A Systematic Review and Taxonomy of Privacy-Preserving Blockchain Consensus Mechanisms

Sahnius Usman[1], Sharifah Khairun Nisa Habib Elias[2], Suriayati Chuprat[3], Ahmad Akmaluddin Bin Mazlan[4]
Malaysia-Japan International Institute of Technology, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia[1]
Faculty of Artificial Intelligence, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia[2, 3]
Fakulti Sains dan Teknologi, Universiti Sains Islam Malaysia, Nilai, Malaysia[4]

Abstract*—Blockchain systems rely on consensus mechanisms to validate transactions and coordinate distributed participants, making consensus a critical layer that shapes security, trust, and privacy. Although blockchain is increasingly applied in privacy-sensitive domains such as healthcare, smart cities, and the Internet of Things, existing review studies primarily examine security or performance and rarely analyse how consensus-level design properties influence privacy risks. As a result, privacy is often treated as a peripheral enhancement rather than a core consensus concern. This study presents a systematic literature review that examines blockchain consensus mechanisms from a privacy-focused perspective. The review aims to identify which consensus classes are most commonly used in privacy-preserving blockchain systems, what privacy limitations are reported across different consensus designs, and how privacy-preserving techniques are integrated into consensus mechanisms. The review follows PRISMA and Kitchenham-guided procedures, using structured search and screening of peer-reviewed journal articles from major academic databases, followed by relevance and quality assessment. 72 peer-reviewed journal articles were synthesised using taxonomy-based and thematic analysis. The proposed taxonomy explicitly classifies studies by consensus mechanism class, privacy limitation, and integration level, enabling structured comparison beyond existing surveys. The findings show that Byzantine Fault Tolerant (BFT)-based consensus mechanisms are most frequently adopted in privacy-preserving blockchain applications. However, privacy challenges such as identity exposure and communication pattern leakage remain common and are closely linked to consensus design properties. In addition, most studies rely on external privacy mechanisms rather than embedding privacy directly into the consensus layer. This review contributes a structured taxonomy, clear analytical insights, and practical guidance that support the development and evaluation of privacy-aware blockchain consensus mechanisms.

Keywords*—Blockchain; Byzantine Fault Tolerance; consensus mechanisms; privacy-aware consensus; privacy preserving; systematic literature review

I. Introduction

A. Background and Importance

Blockchain technology has emerged as a critical infrastructure for decentralised and tamper-resistant data management in distributed systems. Blockchain promotes data integrity, transparency, and fault tolerance in untrusted environments by allowing a network of nodes to reach an agreement without the need for a central authority [1], [2]. These characteristics have prompted its use in industries like healthcare, supply chain management, smart cities, and the Internet of Things (IoT), where secure and auditable data sharing is critical [3], [4]. Despite these advantages, privacy is still a major concern in blockchain-based systems. The transparency of distributed ledgers can reveal sensitive information, such as transaction metadata, participant identities, and communication patterns [5]. Previous studies have identified several barriers to blockchain adoption in privacy-sensitive applications, including scalability limitations, high communication overhead, identity exposure, and limited support for fine-grained access control [6], [7]. Addressing these issues is critical to deploying blockchain in regulated and data-sensitive environments. The consensus mechanism is a critical element that directly impacts the behaviour of blockchains. Consensus mechanisms allow distributed nodes to agree on the ledger's state, validate transactions, resolve conflicts, and tolerate errors or adversarial behaviour [2], [8]. Consensus mechanisms are traditionally evaluated in terms of security, performance, and scalability, but they also influence how information flows across the network. Validator roles, leader election strategies, and message exchange patterns can unintentionally reveal sensitive information. As a result, consensus mechanisms have a direct and frequently overlooked impact on privacy.

B. Current Research Landscape

Research on blockchain consensus mechanisms has expanded rapidly in recent years. Numerous studies focus on improving throughput, reducing latency, enhancing fault tolerance, and lowering energy consumption [9], [10]. Proof-based mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) have been widely studied due to their applicability in public blockchains [2], [10]. In parallel, Byzantine Fault Tolerant (BFT) mechanisms, particularly Practical Byzantine Fault Tolerance (PBFT) and its variants, have gained attention in permissioned and consortium blockchain settings because of their strong consistency and fault tolerance guarantees [8], [11]. At the same time, a growing body of research addresses privacy preservation in blockchain systems. These studies commonly employ cryptographic techniques such as encryption, anonymisation, access control, and off-chain storage to protect sensitive data [5], [12]. Such approaches improve confidentiality and regulatory compliance, particularly in healthcare and IoT applications.

However, these two research streams are often treated independently. Privacy-focused studies typically concentrate on the data or application layer, while consensus-focused studies prioritise efficiency and robustness. As a result, privacy is frequently treated as an external enhancement layered on top of existing consensus protocols rather than as a property influenced by consensus design itself. This separation limits a deeper understanding of how consensus mechanisms contribute to privacy risks or protections in blockchain systems.

C. Limitation of Current Review Studies

Numerous review articles and surveys have investigated blockchain technology and consensus mechanisms, offering valuable insights into protocol designs, performance trade-offs, and scalability challenges [9], [10], [13]. Some surveys also address security and privacy concerns in blockchain environments. The existing reviews are notable for their limitations, despite their contributions. Performance, scalability, and fault tolerance are the primary focus of the majority of surveys, while privacy is only briefly reviewed. Secondly, privacy is frequently addressed as an application-layer concern, without a formal examination of the ways in which consensus mechanisms introduce or exacerbate privacy risks. Thirdly, the consensus mechanism classes, reported privacy limitations, and the extent to which privacy-preserving techniques are integrated into the consensus process are rarely linked in existing reviews in a structured taxonomy.

As a result, the current reviews do not provide a clear explanation of the reasons why specific consensus mechanisms are preferred in privacy-sensitive systems, the impact of consensus-level operations on privacy, or whether privacy is addressed internally or externally. This gap restricts their usefulness as design references for privacy-aware blockchain systems.

D. Research Gap

Based on the existing literature, there is a clear lack of systematic, consensus-centric reviews that examine blockchain consensus mechanisms explicitly through a privacy-focused perspective. In particular, there is insufficient synthesis of 1) which consensus mechanism classes are most frequently adopted in privacy-preserving blockchain systems, 2) what privacy limitations are reported for different consensus designs, and 3) how privacy-preserving techniques are integrated into consensus mechanisms.

Without such analysis, privacy risks originating from consensus design remain poorly understood, and system designers may select consensus mechanisms without clear insight into their privacy implications. Addressing this gap requires a structured review that places consensus mechanisms at the centre of privacy analysis rather than treating privacy as a peripheral concern.

E. Objectives and Contributions

To address the identified gap, this study conducts a systematic literature review with the following objectives:

- To identify which classes of blockchain consensus mechanisms are most frequently adopted in privacy-preserving blockchain systems.
- To analyse the privacy limitations reported across different consensus mechanism classes.
- To examine how privacy-preserving techniques are integrated into blockchain consensus mechanisms.

The main contributions of this review are:

- A taxonomy-driven synthesis that classifies existing studies based on consensus mechanism class, reported privacy limitations, and integration level of privacy-preserving techniques.
- An evidence-based analysis linking consensus design properties to observed privacy risks.
- Practical insights to support researchers and practitioners in selecting and designing consensus mechanisms for privacy-sensitive blockchain applications.

The remainder of this paper is organised as follows. Section II describes the research methodology, including study selection and analysis procedures. Section III presents and discusses the results of the systematic review in relation to the research questions. Section IV concludes the paper and outlines future research directions.

II. Methodology

The systematic literature review was conducted in accordance with Kitchenham's guidelines for systematic literature reviews in software engineering [14]. and reported using the PRISMA framework as illustrated in Fig. 1. An initial database search identified relevant peer-reviewed journal articles related to blockchain consensus mechanisms and privacy. After duplicate removal, 1595 records remained for screening. After screening process using inclusion and exclusion criteria, 1478 records are excluded, leaving 117 record for the next process. Full-text eligibility assessment was then applied using predefined practical inclusion and exclusion criteria, resulting in the exclusion of 25 records that did not meet the requirements, and leaving 92 studies**.** These studies were further assessed for conceptual relevance to the research questions, leading to the exclusion of 20 records due to insufficient focus on consensus mechanisms or privacy aspects. The remaining 72 studies were subjected to a quality assessment using a structured scoring rubric. All 72 studies met the minimum quality threshold and were included in the final synthesis.

This structured process guarantees transparency, reproducibility, and methodological rigour in accordance with the established best practices of SLR. Fig. 1 shows the PRISMA diagram that illustrates the comprehensive review process. The detail explanation will be provided in the following section.

A. Review Planning and Research Question Formulation

Following Kitchenham's guidelines for systematic literature reviews in software engineering, the review process began with careful planning to define the scope and objectives of the study. Research questions were formulated using the PICO framework (Population, Intervention, Comparison, Outcome)**,** which Kitchenham identifies as an effective structuring tool for evidence-based software engineering reviews [14] to ensure clarity and relevance. The population was defined as

blockchain-based systems reported in peer-reviewed literature. The intervention corresponds to different classes of blockchain consensus mechanisms, while the comparison dimension captures variations across consensus designs. The outcomes focus on consensus taxonomy, associated privacy limitations, and the level of integration of privacy-preserving techniques.

Using this structured approach, three research questions (RQ1–RQ3) were formulated to enable consistent study identification, data extraction, and synthesis in line with Kitchenham's recommendations. Table I shows how RQ1-RQ3 formulated based on PICO framework. There is no records were retrieved at this stage. This step established the conceptual foundation of the review.

- RQ1- Which classes of blockchain consensus mechanisms are most frequently adopted in privacy-preserving blockchain systems?
- RQ2- What privacy limitations are reported for different classes of blockchain consensus mechanisms across existing studies?
- RQ3 - How are privacy-preserving techniques integrated into blockchain consensus mechanisms in existing studies?

