Blockchain Consensus Mechanisms Contributing to Improved Trust in Knowledge Sharing: A Systematic Review

Mohammad Fairus Bin Zulkifli, Rabiah Abdul Kadir, Mohamad Nazir Ahmad
Institute of Visual Informatics, Universiti Kebangsaan Malaysia, 43600 Bangi, Malaysia

Abstract*—Growing reliance on digital knowledge sharing across academic, corporate, and public sectors has raised serious concerns about data integrity, trust, and security. Blockchain consensus mechanisms offer a promising path forward through decentralized, transparent, and tamper-proof frameworks. This systematic review examines how these mechanisms enhance trust in knowledge sharing platforms, focusing on four directions: how these mechanisms are applied within knowledge sharing contexts, the challenges they introduce for knowledge sharing deployment, and the advantages they provide to trust-based knowledge sharing ecosystems. Following PRISMA 2020 guidelines, three databases Scopus, IEEE Xplore, and Web of Science were searched, and peer-reviewed studies published between 2020 and 2025 were selected for analysis. In terms of knowledge sharing applications, blockchain consensus mechanisms build trust through multiple co-occurring pathways, including distributed verification, transparency, cryptographic security, immutability, incentive alignment, and smart contract automation. Algorithms such as Proof of Work, Proof of Stake, Delegated Proof of Stake, and Byzantine Fault Tolerance variants are widely adopted, each offering different trade-offs between security, efficiency, and scalability. In terms of challenges, scalability, energy consumption, and integration complexity with existing systems remain the most significant barriers to adoption. In terms of advantages, blockchain consistently delivers stronger data security, greater transparency, and reduced dependence on centralized authorities across knowledge sharing contexts. This review concludes that blockchain consensus mechanisms offer layered and compounding trust benefits, yet technical and organizational barriers continue to limit widespread deployment. Future research should focus on energy-efficient protocols, scalable architectures, and real-world effectiveness studies.

***Keywords*—Blockchain technology; consensus mechanisms; knowledge sharing; distributed ledger technology; trust systems**

I. Introduction

A. Background

The rapid digitalization of knowledge sharing across academic, corporate, and public sectors has exposed critical vulnerabilities in centralized knowledge-sharing platforms. These include susceptibility to data breaches, manipulation, and lack of verifiable provenance [1], [2]. Centralized architectures concentrate control with platform operators, creating single points of failure that undermine the integrity of collaborative information ecosystems [3]. As digital knowledge communities grow in complexity and cross-jurisdictional scope, issues such as censorship, unilateral data modification, and opaque attribution have become increasingly consequential for research, industry, and public institutions.

Blockchain technology addresses these challenges through decentralized, cryptographically secured distributed ledgers that allow multiple parties to maintain tamper-evident, verifiable records without relying on central authorities [4], [5]. At the core of any blockchain system are consensus mechanisms protocols through which distributed nodes reach agreement on transaction validity and ledger state, even in the presence of unreliable or malicious participants [6]. These protocols resolve the Byzantine Generals Problem by incentivizing honest behavior and making fraudulent activity computationally or economically impractical [7], [8].

Contemporary consensus mechanisms including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) employ distinct strategies for validator selection, block creation, and network coordination [9]. Each presents different trade-offs across security, throughput, energy efficiency, decentralization, and governance [10], [11]. Selecting the appropriate mechanism is therefore a fundamental design decision that directly shapes the trust properties of any blockchain-based knowledge sharing platform.

Applying blockchain consensus mechanisms to knowledge sharing represents an emerging research domain with broad implications for how digital ecosystems manage provenance, attribution, access control, and contribution incentives [12]. Blockchain-based platforms address trust deficits through cryptographically secured storage, transparent verification, decentralized governance, and incentive systems that reward quality contributions [13]. Smart contracts further enable automated enforcement of knowledge sharing protocols and intellectual property rights without the need for trusted intermediaries [14].

B. Research Gap

Despite growing interest in blockchain for knowledge sharing, research on the specific role of consensus mechanisms in enhancing trust within knowledge sharing platforms remains fragmented [15]. Several gaps are evident. First, no comprehensive synthesis exists of how different consensus mechanisms address trust challenges in knowledge sharing contexts [16]. Second, platform designers lack evidence-based frameworks for evaluating trade-offs between security, scalability, energy efficiency, and governance when selecting mechanisms for knowledge sharing applications [17]. Third, empirical evidence

from real-world deployments is sparse, with most studies focusing on conceptual frameworks or prototypes rather than longitudinal evaluations [18]. Fourth, implementation challenges and practical limitations receive insufficient attention in existing literature [19]. Fifth, recent developments such as Ethereum's transition to Proof of Stake and novel hybrid protocols have not yet been systematically evaluated in knowledge sharing contexts [20].

This systematic review addresses these gaps by providing a comprehensive, evidence-based analysis of how blockchain consensus mechanisms enhance trust in knowledge sharing platforms. Drawing on 77 peer-reviewed studies published between 2020 and 2025, the review identifies patterns across trust mechanisms, consensus algorithm adoption, implementation challenges, and documented benefits.

C. Study Organization

The remainder of this study is organized as follows. Section II presents the research questions formulated using the Population, Interest, and Context (PICo) framework. Section III provides theoretical background on knowledge sharing ecosystems and blockchain fundamentals. Section IV describes the methodology, including the PRISMA 2020 search strategy, study selection, data extraction, and quality assessment. Section V presents the results organized around the four research questions. Section VI provides the discussion, including principal findings, practical implications, and future research directions. Section VII concludes with key findings and recommendations.

II. Research Question

Research questions form the conceptual and methodological foundation of any Systematic Literature Review (SLR), defining its intellectual scope and governing the entire review process from search strategy design through study selection, data extraction, and synthesis [21]. Well-formulated questions reduce selection bias, ensure reproducible search coverage, and provide a framework within which findings from diverse studies can be meaningfully compared. They also support transparency and replicability, enabling other researchers to verify or extend the work. This review adopts the Population, Interest, and Context (PICo) framework to formulate focused and methodologically rigorous research questions. PICo is widely used in qualitative and exploratory systematic reviews to ensure conceptual precision by decomposing the research focus into three elements [23]. Table I presents the PICo elements as applied in this review.

Based on the PICo framework, four research questions were formulated to address the trust mechanisms, algorithm adoption, implementation challenges, and benefits of blockchain consensus mechanisms in knowledge sharing contexts:

RQ1: How do blockchain consensus mechanisms enhance trust in knowledge sharing platforms?

This question examines the theoretical frameworks and empirical evidence regarding mechanisms through which blockchain consensus protocols address trust deficits in knowledge sharing environments. It encompasses cryptographic security, immutability, distributed verification, transparency and auditability, economic incentive alignment, and smart contract automation as candidate trust enhancement mechanisms. The question is motivated by the absence of a systematic, multi-mechanism synthesis of blockchain trust properties specifically in knowledge sharing contexts.

RQ2: What blockchain consensus algorithms are currently used or proposed for knowledge sharing applications?

This question identifies and characterizes the consensus mechanisms deployed or proposed in knowledge sharing contexts, analyzing their technical specifications, performance characteristics, governance models, and application-specific adaptations. It encompasses established protocols (PoW, PoS, DPoS, PBFT) as well as novel and hybrid mechanisms emerging from domain-specific research. The question addresses the need for an evidence-based taxonomy of consensus mechanism usage in knowledge sharing deployments.

