G_i : Geo-location diversity score for the i th validator (1 for unique region, 0 for common region).

S_i : Transaction success rate score for the i th validator (normalised between 0 and 1).

E_i : Energy source score for the i th validator (1.0 for green, 0.75 for nuclear, 0.5 for biofuel, 0 for other non-renewable).

w_g, w_s, w_e : Weights assigned to geo-location, transaction success rate, and energy source, respectively.

The following values are assigned:

$w_g = 0.40$ (geo-location weight).

$w_s = 0.40$ (transaction success rate weight).

$w_e = 0.20$ (energy source weight).

The geo-location diversity score (G_i) is 1 if the validator belongs to a unique or under-represented region (100 nodes or less) or 0 if the validator is from a heavily represented region (100 nodes or more). The geo-location of a node can be determined using a method like IP geo-location, and apart from using GPS information, various methods can be used in extracting a geo-location through an IP address, as explored in [68–71]. The accuracy of the regional information is high; e.g., using <https://iplocation.com>, the location of the IP can be accurately determined at a city level. The website can accurately provide the information about an IP address with a detailed granularity in terms of latitude, longitude, country, region, city, and organisation. In this study, only one IP from each region is allowed to participate for testing purposes, but that can be controlled according to the volume required. However, it is important to note that nodes using a VPN will mislead the representation of the node counts from a region, but such nodes using a VPN will have a slower bandwidth capacity leading to network congestion and higher transaction failure rates compared to other nodes because of a distant server, server load, additional security mechanisms, etc. So, those nodes using a VPN will likely have a lower trust score because of its negative impact on the successful network transaction rate. Validators from the same geo-location with the highest trust value are considered if and only if more validators are required per network requirements, i.e., by ensuring that at least 51% of the validators' geo-locations are unique at all times. This is performed to ensure that the majority of the validating nodes are not selected from the same region, which improves the distributed nature of the network.

Lastly, energy consumption is one of the key concerns in sustaining blockchain solutions [72–74] in the fight against climate change, the energy demand for mining, etc. So, in this proposed solution, nodes using green energy sources are given the highest weight compared to other energy sources. This does not mean that using green energy will solve the sustainability challenges of blockchain networks like the Bitcoin network [75]. However, the work of [76] encourages the use of clean and renewable energy to help the environment and address climate change issues. So, this paper gives higher trust scores to those nodes that use or rely on green energy over other energy sources. However, it is indeed a challenging task to ensure and know who uses what types of energy sources. However, different methods can be used to identify who pollutes the environment more than others through a carbon credit system like the ones described in [77–79] and can determine the types of energy sources through those who provide carbon credits to the mining or validating nodes. The energy source score (E_i) has four levels {1.0, 0.75, 0.5, and 0} for green, nuclear, biofuel, and others. The weight assignments for each feature are

dynamic and controlled depending on the sensitivity of the relationship and friendship between these parameters. In this proposed system, it is tested with a weight of 0.40, 0.40, and 0.2 for w_g , w_s , and w_e , respectively. In the Proof-of-Friendship (PoF) consensus mechanism, the selection criteria for validators are not weighted equally but weighted differently with 40%, 40%, and 20% for geo-location diversity, transaction success rate, and energy source, respectively, during the trust factor calculation. This is to ensure a balance between three factors, i.e., decentralisation, reliability, and sustainability, while ensuring that only the most trustworthy and distributed validators are allowed to participate during the validation process. The PoF mechanism gives a higher and equal weight compared to the energy source factor to enhance decentralisation and reliability, because too much emphasis on geo-location for diversity might lead to selecting less reliable validators. It will also ensure that it does not overpower decentralisation because a validator with a perfect success rate but from a centralised region could pose a decentralisation risk. While sustainability is essential, the primary goals of blockchain are security, decentralisation, and efficiency. So, if energy sources were weighted equally or higher, it might prioritise eco-friendly validators who lack sufficient trust or decentralisation, impacting on overall network reliability. Thus, a weighting distribution of 40% (geo-location), 40% (transaction success rate), and 20% (energy source), rather than weighting them equally for the trust factor evaluation of a validating node, is recommended.

4. Analysis and Discussion

This section will cover the discussion and analysis pertaining to the features used in the Proof-of-Friendship mechanism based on the geo-location, the success rate of a transaction, and the type of fuel used in the validation process.

4.1. Harvesting the Benefit of Proof-of-Friendship Mechanism

It is vital to understand the importance of the geo-location of the validators. It does not mean compromising the location with precision, but rather it means, e.g., knowing the region in terms of, say, the city, country, continent, part of the globe, etc. As discussed in an earlier section, choosing validators for a blockchain network from different regions of the world has several significant positive impacts. These impacts span technical, social, economic, and political dimensions. It may increase network delay, but trust, availability, and scalability are some of the factors that contribute positively to the sustainability of the blockchain network in addition to the following areas:

- (a) **Increased Decentralisation:** Selecting validators from diverse regions reduces the risk of centralisation, as no single country or region can dominate the network. Decentralisation enhances security by making it harder for attackers to coordinate attacks across geographically dispersed nodes.
- (b) **Enhanced Resilience:** Geographic diversity improves network reliability and fault tolerance. Regional validators ensure the network continues to function even if one region experiences downtime due to natural disasters, technical failures, or regulatory actions.
- (c) **Cultural and Socio-Political Trust:** Validators from diverse regions may gain the trust of local transactors who are more comfortable interacting with representatives from their area. This inclusion reduces scepticism or resistance in regions with less familiarity or trust in foreign governance. It is also interesting to note that if two rival countries agree on the same transaction, it is more trustable than two partnering allies agreeing on the same transaction validity.
- (d) **Global Economic Participation:** Spreading validator roles across regions allows stakeholders worldwide to benefit economically from participating in the blockchain net-

work. It fosters inclusivity, allowing smaller or developing economies to engage in and profit from blockchain technology.

