Blockchain: Research and Applications 6 (2025) 100302

Contents lists available at ScienceDirect

Blockchain: Research and Applications

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

Review Article

Enhancing blockchain consensus mechanisms: A comprehensive survey on machine learning applications and optimizations

Syamsul Rizal [a,c], Dong-Seong Kim [a,b,*]

[a] ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, Republic of Korea
[b] Industrial Academic Cooperation Foundation, Kumoh National Institute of Technology, Gumi 39177, Republic of Korea
[c] School of Electrical Engineering, Telkom University, Bandung 40257, Indonesia

ARTICLE INFO

Keywords:
Blockchain
Consensus algorithm
Machine learning

ABSTRACT

This research examines the incorporation of artificial intelligence (AI) in blockchain consensus algorithms, presenting an extensive overview of current improvements and anticipated effects. We conduct a thorough examination of a diverse array of academic sources, encompassing AI methodologies such as machine learning (ML) techniques—including deep learning and reinforcement learning—applied to blockchain consensus mechanisms. The study highlights critical areas where AI can bolster blockchain performance, including enhancing effectiveness, dependability, and flexibility. Despite the promising benefits that AI integration offers, it also presents complexities and potential security risks, including data centralization and increased computational power requirements. In this analysis, we review the risks and examine the proposed mitigation strategies from existing studies, such as federated learning to preserve data privacy, secure multi-party computation (SMPC) to protect sensitive data, and decentralized AI marketplaces to distribute AI resources fairly. This study makes a significant contribution to the field by emphasizing the dual potential of AI to both improve and challenge blockchain systems. By advocating for balanced approaches that prioritize decentralization and security, our findings aim to provide direction for future research and practical applications in this multidisciplinary field.

1. Introduction

Over the past few years, the digital environment has undergone a significant transformation, largely due to the emergence and adoption of blockchain technology. At its essence, blockchain promotes a decentralized approach, which facilitates peer-to-peer interactions without the need for intermediaries, and affords unparalleled levels of transparency, security, and dependability [1–4]. At the heart of this groundbreaking technology is the consensus algorithm, which ensures that all participants in a distributed network collectively concur on the status of the shared ledger, thereby safeguarding the integrity and security of its transactions [5–7].

Blockchain technology, distinguished by its decentralized and immutable features, encounters several obstacles, such as scalability, throughput, and environmental concerns [8]. These challenges emphasize the necessity for innovative and adaptive strategies to improve conventional consensus methodologies. This paper examines current methods and proposes novel methodologies to surmount these barriers, concentrating particularly on mitigating the environmental influence of incorporating artificial intelligence (AI) into blockchain systems.

Parallel to blockchain's rise, AI, especially machine learning (ML), has made substantial inroads into various sectors. The advantages of AI in pattern recognition, predictive modeling, and optimization [9] make it an appealing solution for tackling the complexities and challenges of blockchain consensus algorithms. By leveraging AI, several questions arise: Can we predict transaction validation sequences to expedite processes? Is it feasible to utilize AI-driven analytics for real-time detection of potential security breaches? Could we develop AI-guided adaptive consensus algorithms that respond dynamically to network demand?

1.1. Environmental impact

Blockchain technology's environmental impact is a matter of grave concern, particularly in relation to its electricity consumption. The non-AI blockchains, especially those that use proof of work (PoW) consensus mechanisms, consume substantial amounts of electricity. For instance, the Bitcoin network's estimated annual electricity consumption is around 145.35 TWh in 2023. This high energy usage results in a substantial carbon footprint, with estimates indicating that Bitcoin mining alone produces approximately 96.08 megatons of CO_2 annually [10].

* Corresponding author.
E-mail address: dskim@kumoh.ac.kr (D.-S. Kim).

https://doi.org/10.1016/j.bcra.2025.100302
Received 1 December 2023; Received in revised form 13 August 2024; Accepted 11 February 2025

Available online 8 May 2025

1.2. Scalability and throughput

One of the key difficulties that must be addressed is the issue of scalability and throughput. The public blockchains that are currently in use, such as Bitcoin and Ethereum, have a restricted capacity for the number of transactions that can be processed per second (TPS). Bitcoin, for instance, can handle roughly 7 TPS, while Ethereum has a capacity of approximately 15 TPS. The limitations imposed by these constraints pose obstacles to the extensive utilization of blockchain technology in high-volume applications, which is a significant challenge that must be tackled.

These obstacles emphasize the need for innovative and adaptive techniques to enhance conventional consensus methodologies. This paper critically examines existing methodologies and proposes novel approaches to overcome these challenges, including the incorporation of AI to increase productivity and minimize environmental consequences.

1.3. Organization of the paper

The remainder of this paper is organized as follows:

- **Section 2** provides an overview of blockchain technology and AI, setting the context for their integration.
- **Section 3** explains the systematic approach adopted in this study, including the literature review process and case study analysis.
- **Section 4** discusses how AI can optimize consensus algorithms, including recent advancements and methodologies.
- **Section 5** presents the findings of the study, detailing the performance metrics and their implications.
- **Section 6** addresses the key challenges of integrating AI into blockchain, such as data privacy, computational overhead, and security.
- **Section 7** presents real-world examples where AI has been integrated into blockchain applications, demonstrating the practical benefits and challenges.
- **Section 8** discusses strategies to overcome the identified challenges in AI and blockchain integration.
- **Section 9** outlines potential research areas and technological advancements that could further enhance AI and blockchain integration.
- **Section 10** summarizes the key findings and suggests future research directions.

1.4. Distinction from existing studies

Our review differs from existing studies in several significant ways:

- **Comprehensive scope**. Our review encompasses a broader scope by integrating various AI techniques (supervised learning, unsupervised learning, reinforcement learning, and deep learning) with blockchain technology, specifically focusing on enhancing efficiency, security, adaptability, and consensus mechanisms. Existing studies often focus narrowly on specific AI techniques or particular blockchain applications without providing a holistic view.
- **Systematic literature review methodology**. We employ a systematic literature review methodology, covering a wide range of academic articles, conference papers, and technical reports published between 2010 and 2023. This approach ensures a thorough and unbiased selection of relevant literature, which is detailed in Section 3.
- **Novel integration framework**. Our review introduces a conceptual framework that outlines the potential interactions between AI and blockchain technology, which is not typically found in existing literature. This framework helps to identify and categorize the various ways AI can enhance blockchain applications.
- **Identification of research gaps and future directions**. We not only review the current state of research but also identify significant gaps and propose future research directions to address these gaps. This proactive approach helps in setting a clear agenda for future studies, which is often lacking in existing reviews.
- **Recent developments and case studies**. The inclusion of recent studies and case studies provides practical insights and examples of how AI is currently being implemented in blockchain technology. This practical perspective is crucial for understanding the real-world applications and potential of AI-enhanced blockchain systems.

By addressing these aspects, our review provides a more comprehensive, systematic, and forward-looking analysis compared to existing studies. This distinction makes our work a valuable contribution to the literature on AI-enhanced blockchain technology.

2. Background

2.1. Blockchain

The rise of blockchain technology has led to a significant shift in the digital landscape by eliminating the need for intermediaries in peer-to-peer interactions and ensuring unprecedented levels of transparency, security, and trust [1–4]. Decentralized in nature, blockchain relies on consensus algorithms to maintain the integrity of a shared ledger in distributed networks, providing a foundation for applications such as cryptocurrencies and smart contracts. However, challenges related to scalability, throughput, and environmental concerns have emerged, necessitating the exploration of innovative solutions to enhance traditional methodologies.

2.1.1. Transactions

In the context of blockchain, a transaction refers to any action that results in a modification of stored data. For cryptocurrencies, a transaction usually involves the transfer of currency between digital addresses [11,12]. Each transaction is assigned a unique identifier and contains important information such as the sender and recipient addresses, the transacted amount, and a timestamp. Before being added to the blockchain, network participants meticulously validate each transaction.

2.1.2. Blocks

In blockchain technology, transactions are compiled into structures known as blocks, which function as containers that record and preserve the details of each transaction [13]. As transactions occur, they are subjected to verification and added to a block until a predetermined number is reached. Upon reaching this threshold, the block is considered “closed,” meaning it is completed and no new transactions can be added to it. This closed block is then assigned a unique digital fingerprint, known as a cryptographic hash, which serves as a secure and unforgeable identifier.

Every new block created in a blockchain is assigned a unique identifier that connects it to the preceding block, thus creating a chain of blocks. This unique identifier guarantees that any changes made to the information within a completed block would disrupt the continuity of the chain, thereby providing a record of tampering and upholding the blockchain’s principle of immutability [14]. As a result, the integrity of the entire transaction history is strengthened, making the recorded transaction data permanent and trustworthy. In essence, once recorded on a blockchain, transaction data are secure and unalterable.

Fig. 1 illustrates the architecture of the blockchain, highlighting the intricate structure of individual blocks and the role of the Merkle Tree in verifying transactions. Each block in the chain contains a timestamp indicating its creation time, a unique identifier known as the hash, a reference to the previous block hash, a random value called the

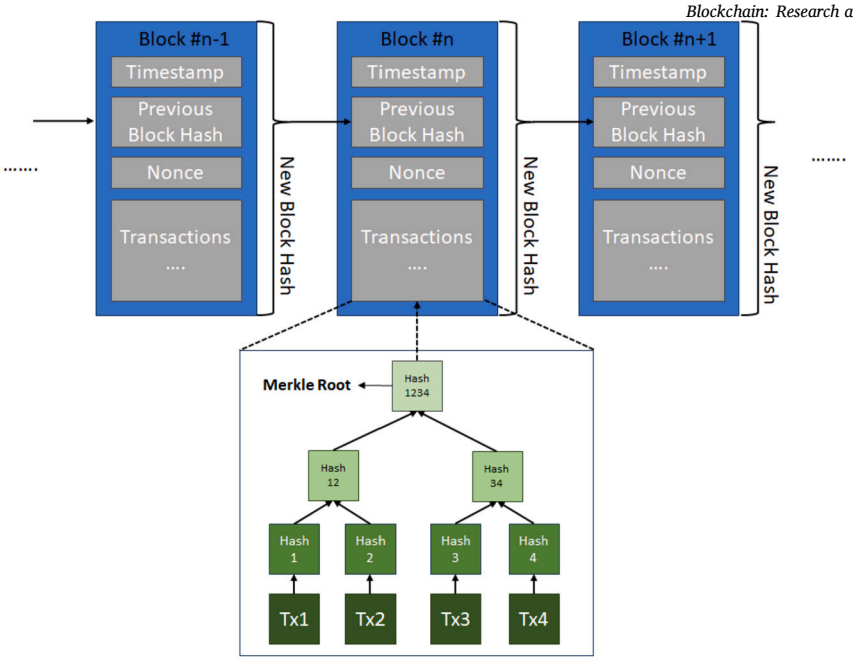

Fig. 1. Blockchain structure and transaction verification.

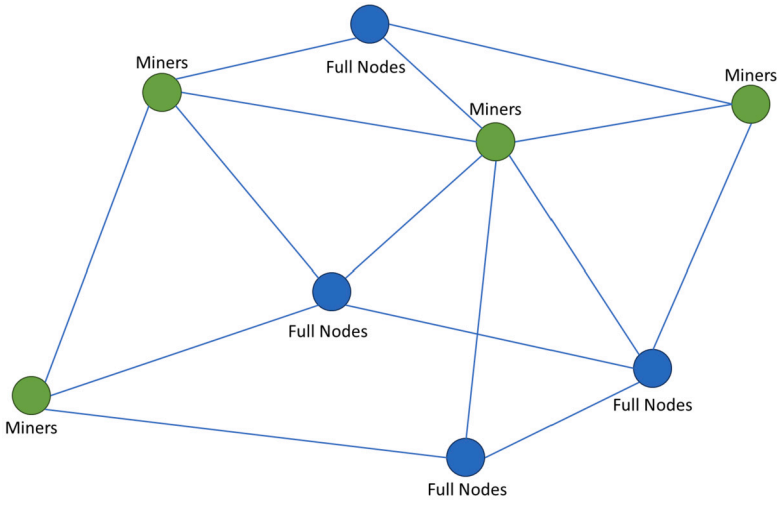

Fig. 2. Schematic representation of the decentralized interactions between miners and full nodes in a blockchain network.

nonce, and a set of transactions. The interconnectedness of the blocks is clear through the bond formed by their respective hashes, ensuring the blockchain's chronological sequence and integrity. Any alteration of information within a block undermines this bond, rendering subsequent blocks invalid.

The Merkle Tree's inclusion in Fig. 1 emphasizes its crucial role in the blockchain's efficiency and security, as highlighted by Refs. [15,16]. Each transaction is assigned a unique hash [17], and pairs of these hashes are combined and re-hashed to form a new set of combined hashes. This process continues until a single hash, the Merkle Root, is derived, which encapsulates all the block's transactions, allowing for rapid and secure transaction verification. The representation in Fig. 1 also emphasizes the blockchain's resilience and tamper-resistant nature, given its meticulous design and verification processes.

2.1.3. Decentralization

Blockchains differ from traditional systems in that they are decentralized, with multiple nodes maintaining a copy of the entire blockchain and collaborating to validate transactions [18–20]. Decentralization improves security by making it challenging for any single party to manipulate the data, while transparency fosters trust by enabling everyone to view transactions on the blockchain.

Fig. 2 demonstrates the interconnected nature of participants in a typical blockchain network. Miners, depicted as green circles, and full nodes, depicted as blue circles, are two distinct entities in the blockchain network. Miners validate and add new transactions to the blockchain, maintaining the network's security and integrity. Full nodes, which store a copy of the entire blockchain, verify the authenticity of transactions, acting as a robust check against potential malicious activities. The connecting lines in the figure symbolize the decentralized nature of the blockchain network, indicating that each participant communicates with multiple peers, ensuring a constant state of synchronization and consensus across the network. This structure ensures that the blockchain remains functional and secure even if a single participant, or even several, were to act maliciously or face an outage, showcasing the blockchain's resilient and decentralized design.

