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

An Investigative Analysis of Adaptive Consensus Mechanisms for Distributed Blockchain Systems

Smita Bhore[1], Natraj N. A.[1,*]

[1] Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, Maharashtra, India

Abstract

INTRODUCTION: Blockchain technology has achieved widespread adoption across diverse application domains, yet its foundational consensus mechanisms remain largely static and may not suited to the dynamic, heterogeneous conditions of modern decentralized networks. While adaptive consensus has emerged as a promising solution, a comprehensive and systematic framework for classifying, evaluating, and selecting adaptive mechanisms remains notably absent.
OBJECTIVES: This survey addresses this critical gap by introducing a structured taxonomy of adaptive consensus mechanisms for distributed blockchain systems, underpinned by a systematic review of performance evidence and real-world deployment experiences.
METHODS: Following PRISMA 2020 guidelines, we conducted a systematic search of 1,675 records from Scopus (2020–2025), ultimately including 68 peer-reviewed studies. We analyze four principal categories of adaptive consensus namely dynamic parameter adjustment, consensus algorithm switching, hybrid mechanisms, and AI/ML-enhanced protocols across five key performance dimensions: throughput, scalability, energy efficiency, security level, and implementation complexity. Case studies of SABEC for UAV coordination, 6G cognitive radio spectrum management, and supply chain networks illustrate real-world deployment trade-offs.
RESULTS: Our comparative analysis reveals fundamental performance–security trade-offs inherent to each adaptive category. Dynamic parameter adjustment mechanisms offer low implementation complexity but limited scalability gains; algorithm-switching approaches achieve high throughput (100–1,000 TPS) at the cost of very high implementation complexity; hybrid schemes such as HyFlexChain demonstrate 112.5+ TPS under BFT mode with high security but remain at the prototype stage; and AI/ML-enhanced protocols show theoretical promise yet face critical security challenges including adversarial attacks and model poisoning that undermine system trustworthiness. The maturity assessment confirms that higher implementation complexity consistently correlates with limited real-world deployment.
CONCLUSION: Our findings demonstrate that no universal adaptive consensus mechanism exists for blockchain applications. This structured, evidence-grounded survey provides an effective methodology for designing, evaluating, and selecting adaptive consensus solutions for diverse decentralized system deployments.

Keywords: Adaptive Consensus, Blockchain Technology, Consensus Mechanisms, Dynamic Consensus, Hybrid Consensus, Proof of Work, Proof of Stake, Byzantine Fault Tolerance, Scalability, Security

Received on 27 November 2025, accepted on 02 April 2026, published on 23 April 2026

doi: 10.4108/eetiot.11144

1. Introduction

Blockchain technology has emerged as a revolutionary innovation, which provides a robust foundation for decentralized, secure data management across diverse

*Corresponding author. Email: natraj@sidtm.edu.in

application domains [1]. A blockchain is a distributed, immutable ledger of transactions that operates without any central authority [1]. The consensus mechanism rules enable distributed participants to agree on transaction validity and ledger state, forming the cornerstone of the decentralized paradigm [2]. Traditional static consensus protocols like Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT) variants have facilitated blockchain's initial success. Nonetheless, such paradigm protocols with specific parameters and predetermined algorithms have great drawbacks in facing varying requirements of the applied field and result to shifting operational conditions. Despite blockchain's potential, critical technical challenges persist regarding scalability, privacy, and security vulnerabilities such as selfish mining [3]. The unpredictability of the real-world networks significantly impairs the performance and reliability of the traditional consensus algorithms [4].

1.1 Terminology and Definitions

The following important terms are being defined here to keep themselves clear and consistent when discussing this survey: Adaptive Consensus: An umbrella term under which all consensus mechanisms could signal their change in behavior, parameters, or algorithms due to changing network conditions or requirements. Dynamic Consensus: A subclass of adaptive consensus focused specifically on mechanisms that modify certain operational parameters (e.g., difficulty and block time) but within one algorithm framework.
Hybrid Consensus: Consensus mechanisms that combine properties of two or more different consensus algorithms, simultaneously or in turn.
Switching of Consensus Algorithms: Means the ability to change from one consensus algorithm to another, a completely different one, while the program is running.
Static Consensus: The Traditional consensus mechanism is comprised of fixed parameters and algorithms that do not have any flexibility to meet changing conditions.
Self-Calibrating Consensus: Adaptive consensus mechanisms that adjust themselves in parameters automatically without requiring external intervention. Meta-Consensus: Protocols higher than the others on which depend the selection and transitions among different consensus mechanisms.

1.2 Research Gap and Motivation

Concepts of static consensus mechanisms are tradeoffs - protocols that are secure might be slow, or be energy intensive. These fixed protocols do not work optimally when blockchain networks are highly dynamic, in terms of size, the volume of transactions or when the systems witness new adversarial agent behaviors. The existing blockchain implementations do not have the resilience to dynamically adapt to dynamic conditions, which makes more flexible methods urgent. Adaptive consensus has now been worked out as a potential solution to these issues [5]. Through this method, blockchain networks can dynamically modify the consensus mechanism or operation parameters with regard to the changing network situations, security threats, or application needs [5]. With the contextualization of the agreement process, the model of adaptive consensus, in theory, may provide improved performance guarantees, additional security, more quantity/cost-efficient resource use, and cross-application versatility of the blockchain. While many adaptive models remain theoretical, a systematic, application-driven framework has recently been introduced to provide a quantitative synthesis of performance benchmarks for hybrid mechanisms, specifically addressing the resource constraints of IoT environments [6].

1.3 Research Contribution

This survey provides several key contributions to the blockchain research community:

- A detailed technical discussion of adaptive consensus algorithms, and how these algorithms evolved out of earlier, static algorithms
- A novel four-category taxonomy classifying adaptive consensus mechanisms by adaptation strategy (dynamic parameter adjustment, algorithm switching, hybrid design, and AI/ML-driven adaptation)
- Objective assessment of technical issues and constraints peculiar to adaptive consensus systems
- Identification of high-priority future research directions including standardization, interoperability, and AI trustworthiness in adaptive consensus.

Unlike existing surveys that address consensus mechanisms in general (e.g., Hussein et al. [17]; Shen et al. [3]) without systematic differentiation of adaptive strategies, this survey focuses exclusively on adaptive mechanisms through a purpose-built taxonomy. In contrast to bibliometric overviews such as Ahn et al. [69] and broad algorithmic reviews by Xiong et al. [43] and Li [44], this work provides domain-specific quantitative benchmarking across UAV, 6G, and supply chain environments. Critically, this survey directly extends the foundational IoT-focused quantitative framework introduced by Natraj et al. [6] (EAI Endorsed Transactions on Internet of Things), expanding the scope from hybrid mechanisms in IoT resource-constrained systems to the full spectrum of adaptive consensus strategies. The current paper's PRISMA-guided methodology, four-level deployment maturity model, and cross-domain case study synthesis offer contributions not present in any of the foregoing works.
This article is composed as follows: Section 2 is a literature

review of blockchain consensus-related mechanisms with a specific focus on recent developments and transition to adaptive approaches. Section 3 identifies and examines the principal adaptive consensus mechanisms. In Section 4, important technical problems and constraints are reviewed. Section 5 investigates future research opportunities, and Section 6 makes concluding remarks detailing the most important findings and future perspectives of adaptive consensus in blockchain technology.

1.4 Literature survey strategy

This section describes our systematic and purposive approach following PRISMA 2020 guidelines [7] to ensure transparency and reproducibility.