RQ3: What challenges and limitations affect blockchain implementation for knowledge sharing?

This question critically examines the obstacles that constrain or complicate the adoption of blockchain consensus mechanisms in knowledge sharing platforms. It encompasses technical constraints (scalability, energy consumption), economic barriers (cost, sustainability), integration complexity, governance and regulatory uncertainty, and usability challenges. The question reflects recognition that a balanced, evidence-based assessment of limitations is as important as documenting benefits for informing practical adoption decisions.

RQ4: What benefits do blockchain consensus mechanisms provide for knowledge sharing platforms?

This question synthesizes the documented advantages of blockchain consensus mechanisms in knowledge sharing contexts, including security and integrity improvements, transparency and auditability enhancements, decentralization and censorship-resistance benefits, smart contract automation efficiency gains, economic incentive alignment, and interoperability improvements. The question provides the positive case against which RQ3 challenges must be weighed in forming a balanced evidence-based assessment.

TABLE I. PICo Framework Applied to this Systematic Review

Element	Meaning	Application in This Review	Derived Research Question
Population	The entities or systems being studied	Blockchain-enabled knowledge sharing platforms and systems utilising consensus mechanisms	Platforms as the context of investigation
Interest	The phenomenon of interest what is being examined or observed	Blockchain consensus mechanisms and their effects on trust, security, and knowledge governance	The mechanism-trust relationship core of RQ1–RQ4
Context	The setting or circumstances in which the phenomenon occurs	Knowledge sharing environments spanning healthcare, supply chain, IoT, vehicular, energy, and academic domains (2020–2025)	Domain-specific and temporal scope of the review

Together, the four research questions form a complete analytical framework examining how blockchain achieves trust (RQ1), through which mechanisms (RQ2), at what cost (RQ3), and to what benefit (RQ4), thereby enabling a comprehensive and balanced synthesis of the current evidence base on blockchain consensus mechanisms for knowledge sharing.

III. Theoretical Background

A. Knowledge Sharing in Digital Ecosystems

Knowledge sharing encompasses the exchange of information, expertise, and intellectual resources across academic, corporate, governmental, and open-source contexts [24]. Digitalization has transformed these processes from physical document exchange to networked repositories and collaborative platforms, improving dissemination efficiency while simultaneously introducing new vulnerabilities in knowledge integrity, provenance, and governance.

Trust is a foundational prerequisite for effective knowledge sharing. Participants must trust that a platform faithfully preserves contributions, accurately attributes authorship, enforces transparent governance, and protects sensitive knowledge from unauthorized access [2], [5]. In centralized platforms, including institutional repositories, corporate knowledge systems, and academic databases, these requirements are delegated entirely to the platform operator, creating a structural dependency on a single party whose incentives may not align with those of contributors and consumers.

The risks of this model are well-documented. Breaches expose confidential knowledge assets; operators may censor contributions; provenance records can be altered to misattribute intellectual work; and access policies may change unilaterally [3], [1]. These failures have motivated research into decentralized alternatives that distribute trust across multiple independent participants, reflecting a design philosophy that aligns directly with blockchain technology.

B. Blockchain Technology Fundamentals

Blockchain is a form of distributed ledger technology (DLT) that enables multiple untrusted parties to maintain shared, append-only records without central coordination or a trusted third party [25]. No single participant controls the record; each node maintains a copy of the ledger, and changes require agreement from a defined quorum of nodes through a consensus process.

The data structure consists of cryptographically linked blocks, each containing validated transactions, a timestamp, metadata, and a hash of the preceding block forming an immutable chain back to the genesis block [4]. Any retroactive modification invalidates all subsequent hashes, making tampering computationally detectable across the entire network. Integrity is therefore enforced mathematically rather than institutionally.

A blockchain system comprises six core components: a distributed peer-to-peer network of nodes; cryptographic hash functions (such as SHA-256) for data integrity, digital signature schemes (such as ECDSA) for authentication, a consensus mechanism for coordinating agreement on transaction validity, an immutable append-only ledger; and smart contracts, which are self-executing programs that enforce predefined rules automatically [9], [10]. Blockchain systems are classified as public, private, or consortium networks, each presenting distinct trade-offs between openness, performance, and trust assumptions [17].

Consensus mechanisms are protocols by which distributed nodes reach agreement on the valid ledger state despite faulty, offline, or malicious participants [6], [7]. They address the Byzantine Generals Problem by achieving reliable agreement when some nodes may behave arbitrarily or deceptively [8]. Each mechanism does so through distinct assumptions about participant behaviour, different validator selection strategies, and specific trade-offs between security, performance, energy efficiency, and decentralization.

Proof of Work (PoW), pioneered by Bitcoin, requires miners to solve cryptographic puzzles to earn the right to append the next block [9]. While PoW offers strong Sybil resistance and a proven security record, its high energy demands and limited throughput make it poorly suited for knowledge sharing applications. Proof of Stake (PoS) selects validators based on staked collateral, incentivizing honest behaviour through the threat of stake forfeiture [10]. PoS consumes significantly less energy than PoW while maintaining comparable security, and its adoption by Ethereum in 2022 has validated it at global scale.

Delegated Proof of Stake (DPoS) extends PoS through a governance layer in which token holders elect delegates responsible for block production [11]. This enables higher throughput while maintaining stakeholder governance well-suited to knowledge sharing platforms where community members elect trusted curators. Practical Byzantine Fault Tolerance (PBFT) and its variants (HotStuff, Tendermint) operate in permissioned environments with known, identity-verified validators, achieving consensus through multi-round messaging that tolerates up to one-third of faulty or malicious nodes [8]. PBFT delivers deterministic finality, low energy use, and high throughput, making it particularly suitable for consortium knowledge sharing systems with pre-identified institutional participants.

Table II summarizes the comparative characteristics of the principal consensus mechanism families. Selecting an appropriate mechanism for knowledge sharing requires consideration of four key factors: the trust model (who the participants are and their level of mutual trust), performance requirements (transaction frequency and acceptable latency), energy constraints (platform sustainability needs), and governance model (how validator authority should be distributed). These trade-offs directly shape the trust properties a blockchain-based knowledge sharing platform can deliver, and form the theoretical foundation for the systematic review conducted in this study.

TABLE II. COMPARATIVE OVERVIEW OF BLOCKCHAIN CONSENSUS MECHANISMS FOR KNOWLEDGE SHARING CONTEXTS

Mechanism	Validator Selection	Energy Consumption	Fault Tolerance	Throughput	Suitable Network	KS Applicability
Proof of Work (PoW)	Computational puzzle	Very High	Up to 50%	Low (7–15 TPS)	Public	Low
Proof of Stake (PoS)	Staked assets	Low	Up to 33%	Medium	Public	Medium
Delegated PoS (DPoS)	Elected delegates	Low	Up to 33%	High	Public	Medium
PBFT / BFT Variants	Pre-known nodes	Very Low	Up to 33%	High (1000+ TPS)	Permissioned	High
Proof of Authority (PoA)	Approved validators	Very Low	Identity-based	Very High	Consortium	High
Novel / Hybrid Mechanisms	Domain-specific	Variable	Variable	Variable	Any	Emerging

IV. MATERIAL AND METHODS

A. Study Design and Protocol

This systematic review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines [26], providing a transparent and reproducible methodological framework. The review is a qualitative evidence synthesis employing thematic, frequency, comparative, and temporal analytical approaches to synthesize findings from heterogeneous studies across multiple blockchain and knowledge sharing domains. The PRISMA framework structures the review across four phases, namely identification, screening, eligibility assessment, and data synthesis, each with explicit decision criteria to minimize selection bias.