- (e) **Regulatory Compliance and Adaptability:** Distributed validators can better navigate region-specific regulations and compliance requirements. Local validators are familiar with their jurisdiction's legal frameworks, reducing the risk of unintentional violations.

The transaction success rate of the past is vital in trusting the validator's future successful transactions and maintaining a trustful distributed network. The successful validation of transactions not only saves on gas fees due to network failure but also brings lots of advantages to the validating nodes as discussed below:

- (a) **Network Reliability and Efficiency:** Validators with a high transaction success rate contribute to the smooth operation of the network by consistently processing and validating transactions without errors or delays. A low success rate could lead to failed or delayed transactions, undermining user trust and the network's reliability.
- (b) **Maintaining Consensus Integrity:** Validators are responsible for ensuring that only valid transactions are added to the blockchain. A low success rate could indicate poor validation practices, risking the inclusion of invalid or fraudulent transactions, wasting of network computation energy, and loss of gas fees. High success rates ensure that the network reaches consensus efficiently and securely.
- (c) **User Trust and Confidence:** Users expect their transactions to be processed promptly and correctly. Validators with a high success rate build confidence in the network's ability to handle transactions reliably. Repeated transaction failures can drive users away and damage the network's reputation.
- (d) **Resource Optimisation:** Each failed transaction consumes network resources like bandwidth, computation, and storage without contributing to meaningful progress. High success rates reduce resource wastage, ensuring the blockchain network operates cost-effectively. This will allow validators with higher success rates to be given equal opportunity across different regions to earn rewards consistently, aligning their interests with the network's overall health.
- (e) **Fairness in Validator Selection:** Networks that consider transaction success rates when selecting validators can ensure that only competent and reliable validators participate. This reduces the risk of disruptions caused by underperforming or malicious validators.
- (f) **Protection Against Malicious Activity:** Validators with low success rates might be engaging in malicious activities, such as double-spending or spamming the network. Monitoring and prioritising high success rates help safeguard the network against such threats.
- (g) **Scalability and Growth:** As blockchain networks grow and handle more transactions, maintaining high success rates becomes critical for scalability. Validators with consistent performance ensure that the network can manage increased traffic without compromising transaction finality or speed.

Lastly, the induction of eco-friendly energy sources as a factor and the geolocation and trust of the validators in the consensus process will make the network sustainable, scalable, and more acceptable and adaptable. Other benefits include the following:

- (a) **Environmental Benefits:** Validation using renewable energy sources like solar, wind, and hydropower significantly reduces greenhouse gas emissions compared to fossil fuels. This aligns blockchain operations with global efforts to combat climate change. Renewable energy is inexhaustible compared to finite resources like coal and oil, ensuring a long-term energy supply for blockchain networks.

- (b) **Cost Savings:** Renewable energy sources, especially solar and wind, have decreasing costs over time due to advancements in technology and economies of scale. Once the infrastructure is established, the ongoing energy costs are significantly lower than those relating to fossil fuels. Moreover, renewable energy is less susceptible to price volatility than fossil fuels, providing predictable costs for blockchain operations.
- (c) **Regulatory and Social Acceptance:** Many governments are introducing stricter environmental policies. Using renewable energy helps blockchain miners comply with these regulations and avoid penalties. As blockchains often face criticism for their high energy consumption, adopting renewable energy demonstrates a commitment to sustainability, thus enhancing trust and reputation.
- (d) **Decentralisation and Accessibility:** Renewable energy enables mining and validation in remote or underdeveloped areas with abundant natural resources (e.g., solar energy in deserts, wind in coastal areas). This promotes decentralisation, a core principle of blockchain technology. By relying on locally available renewable energy, miners reduce the dependency on centralised power grids and external energy providers.
- (e) **Enhanced Network Resilience:** Using renewables reduces the reliance on traditional power grids, which may be subject to outages or geopolitical risks. A distributed network of renewable-powered nodes increases the robustness of blockchain operations. Renewable energy systems can be integrated with microgrids, ensuring a continuous energy supply even during larger grid failures.
- (f) **Long-Term Viability:** As blockchain adoption grows, energy demands will increase. Renewable energy ensures that this growth does not come at the expense of environmental degradation. Companies and organisations utilising blockchain can meet Environmental, Social, and Governance (ESG) goals by adopting renewable energy, making their solutions more attractive to investors and customers.
- (g) **Technological and Economic Innovation:** The demand for renewable energy from blockchain miners can drive investment in renewable energy infrastructure and innovation. Blockchain networks powered by renewables appeal to environmentally aware users, developers, and investors. Moving to renewable energy mitigates risks associated with the future scarcity of fossil fuels and potential regulatory crackdowns on energy-intensive operations.

4.2. Addressing Security Issues Using Proof of Friendship

Moreover, in regard to the contribution of security solutions offered by Proof of Friendship, the proposed consensus tackles the following security issues highlighted in the literature review:

- (a) **Node spoofing:** Malicious nodes, on the lower end of the scale, can target transactors and purposefully fail transactions. They enable Sybil and Eclipse attacks. Since Proof of Friendship requires a background check with its users—at least to verify their location, transaction success rate and energy source—there is a higher chance that the nodes are genuine. The mechanism removes validators that have lower trust values. Even if the IP of the node is spoofed, it will be very challenging to spoof the location using VPN, and attempt to meet the required minimum transaction success rate using VPN.
- (b) **Pool hopping/Block withholding/FAW:** These are attacks limited to the Proof-of-Work mechanism. Proof of Friendship does not utilise mining pools, or even miners. So, such an attack will not be possible in the PoF consensus mechanism.
- (c) **Frontrunning:** Since Proof-of-Friendship blockchains will not use mempools, and transactions are processed much more rapidly than in an average Proof-of-Work network, there is no current potential for insider information. Removing the primary

component for a frontrunning operation leaves no room for the operation to take place. Keeping this mechanism open-source will facilitate community improvements to further prevent frontrunning.

