Journal of Network and Computer Applications 241 (2025) 104204

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Research paper

Fuzzychain: An equitable consensus mechanism for blockchain networks

Bruno Ramos-Cruz [a,*], Javier Andreu-Perez [a,b], Francisco J. Quesada-Real [a], Luis Martínez [a,c]

[a] Computer Science Department, University of Jaen, Jaen, Jaen, 23071, Spain
[b] Centre for Computational Intelligencer, School of Computer Science and Electronic Engineering, University of Essex, Colchester, United Kingdom
[c] Andalusian Research Institute in Data Science and Computational Intelligence, Jaen, Jaen, 23071, Spain

ARTICLE INFO

Keywords:
Fuzzychain
Fuzzy sets
Consensus algorithm
Blockchain
Distributed networks

ABSTRACT

Blockchain technology has become a trusted method for establishing secure and transparent transactions through a distributed, encrypted network. The operation of blockchain is governed by consensus algorithms, among which Proof of Stake (PoS) is popular yet has its drawbacks, notably the potential for centralising power in nodes with larger stakes or higher rewards. Our proposed novel solution, Fuzzychain, leverages fuzzy sets to define stake semantics, introducing a degree of softness in validator selection. This approach mitigates rigid threshold-based decision-making by allowing gradual transitions between stake levels, reducing sharp disparities among validators. By incorporating this enhanced stake evaluation, Fuzzychain promotes a more adaptive and distributed selection process, ensuring a fairer and more inclusive blockchain network. A thorough assessment of a real-time multi-agent blockchain system to examine validator selection and reduce inequality, promoting a more equitable distribution of stakes among validators compared to other consensus mechanisms. This fosters a more inclusive selection process and a more equitably distributed network.

1. Introduction

The transition to digital business models highlights a key challenge: establishing trust among stakeholders in a virtual environment. Several strategies, including using trusted third parties, digital signatures, distributed systems, and peer-to-peer networks Sankar et al. (2017), have been explored to address this issue. However, these methods have limitations, steering focus towards blockchain technology as a promising solution to build and maintain trust in digital transactions. Unlike conventional distributed systems, blockchain is a specialised decentralised system that offers various properties such as immutability, transparency, integrity, and privacy, among others.

Blockchain, a decentralised, secure, and peer-to-peer network, addresses the challenges of trust and secure transactions in digital ecosystems (Swan, 2015; Zheng et al., 2018; Pérez et al., 2022; Jahid et al., 2023). It links blocks through cryptographic mechanisms, each one containing transaction data among network participants or nodes. These transactions are recorded and formed into new blocks, then validated by specialised nodes like miners, validators, or delegates and added to the blockchain Panda et al. (2021). Blockchains are classified as either public (permissionless), allowing open access and participation, or private (permissioned), with restricted access (Xu et al., 2023a). However, hybrid and consortium blockchains combine features of both public and private models to balance transparency, control, and scalability.

Public blockchains, such as Bitcoin Pilkington (2016) and Ethereum (Ethereum, 2023a), stand out for their decentralised structure, offering transparency, security, and immutability, suitable for applications including smart contracts (Wang et al., 2019; Górski, 2024; Bartoletti et al., 2025). The decentralised nature of these systems requires *consensus algorithms* to maintain trust and proper network functioning. A consensus algorithm establishes rules for nodes in a distributed network to agree on the system's state. In blockchain, these algorithms are crucial for verifying and validating transaction blocks, ensuring network integrity and trust. Common consensus algorithms include Proof of Work (PoW) (Dwork and Naor, 1992; Back et al., 2002; Nakamoto, 2008), Proof of Stake (PoS) (Ethereum, 2023b), and Delegated Proof of Stake (DPoS) (Larimer, 2014; BitShares Documentation, 2018). The selection of an algorithm is influenced by security, scalability, energy efficiency, and desired decentralisation level in a blockchain network.

The widely recognised PoW algorithm selects miners by requiring nodes to solve complex mathematical puzzles and submit solutions swiftly. Solving these puzzles demands substantial computational power, with the node that successfully solves the puzzle being the

* Corresponding author.
E-mail addresses: brcruz@ujaen.es (B. Ramos-Cruz), j.andreu-perez@essex.ac.uk (J. Andreu-Perez), fqreal@ujaen.es (F.J. Quesada-Real), martin@ujaen.es (L. Martínez).

https://doi.org/10.1016/j.jnca.2025.104204
Received 21 March 2024; Received in revised form 22 February 2025; Accepted 27 April 2025
Available online 14 May 2025

first to gain the privilege of mining the next block. However, PoW exhibits a significant limitation, as it consistently favours nodes with the highest computational power, thus challenging the achievement of a truly decentralised and equitable system.

To address the shortcomings of PoW, the PoS consensus algorithm, as referenced in Saleh (2021), Nguyen et al. (2019), Maung Maung Thin et al. (2018), was introduced. PoS chooses validators based on their staked utility tokens, ensuring they do not manipulate the blockchain for personal gain. Validators confirm blocks and stake bets on them, with rewards proportional to their stakes. PoS operates on a staking-based incentive model. DPoS differs from PoS by having network users vote for delegates to validate blocks, enhancing democracy but potentially affecting decentralisation (Liu and Xu, 2021). While PoS and DPoS improve upon PoW by not requiring extensive hardware for block validation, they still face particular challenges.

One of the key limitations of PoS stems from the subjective and imprecise nature of stake values. While stake values are expressed numerically, their interpretation is influenced by human perception, resulting in inherent vagueness and uncertainty. For instance, if a group of individuals were surveyed about their perception of a monetary amount, whether in cryptocurrencies or traditional forms, they would provide a range of responses such as 'very low,' 'low,' 'moderate,' 'high,' or 'very high.' This diversity of responses underscores the intrinsic uncertainty and vagueness within human perception. Additionally, PoS confronts the challenge of nodes with higher stake values exerting undue control over the blockchain, echoing the centralisation issues of PoW. This power imbalance stifles the growth and participation of smaller stakeholders within the network.

Regardless of the limitations facing each consensus algorithm, there is one common challenge: diversification to choose miners, validators or delegates. Diversification is a crucial characteristic in the blockchain environment because it helps prevent the centralisation of power within the network. When a small group of entities controls the majority of mining or validation power, they can potentially manipulate the network for their own gain, violating the principles of decentralisation and trustlessness that are key to blockchain technology. From a security standpoint, a diverse set of miners, validators, or delegates enhances the network's resilience to attacks. By diversifying the selection of miners or validators, consensus algorithms make it more challenging for attackers to amass enough influence to execute attacks, such as the Sybil attack (Chen et al., 2022), successfully. Furthermore, a diverse set of participants in the validation process brings different perspectives and transparency, leading to a more dynamic and resilient ecosystem.

In response to these identified limitations, we propose an innovative blockchain protocol named Fuzzychain. Fuzzychain introduces a novel concept by incorporating Fuzzy Sets (FSs) theory to represent stake values, thereby introducing a degree of fuzziness into stake-based consensus mechanisms. This pioneering approach aims to enhance the equity and security of blockchain networks. By incorporating FSs, Fuzzychain offers validators with diverse stake amounts more opportunities for periodic selection, fostering a **more inclusive and equitable system**. This unique contribution aims to mitigate the challenges associated with the imprecise nature of stake values in traditional PoS consensus algorithms, ultimately promoting a more robust and participatory blockchain network.

The **contributions of this paper** are the following:

- An innovative consensus algorithm enabling stake selection through the soft association of a validator with multiple fuzzy groups, rather than relying solely on the conventional mean crisp value of the stake, as typically used in PoS.
- A soft categorisation and reputation-based validator selection approach that ensures validators are chosen based on both stake and reputation rather than solely on stake.
- A function that models the behaviour of reputation is incorporated to enhance the consensus algorithm in the selection phase.
- A novel penalisation mechanism where validators who perform incorrect validations face a rapid decrease in their reputation, while reputation recovery is harder and gradual.

and the finding **highlights**:

- This method surpasses contemporary leading consensus algorithms in ensuring broader stake distribution while maintaining the same functionality.
- A security assessment was conducted with favourable outcomes to verify the proposed approach's resilience against potential threats and its ability to preserve network integrity.

Finally, an illustrative example is presented to show the performance of the equitable consensus algorithm, as well as its advantages concerning other consensus algorithms such as PoW, PoS, and DPoS, PBFT, and PoR.

The paper is structured as follows: Table 1 displays the nomenclature used in this work. Section 2 gives a background on blockchain and fuzzy logic. Section 3 reviews related work. Section 4 details the methodology of the proposed *'Fuzzychain'* and its consensus algorithm. Section 5 analyses the security of the proposed algorithm. Section 6 discusses implementation features and key results. Section 7 examines the advantages, disadvantages, and challenges of the algorithm. The paper finishes with the conclusions and future work in Section 8.

Table 1
This table shows the nomenclature used in this article.

Nomenclature	
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
PoR	Proof of Reputation
PoCC	Proof of Contribution
FSs	Fuzzy Sets
RSA	Rivest, Shamir and Adleman
ECC	Elliptic Curve Cryptography
CCW	Computing With Words
LL	Linguistic Label
MF	Membership Function
T1-MFs	type-1 fuzzy membership functions
$HMDF(x)$	Highest Membership Degree Function
μ_i	Fuzzy membership function
T_i	Set of fuzzy sets
t_i	Participants in T_i
j	Round
$rep(t_i, j)$	Reputation of t_i at the round j
$E(t_i)$	Expulsion rate of t_i

2. Background

This section provides concepts focusing mainly on block- chain technology and fuzzy sets, which have been used to develop this proposed work. Section 2.1 defines blockchain, public blockchain (permissionless), and elliptic curve cryptographic. Section 2.2 describes the fuzzy sets, triangular fuzzy sets, and finally, linguistic variables.

2.1. Blockchain technology

Blockchain technology is a decentralised and distributed ledger system that records and verifies transactions across multiple computers or nodes in a network (Zhang et al., 2024a). A public blockchain is a type of blockchain network known as a permissionless blockchains. This kind of blockchain is open to anyone and is maintained by a decentralised network of nodes (computers), where the nodes can validate transactions and contribute to the census mechanism (Ferdous et al., 2021). To add a new block to the blockchain, nodes must agree

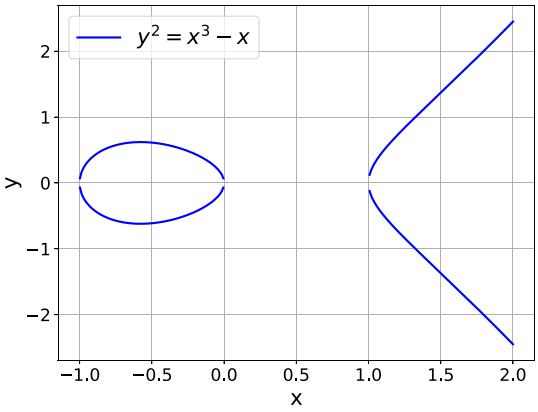

Fig. 1. The figure depicts the elliptic curve defined by $y^2 = x^3 - x$.

on the validity of the transactions through a consensus mechanism. Various consensus mechanisms, such PoW (Dwork and Naor, 1992; Back et al., 2002; Nakamoto, 2008) and PoS (Ethereum, 2023b), are used to achieve this agreement.

Blockchain often has high levels of security due to its decentralised nature and the use of cryptography. Cryptography plays a critical role in blockchain technology, which is applied to secure transactions, protect data, and control access to the blockchain. Specifically asymmetric cryptography is used to generate two keys: a public key and a private key, these keys are occupied to authenticate users and sign transactions, among others (Menezes et al., 1996). There are different asymmetric encrypted algorithms. The most popular are ElGamal (Elgamal, 1985), RSA (Rivest et al., 1978), and Elliptic Curve Cryptography (ECC) (Koblitz, 1994). ECC has been widely used because it uses smaller parameters but with equivalent levels of security than other algorithms, obtaining advantages such as faster computations and smaller keys (Johnson et al., 2001). According to Koblitz (1994), an elliptic curve is defined as follows and depicted in Fig. 1.

Definition 1. Let K be a field of characteristic $\neq 2, 3$, and let $x+ax+b$ be a cubic polynomial with no multiple roots, where $a, b \in K$. An elliptic curve over K is the set of points (x, y) with x, which satisfy the equation:

$$y^2 = a^3 + ax + b$$

with a single element denoted by $\odot$ and is called the point at infinity.

Blockchain offers multiple properties such as transparency and security, among others, nevertheless, still it faces challenges like scalability limitations (Sanka and Cheung, 2021) due to the high computational requirements and efficient consensus mechanisms (Pérez et al., 2022).

2.2. Fuzzy sets

Fuzzy sets theory, introduced by Zadeh in 1965 (Zadeh, 1965), extends the classical set theory to handle uncertainty and vagueness by allowing elements to have degrees of membership rather than just being either fully in or out of a set. This extension is particularly valuable in situations where precise classification is difficult due to ambiguity or imprecision in the data.