Three databases were systematically searched: Scopus (Elsevier), offering multidisciplinary coverage across computer science, engineering, and information systems; IEEE Xplore (IEEE), providing depth in technical computing literature including conference proceedings and standards; and Web of Science (Clarivate), a high-quality interdisciplinary citation database covering over 12,000 journals. These databases were selected for their complementary coverage profiles, collectively capturing the full range of relevant peer-reviewed evidence with minimal duplication. The search strategy combined three concept clusters using Boolean operators, applied consistently across all three databases (Table III):

TABLE III. THE SEARCH STRING

Concept	String
Blockchain concepts	("blockchain" OR "distributed ledger")
Consensus mechanisms	("consensus mechanism" OR "consensus algorithm" OR "consensus protocol")
Knowledge sharing	("knowledge sharing" OR "knowledge management" OR "information sharing" OR "data sharing")

- Complete search string:

("blockchain" OR "distributed ledger") AND ("consensus mechanism" OR "consensus algorithm" OR "consensus protocol") AND ("knowledge sharing" OR "knowledge management" OR "information sharing" OR "data sharing")

B. Study Selection Process

Study selection followed four sequential PRISMA phases, as illustrated in Fig. 1. Inclusion and exclusion criteria applied at each phase are presented in Table IV.

TABLE IV. INCLUSION AND EXCLUSION CRITERIA FOR STUDY SELECTION

Criterion	Inclusion	Exclusion
Language	English	Non-English
Time line	2020 – 2025	< 2020 & >2025
Literature type	Journal (Article), Conference	Book, Review
Publication Stage	Final	In Press
Subject	Focus on blockchain consensus mechanisms and knowledge sharing applications	• Studies focusing exclusively on cryptocurrency trading or financial applications without knowledge sharing relevance • Studies not directly addressing both blockchain consensus and knowledge sharing

Phase 1 Identification: Database searches identified 1,660 records (Scopus: 646; IEEE Xplore: 632; Web of Science: 382). After removing 522 duplicates using Endbook reference management software with manual verification, 1,138 unique records proceeded to the screening phase.

Phase 2 Screening: Two reviewers independently screened all 1,138 titles and abstracts against the eligibility criteria, resolving disagreements through discussion or third-reviewer arbitration. A total of 203 records were excluded: 3 fell outside the 2020–2025 date range, and 200 did not address all three concept groups (blockchain, consensus mechanism, and knowledge sharing). The remaining 935 records advanced to full-text assessment.

Phase 3 Full-Text Eligibility Assessment: Full texts of 935 articles were retrieved and assessed. In total, 858 were excluded: 548 did not address consensus mechanisms in knowledge sharing contexts; 150 showed insufficient methodological rigour; 100 were not original empirical research or systematic reviews; 30 were unavailable as full text; and 30 raised quality or integrity concerns (including 2 retracted articles). The remaining 77 studies met all criteria and were included for data extraction.

Phase 4 Citation Searching: Reference lists and forward citations of all 77 included studies were examined. No additional studies meeting all inclusion criteria were identified.

C. PRISMA Flow Diagram

Fig. 1 presents the PRISMA 2020 flow diagram summarizing the complete selection process from 1,660 initially identified records, through 522 duplicate removals, 203 screening exclusions, and 858 full-text exclusions, to the final corpus of 77 included studies. The diagram ensures full transparency and reproducibility in accordance with PRISMA 2020 reporting standards [26].

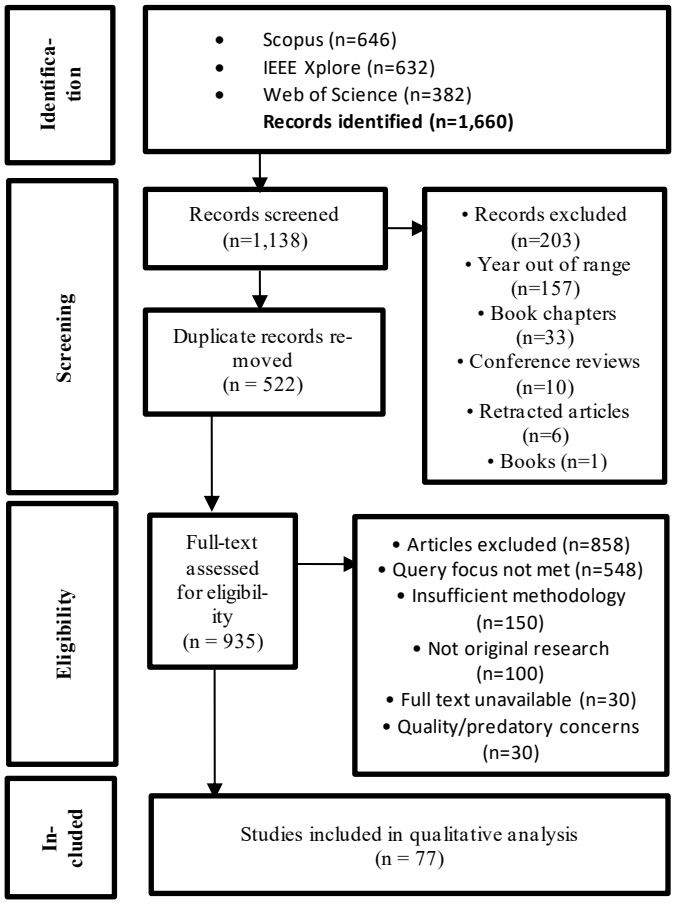

Fig. 1. Flow diagram of the proposed searching study.

D. Study Selection Process

A standardized data extraction form was developed, piloted on five studies, and refined based on reviewer feedback. Two reviewers independently extracted data from all 77 studies, with discrepancies resolved through discussion or third-reviewer arbitration. Extracted data were organized into four categories: 1) study characteristics authors, year, journal, country, and research design; 2) technical details blockchain platform, consensus mechanism, knowledge sharing domain, and system architecture; 3) research findings trust mechanisms (RQ1), consensus algorithms (RQ2), implementation challenges (RQ3), and documented benefits (RQ4); and 4) quality indicators limitations acknowledged, data collection described, and conclusions supported by evidence. All data were entered into structured spreadsheets with automated completeness checks.

E. Quality Assessment and Risk-of-Bias Evaluation (PRISMA 2020)

All 77 studies were appraised using a 7-criterion adapted Critical Appraisal Skills Program (CASP) checklist [21], [22], with a maximum score of 12 points. Each criterion was scored as fully met (full marks), partially met (half marks), or not met (0). Table V presents the criteria and their descriptions as applied during screening and data extraction.