- (d) Politically charged transaction manipulation: Proof of Friendship takes into account geo-location and allows users to select validators from the different regions. If a transaction has any reason to suspect that their transaction might be targeted, they have an option to choose a trusted validator from their personalised list of validators, who have previously validated one of their transactions. This will not allow validators from one region to dominate or monopolise the process.
- (e) Attack minimisation: The level of decentralisation is very high, due to the consideration of geo-location as one of the key factors to select validators, so it will be very challenging to coordinate among nodes to perform attack and network manipulation. If any manipulation-related actions are visible, then the trust value of the node will be affected due to the consideration of the transaction success rate as one of the factors for validator selection, so a coordinated attack is highly unlikely. Moreover, the reliability of the transaction validation is higher when nodes from different regions agree and maintain the network integrity and security.

Overall, since validators with the highest number of successful transactions are promoted, there is an increased reliability factor. This is complemented by the fact that validators with lower trust values are booted from the network. When the aspect of geo-location is taken into the validator selection, it may sound like centralising the network, but in reality, it improves the level of decentralisation over the network distribution. One of the biggest challenges will be the methods of determining the energy source used by the validators; at this point, it is assumed that the participating validators made a disclosure, but it will be challenging to trust unless a third party verifies the claim.

4.3. Possible Attack Scenario of PoF: Geo-Location Spoofing and Validator Control

An attacker may want to gain disproportionate control over the validator selection process. By doing so, they can manipulate transactions, delay confirmations, or even attempt a censorship attack by selectively approving or rejecting transactions. The process involves three distinct steps, as shown in Figure 4 (below).

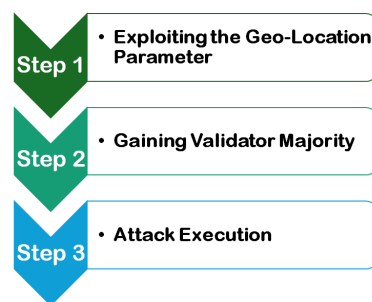


Figure 4. Possible attack scenario: geo-location spoofing and validator control.

Step 1: Exploiting the Geo-Location Parameter: Since the PoF mechanism requires 51% of validators to be from different regions, the attacker exploits this rule by creating multiple fake validator nodes that appear to be from different geographic locations. They do this by using the following methods:

- (a) VPNs and Proxies: The attacker configures their nodes to appear as if they originate from different countries by using VPNs or proxy services.
- (b) Satellite Internet Providers: The attacker registers nodes under different ISPs that provide global coverage, making their location seem diverse.

- (c) Fake Regional Registrations: The attacker leases cloud servers in various countries and registers validators from those regions.

Step 2: Gaining Validator Majority: Once the attacker has manipulated the geo-location factor, they ensure their fake validators meet the rest of the validator's parameters to take part in the validation process.

- (a) High Transaction Success Rates: The node can execute low-risk transactions (e.g., sender and receiver belonging to the same entity, smart contract interactions that do not require external validation, etc.), and they can attempt to artificially boost their success rate to meet the 90% success rate requirement. In the future, this aspect will be further mitigated to avoid such scenarios. In the PoF mechanism, it is assumed that any successful transactions are part of the commutative successful transaction rates irrespective of being low-risk transactions or not.
- (b) Green Energy Certification Spoofing: If the blockchain uses weakly verified energy sources from a third party, the attacker can falsely claim to use green energy to maximise selection probability. In the PoF mechanism, we assume that a trusted third party has verified the energy sources, and their reports are considered accurate. However, in reality, globally secure energy-source-verifying agents are required to correctly identify and verify the energy sources, but that challenge is not addressed in this paper.

By achieving all three factors (geo-location diversity, high success rate, and green energy compliance), the attacker's validators dominate the selection process.

Step 3: Attack Execution: If the majority of the validators are under the attacker's control, they may be able to conduct transaction censorship by selectively approving or rejecting transactions from certain users or addresses. They can intentionally slow down transaction processing, and they degrade the network's performance. The validators may appear to be from multiple countries to manipulate regulations but are secretly controlled by one entity, and if that happens, then regulators may struggle to enforce compliance rules effectively.

Example: Suppose the blockchain has 1000 potential validators, but 10 are selected for each round. The blockchain enforces that at least 51% of selected validators come from different regions (i.e., six different regions). The attacker deploys 50 validator nodes across 10 different cloud providers, disguising their locations via VPNs. The attacker ensures all nodes maintain at least a 90% success rate through automated transactions and fake green energy compliance is successfully declared for all nodes. Then, out of the 10 selected validators, let us suppose 7 belong to the attacker, but they appear to be from different locations, thus by-passing the geo-location diversity rule; then, the remaining 3 honest validators have no control over consensus decisions. If that is the case, the attacker can reject transactions from a competitor while approving only their transactions. They may even be able to execute double-spending by reorganising transaction history and delaying transactions from specific regions or users, causing disruptions.

So, relying on geo-location checks using IP may not be reliable if the transaction success rates and the green energy sources are compromised. However, compromising all three factors will be challenging because spoofing geo-location through, e.g., a VPN will lead to network congestion and will slow down the throughput, while successfully verifying the green energy source means that the region and the nodes are directly captured. So, compromising a PoF network is a possibility like in any other consensus mechanism, but will be a daunting task if all three factors are accurate and reliable. However, making the trust scoring system dynamic instead of a fixed-weighted system among the three factors (i.e., geo-location, successful transaction rate, and energy source) might be a better

option, e.g., introducing penalties for suspicious behaviour (e.g., unusual geo-location change, identical IP ranges, repeated patterns).