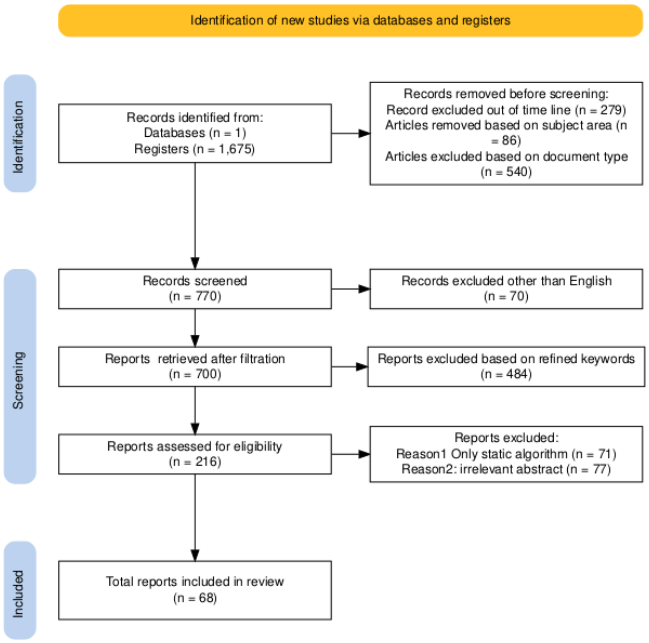

Figure 1. PRISMA 2020 Flow Diagram

The literature search conducted using the PRISMA model[2] in Figure 1, was explored through Scopus as the primary database, yielding 1,675 initial records from databases and registers. The search strategy employed carefully crafted strings combining terms related to adaptive consensus mechanisms ("adaptive consensus," "dynamic consensus," "flexible consensus," "self-adjusting consensus," "hybrid consensus," "algorithm switching") with blockchain-related terminology ("blockchain," "distributed ledger," "DLT") and implementation descriptors ("mechanism," "algorithm," "protocol"). The search was restricted to English-language publications from 2020-2025, with execution occurring between September 15-30, 2025, and an update conducted on October 15, 2025. Scopus was selected for its comprehensive peer-reviewed content coverage, rigorous indexing standards, and advanced search capabilities essential for capturing the interdisciplinary nature of adaptive consensus research spanning AI/ML, IoT, telecommunications, and distributed systems. The complete Scopus query string executed was: TITLE-ABS-KEY ((“adaptive consensus" OR "dynamic consensus" OR "flexible consensus" OR "self-adjusting consensus" OR "hybrid consensus" OR "algorithm switching”) AND ("blockchain" OR "distributed ledger" OR "DLT") AND ("mechanism" OR "algorithm" OR "protocol")) AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND SUBJAREA (comp OR engi) AND LANGUAGE (english) AND DOCTYPE (ar OR re) Records retrieved from Scopus were exported to Microsoft Excel for manual deduplication. Duplicate records were identified by cross-checking DOI, title, and author fields. This process confirmed that no duplicate entries were present in the retrieved dataset of 1,675 records, consistent with Scopus's built-in deduplication applied at the point of export. All 1,675 records therefore proceeded directly to the title and abstract screening stage. Studies were assessed for inclusion or exclusion based on the following pre-defined operational criteria. **Inclusion criteria:** (1) published between January 2020 and October 2025; (2) written in English; (3) published as a peer- reviewed journal article, conference paper, or arXiv preprint; (4) proposes, implements, or evaluates a blockchain consensus mechanism with at least one adaptive element defined as dynamic parameter adjustment, algorithm switching, hybrid design, or AI/ML-driven adaptation; (5) provides quantitative performance metrics or formal qualitative analysis. Foundational whitepapers (Bitcoin, Ethereum) were included selectively to provide essential historical context. **Exclusion criteria:** (1) publications outside the 2020–2025 date range; (2) non-English language; (3) editorials, opinion pieces, or secondary news articles with no original technical contribution; (4) papers in which the term "adaptive" appears only descriptively but the consensus mechanism itself uses fixed parameters; (5) duplicate records.

The screening process followed a systematic approach that reduced the initial 1,676 records to 68 final included studies through multiple filtration stages. During identification, 905 records were removed due to following reasons:

1) temporal constraints (279) 2) subject area relevance (86), 3) document type appropriateness (540). The screening phase further excluded 70 non-English records and 484 reports based on refined keyword criteria, leaving 216 reports for eligibility assessment. The final exclusion removed 71 studies presenting only static algorithms without adaptive elements and 77 with irrelevant abstracts, ultimately including peer-reviewed papers demonstrating genuine adaptability in consensus mechanisms, theoretical frameworks with quantitative metrics or qualitative analysis, and seminal foundational documents such as the Bitcoin and Ethereum whitepapers that provide essential context for understanding consensus

[2] Generated using PRISMA2020 R package [7] for PRISMA 2020 compliance.

evolution in distributed systems.
Our systematic search focused exclusively on peer- reviewed publications indexed in Scopus to maintain quality control and ensure rigorous vetting. However, adaptive consensus is a rapidly evolving field where significant contributions often appear first as preprints. We therefore supplemented our systematic search with targeted inclusion of preprints meeting these criteria. Out of the final included studies, some are preprints (marked with arXiv identifiers in references. This hybrid approach balances systematic rigor with coverage of cutting-edge developments. White papers included represent historical context rather than claims of novel adaptive mechanisms.

2. Literature Review

Blockchain consensus mechanisms have evolved considerably, with recent attention shifting toward adaptive approaches. This survey examines developments in adaptive consensus from 2020-2025, including analysis of real-world deployments in IoT, 6G, UAV, and supply chain applications.

2.1 Traditional Consensus Mechanisms

Bitcoin's Proof of Work (PoW) [8] provides security guarantees but faces challenges with energy consumption and scalability [9][10]. PoW exhibits a significant limitation, as it consistently favours nodes with the highest computational power, thus challenging the achievement of a truly decentralised and equitable system [11]. Alternative mechanisms include Proof of Stake (PoS), which selects validators based on stake holdings [12], and Delegated Proof of Stake (DPoS), where token holders elect validators [13]. Byzantine Fault Tolerance (BFT) algorithms like Practical Byzantine Fault Tolerance (PBFT) address consensus with faulty or malicious nodes, particularly in permissioned networks [14]. Table 1 compares attack resistance characteristics across these mechanisms.

Table 1. Attack Resistance Comparison

Consensus Algorithm	Attacks					
	Sybil	DoS	Byzantine	Eclipse	51%	Routing
PoW	Strong Resistance	Moderate Resistance	Strong Resistance	Low Resistance	Low Resistance	Moderate Resistance
PoS	Moderate Resistance	Moderate Resistance	Moderate Resistance	Low Resistance	Low Resistance	Moderate Resistance
DPoS	Moderate Resistance	Low Resistance	Low Resistance	Low Resistance	Moderate Resistance	Moderate Resistance
PBFT	Strong Resistance	Low Resistance	Moderate Resistance	Low Resistance	Strong Resistance	Low Resistance
PoA	Strong Resistance	Low Resistance	Moderate Resistance	Low Resistance	Strong Resistance	Low Resistance

2.2 Evolution Toward Adaptive Consensus

Dynamic Parameter Adjustment

Several studies propose dynamically modifying consensus parameters. Adaptive Proof of Work (APoW) adjusts the mining difficulty in response to hash rate fluctuations to improve resilience [15].

Algorithm Switching

The parallel execution of multiple consensus algorithms is an emerging strategy to enhance scalability, efficiency, and fault tolerance in distributed systems and blockchains [16]. Meta-consensus frameworks enable parallel execution of multiple consensus algorithms, routing transactions based on current requirements [17]. This approach extends beyond traditional single-algorithm implementations.

Hybrid Consensus

Hybrid consensus mechanisms in blockchain integrate features from multiple traditional consensus algorithms—such as Proof of Work (PoW) and Proof of Stake (PoS) in [18], and Practical Byzantine Fault Tolerance (BFT) and Proof of Stake (PoS) in [19] to overcome the limitations of single-method approaches. These hybrid models aim to achieve better scalability, security, energy efficiency, and adaptability, making them increasingly relevant for modern blockchain applications. Hybrid approaches combine different consensus mechanisms: DP-Hybrid combines CPoW and PBFT, claiming up to 10× throughput increase versus traditional PBFT [20]; HyFlexChain reports 9-14.6 TPS under PoW and 112.5+ TPS under BFT protocols [21].

2.3 AI and Machine Learning Integration

Recent work explores integrating machine learning with consensus mechanisms for anomaly detection and security enhancement [22]. An AI-based approach for consensus uses convolutional neural networks for dynamic node selection,

though it faces challenges with data dependency and interpretability [23]. Studies suggest AI optimization may improve energy efficiency, throughput, and security in hybrid models [24], though practical implementation remains limited.

2.4 Reputation and Security-Based Approaches

Several studies propose reputation-based consensus mechanisms. Dynamic PBFT (DPBFT) uses credit-based node election, reporting lower CPU usage than traditional PBFT [25]. Reputation-DPoS incorporates token rewards to enhance voting mechanisms [26]. Proof of Intelligent Reputation (PoIR) employs BiLSTM and NERD for node selection [27].

2.5 Domain-Specific Case Studies

This section examines adaptive consensus implementations across different application domains.

SABEC: UAV Network Coordination

The SABEC protocol addresses challenges in drone swarm coordination including dynamic topology, intermittent communications, and resource constraints [5]. It employs Fuzzy C-Means Clustering for network partitioning with trust-based cluster formation, allowing nodes to participate in multiple logical clusters via membership vectors.

Simulation results show: PDR exceeds 90% with 35 malicious nodes compared to 20-30% degradation in traditional protocols; blockchain storage remains below 200 units versus over 1000 for traditional implementations at 1000 blocks; energy consumption ranges 100-150 units versus 400-500 for PoS/PBFT at 100 nodes [5].

6G Cognitive Radio Networks

Proposed 6G spectrum management systems utilize blockchain for decentralized resource allocation [28],[29],[30] [31]. Implementations combine hybrid consensus mechanisms with Deep Reinforcement Learning agents for spectrum optimization, storing reputation scores on-chain [32]. Blockchain oracles provide real-world sensing data for smart contract execution [33].

Studies report various improvements: STBC protocol showed 30% increased spectrum utilization with reduced transaction delays [37]; a CRAHNs security model reported 18.5% reduced communication delays, 19.5% increased throughput, 19.4% improved PDR, and 12.5% energy savings [38]; BSM-6G with Proof-of-History aims to process thousands of transactions per second for IoT deployments [33].Challenges include integrating with legacy infrastructure [33], balancing the scalability trilemma, and addressing regulatory uncertainty regarding tokenized spectrum rights.

Supply Chain Management

Adaptive consensus mechanisms have been proposed for supply chain transparency and resilience [34-35]. Designs include role-based validator selection (manufacturers, logistics providers, retailers) with varying finality requirements based on product value and regulatory needs. Implementation requires hybrid governance models [36]. Reported challenges include resistance from traditional partners [39], data privacy requirements across jurisdictions [40], complex ERP system integration [41], and stakeholder training needs.

2.6 Synthesis of case studies across various domains

This section synthesizes the key characteristics of the three case study domains examined in above sections, presenting their adaptive mechanisms, evaluation metrics, and maturity levels in a structured format to facilitate informed interpretation.