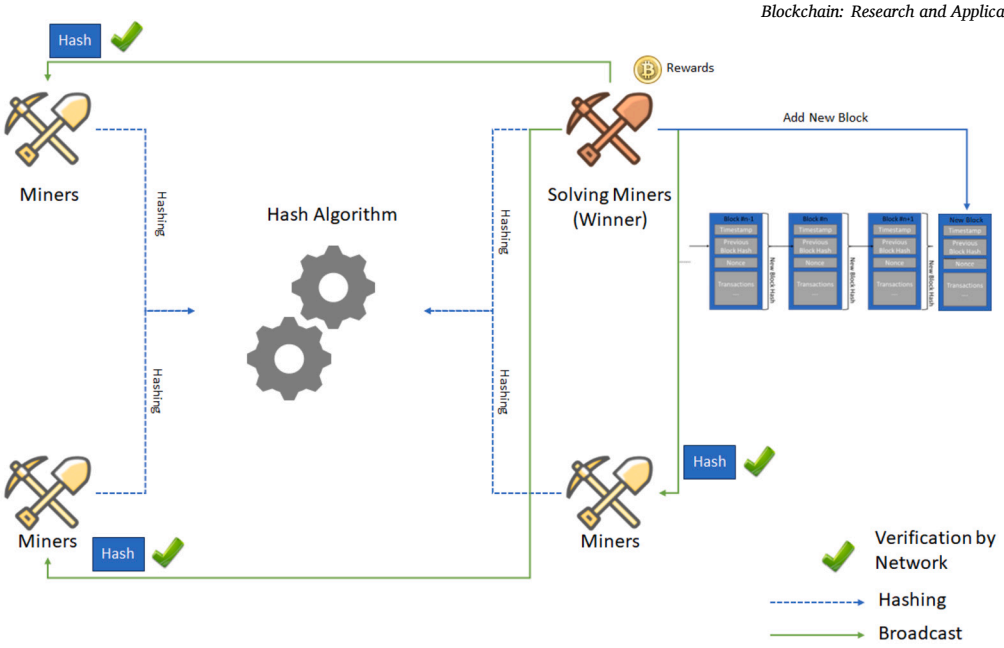

Fig. 3. Proof of work consensus mechanism in cryptocurrency mining.

2.2. Consensus algorithm

The consensus algorithm plays a crucial role as the foundation that guarantees that all members of a blockchain network concur on the state of a distributed ledger. Its primary objective is to promote agreement among the distributed nodes on the validity of transactions, ensuring that each participant in the network has an identical copy of the ledger. This is because of the decentralized nature of these systems, where there is no central authority to validate transactions. Instead, network participants collectively validate and record transactions on the blockchain. Different consensus mechanisms are designed to address various challenges such as security, scalability, and energy efficiency [21].

2.2.1. Proof of work

PoW is widely recognized as a consensus algorithm that was popularized by Bitcoin and is considered a pioneer in the blockchain industry. It operates by requiring participants, known as miners, to compete in solving complex mathematical puzzles [22,23]. The first miner to provide a solution is rewarded with the privilege of adding the next block to the blockchain, a process commonly referred to as mining. This computational process requires significant computational power and energy [24].

The primary advantage of PoW lies in its security, as the significant computational effort required to add a block makes it prohibitively expensive for malicious actors to alter any information in the blockchain. In order to successfully conduct a double-spending attack or alter past transactions, an attacker would need to control more than 50% of the network's total computational power, which is practically unfeasible for major blockchains [25].

However, PoW also has its critics. One of the primary concerns is the high energy consumption associated with its competitive nature, which requires continuous and intensive computational work. As a result, there are growing calls for more energy-efficient consensus algorithms due to the environmental concerns associated with PoW [26].

Furthermore, as the difficulty level of puzzles increases and the computing power required becomes more expensive, there is a growing centralization risk, as only a few entities can afford the massive infrastructure required for mining [27].

Fig. 3 provides a clear explanation of the PoW consensus mechanism as it pertains to cryptocurrency mining. The illustration depicts multiple mining icons representing various nodes or miners actively participating in the PoW algorithm by solving a cryptographic puzzle through hashing. The process of puzzle-solving is fundamental to PoW, as miners compete to find a specific value (or nonce) that, when hashed, produces a result that meets a predetermined condition.

Miners work tirelessly to solve intricate mathematical problems, and upon verification of a successful solution, the miner is designated as the "solver." This accomplishment is denoted by the green check mark adjacent to the hash symbol. As a token of appreciation for their efforts, the solver is granted a certain amount of Bitcoin, which serves as a testament to the incentive structure of the PoW mechanism. The reward motivates miners to continue offering their computational resources to the network.

Following the rewarding phase, the miner endeavors to add a new block to the blockchain. The diagram depicts the blockchain's uninterrupted flow, illustrating a succession of interconnected blocks. The most recent block, enhanced with fresh transactional data, is attached to the chain.

The figure demonstrates the competitive and reward-driven characteristics of the PoW mechanism, including the cryptographic puzzle-solving and collaborative verification processes that are fundamental to the security and reliability of blockchains. The process commences with a successful block addition by a solver, but it does not conclude there. The entire miner network must verify this new block, ensuring the validity and trustworthiness of the blockchain. The arrows indicating "Verification by Network Hashing" and "Broadcast" emphasize the importance of the peer verification phase. Achieving consensus from a majority of the network is necessary for the new block to permanently join the blockchain.

2.2.2. Proof of stake

The proof of stake (PoS) consensus mechanism deviates from the PoW mechanism by using a distinct method to authenticate transactions and reach consensus within a blockchain network. Unlike PoW, which mandates the involvement of miners to solve complex mathematical problems in order to validate transactions, PoS employs an alternative strategy.

In a PoS system, validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to lock up as collateral. The likelihood of being chosen to validate a block increases in

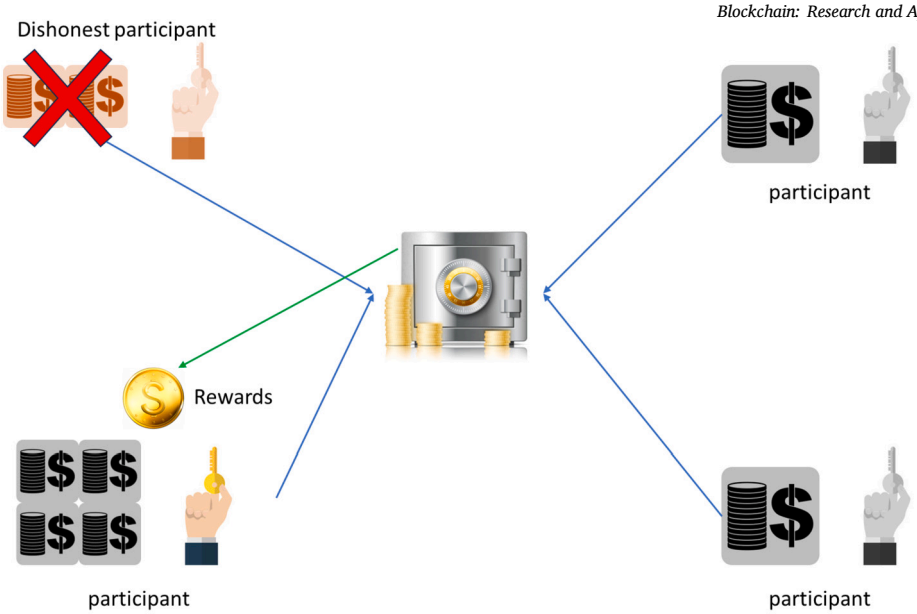

Fig. 4. Proof of stake consensus mechanism.

proportion to the amount of cryptocurrency staked, and this mechanism serves as a strong commitment from participants, as they risk losing their staked assets in the event of a failed validation attempt [28–30].

The core advantage of the PoS consensus mechanism is its energy efficiency, which has been proven in various studies [31,32]. In contrast to PoW, which requires significant computational power and thus consumes large amounts of energy, PoS achieves consensus without the need for resource-intensive calculations, making it a more environmentally friendly option. This not only contributes to a cleaner and healthier planet but also leads to faster transaction validations.

Moreover, PoS provides a built-in security measure, as validators have a stake in the network. They are motivated to validate transactions correctly since any misbehavior or malicious intent could result in the forfeiture of their stake, making it economically unviable to attack the network.

To further illustrate this concept, consider PoS as a bank's term deposit. By locking away a portion of your funds for a predetermined period, you earn interest. In the realm of blockchain, staking your coins grants you the opportunity to participate in validating transactions, and if selected, you receive rewards for your service.

Fig. 4 depicts a secure vault or safe, representing the protected nature of a blockchain in a PoS system. The vault is surrounded by various participants, each holding different amounts of coins or tokens, symbolizing stakeholders in the PoS mechanism who "stake" or lock up their cryptocurrency as collateral to participate in the network's validation process.

In the left of Fig. 4, a participant is shown with a red cross above them, indicating a "dishonest participant." This highlights the PoS principle, where malicious actors or those attempting to cheat the system risk losing their staked cryptocurrency as a penalty.

A golden coin labeled "Rewards" is emitted from the vault towards one of the participants, demonstrating the incentive mechanism in PoS. Validators, after successfully adding a new block to the chain or validating transactions, are rewarded with cryptocurrency.

The connecting lines between the vault and the participants illustrate the dynamic relationship between the network and its validators. Validators are chosen based on the amount they have staked, often with those staking larger amounts or for longer durations having a higher probability of being selected. Once chosen, these validators propose and verify new blocks in the blockchain, ensuring its integrity and security.

Overall, the figure effectively captures the essence of the PoS mechanism, emphasizing security, stake-based validation, rewards, and the potential risks for dishonest participants.

2.2.3. Delegated proof of stake

In Fig. 5, the delegated proof of stake (DPoS) consensus mechanism is presented in an easy-to-understand manner. The central part of Fig. 5 depicts a circle of coin holders, symbolizing the decentralized nature of the community. These coin holders actively participate in the voting process, as indicated by the arrows pointing towards their elected representatives [33,34]. A subset of these coin holders, referred to as the "Elected Delegates Circle," are chosen as validators who are responsible for validating transactions and creating blocks, emphasized by the centralized "Block Production" cube. The democratic selection of these validators is crucial to the reliability and functioning of the DPoS system. However, the system includes checks and balances. A delegate marked with a distinct color and associated with the "remove" sign represents the network's accountability measures. If a delegate acts against the interests of the network, the community has the authority to vote them out, ensuring the network's ongoing trustworthiness and efficiency [35]. This visual representation effectively conveys the essence of DPoS, highlighting the significance of community participation, democratic election, and built-in accountability [29].

The ongoing development of blockchain technology has led to the creation of various consensus algorithms that cater to the unique needs and challenges of different networks. Although PoW and PoS are commonly used, they are just the tip of the iceberg, with other mechanisms such as DPoS [34], proof of authority (PoA) [36,37], proof of space (PoSpace) [38], and byzantine fault tolerance (BFT) variants [39,40], offering tailored solutions. Each algorithm has its own set of advantages, trade-offs, and intended applications, showcasing the rich diversity of blockchain innovations. As the technology continues to evolve and diversify, the exploration and adoption of diverse consensus algorithms remain crucial in shaping the future of decentralized systems.

2.3. Artificial intelligence

AI is a rapidly evolving field that has garnered significant attention for its innovative approach in developing machines that can mimic human intelligence. With a primary objective of creating machines that can think and learn like humans, AI has revolutionized the way we approach

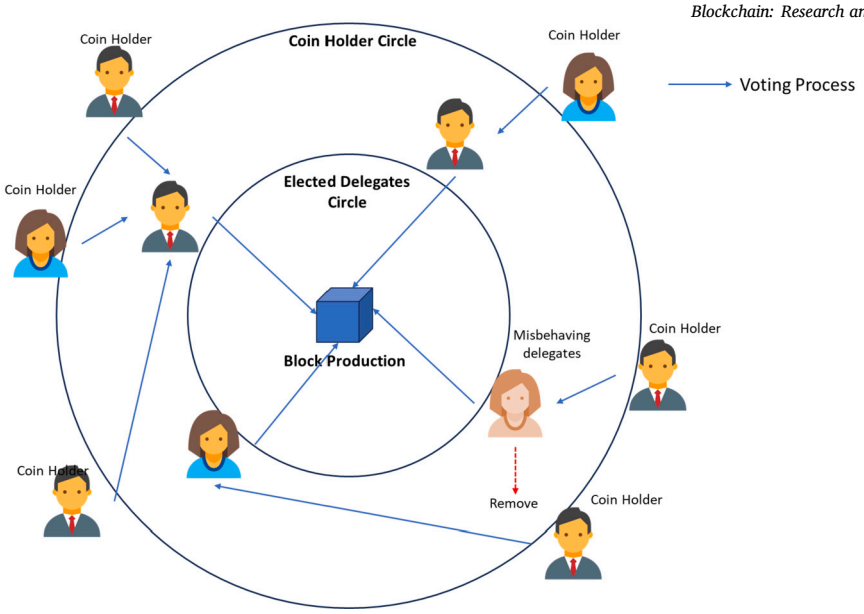

Fig. 5. Delegated proof of stake consensus mechanism.

problem-solving, enabling them to perform tasks that were once considered exclusively human, such as understanding language, identifying patterns, solving complex problems, and making informed decisions.

ML is a critical subset of AI that allows computers to learn from data without the need for explicit programming. Unlike traditional programming methods, ML enables systems to analyze vast datasets, identify patterns, and then make predictions or decisions based on this analysis. The unique advantage of ML systems is that they can adapt and improve their performance over time, becoming more accurate and efficient at their designated task with each new data point they process.

Several techniques underpin ML, including supervised learning, unsupervised learning, reinforcement learning, and deep learning.

- **Supervised learning** is the most common technique, where the algorithm is trained on labeled data with the correct answer and then makes predictions based on this training [41,42].
- **Unsupervised learning** is an approach where the algorithm is given data without explicit instructions and tries to learn the patterns and structure from the data [43,44].
- **Reinforcement learning** is a technique where the algorithm learns by interacting with an environment and receiving feedback in the form of rewards or penalties [45,46].
- **Deep learning** is a subset of ML that uses neural networks with many layers to analyze various factors of data, and is particularly effective in tasks such as image and speech recognition [47,48].

With the increasing use of AI and ML in the modern digital era, numerous industries and domains are experiencing the potential for revolutionary change. From healthcare diagnostics and financial forecasting to virtual assistants and autonomous vehicles, AI has the ability to drive efficiencies, automate complex tasks, and provide new insights from data. This technological advancement is ushering in a new era of innovation and growth, with boundless possibilities for the future.

Fig. 6 provides a clear and concise overview of the major ML techniques and their corresponding data inputs and desired outputs. The input data are categorized into three main types: labeled data, unlabeled data, and data represented as states and actions.

For labeled data, the algorithm of choice is typically supervised learning. In this paradigm, the model is trained using data that have a clear label or outcome attached, allowing it to make accurate predictions. The model gauges its accuracy by calculating the error between its predictions and the actual labels, aiming to minimize this over time. Supervised learning techniques can be applied for tasks such as classification, where items are categorized into predefined classes, or regression, where a continuous outcome is predicted.