A fuzzy set is a collection of items where each element has a membership value that represents the degree to which it belongs to the set. These membership values range between 0 and 1, where 0 indicates no membership (completely outside the set) and 1 indicates full membership (completely inside the set). Values between 0 and 1 represent partial membership, indicating varying degrees of belongingness. The next paragraph provides a formal definition of a fuzzy set according to Aisbett et al. (2010), Mendel (2017).

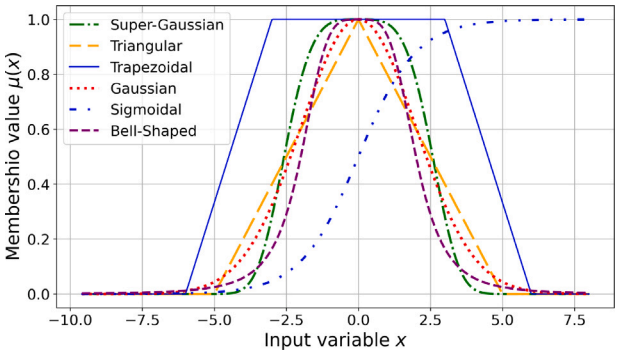

Fig. 2. The figure depicts six parametric membership functions.

Definition 2. Let X be a universe set. A is a fuzzy set if exist a function $\mu_A : X \to [0, 1]$ such that

$$A = \{(x, \mu_A(x)) : x \in X\}.$$

where μ_A denotes the membership function of A and $\mu_A(x)$ is called the degree of membership, or membership grade, of x in A.

Different membership functions have been used to represent fuzzy sets. For instance, parametric and non-parametric membership functions. Parametric functions are suitable for scenarios where data distributions exhibit uniformity (Mendel, 2017; Jain and Sharma, 2020). Examples include triangular, trapezoidal, Gaussian, sigmoidal, bell-shaped, and Super-Gaussian functions, as illustrated in Fig. 2. Non-parametric membership functions are often derived from data-driven methods and provide greater adaptability in representing gradual or abrupt changes. The use of approximated assessments, such as fuzzy values, has shown that very accurate values are unnecessary (Delgado et al., 1998). Therefore, using triangular fuzzy membership functions is common and simpler. Consequently, for the development of experiments and testing the performance of the proposed consensus algorithm (see Section 6), the triangular fuzzy membership function is employed, as defined below (Mendel, 2017):

$$\mu_A(x) = \begin{cases} 0 & \text{if } x < a \\ \frac{x-a}{b-a} & \text{if } a \leq x \leq b \\ \frac{c-x}{c-b} & \text{if } b \leq x \leq c \\ 0 & \text{if } x > c \end{cases}$$

One of the most interesting uses of fuzzy logic and fuzzy sets theory was given by Zadeh (Zadeh, 1999) when he proposed the idea of computing with words (CWW), "*a methodology in which the objects of computation are words and propositions drawn from a natural language*". The words in this paradigm CWW may be modelled using linguistic variables. According to Mendel (2017), a linguistic variable is a variable whose values can take words or sentences in a natural language and may be represented by fuzzy sets.

Definition 3. A linguistic variable is characterised by a quintuple (L, T, X, G, μ), where:

- L is the name of the variable,
- T is the set of linguistic terms of L,
- X is the universe of discourse,
- G is a syntactic rule that generates linguistic terms of L, and
- μ is a semantic rule that associates each linguistic term $t \in T$ its meaning, $\mu(t)$, which is a fuzzy set on X.

Notice that, μ can be seen as a function $\mu : T \to F(X)$, where $F(X)$ denotes the set of fuzzy sets of X, one fuzzy set for each $t \in T$.

Table 2
This table summarises the related work where the reputation-based consensus algorithms for blockchain networks are proposed.

Author	Year	Algorithm	Technique	Implementation tool	Type
Padma and Ramaiah	2025	Adaptive PoW	Genetically Modified Swarm Optimisation (SSO)	NS-3	–
Wang et al.	2025	Dynamic Grouping-based PBFT	Weighted Federal Average	Python	Consortium
Chen et al.	2025	Hybrid Multi-layer BFT	Commitee Election	Hyperledger Fabric	Consortium
Jia et al.	2025	Reputation-Weighted Asynchronous BFT	Filtering	Go	Hybrid
Hussain et al.	2025	Reputation-Based Leader Selection	Vote-based Method	Hyperledger Fabric	Consortium
Su et al.	2025	Proof of Contribution (PoCC)	Federated Learning	C++, Python	–
Gan et al.	2025	Proof of Reputation (PoR)	Tripartite Evolutionary Game Model	Python	–
Li et al.	2025	Game PBFT	Gaming	Go	–
Singh et al.	2025	Fair PoR	Variational Onsager Neural Networks (VONN)	Matlab	Consortium
Zhang et al.	2024	PoW,PBFT	Commitee Election	Python	–
Wen and Yang	2024	Multilevel Adaptive Practical BFT	Discourse Power Mechanism	–	Private
Wu et al.	2024	Reputation RAFT, Multiparty Optimised PBFT	Master-Slave Blockchain (MSB)	–	–
Deng et al.	2024	PoS, PBFT	Bottom-up Hierarchical architecture	Matlab	Private
Hu et al.	2024	Hierarchical Delegated Proof of Reputation (hDPoR)	Multi-weight Subjective Logic Model	Matlab	Hybrid
Ye et al.	2024	Lightweight adaptive BFT (LA-BFT)	Consensus Committee	OpenJDK	–
Rui et al.	2024	Distributed Authentication DPoS	Smart Contracts	Java	–
Li et al.	2024	Layered Cross-Chain PBFT	PageRank algorithm	Python	Hybrid
Tang et al.	2024	Threshold Proxy Signature PBFT (TP-PBFT)	Two Step Clustering	–	Hybrid
Du et al.	2024	Affinity-Propagation PBFT	Affinity-Propagation PBFT	Python	–
Hao et al.	2024	Reputation PoS	Deep Reinforcement Learning	Python	–
Chen et al.	2024	Reputation Slice PBFT (RSPBFT)	Slicing Approach	–	Consortium
Zhang et al.	2024	PoR	Short-term Pseudo-Identity Algorithm	–	Consortium
Zhang et al.	2024	Raft, PoA	Identity Information	NS-3	–
Liu et al.	2024	Improved PBFT	Improved PBFT	Python	Consortium
Yang et al.	2024	PoS and hybrid BFT (SG-FCB)	Stackelberg game-based	–	Hybrid
Li et al.	2024	Reputation Regression Raft	R-Logistic Regression	Go, Python	–
Xu et al.	2023	Efficient and Scalable PBFT (Me-PBFT)	Sigmoid Function	–	–
Du et al.	2023	Calculate Reputation MWSL-PBFT	Multi-weighted Subjective Logic	Go	–
Dehez-Clementi et al.	2023	Privacy-Preserving PoR	Ring Signatures and Dlog-based Zero-knowledge proof	Python	Private
Zhou et al.	2023	Proof of Training Quality (PoQ)	Bayesian Theory and Multiple Subjective Logic Models	Python	Consortium
Zhu et al.	2023	DPoS and PoW	Logistic Regression Model	Hyperledger Fabric	Public

3. Related work

Both in the domain of blockchain technology and others (Liu et al., 2021), numerous studies have underscored the pivotal role played by consensus algorithms in shaping the success and viability of blockchain. The comparative analysis of PoW and PoS conducted in Vashchuk and Shuwar (2018) highlights the sustainability concerns associated with PoW-based blockchains. The sheer energy consumption of PoW, which in 2019 equated to the energy requirements of an entire country like Denmark, accentuates the urgency of exploring more energy-efficient alternatives. PoS, with its focus on stake rather than computational power, presents a greener and more environmentally responsible approach. However, the transition to a PoS-based model introduces unique challenges, particularly regarding centralisation risks and the potential for stake concentration among a small group of participants.

One of the primary advantages of PoS over PoW is its inherent security against certain attack vectors. In PoS, users aiming to become validators must commit a portion of their stake as collateral, thereby subjecting their potential gains to risk. However, a well-recognised deficiency of PoS systems is their vulnerability to scenarios in which a malicious user, through legitimate investment or illicit means such as secret block creation (Eyal and Sirer, 2018) or selfish mining (Gemeliarana and Sari, 2018), amasses enough stake to control a majority (51% or more) of the PoS blocks. This level of control not only jeopardizes the integrity of the blockchain but can also disrupt its operations, as vividly described by Larimer in Larimer (2013). The deterministic nature of stake-based selection in PoS increases the risk of centralisation, as participants with a consistently higher stake are more likely to be chosen repeatedly, reinforcing their control over time.

To mitigate these centralisation risks, reputation-based consensus mechanisms have been explored as an alternative. Table 2 presents an overview of recent reputation-based consensus mechanisms, categorising them based on the algorithm, selection technique, implementation tools, and blockchain type. These models integrate trustworthiness as a selection criterion alongside financial stake, aiming to foster a more balanced validator selection process. Various studies have proposed reputation-driven consensus mechanisms, leveraging techniques such as vote-based selection, machine learning models, and federated learning. For instance, Reputation-Based Leader Selection (Hussain et al., 2025) employs a voting mechanism to determine validators, while Reputation PoS (Hao et al., 2024) incorporates deep reinforcement learning to dynamically adjust validator weights. Other models, such as Proof of Contribution (PoCC) (Su et al., 2025), use federated learning techniques to aggregate distributed node behaviours and enhance fairness in validator selection. Hybrid architectures, such as Hybrid Multi-Layer BFT (Chen et al., 2025), combine reputation scoring with committee-based election strategies to achieve a balance between fairness and efficiency.

Despite their improvements, reputation-based models still suffer from key drawbacks. One major issue is that long-term participation biases the system in favour of experienced validators, limiting opportunities for new participants. Many reputation mechanisms rely on static penalty models, which fail to dynamically adjust to real-time validator behaviour, making them vulnerable to manipulation or collusion. Furthermore, deterministic reputation-based selection methods create predictability in validator selection, allowing adversarial actors to exploit the system. Although, reputation models provide

additional security layers compared to traditional PoS, they often struggle to balance fairness, decentralisation, and resilience against Sybil attacks (Kumar et al., 2023).

To address these challenges, we propose Fuzzychain, a novel consensus mechanism that integrates stake values, reputation, and a degree of randomness in the validator selection process. Unlike existing PoS and reputation-based models, Fuzzychain introduces a "halo of fuzziness" into the evaluation of stake and reputation, ensuring that the selection process is not entirely deterministic. By incorporating randomness alongside stake and reputation, Fuzzychain reduces the likelihood that the same high-stake or long-standing participants will be continuously selected, thereby mitigating centralisation risks and ensuring a more equitable selection process. This randomness prevents adversarial entities from precisely predicting or manipulating the validator selection process, making the network more resistant to collusion and attacks. Additionally, Fuzzychain allows for adaptive reputation scoring, enabling participants to recover from penalties and dynamically adjust their standing based on real-time behaviour.

The evolution of consensus mechanisms in blockchain has evolved from computational power-based models (PoW) to financial stake-driven approaches (PoS) and, more recently, to reputation-based algorithms. While reputation-based consensus models introduce fairness and security improvements, they still suffer from deterministic selection biases and centralisation risks. Fuzzychain represents a significant advancement by introducing controlled randomness into stake and reputation-based selection, enhancing fairness, decentralisation, and security. This approach strengthens the resilience of blockchain networks, ensuring a more adaptive, sustainable, resilient, and equitable consensus mechanism that mitigates the pitfalls of existing models.

4. Fuzzychain: equitable consensus algorithm

In this section, we propose the Fuzzychain: an equitable consensus algorithm. A general description is given in Section 4.1 and the specific details are further explained in Section 4.2.

4.1. General description

In order to provide a clearer explanation of Fuzzychain, it has been segmented into three distinct stages, as depicted in Fig. 3.

Stage 1: Transaction initialisation and block creation

This stage considers the client nodes and the validators. The former generates transactions and the latter collects and aggregates these transactions to form a potential block for validation. These transactions represent digital agreements, exchanges of value, or any form of data that participants within the blockchain network wish to record. Each transaction contains details such as the sender, recipient, the amount involved, and a digital signature to ensure its integrity and authenticity. Once these transactions are collected and validated, a new block is generated. This block acts as a container, grouping a set of transactions. The creation of a new block involves cryptographic processes that secure the data within it, making it tamper-proof. After the new block is constructed, it is disseminated across the network to all participating nodes. This stage establishes the foundation for blockchain operations as it assembles the transactions and prepares them for validation.

Stage 2: Block validation and consensus

The second stage of Fuzzychain is the block validation process. In this critical phase, a consensus algorithm comes into play to determine the authenticity and validity of the transactions included within the newly created block. Consensus is a fundamental concept in blockchain technology, as it ensures that all participants in the network agree on the order and content of transactions. Various consensus algorithms can be employed, such as PoW, PoS or DPoS, depending on the blockchain's design. The consensus algorithm checks the transactions for compliance with the network's rules and validates that the participants involved have the necessary permissions and resources. Once consensus is achieved, a collective decision is made on which participants (often referred to as miners, validators, or delegates) will have the responsibility to add the new block to the blockchain. This phase is essential for maintaining the integrity and security of the blockchain, preventing fraudulent or erroneous transactions from being added.