4.4. Example Discussion with Simulation Results

The simulation platform and the systems hardware characteristics of each validator are as follows: CPU: 3 GHz; memory: 16 GB; storage: 1 TB; average network speed: 50 Mbps; energy consumption: (idle: 50 W; active: 100 W). In the test lab: validators selected: $N_{\text{selected}} = 10$; validators operate simultaneously. It is assumed that the block size is around 1 MB, the block creation time is 10 minutes (every 10 min, a set of successful transactions are combined to create a block), and the theoretically expected number of transactions per block is 2000 (average transaction size: 500 bytes).

The system is simulated with 10 possible validators using the above system configurations. The geo-location (G_i), success rate (R_i), and energy source (E_i) in Equation (2) and values of Table 4 are used, and the weights of 40%, 40%, and 20%, respectively, are considered. Do note that the energy sources of a validator could be a mixture of sources; in that regard, Equation (1) is used to calculate the energy source’s probability. However, in Table 4, for simplicity, only one type of energy source is considered for each validator. In reality, it will be challenging to also collect the respective weights of the energy sources. Table 5 shows the trust ranking of the validators based on the blockchain parameters of PoF from Table 4.

Table 4. Validators’ geo-location, success rate, and energy sources.

Validator	Geo-Location (G_i)	Success Rate (S_i)	Energy Source (E_i)
1	1 (Unique)	0.99	1.0 (Green)
2	1 (Unique)	0.95	0.5 (Biofuel)
3	0 (Common)	0.98	0.5 (Biofuel)
4	1 (Unique)	0.97	0.0 (Non-renewable)
5	0 (Common)	0.96	1.0 (Green)
6	1 (Unique)	0.99	1.0 (Green)
7	1 (Unique)	0.94	0.0 (Non-renewable)
8	0 (Common)	0.93	0.5 (Biofuel)
9	1 (Unique)	0.98	1.0 (Green)
10	0 (Common)	0.92	0.75 (Nuclear)

Table 5. Ranking the validators using the trust value.

Validator	G_i	S_i	E_i	T_i	Rank
1	1	0.99	1.0	0.996	1st
2	1	0.95	0.5	0.88	3rd
3	0	0.98	0.5	0.492	-
4	1	0.97	0.0	0.788	4th
5	0	0.96	1.0	0.584	-
6	1	0.99	1.0	0.996	1st
7	1	0.94	0.0	0.776	5th
8	0	0.93	0.5	0.472	-
9	1	0.98	1.0	0.992	2nd
10	0	0.92	0.75	0.518	-

Thus, the proposed trust factor equation ensures a balanced selection favouring geo-diversity, high success rates, and renewable energy usage.

System and Network Performance: In this test, a block is created after every 10 min. This is performed to systematically store the transactions in groups in the form of a chain of blocks. During the block creation, all the successful transactions within a time frame of 10 min are combined to create a block. The system and blockchain network are tested using the RSA 2048 bit key for the certificate, digital signature, and AES-256 bit session key exchange. SHA 256 is used for hashing and data integrity checks. The average network performance is given below in Table 6. To estimate the cumulative average delay per block, three factors are taken into account, i.e., processing latency, network latency, and validators synchronisation delays. It means that for a larger validator population, the cumulative delay per block will be much higher since the validator synchronisation delay is the biggest contributor in the total delays created in the network to reach consensus across the distributed peer-to-peer network of the blockchain system. The theoretical average number of successful transactions per block is 2000 when each transaction size is 500 bytes and the block size is 1 MB; however, the simulation result shows that only an average of 291 transactions are in each block; i.e., $(10 \times 60 \times 1000)/2059 = 291$, where 2059 ms is the average cumulative delay per transaction. Thus, the delays are mainly caused by the network latency and the synchronisation process among the validators. It means that the higher the number of node participations in the validation process, the higher the transaction time, leading to a smaller number of transactions per block. It means that the number of transactions within the block is dynamic (changes depending on the number of participating validators and the network size).

Table 6. System and network performance of Proof-of-Friendship consensus mechanism.

Metrics	Values
Processing latency (PL)	85 ms
Network latency (NL) [transaction size/network speed]	172 ms
Synchronisation delays (SDs)	1802 ms
Cumulative delay per transaction [PL + NL + SD]	2059 ms

4.5. Comparison of Proof of Friendship (PoF) with PoW and PoS

The Proof-of-Friendship (PoF) consensus mechanism introduces a novel approach by incorporating a multi-factor validator selection process. Below is a comparison of PoF with traditional mechanisms, Proof of Work (PoW) and Proof of Stake (PoS), across some of the key consensus aspects as shown in Table 7:

Table 7. Comparison of PoF with PoW and PoS.

Criteria	Proof of Work (PoW)	Proof of Stake (PoS)	Proof of Friendship (PoF)
Selection Basis	Computational power	Cryptocurrency stake	Geo-location, transaction success rate, and energy source
Decentralisation	High initially, but centralisation occurs due to mining pools	Tends to favour wealthy participants, leading to validator monopoly	Promotes decentralisation by selecting validators from diverse locations
Energy Efficiency	Very low (high energy consumption)	Moderate (no mining, but requires computational power for staking mechanisms)	Moderate (energy consumption by relying on green energy and trust)

Table 7. Cont.