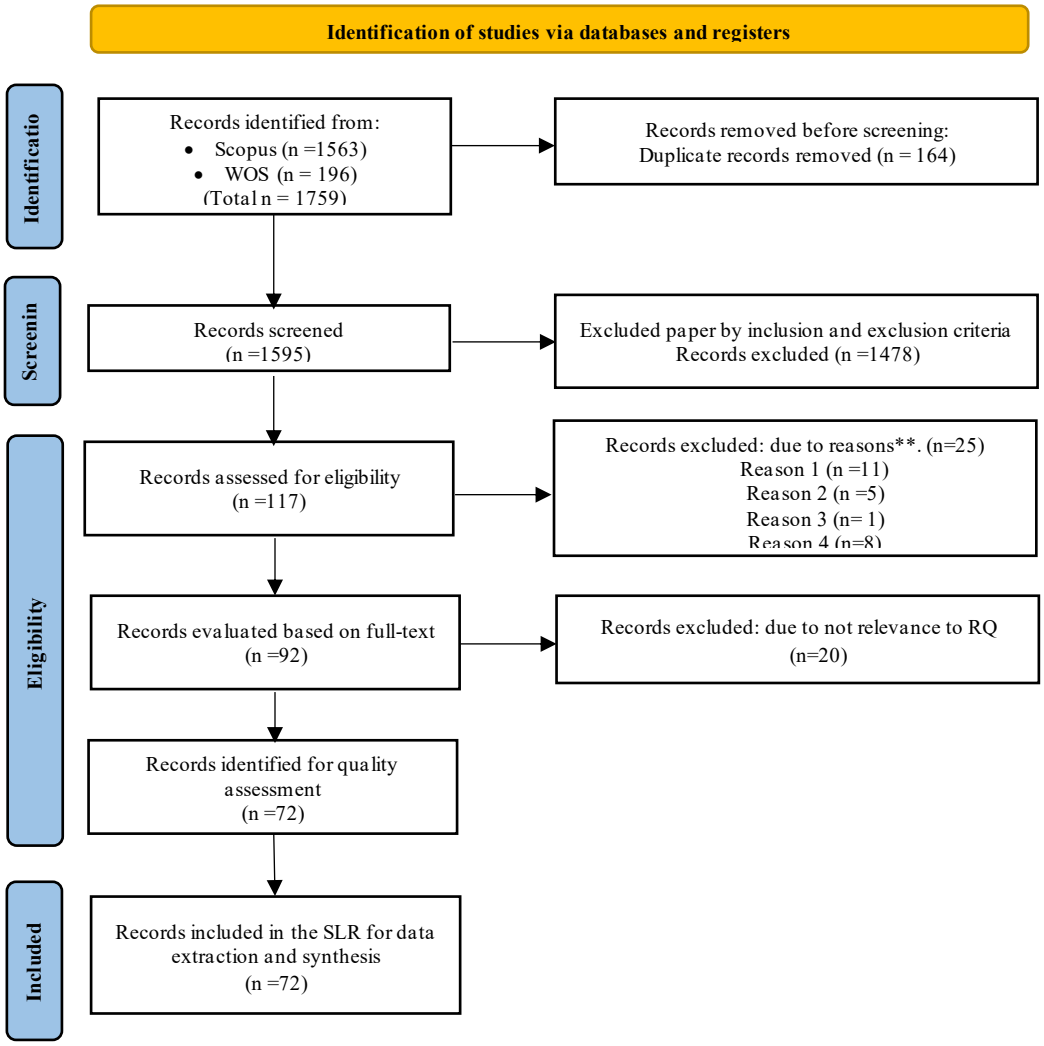

Fig. 1. The comprehensive review process is illustrated in the PRISMA diagram. (**Notes: Reason 1-Blockchain not actively used in objectives/method/results, Reason 2 - Review/survey without system evaluation, Reason 3 -No evaluation/validation-conceptual only, Reason 4 - No evaluation/validation-conceptual only).

TABLE I. SEARCH STRING

Database	Search string
Scopus	TITLE-ABS-KEY (("consensus mechanism" OR "consensus algorithm" OR "voting system" OR "agreement protocol") AND ("blockchain" OR "distributed ledger" OR "DLT" OR "crypto*") AND ("privacy" OR "confidentiality" OR "anonymity" OR "data protection") AND ("limitation" OR "challenge" OR "drawback" OR "issue"))
WoS	Refine results for ("consensus mechanism" OR "consensus algorithm" OR "voting system" OR "agreement protocol") AND ("block chain" OR "distributed ledger" OR "DLT" OR "crypto*") AND ("privacy" OR "confidentiality" OR "anonymity" OR "data protection") AND ("limitation" OR "challenge" OR "drawback" OR "issue") (Topic)

B. Identification of Relevant Articles

A comprehensive search was conducted using two major academic databases: Scopus and Web of Science (WoS). These databases were selected due to their broad coverage of high-quality, peer-reviewed research in computer science and engineering. computer science, blockchain technology, and information security domains.

The search was performed using predefined keyword combinations targeting blockchain consensus mechanisms and privacy-related limitations. The search focused on peer-reviewed journal articles related to blockchain, consensus mechanisms, and privacy preservation. The initial search retrieved 1,759 records, including 1,563 records from Scopus and 196 records from WoS. The search strings were applied to titles, abstracts, and keywords in Scopus, and to topic fields in Web of Science as shown in Table II.

Before screening, 164 duplicate records were identified and removed. After deduplication, 1,595 unique records remained and were carried forward to the screening stage.

- Records identified: 1,759
- Duplicate records removed: 164
- Records after deduplication: 1,595

TABLE II. RQS FORMULA BASED ON PICO

Research Question	Population (P)	Intervention (I)	Comparison (C)	Outcome(O)
RQ1	Blockchain-based systems reported in peer-reviewed studies	Adoption of different consensus mechanism classes (e.g., BFT-based, proof-based, authority-based)	Comparison across consensus mechanism classes	Taxonomic distribution and application contexts of consensus mechanisms in privacy-related blockchain systems
RQ2	Blockchain consensus mechanisms used in existing studies	Consensus design choices and operational characteristics	Comparison between different consensus classes and designs	Identified privacy limitations (e.g., identity exposure, communication leakage, metadata inference) associated with each class
RQ3	Blockchain systems employing privacy-preserving solutions	Integration of privacy-preserving techniques at or beyond the consensus layer	Integrated vs. external (overlay) privacy mechanisms	Degree of privacy integration within consensus mechanisms and its implications for privacy preservation

C. Inclusion and Exclusion Criteria

The SLR establishes inclusion criteria to identify papers relevant to the research objectives. These standards ensure that studies that are directly relevant to the research issue are included, while studies that are irrelevant to the research emphasis or do not adhere to the established standards are excluded. The titles and abstracts of the 1,595 records were screened using predefined inclusion and exclusion criteria. Studies were excluded at this stage if they:

- were not related to blockchain technology,
- did not involve consensus mechanisms,
- did not address privacy or privacy-related concerns, or
- were not peer-reviewed journal articles.

As a result of this screening process, 1,478 records were excluded. The remaining 117 records were retained for full-text eligibility assessment. Fig. 1 illustrates the paper selection process and Table III describes the primary inclusion criteria for this investigation.

- Records screened: 1,595
- Records excluded during screening: 1,478
- Records retained for full-text assessment: 117

After applying practical eligibility filters, studies were further assessed for topical relevance to the research question. Only studies providing direct evidence on consensus mechanism limitations related to privacy preservation were retained. A subsequent quality assessment was then conducted to evaluate the methodological rigor of the included studies, in line with Kitchenham's guidelines.

TABLE III. INCLUSION AND EXCLUSION CRITERIA IN SCREENING PROCESS

Criterion	Inclusion	Exclusion
Source Type	Journal	• Conference • proceeding • Book series • Book • Trade journal
Document Type	Article	• Conference paper • Book chapter • Review • Conference review • Book • Editorial • Retracted • Note • Erratum • Short survey • Letter • Data paper
Subject Area	Computer Science	Other than Computer Science
Year	2024-2026	Before 2024
Language	English	Non-English
Keywords	• Consensus Algorithm • Consensus Algorithms • Consensus mechanism • Consensus Protocols • Data Privacy • Data Privacy • Protections • Data Security	Other than selected keywords

D. Eligibility Assessment

Full texts of the 117 retained articles were assessed in detail to determine their relevance to the research questions. Studies were excluded if the full text:

- did not provide sufficient discussion of consensus mechanisms,
- did not address privacy limitations or privacy-preserving approaches, or
- lacked relevance to the defined research questions.

At this stage, 25 articles were excluded for specific reasons, including insufficient consensus-related content, limited privacy discussion, or methodological inadequacy, as documented in Table IV. Each excluded article was recorded with a specific reason to ensure auditability. After full-text eligibility assessment, 92 articles remained.

- Full-text articles assessed: 117
- Full-text articles excluded: 25
- Records evaluated based on full text: 92

TABLE IV. INCLUSION AND EXCLUSION CRITERIA IN ELIGIBILITY ASSESSMENT

Reason ID	Detail
Reason 1	Blockchain not actively used in objectives/method/results
Reason 2	Review/survey without system evaluation
Reason 3	No evaluation/validation-conceptual only
Reason 4	no access, cannot validate

E. Relevance Assessment

The remaining studies were evaluated for conceptual relevance to the research questions. Following the application of practical eligibility criteria (Step 3), 92 full-text articles were retained and assessed for topical relevance (Step 4) using Kitchenham's evidence-based selection principle. Each article was evaluated to determine whether it provided direct evidence related to the research question on limitations of blockchain consensus mechanisms in supporting privacy preservation. As a result, 20 studies were excluded due to insufficient relevance to the research questions

- Records excluded due to insufficient relevance: 20 records
- Records included after relevance assessment: 72 records

F. Quality Check

A quality assessment was conducted on the 72 studies that passed the relevance screening stage to evaluate their methodological rigor and reliability, following Kitchenham's guidelines for systematic literature reviews. Each study was assessed based on clarity of objectives, explicit description of the consensus mechanism, and adequacy of privacy-related analysis. All studies met the predefined quality threshold and were included in the final synthesis.

- Records assessed for quality: 72
- Records excluded at quality stage: 0
- Final studies included in the SLR: 72

G. Data Extraction and Synthesis

For the included studies, structured data extraction was performed to capture information related to consensus mechanism class, privacy limitations, and the integration level of privacy-preserving techniques. The extracted data were synthesised using taxonomy-based and thematic analysis, enabling quantitative comparison and cross-study interpretation. This approach supports Kitchenham's recommendation to combine descriptive statistics with qualitative synthesis when addressing complex design-oriented research questions.

H. Reporting

The results of the SLR are reported using tables and structured discussion to ensure clarity and reproducibility. Quantitative summaries and taxonomic classifications are presented to support transparent interpretation of findings.