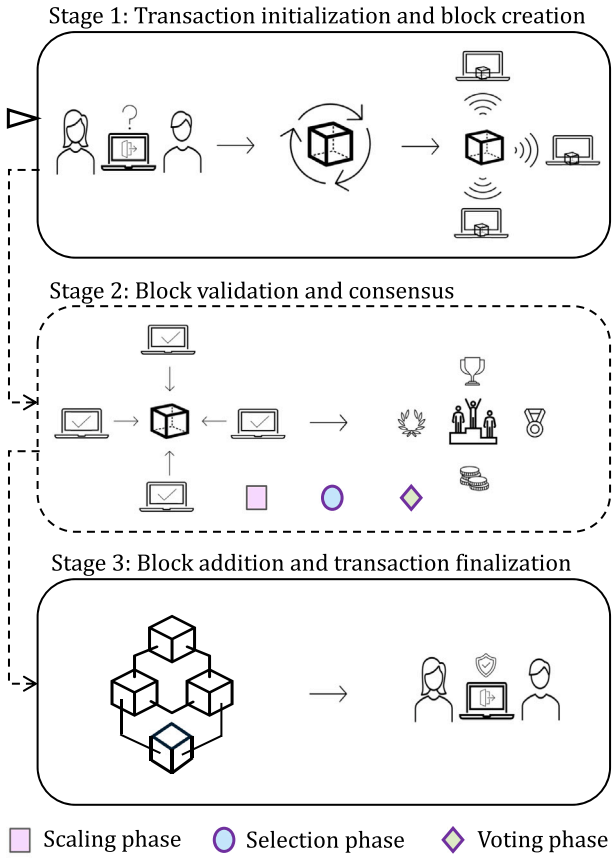

Fig. 3. The figure shows the blockchain process explained in three stages. Stage 1: Initialise the transaction, generate a new block, and send it to the participating network. Stage 2: Block validation and consensus process. In this stage, three phases are executed: scaling, selection and voting. Stage 3: The new block was added to the blockchain and transaction finalisation.

Stage 3: Block addition and transaction finalisation

The final stage, Stage 3, marks the process of adding the newly validated block to the blockchain, thus finalising the transactions it contains. Once the consensus algorithm has verified the transactions and designated the responsible participants, they undertake the task of appending the new block to the existing blockchain. This process ensures that the transactions are immutably recorded sequentially and chronologically. The added transactions are considered complete, and the agreed-upon changes to the blockchain state take effect. The added block becomes a permanent part of the blockchain's history, forming a secure and transparent ledger of all network activities. The blockchain's value lies in this stage, as it guarantees the reliability and trustworthiness of the recorded transactions, enabling the blockchain network to maintain its integrity and functionality.

General performance of Fuzzychain

These three stages collectively form the core of the Fuzzychain protocol, providing a systematic and secure approach to handling transactions within a blockchain network. By breaking down the process into these distinct stages, Fuzzychain enhances the transparency and

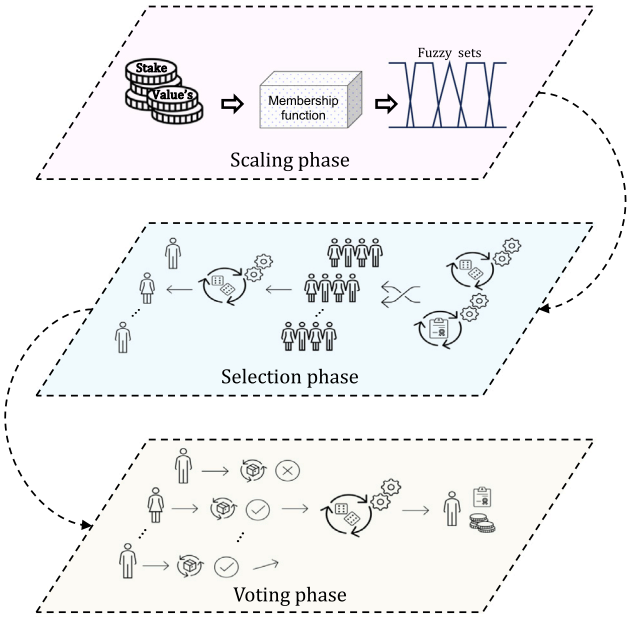

Fig. 4. The figure illustrates an overview of the scaling, selection, and voting phases employed in the development of the equitable consensus algorithm. These phases are applied during the second stage, where block validation and consensus occur.

reliability of blockchain operations, offering a practical solution to the challenges associated with trust, stake value, and control.

This research work will focus on Stage 2, a pivotal step in the functioning of a blockchain network. During this stage, a consensus algorithm is employed to ensure the integrity and security of the network. Through this intricate process, various nodes or validators participate in verifying the transactions and aiming to validate the block. This verification process is critical as it enhances the transparency and immutability of the blockchain, ensuring that only legitimate transactions are added to the distributed ledger. Once a consensus is reached among the participating nodes, the network can collectively decide on the next valid block to be added, thereby reinforcing the decentralised nature of the blockchain ecosystem.

Fuzzychain employs an equitable consensus algorithm based on proof of stake to validate block transactions. In the proposed algorithm, a numerical value representing a participant's stake is scaled into a set of fuzzy sets by using a membership function. Each numerical value is then assigned to an associated linguistic label, introducing an element of fuzziness to the stake representation. Fig. 4 illustrates an overview of the proposed equitable consensus algorithm. Subsequently, a set of participants is chosen based on their reputation from each fuzzy set. From each set of participants, selected randomly one or two validators, engage in the validation process and indicate whether the block should be accepted or rejected.

To determine the block's validity, a voting mechanism is employed, with consensus reached based on the majority of participants' decisions. If the majority indicates acceptance, the block is added to the Fuzzychain; otherwise, it is rejected. Subsequently, from the successful participants, one is randomly chosen to add the new block to the blockchain. These successful participants maintain their reputations and the selected participant who added the block receives a commission for completing the validation process. Conversely, unsuccessful participants are penalised, decreasing their reputation. Consequently, in the next round, they will be less likely to be chosen. A detailed description is provided in the following section for a more comprehensive understanding of the proposed equitable consensus algorithm.

4.2. Equitable consensus algorithm: design and specifications

Our proposal introduces an equitable consensus algorithm based on the proof of stake and fuzzy set theory to validate and verify block transactions, thus giving rise to the first Fuzzychain. Moreover, our method can be adapted and extended to other consensus mechanisms that rely on stake-based validator selection, such as DPoS, hybrid PoS/PoW system, and other approaches that incorporate stake and reputation in the validator selection process.

The proposed equitable consensus algorithm is composed by three phases: scaling, selection and voting phase, depicted in Fig. 4 and further detailed below.

Scaling phase

In this phase, the procedure entails scaling a participant's stake, represented by the numerical value into a set of fuzzy sets through the application of a membership function (MF) (in our case a triangular fuzzy membership). Therefore, it is defined the linguistic variable used by the consensus algorithm.

Definition 4. Let L be the linguistic variable defined by the Participant's stakes. The set of linguistic terms of L is $T = \{T_1, T_2, T_3, \dots, T_n\}$ and the universe of discourse is the interval $X = [l, r]$ with $l < r$ and $r, l \in \mathbb{N}$.

According to Zadeh in Zadeh (1975), the set T, in principle, could have an infinite number of linguistic terms. For practical purposes, and based on Miller's observation regarding the fact that human beings can reasonably manage to bear in mind seven or so items (Miller, 1994). Therefore, a few number of terms may suffice for broad distinctions, while finer categories (e.g., Very Low, Low, Medium, High, Very High) provide more detail. The chosen number should balance precision and usability, ensuring that stakeholders can easily differentiate between categories without excessive complexity.

For the linguistic variable L, one example of the set of linguistic terms, T, could be $T = \{Very\ Low, Low, Moderate, High, Very\ High\}$. The terms in T, for instance, *Very low*, *Low*, *Moderate*, etc. can be called linguistic labels (LL).

The first step of this phase is to divide the universe of discourse X into n uniformly spaced and distributed type-1 fuzzy membership functions (T1-MFs), where each T1-MF is related with a corresponding fuzzy set. In the next step, any user's stake's numeric value x is scaled and located in a fuzzy set defined on X, and each stake value is identified by a linguistic label. Since the value x may belong to different fuzzy sets with different degrees of membership, the following definition is presented.

Definition 5. Highest membership degree function . Let x be a stake value and let $T_1, T_2, T_3, \dots, T_n$ be fuzzy sets defined on the scale l to r. The highest membership degree function (HMDF) of the element x across these fuzzy sets is defined as:

$$HMDF(x) = \max\{\mu_{T_1}(x), \mu_{T_2}(x), \mu_{T_3}(x), \dots, \mu_{T_n}(x)\}$$

where

- $\mu_{T_i}(x)$ represents the degree of membership of the element x in fuzzy set T_i.

According to Definition 5, the numeric value x of the participant's stake corresponds to a unique fuzzy set assigned through the highest membership degree function. Furthermore, each fuzzy set is identified with a unique linguistic label. At this moment, the items $x's$ in the set of participant's stake values have been scaled into fuzzy sets T_i, each bearing the appropriate linguistic label (Very low, Low, Moderate, among others), using the adequate fuzzy membership function $\mu_{T_i}(x)$. The scaling phase can be visualised in Fig. 5 and is computed in Algorithm 1. Continuously with the proposal, the selection phase is described as follows.

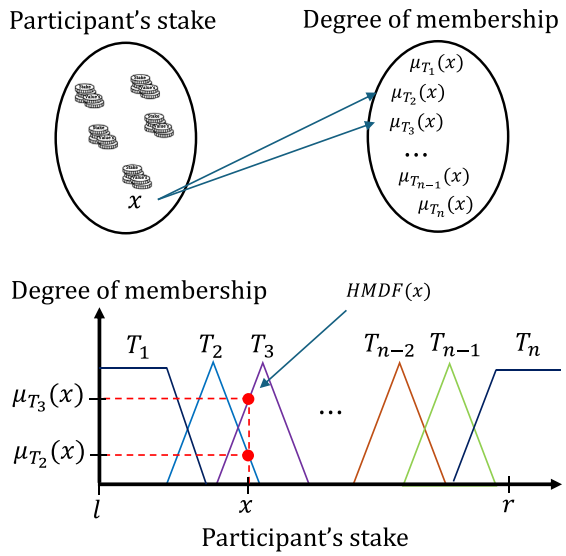

Fig. 5. The figure displays the scaling phase in the equitable consensus algorithm used in Stage 2. The items x in the set of Participant's stakes are scaled through the fuzzy membership function $\mu_{T_i}(x)$ into fuzzy sets T_i on the universe of discourse defined from l to r for the linguistic variable "Participant's stake". The degree of membership for x is the highest membership degree function (HMDF).

Algorithm 1 ScalingPhase (x)

Input : Stake value x ;
Output : Assigning T_i ;
function SP(x)
  for $j = 1$ **to** $numberParticipant'sStake$ **do**
    $MDF[]$;
    $HMDF[]$;
    $L = Participant's\ stake$;
    $T(L) = [T_1, T_2, T_3, \ldots, T_n]$;
    for $i = 1$ **to** n **do**
      $MDF \leftarrow \mu_{T_i}(x_j)$;
    end for
    $HMDF \leftarrow \max(MDF)$;
    $T_i \leftarrow ScaleStake(x_j, HMDF)$;
  end for
  return T_i ;
end function

Selection phase

This phase aims to choose participants t_i from each fuzzy set T_i. To achieve it, the phase involves two selection algorithms

(i) validator random selection and
(ii) validator selection according to the reputation.

The former is an algorithm that randomly chooses the participants, and the latter is then used to select participants based on their reputation from each fuzzy set. Reputation is a key concept in the development of this proposed algorithm, therefore the following definition is presented.

Definition 6 (*Reputation Range*)**.** Let t_i be a participant in the fuzzy set T_i. For all $t_i \in T_i$, the reputation $rep(t_i, j)$ at the round j, is defined on interval $[0, 1]$.

Each participant t_i entering a specific fuzzy set starts with an initial reputation set to 1 (maximum reputation). Subsequently, their reputation may be maintained or decreased contingent upon their performance, i.e., success or failure in their validation and verification tasks. To model the behaviour of the reputation when the validator's reputation differs from 1 the following function is defined.