Criteria	Proof of Work (PoW)	Proof of Stake (PoS)	Proof of Friendship (PoF)
Security	High (resistant to attacks due to computational difficulty)	Moderate (51% stake attack possible, leading to network control)	High (Sybil-resistant via social trust validation through multifactor association and reducing fake identities)
Scalability	Low (slow transaction processing due to mining complexity)	High (faster than PoW, but can face congestion in high-demand networks)	High (trust-based validation allows efficient and fast transaction processing)
Trust Factor	No inherent trust factor relies purely on computational power	Trust is based on financial investment, not actual reliability	Trust is based on network diversity, past transaction success, and sustainability efforts
Attack Resistance	Vulnerable to 51% hash power attacks	Vulnerable to 51% stake attacks and centralisation risks	Resists Sybil
Environmental Impact	High carbon footprint due to mining	Moderate (energy consumption varies based on staking mechanisms)	Low (rewards validators using renewable energy sources)
Fairness	Favours miners with expensive hardware	Favours wealthy individuals with large crypto holdings	Promotes fairness by selecting validators based on the node's location, success rates, and sustainability

PoF addresses the centralisation issues in PoW and PoS by ensuring validators are selected from diverse locations and trusted networks rather than those with the most computational power or financial resources. It significantly reduces energy consumption compared to PoW, making it a sustainable blockchain consensus model. It also enhances security by leveraging trust relationships, making it harder for attackers to manipulate the system with fake identities or financial monopolies. Lastly, it is Sybil-resistant, unlike PoS, which can be manipulated by wealthy stakeholders, or PoW, which is dominated by mining pools.

5. Limitations and Future Directions

Limitations of PoF and its future direction: The following limitations open areas to explore for future work and for further investigation:

1. **Trust Manipulation:** Malicious actors could attempt to forge relationships or create fake trust connections to manipulate the system by IP spoofing using, e.g., a VPN.
2. **Network Bootstrapping and Adoption Hurdles:** PoF requires an established trust graph to function effectively, making initial adoption difficult in new or small networks. A mechanism for verifying new participants without excessive centralisation needs further refinement.
3. **Scalability of Trust-Based Consensus:** PoF introduces additional computational overhead in validating trust relationships, which may become computationally expensive in large-scale networks. Efficient algorithms for real-time trust verification need further development.
4. **Privacy Concerns:** To verify friendships, regional information, transaction success rates, and energy sources are needed, leading to privacy risks unless the node's data are filtered appropriately to avoid any revelation of personal information. Ensuring zero-knowledge proofs (ZKPs) to verify trust without revealing the node's identity remains an open challenge.
5. **Need for Verification of Renewable Energy Sources:** Since verifying renewable energy usage in blockchain networks often depends on external certifiers, ensuring long-term

trustworthiness requires a dynamic, automated, and tamper-resistant verification mechanism. So, the PoF system can continuously verify and update renewable energy certifications for validators in real-world conditions by integration with Decentralised Energy Tracking Systems: To avoid relying solely on third-party certifiers, PoF can integrate with blockchain-based energy tracking systems, e.g., Energy Attribute Certificates (EACs), referred to as Guarantees of Origin (GO) in Europe [80]. Such a system can allow validators to register their energy source with an on-chain energy registry. It can also be linked with smart contracts to verify and store certificates or real-time energy consumption data, and then conduct periodic re-verification to check if validators are continuing to use renewable energy.

6. Conclusions

The Proof-of-Friendship blockchain consensus mechanism integrating geo-location, transaction success rate, and energy source as key parameters offers a robust and balanced approach to validator selection. By equally weighting these factors, the mechanism promotes trust, performance, and sustainability in the blockchain network. The use of geo-location enforces diversity in such a way that at least 51% of validators have to come from different regions, reducing the risk of centralisation and socio-political interference. This enhances the network's resilience and global inclusivity. Setting a minimum success rate threshold of 90% ensures validators are reliable and capable of handling transactions effectively. This criterion boosts the network's overall efficiency and user trust, allowing for minor exceptions due to technical failures. Moreover, prioritising green energy validators (100% weighting) over nuclear (75%) and biofuel users (50%) aligns the blockchain network with global sustainability goals. This approach minimises the environmental impact and encourages validators to adopt renewable energy solutions. Finally, by considering all three parameters, the mechanism avoids an over-reliance on any single factor, resulting in a fair and decentralised validator selection process. However, despite these benefits, the mechanism faces potential challenges, including maintaining validator diversity in underrepresented regions, managing nodes that might use a VPN, addressing technical barriers to achieving high success rates, and ensuring accessibility to renewable energy resources globally. But this consensus mechanism strikes a balance between trust, performance, and environmental responsibility, making it a promising model for modern blockchain networks seeking to ensure fairness, efficiency, and sustainability.

Author Contributions: Conceptualisation, J.M., R.S. and S.K.; methodology, J.M., R.S. and S.K.; software, J.M. and R.S.; validation, J.M., R.S. and S.K.; formal analysis, J.M., R.S. and S.K.; investigation, J.M., R.S. and S.K.; resources, J.M., R.S. and S.K.; data curation, J.M., R.S. and S.K.; writing—original draft preparation, J.M. and R.S.; writing—review and editing, J.M., R.S., S.K. and I.K; visualisation, J.M., R.S., S.K. and I.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The experimental data and its findings are reported in this paper. If more detail raw data are required then it will be made available on request. For the purpose of open access, the author has applied a Creative Commons Attribution (CC BY) licence to any Author Accepted Manuscript version arising from this submission.

Acknowledgments: We would like to thank the Sheffield Hallam University, School of Computing and Digital Technologies for providing the lab resources for network testing. I would also like to thank Wungramthem Albert Marchang for proofreading this work.