I. Threats to Validity

Several potential threats to validity were considered. First, publication bias may exist due to the exclusion of non-English studies and grey literature. Second, database selection may limit coverage, although Scopus and Web of Science provide extensive indexing of relevant journals. To mitigate these threats, carefully designed search strings, multiple databases, and expert-driven eligibility assessment were employed.

III. RESULTS AND DISCUSSION

This section discusses the findings of the systematic literature review based on the 72 included studies, with emphasis on interpreting observed research patterns and their implications for privacy-preserving blockchain design. The discussion is structured around the three research questions (RQ1–RQ3) and adopts a taxonomy- and theme-based synthesis to examine how consensus mechanisms are selected, analysed, and implemented in existing studies. First, the prevalence of different consensus mechanism classes is examined to understand dominant design choices and underlying assumptions in privacy-sensitive blockchain systems. Next, recurring privacy limitations associated with consensus designs are discussed to reveal structural weaknesses that persist across studies. Finally, the extent to which privacy-preserving techniques are integrated into the consensus layer is analysed to highlight current design practices and unresolved challenges. By linking these observations, this section identifies critical gaps between consensus selection and privacy-by-design principles, providing a foundation for the research directions outlined later.

A. RQ1: Which Classes of Blockchain Consensus Mechanisms are Most Frequently Adopted in Privacy-Preserving Blockchain Systems?

This subsection addresses RQ1, which investigates the classes of blockchain consensus mechanisms examined in the literature and their taxonomic distribution. The analysis is based on the synthesis presented in Table V, which classifies the consensus mechanisms adopted across the 72 included studies. According to Table V, the Byzantine Fault Tolerant (BFT) based class is the consensus mechanism class that is most frequently

reported in privacy-preserving blockchain systems. This class is referenced in 18 papers, which is 25 percent of the total papers as shown in Fig. 2. The leader-based consensus class, which is represented in four papers, is the least frequently reported class.

The BFT-based class's dominance is telling of its widespread adoption in permissioned and consortium blockchain environments. In the reviewed studies, Practical Byzantine Fault Tolerance (PBFT), ZK-BFT, and MGRS-PBFT are common examples of BFT-based consensus mechanisms. In contrast, RAFT is an example of a leader-based consensus mechanism that has received little attention in privacy-focused blockchain research.

The BFT class is the most popular because it works well in permissioned blockchain environments, where nodes that are part of the network are known and access is controlled [15]. This controlled participation reduces the unnecessary dissemination of data during consensus execution and limits the exposure of sensitive data to unauthorised nodes. Therefore, BFT-based consensus mechanisms improve privacy by limiting the access of validators and minimising the leakage of identity and communication within the network [16].

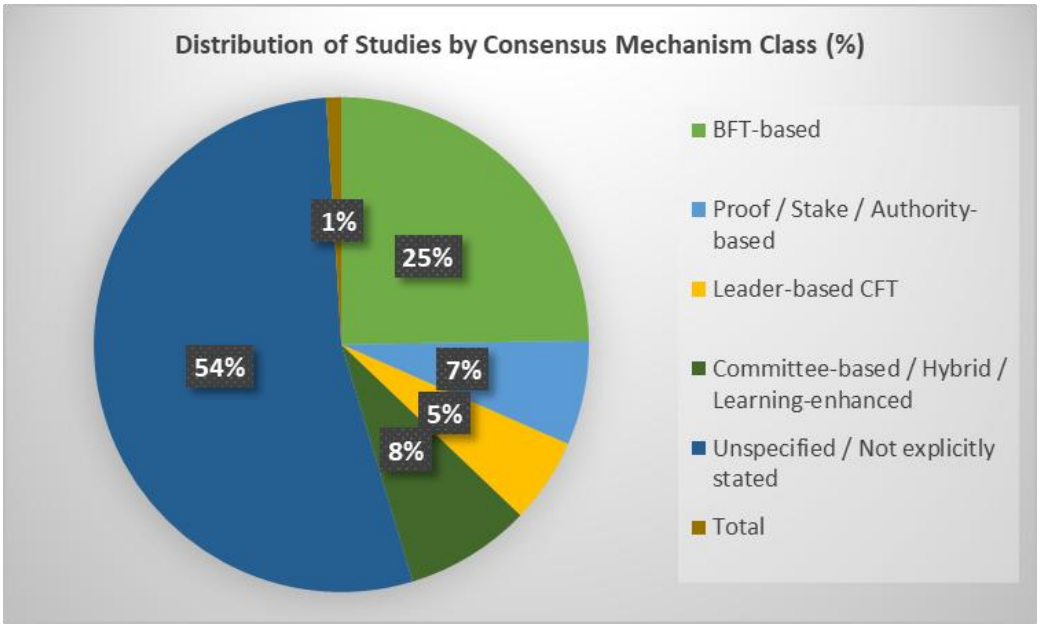

Fig. 2. Distribution of consensus classes.

TABLE V. DISTRIBUTION OF STUDIES BY CONSENSUS MECHANISM CLASS

Consensus Mechanism Class	Percentage (%)	No. of Papers	Consensus Mechanism Type	References
BFT-based	25	18	PBFT, dBFT, DG-PBFT, Grouped PBFT, MGRS-PBFT, TRUG-PBFT, CRBFT, Reputation-Enhanced PBFT, Improved PBFT, RL-Enhanced PBFT, QBFT, HotStuff, Efficient-HotStuff, Lightweight BFT, Context-Aware BFT, RSHS, MuLCOff	[15], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49] [15], [33]-[49]
Proof / Stake / Authority-based	6.9	5	PoW, PoS, Hybrid PoW–PoS, DPoS, RC-DPoS, PoA, Improved PoA, PoSS	[50], [51], [52], [53], [54] [50]-[54]
Leader-based CFT	5.6	4	RAFT	[55], [56], [57], [58] [37]-[40]
Committee-based / Hybrid / Learning-enhanced	8.3	6	Proof-of-Contribution Committee, PoLU, PoTP, RCME, Q-Learning–Enhanced Consensus, DQN-Enhanced Consensus	[59], [60], [61], [62], [63], [64] [59]-[64]
Unspecified / Not explicitly stated	54.2	39	Not specified by authors	[65], [66], [67], [68] [49],[65]-[103] [69], [70], [71], [72], [73], [74], [75], [76], [77] [78], [79], [80], [81], [82], [83], [84], [85], [86] [49], [87], [88], [89], [90], [91], [92], [93], [94] [95], [96], [97], [98], [99], [100], [101], [102], [103]
Total	**100%**	**72**	—	—

In Byzantine Fault Tolerance (BFT)-based blockchain systems, three synthesised strategies are commonly used to improve privacy. First, identity privacy is enhanced by integrating ring-signature mechanisms into BFT consensus, which conceal validator identities while maintaining consensus correctness, as demonstrated by MGRS-PBFT [15]. This approach is consistent with previous ring-based Byzantine consensus designs that conceal signer identities during validation [17], and it is further supported by research highlighting anonymity as a critical privacy requirement in BFT-driven blockchain services [18].

Second, integrating zero-knowledge proofs into BFT protocols improves transaction confidentiality by allowing nodes to verify transaction validity without disclosing sensitive data, as demonstrated in ZK-BFT [16]. Similar privacy guarantees are explored in quantum-resistant Byzantine consensus models [19] and cryptography-enhanced BFT frameworks [18]. Third, privacy exposure is decreased through group-based or sharded BFT architectures, where only subsets of validators process transactions [20], consistent with sharded Byzantine consensus designs [21] and scalability-driven consensus partitioning studies [22].

The Leader-based Class Consensus Mechanism like RAFT is not frequently used to enhance privacy preservation in blockchain systems due to two key factors. First, RAFT provides only crash fault tolerance and does not protect against malicious or Byzantine behaviour, which is critical in privacy-sensitive environments [23], [24]. Second, RAFT relies on a leader-based architecture, where a single leader coordinates all consensus operations. This design creates a potential single point of failure and increases privacy risks if the leader node is compromised [25], [26]

Unlike BFT-oriented designs, privacy enhancement in RAFT-based blockchain systems is typically accomplished through additional mechanisms rather than core consensus features. Firstly, numerous studies have improved the privacy of RAFT by integrating it with trusted execution environments (TEEs). In these environments, transaction execution and state management take place within secure enclaves, thereby restricting data exposure, despite the fact that RAFT is still crash-fault tolerant [23]. This approach is consistent with consortium blockchain designs that use hardware-assisted isolation for confidentiality [27] and proxy-signature-based trust delegation [28]. Second, privacy is enhanced through hybrid consensus and cryptographic modifications, in which RAFT is combined with mechanisms such as Proof of Work or credit-based models to reduce trust concentration and mitigate the inference risks associated with leader-based coordination [24], [29], [30]. Third, RAFT deployments frequently rely on strict access control and permissioned governance to ensure that only authenticated nodes participate in consensus, which indirectly promotes privacy by limiting data visibility to trusted members [24], [25], [31]. Overall, these enhancements show that RAFT-dependent privacy preservation is primarily architectural and operational, rather than consensus-based.

Overall, the differences in privacy outcomes between BFT-based systems and RAFT stem from their fundamental design philosophies. BFT-based consensus, such as PBFT, is inherently designed for competitive environments, so privacy is built into the consensus core by tolerating malicious behaviour, decentralising trust, and supporting cryptographic techniques like ring signatures and zero-knowledge proofs to protect identity and data [15], [16], [18]. RAFT, on the other hand, puts more value on simplicity, performance, and crash fault tolerance, assuming that participants are trustworthy and that there are no conflicting settings. Because of this, privacy protection is only possible through external methods like access control, trusted execution environments, or hybrid architectures, rather than through native consensus logic [23], [24], [32]. This philosophical distinction explains why BFT-based approaches are more suitable for privacy-sensitive blockchain applications.

B. *RQ2: What Privacy Limitations are Reported for Different Classes of Blockchain Consensus Mechanisms Across Existing Studies?*

This subsection answer RQ2, which examines the privacy limitations reported across different classes of blockchain consensus mechanisms and how these limitations vary by consensus design. The analysis is based on the evidence synthesised in Table VI, where privacy-related issues are mapped to consensus mechanism classes and supported by explicit paper-level citations.