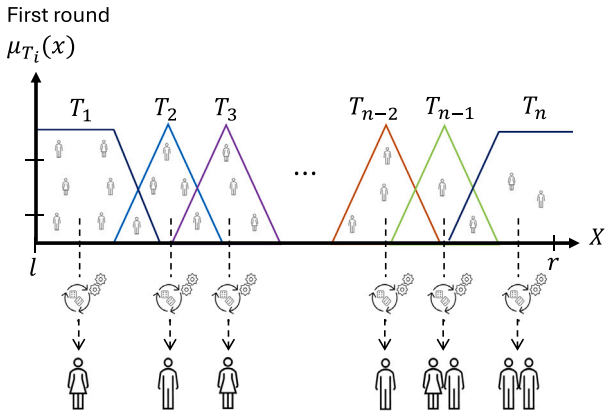

Fig. 6. This figure displays the selection phase during the first round, where the validator random selection algorithm is applied to choose the participants from the fuzzy sets T_i, respectively.

Definition 7. Let η be the decrease rate and let $\frac{\eta}{l}, l \in \mathbb{N}$ be the increase rate. If $rep(t_i, j)$ is the reputation for the validator t_i in the round j, then $rep(t_i, j+1)$ for the round $j+1$ is defined by

$$rep(t_i, j+1) = \begin{cases} 1 & \text{if } t_i \text{ is a successful validator} \\ & \text{and } rep(t_i, j) = 1 \\ rep(t_i, j) + \frac{\eta}{l} & \text{if } t_i \text{ is a successful validator} \\ rep(t_i, j) - \eta & \text{if } t_i \text{ is a unsuccessful} \\ & \text{validator} \end{cases}$$

where $0 \leq rep(t_i, j+1) \leq 1$.

In order to choose the participants t_i, in the first round (to validate the first block), when all the participants have the same reputation, the validator random selection algorithm is applied to select one participant from each fuzzy set $T_1, T_2, \ldots, T_{n-2}$ and two participants from each fuzzy set T_{n-1} and T_n. Fig. 6 shows the selection process for the first round.

Remark 1. This selection is based on the assumption that participants in fuzzy sets with the highest stake percentages have a greater interest in ensuring the network functions effectively and securely. Consequently, these participants are more trusted than those with lower stake percentages in the verification and validation process. Therefore, selecting an additional participant from the fuzzy sets with the highest stakes helps prevent participants with lower stakes from gaining control of the network, decreasing the risk of the 51% attacks. Moreover, this selection ensures an odd number of participants, which is crucial for the voting phase because, in the voting process is not possible to get a tie, Section 5 will explain it in more detail.

For the next jth rounds, to select the participants t_i the reputation is considered, viz., the participants that have the highest reputation in each fuzzy set T_i have more probability of being chosen than participants with a lower reputation. The candidates are selected using the validator selection algorithm according to their reputation, which will explain to continue. This algorithm generates two subsets A_i and B_i from each fuzzy set T_i and both are defined as follows:

$$A_i = \{t_i \in T_i : rep(t_i, j) = 1\},$$

$$B_i = \{t_i \in T_i : rep(t_i, j) \leq 1\}.$$

Notice that the subset A_i contains only participants with the reputation set to 1, while the subset B_i includes participants with reputations less than 1 as well as those with a reputation of 1, hence $A_i \subseteq B_i$. These sets are designed with the intention that participants with the highest

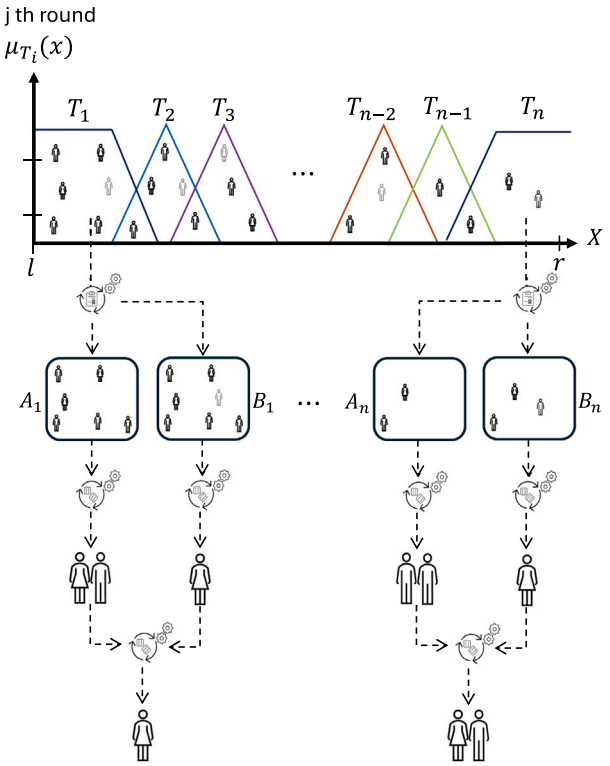

Fig. 7. The figure depicts the validator selection algorithm according to the reputation to choose the participants t_i from each fuzzy set T_i during the jth round.

reputation (set to 1) are more likely to be chosen than those with a lower reputation.

Once the subsets are defined, the random selection algorithm chooses two participants from subset A_i and one from subset B_i. In this way, the participants with the highest reputation have a higher probability of being chosen compared to the participants with a lower reputation. While participants with lower reputations may have fewer opportunities, but they still can excel in subsequent tasks and improve their reputations. Hence, they may ascend to the group with the highest reputation. Nevertheless, if one participant continues incorrectly doing the tasks, they will be expelled from the group of validators or even from the network. To manage this case, the validators have an error rate based on their reputation, which is presented in the following definition.

Definition 8. Expulsion rate. Let $rep(t_i, j)$ be the reputation of the validator t_i. The expulsion rate of t_i, $E(t_i)$, is defined by:

$$E(t_i) = \begin{cases} 0 & If\ rep(t_i, j) = 1 \\ 1 - rep(t_i, j) & If\ rep(t_i, j) \neq 1 \end{cases}$$

As a consequence of Definition 8, the next exclusion condition is presented.

Definition 9 (*Exclusion Condition*)**.** Let ϵ be the expulsion rate defined and allowed in the fuzzychain. If the $E(t_i) > \epsilon$ then the participant t_i is excluded from the set of validators.

In the final step of this phase, participants from both subsets are combined, and the random selection algorithm is applied. It selects one participant from the sets $T_1, T_2, \ldots, T_{n-2}$, two participants for T_{n-1} and others two for T_n. Fig. 7 illustrates the process for the jth round and is detailed in Algorithm 2.

After the participants are selected for each fuzzy set, the validation and verification process of the block ensues. To do this, the voting phase is used and described in detail in the following paragraphs.

Algorithm 2 SelectionPhase (x)

Input : Fuzzy set T_i ;
Output : Validator V_i ;
function SP(x)
  $rep[] = 1$;
  if $round\,j == 1$ **then**
    for $i = 1$ **to** $n - 2$ **do**
      $t_i \leftarrow randomlyChosenOne(T_i)$;
    end for
    $t_{n-1} \leftarrow randomlyChosenTwo(T_{n-1})$;
    $t_n \leftarrow randomlyChosenTwo(T_n)$
  else
    $A_i \leftarrow generateSubsetA(T_i)$;
    $B_i \leftarrow generateSubsetB(T_i)$
    for $i = 1$ **to** $n - 2$ **do**
      $a_i \leftarrow reputationChosenTwo(A_i)$;
      $b_i \leftarrow reputationChosenOne(B_i)$;
    end for
    $a_{n-1} \leftarrow reputationChosenTwo(A_{n-1})$;
    $b_{n-1} \leftarrow reputationChosenOne(B_{n-1})$;
    $a_n \leftarrow reputationChosenTwo(A_n)$;
    $b_n \leftarrow reputationChosenOne(B_n)$;
  end if
  for $i = 1$ **to** n **do**
    $M[i] \leftarrow mix(a_i, b_i)$
    $V_i \leftarrow randomlyChosenOne(M)$;
  end for
  return $Validators\ V_i$;
end function

Voting phase

The selection phase chooses one participant for the first $n - 2$ fuzzy sets and two participants for the last $n - 1$ and n fuzzy sets. Therefore, the number of participants in the voting mechanism depends on the number of fuzzy sets, then there is an important requirement related to the fuzzy sets. The number of fuzzy sets on X should be an odd number, this is crucial, particularly in the context of the voting phase within the consensus algorithm. This stipulation aligns with the design of the voting mechanism, which facilitates the selection of participants in a balanced and equitable manner during the voting phase. With an odd number of fuzzy sets, there will always be a clear majority when it comes to decision-making, minimising the likelihood of ties. In essence, the requirement for an odd number of fuzzy sets on X serves to optimise the efficiency of the consensus algorithm, particularly in the critical voting phase where decisions are made regarding the acceptance or rejection of blocks within the Fuzzychain network.

Once the validators have been selected from each fuzzy set T_i at the selection phase, every one of them individually engages in the validation process and subsequently indicates whether the block should be accepted or rejected. This phase involves a voting mechanism employed to determine the block's validity, wherein a consensus is reached based on the majority of participants' decisions. If the majority indicates acceptance, the block is accepted; otherwise, it is rejected.

The sample spaces of the voting mechanism is $\Omega = \{accepted, rejected\}$; there are no other possibilities. The validators who won the vote will be considered successful, that is if the majority indicates that the block is accepted or rejected. Therefore, to encapsulate this idea, the next definition is presented.

Definition 10 (*Successful Validator*)**.** A validator V that participates in the voting mechanism is considered a successful validator if and only if V is in the group of the validators who secure the majority vote.

Definition 11 (*Unsuccessful Validator*)**.** A validator V_u that participates in the voting mechanism is considered an unsuccessful validator if and only if V_u is in the group of the validators who secure the minority vote.

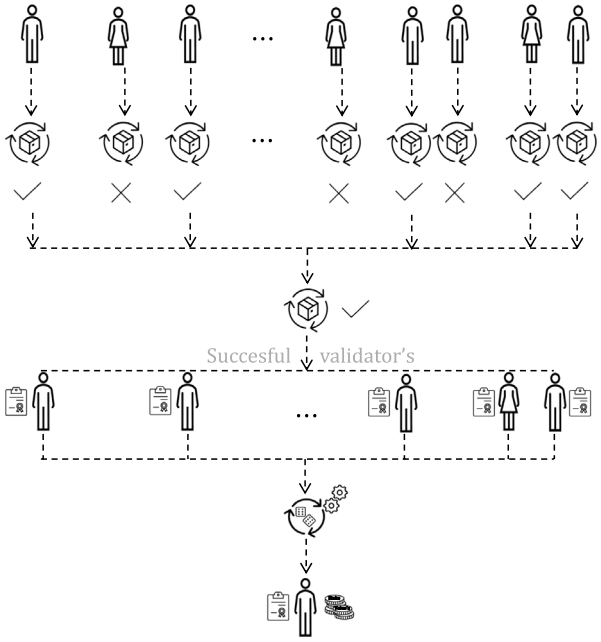

Fig. 8. The figure depicts the voting phase between participants chosen in the selection phases. Each participant verifies and validates the transactions in the block and then casts their vote to accept or reject the block. Then, the winner validator is obtained by employing the random selection algorithm.

When the validation process is finished and it has been decided whether the block is accepted or rejected, a new selection process is carried out among the successful participants to know which of them is the winner because only one of them can take the full reward. The selection process is performed by the validator random selection algorithm presented in the selection phase.

The reward for all successful validators is an increase in their reputation if the reputation is less than 1 and maintaining their reputation if the reputation is equal to 1. Nevertheless, for the winner validator, in addition to the reputation, a commission for having completed validation is obtained. The voting phase is depicted in Fig. 8 and computed in Algorithm 3.

It is important to note that in this algorithm the increase and decrease in reputation are not proportional, reputation increases more slowly and decreases more quickly. Unsuccessful validators are penalised by lowering their reputation, which limits them to having less chance of being selected the next time. In this proposal, any participant can make a mistake, so the penalty is the same for everyone regardless of whether you have more or less stake.

In summary, the proposed equitable consensus algorithm for Fuzzychain combines elements of proof of stake and fuzzy set theory to achieve a fair and reliable method for validating block transactions. By introducing linguistic labels to represent participants' stakes and utilising reputation as a selection criterion, the algorithm establishes a balanced approach to participant involvement in the validating process. The incorporation of a robust voting mechanism, where consensus is reached through the majority decision of selected participants, adds an additional layer of reliability to the validation process.

The algorithm ensures that successful participants not only contribute to the blockchain by adding accepted blocks but also receive dual rewards in the form of a commission for validations and an increase in reputation. Conversely, unsuccessful participant validators face penalties, including a reduction in reputation, impacting their chances of selection in subsequent rounds. This approach encourages participants to engage actively in the network, ensuring a balanced distribution of opportunities.