For datasets without explicit labels, unsupervised learning is employed. Since there is no clear output to guide the learning process, the model focuses on finding patterns or structures within the data. A common application for unsupervised learning is clustering, where data are grouped based on similarities without prior knowledge of these group definitions.

Lastly, when dealing with data that consist of states and actions, reinforcement learning becomes relevant. In reinforcement learning, an agent interacts with an environment, taking actions based on states to maximize some notion of cumulative reward. The feedback loop in reinforcement learning is unique, as the model receives rewards or penalties for its actions, adjusting its strategies to optimize for future actions.

2.4. AI applications in blockchain consensus

AI has the potential to significantly enhance blockchain consensus mechanisms by improving efficiency, security, and adaptability. Key AI applications include the following:

- **Predictive analytics**: AI can predict transaction patterns and network behavior, enabling more efficient resource allocation and reducing latency in transaction validation.
- **Anomaly detection**: ML algorithms can identify and mitigate security threats in real time by detecting unusual patterns and potential attacks on the network.
- **Adaptive consensus mechanisms**: AI-driven adaptive consensus algorithms can dynamically adjust parameters based on network conditions, improving scalability and responsiveness.

2.5. Gaps in existing research

Despite these advancements, there are still gaps in existing research that need to be addressed:

- Scalability: Many consensus mechanisms struggle with scalability, especially in large networks with high transaction volumes. Further research is needed to develop scalable solutions that maintain security and decentralization.

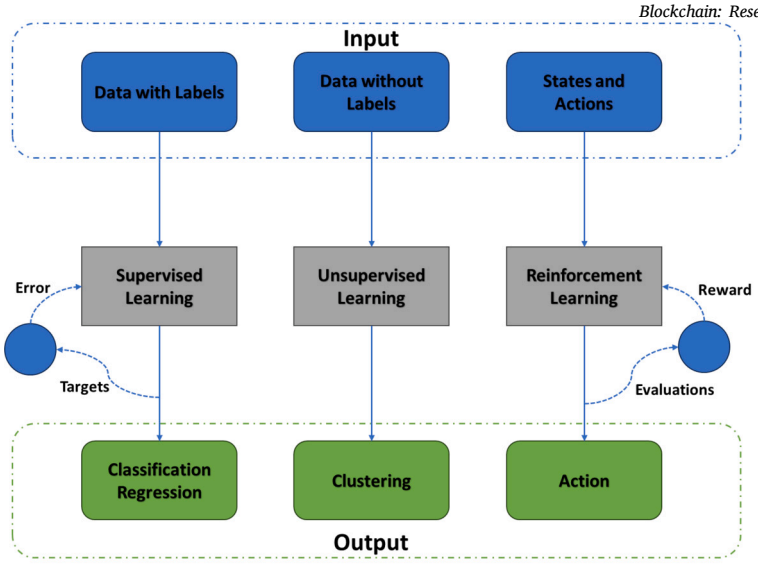

Fig. 6. Machine learning frameworks: inputs, techniques, and outputs.

- Energy efficiency: Reducing the energy consumption of blockchain networks without compromising security remains a critical challenge. Innovative approaches, such as AI-driven optimization, need to be explored further.
- Security: Ensuring the security of blockchain networks against sophisticated attacks is an ongoing concern. AI can enhance security, but its integration must be carefully managed to avoid introducing new vulnerabilities.

3. Methodology

The goal of this systematic literature review is to provide a comprehensive overview of the integration of AI into blockchain technology. This section outlines the scope of our review, the employed search strategy, the criteria for selecting relevant literature, and the methods used for analysis.

Our literature review encompasses academic articles, conference papers, and technical reports that were published between 2010 and 2023. Our focus is on literature that explores the application of AI in blockchain, with a particular emphasis on the aspects of efficiency, security, adaptability, and consensus mechanisms.

Our search for relevant information is comprehensive and used multiple databases, such as IEEE Xplore, SpringerLink, ScienceDirect, and Google Scholar. The keywords we used in our search include combinations of the following terms: “blockchain,” “Artificial Intelligence,” “AI,” “machine learning,” “consensus mechanisms,” “security,” “efficiency,” and “adaptability.”

3.1. Identification of relevant literature

The initial search yielded over 500 papers. We applied the following inclusion criteria to narrow down the list:

- Papers that published in peer-reviewed journals or presented at reputable conferences.
- Studies that specifically address the integration of AI into blockchain technology.
- Articles that discuss the impact of AI on blockchain’s efficiency, security, or adaptability.

We excluded papers that

- are not in English;
- lack a clear focus on blockchain or AI;
- are primarily opinion pieces or lack empirical evidence.

After applying this criteria, we identified 120 relevant papers for detailed review.

3.2. Analysis of literature

The identified papers were analyzed based on the following aspects:

- **AI techniques**: The types of AI methods used (e.g., ML, deep learning, reinforcement learning).
- **Blockchain applications**: Specific blockchain applications enhanced by AI (e.g., consensus mechanisms and security improvements).
- **Outcomes**: The reported outcomes of integrating AI into blockchain, focusing on efficiency gains, security enhancements, and adaptability.
- **Challenges**: Identified challenges and limitations in integrating AI with blockchain.

We categorized the findings into themes and sub-themes to systematically address the research questions posed in our study.

3.3. Methodological approach

Our methodological approach combines both qualitative and quantitative methods to explore the integration of AI into blockchain technology. The following steps were taken:

- **Literature review**: As described above, we conducted a systematic literature review to gather existing knowledge and identify research gaps.
- **Framework development**: Based on the literature review, we developed a conceptual framework that outlines the potential interactions between AI and blockchain technology.
- **Case studies**: We selected several case studies where AI has been integrated into blockchain applications. These case studies were analyzed to validate the conceptual framework and understand real-world implementations.
- **Data collection and analysis**: For the case studies, we collected data through a combination of primary sources (interviews with industry experts) and secondary sources (technical documentation and project reports). We used statistical methods to analyze quantitative data and thematic analysis for qualitative data.

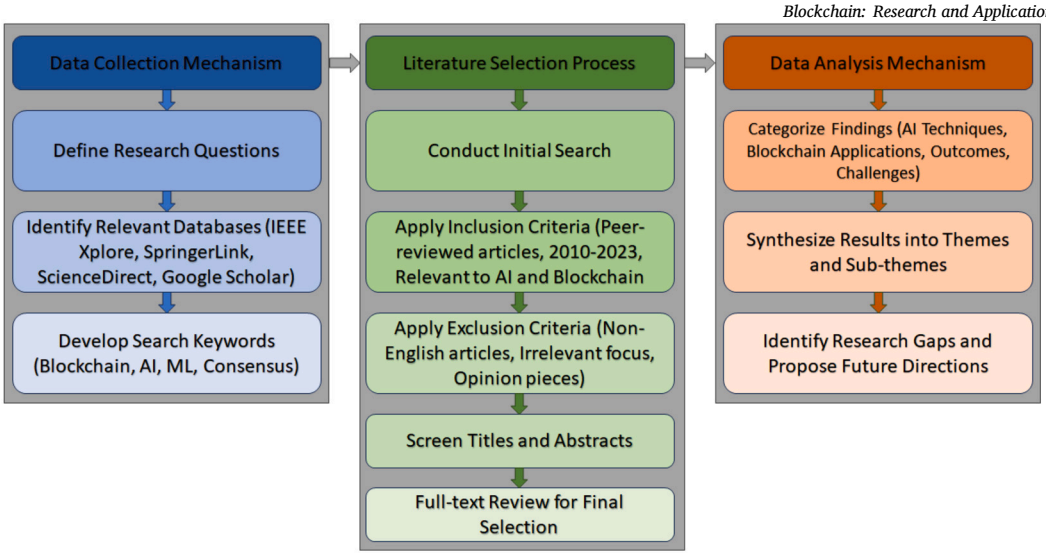

Fig. 7. Overview of literature review method.

This methodological approach ensures a comprehensive understanding of how AI can enhance blockchain technology, supported by both theoretical insights and practical examples, as shown in Fig. 7.

4. AI in blockchain consensus

The utilization of AI and blockchain consensus is a developing field that aims to enhance the fundamental operations of blockchain technology. By integrating AI's analytical capabilities with the robustness of blockchain, common issues can be addressed, security can be improved, and the system can become more adaptable. This convergence signifies a more intelligent and efficient approach to achieving consensus within the blockchain, leading to a more refined and advanced blockchain ecosystem.

4.1. Optimizing existing algorithms

4.1.1. Using AI to predict the next miner or validator

Predicting the next validator in blockchain consensus mechanisms is essential for ensuring efficient block generation and validation. With the growth of ML, particularly predictive modeling, there has been increased interest in applying these techniques to the blockchain domain.

In traditional PoW or PoS systems, the selection of the next validator is typically random or based on specific conditions, such as stake or computational power. However, with the use of AI, it is feasible to predict which node will be the next validator based on historical data and various parameters. This can result in a more efficient and optimized consensus process.

A recent publication by Simon and Geetha [49] explored the complexities of predicting block mining rewards on the Ethereum blockchain through the use of three distinct methodologies: polynomial regression, long short-term memory (LSTM), and the Prophet application programming interface (API). The primary objective of the authors is to improve the understanding and prediction accuracy of mining rewards, which is a crucial component that motivates miners to maintain the integrity of the blockchain. By comparing the performance of these three distinct predictive models, the authors provided readers with a comprehensive analysis of each method's strengths and potential drawbacks. Polynomial regression, known for capturing nonlinear relationships, offers a foundational approach. Meanwhile, LSTM, a type of recurrent neural network (RNN), sheds light on the temporal dependencies of the blockchain data. The inclusion of the Prophet API, a tool designed for forecasting time-series data with daily observations, further enhances the comparative study.

What sets this paper apart is the thorough experimentation and meticulous evaluation criteria. The authors ensured that their findings were not only theoretically sound but also practically implementable, providing tangible benefits for Ethereum miners. However, it would have been beneficial if the authors had delved deeper into the real-world implications of their findings, particularly in the context of the fluctuating Ethereum market. Additionally, future work may explore the integration of these models or the development of ensemble methods for even more accurate predictions.

4.1.2. Predictive modeling for fee estimation

Butler and Crane [50] compared the performance of various ML methods for forecasting blockchain transaction fees on the Ethereum blockchain using a dataset of transaction fee data from the London hard fork period. They examined three ML methods—direct-recursive hybrid LSTM (RDH-LSTM), CNN-LSTM, and attention-LSTM—which are all based on RNNs and well-suited for time series forecasting tasks. The authors also proposed a novel preprocessing method for the transaction fee data, which involves wavelet threshold denoising to remove noise and matrix profile data processing to highlight important features in the data. The results indicated that the DRH-LSTM model outperformed the other models, particularly for longer forecasting horizons, and that their preprocessing method improved the forecasting performance of all models.

Laurent et al. [51] proposed a new model for optimizing transaction fees on the Ethereum blockchain, which uses a ML algorithm known as a gradient boosting machine (GBM). The model is trained using a dataset of historical transaction fee data and is able to learn the relationship between various factors that impact transaction fees, such as the gas price, block size, and network congestion. The model predicts the optimal transaction fee for a given transaction, which is defined as the fee that will minimize the expected waiting time for confirmation. Additionally, the authors proposed a new preprocessing method for transaction fee data, which is designed to remove noise from the data and highlight important features. The performance of the model is evaluated on a test dataset of historical transaction fee data, with a focus on predicting the lowest gas price required to ensure a transaction is mined before a specified date with a certain probability. The method is capable of forecasting the gas price for the upcoming 24 blocks, with a computational time of up to 2 s. The precision of the method is noteworthy, as the gas price calculated using this approach guarantees a probability of the transaction being successfully mined within the given timeframe, with a deviation of less than or equal to 2% from the stipulated probability. The model

offers configurability, allowing users to adjust both the probability of a transaction being mined and the limit date for the mining process.

Zhang et al. [52] addressed the need for accurate transaction fee estimation in Bitcoin to ensure timely transaction confirmations. It critiqued existing methods for their reliance on explicit analytical models and limited data, which failed to capture the complex interactions affecting transaction fees. The authors proposed a new framework, fee estimation neural network (FENN), which integrates diverse data sources, including transaction details, mempool states, and the blockchain environment, into a neural network model to enhance fee prediction accuracy. Their experimental results on real blockchain datasets demonstrated that FENN significantly outperformed existing methods, such as BtcFlow and Bitcoin Core, in terms of root mean square error (RMSE) and mean absolute percentage error, highlighting its efficiency in processing real-time transaction updates within the Bitcoin blockchain. Additionally, FENN's variants, especially those using additive attention mechanisms, showed superior performance in predictive accuracy and training efficiency, indicating its potential for practical deployment in dynamic blockchain environments.

4.1.3. Network optimization to reduce orphaned blocks

Orphaned blocks, also known as "stale blocks," are those that are not included in the prevalent blockchain due to the addition of another block of the same height [25,53]. The occurrence of orphaned blocks can be caused by network latency, where delays in transmitting a new block lead other miners to continue their efforts on an old block, or by simultaneous block discoveries by multiple miners [27]. Minimizing orphaned blocks is crucial in blockchain operations since they consume computational resources and can compromise network security. Strategies for achieving this include optimizing the speed of block propagation across the network, managing block sizes to prevent delays in transmission, ensuring stable connections among crucial network nodes, enhancing the blockchain protocol to accommodate orphaned blocks, and strategically placing nodes geographically for swifter communication. By employing these tactics, blockchain networks can reduce inefficiencies and maintain heightened security and stability.

Mohammadi and Rabieinejad conducted a study to investigate the feasibility of using ML to predict blockchain forks [54]. They proposed an ML model trained on historical data of blockchain forks that considers factors such as the number of active nodes on the network, the hash rate distribution, and the number of pending transactions. Multiple ML algorithms were compared, including naive Bayes (NB), KNN, decision tree (DT), and multi-layer perceptron (MLP). The models were also evaluated with and without clustering. The trained model can predict the probability of a fork occurring in the next time period. The authors achieved an accuracy of around 99.62% when using KNN with clustering on a real-world dataset of blockchain forks. However, their study did not provide information on the parameters used for all the models or the preprocessing of the dataset, making it difficult to replicate the study as a reference model.