Table 2. Synthesis of Case Study Characteristics Across Domains

Attribute	Various Domains		
	SABEC (UAV) [5]	6G Cognitive Radio [37][38][33]	Supply Chain [34–36]
Adaptive Mechanism	Fuzzy C-Means + trust-based switching	DRL-based hybrid consensus	Role-based validator selection
Baseline	PoS / PBFT	Legacy spectrum allocation	Traditional ERP systems
Key Metric	PDR, energy, storage	Spectrum utilization, throughput, delay	Qualitative only
Key Result	PDR >90% vs. 20–30% (traditional); energy 100–150 vs. 400–500 units	30% spectrum gain; 18.5% delay reduction; 19.5% throughput gain	Improved transparency; no unified benchmark
Test Environment	Simulation, 100 nodes	Emulation	Conceptual/prototype

Table 2 summarizes findings across the three case study domains. Direct cross-paper comparability is limited due to heterogeneous test environments (simulation vs. emulation vs. conceptual), non-standardized metrics, and differing baselines across domains. These differences reflect the domain-specific nature of adaptive consensus research; standardized benchmarking frameworks remain an important direction for future work.

2.7 Research Gaps and Survey Contributions

Identified Gaps:

- Limited Integration: Most hybrid strategies combine only two consensus types
- Scalability Verification: Limited large-scale deployment validation of adaptive mechanisms
- Security-Performance Tradeoffs: Dynamic optimization approaches remain underexplored
- AI Integration: Frameworks for AI-enhanced consensus are still developing
- Cross-Domain Applicability: Solutions often remain domain-specific
- Interoperability: Cross-chain consensus coordination lacks standardization
- Production Deployment: Gap exists between research prototypes and production systems

Survey Contributions: This survey addresses these gaps through: (1) a taxonomy for classifying adaptive consensus mechanisms; (2) analysis of quantitative results from SABEC, 6G, and supply chain case studies; (3) a maturity framework for assessing production readiness; (4) examination of security considerations in adaptive systems; (5) analysis of conflicting claims in literature; (6) discussion of interoperability challenges; (7) coverage of developments through 2024 including Ethereum's PoS transition (2022) and emerging applications.

3. Main Content: Category of Adaptive Consensus Mechanisms in blockchain

Various adaptive consensus mechanisms have been developed due to the search of efficient and secure blockchain networks able to perform under different and evolving conditions and circumstances. All these mechanisms can be split into three main different preferences in how they go about achieving adaptability, including dynamically adjusting parameters, consensus algorithm switching, hybrid consensus, and the emerging topic of AI and machine learning based assisted consensus. Figure 2 provides the categories of adaptive consensus mechanisms in blockchain.

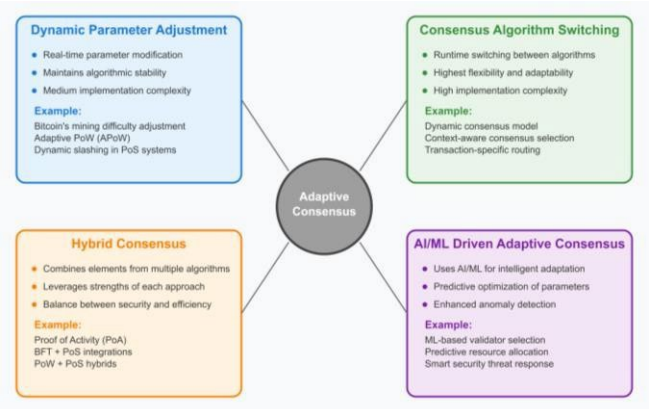

Figure 2. Types of adaptive consensus mechanisms in blockchain

3.1 Dynamic Parameter Adjustment Mechanisms

Dynamic parameter adjustment mechanisms provide a way to achieve a consensus algorithm's scalability. A dynamic parameter adjustment mechanism can also be used to introduce adaptability into blockchain consensus. Most parameter adjustment mechanisms modify operational parameters already in operation and a given network to adapt to changes in the network based on its demands. One such example that is comparatively established is modifying mining difficulty in Proof of Work (PoW) blockchain such as Bitcoin. The difficulty is periodically recalibrated based on the network's hashing power to ensure that blocks are generated at a relatively constant rate. Such a dynamic change assists in ensuring the stability and predictability of the blockchain, even in conditions of changing the number of miners or changes in their computational capabilities [42]. The decision flow diagram of adaptive parameter adjustment is the one depicted in Figure 3. Other related adaptive solutions are used in Proof of Stake (PoS) systems, whereby parameters like minimum stake to achieve the right to become the validator or the reward payout schemes are subject to adaptation to network performance/security or governance choices. As an example, to secure new Proof-of- Stake sidechains containing possibly low initial stake against attacks, a mechanism has been proposed known as merged-staking where stakeholders of the mainchain can pool together to help securing the new chain, essentially adding extra security coverage of a system at a potentially vulnerable point in time. Outside the above examples, adaptive difficulty adjustment protocols have also been studied to prevent cases of specific vulnerabilities such as selfish mining attacks in PoW blockchains [14]. These dynamic parameter changes will allow blockchain networks to safeguard their operating efficiency and security profiles without a paradigm shift in the underlying consensus algorithm by extending the continuous monitoring of network conditions and performance indicators [4].

3.2 Switching mechanisms of consensus algorithms

Another, more drastic vision of adaptive consensus is the ability of the network of blockchain to dynamically switch between two or more different consensus algorithms [43]. This strategy provides a high degree of flexibility by enabling the network to optimize for different priorities as conditions demand. As an example, a blockchain may use a consensus algorithm (such as Proof of Authority (PoA) that uses very little energy when the network is not busy to reduce the consumption of resources [44]. Nevertheless, what would happen in the event of a spike in transaction volume or a potential threat to the network's security is dynamic migration

to a more fault- tolerant and robust algorithm, such as Practical Byzantine Fault Tolerance (PBFT)[44]. An example of such an approach is the Dynamic Consensus model, offering the option of enterprise blockchain deployment, in which the transaction can be sent to the most suitable candidate algorithm depending on its individual needs and the context of the network at that particular time [45]. The use of such a mechanism demands an advanced system of governance and attention to the transition process between algorithms in order to support the stability of the network and the consistency of the data [46].FlexBFT[47] can continually operate round after round within the slow lane until the network conditions improve. ATBFT[48] proposed automatic switching between leaderlessBFT consensus and leaderBFT consensus, which in principle eliminates the transaction interruption time in the consensus process, ensures uninterrupted transactions, and improves the efficiency of block generation and tx execution.

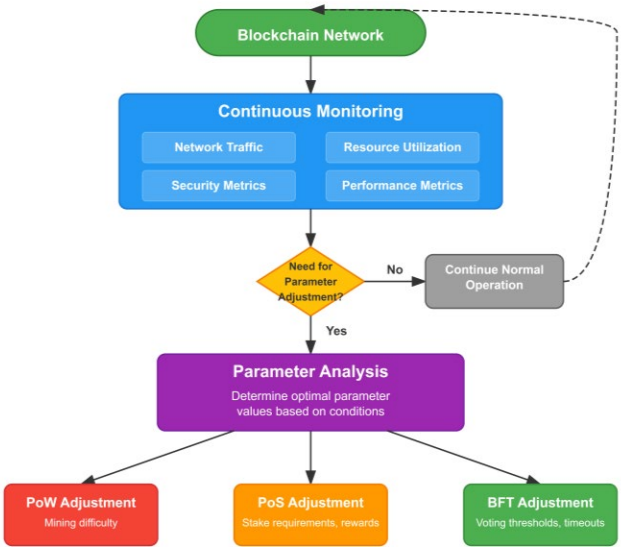

Figure 3. Decision Flow Diagram for Adaptive Parameter Adjustment

3.3 Hybrid Consensus Mechanisms

Hybrid consensus mechanisms are the other major covariates of adaptive protocols, which mix parts and functions of two or even more various underlying consensus algorithms [2]. The motivation of these hybrid methods is to use the advantages of each of the individual algorithms and overcome the disadvantages of one another, creating a more balanced consensus mechanism. A widely known example is Proof of Activity (PoA), in which consensus begins with a PoW-style leader election: miners hash a block header to compete to take charge and begin reaching a consensus. After the election of a leader, it shifts to a PoS-analogous validate interval, where a set of validators, selected on the basis of their stake, confirm they agree on the validity of the proposed block. This combination aims to harness the security of PoW's computational difficulty and the energy efficiency of PoS's stake-based validation. Other hybrid systems may use BFT algorithms along with PoS to increase the fault tolerance of stake-based systems or PoW combined with other Sybil-resistance mechanisms in permissionless networks [49]. The algorithm is a mashup of Proof of Stake, Delegated Proof of Stake, and threshold cryptography to achieve energy efficiency, security, as well as scalability [50]. Hybrid strategies offer a nuanced approach to adaptability, carefully combining the strengths of individual protocols into a coherent, balanced framework.

3.4 Adaptive Consensus Algorithm based on AI and ML

Optimisation of performance and security:

Artificial Intelligence (AI) and Machine Learning (ML) are the key features of adaptive consensus mechanisms in blockchain and can become a game-changer to enhance the performance and security of the processes [16][45]. AI/ML may enable smart selection of validators, dynamic consensus parameter selection based on predictive analytics and anomaly detection with the help of pattern recognition, and more efficient resource selection when participating in consensus [51]. A high standard of training and validation of models is needed in the implementation of such systems. The most common method that is used by neural networks to predict optimum parameters or identify malicious behavior is supervised learning, which relies on the historical data of a network [52]. Such training sets have to be extensive by incorporating performance statistics, transaction histories, attack vectors, and network structures to operate successfully in any conditions [53]. Such AI systems run the risk of overfitting, which remains one of the major concerns that is alleviated through the application of methods such as cross-validation processes, regularization, and ensemble approaches. The dynamic character of blockchain requires frequent modifications of the model and offline and controlled online experimentation of the model prior to its deployment. An adaptive approach is proposed in which a DRL agent on a peer moves blocks between the cloud and local storage depending on the organization's needs and the network state to ensure optimal blockchain performance [54]. Three tip selection algorithms based on the DAG consensus is developed in [55] to ensure efficient training while achieving concurrent control of DAG.