Algorithm 3 VotingPhase (x)

Input : Validator V ;
Output : Validator V_{winner} ;
function VP(x)
  $listDecision[]$;
  $listValidators[]$;
  for $i = 1$ **to** $NumValidators$ **do**
    $listValidators[i] \leftarrow Validator\ V_i\ validate\ the\ block$;
    $listDecision[i] \leftarrow Validator\ V_i\ accepted\ or\ rejected$;
  end for
  $Res \leftarrow votingMechanism(listDecision)$;
  if $Res == True$ **then**
    $Transactions\ block\ is\ accepted$;
  else
    $Transactions\ block\ is\ rejected$;
  end if
  $Succ_v \leftarrow chosenSuccessValidators(listValidators)$;
  if $V\ is\ Succ_v$ **then**
    $increaseReputation(V)$;
  else
    $decreaseReputation(V)$;
  end if
  $V_{winner} \leftarrow randomlyChosenOne(Succ_v)$;
  $Reward(V_{winner})$;
  return V_{wineer} ;
end function

The detailed description of the proposed equitable consensus algorithm provides a foundation for understanding its inner workings and sets the stage for further implementation and optimisation. This algorithm stands as a key component in Fuzzychain's pursuit of a secure, transparent, and inclusive blockchain network. In the next section, a security analysis is presented.

5. Security analysis

Ensuring the robustness and security of the proposed equitable consensus algorithm for Fuzzychain is paramount for its successful deployment in blockchain networks. This section analyzes the proposed consensus algorithm to prove that possesses the characteristics of a consensus algorithm. In addition, a comprehensive security analysis to assess the algorithm's resilience to potential threats and its ability to maintain the integrity of the network.

5.1. Consensus algorithm properties

The properties that an algorithm must satisfy to be considered a consensus algorithm were initially proposed in the context of distributed systems (Lamport et al., 1982). Later, these properties are adapted to the blockchain and cryptocurrency context. A consensus algorithm should satisfy four fundamental properties: Validity, Agreement, Termination, and Integrity. This section discusses how the proposed consensus algorithm meets these properties, providing proofs for each.

Validity: *If all honest nodes propose the same value v, then v must be chosen.*

Proof. In FuzzyChain, the selection phase ensures that only validators selected based on their stake and reputation participate in the block validation process. During the voting phase, these selected validators verify the correctness of proposed blocks before casting their votes. Given that all honest nodes adhere to the validation procedure, they will consistently vote for the correct value. The voting mechanism follows a majority decision rule, which accurately reflects the consensus when honest nodes propose the same valid block. Consequently, the block is either accepted or rejected based on the majority decision,

ensuring all honest nodes reach the same conclusion. As the voting process is deterministic under honest behaviour, the proposed consensus algorithm satisfies the validity property, guaranteeing that consensus is reached on a correctly proposed value.

Agreement: *All honest nodes must agree on the same value.*

Proof. In the proposed consensus algorithm, the selection phase is designed to ensure a fair and equitable choice of validators from diverse fuzzy sets, with validators exhibiting greater reliability and reputation having a higher probability of selection. During the voting phase, a majority rule is employed to determine the outcome, and the use of an odd number of fuzzy sets eliminates the possibility of ties, thereby ensuring a clear and unambiguous decision. Since all honest validators adhere to the same protocol rules and base their votes on identical transaction data, they are guaranteed to reach a consistent consensus. Consequently, the algorithm ensures that all honest nodes cannot arrive at different values, thus satisfying the agreement property.

Termination: *Every honest node eventually decides on a determined value.*

Proof. Given the proposed consensus algorithm, the selection phase ensures that validators are chosen in every round, enabling the consensus process to proceed systematically. During the voting phase, once validators cast their votes, the outcome is determined within a finite time, ensuring timely resolution. The algorithm is designed to employ an odd number of validators to guarantee a decisive outcome. In this way, the algorithm ensures that the process will always conclude and every honest node eventually decides on a determined value.

Integrity: *If an honest node decides on value v, then v must have been proposed by some honest nodes.*

Proof. In the proposed consensus algorithm, the integrity of the process is upheld by ensuring that only values validated by honest validators are considered during consensus. The selection process is designed to choose validators fairly, with nodes exhibiting poor reputations having a reduced likelihood of being selected, thereby promoting a trustworthy validator pool. The voting mechanism further reinforces this integrity by ensuring that only properly validated transactions can reach a consensus. Since the decision-making process relies on majority voting among pre-selected, high-reputation nodes, an honest validator is inherently prevented from deciding on an invalid or unproposed value. Consequently, any value that is decided upon must have been proposed by at least one honest node, ensuring that the integrity property is satisfied and maintaining the reliability of the consensus outcome.

These properties collectively demonstrate that the proposed algorithm is both reliable and secure, capable of achieving consensus in a decentralised environment while preventing malicious behaviour and ensuring consistent outcomes. As such, the proposed algorithm meets the criteria for a consensus algorithm and provides a solid foundation for decentralised decision-making in distributed systems.

5.2. Fuzzychain security

This section presents an analysis of the core concepts underlying the proposed consensus algorithm.

Untrustworthy validators

The security of blockchain networks relies on the assumption that a significant portion of the validators are honest and act in the best interest of the network. If a large majority of validators collude or behave maliciously, they could potentially compromise the integrity of the blockchain. To mitigate these risks, blockchain protocols often set a threshold of honest validators required for the network to operate securely. This threshold could be expressed as a certain percentage of the total of the set of validators. Nevertheless, Fuzzychain does not focus on the total percentage of validators, on the contrary, it focuses on some fuzzy sets being reliable. In Fuzzychain the specific threshold of honest validators required to operate securely is determined by a minimum of fuzzy sets trusted.

Definition 12. Let n be the number of fuzzy sets on the universe of discourse X, the minimum number of fuzzy sets trusted required to operate securely is determined by

$$\left\lfloor \frac{n-2}{2} \right\rfloor + 1$$

where $\lfloor\rfloor$ denotes the floor function.

This stipulation holds profound significance in fortifying the consensus process against potential threats posed by malicious activities or coordinated attacks. By mandating trust in a significant majority of fuzzy sets, the algorithm provides formidable defences, shielding the system from attempts aimed at compromising its integrity or disrupting its functionality.

Fuzzy stake representation

The introduction of fuzzy sets in representing participants' stakes adds an element of uncertainty and flexibility to the algorithm. Fuzzy representations allow for a nuanced and distributed approach to stake distribution, making it challenging for an attacker to predict or control the specific stake distribution necessary to compromise the majority of validator positions.

Reputation-based selection

The algorithm emphasises reputation as a factor in the participant selection process. Validators are chosen based not only on their stake but also on their reputation within the network. This reputation-based selection introduces an additional layer of complexity for potential attackers, as they would need to influence both stake and reputation to control the majority of validator slots. Another point of view is that the algorithm employs a mechanism that involves the randomised selection of validators from diverse groups. This decentralisation in the validator selection process prevents a single entity from gaining control over the majority of validator slots in a deterministic manner. As a result, even if an entity has a significant stake, the randomness in validator selection mitigates the risk of concentration and control.

Incentive structure

The dual rewards system, combining both commissions for successful validations and reputation increases, incentivises active and honest participation. Attackers attempting a 51% attack would risk reputational damage and reduced chances of future selection, discouraging malicious behaviour. In addition, the algorithm's randomised selection and the inclusion of reputation as a factor ensure a dynamic and ever-changing participant landscape. This dynamic nature makes it challenging for an attacker to consistently maintain control over the majority of the network's computational power.

Continuous improvement and adaptability

The penalties imposed on unsuccessful participants, including a decrease in reputation and reduced chances of selection in the next round, contribute to an environment of continuous improvement. This adaptability further deters malicious actors as the network adjusts to minimise the impact of unfavourable behaviours.

The proposed equitable consensus algorithm's resistance against 51% attacks is rooted in its decentralised, reputation-based, and dynamic participant selection process, coupled with the introduction of fuzzy sets for stake representation. These features collectively enhance the algorithm's robustness and make it inherently challenging for any single entity to gain control over the majority of the network's computational power in a predictable or sustained manner.

6. Experiments and results

This section performs and discusses a set of experiments designed to assess the performance of the equitable consensus algorithm and the Fuzzychain proposed within a permissionless scenario. An overview of the information system, the outcomes and the findings from these experiments are presented.

The experiments were developed on the following software and computer specifications. It includes a CPU and an Intel® Core™ i7-7500U processor, featuring a clock speed of 2.70 GHz and four cores. The operating system used is Ubuntu 22.04.3. For compiling, A C++ compiler, GCC version 7.4.0 is utilised. The programming language employed is Python, specifically version 3.10.12. Additionally, the system makes use of two libraries: ECDSA and SIMPFUL.

6.1. Experimental results

This proposal encompasses the execution of two experiments. Experiment 1 is dedicated exclusively to displaying the performance of the equitable consensus algorithm. Experiment 2 is designed to showcase a comparison concerning the equitable consensus algorithm proposed with other consensus algorithms such as PoW, PoS, and DPoS.

Experiment 1

The objective of this experiment is to demonstrate the performance of the equitable consensus algorithm. To accomplish this, simulations have been developed to illustrate how the consensus algorithm operates when selecting participants in each round to validate the block. Furthermore, the experiment offers insights into the frequency with which each winning participant is chosen. This analysis allows us to gain a comprehensive understanding of not only the algorithm's functionality but also the distribution of selection among participants of the different fuzzy sets, a critical element of an equitable consensus algorithm.

For this experiment, we considered 990 validators participating in the equitable consensus algorithm, with each validator assigned a stake value. According to Definition 4, we defined the information representation scale for the stake values with bounds $l = 0$ and $r = 10$. We then segmented this scale into five linguistic terms: Very Low (VL), Low (L), Moderate (M), High (H), and Very High (VH).

Remark 2. For this experiment, we have used distributed symmetric linguistic labels. Nevertheless, the proposed algorithm allows the use of unbalanced linguistic labels (Herrera et al., 2008).

Following the scaling phase in Section 4.2, to develop this experiment, the validators are distributed using a triangular membership function as follows: 500 in the linguistic term 'VL', 300 in 'L', 150 in 'M', 30 in 'H' and 10 in 'VH' as illustrated in Fig. 9.

From each one of these linguistic terms, we select a set of validators based on their reputation. Nevertheless, in the first round, since all the validators have the same initial reputation set to 1, the selection process is random. According to the selection phase presented in Section 4.2, to validate the first block, one validator is chosen randomly from each linguistic variable VL, L, and M, and two validators from each linguistic variable H and V. From this set of validators, only one validator is further selected to perform the validation process. The seven validators corresponding to each linguistic term initiate the validation process, with each of them casting their vote.

According to the voting phase in Section 4.2, the block is either accepted or rejected, and the successful and unsuccessful validators are then announced. On the one hand, each successful validator receives a reputation increase of 0.005 as a reward for doing well; on the other hand, unsuccessful validators decrease their reputation by 0.1 every time they want to damage the network. Finally, from the pool of successful validators, only one is randomly chosen as the winner, who is entitled to receive a commission in addition to the increase in reputation.

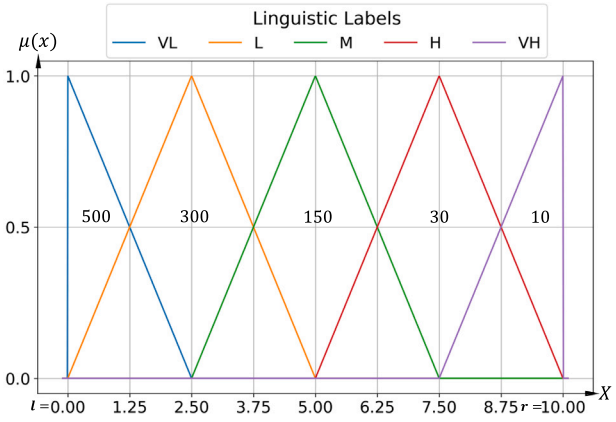

Fig. 9. Membership functions for linguistic terms T(Participant's stakes)= {Very Low (VL), Low (L), Moderate (M), High (H), Very High (VH)}.

For the next round, to choose the validators from each linguistic term, everyone's reputation is considered. We select a set of validators using the validator selection algorithm according to the reputation shown in the selection phase in Section 4.2. Analogous to the first round, from this set of validators, only one validator is selected to perform the validation process. The seven validators corresponding to each linguistic term initiate the validation process, and each of them casts their vote. According to the voting phase in Section 4.2, the block is either accepted or rejected, and both successful and unsuccessful validators are announced. Successful validators receive an increase in reputation of 0.005, while unsuccessful validators have their reputation decreased by 0.1. From the group of successful participants, one winner is randomly selected and entitled to receive a commission.

This algorithm is executed every time a block needs validation. For this experiment, the algorithm was run for 100, 200, 300, 400, and 500 rounds, aiming to demonstrate the frequency count of validators selected for each linguistic term. The validators selected change in each round, that is because in each round, the reputation is recalculated, and the validator with the highest reputation is chosen according to the algorithms presented in 4.2. First, the outcomes of the experiment for 100 rounds are presented. Fig. 10 shows the selections of validators in each iteration after running the algorithm at 100 rounds. From the figure, the proposed method shows the variations in the selection of validators. Fig. 11 summarises the number of validators selected for each linguistic term at 100 rounds. The X-axis represents the linguistic terms of each validator, and the Y-axis illustrates the frequency count. From the figure, it is evident that most validators are selected from the linguistic terms H and VH. That means a greater number of validators with a higher interest in the network working well have participated in the verification and validation process. Always consider the participation of the other validators corresponding to the linguistic terms VL, L, and M. The mean of selected validators is 20 with a standard deviation of 7.07. Therefore, the dispersion of selection among validators for the linguistic terms VL, L, and VH are within the first standard deviation and the terms M and H are within the second standard deviation.