TABLE V. QUALITY ASSESSMENT CRITERIA FOR SYSTEMATIC LITERATURE REVIEW (CASP RISK-OF-BIAS INSTRUMENT, PRISMA 2020)

Code	Criterion	Description
C1	Clear research objectives (max 2)	Research aims and questions explicitly stated and aligned with study scope
C2	Appropriate methodology (max 2)	Study design suitable to address research objectives
C3	Rigorous data collection (max 2)	Databases, inclusion/exclusion criteria, PRISMA applied
C4	Appropriate data analysis (max 2)	Systematic qualitative synthesis or quantitative evaluation conducted
C5	Clear results presentation (max 1)	Findings summarized clearly using tables and structured discussion
C6	Limitations discussed (max 1)	Study limitations explicitly acknowledged
C7	Contribution significance (max 2)	Provides comprehensive insights and identifies research gaps

F. Data Synthesis and Analysis

Data synthesis employed four complementary analytical approaches [27]. Thematic analysis identified recurring themes across trust mechanisms, consensus algorithms, challenges, and benefits, grouping studies by conceptual alignment. Frequency analysis calculated the proportion of studies reporting each theme, enabling quantitative comparison across the 77-study corpus. Comparative analysis examined differences across consensus mechanism types, application domains, and performance profiles to identify selection patterns and outcome variation. Temporal analysis tracked publication trends across 2020–2025 to surface emerging research directions and shifts in focus over time.

V. RESULT

Quality appraisal of all 77 included studies confirmed a high overall methodological standard. Studies were classified as High (≥9/12), Moderate (6–8/12), or Low (<6/12). Of the 77 studies, 72 (93.5%) were rated High quality and 5 (6.5%) Moderate; none were rated Low or excluded on quality grounds.

TABLE VI. PERFORMANCE OF QUALITY ASSESSMENT: FULL SCORING MATRIX (77 STUDIES)

No	Authors	C1	C2	C3	C4	C5	C6	C7	Total /12	Quality
1	[119]	2/2	2/2	2/2	2/2	1/1	1/1	2/2	12/12	High
2	[94]	2/2	1/2	2/2	2/2	1/1	0/1	2/2	10/12	High
3	[30]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
4	[73]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
5	[51]	2/2	2/2	1/2	2/2	1/1	0/1	1/2	9/12	High
6	[45]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
7	[50]	1/2	2/2	2/2	2/2	1/1	0/1	2/2	10/12	High

8	[59]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
9	[115]	2/2	1/2	1/2	2/2	1/1	1/1	2/2	10/12	High
10	[44]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
11	[117]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
12	[63]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
13	[89]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
14	[46]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
15	[99]	2/2	2/2	2/2	1/2	1/1	1/1	1/2	10/12	High
16	[85]	2/2	2/2	1/2	1/2	1/1	1/1	2/2	10/12	High
17	[82]	2/2	1/2	2/2	1/2	1/1	0/1	2/2	9/12	High
18	[81]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
19	[47]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
20	[93]	2/2	2/2	2/2	2/2	1/1	1/1	2/2	12/12	High
21	[42]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
22	[110]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
23	[90]	2/2	2/2	2/2	1/2	0/1	0/1	2/2	9/12	High
24	[112]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
25	[84]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
26	[65]	2/2	2/2	2/2	2/2	1/1	1/1	1/2	11/12	High
27	[34]	2/2	2/2	2/2	2/2	1/1	1/1	2/2	12/12	High
28	[35]	2/2	2/2	1/2	1/2	1/1	0/1	2/2	9/12	High
29	[66]	2/2	1/2	2/2	2/2	1/1	0/1	2/2	10/12	High
30	[75]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
31	[98]	1/2	2/2	1/2	2/2	1/1	1/1	2/2	10/12	High
32	[104]	2/2	2/2	2/2	2/2	1/1	1/1	1/2	11/12	High
33	[121]	2/2	2/2	2/2	2/2	1/1	1/1	2/2	12/12	High
34	[83]	2/2	1/2	1/2	2/2	0/1	0/1	1/2	7/12	Moderate
35	[53]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
36	[43]	1/2	2/2	1/2	2/2	0/1	0/1	2/2	8/12	Moderate
37	[105]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
38	[76]	2/2	1/2	2/2	2/2	1/1	1/1	1/2	10/12	High
39	[31]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
40	[38]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
41	[80]	1/2	2/2	1/2	1/2	0/1	1/1	2/2	8/12	Moderate
42	[87]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
43	[109]	2/2	2/2	2/2	2/2	0/1	0/1	2/2	10/12	High
44	[101]	2/2	1/2	2/2	2/2	1/1	0/1	2/2	10/12	High
45	[103]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
46	[72]	1/2	1/2	2/2	2/2	1/1	1/1	2/2	10/12	High
47	[96]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
48	[57]	2/2	2/2	2/2	1/2	1/1	1/1	2/2	11/12	High
49	[58]	2/2	2/2	2/2	1/2	0/1	1/1	2/2	10/12	High
50	[97]	2/2	2/2	2/2	1/2	1/1	1/1	2/2	11/12	High
51	[92]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
52	[111]	2/2	2/2	2/2	2/2	1/1	1/1	1/2	11/12	High
53	[118]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
54	[106]	2/2	1/2	1/2	1/2	1/1	1/1	2/2	9/12	High
55	[54]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
56	[107]	2/2	2/2	1/2	1/2	0/1	0/1	1/2	7/12	Moderate
57	[64]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
58	[113]	2/2	2/2	2/2	2/2	1/1	1/1	1/2	11/12	High
59	[95]	2/2	2/2	2/2	2/2	1/1	1/1	2/2	12/12	High
60	[79]	2/2	2/2	2/2	2/2	0/1	0/1	1/2	9/12	High
61	[71]	2/2	2/2	1/2	1/2	0/1	1/1	2/2	9/12	High
62	[40]	2/2	2/2	2/2	2/2	1/1	1/1	2/2	12/12	High
63	[100]	2/2	2/2	1/2	2/2	1/1	0/1	2/2	10/12	High
64	[120]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
65	[102]	2/2	2/2	2/2	1/2	0/1	0/1	2/2	9/12	High
66	[116]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
67	[108]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
68	[49]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
69	[48]	2/2	2/2	1/2	1/2	1/1	0/1	2/2	9/12	High
70	[61]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
71	[114]	2/2	2/2	1/2	2/2	1/1	1/1	2/2	11/12	High
72	[67]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
73	[62]	1/2	2/2	1/2	2/2	0/1	0/1	2/2	8/12	Moderate
74	[91]	2/2	2/2	1/2	2/2	0/1	1/1	2/2	10/12	High
75	[88]	2/2	2/2	2/2	2/2	1/1	1/1	2/2	12/12	High
76	[86]	2/2	2/2	2/2	2/2	1/1	0/1	2/2	11/12	High
77	[77]	2/2	2/2	2/2	2/2	1/1	1/1	2/2	12/12	High

The mean CASP score was 10.3/12, indicating a consistently strong evidence base. The full scoring matrix is presented in Table VI, and a summary of quality distribution is presented in Table VII.

TABLE VII. PERFORMANCE OF QUALITY ASSESSMENT: SUMMARY

CASP QUALITY ASSESSMENT			
High quality (≥9/12)	72	93.5%	Score 9–12/12
Moderate quality (6–8/12)	5	6.5%	Score 6–8/12
Low quality (<6/12)	0	0.0%	No papers excluded on quality
Mean CASP score	10.3/12		Average across 77 papers

A. RQ1: Trust Enhancement Mechanisms

Six mechanisms through which blockchain consensus protocols enhance trust in knowledge sharing platforms were identified. Distributed verification and transparency form the dominant complementary pair, supported by cryptographic security, immutability, economic incentives, and smart contract automation at varying frequencies (Table VIII).