Zahra et al. [55] examined the problem of orphan blocks in the Nakamoto consensus protocol, which can negatively impact network throughput and be susceptible to abuse. To address this issue, the authors proposed a novel technique that incorporated a small database within each block. This approach ensured the finalization of almost all correctly mined blocks at any height, thereby improving system security and promoting honest miner behavior. By preventing conflicting transactions and detecting exceptional circumstances, the proposed method significantly increased throughput and reduced the creation of orphan blocks. Simulation results based on real network data for Bitcoin demonstrated the effectiveness of this method in maintaining blockchain safety and liveness while ensuring fairness and resource efficiency. This approach is a promising solution for optimizing blockchain network performance and enhancing the overall system efficiency.

4.1.4. Comparison with state-of-the-art studies

To clarify the novelty and contribution of our study, we compare it with other recent literature reviews that cover related topics. Tables 1 and 2 summarize the key aspects of these studies.

4.2. Anomaly detection & security

Anomaly detection refers to the process of identifying irregularities in data that do not conform to expected patterns. These anomalies may indicate malicious activities or security breaches, which makes them critical to detect and resolve in blockchain systems to maintain the integrity and authenticity of transactions. Various techniques have been developed over time to address anomaly detection, each designed to address specific challenges and data types. While traditional statistical methods remain foundational, the increasing complexity and volume of data have led to the rise of ML techniques. These techniques, ranging from clustering to deep learning, provide a more adaptive and scalable approach for detecting complex patterns that may elude classical methods. As blockchains continue to evolve and gain widespread adoption, the demand for more advanced anomaly detection mechanisms will likely increase.

4.2.1. Using ML to detect unusual patterns or potential attacks

Kim et al. [61] proposed a ML approach that uses an AutoEncoder (AE) framework to detect anomalies in real-time blockchain networking traffic data. To enhance the quality of the input data, the research employed preprocessing techniques such as feature extraction and prioritization. The study compared the performance of the AE-based model against several algorithms, including one class support vector machines (OCSVM), logistic regression (LR), random forests (RF), gradient boosting (GB), and DNN, and demonstrated its superiority or comparability in terms of anomaly detection. Specifically, the AE-based model achieved high accuracy, F1 scores, and real-time operational capability, making it a promising tool for identifying malicious activities within blockchain networks.

Sayadi et al. [62] introduced a sophisticated approach to detect anomalies in blockchain networks by employing two prominent ML algorithms: OCSVM and the K-means algorithm. OCSVM is intended to identify outliers, while the K-means algorithm is used to cluster similar outliers and classify them based on the type of anomalies. The data were subjected to normalization as a preprocessing step, followed by classification into three categories: distributed denial of service (DDoS) attack, double spending attack, and other attacks. The authors reported that both algorithms demonstrated a remarkable accuracy of approximately 93%.

Venkatesan and Rahayu [63] proposed a consensus algorithm that integrates ML techniques to address security challenges in blockchain networks. By combining various consensus mechanisms, such as DPoS and practical byzantine fault tolerance (PBFT), with ML models, the study aims to enhance anomaly detection and predict cyber-attacks. The proposed framework used supervised and unsupervised learning for real-time anomaly detection, feature extraction, and proactive defense mechanisms against potential threats. The authors demonstrated the effectiveness of the hybrid approach by implementing it on the ProximaX blockchain platform, which improves security, scalability, and adaptability, ensuring robust and efficient blockchain operations. The results of the study validated the proposed framework's ability to address challenges such as scalability, latency, and resource requirements, making it a promising solution for securing blockchain networks.

4.2.2. Identifying and countering Sybil attacks

A Sybil attack is a malicious action where a single perpetrator controls multiple nodes in a network with the intention of disrupting its functioning. These multiple nodes, known as Sybil nodes, can be used to exert excessive influence, disseminate false information, or impair

Table 1
Comparison of AI Models in blockchain consensus (part 1).

References	AI model	Objective	Drawback
[49]	Linear and polynomial regression, LSTM	Predicts block reward and ether price	Dataset is not split into training, validation, and testing sets.
[51]	Monte Carlo model	Predicts transaction mining probability within a time limit	Higher computation time than other methods.
[54]	NB, KNN, DT, MLP	Predicts probability of a fork occurring	Lack of dataset preprocessing and validation details.
[56]	ANN-based	Select optimal number of mobile consensus nodes (MCNs)	Criteria for static cluster assumptions are not well-defined.

Table 2
Comparison of AI Models in blockchain consensus (part 2).

References	AI model	Objective	Drawback
[57]	CNN	Validates blocks for secondary verification	Lower TPS than general IT commercial services.
[58]	PoS and PBFT	Optimizes hybrid consensus algorithm	Complex implementation and high resource requirements.
[59]	Various ML techniques	Surveys on consensus mechanisms and mining strategies	Broad scope with limited depth on specific techniques.
[60]	Federated learning, differential privacy	Enhances privacy through advanced ML techniques	High complexity and computational overhead.

mechanisms that rely on trust and redundancy. By creating and presenting numerous fake identities, the attacker can compromise the outcomes of crucial processes such as voting, data aggregation, or resource allocation in peer-to-peer networks [64]. Essentially, the attacker can manipulate the outcomes of critical processes by creating and presenting numerous fake identities.

Haddaji et al. [65] proposed a tripartite trust management mechanism—horizontal trust management (HTM), vertical trust management (VTM), and distributed trust management (DTM)—to enhance the security of vehicular networks against Sybil attacks. This mechanism allows vehicles to establish trust based on individual reputation scores and social network data derived from historical behaviors and relationships with neighbors. The decentralization of HTM and the intricate layering of VTM and DTM contribute to a highly resistant system to potential malicious interventions. Through vehicular network simulations, the authors observed a 70% reduction in successful Sybil attacks. To further refine the trust evaluation process, ML models, including SVM, KNN, and RF, were used.

Azzam et al. [66] proposed a collaborative learning-based approach to detect Sybil attacks in VANETs, where each vehicle uses individual classifiers trained on features indicative of Sybil behavior. The classifiers are exchanged among vehicles and integrated with those of neighbors to anticipate Sybil activity, with a decision ultimately being reached through majority voting. To enhance prediction accuracy and robustness, supervised ML classifiers, including KNN, NB, DT, SVM, and LR, are used as base classifiers. These classifiers process the dataset concurrently. Remarkably, the DT and KNN classifiers consistently exhibited superior performance across different node datasets, achieving an accuracy and recall of 99%. Similarly, the voting techniques, especially the Soft voting strategy, demonstrated high efficacy with accuracy levels frequently nearing 97%. This method's collaborative design draws from the collective insights of the entire vehicle network, ensuring scalability without centralized coordination and robust resistance against malicious interventions.

Mounica et al. [67] proposed an ML model to detect Sybil attacks in wireless sensor networks. This model uses multiple ML algorithms such as SVMs, DTs, LR, and RF to classify sensor nodes as either legitimate or malicious. The ML models are trained using features such as the number of neighboring nodes, the average distance to neighboring nodes, and the packet delivery ratio. The study revealed that SVM has a high accuracy of 93% in predicting Sybil attacks.

Zhu et al. [68] offered a method for detecting and tracing Sybil attacks in connected vehicular networks. The suggested mechanism involves the use of roadside units to instruct vehicles to perform customized key broadcasting and listening, which enables the detection of physical presence and the construction of a neighbor graph based on beacon packets. This graph is used to calculate the edge success probability, which accurately identifies Sybil vehicles and traces malicious vehicles responsible for these attacks. The experimental results show high precision (98.53%) and recall (95.93%) rates, significantly improving the detection and traceability of Sybil and malicious vehicles compared to existing methods. This approach effectively mitigates Sybil attacks from their source, enhancing the security and reliability of connected vehicle networks.

4.2.3. *Identifying double spending*

Double spending, which refers to the risk or act of using the same digital currency unit more than once, is a significant threat to blockchain networks. This issue is particularly concerning in the realm of digital currencies and electronic payment systems, as digital tokens are easily duplicated or falsified. However, the use of a decentralized ledger called the blockchain effectively addresses and prevents the issue of double spending in cryptocurrencies like Bitcoin. The blockchain provides a tamper-evident record of all transactions, and its decentralized consensus mechanisms ensure that all participants in the network agree on the validity of transactions. If an attempt at double spending is made, the network's nodes will detect the inconsistency and reject the fraudulent transaction.

Aladhadh et al. proposed a novel method for detecting cyber threats within blockchain systems by combining the strengths of ML, specifically SVM and MLP, with smart contracts [69]. In their study, the utilized dataset exhibited an imbalance, with threat transactions constituting 20% and normal transactions comprising the remaining 80%. This imbalance has the potential to skew ML models towards predictions favoring the majority class, thereby reducing the efficiency in identifying genuine threats. To address this, the framework gathers data from blockchain transactions and relevant events to train these ML models, ensuring they are proficient in identifying cyberthreats even in the presence of data skewness. Successful training leads to the embedding of SVM and MLP models within a blockchain's smart contract. As the smart contract oversees blockchain activity, the integrated ML models actively scan for potential threats. In the event of detecting any malicious activity, the smart contract raises an alert and takes necessary preventive actions, such as halting the suspicious transaction or notifying the concerned authorities. When tested in a simulated blockchain environment, the BChainGuard achieved an impressive detection accuracy rate exceeding 95%, while maintaining minimal overhead. Compared to conventional methods, this framework boasts greater security due to the immutable nature of smart contracts, increased efficiency through the rapid threat detection capabilities of SVM and MLP, and unparalleled scalability as it can be seamlessly integrated into diverse blockchain networks. The effectiveness of BChainGuard in addressing the dataset imbalance highlights the robust design of the framework and its promising potential in the realm of blockchain cyberthreat mitigation.

4.3. Adaptive consensus mechanisms

Sophisticated systems known as adaptive consensus protocols are used in blockchain and other decentralized networks to reach a unanimous agreement on the verified state of data among nodes. These protocols differ from static consensus approaches in that they adjust their parameters to reflect current network conditions. The flexibility of adaptive protocols allows for maintained efficiency, heightened security, and improved scalability. The key advantage of adaptive consensus lies in its real-time reactivity to changes in network status, potential security threats, or periods of high traffic, which ensures the blockchain's consistent effectiveness and robustness. These mechanisms are particularly valuable in situations where user activity and network conditions are subject to frequent alterations.

Sabry et al. [70] presented a novel method that combines the capabilities of blockchain technology with the complexity of the traveling salesman problem (TSP) to optimize product distribution. This method employs a unique proof of useful work (PoUW) mechanism within the blockchain network, redirecting miners' computational power to find the most efficient solutions to the TSP. The approach begins by collecting distribution location data, which is then clustered based on proximity to streamline the problem. Each group of locations then undergoes the guided local search algorithm to determine the shortest possible path for the salesmen within that cluster. This innovative approach diverges from the traditional blockchain's PoW mechanism, which usually involves solving complex mathematical problems. Instead, miners' efforts and computational resources are harnessed to enhance the efficiency of product distribution, with the ultimate goal of reducing the overall distance that salesmen must travel.

The paper examines the combination of ML and blockchain, with a specific focus on the proof of learning (PoLE) method. This method integrates neural network training into the consensus-building process of blockchain networks, demonstrating the synergistic relationship between deep learning and blockchain technologies. Furthermore, the paper introduces the "DLChain" concept, which merges deep learning with blockchain as a PoUW, showcasing the vast potential of combining these two technological domains.

Leduc et al. [71] introduced a novel solution to address the challenges faced by the PBFT consensus protocol, which is known for its impressive transaction throughput but often encounters a trade-off between security and throughput due to increased validators. To address this issue, they proposed Sabine, a self-adaptive consensus protocol that dynamically adjusts the number of validators to align with the application's input needs and ensure seamless throughput while maintaining robust security. The paper employs ML based on polynomial regression to construct a model that correlates the number of validators, delay, and the blockchain's capacity. The methodology is divided into two phases: the training phase involves Sabine gathering samples of maximum network throughput by modifying validator numbers and inducing network delays. These data are then used to inform the model. In the action phase, the protocol uses the developed model to recalibrate the ideal validator count periodically, broadcasting any updates to all nodes through a dedicated transaction. While this validator selection can be tailored according to specific chains, Sabine ensures that modifications in subsequent blocks are consistent. Experimental outcomes demonstrate the superior efficiency of Sabine, revealing a minimal 7.79% discrepancy between anticipated and achieved transaction throughput, a vast improvement over the 39.5% observed in conventional chains with all-inclusive node participation in consensus. As a result, Sabine represents a streamlined blockchain mechanism that reduces latency, meets throughput demands effectively, and ensures robust security.

4.4. Energy efficiency in PoW

The research conducted by Alofi et al. [72] addresses the pressing problem of excessive energy consumption and elevated carbon emissions in blockchain-based systems, by proposing a comprehensive optimization model that can be used for the strategic selection of miners. The primary objective of this model is to minimize energy consumption and carbon emissions while maintaining optimal system performance, thereby making a significant contribution to the development of sustainable blockchain operations.

The optimization model relies on various evolutionary algorithms to identify the most environmentally conscious and energy-efficient group of miners. The rigorous evaluation process considers several aspects, including computational power, energy efficiency ratings, and carbon emission factors, to guide the algorithms towards solutions that align with the established sustainability objectives.

The model's primary feature is its implementation of multi-objective optimization, which enables a delicate balance between minimizing the system's energy and carbon footprint and maximizing its operational performance. This equilibrium is essential to ensure that the pursuit of sustainability does not compromise the system's functionality, resulting in a harmonious blend of ecological responsibility and technical proficiency.

The study delves into multiple evolutionary algorithms, such as non-dominated sorting genetic algorithm II, strength Pareto evolutionary algorithm 2, Pareto archived evolution strategy, indicator-based evolutionary algorithm, and non-dominated sorting genetic algorithm III. These algorithms are critical in maintaining solution diversity and directing the search process across the extensive solution space.

Empirical examination validates the efficacy of the suggested optimization model, evidencing a substantial decrease in energy consumption and carbon emissions relative to conventional arrangements. The model provides decision-makers with a variety of optimal alternatives, allowing them to choose the most suitable option based on their particular criteria and preferences. In conclusion, this article confronts the challenges present in the realm of blockchain-based systems and lays the foundation for more sustainable practices. It presents a persuasive argument for the concurrent pursuit of environmental responsibility and system effectiveness.

4.5. Maintaining decentralization while leveraging AI

The incorporation of AI in blockchain technology possesses the potential to substantially improve efficiency, security, and adaptability. On the other hand, it presents concerns regarding centralization, particularly when computational resources become a significant factor. This subsection aims to examine the possible risks and approaches to ensure decentralization, as discussed by Abhishek et al. [73] and McMahan et al. [74].