The findings show that BFT-based consensus mechanisms have the most reported privacy limitations of any specifically identified consensus type. The most frequently observed issues are identity exposure and communication-pattern leakage, implying that privacy risks in BFT systems extend beyond transaction content to participant identifiability and traffic observability. These findings imply that privacy flaws in BFT mechanisms are inherent in their design rather than implementation-related. Hybrid consensus mechanisms exhibit recurring privacy limitations, albeit less frequently than BFT-based mechanisms. The reported issues are primarily related to architectural complexity and cross-layer information exposure. Importantly, the quantitative results show that hybridisation does not eliminate privacy risks and, in some cases, introduces new challenges.

BFT-class consensus mechanisms, such as PBFT and its variants, have inherent privacy constraints due to their operational characteristics. In BFT protocols, transactions and consensus messages are distributed among multiple replicas to accommodate Byzantine faults. This process results in a greater exposure of transaction data and metadata to consensus participants, which in turn increases the risk of privacy leakage [16]. Furthermore, traditional BFT mechanisms lack native privacy-preserving capabilities. Validator identities are commonly known, and the roles of primary and replica nodes are predictable. This predictability facilitates traffic analysis and allows adversaries to infer participant behaviour and system activity [15]. The high communication overhead required for multi-round voting increases these risks by increasing the visibility of communication patterns [104].

To address these limitations, several studies suggest enhancing BFT mechanisms with cryptographic privacy techniques. Ring signatures and traceable ring signatures are widely used to conceal validator identities while maintaining accountability [15], [17]. Zero-knowledge proofs enable nodes

to verify transaction correctness without revealing sensitive data, thereby significantly reducing information exposure [16]. Other approaches use dynamic grouping and reputation-based participation to limit long-term role exposure and mitigate the influence of malicious nodes [104]. Instead of completely replacing BFT, these solutions preserve its fault tolerance while improving privacy.

TABLE VI. PRIVACY LIMITATIONS IDENTIFIED ACROSS CONSENSUS MECHANISM CLASSES

Consensus Mechanism Class	Privacy Limitation	Description of Limitation	No. of papers	Paper IDs
BFT-based	Identity exposure	Validator or participant identities are revealed during consensus rounds, enabling traceability	9	[15]-[21], [24],[54]
	Communication pattern leakage	Frequent message exchanges expose network topology and interaction patterns	6	[15], [34], [36], [46], [47], [72]
	Metadata leakage	Transaction timing and ordering reveal sensitive operational information	4	[37], [39], [41], [43]
	Limited anonymity support	Native consensus does not support anonymity or unlinkability guarantees	4	[35], [38], [42], [53]
Proof / Stake / Authority-based	Stake / authority traceability	Stakeholders or authorities are directly linkable to consensus decisions	3	[50], [52], [53]
	Centralisation risk	Small validator sets or authorities weaken privacy through control concentration	2	[52], [53]
	Transaction linkage	Repeated validator participation enables transaction correlation	2	[41], [50]
Leader-based CFT	Leader identity exposure	Fixed or elected leaders expose control and communication endpoints	4	[37]-[40]
	Limited privacy awareness	Consensus prioritises performance over privacy guarantees	2	[55], [57]
Committee / Hybrid / Learning-enhanced	Partial privacy integration	Privacy mechanisms are selectively applied, not end-to-end	4	[41]-[43],[46]
	Model / role inference	Learning-based or committee selection leaks role or contribution information	3	[43], [59], [63]
Unspecified	Implicit consensus assumption	Privacy analysis is conducted without stating or analysing the consensus layer	13	[31],[69]-[76],[78],[80]-[82]
	Unclear privacy responsibility	Responsibility for privacy is shifted to upper layers without justification	7	[78], [83], [95], [97], [101], [102], [103]
	Lack of reproducibility	Absence of consensus details prevents comparative or reproducible evaluation	20	[47]-[59],[61]-[64],[66]-[68]

Hybrid consensus mechanisms, which integrate components from various consensus protocols, are designed to achieve a balance between security, scalability, and efficiency in blockchain systems. However, this integration introduces new privacy challenges. The interaction between heterogeneous consensus layers can lead to information leakage at protocol boundaries, rather than within a single mechanism [105]. According to [106], hybrid mechanisms frequently necessitate additional coordination and parameter exchange, which results in increased metadata exposure and communication overhead. Furthermore, hybrid systems may introduce trade-offs between privacy and performance, such as increased computational cost or latency, as a result of privacy-preserving enhancements. If not managed carefully, these trade-offs can indirectly weaken privacy guarantees [107].

Despite these challenges, hybrid consensus mechanisms can improve privacy with proper design. Anonymous communication techniques, such as Tor-based routing, are used to conceal node identities and mitigate targeted attacks [105]. Other approaches use disruption methods, dynamic key management, and privacy-aware consensus protocols to conceal sensitive states exchanged during consensus [106]. Hybrid architectures, which combine public and private blockchains, enhance privacy by limiting sensitive data to permissioned environments while ensuring public authenticity [107].

Consensus mechanisms are central to the philosophy of blockchain systems because they enable distributed agreement, trust establishment, and fault tolerance without the need for a central authority. Classical consensus designs prioritise correctness, consistency, and resilience, frequently assuming that transparency and information sharing are required to reach an agreement among distributed nodes [2], [4]. RQ2 findings show that privacy limitations in both BFT-based and hybrid consensus mechanisms are not intentional flaws, but rather structural consequences of these foundational design objectives. The emphasis on collective verification and Byzantine resilience in BFT-based mechanisms requires extensive message exchanges and role transparency, which inevitably increases identity and communication pattern exposure [2].

Hybrid consensus mechanisms use multiple protocols to balance performance, scalability, and security; however, this architectural layering introduces new privacy risks due to cross-layer interactions and increased coordination complexity [3], [4]. Recent research shows a gradual shift in consensus philosophy. Instead of treating privacy as an optional extra, modern designs increasingly incorporate cryptographic protection, anonymity, and controlled disclosure directly into the consensus layer. Techniques such as zero-knowledge proofs, anonymous authentication, and adaptive participation mechanisms aim to maintain agreement and fault tolerance while minimising unnecessary data exposure [2], [3].

In general, the RQ2 synthesis suggests that the evolution of consensus mechanisms is transitioning from a model of agreement through visibility to agreement with controlled disclosure. This shift aligns the technical operation of consensus mechanisms with broader privacy expectations in blockchain-based systems, particularly in sensitive areas like data sharing and governance. Consequently, the ongoing development of blockchain technologies is increasingly characterised by the implementation of privacy-aware consensus design.

C. RQ3: How are Privacy-Preserving Techniques Integrated Into Blockchain Consensus Mechanisms in Existing Studies?

This subsection addresses RQ3, which examines whether privacy-preserving techniques are integrated into blockchain consensus mechanisms or applied as external solutions. The analysis is based on Table VII, which maps consensus mechanism classes to privacy techniques and their integration levels.

TABLE VII. PRIVACY-PRESERVING TECHNIQUE USED IN REVIEWED STUDIES

Consensus Mechanism Class	Privacy-Preserving Technique	Integration Level	No. of Papers	References
BFT-based	Reputation / Incentives (privacy-related)	Not specified	4	[39], [42], [44], [48]
	Anonymous Authentication / Pseudonyms	Integrated (consensus-level)	2	[15], [38]
	Federated Learning Privacy (FL + privacy)	External / overlay	2	[36], [43]
	Federated Learning Privacy (FL + privacy)	Not specified	2	[42], [72]
	Not specified	Not specified	2	[37], [47]
	Sharding / Sidechain / Off-chain	Integrated (consensus-level)	2	[35], [45]
	Sharding / Sidechain / Off-chain	Not specified	2	[44], [48]
	Access Control (ACL/ABAC/RBAC/Smart contracts)	External / overlay	1	[41]
	Access Control (ACL/ABAC/RBAC/Smart contracts)	Not specified	1	[34]
	Anonymous Authentication / Pseudonyms	External / overlay	1	[46]
	Attribute-Based Encryption (ABE/CP-ABE/MA-ABE)	External / overlay	1	[41]
	Encryption (generic)	Integrated (consensus-level)	1	[35]
	Federated Learning Privacy (FL + privacy)	Integrated (consensus-level)	1	[33]
	IPFS / Distributed Storage with encryption	External / overlay	1	[41]
	IPFS / Distributed Storage with encryption	Integrated (consensus-level)	1	[35]
	Reputation / Incentives (privacy-related)	External / overlay	1	[43]
	Reputation / Incentives (privacy-related)	Integrated (consensus-level)	1	[33]
	Ring Signatures / Group Signatures	Integrated (consensus-level)	1	[15]
	Sharding / Sidechain / Off-chain	External / overlay	1	[41]
	Trusted Execution / Secure Hardware	Not specified	1	[44]
	Zero-Knowledge Proofs (ZKP)	Integrated (consensus-level)	1	[38]
Proof/Stake/Authority-based	Encryption (generic)	External / overlay	3	[50], [52], [54]
	Access Control (ACL/ABAC/RBAC/Smart contracts)	External / overlay	2	[41], [50]
	Attribute-Based Encryption (ABE/CP-ABE/MA-ABE)	External / overlay	1	[41]
	Homomorphic Encryption (HE)	External / overlay	1	[54]
	IPFS / Distributed Storage with encryption	External / overlay	1	[41]
	Not specified	Not specified	1	[53]
	Reputation / Incentives (privacy-related)	External / overlay	1	[52]
	Sharding / Sidechain / Off-chain	External / overlay	1	[41]
Leader-based CFT	Access Control (ACL/ABAC/RBAC/Smart contracts)	Integrated (consensus-level)	1	[56]