TABLE VIII. FREQUENCY ANALYSIS: TRUST ENHANCEMENT MECHANISMS (RQ1)

Rank	Trust Mechanism	Count	Percentage	Interpretation for Results Section
1	Distributed Verification & Decentralization	60	77.9%	Dominant mechanism (78%) consensus-based validation eliminates need for central trust authority; directly addresses single-point-of-failure in centralized knowledge systems
2	Transparency & Auditability	40	51.9%	Second most common (52%), blockchain's immutable audit trail directly resolves knowledge provenance concerns in collaborative ecosystems
3	Cryptographic Security & Data Integrity	30	39.0%	Third (39%) mathematical proof of integrity via hash functions, digital signatures; foundational to blockchain's trust model
4	Immutability & Tamper-Evidence	25	32.5%	Fourth (32%) prevents retroactive falsification of contributions; critical for academic knowledge and IP protection contexts
5	Economic Incentive Alignment	21	27.3%	Fifth (27%) token/reputation mechanisms align participant self-interest with honest sharing; addresses free-rider problem in open knowledge platforms
6	Smart Contract Automation	15	19.5%	Sixth (19%) automated rule enforcement removes need for trusted human intermediaries; structurally significant despite lower frequency

1) Distributed verification and decentralization: Distributed verification was the most extensively documented mechanism, reported in 60 studies (78%). It reflects blockchain's core architectural role in eliminating reliance on central authorities by distributing validation across independent nodes, directly addressing the trust deficit of centralized platforms [28], [29], [30]. The mechanism appeared prominently in IoT knowledge systems [31], [32], vehicular data exchange [32], [33], and cross-organizational sharing contexts [34], [35]. Reporting grew consistently from 4 studies in 2020 to 13–15 annually from 2023 to 2025, confirming a maturing rather than transient evidence base. Distributed verification demonstrated strong co-occurrence with transparency (34 studies, 44%), suggesting that these mechanisms are typically studied and implemented together as complementary pillars of blockchain-based trust.

2) Transparency and auditability: Transparency and auditability were reported in 40 studies (52%). Blockchain's publicly verifiable, chronologically ordered transaction records establish knowledge provenance and enable independent audit, directly addressing scepticism about data origin and modification history [36], [37], [38]. The mechanism was prominent in supply chain [35], [39], healthcare [40], [41], and institutional governance contexts [42], [43]. Its co-occurrence with cryptographic security in 18 studies (23%) confirms that these mechanisms operate synergistically; cryptography makes transparency claims mathematically verifiable rather than merely asserted.

3) Cryptographic security and data integrity: Cryptographic security was documented in 30 studies (39%), providing the mathematical foundation for trust through hash functions, digital signatures, Merkle trees, and asymmetric encryption. Operating at the protocol level, it ensures that any tampering is computationally detectable, complementing transparency and distributed verification, which are architectural properties. Applications span medical data [44], [45], industrial systems [46], [47], and financial knowledge sharing [48], [49]. Co-occurrence with distributed verification in 24 studies (31%) confirms that cryptography and consensus verification operate as complementary rather than substitutable mechanisms.

4) Immutability and tamper-evidence: Immutability was reported in 25 studies (32%). Once confirmed by consensus, a transaction cannot be altered without invalidating all subsequent blocks, making retroactive falsification computationally infeasible. This was particularly valued in academic provenance [32], intellectual property records [37], and healthcare data contexts [45], [50]. The mechanism co-occurred with distributed verification in 24 studies (31%) and cryptographic security in 12 studies (16%), confirming that immutability is most meaningful when combined with the mechanisms that enforce and govern it.

5) Economic incentive alignment: Economic incentive alignment was documented in 21 studies (27%), encompassing token rewards, reputation mechanisms, and game-theoretic structures that make dishonest behaviour economically irrational rather than merely detectable. Applications include decentralized knowledge curation [28], [51], supply chain sharing [39], [52], vehicular networks [53], [54], and platform governance [55], [56]. Co-occurrence with distributed verification (19 studies, 25%) and transparency (11 studies, 14%) confirms that incentive mechanisms are typically deployed as complements to architectural trust properties, not as standalone solutions.

6) Smart contract automation: Smart contract automation was the least cited mechanism (15 studies, 19%), yet is structurally significant. By encoding rules as self-executing code, smart contracts remove reliance on human intermediaries. Applications include access control [57], [58], attribution management [39], [40], and autonomous governance [43], [36]. References grew from 1 study in 2021 to 5 each in 2022 and

2025, reflecting accelerating adoption as tooling matures. Its strongest co-occurrence with cryptographic security (11 studies, 14%) reflects the cryptographic foundations required for tamper-resistant execution.

Blockchain consensus mechanisms enhance trust through six complementary and co-occurring mechanisms, not a single dominant feature. The strong co-occurrence of distributed verification with transparency (44%) and cryptographic security (31%) confirms that effective trust architectures deploy multiple mechanisms simultaneously. Only 6 of 77 studies (8%) documented none of the six mechanisms, while 18 studies (23%) documented four or more, affirming that comprehensive trust enhancement through blockchain is a multi-mechanism phenomenon.

Within the context of knowledge sharing platforms, these six co-occurring trust mechanisms collectively address the fundamental challenge of establishing trust among participants who contribute intellectual assets without the assurance of a central authority. Distributed verification and transparency directly resolve the knowledge provenance problem, enabling participants to independently verify the authenticity and attribution of contributed knowledge. Cryptographic security and immutability protect intellectual contributions from post-submission manipulation a critical concern in academic and research KS platforms where misattribution carries significant professional consequences. Economic incentive alignment confronts the free-rider problem endemic to open KS communities by making dishonest or low-quality contributions economically irrational, while smart contract automation enforces contribution protocols without the need for trusted human intermediaries. The multi-mechanism finding has a direct implication for KS platform design: a blockchain implementation targeting only one or two trust properties, such as immutability without decentralization, remains vulnerable to operator manipulation and therefore fails to resolve the core trust deficit that motivates blockchain adoption in knowledge sharing contexts.

B. RQ2: Current Consensus Algorithms for Knowledge Sharing

No single consensus mechanism dominates knowledge sharing research; mechanism choice is driven by the trust, performance, and governance requirements of each context (Table IX). Notably, 38 studies (49%) did not specify a named mechanism, focusing instead on architectural-level blockchain properties. This represents a significant empirical gap limiting cross-study comparison and reproducibility. A complete mapping of all 77 reviewed studies to their respective consensus mechanisms and the specific trust dimensions they address is provided in Table X.

1) PBFT and BFT-based variants: PBFT and its variants were the most examined mechanism, reported in 18 studies (23%). Their suitability for permissioned architectures with known participants, verified identity, and deterministic finality aligns closely with enterprise knowledge sharing and inter-organizational sharing. Applications span vehicular networks [45], [33], IoT platforms [59], [60], and supply chain knowledge systems [61], [62]. Studies grew from 1 in 2020 to 5 each in 2023 and 2025, reflecting growing confidence in BFT consensus for knowledge sharing. Its ability to tolerate a bounded number of malicious nodes makes it well-suited to consortium platforms where participants have established institutional accountability.