Conflicts of Interest: Author Rengaprasad Srikanth was employed by the company Supply Chain Security, BT Group. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Pilkington, M. Blockchain technology: Principles and applications. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016; pp. 225–253.
2. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
3. Efanov, D.; Roschin, P. The all-pervasiveness of blockchain technology. *Procedia Comput. Sci.* **2018**, *123*, 116–121. [CrossRef]
4. Lashkari, B.; Musilek, P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [CrossRef]
5. Xie, M.; Liu, J.; Chen, S.; Lin, M. A survey on blockchain consensus mechanism: Research overview, current advances and future directions. *Int. J. Intell. Comput. Cybern.* **2023**, *16*, 314–340. [CrossRef]
6. Zhang, C.; Wu, C.; Wang, X. Overview of blockchain consensus mechanism. In Proceedings of the 2020 2nd International Conference on Big Data Engineering, Shanghai China, 29–31 May 2020; pp. 7–12.
7. Nguyen, G.T.; Kim, K. A survey about consensus algorithms used in blockchain. *J. Inf. Process. Syst.* **2018**, *14*, 101–128.
8. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 10 January 2025).
9. Buterin, V. Ethereum white paper. *GitHub Repos.* **2013**, *1*, 22–23.
10. Rajavat, A.; Bhardwaj, V.; Kaur, N.; Rawat, R.; Rawat, A.; Jadon, G.S. Sustainable Futures: Navigating Blockchain's Energy Dilemma. In *Online Social Networks in Business Frameworks*; John Wiley & Sons: Hoboken, NJ, USA, 2024; pp. 85–112.
11. Taherdoost, H. Blockchain Integration and Its Impact on Renewable Energy. *Computers* **2024**, *13*, 107. [CrossRef]
12. Khosravi, A.; Säämäki, F. Beyond Bitcoin: Evaluating Energy Consumption and Environmental Impact across Cryptocurrency Projects. *Energies* **2023**, *16*, 6610. [CrossRef]
13. Kohli, V.; Chakravarty, S.; Chamola, V.; Sangwan, K.S.; Zeadally, S. An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions. *Digit. Commun. Netw.* **2023**, *9*, 79–89. [CrossRef]
14. Udeh, E.O.; Amajuoyi, P.; Adeusi, K.B.; Scott, A.O. Blockchain-driven communication in banking: Enhancing transparency and trust with distributed ledger technology. *Financ. Account. Res. J.* **2024**, *6*, 851–867.
15. Lal, R.; Chhabra, A.; Singla, S.; Sharma, D. Blockchain Technology: Revolutionizing Trust, Transparency, and Transaction Efficiency. In Proceedings of the 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Chikkaballapur, India, 23–24 April 2024; Volume 1, pp. 1–5.
16. Udeh, E.O.; Amajuoyi, P.; Adeusi, K.B.; Scott, A.O. The role of Blockchain technology in enhancing transparency and trust in green finance markets. *Financ. Account. Res. J.* **2024**, *6*, 825–850.
17. Ali, V.; Norman, A.A.; Azzuhri, S.R.B. Characteristics of blockchain and its relationship with trust. *IEEE Access* **2023**, *11*, 15364–15374. [CrossRef]
18. Rijal, S.; Saranani, F. The Role of Blockchain Technology in Increasing Economic Transparency and Public Trust. *Technol. Soc. Perspect. (TACIT)* **2023**, *1*, 56–67. [CrossRef]
19. Cambridge Blockchain Network Sustainability Index. Bitcoin Power Consumption. Available online: <https://ccaf.io/cbnsi/cbeci> (accessed on 31 December 2024).
20. Cambridge Blockchain Network Sustainability Index. Ethereum Power Consumption. Available online: <https://ccaf.io/cbnsi/ethereum> (accessed on 31 December 2024).
21. Ethereum. Proof-of-Stake (PoS). 2022. Available online: <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> (accessed on 23 August 2024).
22. Aponte-Novoa, F.A.; Orozco, A.L.S.; Villanueva-Polanco, R.; Wightman, P. The 51% attack on blockchains: A mining behavior study. *IEEE Access* **2021**, *9*, 140549–140564. [CrossRef]
23. Vashchuk, O.; Shuwar, R. Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake. *Electron. Inf. Technol.* **2018**, *9*, 106–112. [CrossRef]
24. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11–14 December 2017; pp. 557–564.
25. Chainspect. What Is Block Time? [Definition & Real Metrics]. Chainspect. 2024. Available online: <https://chainspect.app/blog/block-time> (accessed on 19 February 2025).
26. Crypto.com. ConfirmationTime. Crypto.com. Available online: <https://crypto.com/glossary/confirmation-time> (accessed on 19 February 2025).
27. Gorenflo, C.; Lee, S.; Golab, L.; Keshav, S. FastFabric: Scaling hyperledger fabric to 20 000 transactions per second. *Int. J. Netw. Manag.* **2020**, *30*, e2099. [CrossRef]
28. Bitstamp. What Is Block Size? 2024. Available online: <https://www.bitstamp.net/en-gb/learn/crypto-101/what-is-block-size/> (accessed on 19 February 2025).