	Access Control (ACL/ABAC/RBAC/Smart contracts)	Not specified	1	[55]
	Differential Privacy (DP)	External / overlay	1	[57]
	Federated Learning Privacy (FL + privacy)	External / overlay	1	[58]
Committee/Hybrid/Learning-enhanced	Federated Learning Privacy (FL + privacy)	External / overlay	2	[43], [60]
	Federated Learning Privacy (FL + privacy)	Not specified	2	[59], [61]
	Reputation / Incentives (privacy-related)	Not specified	2	[59], [61]
	Access Control (ACL/ABAC/RBAC/Smart contracts)	Integrated (consensus-level)	1	[63]
	Encryption (generic)	Integrated (consensus-level)	1	[63]
	Not specified	Not specified	1	[64]
	Reputation / Incentives (privacy-related)	External / overlay	1	[43]
	Reputation / Incentives (privacy-related)	Integrated (consensus-level)	1	[63]
	Sharding / Sidechain / Off-chain	External / overlay	1	[60]
	Trusted Execution / Secure Hardware	Integrated (consensus-level)	1	[63]
	Trusted Execution / Secure Hardware	Not specified	1	[59]
Unspecified/Not stated	Not specified	Not specified	9	[67], [68], [69], [70], [76], [91], [102], [103], [114]
	Encryption (generic)	External / overlay	8	[49], [66], [71], [74], [78], [80], [92], [95]
	Access Control (ACL/ABAC/RBAC/Smart contracts)	External / overlay	7	[49], [66], [74], [80], [85], [88], [96]
	Access Control (ACL/ABAC/RBAC/Smart contracts)	Not specified	7	[75], [79], [84], [89], [90], [93], [94]
	Federated Learning Privacy (FL + privacy)	External / overlay	5	[71], [78], [81], [82], [83]
	Anonymous Authentication / Pseudonyms	External / overlay	3	[74], [88], [92]
	Federated Learning Privacy (FL + privacy)	Not specified	3	[72], [97], [98]
	IPFS / Distributed Storage with encryption	External / overlay	3	[66], [87], [95]
	Reputation / Incentives (privacy-related)	External / overlay	3	[78], [80], [82]
	Sharding / Sidechain / Off-chain	Not specified	3	[86], [99], [100]
	Access Control (ACL/ABAC/RBAC/Smart contracts)	Integrated (consensus-level)	2	[65], [115]
	Attribute-Based Encryption (ABE/CP-ABE/MA-ABE)	External / overlay	2	[49], [80]
	Encryption (generic)	Integrated (consensus-level)	2	[73], [101]
	Encryption (generic)	Not specified	2	[75], [90]
	Homomorphic Encryption (HE)	External / overlay	2	[71], [74]
	IPFS / Distributed Storage with encryption	Not specified	2	[86], [99]
	Sharding / Sidechain / Off-chain	External / overlay	2	[80], [95]
	Attribute-Based Encryption (ABE/CP-ABE/MA-ABE)	Integrated (consensus-level)	1	[73]
	Attribute-Based Encryption (ABE/CP-ABE/MA-ABE)	Not specified	1	[75]
	IPFS / Distributed Storage with encryption	Integrated (consensus-level)	1	[65]
	Reputation / Incentives (privacy-related)	Integrated (consensus-level)	1	[101]
	Secure Multi-Party Computation (SMPC)	External / overlay	1	[77]
	Sharding / Sidechain / Off-chain	Integrated (consensus-level)	1	[101]
	Trusted Execution / Secure Hardware	External / overlay	1	[80]
	Zero-Knowledge Proofs (ZKP)	Integrated (consensus-level)	1	[101]

Table VII classifies the reviewed studies based on where privacy-preserving techniques are used in BFT-class consensus systems. The table distinguishes between (i) privacy mechanisms built directly into the consensus protocol and (ii) external or overlay-level privacy mechanisms, such as cryptographic add-ons or architectural layers that exist outside of the core consensus protocol. The table shows the frequency of studies using each approach, allowing for a comparison of design preferences and implementation trends in the literature. The findings indicate that privacy-preserving techniques are more commonly integrated at the consensus level in BFT-class mechanisms than at the external or overlay level. A large portion of research focuses on modifying PBFT-style protocols by incorporating cryptographic primitives directly into consensus operations like message validation and leader coordination. Fewer studies rely solely on externalised privacy mechanisms, though such approaches remain important. In qualitative terms, consensus-level integration is typically motivated by strong competitive implications and the need for Byzantine resilience, whereas external mechanisms are frequently used to improve modularity, flexibility, and system interoperability. These results show that privacy arrangement is not just a random design choice, but a planned architectural trade-off.

BFT-class consensus mechanisms work in environments where nodes may act maliciously. As a result, privacy-preserving techniques are frequently embedded at the consensus level to safeguard node identities, transaction data, and coordination messages during agreement execution. Ring signatures, threshold signatures, and zero-knowledge proofs are used to prevent malicious nodes from obtaining sensitive information while still allowing for transaction verification and fault tolerance [15], [16], [104]. The risk of Byzantine manipulation is also mitigated by embedding privacy within the consensus layer, as privacy and security guarantees are enforced during message exchange and validation, rather than relying on external safeguards [17], [108]. Because of this, consensus-level privacy is frequently seen as essential in permissioned or consortium blockchains, which have lower trust assumptions.

Despite the advantages of consensus-level privacy, many BFT-based systems incorporate privacy mechanisms at the external or overlay level in order to maintain protocol simplicity and performance. External mechanisms enable designers to implement encryption, deception, or anonymisation without significantly altering the consensus logic [15], [16]. This approach improves modularity by allowing privacy mechanisms to be updated or replaced independently. Overlay-level privacy is also used to protect against external adversaries, such as traffic analysis or data inference attacks that take place outside of the consensus process, while remaining compatible with existing BFT implementations [17]. As a result, externalised privacy mechanisms are frequently preferred in systems that value deployment and scalability.

The literature suggests several approaches to translating externalised privacy mechanisms into actionable design principles. First, privacy-by-design necessitates that privacy objectives be explicitly defined at the architectural stage, even if they are implemented outside the consensus layer [109], [110]. Second, privacy design strategies and patterns, such as anonymisation, encryption, and access control, are reusable building blocks that can be systematically evaluated [110], [111]. Third, effective frameworks prioritise ongoing privacy evaluation and monitoring to ensure that external mechanisms remain effective as system conditions change [112]. Lastly, it is imperative to evaluate externalised privacy in the context of regulatory and contextual requirements, particularly in sensitive domains like healthcare and governance [113]. These principles establish concrete criteria for determining whether external privacy mechanisms effectively supplement consensus security.

The findings of RQ3 demonstrate that privacy placement reflects the underlying philosophy of consensus mechanisms. When strong adversarial resistance and minimal internal trust are needed, BFT-class systems build privacy into the consensus level. Externalised privacy mechanisms, on the other hand, are based on a philosophy of modularity and controlled disclosure, with privacy complementing rather than reshaping consensus logic [2], [3]. In summary, modern blockchain design increasingly recognises privacy as a fundamental architectural concern, whether enforced internally or externally. This evolution shows a shift from achieving agreement through transparency to achieving agreement through carefully managed exposure, which aligns consensus mechanisms with modern privacy expectations.

IV. Conclusion and Future Research Directions

This systematic literature review examined blockchain consensus mechanisms from a privacy-focused perspective, with particular attention to how consensus design influences privacy risks and mitigation strategies. By analysing 72 peer-reviewed journal articles, the review moves beyond performance- or security-oriented surveys and provides a consensus-centric understanding of privacy preservation in blockchain systems.

The findings show that Byzantine Fault Tolerant (BFT)-based consensus mechanisms are the most frequently adopted in privacy-preserving blockchain applications, especially in permissioned and consortium environments. However, the review also demonstrates that privacy challenges remain common across studies. Issues such as identity exposure, communication pattern leakage, and metadata inference are repeatedly linked to consensus-level properties, including validator roles, message exchange patterns, and quorum structures. These results highlight that privacy risks are not solely caused by data handling at the application layer but are deeply influenced by how consensus mechanisms operate.

Another important insight is that privacy-preserving techniques are predominantly implemented as external or overlay solutions rather than being integrated directly into consensus mechanisms. While such approaches improve data confidentiality, they do not fully address privacy risks that originate from consensus operations themselves. This separation reveals a structural limitation in current blockchain designs, where privacy is often treated as an additional feature rather than a fundamental design requirement of the consensus layer.

The main contribution of this review is a taxonomy-driven synthesis that explicitly connects consensus mechanism classes, reported privacy limitations, and levels of privacy integration. By organising fragmented findings into a coherent framework,

this work provides a clear reference for analysing consensus mechanisms through a privacy lens and supports more informed decision-making in both research and practice.

Building on these insights, future research should focus on designing consensus mechanisms with privacy embedded at the protocol level, rather than relying on external protections. Comparative studies using consistent privacy evaluation criteria are needed to better understand trade-offs across consensus classes. In addition, underexplored consensus designs, such as leader-based and hybrid mechanisms, warrant further investigation to assess their privacy potential when appropriately adapted. Addressing these directions can support the development of blockchain systems where privacy is considered a core consensus property rather than an afterthought.

REFERENCES

[1] C. E. Ngubo and M. Dohler, "Wi-Fi-Dependent Consensus Mechanism for Constrained Devices Using Blockchain Technology," IEEE Access, vol. 8, pp. 143595–143606, 2020, doi: 10.1109/ACCESS.2020.3014287.

[2] S. Aggarwal and N. Kumar, "Cryptographic consensus mechanisms," 2021, pp. 211–226. doi: 10.1016/bs.adcom.2020.08.011.

[3] S. Barj, A. Ouaddah, and A. Mezrioui, "A Survey and a State-of-the-Art Related to Consensus Mechanisms in Blockchain Technology," 2023, pp. 208–217. doi: 10.1007/978-3-031-29857-8_21.

[4] H. S. Jennath and S. Asharaf, "Survey on Blockchain Consensus Strategies," 2020, pp. 637–654. doi: 10.1007/978-981-15-1420-3_68.

[5] M. Conti, K. E. Sandeep, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys and Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018, doi: 10.1109/COMST.2018.2842460.

[6] A. Imteaj, M. Hadi Amini, and P. M. Pardalos, "Toward Smart Contract and Consensus Mechanisms of Blockchain," 2021, pp. 15–28. doi: 10.1007/978-3-030-75025-1_2.

[7] M. Abbasi, J. Prieto, M. Plaza-Hernández, and J. M. Corchado, "A Novel Aging-Based Proof of Stake Consensus Mechanism," 2023, pp. 49–61. doi: 10.1007/978-3-031-36957-5_5.

[8] H. Qushtom, J. Mišić, V. B. Mišić, and X. Chang, "A Two-Stage PBFT Architecture With Trust and Reward Incentive Mechanism," IEEE Internet Things J., vol. 10, no. 13, pp. 11440–11452, Jul. 2023, doi: 10.1109/JIOT.2023.3243189.

[9] C. Su and X. Li, "A Review of Blockchain Consensus," in 2021 International Conference on Intelligent Computing, Automation and Applications (ICAA), IEEE, Jun. 2021, pp. 598–604. doi: 10.1109/ICAA53760.2021.00110.