2) Novel, hybrid, and application-specific mechanisms: Novel and hybrid mechanisms formed the second largest category (13 studies, 17%), encompassing Proof of Authority for identity-verified networks [30], [63], DAG-based approaches for high-throughput IoT sharing [64], and reputation-integrated consensus for trust-weighted contribution [54], [55]. Growing from 1 study in 2020 to 4 in both 2022 and 2023, this category reflects a maturing trend toward purpose-built consensus that prioritises domain-specific requirements particularly relevant for agricultural, federated learning, and energy trading contexts where standard protocols impose excessive overhead.

TABLE IX. FREQUENCY ANALYSIS: CONSENSUS ALGORITHM ADOPTION (RQ2)

Rank	Consensus Mechanism	Count	Percentage	Interpretation for Results Section
1	PBFT / BFT Variants	18	23.4%	Most examined (23%) deterministic finality and low latency make PBFT ideal for permissioned knowledge sharing platforms where all participants are known
2	Novel / Hybrid / Other Mechanisms	13	16.9%	Second (17%) growing category of novel/hybrid mechanisms tailored to specific knowledge domains; reflects maturation of consensus research beyond standard protocols
3	Proof of Work (PoW)	8	10.4%	Third (10%) declining relevance due to energy concerns; still used for high-security timestamping of knowledge records in public blockchains
4	Proof of Stake (PoS)	6	7.8%	Fourth (8%) growing adoption following Ethereum's Merge; preferred for sustainable knowledge platforms requiring frequent transactions
5	Delegated Proof of Stake (DPoS)	3	3.9%	Least common (4%) niche application in high-throughput knowledge platforms; governance model suits decentralized academic or community knowledge systems

3) Proof of work: Proof of work appeared in 8 studies (10%), primarily for high-security timestamping of knowledge

records rather than high-frequency transactions. Applications include energy sector management [64], [50], industrial data sharing [37], [65], and federated knowledge exchange [46], [53]. The concentration of 4 studies in 2024 suggests a declining and increasingly selective role, consistent with the industry shift away from energy-intensive consensus following Ethereum's 2022 transition.

TABLE X. MAPPING OF REVIEWED STUDIES TO CONSENSUS MECHANISMS AND TRUST DIMENSIONS

No	Authors	Consensus Mechanism	Dist. Verif.	Transparency	Crypto Security	Immutability	Econ Incentive	Smart Contract
1	[59]	Not specified	✓	✓	✓	✓		
2	[53]	PoS + DPoS	✓	✓	✓	✓		✓
3	[54]	Novel/Hybrid	✓	✓		✓	✓	
4	[66]	PBFT/BFT	✓	✓	✓			✓
5	[47]	Not specified	✓		✓	✓		
6	[30]	PBFT/BFT	✓	✓	✓			
7	[93]	PoW	✓	✓		✓	✓	✓
8	[65]	PBFT/BFT	✓	✓	✓			
9	[119]	Not specified	✓	✓	✓	✓		
10	[50]	Not specified	✓		✓	✓		
11	[30]	Novel/Hybrid	✓	✓		✓		
12	[44]	Novel/Hybrid	✓	✓	✓			✓
13	[38]	PBFT/BFT + Novel/Hybrid	✓	✓		✓		✓
14	[82]	PoW	✓		✓	✓		
15	[39]	Not specified	✓	✓	✓		✓	✓
16	[42]	PBFT/BFT	✓	✓		✓	✓	
17	[100]	Not specified	✓	✓	✓			✓
18	[65]	Not specified	✓	✓		✓	✓	
19	[90]	Novel/Hybrid	✓		✓	✓		
20	[63]	PBFT/BFT + PoS	✓	✓	✓		✓	
21	[52]	Not specified	✓	✓	✓	✓		✓
22	[75]	Not specified	✓	✓	✓	✓		
23	[76]	Not specified	✓		✓	✓		
24	[46]	PBFT/BFT	✓	✓			✓	✓
25	[45]	PBFT/BFT	✓	✓	✓			
26	[101]	PoW + Novel/Hybrid	✓	✓		✓		✓
27	[12]	Not specified	✓	✓	✓			✓
28	[36]	Not specified	✓		✓	✓		
29	[13]	PoS + DPoS		✓	✓			✓
30	[117]	Not specified	✓	✓		✓		✓
31	[57]	PBFT/BFT	✓	✓	✓	✓		
32	[41]	Not specified	✓	✓		✓		✓
33	[39]	Not specified	✓		✓	✓		
34	[43]	PoW	✓	✓	✓		✓	
35	[32]	PoW	✓	✓	✓	✓		
36	[58]	Not specified		✓	✓			✓
37	[70]	PoW	✓	✓		✓		✓
38	[71]	PBFT/BFT	✓	✓	✓			
39	[72]	Not specified	✓		✓	✓		
40	[44]	Not specified	✓		✓	✓		
41	[48]	Not specified	✓	✓			✓	✓
42	[49]	PBFT/BFT + PoS	✓	✓	✓			✓
43	[84]	PBFT/BFT	✓	✓	✓	✓		
44	[85]	Not specified	✓		✓	✓		
45	[80]	Novel/Hybrid	✓	✓		✓	✓	
46	[32]	Novel/Hybrid	✓	✓	✓			
47	[105]	Not specified	✓	✓	✓	✓	✓	✓
48	[60]	Not specified	✓	✓		✓		
49	[61]	Not specified		✓	✓		✓	
50	[49]	Not specified	✓	✓	✓			
51	[56]	Novel/Hybrid	✓		✓	✓		
52	[55]	PBFT/BFT	✓	✓	✓		✓	
53	[54]	Not specified	✓	✓		✓	✓	
54	[64]	Not specified	✓	✓	✓			✓
55	[95]	Novel/Hybrid	✓	✓	✓	✓		
56	[57]	Not specified	✓	✓		✓		✓
57	[115]	PoW	✓	✓	✓		✓	✓
58	[53]	Not specified	✓		✓	✓		
59	[83]	Novel/Hybrid	✓	✓		✓		
60	[58]	Not specified	✓	✓	✓			✓
61	[62]	Not specified	✓	✓	✓	✓		
62	[99]	Not specified	✓		✓	✓		✓
63	[95]	PoS + PoW	✓	✓		✓		
64	[87]	Novel/Hybrid	✓	✓	✓			
65	[88]	Not specified	✓	✓	✓	✓		

66	[89]	Not specified	✓	✓		✓		✓
67	[98]	PBFT/BFT	✓	✓	✓		✓	
68	[45]	Not specified	✓	✓	✓	✓		
69	[46]	PBFT/BFT + Novel/Hybrid	✓		✓	✓		
70	[99]	PBFT/BFT	✓	✓		✓	✓	✓
71	[109]	Not specified		✓	✓			✓
72	[100]	PoS + DPoS	✓	✓	✓	✓		
73	[90]	PBFT/BFT	✓		✓	✓		
74	[91]	Not specified	✓	✓	✓			
75	[92]	PBFT/BFT	✓	✓		✓		✓
76	[101]	Not specified	✓	✓	✓		✓	
77	[101]	Not specified	✓	✓		✓		✓

4) Proof of stake: Proof of stake appeared in 6 studies (8%), with interest accelerating after Ethereum's 2022 Merge. Applications include vehicular networks [33], [66], healthcare sharing [36], and energy-efficient IoT platforms [67], [68]. The growing adoption from 1 study in 2022 to 3 in 2023 reflects its energy efficiency, faster finality than PoW, and alignment with institutional sustainability requirements. Co-occurrence with PBFT in 2 studies points to emerging hybrids combining stake-based efficiency with Byzantine fault-tolerant finality.