4.5.1. Potential risks of centralization

The integration of AI into blockchain technology presents a significant challenge, particularly with regards to the disparity in computational resources. AI models, particularly deep learning algorithms, necessitate substantial computational power for both training and inference. This disparity could result in entities with more powerful computational resources dominating the network, which in turn could lead to centralization. Such centralization would undermine the fundamental principle of decentralization, where no single entity should have disproportionate control over the network.

The potential drawback of centralizing data is another concern. AI models frequently require substantial datasets for their training. Storing data in a centralized manner may result in vulnerable areas that could compromise the system, and it increases the likelihood of data breaches. It is essential to strike a balance between maintaining the decentralization of data and harnessing AI's potential to protect the security and integrity of blockchain networks.

Table 3
Performance metrics of various models to predict mining reward [49].

Model	Metric	Value
K-means clustering	Silhouette score	71%
Linear regression	R-squared	Low
Polynomial regression	R-squared	0.005977
Polynomial regression	RMSE	1.336e+152
LSTM	RMSE	36.45%
Prophet API	MAE	1326.71

4.5.2. Strategies to maintain decentralization

To mitigate these risks, several strategies can be implemented. One of these is federated learning, which is a method of training AI models in a distributed manner, where data remain localized. Instead of combining data in a central location, the model is trained across multiple nodes using their individual data. This enhances privacy and reduces the risk of centralization by distributing the computational load and data storage across the network.

Another approach is to use consensus algorithms like PoS and DPoS, which can be integrated with AI to enhance network efficiency without requiring significant computational resources. These algorithms allocate validation responsibilities based on the quantity of tokens held, thereby promoting a more equitable distribution of control and mitigating the risk of centralization stemming from computational advantages.

One strategy that can aid in preserving decentralization is edge computing. This method entails processing data at the network's edge, which is closer to the data source. By doing this, it decreases latency and the reliance on centralized data centers. Implementing edge computing enables AI algorithms to be executed on local nodes, thereby sustaining a decentralized network configuration.

Decentralized AI marketplaces represent a novel solution that is gaining traction. These marketplaces enable multiple entities to collaborate and benefit from AI services while avoiding centralized control. By facilitating the sharing of AI models and computational resources in a decentralized manner, these marketplaces prevent any single entity from amassing excessive control [75].

Ultimately, the creation of incentive structures that reward decentralized participation can help to promote a more equitable distribution of computational resources. This might involve offering token rewards to nodes that actively contribute to the training and deployment of AI models in a decentralized manner, thereby fostering a balanced and fair network.

5. Results and discussion

Simon and Geetha [49] conducted research on the application of ML and deep learning algorithms to predict mining rewards and cryptocurrency prices on the Ethereum blockchain. The study employs various techniques, including linear regression, polynomial regression, *K*-means clustering, LSTM, and the Prophet API, to analyze and predict the rewards and prices.

The findings presented in Table 3 showcase the promising prospects of applying ML and deep learning approaches to forecasting mining rewards and cryptocurrency prices. Despite polynomial regression offering a superior fit compared to linear regression, the data's skewness and elevated RMSE suggest that further refinement and enhancement of preprocessing and modeling techniques are required.

Laurent et al. [51] examined the optimization of transaction fees in the Ethereum blockchain, aiming to determine the minimum gas price a user should pay to ensure that their transaction is processed within a specified time frame with a certain probability. The authors proposed a novel solution rooted in a Monte Carlo approach to predict the probability of a transaction being mined within a predetermined time limit. The paper comprises comprehensive numerical results based on real-world data to showcase the effectiveness of their method.

The research demonstrates an innovative technique for enhancing transaction fees within the Ethereum blockchain, surpassing the constraints of previous methods. The proposed Monte Carlo-based approach integrates customizable time and probability parameters, thereby providing increased accuracy and versatility, as evidenced in Table 4.

Mohammadi and Rabieinejad [54] conducted a study to explore the potential of employing ML techniques to anticipate blockchain forks and alleviate the accompanying risks and expenses. Blockchain forks can lead to significant problems, including increased energy consumption, security breaches, and higher operational expenses. The researchers evaluated the performance of various widely-used ML approaches in predicting blockchain forks.

The graph in Fig. 8 illustrates that ML methods, especially when combined with clustering, can accurately predict blockchain forks with a high degree of precision. Among the various models tested, the MLP with clustering demonstrated the greatest accuracy, suggesting that the integration of clustering with classification enhances predictive performance.

Saadat et al. [56] put forward a novel framework for selecting MCNs in vehicular networks using artificial neural networks. The proposed framework, known as the mobility-aware reputation-based blockchain framework, aims to enhance the stability and performance of blockchain networks with highly mobile nodes by considering the reputation and stability of nodes as per Ref. [56].

Fig. 9 showcases the influence of the intelligent consensus node selection (ICNS) algorithm on three essential metrics: reputation, stability, and message counts. The depiction provides a comparison between scenarios with and without the implementation of ICNS, emphasizing the enhancements attributable to the algorithm.

In terms of reputation and stability, the ICNS algorithm demonstrates significant improvements in both areas. Without ICNS, the baseline reputation value is set at 100.0%, while the stability baseline is also set at 100.0%. However, with the implementation of ICNS, reputation improves by 6.8%, reaching a value of 106.8%. This indicates that ICNS enhances the selection of high-reputation nodes for consensus, leading to more trustworthy network operations. Additionally, stability improves significantly by 17.5%, reaching a value of 117.5%. This substantial increase demonstrates that ICNS selects more stable nodes, which contributes to a more reliable and consistent blockchain network.

The baseline value for message counts without the intervention of the ICNS algorithm is 100.0%. With the implementation of ICNS, the message count is reduced by 33.9%, resulting in a value of 66.1%. This decrease in message count demonstrates that the ICNS algorithm streamlines communication within the network, minimizing overhead and enhancing efficiency.

In conclusion, the integration of the ICNS algorithm results in improvements in node reputation and stability, along with a reduction in message counts. These improvements contribute to enhanced performance and efficiency of the blockchain network as a whole.

Kim [57] investigated the potential application of blockchain technology in conjunction with AI algorithms to prevent diploma forgery. The proposed system leverages AI to validate the authenticity of diplomas and employs blockchain technology to securely and preventatively maintain records.

Table 5 provides a comprehensive overview of the key performance metrics of the proposed system designed to prevent the forgery of degree certificates using AI and blockchain technology. The system's impressive throughput and efficiency are demonstrated by its ability to handle up to 4100 TPS. Moreover, the system's scalability and robustness in a distributed environment are evident from the successful testing with 500 nodes. The AI-based verification process has achieved an average accuracy of 99.8%, ensuring a high level of reliability in detecting forged certificates. The system's cryptographic foundation is further strengthened by the use of SHA-512, MD5, and HAS-160 hash algorithms, which guarantee data integrity and security. These metrics collectively underscore the efficiency, scalability, accuracy, and security of the proposed

Table 4
Comparison of different methods for gas price prediction [51].

Method	Pending list	Gas limit	Time limit	Probability	Comp. time
ETH gas station	No	No	Speed indicator	No	-
Singh et al. (2019)	Yes	No	No	No	-
Liu et al. (2020)	No	Yes	No	No	0.04 s
Werner et al. (2020)	No	No	Speed indicator	No	-
Mars et al. (2021)	No	No	Yes	No	-
Proposed method	Yes	Yes	Yes	Yes	Up to 2 s

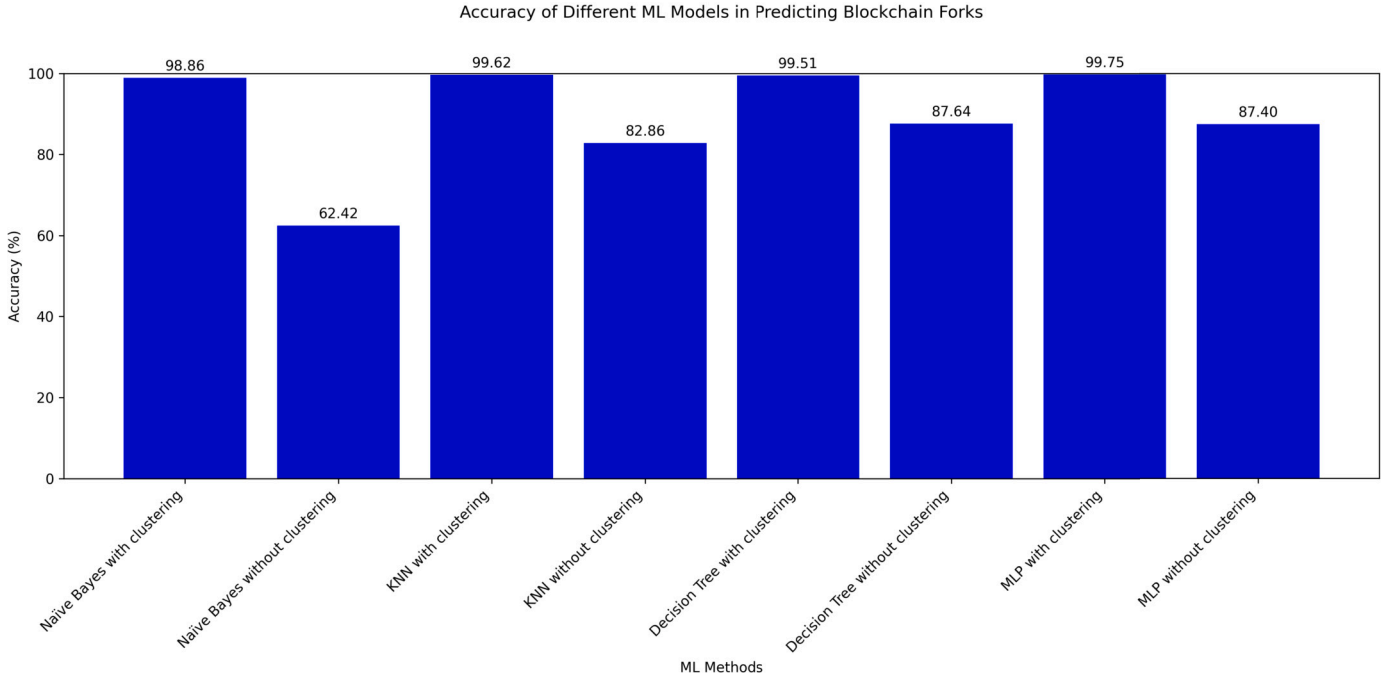

Fig. 8. Accuracy of different ML models in predicting blockchain forsk [54].

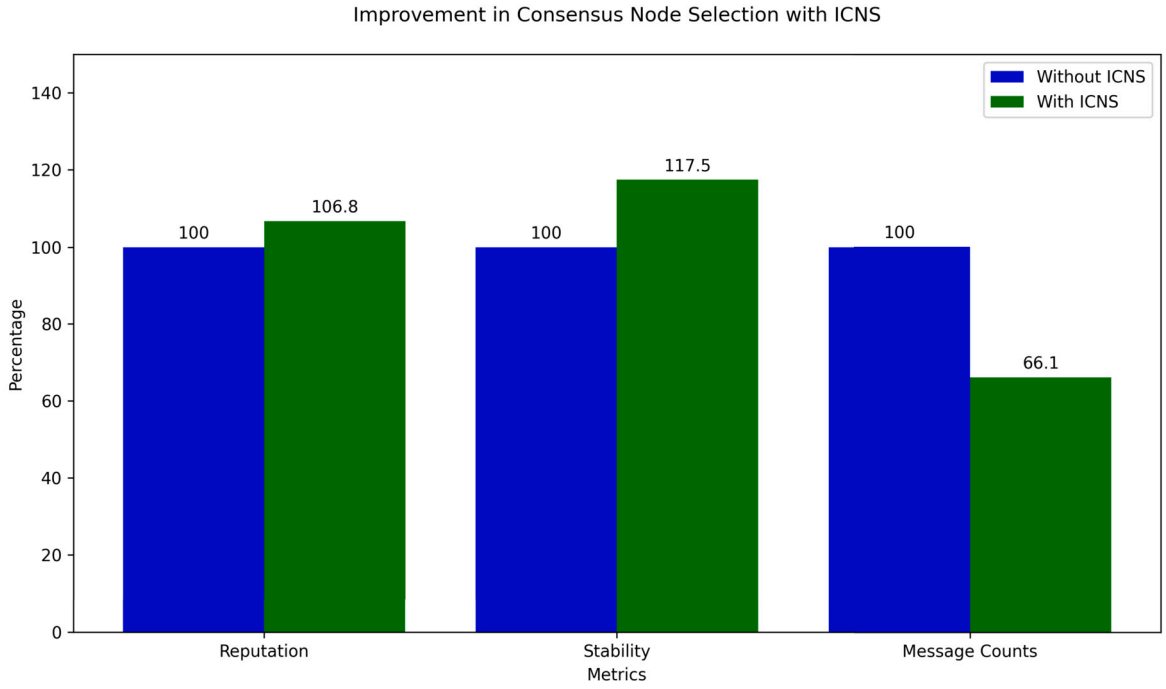

Fig. 9. Improvement in consensus node selection with ICNS [56].

Table 5
Performance metrics of the proposed system [57].

Metric	Value
TPS	4100
Number of nodes	500
Average verification accuracy	99.8%
Security level (Hash algorithms)	SHA-512, MD5, HAS-160

Table 6
Performance comparison of consensus algorithms [58].

Metric	PoW	PoS	PBFT	Hybrid (PoS+PBFT)
TPS	3-7	30-70	700-1500	1100-1400
Scalability	Low	High	Low	High
Latency	High	High	Low	Low
Energy consumption	High	Low	Low	Low
Byzantine tolerance	No	Yes	Yes	Yes

system, making it a promising solution for preventing the forgery of degree certificates.

Wu et al. [58] proposed a consensus algorithm that combines the PoS and PBFT algorithms to improve the performance of blockchain networks. By enhancing throughput, scalability, and latency, this hybrid approach aims to address some of the limitations of traditional blockchain systems. According to Wu et al., this innovative approach has the potential to significantly impact the field of distributed ledger technology.

Table 6 provides a comparison of various consensus algorithms, including PoW, PoS, PBFT, and a hybrid algorithm that combines PoS and PBFT. The table highlights several key performance metrics. In terms of throughput, PoW achieves a relatively low range of 3–7 TPS, while PoS improves to 30–70 TPS. PBFT demonstrates significantly higher throughput, ranging from 700 to 1500 TPS. The hybrid algorithm achieves a similarly high throughput of 1100 to 1400 TPS, indicating robust transaction processing capabilities.