For rounds 200, 300, 400, and 500, the outcomes are summarised in Fig. 12. This figure, despite five plots, corresponds to the selection of validators for each linguistic label in different rounds. For instance, the green graph illustrates the number of validators selected from each linguistic term when the algorithm runs in a set of 300 rounds. In this scenario, 46 validations were done by the validators selected from the linguistic term VL, 45 from L, 35 from M, 83 from H and 91 from VH. At the different rounds, the linguistic terms 'H' and 'VH' participate more than others in the validation and verification process. This is beneficial as the algorithm was designed to select validators with

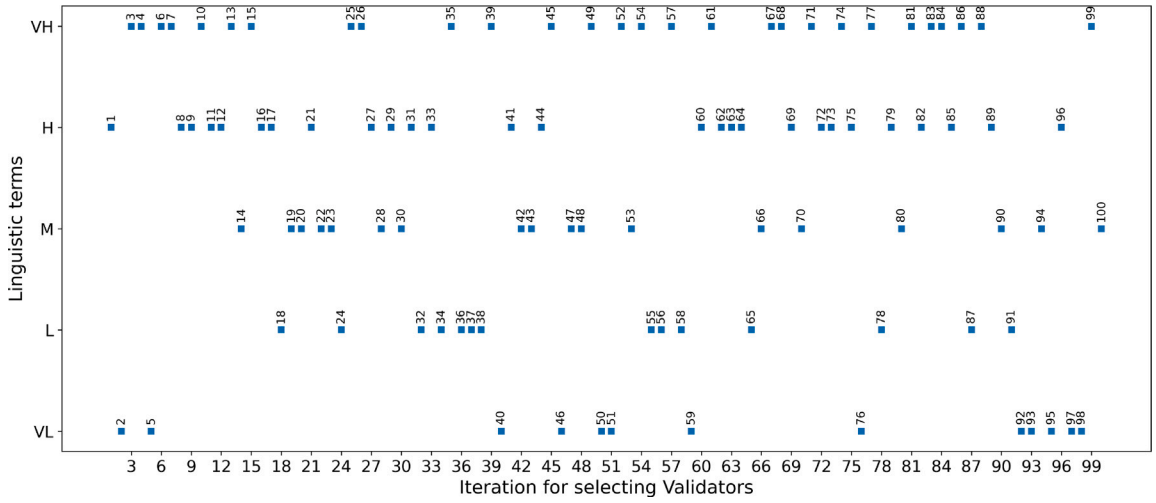

Fig. 10. The figure shows the selection of validators in each iteration after running the algorithm at 100 rounds.

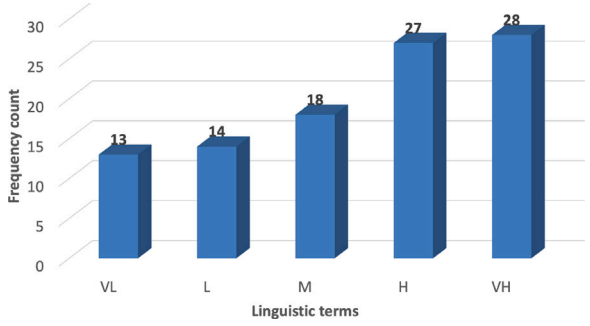

Fig. 11. The figure summarises the number of validators selected for each linguistic term at 100 rounds.

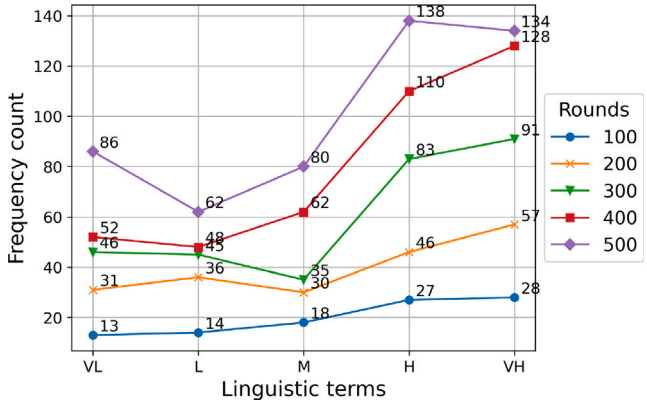

Fig. 12. The figure despite five plots corresponds to the selection of validators for each linguistic label in 100, 200, 300, 400 and 500 rounds.

higher reputations, higher stakes and, consequently, higher trust, thus increasing trust in the system.

Intending to study the behaviour of the proposed algorithm, we decided to repeat 20 times the experiment where the validators are selected during 500 rounds. The idea is to show the outcomes obtained in each round; nevertheless, since there are multiple numeric values, we decided to use a boxplot to group the results. Fig. 13 presents a boxplot for each linguistic term VL, L, M, H, VH and the Y-axis show the frequency count. From the figure, it is clear that the data in the boxplot for H and VH are greater than the data in the boxplot for VL, L, and M. For instance, for the linguistic term VH the minimum value of

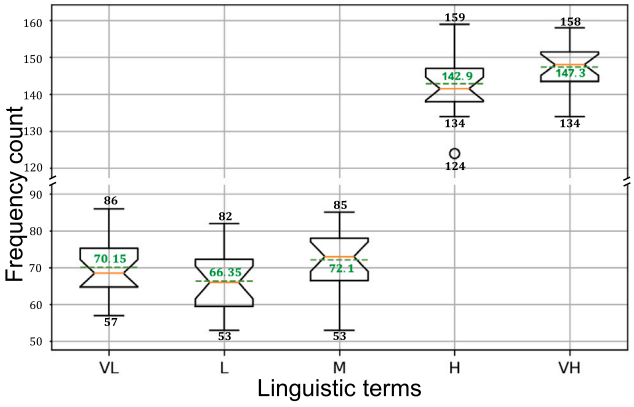

Fig. 13. Figure shows a boxplot representing the frequency and distribution of the validator selected by the equitable consensus algorithm in twenty repetitions.

selected validators during the 20 repetitions is 134 and the maximum is 158 with a mean of 147.3 which is displayed with a green dashed line. For the linguistic term M, the minimum value obtained in the twenty repetitions is 53, and the maximum value is 85, where the mean is 72.1. It is important to mention that this event never happens in the PoS consensus algorithm because, in PoS, the distribution of the validator selection process is always oriented towards validators with a higher stake.

Experiment 2

This section presents a comparison concerning the proposed consensus algorithm and other consensus algorithms used in blockchain. In this comparative analysis, we delve into the distinctive features of the proposed consensus algorithm with well-established blockchain consensus mechanisms, such as PoW, PoS, and DPoS. Each of these consensus algorithms operates on distinct principles and exhibits unique strengths and weaknesses. Firstly, PoW, the pioneer in consensus mechanisms, relies on computational power to validate transactions through complex mathematical puzzles (Bach et al., 2018; Wendl et al., 2023). On the other hand, PoS introduces a more energy-efficient approach, where validators are chosen based on the amount of stake they hold and are willing to "stake" as collateral (Saad et al., 2021; Fahim et al., 2023). Meanwhile, DPoS further optimises scalability by employing a selected group of delegates to validate transactions, nevertheless, this specific group of delegates can contribute to the risk of centralisation (Saad et al., 2021; Alrowaily et al., 2023). Table 3 summarises

Table 3
This table summarises a qualitative comparison between PoW, PoS, DPoS, PBFT, PoR, and Fuzzychain.

	PoW	PoS	DPoS	PBFT	PoR	Fuzzychain
Time complexity	High	Lower than DPoS	Lower than PoW	Low	Low	Lower than PoS
Energy consumption	High	Lower than PoW	Lower than PoW	High	Moderate	Lower than PoW
Security	High	Lower than PoW	High	Low	Moderate	High
Decentralisation	Lower than Fuzzychain	Lower than Fuzzychain	Lower than Fuzzychain	Lower than Fuzzychain	Lower than Fuzzychain	High

the properties of each consensus mechanism. This section aims to highlight the differences, enabling a comprehensive understanding of how the proposed consensus algorithm contributes to time complexity, energy consumption, security, and decentralisation and improvement of blockchain technology.

In order to provide a quantitative comparison, the consensus algorithms PoW, PoS and DPoS, PBFT, and PoR were simulated and set to the following conditions. For the PoW, 100 miners were selected to participate in the verification and validation process during 100 rounds. The consensus PoW chooses the first miner who solves the mathematical proof. The frequency of selected miners was registered, and then the data were used to compute the following metrics: Gini coefficient, Skewness, and Kurtosis. These metrics also are computed for consensus PoS, DPoS, PBFT, PoR, and Fuzzychain. For the consensus algorithm PoS, a set of 100 validators is defined to participate in the validation process. In this implementation, the validators have different stakes, and the validator with a higher stake has more probability of choosing the winner to do the validation process. This experiment was executed 100 rounds and the frequency of the selected validators was registered, and then calculate the three metrics as well. For the consensus algorithm DPoS, 100 delegates were defined to participate in the verification and validation process. In this experiment, the validator is chosen according to the stake and the reputation; that is, the delegate that has a higher stake with a higher reputation will have a higher probability of being the winner delegated. Similar to the others, the number of rounds in this experiment was 100, consequently the frequency of selected delegates was calculated and then the metrics were computed also. For the PBFT consensus algorithm, a total of 100 validators were defined to participate in the consensus process. In this implementation, the network operates leader-based, where one validator is randomly selected as the primary node (leader) for each round, and the remaining validators act as backups. Each round follows the standard PBFT protocol, consisting of pre-prepare, prepare, and commit phases to reach an agreement on a proposed block. The experiment was executed for 100 rounds, during which the frequency of selected primary nodes was recorded, and the consensus efficiency was evaluated using three defined metrics. For the Proof of Reputation (PoR) consensus algorithm, 100 validators were selected based on their reputation scores, which were dynamically adjusted according to historical behaviour and participation in the network. In this implementation, validators with higher reputation scores had a greater probability of being chosen to validate transactions and propose new blocks. The experiment was executed for 100 rounds, and the frequency of selected validators was tracked. Subsequently, the three metrics were computed to assess the consensus process as well. In the case of Fuzzychain, we considered 990 validators participating in the equitable consensus algorithm, with each validator assigned a stake value. The validators are distributed using a triangular membership function as follows: 500 in the linguistic term 'VL', 300 in 'L', 150 in 'M', 30 in 'H' and 10 in 'VH' as illustrated in Fig. 9. The results are displayed in Table 4 where a numerical comparison is presented.

Table 4 presents a comparison between PoW, PoS, DPoS, and the proposed consensus algorithm under Fuzzychain. To do this, the Gini coefficient is calculated for every consensus algorithm discussed before. The Gini coefficient assesses the disparity within the values of a frequency distribution, such as income levels. A Gini coefficient of 0 denotes total equality, reflecting a situation where all individuals have the same income or wealth. On the other hand, a Gini coefficient of 1 denotes maximal inequality, where all income or wealth is concentrated with a single individual, leaving none for others. Skewness near zero suggests a more symmetric and, thus, more evenly structured distribution. Additionally, the lower the kurtosis, the lesser the chances of encountering extreme values.

Table 4
This table shows the numerical comparison between PoW, PoS, DPoS, PBFT, PoR and the proposed consensus algorithm. In bold are the top scores, indicating the most favourable interpretation of these statistics in relation to equality.

	PoW	PoS	DPoS	PBFT	PoR	Fuzzychain
Gini coefficient	0.5992	0.4934	0.4126	0.5147	0.3728	**0.1720**
Skewness	1.8855	1.5243	0.9630	1.5569	0.5201	**0.2243**
Kurtosis	3.3206	2.8247	1.3253	3.0123	0..6985	**−1.7489**

In Table 4, the Gini coefficient in Fuzzychain stands out as being notably lower than that of the other algorithms, indicating a higher degree of fairness in the selection of validators. The equitable consensus algorithm employed by Fuzzychain excels in promoting a more balanced distribution of validation responsibilities among network participants compared to its counterparts. A lower Gini coefficient suggests that Fuzzychain is successful in mitigating the concentration or centralisation of validation power, thereby fostering a more inclusive and democratic blockchain network. This enhanced equity in validator selection is crucial for maintaining the decentralisation and security of the network, as it reduces the risk of a single entity gaining disproportionate influence. The findings underscore the effectiveness of Fuzzychain's approach to consensus, emphasising its commitment to creating a robust and fair blockchain ecosystem.