5) Delegated proof of stake: Delegated proof of stake was the least examined (3 studies, 4%), appearing in high-throughput IoT sharing [29], [66] and vehicular networks [67]. Its low frequency likely reflects its primary association with public cryptocurrency platforms, though its governance model of elected validators offers a natural analogue for democratic knowledge platform governance.

The consensus mechanism landscape is characterized by diversity and domain-specificity rather than convergence. PBFT leads (23%) for permissioned environments, followed by novel and hybrid mechanisms (17%). The 49% of studies that did not specify a mechanism represent a critical empirical gap; future research should explicitly report and justify mechanism selection to enable precise cross-study comparison of trust outcomes.

For knowledge sharing applications specifically, consensus mechanism selection is not merely a technical optimization decision but a fundamental trust governance choice that directly shapes the trust claims a platform can make to its participants. The dominance of PBFT and BFT variants (23%) reflects the consortium and inter-organizational nature of most institutional KS deployments, where participants are pre-identified, and accountability structures are pre-established. However, the critical gap, whereby 49% of reviewed studies failed to specify a consensus mechanism, is particularly problematic for KS research, because trust properties such as Byzantine fault tolerance, finality guarantees, and validator incentive structures are directly determined by mechanism choice. A KS platform claiming tamper-resistance and censorship-resistance cannot substantiate those claims without specifying how its consensus process prevents validator collusion or Sybil attacks. Future research in blockchain-based knowledge sharing must treat consensus mechanism reporting as a mandatory methodological disclosure, equivalent in importance to specifying data collection instruments in empirical research.

C. RQ3: Challenges and Limitations

TABLE XI. FREQUENCY ANALYSIS: IMPLEMENTATION CHALLENGES (RQ3)

Rank	Challenge Category	Count	Percentage	Interpretation for Results Section
1	Scalability & Performance Constraints	40	51.9%	Most prevalent (52%) throughput limitations and high latency are inherent to most consensus mechanisms; directly linked to the consensus overhead required for trustless verification
2	Integration Complexity with Existing Systems	23	29.9%	Second (30%) enterprise knowledge systems are deeply embedded in legacy infrastructure; blockchain's architectural differences create significant migration and interoperability challenges
3	Energy Consumption & Environmental Impact	22	28.6%	Third (29%) particularly acute for PoW-based systems; growing concern as sustainability becomes a governance priority for knowledge institutions
4	Economic Sustainability & Cost	20	26.0%	Fourth (26%) gas fees and token volatility create unpredictable operational costs; challenges sustainable deployment in academic or non-profit knowledge sharing contexts
5	Governance & Regulatory Uncertainty	11	14.3%	Fifth (14%), regulatory ambiguity around data ownership, smart contract enforceability, and cross-border data flows creates institutional hesitancy
6	Usability & User Experience Barriers	8	10.4%	Sixth (10%), despite being the least reported, user experience barriers are a critical adoption constraint; technical complexity alienates non-expert knowledge workers

Substantial implementation challenges were identified, with 63 of 77 studies (82%) reporting at least one barrier. Challenges are rarely isolated; 38 studies (49%) reported two or more concurrently, confirming a compounding rather than sequential barrier landscape. The following findings are ordered by frequency (Table XI).

1) Scalability and performance constraints: Scalability and performance constraints were the most pervasive challenge, reported in 40 studies (52%). The distributed consensus process that creates trust necessarily introduces computational overhead and throughput ceilings. Applications affected include IoT platforms [119],[81], vehicular networks [31], [59], and broader knowledge sharing systems facing the blockchain trilemma [69], [64]. The challenge persisted across all years (4 studies in 2020 to 9 in 2025), indicating it remains unresolved. Co-occurrence with integration complexity (15 studies, 19%) and economic costs (12 studies, 16%) creates a particularly significant compound barrier for enterprise adoption.

2) Integration complexity with existing systems: Integration complexity was reported in 23 studies (30%), covering challenges in bridging blockchain with legacy repositories [44], [32], cross-chain interoperability [34], [55], and deploying permissioned networks within existing IT governance frameworks [46], [58]. A strong upward trend from 1 study in 2021 to 10 in 2025 confirms that integration barriers intensify as deployments move from prototype to production. Co-occurrence with energy consumption in 8 studies (10%) suggests that green blockchain adoption adds further integration complexity.

3) Energy consumption and environmental impact: Energy consumption was reported in 22 studies (29%), particularly for PoW-based implementations whose mining demands conflict with institutional sustainability commitments. Concerns were documented in industrial IoT sharing [70], [71], energy sector platforms [72], [64], and vehicular networks [67], [54]. Co-occurrence with scalability in 11 studies (14%) reflects the dual burden of PoW: high energy use without proportional throughput gains. Appearing consistently across 2021–2025, this is an enduring rather than resolving barrier, and increasingly framed as a governance concern in contexts subject to European sustainability reporting requirements.

4) Economic sustainability and cost: Economic sustainability was raised in 20 studies (26%), covering transaction fees, storage costs, token volatility, and the financial viability of operating blockchain platforms at scale. Issues include gas fees in Ethereum-based systems [73], [31], storage cost escalation [74], [75], and economic misalignment in incentive token structures [68], [64]. Growing from 3 studies in 2020 to 6 in 2025, this reflects increasing recognition that technical feasibility must be matched by viable economic models before institutional adoption. This is particularly acute for academic and non-profit contexts where cost recovery through tokenization remains legally and organizationally complex.

5) Governance and regulatory uncertainty: Governance and regulatory uncertainty was documented in 11 studies (14%), covering unclear enforceability of smart contract agreements [94], [39], cross-jurisdictional data governance conflicts [36], [38], and absent standardized governance frameworks [76], [40]. Rising from 1 study in 2020 to 5 in 2025, this is the fastest-growing challenge category reflecting the pattern of governance maturation seen in healthcare AI and fintech regulation as deployments approach production.

6) Usability and user experience barriers: Usability barriers were the least cited challenge (8 studies, 10%), yet are strategically significant for mainstream adoption. Issues include key management complexity [59], [41], interface design that obscures trust benefits [39], [37], and steep learning curves for governance participation [57], [48]. Studies grew from 1 annually in 2021–2023 to 4 in 2025, signaling growing attention to human factors. The relative underrepresentation may reflect systematic bias in technically oriented research communities toward engineering challenges over user-facing ones.

Across 77 studies, challenges form a compound barrier landscape where technical (scalability, integration), environmental (energy), financial (economic sustainability), and institutional (governance, usability) barriers co-occur and amplify each other. The consistent increase across all six categories from 2020 to 2025 indicates an expanding rather than contracting challenge landscape, underscoring the need for multi-dimensional solution frameworks that address technical, economic, governance, and human factors simultaneously rather than in isolation.