Vulnerabilities and Threat Vector Security

Consensus methods with AI create new sources of security threats. The adverse attack enables malicious groups to design a misleading input that controls the way AI models operate without directly hacking them, e.g., to change transaction patterns to normalize ill behavior [22]. Another threat is model poisoning, where an attacker introduces poison data into training data sets; mostly an issue in

decentralized systems with difficult control of data integrity. The use of the poisoned models can result in the introduction of biases or neglect of certain threats [56]. More violently, the Byzantine AI nodes-compromised intelligent members can coordinate advanced, multi-vector, time- changing attacks with internal knowledge of the consensus mechanics. Repeated subversion of this kind may lead to sophisticated and unpredictable disruptions when cooperating with other such nodes [57]. Mitigating these risks requires well-validated training data, robust anomaly detection, and architecturally resilient consensus designs.

Transparency and trust:

The black box or opaque nature of AI models poses critical issues for blockchain systems, whose pillars are transparency and the ability to audit. Network members should also be able to comprehend the reasoning behind a consensus outcome through rejection of transactions or the selection of validators [58]. Interpretability approaches, which explain the decisions of AI models without reducing their complexity, such as attention mechanisms, Local Interpretable Model-agnostic Extension (LIME), SHapley Additive exPlanations(SHAP), and hybrids of rule-based and accordance models, can illuminate the reasoning behind any AI decision [59]. In addition, decentralization and equality principles may also be hindered by algorithmic bias, wherein training data can lead to unfair treatment of users or transactions. The integration of blockchain consensus in a form that is trustworthy requires dealing with these concerns using safe, interpretable, and regulation- savvy AI systems. Table 3 is a comparative analysis of the adaptive consensus mechanism.

Table 3. Comparative Analysis of Adaptive Consensus Mechanisms

Consensus Mechanism	Different Parameters				
	Throughput (TPS)	Scalability	Energy Efficiency	Security Level	Implementation Complexit
Bitcoin Difficulty Adjustment	7	Low	Very Low	High	Low
Adaptive PoW [14]	10-15	Low-Medium	Low	High	Medium
Consensus Algorithm Switching [16]	100-1,000	High	Medium	Variable	Very High
HyFlexChain [21]	112.5+ (BFT mode)	High	High	High	Very High
Proof of Probability [64]	Variable	Unknown	Medium	Medium	Very High

3.5 Discussion and Analysis

Analysis of Performance-Security Trade-off Analysis

Comparative analysis the Table 3 makes it clear that there is an underlying dichotomy between performance and security among the existing consensus mechanisms. Conventional mechanisms, such as Bitcoin difficulty adjustment, represent secure mechanisms that lean towards security (secure rate) at the expense of scalability (7 TPS), whereas dynamic consensus switching-based mechanisms represent throughput maximised tradeoffs with instances of variable guarantees of security (100-1,000 TPS). This mutual exclusivity highlights one of the remaining problems of the blockchain trilemma: it is impossible to optimize scalability, security, and decentralization simultaneously [60]. The hybrid mechanisms show positive trends in the solution of this trade-off. HyFlexChain has a TPS of 112.5+ at high security in BFT mode, but with an extremely high complexity of implementation.

Implications of Energy Efficiency and Sustainability

Energy efficiency is pointed out in the analysis as an essential characteristic to distinguish different consent mechanisms. There is very low energy efficiency of traditional PoW-based systems; and new hybrid mechanisms have high efficiency with minimal negative implications on security. This shift coincides with increased sustainability demands in blockchain systems and implies that the energy- efficient consensus design will continue to gain prominence to achieve wide-spread use. Observably, adaptive PoW systems are energy inefficient, given the increased functionality, which implies that optimization of energy will issue basic algorithmic advancement instead of refinement of the present PoW design.

Complexity of implementation and Adoption barriers

The complexity of implementation turns out to be a major adoption barrier, especially to advanced mechanisms. Extremely high complexity-rated systems (Dynamic Consensus Switching, HyFlexChain, PoAI) are to a large extent still in the pure research or prototyping phase, which implies the innovation goes through theoretical innovations and deployment strategies. The disparity between innovation research and the actual practice supports the necessity to create standardized frameworks and development tools to minimize the complexity boundaries. The fact that complexity and restricted real-world deployment go hand- in-hand demonstrates that algorithmic complexity and feasibility regarding the implementation of the ideas in consensus mechanisms should be balanced.

3.6 Research gaps and Technology Maturity

The assessment indicates a great maturity difference among the consensus groups. Although conventional mechanics find advantageous use all over, sophisticated hybrid and AI- based solutions are still at the research phase. Although consensus mechanisms based on AI have a theoretical potential, they yield varying performance metrics and unknown scalability properties, which means that there is enough room to conduct research in this field. The academic character of prototypes and implementations of research indicate that it must undergo specific dedication toward creation of a mechanism using research into production-ready systems via rigorous verification and validation procedures.

Peculiarities Optimization

The application-specific consensus optimization is needed because of the different use case requirements. This trend of specialization indicates that in future development of consensus mechanism, it might be good to focus on targeted solutions built to optimize in specific deployment scenarios, instead of striving to find general solutions.
Our qualitative assessment of the surveyed mechanisms suggests an inverse relationship between implementation complexity and real-world deployment. Among the 68 mechanisms reviewed, those characterized as 'very high complexity' in Table 3 (HyFlexChain, Consensus Switching, PoAI) remain primarily at the conceptual or prototype stage, while simpler mechanisms like Bitcoin's difficulty adjustment have achieved large-scale production deployment. This pattern indicates that future research should balance theoretical sophistication with practical deployability considerations.

Research Future Directions

It is based on this comparative analysis that we will find three research priorities that include (1) devising quantifiable metrics of security to be used in place of the subjective measure, (2) the production of standardized test models that seek to evaluate comprehensively the mechanisms put to test and (3) the development of hybrid systems that can continually optimize the security-performance-efficiency trade-off based on network states and requirements of applications. Also, the paradigm shift of AI-driven consensus mechanisms under simulation environments into practical implementations is another opportunity that would contribute to the further development of the field.

4. Technical Challenges and Limitations of Adaptive Consensus Protocols

Although the benefits of adaptive consensus mechanisms on blockchain are considerable, they are surrounded by a number of technical issues and inherent constraints that should not be overlooked since they accompany implementation and deployment of the technology.

4.1 Added Complexity and Implementation Cost:

The simple fact of adaptability presents a large amount of additional complexity to design, implementation, and maintenance of such a consensus protocol [49]. In contrast to the static algorithms that preset the rules to be followed, adaptive mechanisms involve the use of sophisticated algorithms to track the situation in the network, measure the performance to create wise decisions regarding the manner and time to adjust [49]. Such intricacy may equate to greater expenses of development, more probability of software defects, and a higher level of specialist skill needed to operate and troubleshoot these systems [49]. Moreover, certain adaptive mechanisms (especially those based on runtime switches between consensus algorithms or the use of AI/ML) can have a high computational and communication overhead, which is dependent on not only the adaptation mechanism itself but also ongoing network parameter monitoring. These overheads may adversely affect the overall performance and efficiency of the blockchain network especially during heavy transaction loads.

4.2 Security Vulnerabilities and Attack Vectors

Adaptive consensus protocols allow configuration to respond to new threats and are thus in their most natural form, dynamic as well as reconfigurable protocols, which is a potential source of security vulnerabilities and attack vectors unless carefully designed and thoroughly tested. This is to say that in case the mechanisms that drive adaptations or the parameters that govern the adaptations can be manipulated by malicious actors, it may result in the compromise of the consensus process or the awarding of undue benefit to the attackers [61]. A very challenging issue is to guarantee the security and trustworthiness of the adaptation logic itself. Adaptation decisions are made by the algorithms, which have to be resistant to adversarial input and cannot inject unknown weaknesses or biases into the system. Further, the algorithm switching mechanism in certain adaptive models has to be well choreographed so that the transition mechanism does not cause disruption or potential attack during the switching period.

4.3 Limitations of Scalability

Basically, the scalability problem emerges as the number of nodes and transactions rise in blockchain [62], whereas some adaptive consensus mechanism is specifically tailored towards overcoming the alleged problems of blockchain technology scalability, others may still be constrained in their ability to support numerous nodes or respond to a large number of transactions per second.Specifically, the overhead of periodically checking network activities and making corresponding changes may be considered a stumbling block once a large number of nodes are involved. When switching

a consensus algorithm, integrating all nodes in a large network to switch to the new algorithm without suffering forks or discrepancies may be a serious obstacle [46]. Adaptive consensus using AI/ML, though projected to work in intelligent resource allocation, may not be scalable in demanding AI models and computational resources needed to run them in real time. Thus, critical considerations should be devoted to the scalability effects of every single adaptive strategy.