Scalability is low for both PoW and PBFT, whereas PoS and the hybrid algorithm demonstrate high scalability, allowing the network to handle an increasing number of nodes efficiently. In terms of latency, both PoW and PoS have high latency, meaning slower transaction processing times. In contrast, PBFT and the hybrid algorithm offer low latency, which is crucial for applications that require quick transaction confirmations.

The energy consumption associated with PoW is significant, as it is a computationally intensive process. On the other hand, PoS, PBFT, and the hybrid algorithm exhibit lower energy consumption, which makes them more environmentally friendly and cost-effective. In terms of Byzantine tolerance, PoW is lacking in this capacity, whereas PoS, PBFT, and the hybrid algorithm all demonstrate resilience against specific types of failures, thereby enhancing network security and reliability.

Kim et al. [60] focused on the necessity of privacy-preserving distributed machine learning (DML) within blockchain networks. The authors introduced a novel approach that integrates differentially private stochastic gradient descent with an error-based aggregation rule to enhance privacy, security, and efficiency in permissioned blockchain settings. This innovative model has been documented in their research paper.

Table 7 compares the effectiveness of privacy-focused DML models by evaluating the proposed model against multi-Krum and LearningChain. The proposed model, similar to the other models, employs differential privacy to safeguard user privacy. However, the proposed model distinguishes itself by exhibiting a higher level of resilience against attacks, in contrast to the moderate resilience of multi-Krum and the low resilience of LearningChain. In terms of computational complexity, the proposed model is more efficient, operating at $O(KlogK)$, while multi-Krum has a higher complexity of $O(K^2d)$ and LearningChain operates at $O(Kd)$. Additionally, the proposed model demonstrates low transaction latency, typically less than one minute, whereas both Multi-Krum and LearningChain have higher latency. Lastly, the proposed model boasts high accuracy, surpassing the moderate accuracy of multi-Krum and the low accuracy of LearningChain. This comparison underscores the superior performance of the proposed model in terms of privacy, efficiency, and resilience.

6. Challenges & considerations

6.1. Data privacy

AI models are inherently data-driven, necessitating extensive datasets for training to ensure efficacy and reliability in their output. In the context of blockchain, where data integrity and security are paramount, the integration of AI poses unique challenges, particularly in the realm of privacy.

Blockchain systems are renowned for their ability to secure data through decentralization and cryptographic techniques. However, the introduction of AI into this ecosystem requires access to granular and, often, sensitive data such as personal user information, transaction details, and other confidential data elements. For example, in healthcare applications on blockchain, AI models might need to access and analyze patient records, medical images, and other personal health information to provide accurate diagnoses, treatment recommendations, or drug discovery insights.

While the benefits of integrating AI in blockchain for healthcare are evident, ranging from improved diagnostic accuracy to personalized treatment plans and efficient drug discovery, it raises significant privacy concerns [76]. The transparency and immutability of blockchain can conflict with the need for privacy in handling sensitive healthcare data. Furthermore, AI's capability to learn complex patterns in data exacerbates the risk, as it could potentially be used to re-identify individuals from anonymized or pseudonymized data, infringing upon their privacy.

To address these concerns, there is a need for robust privacy-preserving techniques that align with the principles of blockchain. Methods such as differential privacy could be employed to protect individual privacy while allowing AI models to learn from the data. Furthermore, ensuring responsible and transparent data collection and usage practices are crucial. Organizations should clearly communicate their data practices to users and provide them with control over their data, including the option to opt out if they wish.

In summary, while the integration of AI in blockchain healthcare applications offers numerous advantages, it is paramount to address the inherent privacy concerns proactively. Employing privacy-preserving methods, maintaining transparency in data practices, and empowering users to control their data are vital steps towards achieving a harmonious balance between leveraging AI for healthcare advancements and protecting individual privacy on the blockchain.

6.2. Overhead

Deploying AI models in systems can provide enhanced functionalities and improve performance in various applications. However, a notable concern is the computational overhead associated with these models. The computational resources required for processing, memory usage, and latency due to complex AI operations can be significant. This overhead might, in some cases, negate the benefits AI promises. Particularly in real-time applications or systems with limited computational capacity, the additional burden of running AI models might result in reduced overall efficiency. It is essential to balance the AI model's sophistication with the system's capability to ensure that the gains from AI are not overshadowed by its computational demands.

You [77] introduced an innovative blockchain model that integrates PoW computation with AI model learning. With a central aim to concurrently and efficiently execute both blockchain consensus mechanisms

Table 7
Performance comparison of privacy-preserving DML models [60].

Metric	Proposed model	Multi-Krum	LearningChain
Privacy guarantee	Differential privacy (DP)	DP	DP
Attack resilience	High	Moderate	Low
Computational complexity	$O(KlogK)$	$O(K^2d)$	$O(Kd)$
Transaction latency	Low ($\leq$ 1 min)	High	High
Utility (accuracy)	High	Moderate	Low

and AI computations, the author employed reinforcement learning—a ML method where an agent iteratively acts in an environment to optimize a reward signal. In this model, each blockchain block serves as a state in a Markov state machine, with the block creation and linkage mimicking a Markov decision process. An oracle, acting as the environment, furnishes the blockchain system with data via state transitions. As the blockchain system, or the agent, selects actions based on its prevailing policy, it reaps rewards from this environment. Simultaneously, the blockchain nodes fine-tune and update this policy model, aligning it with upcoming actions and states. This dual-function approach harmonizes the demands of PoW computations with the nuances of AI model training, paving the way for a more resource-efficient blockchain system.

6.3. AI in permissioned and private blockchains

While the primary focus of our paper is centered on public blockchains, it is essential to acknowledge the vital role that AI can play in both permissioned and private blockchains. Permissioned blockchains, which restrict access to a predetermined group of participants, and private blockchains, which are managed by a single organization, present distinctive prospects and obstacles for the integration of AI.

6.3.1. Enhanced privacy and security

Permissioned and private blockchains provide a unique opportunity to incorporate AI to improve privacy and security. ML algorithms, in particular, can be used to monitor transaction patterns and detect irregular activities that may indicate security breaches or fraudulent behavior. This capability is especially beneficial in environments where access is restricted, and security is a top priority. By leveraging AI in this manner, organizations can enhance the overall security of their systems while maintaining the privacy of their users.

6.3.2. Improved efficiency and scalability

AI can optimize the performance of private and permissioned blockchains by predicting transaction loads and dynamically adjusting resource allocation. This can help reduce latency and improve throughput, which are critical factors for enterprise applications. Furthermore, AI can assist in optimizing consensus algorithms specifically designed for these types of blockchains, thereby enhancing their efficiency and scalability.

6.3.3. Intelligent contract management

AI can be utilized to enhance contract administration in private and permissioned blockchains using AI-driven analytics. With this approach, organizations can automate contract execution, monitor adherence to contractual obligations, and proactively identify potential disputes. This streamlined process minimizes the need for manual intervention and ensures that contractual obligations are met in a timely and efficient manner.

6.3.4. Case studies and applications

Recent research has exhibited the effective utilization of AI in permissioned and private blockchains. One such application is in the enhancement of supply chain management through real-time tracking and predictive maintenance. Additionally, financial institutions have used AI to automate compliance checks and optimize transaction processing within private blockchain networks.

6.4. Environmental impact of AI integration

The incorporation of AI into blockchain technology is likely to have notable environmental consequences. Although AI presents potential advantages in terms of productivity and security, it also brings about additional computational demands that may affect energy utilization, carbon emissions, and general expenses associated with operations.

6.4.1. Energy consumption

AI models, particularly those that rely on deep learning algorithms, necessitate substantial computational resources for both training and inference. When these models are incorporated into blockchain networks, the overall energy consumption may rise considerably. This is particularly relevant for public blockchains that rely on energy-intensive consensus mechanisms, such as PoW. AI-driven optimizations may result in more frequent model updates and additional processing, further increasing energy demands [78].

6.4.2. Carbon footprint

The utilization of AI can result in increased energy consumption, which in turn contributes to a larger carbon footprint. Data centers and mining operations that support AI-enhanced blockchain networks frequently depend on non-renewable energy sources, leading to a rise in greenhouse gas emissions. To tackle this issue, it is essential to develop and implement more energy-efficient AI algorithms and harness renewable energy sources for blockchain operations [79].

6.4.3. Cost implications

The costs associated with the implementation of AI in blockchain networks can lead to increased operational expenses. These costs include the acquisition and maintenance of high-performance hardware, increased energy usage, and potential requirements for cooling systems in data centers. Although AI can optimize certain aspects of blockchain operations, it is important to carefully manage these cost implications to ensure that the benefits outweigh the expenses.

6.4.4. Mitigation strategies

To mitigate the environmental impact of AI integration, several strategies can be employed:

- **Energy-efficient AI models**: Developing and using AI models that require less computational power without compromising performance can help reduce energy consumption.
- **Renewable energy adoption**: Encouraging the use of renewable energy sources for data centers and mining operations can significantly lower the carbon footprint.
- **Hybrid consensus mechanisms**: Implementing hybrid consensus mechanisms that combine AI with less energy-intensive consensus protocols, such as PoS, can reduce overall energy usage.
- **Optimization of AI workloads**: Employing techniques such as model pruning, quantization, and federated learning can optimize AI workloads, minimizing their environmental impact.

6.5. Security

The integration of AI into various systems has undeniably led to enhanced capabilities, greatly impacting the way businesses and industries operate. The remarkable abilities of AI models in data analysis, pattern recognition, and predictive analytics have brought about unparalleled advancements in automation, decision-making, and problem-solving. However, there is an important consideration to take into account: the emergence of intricate security challenges. As systems become more intelligent and interconnected, they also become attractive targets for cybercriminals, particularly in critical sectors that are crucial to the infrastructure and economy.

One of the most alarming threats in AI-driven systems is the prospect of adversarial attacks [80]. In such scenarios, malevolent actors deliberately manipulate input data to deceive AI models, causing them to produce incorrect or misleading results. For instance, subtle alterations to an image, indiscernible to the human eye, can cause an AI-driven recognition system to misclassify it entirely. This capability is especially concerning when considering applications in sectors like defense, finance, or healthcare, where an AI's erroneous decision can have grave consequences. Moreover, the often opaque and complex nature of AI models, sometimes referred to as the "black-box" phenomenon, exacerbates these vulnerabilities. When a system operates in ways not entirely understood even by its creators, identifying the root causes of breaches or failures becomes a daunting task.

The integration of AI into systems is not merely about harnessing its capabilities; it is equally about understanding and countering its vulnerabilities. Comprehensive security protocols, continuous monitoring, and rigorous testing are no longer optional—they are imperative. Understanding the intricacies of AI models, ensuring the integrity of the data they are trained on, and adopting a proactive stance towards potential threats can help in mitigating the risks. While the promise of AI is immense, safeguarding its deployment is crucial to truly harness its potential without compromising security.

6.6. Decentralization

Decentralization is a cornerstone of blockchain technology, offering transparency, trust, and resilience by distributing authority across multiple participants rather than concentrating it within a single entity [19,81]. However, the integration of AI into blockchain presents a paradox. Advanced AI models, despite their potential for optimization and enhanced efficiencies, often require significant computational resources. This could inadvertently favor participants with superior computational capabilities, leading to a potential centralization bias. If a small number of entities, equipped with the resources to run these intensive AI models, begin to dominate the blockchain network, it could undermine the trust and principles upon which blockchain is built.

Such a dominance by a select few not only disrupts the fundamental ethos of blockchain—a democratic system where every participant, regardless of their resources, has an equal stake—but also raises security concerns. Centralized nodes become attractive targets for malevolent actors, jeopardizing the system's integrity [19,82]. It becomes paramount, then, to ensure that the efficiencies promised by AI do not erode the essence of decentralization. This balance can be maintained through mechanisms such as equitable access to AI tools and incentives promoting diverse participation. Regular audits and vigilant monitoring can further prevent undue concentration of power. In essence, while the union of AI and blockchain heralds promising advancements, it is crucial that the spirit of decentralization remains intact.

7. Case studies

In recent years, the AI and blockchain consensus mechanisms has gained significant traction. This convergence aims to leverage the predictive and analytical capabilities of AI to enhance the efficiency, security, and adaptability of blockchain systems. Numerous AI models have been introduced to optimize the consensus process, reduce computational overhead, and address challenges inherent in traditional methods. By incorporating ML algorithms and neural network structures, these innovative models strive to ensure quicker transaction validations, minimize energy consumption, and offer a more resilient and dynamic consensus environment. Combining AI with blockchain's decentralized structure offers a promising future for smarter and self-adjusting blockchain systems [73,74].

7.1. AI for predicting miner selection

In Ethereum, several AI models, including linear regression, polynomial regression, and LSTM networks, have been employed to predict the next block reward and ether price [49]. This forecast assists miners in optimizing their operations by enhancing efficiency, increasing profitability, and reducing energy consumption. AI predictions enable miners to allocate resources more effectively, reducing waste and improving overall efficiency. By accurately anticipating block rewards, miners can maximize their profits and minimize the risk of losses. Optimized operations also contribute to lower energy consumption, promoting environmental sustainability. However, significant challenges exist. The requirement for substantial computational power can create a barrier to entry for smaller miners, potentially resulting in centralization. Accurate predictions demand substantial datasets, which can be difficult to obtain and manage. Moreover, developing and maintaining complex AI models necessitates specialized knowledge and resources [51].

7.2. Federated learning for consensus optimization

Federated learning is a technique used to train AI models across multiple nodes without centralizing data. This method enhances the security and privacy of the data used in the consensus process [73]. The primary advantages of federated learning include privacy preservation, decentralization, and scalability. Since data remain localized, the risk of data breaches is reduced, and privacy is enhanced. Distributing the training process across multiple nodes prevents centralization and ensures that no single entity dominates the network. Furthermore, federated learning allows the network to scale more efficiently by leveraging distributed computational resources. However, federated learning also presents challenges. One significant challenge is the need for frequent communication between nodes, which can increase latency and reduce efficiency. Additionally, variations in data quality and quantity across nodes can affect the performance of the AI models. Lastly, combining models from different nodes without centralizing data is complex and requires advanced techniques.

7.3. AI for detecting anomalous transactions

AI models, including neural networks and anomaly detection algorithms, are used to identify unusual patterns and potential attacks in blockchain transactions. The advantages of using AI for this purpose are enhanced security, real-time monitoring, and improved trust. AI algorithms can detect and mitigate fraudulent activities more effectively than conventional methods. Continuous monitoring of transactions assists in identifying and responding to threats promptly, which increases trust among users and stakeholders. However, implementing AI for detecting anomalous transactions also presents its own unique set of challenges. AI models may generate false positives, labeling legitimate transactions as suspicious. Monitoring transactions may raise privacy concerns, particularly if sensitive data are involved. Furthermore, implementing real-time monitoring necessitates substantial computational resources and infrastructure [83].