[10] M. Tan, J. Yang, L. Ding, X. Li, and S. Xia, "Review of consensus mechanism of blockchain," Jisuanji Gongcheng/Computer Engineering, vol. 46, no. 12, pp. 1–11, 2020.

[11] Y.-Z. Liu, J.-W. Liu, Z.-Y. Zhang, T.-G. Xu, and H. Yu, "Overview on blockchain consensus mechanisms; [区块链共识机制研究综述]," Journal of Cryptologic Research, vol. 6, no. 4, pp. 395 - 432, 2019, doi: 10.13868/j.cnki.jcr.000311.

[12] G. Zyskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in 2015 IEEE Security and Privacy Workshops, IEEE, May 2015, pp. 180–184. doi: 10.1109/SPW.2015.27.

[13] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLoS One, vol. 11, no. 10, p. e0163477, Oct. 2016, doi: 10.1371/journal.pone.0163477.

[14] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," Jan. 2009. doi: 10.1016/j.infsof.2008.09.009.

[15] J. Zheng and J. Li, "MGRS-PBFT: An Optimized Consensus Algorithm Based on Multi-Group Ring Signatures for Blockchain Privacy Protection," IEEE Transactions on Network and Service Management, vol. 22, no. 5, pp. 4856–4870, 2025, doi: 10.1109/TNSM.2025.3580403.

[16] W. Li, C. Meese, M. Nejad, and H. Guo, "ZK-BFT: A Zero-knowledge and Byzantine Fault Tolerant Consensus for Permissioned Blockchain Networks," in Proceedings of the 2023 6th International Conference on Blockchain Technology and Applications, New York, NY, USA: ACM, Dec. 2023, pp. 70–77. doi: 10.1145/3651655.3651663.

[17] X. Wu, H. Ling, H. Liu, and F. Yu, "A privacy-preserving and efficient byzantine consensus through multi-signature with ring," Peer. Peer. Netw. Appl., vol. 15, no. 3, pp. 1669–1684, May 2022, doi: 10.1007/s12083-022-01317-4.

[18] T. Luo and Y. Chen, "Research on the Algorithm of Blockchain Technology in Enhancing the Transparency of Network Services and the Protection of User Privacy," in 2024 First International Conference on Software, Systems and Information Technology (SSITCON), IEEE, Oct. 2024, pp. 1–7. doi: 10.1109/SSITCON62437.2024.10795919.

[19] S. N. Paing et al., "Counterfactual Quantum Byzantine Consensus for Human-Centric Metaverse," IEEE Journal on Selected Areas in Communications, vol. 42, no. 4, pp. 905–918, Apr. 2024, doi: 10.1109/JSAC.2023.3345420.

[20] M. Labib, H. Aslan, and T. Arafa, "Scaling Byzantine Consensus: A Sharded and Pipelined Approach for Permissioned Blockchains," in 2025 Intelligent Methods, Systems, and Applications (IMSA), IEEE, Jul. 2025, pp. 169–175. doi: 10.1109/IMSA65733.2025.11167524.

[21] C.-X. Zhou, Q.-S. Hua, and H. Jin, "HotDAG: Hybrid Consensus via Sharding in the Permissionless Model," 2020, pp. 807–821. doi: 10.1007/978-3-030-59016-1_66.

[22] A. Aldoubaee, N. H. Hassan, and F. A. Rahim, "A Systematic Review on Blockchain Scalability," International Journal of Advanced Computer Science and Applications, vol. 14, no. 9, pp. 774–784, 2023, doi: 10.14569/IJACSA.2023.0140981.

[23] T. H. Pun, Y. J. He, and C. D. Shum, "Strengthening Fault Tolerance of Private/Consortium Blockchain with Trusted Execution Environment," in 2024 International Conference on Sustainable Technology and Engineering (i-COSTE), IEEE, Dec. 2024, pp. 1–6. doi: 10.1109/i-COSTE63786.2024.11024869.

[24] Y. Chen, P. Liu, and W. Zhang, "Raft consensus algorithm based on credit model in consortium blockchain," Wuhan University Journal of Natural Sciences, vol. 2, no. 8, 2020.

[25] V. Arora, T. Mittal, D. Agrawal, A. El Abbadi, and X. Xue, "Leader or majority: Why have one when you can have both? Improving read scalability in raft-like consensus protocols," in In 9th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 17), 2017.

[26] Y. Sun, B. Guo, D. Jia, and S. He, "Improving Raft Consensus Algorithm with Relay and Lease Mechanism," 2025, pp. 84–94. doi: 10.1007/978-3-031-77095-1_6.

[27] Y. Du, H. Yi, Y. Zhang, and X. Hu, "An efficient consensus algorithm based on proxy signature of SM2," in Proceedings of SPIE - The International Society for Optical Engineering, 2024. doi: 10.1117/12.3026135.

[28] J.-F. Paris and D. D. E. Long, "Reducing the Energy Footprint of a Distributed Consensus Algorithm," in 2015 11th European Dependable Computing Conference (EDCC), IEEE, Sep. 2015, pp. 198–204. doi: 10.1109/EDCC.2015.25.

[29] M. Köse Ulukök, I. Sariyildiz, and V. Evrim, "Hybrid Raft-PoW Blockchain Consensus Algorithm," IEEE Access, vol. 13, pp. 72067–72076, 2025, doi: 10.1109/ACCESS.2025.3562725.

[30] Z. Xu, Y. Lei, H. Han, X. Dong, X. Chen, and Z. Zhu, "MCRaft: synergistic collaboration of multi leaders for IoT cluster stability optimization," in 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), IEEE, Dec. 2022, pp. 1702–1709. doi: 10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00257.

[31] X. Liu, Z. Huang, and Q. Wang, "An Optimized Snapshot Raft Algorithm for Log Compression," in 2023 2nd International Conference on Artificial

Intelligence and Blockchain Technology (AIBT), IEEE, Jun. 2023, pp. 6–10. doi: 10.1109/AIBT57480.2023.00008.

[32] X. Xu, L. Hou, Y. Li, and Y. Geng, "Weighted RAFT: An Improved Blockchain Consensus Mechanism for Internet of Things Application," in 2021 7th International Conference on Computer and Communications (ICCC), IEEE, Dec. 2021, pp. 1520–1525. doi: 10.1109/ICCC54389.2021.9674683.

[33] S. Pang et al., "Reputation-based federated learning and blockchain for trustworthy service recommendations in edge computing," Cluster Comput., vol. 28, no. 11, Oct. 2025, doi: 10.1007/s10586-025-05314-z.

[34] Q. Wang, Z. Wu, and Y. Lu, "A Multi-Layer Secure Sharing Framework for Aviation Big Data Based on Blockchain," Future Internet, vol. 17, no. 8, Aug. 2025, doi: 10.3390/fi17080361.

[35] L. Vishwakarma, S. A. Saji, and D. Das, "CuraFrame: a patient-centric secure and privacy preserving medical framework with zero-leak using blockchain," Peer. Peer. Netw. Appl., vol. 18, no. 4, Jul. 2025, doi: 10.1007/s12083-025-02061-1.

[36] B. Wang, Z. Tian, X. Liu, Y. Xia, W. She, and W. Liu, "A multi-center federated learning mechanism based on consortium blockchain for data secure sharing," Knowl. Based. Syst., vol. 310, Feb. 2025, doi: 10.1016/j.knosys.2025.112962.

[37] J. Hu, "Research on the Transformation and Development of University Journal Editors Based on Blockchain Technology," International Journal of e-Collaboration, vol. 21, no. 1, pp. 1–21, Nov. 2025, doi: 10.4018/ijec.394330.

[38] W. Jiang and Z. Guo, "An Anonymous Authentication Scheme for Internet of Vehicles Based on TRUG-PBFT Main-Secondary Chains and Zero-Knowledge Proof," IEEE Internet Things J., vol. 12, no. 7, pp. 7763–7777, 2025, doi: 10.1109/JIOT.2024.3429342.

[39] S. Shen, T. Wang, G. Zhang, F. Chen, D. Xie, and C. Zhao, "A Blockchain-Based Fine-Grained Reputation-Enhanced Consensus Mechanism for Secure Health Data Trading," IEEE Trans. Comput. Soc. Syst., 2025, doi: 10.1109/TCSS.2025.3605234.

[40] G. Li, H. Wu, J. Wu, and Z. Li, "Efficient and secure privacy protection scheme and consensus mechanism in MEC enabled e-commerce consortium blockchain," Journal of Cloud Computing, vol. 13, no. 1, Dec. 2024, doi: 10.1186/s13677-024-00652-6.

[41] I. Ahmed, M. Turki, M. Baklouti, B. Dammak, and A. Alshahrani, "Towards an Optimized Blockchain-Based Secure Medical Prescription-Management System," Future Internet, vol. 16, no. 7, Jul. 2024, doi: 10.3390/fi16070243.

[42] Y. Zhao, Y. Qu, Y. Xiang, F. Chen, and L. Gao, "Context-Aware Consensus Algorithm for Blockchain-Empowered Federated Learning," IEEE Transactions on Cloud Computing, vol. 12, no. 2, pp. 491–503, Apr. 2024, doi: 10.1109/TCC.2024.3372814.

[43] X. Zhou et al., "Federated distillation and blockchain empowered secure knowledge sharing for Internet of medical Things," Inf. Sci. (N Y)., vol. 662, Mar. 2024, doi: 10.1016/j.ins.2024.120217.

[44] N. Haliza Abdul Wahab, Z. Dayong, J. Nur Fadila, K. Yinn Wong, T. Malaysia, and J. Bahru, "Advances in Consortium Chain Scalability: A Review of the Practical Byzantine Fault Tolerance Consensus Algorithm." [Online]. Available: www.ijacsa.thesai.org

[45] J. A. Abdella, Z. Tari, N. Sohrabi, and R. Mahmud, "MuLCOff: A Multi-Layer Consensus and Off-Chain Computation for Efficient and Privacy-Aware Blockchain-Based Peer-to-Peer Energy Trading," IEEE Netw., vol. 38, no. 5, pp. 264–272, 2024, doi: 10.1109/MNET.2024.3355987.

[46] D. Zhai et al., "EPDB: An Efficient and Privacy-Preserving Electric Charging Scheme in Internet of Robotic Things," IEEE Internet Things J., vol. 11, no. 20, pp. 32464–32477, 2024, doi: 10.1109/JIOT.2024.3426536.