29. Tardi, C.; Mansa, J.; Jackson, A. Gwei. 2022. Available online: <https://www.investopedia.com/terms/g/gwei-ethereum.asp> (accessed on 14 August 2024).
30. Coinbase. What Is Hash Rate? Available online: <https://www.coinbase.com/en-gb/learn/crypto-glossary/what-is-hash-rate> (accessed on 19 February 2025).
31. Centieiro, H. Bitcoin Proof of Work—The Only Article You Will Ever Have to Read. 2021. Available online: <https://levelup.gitconnected.com/bitcoin-proof-of-work-the-only-article-you-will-ever-have-to-read-4a1fcd76a294> (accessed on 23 July 2024).
32. Aggelos Kiayias, G.P. Speed-Security Tradeoffs in Blockchain Protocols. *Cryptol. ePrint Arch.* **2015**. Available online: <https://eprint.iacr.org/2015/1019> (accessed on 10 January 2025).
33. Bączkowski, A. Fundamentals: TPS vs. Latency vs. Finality. 2022. Available online: <https://alephzero.org/blog/tps-latency-finality/> (accessed on 20 July 2024).
34. Catt, M. Blockchain Fundamentals: Latency & Capacity—Featuring the Ark Ecosystem. 2018. Available online: <https://medium.com/ku-blockchain-institute/blockchain-fundamentals-featuring-the-ark-ecosystem-part-1-af1f9052e579> (accessed on 20 July 2022).
35. Edwood, F. Block Size and Scalability, Explained. 2020. Available online: <https://cointelegraph.com/explained/block-size-and-scalability-explained> (accessed on 20 July 2024).
36. Alameda, T. Zero Knowledge Proof: How to Maintain Privacy in a Data-Based World. 2020. Available online: <https://www.bbva.com/en/zero-knowledge-proof-how-to-maintain-privacy-in-a-data-based-world/> (accessed on 2 August 2022).
37. Chainlink. What Is a Blockchain Oracle? 2021. Available online: <https://chain.link/education/blockchain-oracles> (accessed on 11 August 2024).
38. Sharma, T.K. Blockchain Oracle: A Deep Dive. 2022. Available online: <https://www.blockchain-council.org/blockchain/blockchain-oracle-a-deep-dive/> (accessed on 12 June 2024).
39. Chen, Y.; Chen, H.; Zhang, Y.; Han, M.; Siddula, M.; Cai, Z. A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High-Confid. Comput.* **2022**, *2*, 100048. [CrossRef]
40. Ethereum. Smart Contract Security. 2021. Available online: <https://ethereum.org/en/developers/docs/smart-contracts/security/#attacks-and-vulnerabilities> (accessed on 2 August 2024).
41. Marshall, B. Beginner’s Guide to an MEV Bot: Creating an Arbitrage Bot on Ethereum Mainnet. 2022. Available online: <https://www.blocknative.com/blog/mev-and-creating-a-basic-arbitrage-bot-on-ethereum-mainnet> (accessed on 12 August 2024).
42. Craig, T. MEV and Proof-of-Stake with Eden Network’s Caleb Sheridan. 2021. Available online: <https://cryptobriefing.com/mev-and-proof-of-stake-with-eden-networks-caleb-sheridan/> (accessed on 12 August 2024).
43. Radix DLT. What are Proof of Work and Proof of Stake? 2021. Available online: <https://learn.radixdlt.com/article/what-are-proof-of-work-and-proof-of-stake> (accessed on 12 August 2024).
44. Cryptopedia. Eclipse Attacks: Explanations and Preventions. 2022. Available online: <https://www.gemini.com/cryptopedia/eclipse-attacks-defense-bitcoin> (accessed on 12 August 2022).
45. Frankenfield, J. Selfish Mining. 2022. Available online: <https://www.investopedia.com/terms/s/selfish-mining.asp> (accessed on 1 July 2024).
46. Sriman, B.; Ganesh Kumar, S.; Shamili, P. Blockchain technology: Consensus protocol proof of work and proof of stake. In *Intelligent Computing and Applications: Proceedings of ICICA 2019*; Springer: Singapore, 2021; pp. 395–406.
47. Raikwar, M.; Gligoroski, D. Dos attacks on blockchain ecosystem. In *Proceedings of the European Conference on Parallel Processing*, Lisbon, Portugal, 1–3 September 2021; Springer International Publishing: Cham, Switzerland, 2021; pp. 230–242.
48. Singh, N.; Singh, H.P.; Mishra, A.; Khare, A.; Swarnkar, M.; Almas, S.K. Blockchain Cloud Computing: Comparative study on DDoS, MITM and SQL Injection Attack. In *Proceedings of the 2024 IEEE International Conference on Big Data & Machine Learning (ICBDML)*, Bhopal, India, 24–25 February 2024; pp. 73–78.
49. Kumar, A.; Sah, B.K.; Mehrotra, T.; Rajput, G.K. A review on double spending problem in blockchain. In *Proceedings of the 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, Noida, India, 28–30 April 2023; pp. 881–889.
50. Caldarelli, G.; Ellul, J. The blockchain oracle problem in decentralized finance—A multivocal approach. *Appl. Sci.* **2021**, *11*, 7572. [CrossRef]
51. Rodler, M.; Li, W.; Karame, G.O.; Davi, L. Sereum: Protecting existing smart contracts against re-entrancy attacks. *arXiv* **2018**, arXiv:1812.05934.
52. Aggarwal, S.; Kumar, N. Attacks on blockchain. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 399–410.
53. Rehman, Z.; Gregory, M.A.; Gondal, I.; D’Ong, H.; Ge, M. Eclipse Attacks in Blockchain Networks: Detection, Prevention, and Future Directions. *IEEE Access* **2025**, *13*, 25918–25933. [CrossRef]