7. Discussion

The proposed equitable consensus algorithm for Fuzzychain presents a distinctive approach to achieving consensus in blockchain networks, blending elements of proof of stake and fuzzy set theory. One notable feature is the incorporation of linguistic labels to represent participants' stakes within fuzzy sets. This introduces a level of fuzziness, enhancing the flexibility and expressiveness of stake representation. The algorithm's emphasis on reputation as a factor in participant selection during the mining process is noteworthy, promoting a fair and inclusive approach. The randomised selection of participants from each fuzzy set adds an element of unpredictability, preventing any single participant or group from consistently dominating the validation process. The utilisation of a voting mechanism based on the majority decision of participants ensures a collective and democratic approach to block validation. The rewarding of successful participants with both a commission for validations and an increase in reputation creates a positive incentive structure, motivating active and responsible participation. Conversely, the penalties imposed on unsuccessful participants, including a decrease in reputation and reduced chances of selection in the next round, contribute to maintaining a balance and encouraging continuous improvement.

The algorithm presents a consensus mechanism that addresses issues of fairness, security, and participant engagement in the Fuzzychain blockchain network. However, the practical implications and potential challenges of implementing such a system will require further exploration and empirical testing in real-world blockchain scenarios.

In this work, we have presented an equitable consensus algorithm. Nevertheless, it can be seen as a cryptography scheme because it can

work with the different types of membership functions that exist in fuzzy sets, for instance, triangular MF, trapezoidal MF, Gaussian MF, and generalised bell MF, among others. Similarly, it is possible to change the randomly chosen algorithm to another algorithm with a better performance in choosing the participants. Even more, the voting mechanism can be modified to make a decision efficient.

Usually, each fuzzy set has a different number of participants and is probably that this number is bigger in linguistic labels such as VL, L, M than H, and VH. Another important advantage of this proposed algorithm is that the participants in the Fuzzychain may move to other fuzzy sets where the participants are less than others. This is possible because the validator receives a commission to make the process correctly.

In the present iteration of our fair consensus algorithm, threshold values for reputation are defined as crisp, non-fuzzy values. In future works, explore the 'computing with words' technique to enhance this. The idea is to develop a system that dynamically modifies the fuzzified reputation each round based on a range of factors. These include the number of validators associated with each linguistic term, fluctuations in reputation metrics, and the average value of this data. By adopting this approach, the algorithm's resilience would be bolstered, making it more adaptable to shifts in real-world scenarios, such as sudden changes in the number of validators.

8. Conclusion

In this study, we have introduced an innovative approach to the PoS consensus algorithm within the blockchain domain, where validators' stakes are modelled using fuzzy logic values. We have also explored the performance of this PoS paradigm in an agent-based blockchain pool, as detailed in Section 6. In particular, the FuzzyChain algorithm consistently opts for validators from diverse groups, with a predominant selection of the Medium and High categories. However, unlike other PoS consensus methods, FuzzyChain ensures that any group, including lower-stakes validators, is not overlooked. This deliberate approach facilitates a more extensive distribution of rewarded stakes, particularly for well-minted transactions within the Fuzzychain framework. Notably, the flexibility of the Fuzzychain allows a selected validator to belong to any group without necessitating a predetermined precise probability for group selection. This flexible allocation of opportunities promotes an inclusive and unbiased approach to validator selection, strengthening the integrity of the transaction-solving process. It also enhances security by ensuring a broader distribution of validators, rather than concentrating control within an exclusive group of high-stake validators. Furthermore, while fostering diversity, FuzzyChain can also be integrated with a reputation-based mechanism to enable reputable validators to be rewarded more often and to be promoted to wealthier groups more quickly. Future iterations of the Fuzzychain will explore extensions involving sets capable of handling increased uncertainty, and alternative characteristics of the fuzzy stake will be considered to guide the selection process. These ongoing developments aim to further enhance the robustness and applicability of Fuzzychain within diverse blockchain-operative contexts.

CRediT authorship contribution statement

Bruno Ramos-Cruz: Writing – original draft, Methodology, Investigation, Conceptualization. **Javier Andreu-Perez:** Writing – review & editing, Supervision, Methodology, Conceptualization. **Francisco J. Quesada-Real:** Writing – review & editing, Methodology, Conceptualization. **Luis Martínez:** Writing – review & editing, Supervision, Methodology, Conceptualization.

Declaration of competing interest

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

Acknowledgement

We express our sincere gratitude to Dr. Prashant K. Gupta and Dr. Deepak Sharma for their early discussions on this work with Dr. Javier Andreu-Perez. This research was partially supported by the University of Jaén through its Research Support Operational Plan, Action 8a, awarded to the first author, and by the Talentia Senior Program of the Regional Ministry of Economy, Innovation, Science and Employment of Andalusia (Ref. 201899905497765).

Data availability

Data will be made available on request.

References

Aisbett, J., Rickard, J.T., Morgenthaler, D.G., 2010. Type-2 fuzzy sets as functions on spaces. IEEE Trans. Fuzzy Syst. 18 (4), 841–844. http://dx.doi.org/10.1109/TFUZZ.2010.2046176.

Alrowaily, M.A., Alghamdi, M., Alkhazi, I., Hassanat, A.B., Arbab, M.M.S., Liu, C.Z., 2023. Modeling and analysis of proof-based strategies for distributed consensus in blockchain-based peer-to-peer networks. Sustainability 15 (2), http://dx.doi.org/10.3390/su15021478, URL https://www.mdpi.com/2071-1050/15/2/1478.

Bach, L.M., Mihaljevic, B., Zagar, M., 2018. Comparative analysis of blockchain consensus algorithms. In: Skala, K., Koricic, M., Grbac, T.G., Cicin-Sain, M., Sruk, V., Ribaric, S., Gros, S., Vrdoljak, B., Mauher, M., Tijan, E., Pale, P., Janjic, M. (Eds.), 41st International Convention on Information and Communication Technology, Electronics and Microelectronics. MIPRO 2018, Opatija, Croatia, May 21-25, 2018, IEEE, pp. 1545–1550. http://dx.doi.org/10.23919/MIPRO.2018.8400278.

Back, A., et al., 2002. Hashcash-a denial of service counter-measure.

Bartoletti, M., Benetollo, L., Bugliesi, M., Crafa, S., Sasso, G.D., Pettinau, R., Pinna, A., Piras, M., Rossi, S., Salis, S., Spanò, A., Tkachenko, V., Tonelli, R., Zunino, R., 2025. Smart contract languages: A comparative analysis. Future Gener. Comput. Syst. 164, 107563. http://dx.doi.org/10.1016/j.future.2024.107563, URL https://www.sciencedirect.com/science/article/pii/S0167739X24005272.

BitShares Documentation, 2018. Delegated proof of stake (DPOS). https://how.bitshares.works/en/master/technology/dpos.html. ([Online] Last accessed 15 January 2024).

Chen, P., Chen, Y., Wang, X., Yuan, L., Tan, C., Yang, Y., 2024. A high-capacity slicing PBFT protocol based on reputation evaluation model. Wirel. Netw. 30 (9), 7469–7482. http://dx.doi.org/10.1007/s11276-023-03636-7.

Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., Cai, Z., 2022. A survey on blockchain systems: Attacks, defenses, and privacy preservation. High- Confid. Comput. 2 (2), 100048. http://dx.doi.org/10.1016/j.hcc.2021.100048, URL https://www.sciencedirect.com/science/article/pii/S2667295221000386.

Chen, W., Li, X., Wang, G., Li, L., Shen, J., Li, E., 2025. HML-BFT: Hybrid multi-layer BFT consensus with reputation model for large-scale blockchain. Peer- to- Peer Netw. Appl. 18 (1), 26. http://dx.doi.org/10.1007/s12083-024-01888-4.

Dehez-Clementi, M., Rabah, M., Ghamri-Doudane, Y., 2023. A privacy-preserving proof-of-reputation. In: 2023 IFIP NETWORKING CONFERENCE, IFIP NETWORKING. In: IFIP Networking Conference, Int Federat Informat Proc TC6; Huawei; Cisco; i2CAT Fdn; IEEE Commun Soc; i2CAT Foundation; Delft Univ Technol; Univ Girona, http://dx.doi.org/10.23919/IFIPNetworking57963.2023.10186422, 22nd International-Federation-for-Information-Processing (IFIP) Networking Conference (IFIP Networking), Univ Politecnica Catalunya Barcelonatech, Barcelona, SPAIN, JUN 12-15, 2023.

Delgado, M., Vila, M., Voxman, W., 1998. On a canonical representation of fuzzy numbers. Fuzzy Sets and Systems 93 (1), 125–135. http://dx.doi.org/10.1016/S0165-0114(96)00144-3.

Deng, Z., Tang, C., Li, T., He, D., 2024. Permissioned blockchain-based trusted and robust consensus optimization orienting intelligent transportation systems. IEEE Trans Intell. Transp. Syst. http://dx.doi.org/10.1109/TITS.2024.3496553.

Du, D., Feng, W., Huang, M., Feng, S., Wang, J., 2024. Improvement of PBFT consensus algorithm based on affinity propagation clustering in intellectual property transaction scenarios. Electronics 13 (10), http://dx.doi.org/10.3390/electronics13101809.

Du, Z., Zhang, J., Fu, Y., Huang, M., Liu, L., Li, Y., 2023. A scalable and trust-value-based consensus algorithm for internet of vehicles. Appl. Sci.- Basel 13 (19), http://dx.doi.org/10.3390/app131910663.

Dwork, C., Naor, M., 1992. Pricing via processing or combatting junk mail. In: Brickell, E.F. (Ed.), Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings. In: Lecture Notes in Computer Science, vol. 740, Springer, pp. 139–147. http://dx.doi.org/10.1007/3-540-48071-4_10.

Elgamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory 31 (4), 469–472. http://dx.doi.org/10.1109/TIT.1985.1057074.

Ethereum, 2023a. Ethereum Mainnet for enterprise. https://ethereum.org/en/. [Online] Last accessed 8 December 2023.

Ethereum, 2023b. Proof-of-stake (POS). https://ethereum.org/developers/docs/consensus-mechanisms/pos. ([Online] Last accessed 15 January 2024).

Eyal, I., Sirer, E.G., 2018. Majority is not enough: bitcoin mining is vulnerable. Commun. ACM 61 (7), 95–102. http://dx.doi.org/10.1145/3212998.

Fahim, S., Rahman, S., Mahmood, S., 2023. Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV. Int. J. Math. Sci. Comput. 3, 46–57.

Ferdous, M.S., Chowdhury, M.J.M., Hoque, M.A., 2021. A survey of consensus algorithms in public blockchain systems for crypto-currencies. J. Netw. Comput. Appl. 182, 103035. http://dx.doi.org/10.1016/j.jnca.2021.103035, URL https://www.sciencedirect.com/science/article/pii/S1084804521000618.

Gan, C., Xiao, X., Zhang, Y., Zhu, Q., Bi, J., Jain, D.K., Saini, A., 2025. An asynchronous federated learning-assisted data sharing method for medical blockchain. Appl. Intelligence 55 (2), http://dx.doi.org/10.1007/s10489-024-06172-9.

Gemeliarana, I.G.A.K., Sari, R.F., 2018. Evaluation of proof of work (POW) blockchains security network on selfish mining. In: 2018 International Seminar on Research of Information Technology and Intelligent Systems. ISRITI, pp. 126–130. http://dx.doi.org/10.1109/ISRITI.2018.8864381.

Górski, T., 2024. AdapT: A reusable package for implementing smart contracts that process transactions of congruous types. Softw. Impacts 21, 100694. http://dx.doi.org/10.1016/j.simpa.2024.100694, URL https://www.sciencedirect.com/science/article/pii/S2665963824000824.

Hao, X., Yeoh, P.L., She, C., Vucetic, B., Li, Y., 2024. Secure deep reinforcement learning for dynamic resource allocation in wireless MEC networks. IEEE Trans. Commun. 72 (3), 1414–1427. http://dx.doi.org/10.1109/TCOMM.2023.3337376.

Herrera, F., Herrera-Viedma, E., Martinez, L., 2008. A fuzzy linguistic methodology to deal with unbalanced linguistic term sets. IEEE Trans. Fuzzy Syst. 16 (2), 354–370. http://dx.doi.org/10.1109/TFUZZ.2007.896353.

Hu, Z., Liu, B., Shen, A., Luo, J., 2024. Blockchain-based resource allocation mechanism for the internet of vehicles: Balancing efficiency and security. IEEE Trans. Netw. Serv. Manag. 21 (4), 3971–3987. http://dx.doi.org/10.1109/TNSM.2024.3387931.

Hussain, M., Mehmood, A., Khan, M.A., Khan, R., Lloret, J., 2025. Reputation-based leader selection consensus algorithm with rewards for blockchain technology. Computers 14 (1), http://dx.doi.org/10.3390/computers14010020.

Jahid, A., Alsharif, M.H., Hall, T.J., 2023. The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap. J. Netw. Comput. Appl. 217, 103677. http://dx.doi.org/10.1016/j.jnca.2023.103677, URL https://www.sciencedirect.com/science/article/pii/S1084804523000966.