4.4 Network Instability and Fault Tolerance

Instability of network and fault tolerance In practice, blockchain networks frequently have to operate in environments where network conditions are unstable (varying network latency), communication delays, and bad or malicious nodes may exist [4]. Such conditions have to be designed with adaptive consensus protocols to preserve their efficiencies and reliability. As an example, mechanisms that assume that much communication between nodes is necessary to induce adaptations may be disadvantaged by delay or occasional disconnection in the network [4]. On the same note, adaptation logic must be tolerant to faults by Byzantine nodes that could give misleading information to control the decision regarding the adaptation. It is a serious technical challenge to ensure that adaptive consensus protocols have the ability to achieve a high level of fault tolerance and further still operate properly even when encountering network unstable and malicious entities.

4.5 Challenges of Parameter Tuning and Optimisation

Obtaining optimal performance in adaptive consensus mechanisms is frequently dependent upon meticulous tuning and optimisation of numerous parameters, thresholds, and guidelines that specify the adaptation process. Finding optimal settings to these configurations may not be a trivial task as such settings may highly depend on the blockchain network in which it is applied, the use cases, and the current network conditions. Poorly configured adaptation parameters may result in performance degradation. Consequently, it is crucial to have strong monitoring, measuring, and optimizing systems so that the modifications themselves are really useful and will not unintentionally worsen performance and/or security of the network. This can be a complex task that needs a lot of simulation, testing, and practical experimentation to determine the best techniques of adaptation and parameter values.

4.6 Analysis and Maturity Assessment of Real-World Deployment

Deployment Maturity Model

Real-world deployment of adaptive consensus mechanisms reveals significant variation in maturity levels across different approaches. After extensive study of current deployments, we put forward a four-level maturity model discussed in Figure 4. that defines adaptive consensus mechanisms by the state of their real-world deployment and properties of operation. **Level 1 -** Conceptual and Simulation-Based Mechanisms is the least mature state of development, as conceptual deployments of innovative designs of consensus, e.g., Proof of AI (PoAI), and other AI/ML-amplified consensus designs, currently only exist within purely theoretical systems and in controlled model-system experiments. An instance of this category is the AICHAIN project, which has shown promising results in simulated environments but is yet to go through the rigorous validation needed in deployment to production. Such mechanisms impose a fundamental gap between being a theoretical construct and an implementation, because they tend to be based on assumptions that do not apply to distributed systems with network latency, Byzantine failures, and variably capable nodes.

Level 2 - Prototype and Testnet Implementations include mechanisms that have advanced beyond pure simulation to some experimental realization. Examples include HyFlexChain and Dynamic Consensus Switching protocols, with some (academic institutions and research organizations) having built a working prototype that could run a small-scale testnet. Such deployments are usually limited to a small number of nodes and have generally not been stress tested to determine how they respond in the adverse situations (such as a network partition, a coordinated attack, or high traffic loads) where their actions may be quite important.

Level 3 - Limited Production Deployment involves adaptive mechanisms that have so far been deployed in practical blockchain networks, but at limited levels of scope, or with particular applications implied. Different versions of Adaptive Proof of Work and hybrid Proof of Stake systems would fall into this banner, and so far medium and smaller scale cryptocurrency networks have managed to port those capabilities into their functional networks. Although these implementations are proving to be practically feasible, they remain subject to a substantial degree of limitation regarding performance loss during high-computational activities and possible security breaches that also arise only when placed under prolonged and strenuous work conditions.

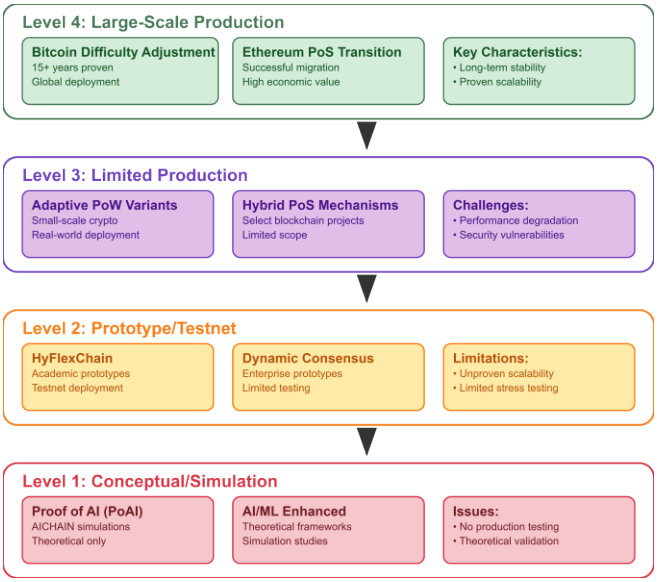

Figure 4. Adaptive Consensus Maturity Progression Framework

Level 4 - Large-scale Production Systems is the most advanced maturity level, where mechanisms become widely used and stable in a high-stakes arena. This is the kind of algorithm that is used in Bitcoin with difficulty, which has worked on a network of thousands of nodes spanning the world since a period of more than fifteen years. In the same manner, the recent and successful shift of the Ethereum network, on the one hand, to Proof of Stake, with all its complications and economic risk attached to it, showed that adaptive consensus mechanisms can be functional within the realm of scaling when they are backed by significant planning, ordinary testing, and social agreement.

Analysis of the Case Studies

Exploring real-world deployments will give important information on real-world problems and success factors of the adaptive consensus mechanism. By analyzing in detail three major implementations, we deduce the major patterns and lessons that become the guidance toward future deployment.

a) Proof of Stake transformation in Ethereum

It is one of the most ambitious and successful adaptive consensus implementations ever in blockchain [63]. This process, which has been going on since the initial Beacon Chain deployment in December 2020 to full Merge in September 2022, has involved the coordination of changes to a network handling hundreds of billions of dollars' worth of value. Its implementation had some critical difficulties, such as validator slashing episodes in the early part of the Beacon Chain that emphasized the significance of high exactness of the parameters in the economic security procedures. The synchronization of networks in the Merge event showed how hard it was to coordinate distributed network state transitions, and failures to achieve finality when the network was excessively busy indicated the trade- off between the efficiency of a consensus and the resilience of a network. This process of transition was successful due to the slow implementation process, which allowed continual improvement and error reduction, thorough testing in many testnets, which in turn confirmed the mechanism's operation across a variety of cases, and the development of a broad consensus with the community, which forms the social anchoring needed to ground such a major shift.

b) Pluggable Consensus Architecture is a Hyperledger Fabric feature

This provides knowledge in how adaptive consensus mechanisms may be used in a business setting. Such implementation allows organizations to choose and instantiate various consensus algorithms depending on their needs, everything from basic majority votes in trusted settings to more complex, to Byzantine fault-tolerant versions in adversarial settings. Nevertheless, the deployment has demonstrated that there are major operational issues, such as configuration complexity in terms of requiring advanced technical knowledge to implement various consensus algorithms correctly, performance variability across different algorithms which makes it hard to conduct proper capacity planning and system tuning, limited documentation concerning hybrid implementations which has so far made it hard to integrate in enterprise developer circles. The experience highlights the immense value attached to standardized interfaces, which not only facilitate the switching of algorithms with no hindrance but also provide thorough benchmarking of performance in every configuration supported, alongside the ability to develop extensive training programs to the operators so that successful rolling and maintenance of the unit becomes a reality.

c) The Nominated Proof of Stake Implementation in Polkadot:

It is the evidence of problems related to dynamic selection of validators and flexible economic incentives. Its solution of constantly perfecting validator sets via nomination mechanisms has brought a significant success in sustaining the decentralization factor in the network and providing security to the network. Nonetheless, operational pressures have arisen, such as validator set rotation events that create short-term network instability as new validators are added and dropped, nomination pool management complexity with a need to otherwise complex tooling and monitoring, and the continuing challenges in balancing slashing parameters to enforce security without losing too many validators. Lessons learned during the implementation of Polkadot risk to focus on the importance of measured parameter adjustment strategies to avoid abrupt network disturbances, open governance processes to generate trust among stakeholders and allowing the general involvement in network consensus parameter decision-making, and automated tooling to eliminate complexity in operations and optimise the chances of failure in the network management process through human error.

Analysis of Production Deployment Barriers There are significant technical, economic, and social obstacles to the conversion of the research prototypes of adaptive consensus mechanisms into products ready to be used in the production process. Knowledge of such barriers would help in creating effective implementation plans and appropriate adoption schedules.

a) Technical obstacles

It introduces some of the most urgent issues that organizations implementing adaptive consensus mechanisms would have to face. Integration with legacy systems is an especially thorny issue, because established blockchain infrastructures tend to be built on assumptions of deterministic consensus that dominate many layers of the system, all the way down to network protocols and up to application-layer APIs. Performance overheads due to adaptive mechanisms that are measured in laboratories often are more than those obtained in production environments due to the need to contend with the variable nature of network latency, mismatched hardware capabilities, and concurrent system resource demands difficult to simulate in a test bed environment. Moreover, the security audit specifications of new consensus mechanisms make this an expensive challenge with regard to development and validation because the conventional security analysis frameworks might not be sufficient in the evaluation of adaptive systems that portray flexible behavior patterns.

b) Barriers to capital Discussion

Economic barriers impose significant friction on adoption, particularly when costs and benefits of migration are difficult to quantify in advance.