54. Alangot, B.; Reijnsbergen, D.; Venugopalan, S.; Szalachowski, P.; Yeo, K.S. Decentralized and lightweight approach to detect eclipse attacks on proof of work blockchains. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1659–1672. [CrossRef]
55. Crypto News. Hope, C. *Solana Network Faces High Failure Rate in Transactions Amid Memecoin Mania*. 2024. Available online: <https://coinmarketcap.com/academy/article/solana-network-faces-high-failure-rate-in-transactions-amid-memecoin-mania> (accessed on 19 February 2025).
56. Singh, S.K.; Salim, M.M.; Cho, M.; Cha, J.; Pan, Y.; Park, J.H. Smart contract-based pool hopping attack prevention for blockchain networks. *Symmetry* **2019**, *11*, 941. [CrossRef]
57. Chen, H.; Chen, Y.; Xiong, Z.; Han, M.; He, Z.; Liu, B.; Wang, Z.; Ma, Z. Prevention method of block withholding attack based on miners' mining behavior in blockchain. *Appl. Intell.* **2023**, *53*, 9878–9896. [CrossRef]
58. Eskandari, S.; Moosavi, S.; Clark, J. Sok: Transparent dishonesty: Front-running attacks on blockchain. In *Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 170–189.
59. Manolache, M.A.; Manolache, S.; Tapus, N. Decision making using the blockchain proof of authority consensus. *Procedia Comput. Sci.* **2022**, *199*, 580–588. [CrossRef]
60. Wang, Q.; Xu, M.; Li, X.; Qian, H. Revisiting the Fairness and Randomness of Delegated Proof of Stake Consensus Algorithm. In Proceedings of the 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCLOUD/SocialCom/SustainCom), Exeter, UK, 17–19 December 2020; pp. 305–312. [CrossRef]
61. Andrey, A.; Petr, C. Review of existing consensus algorithms blockchain. In Proceedings of the 2019 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 23–27 September 2019; pp. 124–127.
62. Karantias, K.; Kiayias, A.; Zindros, D. Proof-of-Burn. In *Financial Cryptography and Data Security. FC 2020*; Lecture Notes in Computer Science; Bonneau, J., Heninger, N., Eds.; Springer: Cham, Switzerland, 2020; Volume 12059. [CrossRef]
63. Cedricwalter/Blockchain-Consensus. Available online: <https://github.com/cedricwalter/blockchain-consensus/blob/master/chain-based-proof-of-capacity-space/proof-of-capacity-poc.md> (accessed on 24 December 2024).
64. Chen, L.; Xu, L.; Shah, N.; Gao, Z.; Lu, Y.; Shi, W. On security analysis of proof-of-elapsed-time (PoET). In *Stabilization, Safety, and Security of Distributed Systems*; Spirakis, P., Tsigas, P., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 282–297. [CrossRef]
65. Frankenfield, J. Proof of Elapsed Time (PoET). 2022. Available online: <https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp> (accessed on 22 June 2024).
66. Moran, T.; Orlov, I. Simple Proofs of Space-Time and Rational Proofs of Storage. In *Advances in Cryptology—CRYPTO 2019. CRYPTO 2019*; Lecture Notes in Computer Science; Boldyreva, A., Micciancio, D., Eds.; Springer: Cham, Switzerland, 2019; Volume 11692. [CrossRef]
67. Xiao, B.; Jin, C.; Li, Z.; Zhu, B.; Li, X.; Wang, D. Proof of Importance: A Consensus Algorithm for Importance Based on Dynamic Authorization. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT '21), Melbourne, VIC, Australia, 14–17 December 2021; Association for Computing Machinery: New York, NY, USA, 2022; pp. 510–513. [CrossRef]
68. Zilberman, A.; Offer, A.; Pincu, B.; Glickshtein, Y.; Kant, R.; Brodt, O.; Otung, A.; Puzis, R.; Shabtai, A.; Elovici, Y. A Survey on Geolocation on the Internet. *IEEE Commun. Surv. Tutor.* **2024**. [CrossRef]
69. Hu, Z.; Heidemann, J.; Pradkin, Y. Towards geolocation of millions of IP addresses. In Proceedings of the 2012 Internet Measurement Conference, Boston, MA, USA, 14–16 November 2012; pp. 123–130.
70. Dan, O.; Parikh, V.; Davison, B.D. IP geolocation using traceroute location propagation and ip range location interpolation. In *Companion Proceedings of the Web Conference 2021*; Association for Computing Machinery: New York, NY, USA, 2021; pp. 332–338.
71. Dan, O.; Parikh, V.; Davison, B.D. IP geolocation through reverse DNS. *ACM Trans. Internet Technol. (TOIT)* **2021**, *22*, 1–29. [CrossRef]
72. Gawusu, S.; Zhang, X.; Ahmed, A.; Jamatutu, S.A.; Miensah, E.D.; Amadu, A.A.; Osei, F.A.J. Renewable energy sources from the perspective of blockchain integration: From theory to application. *Sustain. Energy Technol. Assess.* **2022**, *52*, 102108. [CrossRef]
73. Zhang, D.; Chen, X.H.; Lau, C.K.M.; Xu, B. Implications of cryptocurrency energy usage on climate change. *Technol. Forecast. Soc. Chang.* **2023**, *187*, 122219. [CrossRef]
74. Siddique, I.; Smith, E.; Siddique, A. Assessing the sustainability of bitcoin mining: Comparative review of renewable energy sources. *J. Altern. Renew. Energy Sources* **2023**, *10*, 10–46610. [CrossRef]
75. De Vries, A. Renewable energy will not solve bitcoin's sustainability problem. *Joule* **2019**, *3*, 893–898. [CrossRef]
76. Koemtzopoulos, D.; Zournatzidou, G.; Ragazou, K.; Sariannidis, N. Cryptocurrencies Transit to a Carbon Neutral Environment: From Fintech to Greentech Through Clean Energy and Eco-Efficiency Policies. *Energies* **2025**, *18*, 291. [CrossRef]

77. Vijayamohan Mankayarkarasi, B.; Ramalakshmi Murugan, A. Energy Transition Through Voluntary Carbon Credit System. In *Energy Sustainability*; American Society of Mechanical Engineers: New York, NY, USA, 2024; Volume 87899, p. V001T04A006.
78. Suryanarayana, A.; Rao, V. Embracing Blockchain Technologies for Sustainable Finance Through Carbon Credits and Renewable Energy Trading. *Educ. Adm. Theory Pract.* **2024**, *30*, 1151–1155. [[CrossRef](#)]
79. Richard, M.O. Carbon Credit Concept and Africa's Sustainable Development—An Empirical Review. 2024. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4823877 (accessed on 9 January 2025).
80. Holzapfel, P.K.; Bánk, J.; Bach, V.; Finkbeiner, M. Relevance of guarantees of origin for Europe's renewable energy targets. *Renew. Sustain. Energy Rev.* **2024**, *205*, 114850. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.