[47] D. Luo, Y. Zhang, G. Sun, H. Yu, and D. Niyato, "An Efficient Consensus Algorithm for Blockchain-Based Cross-Domain Authentication in Bandwidth-Constrained Wide-Area IoT Networks," IEEE Internet Things J., vol. 11, no. 19, pp. 31917–31931, 2024, doi: 10.1109/JIOT.2024.3420719.

[48] J. Zheng and Y. Zhang, "RSHS: A Blockchain Consensus Mechanism for Edge Computing-Supported Agri-IoT Systems," IEEE Transactions on Network and Service Management, vol. 21, no. 4, pp. 4104–4118, 2024, doi: 10.1109/TNSM.2024.3415610.

[49] W. Feng and H. Cao, "Blockchain electronic evidence sharing based on improved ciphertext policy attribute encryption," Egyptian Informatics Journal, vol. 32, Dec. 2025, doi: 10.1016/j.eij.2025.100817.

[50] M. K. Singh, S. K. Pippal, and V. Sharma, "Lightweight blockchain mechanism for secure data transmission in healthcare system," Biomed. Signal Process. Control, vol. 102, Apr. 2025, doi: 10.1016/j.bspc.2024.107411.

[51] I. Ahmed, M. Turki, M. Baklouti, B. Dammak, and A. Alshahrani, "Towards an Optimized Blockchain-Based Secure Medical Prescription-Management System," Future Internet, vol. 16, no. 7, Jul. 2024, doi: 10.3390/fi16070243.

[52] X. Li, W. Wu, and T. Chen, "Blockchain-Driven Privacy-Preserving Contact-Tracing Framework in Pandemics," IEEE Trans. Comput. Soc. Syst., vol. 11, no. 3, pp. 4279–4289, Jun. 2024, doi: 10.1109/TCSS.2024.3351191.

[53] A. Liu, Q. Zhang, S. Xu, H. Feng, X. B. Chen, and W. Liu, "QBIoT: A Quantum Blockchain Framework for IoT with an Improved Proof-of-Authority Consensus Algorithm and a Public-Key Quantum Signature," Computers, Materials and Continua, vol. 80, no. 1, pp. 1727–1751, 2024, doi: 10.32604/cmc.2024.051233.

[54] M. A. Mohammed and H. B. Abdul Wahab, "Enhancing IoT Data Security with Lightweight Blockchain and Okamoto Uchiyama Homomorphic Encryption," CMES - Computer Modeling in Engineering and Sciences, vol. 138, no. 2, pp. 1731–1748, 2024, doi: 10.32604/cmes.2023.030528.

[55] S. Subrahmanyam, R. Arunachalam, S. Thouti, S. N. V. Jyotsna Devi Kosuru, J. Rajalakshmi, and P. Palanisamy, "Blockchain access control with consensus algorithm considering optimal members and president election process for secured data sharing on software Defined wireless body area networks using data encryption," Expert Syst. Appl., vol. 297, Feb. 2026, doi: 10.1016/j.eswa.2025.129430.

[56] P. Joshi and P. Mahajan, "Secure and interoperable EHR management via hyperledger fabric: The Mrblock framework," Peer. Peer. Netw. Appl., vol. 18, no. 3, Jun. 2025, doi: 10.1007/s12083-025-01954-5.

[57] M. Kashif and K. Kalkan, "Differential privacy preserving based framework using blockchain for internet-of-things," Peer. Peer. Netw. Appl., vol. 18, no. 1, pp. 1–23, Feb. 2025, doi: 10.1007/s12083-024-01858-w.

[58] W. Zhang, J. Dong, G. Han, and Y. Zhao, "BDAFL: A Blockchain-Integrated Decentralized Asynchronous Federated Learning Algorithm in Industrial Internet," IEEE Transactions on Network and Service Management, vol. 22, no. 5, pp. 4137–4154, 2025, doi: 10.1109/TNSM.2025.3576599.

[59] S. Qiao et al., "LBFL: A Lightweight Blockchain-Based Federated Learning Framework With Proof-of-Contribution Committee Consensus," IEEE Trans. Big Data, vol. 11, no. 4, pp. 1745–1759, 2025, doi: 10.1109/TBDATA.2024.3481952.

[60] L. Tian et al., "Enhancing Security in Parallel Federated Learning with Sharded Blockchain for Internet of Vehicles," IEEE Trans. Veh. Technol., 2025, doi: 10.1109/TVT.2025.3593493.

[61] C. Ying et al., "BIT-FL: Blockchain-Enabled Incentivized and Secure Federated Learning Framework," IEEE Trans. Mob. Comput., vol. 24, no. 2, pp. 1212–1229, 2025, doi: 10.1109/TMC.2024.3477616.

[62] X. Zhou et al., "Federated distillation and blockchain empowered secure knowledge sharing for Internet of medical Things," Inf. Sci. (N Y)., vol. 662, Mar. 2024, doi: 10.1016/j.ins.2024.120217.

[63] N. Yang, C. Tang, Z. Xiong, and D. He, "RCME: A Reputation Incentive Committee Consensus-Based for Matchmaking Encryption in IoT Healthcare," IEEE Trans. Serv. Comput., vol. 17, no. 5, pp. 2790–2806, 2024, doi: 10.1109/TSC.2024.3387691.

[64] W. Li, Q. Zhang, S. Deng, B. Zhou, B. Wang, and J. Cao, "Q-Learning Improved Lightweight Consensus Algorithm for Blockchain-Structured Internet of Things," IEEE Internet Things J., vol. 11, no. 2, pp. 2855–2869, Jan. 2024, doi: 10.1109/JIOT.2023.3294265.

[65] K. Fan et al., "SC-Chain: An Efficient Blockchain Framework for Smart City," IEEE Internet Things J., vol. 11, no. 5, pp. 7863–7877, Mar. 2024, doi: 10.1109/JIOT.2023.3317451.

[66] C. V. N. U. Bharathi Murthy and M. Lawanya Shri, "Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned

Blockchain for Telemedicine," IEEE Access, vol. 12, pp. 106645–106657, 2024, doi: 10.1109/ACCESS.2024.3436075.

[67] A. Aljuhani et al., "A Deep-Learning-Integrated Blockchain Framework for Securing Industrial IoT," IEEE Internet Things J., vol. 11, no. 5, pp. 7817–7827, Mar. 2024, doi: 10.1109/JIOT.2023.3316669.

[68] M. Rifat Hossain, F. A. Nirob, A. Islam, T. M. Rakin, and M. Al-Amin, "A Comprehensive Analysis of Blockchain Technology and Consensus Protocols Across Multilayered Framework," IEEE Access, vol. 12, pp. 63087–63129, 2024, doi: 10.1109/ACCESS.2024.3395536.

[69] L. Vishwakarma and D. Das, "BLISS: blockchain-based integrated security system for internet of things (IoT) applications," Int. J. Inf. Secur., vol. 23, no. 3, pp. 1649–1665, Jun. 2024, doi: 10.1007/s10207-023-00808-6.

[70] S. Wang, L. Shi, H. Shi, Y. Zhang, Q. Hu, and X. Cheng, "Proof of User Similarity: The Spatial Measurer of Blockchain," IEEE Trans. Serv. Comput., vol. 17, no. 3, pp. 1114–1125, May 2024, doi: 10.1109/TSC.2023.3347716.

[71] G. K. Mahato, A. Banerjee, S. K. Chakraborty, and X. Z. Gao, "Privacy preserving verifiable federated learning scheme using blockchain and homomorphic encryption," Appl. Soft Comput., vol. 167, Dec. 2024, doi: 10.1016/j.asoc.2024.112405.

[72] Y. Li, J. Zhang, J. Zhu, and W. Li, "Blockfd: blockchain-based federated distillation against poisoning attacks," Neural Comput. Appl., vol. 36, no. 21, pp. 12901–12916, Jul. 2024, doi: 10.1007/s00521-024-09715-w.

[73] Q. Zhang, X. Xue, and J. Yang, "Blockchain-Enabled Trustworthy Healthcare Data Sharing Mechanism for Reliable 6G-IoT Networks," IEEE Internet Things J., 2025, doi: 10.1109/JIOT.2025.3564782.

[74] H. Xie, J. Zheng, T. He, S. Wei, and C. Hu, "A blockchain-based ubiquitous entity authentication and management scheme with homomorphic encryption for FANET," Peer. Peer. Netw. Appl., vol. 17, no. 2, pp. 569–584, Mar. 2024, doi: 10.1007/s12083-024-01624-y.

[75] A. Ferrer-Rojas, B. T. Maharaj, and M. C. Hlophe, "Blockchain-Enhanced Attribute-Based Encryption Architecture With Feasibility Analysis," IEEE Access, vol. 13, pp. 57629–57638, 2025, doi: 10.1109/ACCESS.2025.3554643.

[76] S. K. Singh, M. Kumar, S. Tanwar, and J. H. Park, "GRU-based digital twin framework for data allocation and storage in IoT-enabled smart home networks," Future Generation Computer Systems, vol. 153, pp. 391–402, Apr. 2024, doi: 10.1016/j.future.2023.12.009.

[77] S. Han, Z. Wang, D. Shen, and C. Wang, "A Parallel Multi-Party Privacy-Preserving Record Linkage Method Based on a Consortium Blockchain," Mathematics, vol. 12, no. 12, Jun. 2024, doi: 10.3390/math12121854.

[78] L. Tian, F. Lin, J. Gan, R. Jia, Z. Zheng, and M. Li, "PEFL: Privacy-Preserved and Efficient Federated Learning With Blockchain," IEEE Internet Things J., vol. 12, no. 3, pp. 3305–3317, 2025, doi: 10.1109/JIOT.2024.3479328.

[79] F. Ahmed, T. Zhou, H. Bilal, F. Ul Islam, R. Ullah, and A. V. Vasilakos, "Enhancing Healthcare Data Integrity and Access Control Using Blockchain and Industry 5.0," IEEE Internet Things J., vol. 12, no. 20, pp. 43630–43643, 2025, doi: 10.1109/JIOT.2025.3598320.

[80] Y. Liu, X. Xing, J. Liu, Q. Wu, Z. Guan, and D. Li, "MetaL: A Fully Decentralized User-Driven Access Control Scheme for Metaverse Utilizing MC-ABE and Sharding Blockchain," IEEE Netw., 2025, doi: 10.1109/MNET.2025.3613572.