It imposes a massive friction of adoption, especially in areas where costs and benefits of migration are challenging to measure. The cost of migrating to or directly to current consensus systems is not only measured by the direct cost of technical implementation, but also opportunity costs on system downtime, retraining human assets, and possible service interruptions in the process between transitions. The question mark of the investment returns on experimental consensus mechanisms can be a major threat to organizations, since adaptiveness benefits can manifest themselves in the environment of certain necessary operations under certain conditions that are hard to predict or assure. Also, the absence of a cover or risk management tools to cover the innovative methods of consensus introduces another level of financial risk, which conservative firms struggle to explain to shareholders and regulators.

c) Barriers to social movement

Social barriers often prove to be the most persistent obstacles to adoption. The resistance to complex adaptive mechanisms by developer communities is based on issues of additional system complexity and difficulty of debugging, and the steep learning curve involved when working with these complex systems. The regulatory ambiguity of innovative models of consensus makes enterprises and financial institutions that work in highly regulated sectors hesitant to adopt adaptive consensus mechanisms because the legal impact of such a change can be ambiguous or liable to change according to regulatory changes. The fact that putting networks with dynamic consent rules to use may be hard regarding conveying the utility of dynamism to final users indicates that the dynamic behaviour of consensus may not be very welcome by the end users who are likely to interpret it as instability or lack of commitment to agreed-upon rules. Such obstacles are not insurmountable but have to be taken into consideration and addressed through specific mitigation methods. The critical factor in the successful implementation of adaptive consensus mechanisms is technical prowess alone; long-term planning, whereby issues of economic incentives, social acceptance, and regulatory compliance are considered, should also be factored. The history of the successful deployments indicates that the deployment strategies should rely on suggestions of incremental implementation, broad stakeholder involvement, and effective risk mitigation plans.

4.7 Problems with Standardization and Interoperability

Current Standardization Landscape

The adaptive consensus ecosystem is working with diverging standards at the moment, which produces massive obstacles to popularization and interchange with other systems. A lack of standardised application programming interfaces (APIs) to switch algorithms in consensus is a key obstacle; the various existing implementations use inconsistent parameter names, and do not share performance measurements or evaluation packages. A similar fragmentation is observed in the realm of protocol compatibility, where different block formats in the different adaptive mechanisms, incompatible forms of transaction validation, and dissimilar cryptographic signature systems cannot be used interoperably.

The aspect of governance poses equally critical issues as there are no consensus transition model standards, consistent voting systems governing parameters adjustment and there are no consistent dispute resolution protocols. Such standardization holes result in a situation in which every instance of consensus adaptation exists as a silo, with less ability to interact at the ecosystem level and a reduced capacity to develop strong, interoperable blockchain networks.

Interoperability Shortcomings and Obstacles to Technical Barrier

Technical constraints of existing systems are most apparent in the cross-chain communication protocols, which are not able to effectively deal with dynamic consensus changes in operation. Bridge contracts often go wrong when consensus variants are changed during transaction and syncing of states across chains with disparate consensus models. Polkadot- Ethereum bridge is a prime example of

these difficulties, with the Ethereum Proof-of-Stake finality mechanism conflicting with the Polkadot Nominated Proof-of-Stake system to create timing irregularities and necessitate various block confirmation prerequisites increasing transaction time and necessitating the frequent upgrading of bridge contracts.[64]
An additional level of complexity is semantic interoperability, where different consensus mechanisms have varying definitions of core concepts such as finality, have inconsistent guarantees of security across adaptive systems, and use different assumptions about transaction order. The result is a splintered environment in which systems are incapable of communicating and coordinating reliably and only have a limited potential to develop unified blockchain ecosystems that internalize the advantages of diverse consensus mechanics.

What are the Challenges of Cross-Chain Transactions and Network Resolution?

Effective adaptive consensus requires the technical enabling conditions to do so revolve around the need to have a standardized Consensus Abstraction Layer (CAL), which can unify the definition of consensus interfaces, include shared messaging protocols to allow cross-chain consensus communication, and unified security model representations. Implementation The work of cross-chain transactions particularly encounters problems concerning the assurance of atomicity between various consensus mechanisms, the treatment of failure conditions during cross-chain operations, and the reconciliation of various block time assumptions, which may lead to issues of synchronization. Another area that is vital in terms of standardization deficiency and poses a risk to operational processes is network partition. The degree at which different consensus mechanisms react to network partitions varies; there are no shared, agreed-upon network partition detection and recovery mechanisms, varying assumptions of Byzantine faults, which may require reliable mechanisms to adapt to partitions, potentially resulting in perceived failures or unsafe conditions of the networks. Such difficulties point out to the necessity of elaborate standards which not only cover normal operation cases but also edge cases and failure situations.

Standardization efforts and directions

Existing work on standardization, such as that of ISO/TC 307 Blockchain and Distributed Ledger Technologies, the W3C Blockchain Community Group, and the Enterprise Ethereum Alliance, has contributed to some progress on overall blockchain standards but has thus far failed to provide sufficient definition on the problems posed by adaptive consensus systems in particular. Key gaps still exist with regard to the absence of a consensus-specific standardization organization, the absence of fully developed adaptive consensus testing environments, and the lack of interoperability certification procedures that might achieve compatibility at the implementation level.
To deal with the challenges, an Adaptive Consensus Standards Consortium that will focus on advancing consortium-specific consensus standards, the development of complete common testing and benchmarking schemes that can assess adaptive consensus functionality along its many dimensions, and certification schemes of interoperable implementations is needed. These efforts would form the basis of a more interoperable adaptive multi-consensus ecosystem in that they would allow the creation of genuinely interoperable blockchain networks that can dynamically composable their consensus mechanism and yet allow them to have seamless cross-chain communication and operation.

5. Future Enhancements and Future Research Directions

The research on adaptive consensus in the area of blockchain technology is dynamic and still progresses rapidly. There are multiple promising areas of future improvements and the most important directions in research that will potentially be the foundation of the new generation of decentralized agreement systems.

5.1 Enhanced More Intelligent and Autonomous Adaptation Strategies

Future studies will probably be aimed at developing more intelligent and autonomous adaptation strategies that would be able to learn and adapt consensus protocols and parameters autonomously on the basis of real time network analytics and predictive modelling [51]. This is done by utilizing the recent developments in Artificial Intelligence (AI) and Machine Learning (ML) to allow blockchain networks to reactively make their consensus mechanisms optimally without the need to have human-assisted manual intervention or set specific guidelines on all foreseeable scenarios [16]. As an example, network-traffic patterns, security threat intelligence, and resource-utilization metrics could be used to dynamically adjust consensus parameters, predict possible bottlenecks, or even smoothly switch between consensus algorithms as the need evolves, using probabilistic network models [65]. The shift into more self-governing and smart adaptation holds great future potential in making blockchain networks more receptive and efficient in changing environments.

5.2 Improving the Security and Trustworthiness of Adaptive Mechanisms:

Security and trustworthiness of the very components of the adaptation will be one of the primary research topics going forward. This involves exploring new cryptography tools that can be used to secure the logic of adaptation against malicious subversion and using formal verification techniques to thoroughly analyze the security of the features of adaptive protocols, and coming up with high-quality

monitoring tools that would identify possible vulnerabilities posed by the flexibility of these protocols and solve them as so. Also, the study of reputation systems and incentive provision might emerge as a method of contributing to the integrity of the adaptation process and making sure that malicious parties will not be able to abuse its course to their advantage.

5.3 Emphasis on Energy Efficiency and Sustainable Consensus

As environmental concerns continue to grow regarding blockchain technology, subsequent research regarding adaptive consensus is expected to considerably emphasize the means of achieving lower energy consumption [2]. It encompasses the investigation of adaptive hybrid protocols that change to more energy-directed protocols, such as Proof of Stake (PoS), as the blockchain is idle or balance resource distribution across protocols relative to the available and required energy levels [66]. Developments of new energy-efficient consensus mechanisms that are intrinsically more energy-efficient and the possible integration of such mechanisms into adaptive frameworks will be essential in the future development of more sustainable blockchain ecosystems as well.

5.4 Resolving the Interoperability and Cross-Chain Consensus Issues

Due to the large number of specialist networks being developed in the blockchain space, future work and academic attention to adaptive consensus may help to answer the question of how different chains should interact in a more interoperable fashion [67]. This entails conducting research in the direction of elaborating an adaptive mechanism of consensus, which could enable smooth and safe transactions and sharing information across the chains and potentially adjusting parameters to align with those of other chains involved in a transaction [68]. In order to truly achieve the vision of a completely connected internet of blockchains, adaptive protocols must be developed and enabled to be able to cross the barriers of the blockchain's consensus mechanisms across some of the existing blockchain domains.

5.5 Synergetic Integration with Developing Technologies:

The combination of adaptive consensus and other upcoming technologies, such as the Internet of Things (IoT), Artificial Intelligence (AI), and edge computing, has huge potential to generate future generation decentralized systems [69] depicted in Figure 5.

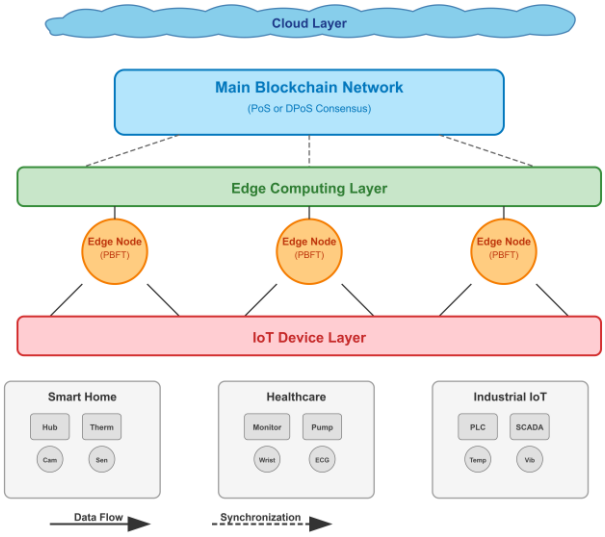

Figure 5. Hybrid Blockchain-IoT architecture with edge computing

Future studies would tend to delve into ways on making adaptive consensus adaptable to the reality and constraints of IoT, including the lack of computational capacity and intermittent connection [66]. The other synergy point is the application of AI and ML to the consensus itself as has been mentioned above [70]. Moreover, adaptive consensus coupled with edge computing may allow more distributed applications to be more efficient and responsive since the data will be processed and a consensus can be reached closer to the data source [71].