7.4. AI for consensus node selection

AI can play a crucial role in optimizing consensus node selection in blockchain networks. With the aid of AI algorithms, the network

can dynamically choose the most suitable nodes for consensus, thus enhancing both efficiency and security as per a recent study conducted by Saadat et al. [56]. The benefits of adopting AI for this purpose include optimized resource utilization, improved network performance, and enhanced security. AI can effectively identify nodes that possess the best performance metrics, thus ensuring that consensus is reached more swiftly and dependably. Nevertheless, this particular use case also faces certain challenges. For instance, the selection process might become biased towards nodes that possess more computational resources, which could potentially lead to centralization. Furthermore, implementing AI-based node selection necessitates continuous monitoring and updating of the selection criteria, which can be quite resource-intensive, as suggested by Kim [57].

7.5. AI for reducing energy consumption

An innovative method for incorporating AI with blockchain technology is the PoUW approach, such as Coin.AI. This method involves employing computational power to carry out useful work, like training deep learning models, rather than performing arbitrary calculations. The advantages of this technique include substantial reductions in energy waste, enhanced computational efficiency, and practical contributions to AI research. By aligning the computational efforts of miners with beneficial tasks, PoUW schemes address one of the main criticisms of conventional PoW systems. However, challenges still exist in terms of guaranteeing the equitable distribution of useful tasks and safeguarding the security and integrity of the blockchain [84].

8. Mitigation strategies

The incorporation of AI into blockchain systems presents several advantages, including increased efficiency, security, and adaptability. However, it also introduces complexities and potential data vulnerabilities. To address these challenges, various strategies have been suggested in the literature. This section examines some of these strategies in greater detail.

8.1. Federated learning and privacy-preserving techniques

Federated learning is a distributed approach to training models that uses local data samples on multiple decentralized devices or servers without requiring data exchange. This method mitigates the risk of data breaches since data remain on local devices. Research has demonstrated that federated learning can bolster privacy and security by ensuring that sensitive data never leave the local environment [73,74]. Moreover, incorporating techniques such as differential privacy can add noise to the data, thereby safeguarding individual data points from being reconstructed [85].

8.2. Secure multi-party computation

SMPC refers to a cryptographic protocol that facilitates multiple parties to jointly compute a function on their respective inputs while maintaining the confidentiality of those inputs. This method can be employed in AI-enhanced blockchain systems to process encrypted data, thereby ensuring that sensitive information remains concealed even during computation. SMPC has been extensively applied in circumstances that demand exceptional levels of privacy and security, thereby emerging as a reliable solution for mitigating data vulnerabilities in AI-integrated blockchain ecosystems [86,87].

8.3. Homomorphic encryption

Homomorphic encryption is a highly effective cryptographic method that enables computations to be carried out on encrypted data without the need for decryption. This allows AI models to be trained and used directly on encrypted data, ensuring that sensitive information remains safeguarded throughout the entire process. While homomorphic encryption may result in increased computational complexity, recent advances in this area have made its practical application in real-world scenarios more feasible [88].

8.4. Blockchain-based access control mechanisms

Incorporating cutting-edge access control mechanisms with blockchain technology can bolster security in AI applications. The immutable ledger of blockchain can be employed to maintain transparent and tamper-proof access control records. With the use of smart contracts, access policies can be automated and enforced, thereby ensuring that only authorized entities are able to access or modify data. This integration of blockchain and AI has the potential to substantially diminish the likelihood of unauthorized access and data breaches [89].

By employing these strategies, AI-enhanced blockchain systems can effectively mitigate the risks associated with increased complexity and the potential for data vulnerabilities. These methods, which have been extensively researched and successfully implemented, provide sturdy frameworks to strengthen security and manage the intricate challenges that arise from the integration of AI.

9. Future directions

Blockchain technology, coupled with the prowess of AI, is heading towards an evolutionary leap. This convergence is set to redefine the paradigms of decentralized consensus and network optimization. Below are some envisioned trajectories for future research and development.

9.1. Hybrid models

The integration of AI with blockchain consensus is anticipated to advance towards hybrid models. These models would seamlessly blend various AI techniques—like supervised, unsupervised, and reinforcement learning—or integrate AI with diverse consensus algorithms to construct a more robust and efficient system. By leveraging the complementary strengths of different methodologies, such as the predictive accuracy of ML and the adaptive capabilities of neural networks, hybrid models could offer enhanced decision-making processes, increased fault tolerance, and improved transaction validation efficiency.

9.2. AI in layer 2 solutions

AI's potential extends into the realm of layer 2 solutions, which operate on top of the blockchain to enhance scalability and speed. AI could significantly optimize these protocols, providing intelligent routing decisions in state channels, smarter payment networks, or even in the automatic scaling of sidechains based on transactional demands and network congestion. AI-driven layer 2 solutions promise to complement the underlying consensus mechanisms of blockchains, facilitating more agile and cost-effective transactions.

9.3. Self-adjusting blockchains

The vision of self-adjusting blockchains is predicated on the deployment of AI that can continuously learn from the network's activity and adapt its parameters in real-time. This could mean dynamic adjustment of block sizes, inter-block times, or even consensus rules based on real-time transaction throughput, node availability, or security threats. Such AI-powered blockchains would not just be reactive but proactively predict and mitigate potential network bottlenecks or security vulnerabilities, ensuring the blockchain operates at an optimal state at all times.

The trajectory of blockchain development is steering towards a more intelligent, responsive, and efficient infrastructure. By harnessing AI, future blockchains will not just perform as ledger systems but evolve into

smart and self-regulating ecosystems, capable of adapting to an ever-changing digital environment. These advancements will likely open up new possibilities for decentralized applications, governance models, and scalability solutions, making blockchain technology an even more integral part of the digital economy.

10. Conclusions

The incorporation of AI into blockchain consensus mechanisms heralds a transformative potential for the evolution of distributed ledger technologies. AI has the capacity to significantly bolster the efficiency, security, and adaptability of blockchain networks.

Opportunities: AI-driven consensus models like PoLE can leverage computational resources for neural network training, thus ensuring the work done by miners contributes directly to valuable computational tasks. Hybrid models combining different AI techniques offer the promise of enhanced decision-making and fault tolerance. With AI's predictive analytics, blockchain systems can adapt in real-time to changes in transaction volume or network threats, optimizing their performance and robustness. Moreover, AI could enhance layer 2 solutions, making them more efficient and responsive to the needs of the network.

Challenges: However, the integration of AI and blockchain is not without its challenges. The introduction of AI opens up new vectors for potential cyberattacks, making security a primary concern. The complexity of AI models also presents issues of transparency and interpretability, often referred to as the "black box" problem, which could hinder trust in the system. Furthermore, the risk of centralization arises if AI optimizations inadvertently give significant advantages to nodes with more computational resources.

In summary, the potential of AI in enhancing blockchain consensus is vast, offering exciting opportunities for innovation and optimization. Yet, caution must be exercised to address the inherent challenges to ensure that the decentralization and security that are the hallmarks of blockchain technology remain intact. The successful fusion of AI and blockchain will depend on a delicate balance between leveraging the capabilities of AI and maintaining the fundamental principles of blockchain technology.

CRediT authorship contribution statement

Syamsul Rizal: Writing—original draft. **Dong-Seong Kim:** Supervision, Validation, Writing—review & editing.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used PAPERPAL in order to check the paper grammar. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

Funding

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2023-2020-0-01612, 50%) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation).

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2018R1A6A1A03024003, 50%).

Declaration of competing interest

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

References

[1] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, http://www.bitcoin.org/bitcoin.pdf, 2009. (Accessed 23 July 2024).

[2] A. Zwitter, J. Hazenberg, Decentralized network governance: blockchain technology and the future of regulation, Front. Blockchain 3 (2020) 12, https://doi.org/10.3389/fbloc.2020.00012.

[3] Y. Chen, C. Bellavitis, Blockchain disruption and decentralized finance: the rise of decentralized business models, J. Bus. Ventur. Insights 13 (2020) e00151, https://doi.org/10.1016/j.jbvi.2019.e00151.

[4] R. Patel, A. Sethia, S. Patil, Blockchain – future of decentralized systems, in: Proceedings of the 2018 International Conference on Computing, Power and Communication Technologies, IEEE, 2018, pp. 369–374, https://doi.org/10.1109/GUCON.2018.8675091.

[5] D. Ongaro, J. Ousterhout, In search of an understandable consensus algorithm, in: Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference, USENIX Association, Berkeley, CA, USA, 2014, pp. 305–320.

[6] Q. Wang, J. Huang, S. Wang, et al., A comparative study of blockchain consensus algorithms, J. Phys. Conf. Ser. 1437 (1) (2020) 012007, https://doi.org/10.1088/1742-6596/1437/1/012007.

[7] M. Du, X. Ma, Z. Zhang, et al., A review on consensus algorithm of blockchain, in: Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics, IEEE, 2017, pp. 2567–2572, https://doi.org/10.1109/SMC.2017.8123011.

[8] K. Croman, C. Decker, I. Eyal, et al., On scaling decentralized blockchains, in: J. Clark, S. Meiklejohn, P.Y. Ryan, et al. (Eds.), Financial Cryptography and Data Security, Springer, Berlin, Heidelberg, 2016, pp. 106–125, https://doi.org/10.1007/978-3-662-53357-4_8.

[9] S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, 3rd ed., Pearson Education, Upper Saddle River, NJ, USA, 2010.

[10] Digiconomist, Bitcoin energy consumption, https://digiconomist.net/bitcoin-energy-consumption, 2023. (Accessed 23 July 2024).

[11] S. Gupta, M. Sadoghi, Blockchain transaction processing, in: S. Sakr, A.Y. Zomoya (Eds.), Encyclopedia of Big Data Technologies, Springer, Cham, 2019, pp. 366–376, https://doi.org/10.1007/978-3-319-77525-8_333.

[12] M. Xie, J. Liu, S. Chen, et al., A survey on blockchain consensus mechanism: research overview, current advances and future directions, Int. J. Intell. Comput. Cybern. 16 (2) (2023) 314–340, https://doi.org/10.1108/ijicc-05-2022-0126.

[13] Y. Liang, Blockchain for dynamic spectrum management, in: Dynamic Spectrum Management, Signals and Communication Technology, Springer, Singapore, 2020, pp. 121–146, https://doi.org/10.1007/978-981-15-0776-2_5.

[14] N. Singh, M. Vardhan, Computing optimal block size for blockchain based applications with contradictory objectives, Proc. Comput. Sci. 171 (2020) 1389–1398, https://doi.org/10.1016/j.procs.2020.04.149.

[15] R.C. Merkle, A digital signature based on a conventional encryption function, in: C. Pomerance (Ed.), Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 1988, pp. 369–378, https://doi.org/10.1007/3-540-48184-2_32.

[16] H. Liu, X. Luo, H. Liu, et al., Merkle tree: a fundamental component of blockchains, in: Proceedings of the 2021 International Conference on Electronic Information Engineering and Computer Science, IEEE, 2021, pp. 556–561, https://doi.org/10.1109/eiecs53707.2021.9588047.

[17] Y. Chen, Y. Chou, Y. Chou, An image authentication scheme using Merkle tree mechanisms, Future Internet 11 (7) (2019) 149, https://doi.org/10.3390/fi11070149.

[18] P. Zheng, Z. Jiang, J. Wu, et al., Blockchain-based decentralized application: a survey, IEEE Open J. Comput. Soc. 4 (2023) 121–133, https://doi.org/10.1109/ojcs.2023.3251854.

[19] J. Zarrin, H. Phang, L. Saheer, et al., Blockchain for decentralization of internet: prospects, trends, and challenges, Clust. Comput. 24 (4) (2021) 2841–2866, https://doi.org/10.1007/s10586-021-03301-8.

[20] J. Lee, B. Lee, J. Jung, et al., DQ: Two approaches to measure the degree of decentralization of blockchain, ICT Express 7 (3) (2021) 278–282, https://doi.org/10.1016/j.icte.2021.08.008.

[21] R. Pandey, M. Faiyaz, G. Singh, et al., Functional analysis of blockchain consensus algorithms, in: R. Pandey, S. Goundar (Eds.), Distributed Computing to Blockchain: Architecture, Technology, and Applications, Academic Press, Cambridge, MA, 2023, pp. 207–233, https://doi.org/10.1016/b978-0-323-96146-2.00005-x.

[22] M. Arakawa, K. Shudo, Block interval adjustment based on block propagation time in a blockchain, in: Proceedings of the 2022 IEEE International Conference on Blockchain, IEEE, 2022, pp. 202–207, https://doi.org/10.1109/Blockchain55522.2022.00035.

[23] Z. Abadin, M. Syed, A pattern for proof of work consensus algorithm in blockchain, in: Proceedings of the 26th European Conference on Pattern Languages of Programs, ACM, 2021, pp. 1–6, https://doi.org/10.1145/3489449.3489994.