[81] H. Dou, X. Wang, M. A. Jan, H. Sang, and Y. Chen, "Blockchain-Based Trustworthy Verifiable Federated Learning for 6G Internet of Vehicles," IEEE Internet Things J., 2025, doi: 10.1109/JIOT.2025.3581415.

[82] J. Li, D. Han, S. Shi, X. Xin, K. C. Li, and C. C. Chang, "An Active Client Selection Scheme Based on Blockchain for Federated Learning in Shipping," IEEE Transactions on Intelligent Transportation Systems, vol. 26, no. 11, pp. 20669–20684, 2025, doi: 10.1109/TITS.2025.3591530.

[83] H. Kumar A, P. Venkatram C, N. Saran, D. Daniel, and P. Joe I. R, "Decentralized digital health ecosystems: a unified architecture for AI-enhanced medical record management," Front. Digit. Health, vol. 7, 2025, doi: 10.3389/fdgth.2025.1685628.

[84] S. Datta, S. Namasudra, M. R. Reddy, A. K. Sangaiah, and S. Kumari, "A Lightweight Few-Shot Learning-Based Traffic Classification System for Secure Internet of Vehicles," IEEE Transactions on Intelligent Transportation Systems, 2025, doi: 10.1109/TITS.2025.3596139.

[85] Q. Gong, J. Zhang, Y. Wang, X. Yan, X. Yuan, and L. Dong, "Blockchain and Deep Reinforcement Learning Empowered Data Storage in Internet of Things," IEEE Internet Things J., vol. 12, no. 22, pp. 47623–47646, 2025, doi: 10.1109/JIOT.2025.3602601.

[86] H. Gao, M. S. Obaidat, H. Huang, Y. Xing, F. Xiao, and Q. Li, "STORChain: A Clustered-MPT-based Blockchain for Data Service and Efficient Storage in Healthcare," IEEE Trans. Serv. Comput., 2025, doi: 10.1109/TSC.2025.3614883.

[87] S. R. Mallick, V. Goswami, R. K. Lenka, R. K. Barik, R. Soorat, and N. K. Ray, "LIVER: A Next-Generation Secure and Lightweight Blockchain-IPFS Edge Computing Model for Healthcare with Queueing Techniques," International Journal of Networked and Distributed Computing, vol. 13, no. 2, Dec. 2025, doi: 10.1007/s44227-025-00070-3.

[88] L. Zhang, Y. Yang, J. Luo, W. Wang, and J. Gu, "DBIA-DA: dual-blockchain and ISCP-assisted data aggregation for fog-enabled smart grid," EURASIP J. Wirel. Commun. Netw., vol. 2025, no. 1, Dec. 2025, doi: 10.1186/s13638-025-02516-2.

[89] I. O. Asante and L. Wu, "Enhancing cybersecurity through hybrid blockchain-enabled intrusion detection systems: A machine learning approach," Peer. Peer. Netw. Appl., vol. 18, no. 5, Sep. 2025, doi: 10.1007/s12083-025-01907-y.

[90] J. Zhang, S. Li, and H. Pei, "Blockchain-enabled one-stop efficient data retrieval privacy protection mechanism industry 4.0," Journal of Supercomputing, vol. 81, no. 13, Aug. 2025, doi: 10.1007/s11227-025-07746-1.

[91] M. I. A. Mohamad Zainal 'Asri, N. F. Mohd Shari, and A. Malip, "Enhanced security of data dissemination in blockchain-based peer-to-peer smart energy trading network," Computers and Electrical Engineering, vol. 126, Aug. 2025, doi: 10.1016/j.compeleceng.2025.110523.

[92] Y. Liu et al., "EUAV: An enhanced blockchain-based two-factor anonymous authentication key agreement protocol for UAV networks," Computer Networks, vol. 270, Oct. 2025, doi: 10.1016/j.comnet.2025.111492.

[93] A. S. Vindhya, V. S. Kumari, L. Karthikeyan, D. Vinoth, and M. Agoramoorthy, "A novel blockchain-integrated IoT framework for secure and efficient vehicle-to-infrastructure communication in smart transportation," Peer. Peer. Netw. Appl., vol. 18, no. 6, Oct. 2025, doi: 10.1007/s12083-025-02119-0.

[94] H. Nandanwar and R. Katarya, "A hybrid Blockchain-Based framework for securing intrusion detection systems in internet of things," Cluster Comput., vol. 28, no. 7, Sep. 2025, doi: 10.1007/s10586-025-05135-0.

[95] G. Shankar, P. Singh, N. K. Dewangan, and P. Chandrakar, "DEMRISEC: security enhancement of patient data in decentralized medical records with IPFS," Multimed. Tools Appl., vol. 84, no. 13, pp. 12123–12140, Apr. 2025, doi: 10.1007/s11042-024-19444-w.

[96] Z. Chen, J. Yi, Y. Zhou, and W. Luo, "Reinforcement learning-enabled swarm intelligence method for computation task offloading in Internet-of-Things blockchain," Digital Communications and Networks, vol. 11, no. 3, pp. 912–924, Jun. 2025, doi: 10.1016/j.dcan.2024.09.001.

[97] H. Wang, H. Gao, T. Ma, C. Li, and T. Jing, "A hierarchical blockchain-enabled distributed federated learning system with model contribution based rewarding," Digital Communications and Networks, vol. 11, no. 1, pp. 35–42, Feb. 2025, doi: 10.1016/j.dcan.2024.07.002.

[98] K. Zhu, M. Lu, H. Li, N. N. Xiong, and W. He, "CMBA-FL: Communication-mitigated and blockchain-assisted federated learning for traffic flow predictions," Digital Communications and Networks, vol. 11, no. 3, pp. 724–733, Jun. 2025, doi: 10.1016/j.dcan.2025.04.011.

[99] F. Xu et al., "FDSS: Flight data sharing scheme based on blockchain with dynamic, secure and efficient consensus algorithm," Computer Networks, vol. 265, Jun. 2025, doi: 10.1016/j.comnet.2025.111275.

[100] G. Pranitha and P. V. Lakshmi, "A novel approach for ensuring drug safety in the pharmaceutical supply Chain by using IoT devices and blockchain technology," Peer. Peer. Netw. Appl., vol. 18, no. 4, Jul. 2025, doi: 10.1007/s12083-025-02024-6.

[101] R. Zhang, Y. Li, and L. Fang, "PBTMS: A Blockchain-Based Privacy-Preserving System for Reliable and Efficient E-Commerce," Electronics (Switzerland), vol. 14, no. 6, Mar. 2025, doi: 10.3390/electronics14061177.

[102] H. Assiri, "Piranha Foraging Optimization Algorithm with Deep Learning Enabled Fault Detection in Blockchain-Assisted Sustainable IoT Environment," Sustainability (Switzerland), vol. 17, no. 4, Feb. 2025, doi: 10.3390/su17041362.

[103] H. R. Ranganatha and A. Syed Mustafa, "Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d Quasi-Recurrent Neural network and blockchain technologies," Expert Syst. Appl., vol. 260, Jan. 2025, doi: 10.1016/j.eswa.2024.125179.

[104] J. Tu, D. Jia, and J. Wang, "Byzantine Fault Tolerant Consensus Algorithm Based on Traceable Ring Signature," Computer Science, vol. 50, no. 6, 2023, doi: 10.11896/jsjkx.220300100.

[105] X. Li, Z. Zheng, and P. Chen, "ACT: Anonymous Consensus Based on Tor," 2021, pp. 460–471. doi: 10.1007/978-981-16-7502-7_42.

[106] L. Sun, D. Ding, and W. An, "Average Consensus Control of Multi‐Agent Systems With Hybrid Privacy‐Preserving Schemes," International Journal of Robust and Nonlinear Control, Nov. 2025, doi: 10.1002/rnc.70284.

[107] W. Zou, C. Li, J. Ge, and B. Luo, "Privacy protection and data accountability of collaborative business processes based on hybrid blockchain," Jisuanji Jicheng Zhizao Xitong/Computer Integrated Manufacturing Systems, CIMS, vol. 30, no. 8, pp. 2897–2912, 2024, doi: 10.13196/j.cims.2023.BPM22.

[108] S. Chen, H. Gao, X. Xu, H. Lei, and Z. Song, "SDTPBFT: Improved Practical Byzantine Fault Tolerance Consensus Algorithm Based on Scored and Dynamic Tenure," 2025, pp. 52–65. doi: 10.1007/978-981-96-4245-8_4.

[109] D. Basin, F. Hublet, S. Krstić, and H. Nguyễn, "Mechanizing Privacy by Design," in Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA: ACM, Nov. 2025, pp. 2–5. doi: 10.1145/3719027.3748271.

[110] M. T. Baldassarre, V. S. Barletta, D. Caivano, G. Dimauro, and A. Piccinno, "A Tool for Improving Privacy in Software Development," in 42nd International Conference on Information Systems, ICIS 2021 TREOs: "Building Sustainability and Resilience with IS: A Call for Action," 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85192375737&partnerID=40&md5=b89260bfbc54e57529c0aabb74d4c314

[111] P. J. Wisniewski and X. Page, "Privacy Theories and Frameworks," in Modern Socio-Technical Perspectives on Privacy, Cham: Springer International Publishing, 2022, pp. 15–41. doi: 10.1007/978-3-030-82786-1_2.

[112] K. Xue, J. Li, R. Xue, Y. Xue, and J. Zhao, "RobustPPFL: A Secure and Robust Privacy-Preserving Federated Learning Framework Against Poisoning Attacks," IEEE Trans. Netw. Sci. Eng., vol. 13, pp. 3351–3368, 2026, doi: 10.1109/TNSE.2025.3632902.

[113] D. Marikyan, S. Papagiannidis, R. Ranjan, and O. Rana, "General data protection regulation," in Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing Companion, New York, NY, USA: ACM, Dec. 2021, pp. 1–6. doi: 10.1145/3492323.3495620.

[114] P. Wang, Q. Xu, and H. Zhang, "DQN-Raft+: A Deep Reinforcement Learning-Optimized Lightweight Consensus Algorithm for Secure Edge Storage in IoT Environments," Informatica (Slovenia), vol. 49, no. 33, pp. 127–148, Jan. 2025, doi: 10.31449/inf.v49i33.8909.

[115] J. Tian, Z. Jiang, and Y. Jin, "HCCAS: A hierarchical consensus-based certificateless aggregate signcryption scheme for drone networks," Journal of Information Security and Applications, vol. 94, Nov. 2025, doi: 10.1016/j.jisa.2025.104260.