6. Conclusion

The core of trust and security in blockchain technology depends on consensus mechanisms, and the growing need to become versatile and efficient has kicked off the development towards adaptivity. This survey has outlined the terrain of adaptive consensus in blockchain, and has outlined its importance in surmounting the innate constraints of underlying conventionally static protocols in attempts to, in the context of modern decentralized networks, and their application, meet the innate heterogeneity and dynamism of user needs. We have considered the broad classes of adaptive consensus: dynamic adjustment of parameters, switching of the consensus algorithm, hybrid schemes, and the most prospective adoption of artificial intelligence and machine learning. All these solutions provide their solutions to increase the flexibility and responsiveness of blockchain consensus and allow networks to maximize their performance, security, and resource use on a time-by-time basis.

Although the advantages of the adaptive consensus protocols are large, the deployment and implementation of the protocols

are not devoid of substantial technical difficulties. A higher level of system complexity and the possibility of some security vulnerabilities of these mechanisms as a consequence of using the dynamic mechanism, restrictions on the scalability of particular methods, as well as the existing challenges and complications to tuning and optimizing parameters within can be considered the obstacles that should be properly overcome with the help of rigorous research and development. A limitation of this study is that full dual independent screening was not performed due to resource constraints, though supervisory validation was maintained throughout the screening process to ensure consistency and minimize selection bias.

Moving forward in time, the adaptive consensus field is specially balanced with opportunities of innovation and development. Future studies may emphasize on coming up with more optimized and self-governing adaptive goals, improved security and reliability of such dynamic behaviors, putting energy efficiency and sustainability first, managing the issue of interoperability and multichain consensus, and studying the synergistic design that adapts towards other new technologies. These innovations will be paramount in the development of blockchain infrastructure that will help the technology to achieve its maximum potential in a broad sector of applications. We have covered only a few of the adaptive consensus mechanisms proposed in the past few years, and indeed, many of these systems are still in early development. There is no doubt that this is where some of the key innovations in blockchain technology will occur in the coming years.

Declarations

During the preparation of this work, the authors used Claude and Gemini in order to improve language. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Acknowledgements

The authors declare that, there is no financial support from any of the institutions or personal relationship to affect the quality of the paper.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Shukla, A., Jirli, P., Mishra, A., & Singh, A. K. (2024). An overview of blockchain research and future agenda: Insights from structural topic modeling. Journal of Innovation & Knowledge, 9(4), 100605. https://doi.org/10.1016/j.jik.2024.100605

[2] Pineda, M., Jabba, D., Nieto-Bernal, W., & Pérez, A. (2024). Sustainable Consensus Algorithms Applied to Blockchain: A Systematic Literature Review. Sustainability, 16(23), 10552.https://doi.org/10.3390/su162310552

[3] Shen, Z., Qu, Q., & Chen, X. B. (2025). Blockchain Consensus Mechanisms: A Comprehensive Review and Performance Analysis Framework. In Electronics (Switzerland) (Vol. 14, Issue 17). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics14173567

[4] Zhuravel, S., Shpur, O., &Klymash, M. (2024). Adaptive Consensus Algorithms: Designing for Durability against Unstable Network Connections. International Journal of Computing, 23(4), 574-582.

[5] Dogan, H., & Setzer, A. (2025). SABEC: Secure and Adaptive Blockchain-Enabled Coordination Protocol for Unmanned Aerial Vehicles (UAVs) Network.

[6] Natraj, N. A., Midhunchakkaravarthy, J. J., & Mishra, B. K. (2024). A Quantitative Framework for the Selection of Hybrid Consensus Mechanisms in Blockchain-IoT Systems. EAI Endorsed Transactions on Internet of Things, 11.

[7] Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis Campbell Systematic Reviews, 18, e1230. https://doi.org/10.1002/cl2.1230

[8] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[9] Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., &Zanolini, L. (2020). A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS. Mathematics, 8(10), 1782.

[10] Adu-Manu, K. S., & Adjetey, C. (2025). PoAD: A Scalable and Energy-Efficient Consensus Algorithm for Smart Contract Execution in Decentralized Systems. Concurrency and Computation: Practice and Experience, 37(18–20). https://doi.org/10.1002/cpe.70197

[11] Ramos-Cruz, B., Andreu-Perez, J., Quesada-Real, F. J., & Martínez, L. (2025). Fuzzychain: An equitable consensus mechanism for blockchain networks. Journal of Network and Computer Applications, 241. https://doi.org/10.1016/j.jnca.2025.104204

[12] Saad, S. M. S., &Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). International Journal of Innovative Computing, 10(2). https://doi.org/10.11113/ijic.v10n2.272

[13] Yakubu, M. M., Hassan, F. B., Danyaro, K. U., Junejo, Z., Siraj, M., Yahaya, S., & Abdulsalam, K.(2024). A Systematic Literature Review on Blockchain Consensus Mechanisms' Security: Applications and Open Challenges. Computer Systems Science & Engineering, 48(6).

[14] Wuthier, S., & Chang, S. Y. (2021, July). Proof-of-work network simulator for blockchain and cryptocurrency research. In 2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS) (pp. 1098- 1101). IEEE.

[15] Ren, S., Lee, C., Kim, E., & Helal, S. (2022). Flexico: An efficient dual-mode consensus protocol for blockchain networks. PLOS ONE, 17. https://doi.org/10.1371/journal.pone.0277092

[16] Butean, A., Pournaras, E., Tara, A., Turesson, H., &Ivkushkin, K. (2020). Dynamic consensus: Increasing blockchain adaptability to enterprise applications. In Applied Informatics and Cybernetics in Intelligent Systems: Proceedings of the 9th Computer Science On- line Conference 2020, Volume 3 9 (pp. 433-442). Springer International Publishing.

[17] Hussein, Z., Salama, M., & El-Rahman, S. (2023). Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. Cybersecurity, 6, 1-22. https://doi.org/10.1186/s42400-023-00163-y.

[18] Wu, Y., Song, P., & Wang, F. (2020). Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on