[24] N. Lasla, L. Al-Sahan, M. Abdallah, et al., Green-PoW: an energy-efficient blockchain proof-of-work consensus algorithm, Comput. Netw. 214 (2022) 109118, https://doi.org/10.1016/j.comnet.2022.109118.
[25] A. Narayanan, J. Bonneau, E. Felten, et al., Bitcoin and Cryptocurrency Technologies, Princeton University Press, Princeton, NJ, USA, 2016.
[26] C. Mora, R. Rollins, K. Taladay, et al., Bitcoin emissions alone could push global warming above 2°C, Nat. Clim. Change 8 (11) (2018) 931–933, https://doi.org/10.1038/s41558-018-0321-8.
[27] A. Gervais, G. Karame, K. Wüst, et al., On the security and performance of proof of work blockchains, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 3–16, https://doi.org/10.1145/2976749.2978341.
[28] W. Maung Maung Thin, N. Dong, G. Bai, et al., Formal analysis of a proof-of-stake blockchain, in: Proceedings of the 2018 23rd International Conference on Engineering of Complex Computer Systems, IEEE, 2018, pp. 197–200, https://doi.org/10.1109/ICECCS2018.2018.00031.
[29] L. Ge, J. Wang, G. Zhang, Survey of consensus algorithms for proof of stake in blockchain, Secur. Commun. Netw. 2022 (1) (2022) 2812526, https://doi.org/10.1155/2022/2812526.
[30] K. Ambili, M. Sindhu, M. Sethumadhavan, On federated and proof of validation based consensus algorithms in blockchain, IOP Conf. Ser. Mater. Sci. Eng. 225 (2017) 1–9, https://doi.org/10.1088/1757-899x/225/1/012198.
[31] Z. Hussein, M. Salama, S. El-Rahman, Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms, Cybersecurity 6 (1) (2023) 30, https://doi.org/10.1186/s42400-023-00163-y.
[32] A. Li, X. Wei, Z. He, Robust proof of stake: a new consensus protocol for sustainable blockchain systems, Sustainability 12 (7) (2020) 2824, https://doi.org/10.3390/su12072824.
[33] Q. Hu, B. Yan, Y. Han, et al., An improved delegated proof of stake consensus algorithm, Procedia Comput. Sci. 187 (2021) 341–346, https://doi.org/10.1016/j.procs.2021.04.109.
[34] V. Bachani, A. Bhattacharjya, Preferential delegated proof of stake (PDPoS): modified DPoS with two layers towards scalability and higher TPS, Symmetry 15 (1) (2023) 4, https://doi.org/10.3390/sym15010004.
[35] W. Li, X. Deng, J. Liu, et al., Delegated proof of stake consensus mechanism based on community discovery and credit incentive, Entropy 25 (9) (2023) 1320, https://doi.org/10.3390/e25091320.
[36] S. Ajakwe, I. Saviour, J. Kim, et al., BANDA: a novel blockchain-assisted network for drone authentication, in: Proceedings of the 2023 Fourteenth International Conference on Ubiquitous and Future Networks, IEEE, 2023, pp. 120–125, https://doi.org/10.1109/ICUFN57995.2023.10201012.
[37] A. Zainudin, R. Alief, M. Putra, et al., Blockchain-based decentralized trust aggregation for federated cyber-attacks classification in SDN-enabled maritime transportation systems, in: Proceedings of the 2023 IEEE International Conference on Communications Workshops, IEEE, 2023, pp. 182–187, https://doi.org/10.1109/ICCWorkshops57953.2023.10283507.
[38] S. Dziembowski, S. Faust, V. Kolmogorov, et al., Proofs of space, in: R. Gennaro, M. Robshaw (Eds.), Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2015, pp. 585–605, https://doi.org/10.1007/978-3-662-48000-7_29.
[39] W. Zhong, C. Yang, W. Liang, et al., Byzantine fault-tolerant consensus algorithms: a survey, Electronics 12 (18) (2023) 3801, https://doi.org/10.3390/electronics12183801.
[40] H. Qin, Y. Cheng, X. Ma, et al., Weighted byzantine fault tolerance consensus algorithm for enhancing consortium blockchain efficiency and security, J. King Saud Univ, Comput. Inf. Sci. 34 (10) (2022) 8370–8379, https://doi.org/10.1016/j.jksuci.2022.08.017.
[41] P. Cunningham, M. Cord, S. Delany, Supervised learning, in: M. Cord, P. Cunningham (Eds.), Machine Learning Techniques for Multimedia, Springer, Berlin, Heidelberg, 2008, pp. 21–49, https://doi.org/10.1007/978-3-540-75171-7_2.
[42] Q. Liu, Y. Wu, Supervised learning, in: N. Seel (Ed.), Encyclopedia of the Sciences of Learning, Springer, Boston, MA, 2012, pp. 3243–3245, https://doi.org/10.1007/978-1-4419-1428-6_451.
[43] Z. Ghahramani, Unsupervised learning, in: O. Bousquet, U. Luxburg, G. Rätsch (Eds.), Advanced Lectures on Machine Learning, Springer, Berlin, Heidelberg, 2004, pp. 72–112, https://doi.org/10.1007/978-3-540-28650-9_5.
[44] M. Khanum, T. Mahboob, W. Imtiaz, et al., A survey on unsupervised machine learning algorithms for automation, classification and maintenance, Int. J. Comput. Appl. 119 (13) (2015) 34–39, https://doi.org/10.5120/21131-4058.
[45] R. Sutton, A. Barto, Reinforcement learning: an introduction, IEEE Trans. Neural Netw. 9 (5) (1998) 1054, https://doi.org/10.1109/tnn.1998.712192.
[46] M. Wiering, M. Otterlo, in: Reinforcement Learning, Springer, Berlin, Heidelberg, 2012, https://doi.org/10.1007/978-3-642-27645-3.
[47] I. Sarker, Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions, SN Comput. Sci. 2 (6) (2021) 420, https://doi.org/10.1007/s42979-021-00815-1.
[48] L. Alzubaidi, J. Zhang, A. Humaidi, et al., Review of deep learning: concepts, CNN architectures, challenges, applications, future directions, J. Big Data 8 (1) (2021) 1–74, https://doi.org/10.1186/s40537-021-00444-8.
[49] J. Simon, K. Geetha, Block mining reward prediction with polynomial regression, long short-term memory, and prophet API for Ethereum blockchain miners, ITM Web Conf. 37 (2021) 01004, https://doi.org/10.1051/itmconf/20213701004.
[50] C. Butler, M. Crane, Blockchain transaction fee forecasting: a comparison of machine learning methods, Mathematics 11 (9) (2023) 2212, https://doi.org/10.3390/math11092212.
[51] A. Laurent, L. Brotcorne, B. Fortz, Transaction fees optimization in the ethereum blockchain, Blockchain Res. Appl. 3 (3) (2022) 100074, https://doi.org/10.1016/j.bcra.2022.100074.
[52] L. Zhang, R. Zhou, Q. Liu, et al., Transaction fee estimation in the Bitcoin system, arXiv, 2024, preprint, arXiv:2405.15293, https://arxiv.org/abs/2405.15293.
[53] C. Decker, R. Wattenhofer, Information propagation in the Bitcoin network, in: Proceedings of the IEEE P2P 2013 Proceedings, IEEE, 2013, pp. 1–10, https://doi.org/10.1109/P2P.2013.6688704.
[54] S. Mohammadi, E. Rabieinejad, Prediction forks in the blockchain using machine learning, in: Proceedings of the 3rd International Conference on Mechanics, Electricals and Computers Engineering, 2020, pp. 1–8, https://doi.org/10.1109/P2P.2013.6688704.
[55] Z. Sharifian, H. Saidi, A. Fanian, et al., A new approach to orphan blocks in the Nakamoto consensus blockchain, IEEE Trans. Netw. Sci. Eng. 11 (2) (2024) 1771–1784, https://doi.org/10.1109/tnse.2023.3331014.
[56] K. Saadat, N. Wang, R. Tafazolli, AI-enabled blockchain consensus node selection in cluster-based vehicular networks, IEEE Netw. Lett. 5 (2) (2023) 115–119, https://doi.org/10.1109/lnet.2023.3238964.
[57] S. Kim, Blockchain smart contract to prevent forgery of degree certificates: artificial intelligence consensus algorithm, Electronics 11 (14) (2022) 2112, https://doi.org/10.3390/electronics11142112.
[58] Y. Wu, P. Song, F. Wang, Hybrid consensus algorithm optimization: a mathematical method based on POS and PBFT and its application in blockchain, Math. Probl. Eng. 2020 (1) (2020) 7270624, https://doi.org/10.1155/2020/7270624.
[59] W. Wang, D. Hoang, P. Hu, et al., A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370, https://doi.org/10.1109/access.2019.2896108.
[60] H. Kim, S. Kim, J. Hwang, et al., Efficient privacy-preserving machine learning for blockchain network, IEEE Access 7 (2019) 136481–136495, https://doi.org/10.1109/access.2019.2940052.
[61] J. Kim, M. Nakashima, W. Fan, et al., A machine learning approach to anomaly detection based on traffic monitoring for secure blockchain networking, IEEE Trans. Netw. Serv. Manag. 19 (3) (2022) 3619–3632, https://doi.org/10.1109/tnsm.2022.3173598.
[62] S. Sayadi, S. Rejeb, Z. Choukair, Anomaly detection model over blockchain electronic transactions, in: Proceedings of the 2019 15th International Wireless Communications & Mobile Computing Conference, IEEE, 2019, pp. 895–900, https://doi.org/10.1109/iwcmc.2019.8766765.
[63] K. Venkatesan, S. Rahayu, Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques, Sci. Rep. 14 (1) (2024) 1149, https://doi.org/10.1038/s41598-024-51578-7.
[64] M. Platt, P. McBurney, Sybil in the haystack: a comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance, Algorithms 16 (1) (2023) 34, https://doi.org/10.3390/a16010034.
[65] A. Haddaji, S. Ayed, L.C. Fourati, Blockchain-based multi-levels trust mechanism against Sybil attacks for vehicular networks, in: Proceedings of the 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), IEEE, 2020, pp. 155–163, https://doi.org/10.1109/bigdatase50710.2020.00028.
[66] S. Azam, M. Bibi, R. Riaz, et al., Collaborative learning based sybil attack detection in vehicular AD-HOC networks (VANETS), Sensors 22 (18) (2022) 6934, https://doi.org/10.3390/s22186934.
[67] M. Mounica, R. Vijayasaraswathi, RETRACTED: Detecting Sybil Attack In Wireless Sensor Networks Using Machine Learning Algorithms, IOP Conf. Ser. Mater. Sci. Eng. 1042 (1) (2021) 012029, https://doi.org/10.1088/1757-899x/1042/1/012029.
[68] Y. Zhu, J. Zeng, F. Weng, et al., Sybil attacks detection and traceability mechanism based on beacon packets in connected automobile vehicles, Sensors 24 (7) (2024) 2153, https://doi.org/10.3390/s24072153.
[69] S. Aladhadh, H. Alwabli, T. Moulahi, et al., BChainGuard: a new framework for cyberthreats detection in blockchain using machine learning, Appl. Sci. 12 (23) (2022) 12026, https://doi.org/10.3390/app122312026.
[70] N. Sabry, B. Shabana, M. Handosa, et al., Adapting blockchain's proof-of-work mechanism for multiple traveling salesmen problem optimization, Sci. Rep. 13 (1) (2023) 14676, https://doi.org/10.1038/s41598-023-41536-0.
[71] G. Leduc, S. Kubler, J. Georges, Sabine: self-adaptive BlockchaIn coNsEnsus, in: Proceedings of the 2022 9th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2022, pp. 234–240, https://doi.org/10.1109/FiCloud57274.2022.00039.
[72] A. Alofi, M.A. Bokhari, R. Bahsoon, et al., Optimizing the energy consumption of blockchain-based systems using evolutionary algorithms: a new problem formulation, IEEE Trans. Sustain. Comput. 7 (4) (2022) 910–922, https://doi.org/10.1109/tsusc.2022.3160491.
[73] V. Abhishek, S. Binny, T. Johan, et al., Federated learning: collaborative machine learning without centralized training data, Int. J. Eng. Technol. Manag. Sci. 6 (5) (2022) 355–359, https://doi.org/10.46647/ijetms.2022.v06i05.052.
[74] H. McMahan, E. Moore, D. Ramage, et al., Communication-efficient learning of deep networks from decentralized data, arXiv, 2016, preprint, arXiv:1602.05629, https://arxiv.org/abs/1602.05629.

[75] A. Shamsan Saleh, Blockchain for secure and decentralized artificial intelligence in cybersecurity: a comprehensive review, Blockchain Res. Appl. 5 (3) (2024) 100193, https://doi.org/10.1016/j.bcra.2024.100193.

[76] M. Amini, M. Jesus, D. Sheikholeslami, et al., Artificial intelligence ethics and challenges in healthcare applications: a comprehensive review in the context of the European GDPR mandate, Mach. Learn. Knowl. Extr. 5 (3) (2023) 1023–1035, https://doi.org/10.3390/make5030053.

[77] J. You, Curvetime: a blockchain framework for Artificial Intelligence computation, Softw. Impacts 13 (2022) 100314, https://doi.org/10.1016/j.simpa.2022.100314.

[78] D. Patterson, J. Gonzalez, U. Holzle, et al., The carbon footprint of machine learning training will Plateau, then shrink, Computer 55 (7) (2022) 18–28, https://doi.org/10.1109/mc.2022.3148714.

[79] C. Stoll, L. Klaaßen, U. Gallersdörfer, The carbon footprint of Bitcoin, Joule 3 (7) (2019) 1647–1661, https://doi.org/10.1016/j.joule.2019.05.012.

[80] S. Qiu, Q. Liu, S. Zhou, et al., Review of artificial intelligence adversarial attack and defense technologies, Appl. Sci. 9 (5) (2019) 909, https://doi.org/10.3390/app9050909.

[81] P. Schmid, A. Schaffhäuser, R. Kashef, IoTBChain: adopting blockchain technology to increase PLC resilience in an IoT environment, Information 14 (8) (2023) 437, https://doi.org/10.3390/info14080437.

[82] M. Hoffman, L. Ibáñez, E. Simperl, Toward a formal scholarly understanding of blockchain-mediated decentralization: a systematic review and a framework, Front. Blockchain 3 (2020) 35, https://doi.org/10.3389/fbloc.2020.00035.

[83] X. Ma, D. Yu, Y. Du, et al., A blockchain-based incentive mechanism for sharing cyber threat intelligence, Electronics 12 (11) (2023) 2454, https://doi.org/10.3390/electronics12112454.

[84] A. Baldominos, Y. Saez, Coin.AI: a proof-of-useful-work scheme for blockchain-based distributed deep learning, Entropy 21 (8) (2019) 723, https://doi.org/10.3390/e21080723.

[85] C. Dwork, A. Roth, The algorithmic foundations of differential privacy, Found. Trends Theor. Comput. Sci. 9 (3–4) (2014) 211–407, https://doi.org/10.1561/0400000042.

[86] Y. Lindell, Secure multiparty computation, Commun. ACM 64 (1) (2020) 86–96, https://doi.org/10.1145/3387108.

[87] P. Mohassel, Y. Zhang, SecureML: a system for scalable privacy-preserving machine learning, in: Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), IEEE, 2017, pp. 19–38, https://doi.org/10.1109/sp.2017.12.

[88] R. Kumar, J. Kumar, A. Khan, et al., Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images, Comput. Med. Imag. Graph. 102 (2022) 102139, https://doi.org/10.1016/j.compmedimag.2022.102139.

[89] G. Zyskind, O. Nathan, A. Pentland, Decentralizing privacy: using blockchain to protect personal data, in: Proceedings of the 2015 IEEE Security and Privacy Workshops, IEEE, 2015, pp. 180–184, https://doi.org/10.1109/SPW.2015.27.