Jain, A., Sharma, A., 2020. Membership function formulation methods for fuzzy logic systems: A comprehensive review. J. Crit. Rev. 7 (19), 8717–8733.

Jia, G., Shen, Z., Sun, H., Xin, J., Wang, D., 2025. RWA-BFT: Reputation-weighted asynchronous BFT for large-scale IoT. SENSORS 25 (2), http://dx.doi.org/10.3390/s25020413.

Johnson, D., Menezes, A., Vanstone, S.A., 2001. The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Sec. 1 (1), 36–63. http://dx.doi.org/10.1007/s102070100002.

Koblitz, N., 1994. A Course in Number Theory and Cryptography, second ed. In: Graduate Texts in Mathematics, vol. 114, Springer.

Kumar, A., Vishwakarma, L., Das, D., 2023. R-PBFT: A secure and intelligent consensus algorithm for Internet of vehicles. Veh. Commun. 41, 100609. http://dx.doi.org/10.1016/j.vehcom.2023.100609, URL https://www.sciencedirect.com/science/article/pii/S2214209623000396.

Lamport, L., Shostak, R.E., Pease, M.C., 1982. The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 4 (3), 382–401. http://dx.doi.org/10.1145/357172.357176.

Larimer, D., 2013. Transactions as proof-of-stake Nov- 2013 909.

Larimer, D., 2014. Delegated proof-of-stake (dpos). Bitshare Whitepaper 81, 85.

Li, J., Cao, L., Zhao, S., Wan, J., Bai, J., 2024a. LC-PBFT: Layered cross-chain consensus algorithm based on forest topology. J. Supercomput. 80 (12), 17849–17873. http://dx.doi.org/10.1007/s11227-024-06122-9.

Li, S., Deng, X., Zou, Y., 2024b. RR-Raft: A raft consensus algorithm based on reputation regression model and RSA signature. In: 2024 2ND INTERNATIONAL CONFERENCE on MOBILE INTERNET, CLOUD COMPUTING and INFORMATION SECURITY. MICCIS 2024, pp. 92–96. http://dx.doi.org/10.1109/MICCIS63508.2024.00024, 2nd International Conference on Mobile Internet, Cloud Computing and Information Security (MICCIS), Changsha, PEOPLES R CHINA, APR 19-21, 2024.

Li, Z., Wang, J., Li, Y., 2025. An improved PBFT consensus algorithm based on reputation and gaming. J. Supercomputing 81 (1), http://dx.doi.org/10.1007/s11227-024-06822-2.

Liu, Y., Liu, Z., Zhang, Q., Su, J., Cai, Z., Li, X., 2024. Blockchain and trusted reputation assessment-based incentive mechanism for healthcare services. Future Gener. Comput. Syst.- Int. J. Esci. 154, 59–71. http://dx.doi.org/10.1016/j.future.2023.12.023.

Liu, Y., Xu, G., 2021. Fixed degree of decentralization DPoS consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value. Comput. Netw. 199, 108432. http://dx.doi.org/10.1016/j.comnet.2021.108432, URL https://www.sciencedirect.com/science/article/pii/S1389128621003947.

Liu, G., Yan, Z., Feng, W., Jing, X., Chen, Y., Atiquzzaman, M., 2021. SeDID: An SGX-enabled decentralized intrusion detection framework for network trust evaluation. Inf. Fusion 70, 100–114. http://dx.doi.org/10.1016/j.inffus.2021.01.003, URL https://www.sciencedirect.com/science/article/pii/S1566253521000099.

Maung Maung Thin, W.Y., Dong, N., Bai, G., Dong, J.S., 2018. Formal analysis of a proof-of-stake blockchain. In: 2018 23rd International Conference on Engineering of Complex Computer Systems. ICECCS, pp. 197–200. http://dx.doi.org/10.1109/ICECCS2018.2018.00031.

Mendel, J.M., 2017. Uncertain Rule-Based Fuzzy Systems; Introduction and New Directions. Springer.

Menezes, J., Katz, A.J., Van Oorschot, P.C., Vanstone, S.A., 1996. Handbook of Applied Cryptography. CRC Press.

Miller, G., 1994. The magical number seven or minus two: some limits on our capacity of processing information. Psychol. Rev. V63 81–97.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus. Rev.

Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., Dutkiewicz, E., 2019. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. IEEE Access 7, 85727–85745. http://dx.doi.org/10.1109/ACCESS.2019.2925010.

Padma, A., Ramaiah, M., 2025. Lightweight privacy preservation blockchain framework for healthcare applications using GM-SSO. Results Eng. 25, http://dx.doi.org/10.1016/j.rineng.2024.103882.

Panda, S.K., Jena, A.K., Swain, S.K., Satapathy, S.C., 2021. Blockchain technology: applications and challenges. Intell. Syst. Ref. Libr.

Pérez, A.T.E., Rossit, D.A., Tohmé, F., Vásquez, Ó.C., 2022. Mass customized/personalized manufacturing in Industry 4.0 and blockchain: Research challenges, main problems, and the design of an information architecture. Inf. Fusion 79, 44–57. http://dx.doi.org/10.1016/J.INFFUS.2021.09.021.

Pilkington, M., 2016. 11 blockchain technology: principles and applications. Res. Handb. Digit. Transform. 225 (2016).

Rivest, R.L., Shamir, A., Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21 (2), 120–126. http://dx.doi.org/10.1145/359340.359342.

Rui, L., Zhao, L., Yan, J., Qiu, X., Guo, S., 2024. Trusted authentication mechanism of IoT terminal based on authorization consensus and reputation evaluation. IEEE Internet Things J 11 (13), 23961–23976. http://dx.doi.org/10.1109/JIOT.2024.3387448.

Saad, S.M.S., Radzi, R.Z.R.M., Othman, S.H., 2021. Comparative analysis of the blockchain consensus algorithm between proof of stake and delegated proof of stake. In: 2021 International Conference on Data Science and Its Applications. ICoDSA, pp. 175–180. http://dx.doi.org/10.1109/ICoDSA53588.2021.9617549.

Saleh, F., 2021. Blockchain without waste: Proof-of-stake. Rev. Financ. Stud. 34 (3), 1156–1190. http://dx.doi.org/10.1093/rfs/hhaa075, arXiv:https://academic.oup.com/rfs/article-pdf/34/3/1156/36264598/hhaa075.pdf.

Sanka, A.I., Cheung, R.C., 2021. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. J. Netw. Comput. Appl. 195, 103232. http://dx.doi.org/10.1016/j.jnca.2021.103232, URL https://www.sciencedirect.com/science/article/pii/S1084804521002307.

Sankar, L.S., Sindhu, M., Sethumadhavan, M., 2017. Survey of consensus protocols on blockchain applications. In: 2017 4th International Conference on Advanced Computing and Communication Systems. ICACCS, pp. 1–5. http://dx.doi.org/10.1109/ICACCS.2017.8014672.

Singh, C.P., Yamaganti, R., Umrao, L.S., 2025. Variational Onsager Neural Networks-based fair proof-of-reputation consensus for blockchain with transaction prioritisation for smart cities. J. Supercomputing 81 (1), http://dx.doi.org/10.1007/s11227-024-06626-4.

Su, Z., Cheng, R., Li, C., Chen, M., Zhu, J., Long, Y., 2025. Federated learning and reputation-based node selection scheme for internet of vehicles. Electronics 14 (2), http://dx.doi.org/10.3390/electronics14020303.

Swan, M., 2015. Blockchain: Blueprint for a New Economy, first ed. O'Reilly Media, Inc.

Tang, F., Xu, T., Peng, J., Gan, N., 2024. TP-PBFT: A scalable PBFT based on threshold proxy signature for IoT-blockchain applications. IEEE Internet Things J. 11 (9), 15434–15449. http://dx.doi.org/10.1109/JIOT.2023.3347232.

Vashchuk, O., Shuwar, R., 2018. 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. 9 (9), 106–112.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., Wang, F.-Y., 2019. Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Trans. Syst. Man, Cybern.: Syst. 49 (11), 2266–2277. http://dx.doi.org/10.1109/TSMC.2019.2895123.

Wang, B., Tian, Z., Liu, X., Xia, Y., She, W., Liu, W., 2025. A multi-center federated learning mechanism based on consortium blockchain for data secure sharing. Knowl.- Based Syst. 310, http://dx.doi.org/10.1016/j.knosys.2025.112962.

Wen, X., Yang, X., 2024. MAPBFT: multilevel adaptive PBFT algorithm based on discourse and reputation models. Comp. J. http://dx.doi.org/10.1093/comjnl/bxae137.

Wendl, M., Doan, M.H., Sassen, R., 2023. The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. J. Environ. Manag. 326, 116530. http://dx.doi.org/10.1016/j.jenvman.2022.116530, URL https://www.sciencedirect.com/science/article/pii/S030147972202103X.

Wu, X., Meng, T., Huang, H., Liu, L., Zhang, J., 2024. A hybrid consensus algorithm for collaborative protection of multi-domain education data. J. Internet Technol. 25 (7), 963–975. http://dx.doi.org/10.70003/160792642024122507002.

Xu, J., Wang, C., Jia, X., 2023a. A survey of blockchain consensus protocols. ACM Comput. Surv. 55 (13s), http://dx.doi.org/10.1145/3579845.

Xu, G., Yao, T., Zhang, K., Meng, X., Liu, X., Xiao, K., Chen, X., 2023b. An optimized Byzantine fault tolerance algorithm for medical data security. Electronics 12 (24), http://dx.doi.org/10.3390/electronics12245045.

Yang, N., Tang, C., Xiong, Z., Chen, Q., Kang, J., He, D., 2024. SG-FCB: a stackelberg game-driven fair committee-based blockchain consensus protocol. In: 44th IEEE International Conference on Distributed Computing Systems. ICDCS 2024, Jersey City, NJ, USA, July 23-26, 2024, IEEE, pp. 403–414. http://dx.doi.org/10.1109/ICDCS60910.2024.00045.

Ye, J., Hu, H., Liang, J., Yin, L., Kang, J., 2024. Lightweight adaptive Byzantine fault tolerant consensus algorithm for distributed energy trading. Comput. Netw 251, http://dx.doi.org/10.1016/j.comnet.2024.110635.

Zadeh, L., 1965. Fuzzy sets. Inf. Control 8 (3), 338–353. http://dx.doi.org/10.1016/S0019-9958(65)90241-X, URL https://www.sciencedirect.com/science/article/pii/S001999586590241X.

Zadeh, L., 1975. The concept of a linguistic variable and its application to approximate reasoning—I. Inform. Sci. 8 (3), 199–249. http://dx.doi.org/10.1016/0020-0255(75)90036-5, URL https://www.sciencedirect.com/science/article/pii/0020025575900365.

Zadeh, L., 1999. From computing with numbers to computing with words. From manipulation of measurements to manipulation of perceptions. IEEE Trans. Circuits Syst. I 46 (1), 105–119. http://dx.doi.org/10.1109/81.739259.

Zhang, H., Fan, W., Wang, J., 2024a. Bidirectional utilization of blockchain and privacy computing: Issues, progress, and challenges. J. Netw. Comput. Appl. 222, 103795. http://dx.doi.org/10.1016/j.jnca.2023.103795, URL https://www.sciencedirect.com/science/article/pii/S108480452300214X.

Zhang, S., Tian, H., Wang, L., Xu, S., Shao, W., 2024b. A reputation-based dynamic reorganization scheme for blockchain network sharding. Connection Sci. 36 (1), http://dx.doi.org/10.1080/09540091.2024.2327438.

Zhang, Y., Wang, W., Shi, F., 2024c. Reputation-based Raft-Poa layered consensus protocol converging UAV network. Comput. Netw. 240, http://dx.doi.org/10.1016/j.comnet.2024.110170.

Zhang, S., Zheng, K., Wang, B., 2024d. A V2V electricity transaction scheme with privacy protection based on the internet of vehicles and consortium blockchain. Int. J. Electr. Power Energy Syst. 157, http://dx.doi.org/10.1016/j.ijepes.2024.109789.

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2018. Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. 14 (4), 352–375. http://dx.doi.org/10.1504/IJWGS.2018.10016848.

Zhou, L., Fu, Y., Zhao, P., Liu, S., Chang, T., Li, C., 2023. Hierarchical Blockchain-enabled Federated Learning with Reputation Management for Mobile Internet of Vehicles. In: 2023 IEEE 97TH VEHICULAR TECHNOLOGY CONFERENCE, VTC2023-SPRING. In: IEEE Vehicular Technology Conference Proceedings, IEEE; Huawei; IEEE VTS, http://dx.doi.org/10.1109/VTC2023-Spring57618.2023.10200733, 97th IEEE Vehicular Technology Conference (VTC-Spring), Florence, ITALY, JUN 20-23, 2023.

Zhu, Q., Jing, A., Gan, C., Guan, X., Qin, Y., 2023. HCSC: A hierarchical certificate service chain based on reputation for VANETs. IEEE Trans. Intell. Transp. Syst. 24 (6), 6123–6145. http://dx.doi.org/10.1109/TITS.2023.3250279.