POS and PBFT and Its Application in Blockchain. Mathematical Problems in Engineering. https://doi.org/10.1155/2020/7270624.
[19] Wei, Y., Xu, Q., & Peng, H. (2024). An enhanced consensus algorithm for blockchain. Scientific reports, 14(1), 17701. https://doi.org/10.1038/s41598-024-68120-4.
[20] Wen, F., Yang, L., Cai, W., & Zhou, P. (2020). DP-Hybrid: a two-layer consensus protocol for high scalability in permissioned blockchain. 2 (pp. 57-71). Springer Singapore. https://doi.org/10.1007/978-981-15- 9213-3_5
[21] Ferreira, H. J. P. C. (2024). Hyflexchain: A Permissionless Decentralized Ledger with Hybrid and Flexible Consensus Plane (Master's thesis, Universidade NOVA de Lisboa (Portugal)).
[22] Venkatesan, K., &Rahayu, S. B. (2024). Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. Scientific Reports, 14(1), 1149 https://doi.org/10.1038/s41598-024-51578-7
[23] Saadat, K., Wang, N., & Tafazolli, R. (2023). AI- Enabled Blockchain Consensus Node Selection in Cluster-Based Vehicular Networks. IEEE Networking Letters, 5, 115-119. https://doi.org/10.1109/lnet.2023.3238964.
[24] Nishad, D., Verma, V., Rajput, P., Gupta, S., Dwivedi, A., & Shah, D. (2025). Adaptive AI-enhanced computation offloading with machine learning for QoE optimization and energy-efficient mobile edge systems. Scientific Reports, 15. https://doi.org/10.1038/s41598- 025-00409-4.
[25] Cai, W., Jiang, W., Xie, K., Zhu, Y., Liu, Y., & Shen, T. (2020). Dynamic reputation–based consensus mechanism: Real-time transactions for energy blockchain. International Journal of Distributed Sensor Networks, 16(3). https://doi.org/10.1177/1550147720907335
[26] Hu, Q., Yan, B., Han, Y., & Yu, J. (2021). An Improved Delegated Proof of Stake Consensus Algorithm. Procedia Computer Science, 187, 341–346. https://doi.org/10.1016/j.procs.2021.04.109
[27] HussainiWindiatmaja, J., Hanggoro, D., Salman, M., & Sari, R. F. (2023). PoIR: A Node Selection Mechanism in Reputation-Based Blockchain Consensus Using Bidirectional LSTM Regression Model. Computers, Materials & Continua, 77(2). 10.32604/cmc.2023.041152
[28] Al-Matari, N. Y., Zahary, A. T., & A Al-Shargabi, A. (2024). A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks. Scientific reports, 14(1), 30990. https://doi.org/10.1038/s41598-024-82126-y
[29] Maksymyuk, T., Gazda, J., Volosin, M., Bugar, G., Horvath, D., Klymash, M., & Dohler, M. (2020). Blockchain-empowered framework for decentralized network management in 6G. IEEE Communications Magazine, 58(9), 86-92.
[30] Zambianco, M., & Verticale, G. (2020, August). Spectrum allocation for network slices with inter- numerology interference using deep reinforcement learning. In 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications (pp. 1-7). IEEE.
[31] Qamar, F., Siddiqui, M. U. A., Hindia, M. N., Hassan, R., & Nguyen, Q. N. (2020). Issues, challenges, and research trends in spectrum management: A comprehensive overview and new vision for designing 6G networks. Electronics, 9(9), 1416.
[32] Pathak, V., Sharma, A., Rathore, M. S., & Pandya, R. J. (2024, June). Reputation-based Resource Allocation Prioritization in 6G: A Coalitional Game Theoretic Approach. In 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
[33] Cuellar, D., Sallal, M., & Williams, C. (2024). BSM-6G: Blockchain-based dynamic Spectrum management for 6G networks: addressing interoperability and scalability. IEEE Access
[34] Vu, N., Ghadge, A., &Bourlakis, M. (2021). Blockchain adoption in food supply chains: a review and implementation framework. Production Planning & Control, 34(6), 506–523.https://doi.org/10.1080/09537287.2021.1939902
[35] Singh, R. K., Mishra, R., Gupta, S., & Mukherjee, A. A. (2023). Blockchain applications for secured and resilient supply chains: A systematic literature review and future research agenda. Computers & Industrial Engineering, 175, 108854. https://doi.org/10.1016/j.cie.2022.108854
[36] Franco, C. W., Benitez, G. B., de Sousa, P. R., Neto, F. J. K., & Frank, A. G. (2024). Managing resources for digital transformation in supply chain integration: The role of hybrid governance structures. International Journal of Production Economics, 278, 109428.
[37] Xue, L., Yang, W., Chen, W., & Huang, L. (2022). STBC: a Novel Blockchain-based spectrum trading solution. IEEE Transactions on Cognitive Communications and Networks, 8, 13–30
[38] Dansana, D. et al. (2024). BSMACRN: design of an efficient blockchain-based security model for improving attack-resilience of Cognitive Radio Ad-hoc networks. IEEE Access, 12, 10047–10058.
[39] Ghode, D. J., Jain, R., & Soni, G. (2020, December). Challenges of adoption of blockchain technology in supply chain: an overview. In International Conference on Evolution in Manufacturing (pp. 157-165). Singapore: Springer Nature Singapore.
[40] Svantesson, D. (2020). Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines. OECD Digital Economy Papers, (301).
[41] Imane, L., Noureddine, M., Driss, S., & Hanane, L. Y. (2023). Towards blockchain-integrated enterprise resource planning: A pre-implementation guide. Computers, 13(1), 11.
[42] Xie, M., Liu, J., Chen, S., & Lin, M. (2023). A survey on blockchain consensus mechanism: research overview, current advances and future directions. International Journal of Intelligent Computing and Cybernetics, 16(2), 314-340.
[43] Xiong, H., Chen, M., Wu, C., Zhao, Y., & Yi, W. (2022). Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms. Future Internet, 14(2), 47.
[44] Li, R. (2024, October). Comparative Analysis and Future Directions of Consensus Algorithms in Blockchain Technology. In 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024) (pp. 333-344). Atlantis Press
[45] Wu, J., Dong, M., Ota, K., Li, J., & Yang, W. (2020). Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT. IEEE Network, 34, 69-75. https://doi.org/10.1109/mnet.001.1900179
[46] Wu, C., Mehta, B., Amiri, M. J., Marcus, R., & Loo, B. T. (2022). AdaChain: A learned adaptive blockchain. arXiv preprint arXiv:2211.01580.
[47] Song, A., & Zhou, C. (2024). FlexBFT: A Flexible and Effective Optimistic Asynchronous BFT Protocol. Applied Sciences (Switzerland), 14(4). https://doi.org/10.3390/app14041461
[48] Lu, Y., Liu, C., Kong, L., & Niu, X. (2025). ATBFT-

automatically switch consensus protocol. Blockchain: Research and Applications, 6(1). https://doi.org/10.1016/j.bcra.2024.100255

[49] Nijsse, J., & Litchfield, A. (2020). A taxonomy of blockchain consensus methods. Cryptography, 4(4), 32.

[50] Yusof, S. H., Zahilah, R., & Othman, S. H. (2024). Blockchain consensus for resources constraint devices: a hybrid approach using PoA, DPoS and threshold cryptography Journal of Engineering and Technology (JET), 15(2).

[51] Bhumichai, D., Smiliotopoulos, C., Benton, R., Kambourakis, G., &Damopoulos, D. (2024). The convergence of artificial intelligence and blockchain: The state of play and the road ahead. Information, 15(5), 268.

[52] Antunes, M., Oliveira, L., Seguro, A., Veríssimo, J., Salgado, R., & Murteira, T. (2022). Benchmarking Deep Learning Methods for Behaviour-Based Network Intrusion Detection. Informatics, 9, 29. https://doi.org/10.3390/informatics9010029.

[53] Khoa, T., Son, D., Hoang, D., Trung, N., Quynh, T., Nguyen, D., Ha, N., & Dutkiewicz, E. (2022). Collaborative Learning for Cyberattack Detection in Blockchain Networks. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 54, 3920-3933. https://doi.org/10.1109/TSMC.2024.3374280.

[54] Qiu, C., Ren, X., & Mai, T. (2021). Deep Reinforcement Learning Empowered Adaptivity for Future Blockchain Networks. IEEE Open Journal of the Computer Society, 2, 99-105. https://doi.org/10.1109/ojcs.2020.3010987.

[55] Xiao, R., Cao, Y., & Xia, B. (2025). Adaptive Tip Selection for DAG-Shard-Based Federated Learning with High Concurrency and Fairness. Sensors, 25(1). https://doi.org/10.3390/s25010019

[56] Feng, C., Celdr'an, A., Von Der Assen, J., Beltr'an, E., Bovet, G., & Stiller, B. (2024). DART: A Solution for Decentralized Federated Learning Model Robustness Analysis. Array, 23, 100360. https://doi.org/10.48550/arXiv.2407.08652.

[57] Konstantinidis, K., Vaswani, N., & Ramamoorthy, A. (2022). Detection and Mitigation of Byzantine Attacks in Distributed Training. IEEE/ACM Transactions on Networking, 32, 1493-1508. https://doi.org/10.1109/TNET.2023.3324697.

[58] Zhang, P., Ding, S., & Zhao, Q. (2023). Exploiting Blockchain to Make AI Trustworthy: A Software Development Lifecycle View. ACM Computing Surveys, 56, 1 - 31. https://doi.org/10.1145/3614424.

[59] Tiamiyu, D., Aremu, S., Emmanuel, I., Ihejirika, C., Adewoye, M., & Ajayi, A. (2024). Interpretable Data Analytics in Blockchain Networks Using Variational Autoencoders and Model-Agnostic Explanation Techniques for Enhanced Anomaly Detection. International Journal of Scientific Research in Science and Technology. https://doi.org/10.32628/ijsrst24116170.

[60] Sun, T., & Yu, W. (2020). A Formal Verification Framework for Security Issues of Blockchain Smart Contracts. Electronics. https://doi.org/10.3390/electronics9020255.

[61] Abellán Álvarez, I., Gramlich, V., &Sedlmeir, J. (2024, April). Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of- work and proof-of-stake. In Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing (pp. 278-287).

[62] Liu, A., Chen, J., He, K., Du, R., Xu, J., Wu, C., ... & Ma, J. (2024). Dynashard: Secure and adaptive blockchain sharding protocol with hybrid consensus and dynamic shard management. IEEE Internet of Things Journal.

[63] Asif, R., & Hassan, S. (2023). Shaping the future of Ethereum: exploring energy consumption in Proof-of- Work and Proof-of-Stake consensus. Frontiers Blockchain, 6. https://doi.org/10.3389/fbloc.2023.1151724.

[64] Schwarz-Schilling, C., Neu, J., Monnot, B., Asgaonkar, A., Tas, E., & Tse, D. (2021). Three Attacks on Proof-of- Stake Ethereum. IACR Cryptol. ePrint Arch., 2021, 1413. https://doi.org/10.1007/978-3-031-18283-9_28.

[65] Wang, B., Li, Z., & Li, H. (2020). Hybrid consensus algorithm based on modified proof-of-probability and DPoS. Future Internet, 12(8). https://doi.org/10.3390/FI12080122

[66] Naeem, Mena. (2024). Adaptive Consensus Mechanism for Energy-Efficient IoT Networks via Power Consumption as a Key Factor. International Journal of Computer Science and Information Security, Vol. 22 No.5. 5.

[67] Pang, Y. (2020). A New Consensus Protocol for Blockchain Interoperability Architecture. IEEE Access, 8, 153719-153730. https://doi.org/10.1109/access.2020.3017549.

[68] Gol, D. A., &Gondaliya, N. (2024). Blockchain: A comparative analysis of hybrid consensus algorithm and performance evaluation. Computers and Electrical Engineering, 117. https://doi.org/10.1016/j.compeleceng.2023.108934

[69] Ahn, J., Yi, E., & Kim, M. (2024). Blockchain consensus mechanisms: A bibliometric analysis (2014–2024) using vosviewer and r bibliometrix. Information, 15(10), 644.

[70] He, Y., Wang, Y., Qiu, C., Lin, Q., Li, J., & Ming, Z. (2021). Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach. IEEE Internet of Things Journal, 8, 2226- 2237. https://doi.org/10.1109/jiot.2020.3035437

[71] Gan, B., Wang, Y., Wu, Q., Zhou, Y., & Jiang, L. (2022). EIoT-PBFT: A multi-stage consensus algorithm for IoT edge computing based on PBFT. Microprocess. Microsystems, 95, 104713. https://doi.org/10.1016/j.micpro.2022.104713.