In the context of knowledge sharing, these challenges carry particular significance because the value of a KS platform depends fundamentally on sustained, voluntary participation from contributors who are often heterogeneous in technical literacy, motivation, and institutional affiliation. Scalability constraints directly threaten the viability of KS platforms that must accommodate high-frequency contributions from large distributed user communities such as open research repositories or enterprise knowledge bases. Integration complexity is especially acute in institutional KS environments, including academic repositories, healthcare knowledge systems, and government information platforms, where blockchain adoption must align with pre-existing governance frameworks, data standards, and regulatory obligations. Economic sustainability barriers are disproportionately severe for non-commercial KS ecosystems, including open science platforms and public knowledge commons, where token-based cost recovery models conflict with open-access mandates. Addressing these barriers in KS contexts requires solution frameworks that extend beyond technical optimization to encompass the organisational, regulatory, and community-governance dimensions that determine whether a blockchain-based KS platform can achieve and sustain real-world adoption among knowledge contributors.

D. RQ4: Benefits of Blockchain Consensus Mechanisms

Despite the challenges identified in RQ3, the literature consistently documents substantial benefits justifying continued research and deployment (Table XII). A strong core cluster of security, transparency, and decentralization co-occurs across the

majority of studies, supported by three domain-specific secondary benefits.

TABLE XII. FREQUENCY ANALYSIS: DOCUMENTED BENEFITS (RQ4)

Rank	Benefit Category	Count	Percentage	Interpretation for Results Section
1	Enhanced Data Security & Integrity	65	84.4%	Most documented benefit (84%) blockchain's cryptographic foundation and consensus mechanisms directly address the core trust problem in knowledge sharing: data integrity and tamper resistance
2	Improved Transparency & Trust	53	68.8%	Second (69%) immutable audit trails and publicly verifiable transactions address provenance and accountability requirements in collaborative knowledge ecosystems
3	Decentralized Control & Censorship Resistance	49	63.6%	Third (64%) elimination of centralized gatekeepers enables democratic access, censorship resistance, and reduced dependency on single platform operators
4	Smart Contract Automation & Efficiency	15	19.5%	Fourth (19%) automated enforcement of sharing rules, licensing agreements, and contribution protocols via smart contracts; lower frequency reflects implementation maturity
5	Economic Incentive Alignment	13	16.9%	Fifth (17%) token economies and reputation systems create sustainable motivation for knowledge contribution; significant for open knowledge platforms
6	Interoperability & Data Portability	6	7.8%	Sixth (8%) cross-chain and cross-platform data portability remains an emerging benefit; lowest frequency reflects current technical limitations in cross-chain standardization

1) Enhanced data security and integrity: Enhanced data security and integrity was the most consistently documented benefit, reported in 65 studies (84%), the highest frequency across all four research questions. This reflects the direct correspondence between blockchain's cryptographic architecture and the core security requirements of knowledge platforms. Benefits span protection against unauthorized modification in healthcare [41], [40], [36], resistance to Sybil attacks in IoT networks [32], [58], and verifiable provenance in supply chain management [28], [35]. Co-occurrence with transparency (47 studies, 61%) and decentralized control (43 studies, 56%) confirms that security is achieved through simultaneous complementary properties, directly validating the multi-mechanism trust model identified in RQ1. This benefit appeared across all domains and all six years, confirming a robust and reproducible finding.

2) Improved transparency and trust: Improved transparency was documented in 53 studies (69%). Blockchain's immutable audit trail enables independent verification that knowledge has not been altered, suppressed, or misattributed. Benefits were demonstrated in cross-organizational research sharing [34], [76], public health communication [41], and academic provenance [69], [32]. Co-occurrence with decentralized control in 36 studies (47%) reinforces a key distinction: a centralized system can provide audit logs, but only a decentralized system ensures those logs cannot be selectively suppressed, particularly significant for multi-institutional consortia and inter-government platforms.

3) Decentralized control and censorship resistance: Decentralized control and censorship resistance was reported in 49 studies (64%). Eliminating centralized gatekeepers enables democratic knowledge curation [28], [51], [39], censorship-resistant archiving in politically sensitive contexts [32], [35], and cross-border sharing that bypasses jurisdictional restrictions [94], [36]. The three-way co-occurrence of security, transparency, and decentralization in 33 studies (43%) confirms that these are deeply interdependent; decentralization is the architectural foundation on which transparency and security claims rest. A centralized platform offering security and transparency still allows a single operator to modify logs or override policies.

4) Smart contract automation and efficiency: Smart contract automation was documented in 15 studies (19%), enabling programmable enforcement of sharing protocols, royalty management [39], [40], access control [77], [58], and self-executing inter-organizational agreements [44], [75]. Co-occurrence with security (14 studies, 18%) and decentralization (12 studies, 16%) reflects that smart contracts are only trustworthy when executing on a secure, decentralized platform. Lower frequency relative to the primary trio reflects the greater implementation complexity requiring domain expertise beyond standard blockchain adoption.

5) Economic incentive alignment: Economic incentive alignment appeared in 13 studies (17%), demonstrating how token rewards and reputation mechanisms sustain quality contributions. Applications include academic curation with governance tokens [28], [73], vehicular micropayments [53], [54], and supply chain contribution tracking [37], [78]. Co-occurrence with security (13 studies, 17%) and transparency (11 studies, 14%) confirms that incentive systems are most

effective on a foundation of verifiable security and transparent tracking; participants only trust systems they believe will accurately record and fairly reward their contributions.

6) Interoperability and data portability: Interoperability and data portability appeared in the fewest studies (6 studies, 8%), reflecting the emerging and technically challenging nature of cross-chain exchange. Applications include multi-database architectures [34], [40], aviation knowledge systems [79], and heterogeneous IoT networks [56], [74]. Low frequency reflects current technical limitations in cross-chain standardization rather than absence of interest; cross-chain bridge proposals in 2024–2025 studies suggest this benefit will feature more prominently in the next generation of research.

The documented benefits form a coherent and mutually reinforcing value proposition. Security (84%), transparency (69%), and decentralization (64%) represent blockchain's core architectural contribution to knowledge trust. Smart contracts (19%), economic incentives (17%), and interoperability (8%) are application-layer amplifiers for domain-specific contexts. The finding that 83% of studies documented two or more concurrent benefits and 52% documented three or more confirms that blockchain delivers compounding rather than marginal value, with the security-transparency-decentralization cluster forming a comprehensive alternative to centralized platform trust models.

In the context of knowledge sharing, these documented benefits map directly onto the specific trust deficits that have historically limited participation in open, distributed, and cross-organizational KS platforms. Enhanced data security and integrity (84%) directly address contributor concerns about unauthorized modification of submitted knowledge, a critical deterrent for researchers, clinicians, and domain experts who risk reputational harm from misrepresented contributions. Improved transparency and auditability (69%) resolve attribution ambiguity, enabling contributors to trust that their intellectual work is permanently and publicly traceable, which is particularly significant in academic and research KS contexts where provenance constitutes a form of professional currency. Decentralized control and censorship resistance (64%) remove structural dependence on platform operators whose policies may suppress, selectively curate, or commercially exploit contributed knowledge, replacing operator trust with mathematically and consensus-enforced guarantees. Smart contract automation and economic incentive alignment together create the conditions for self-sustaining KS communities where contribution quality is structurally rewarded rather than merely assumed. Critically, the co-occurrence of security, transparency, and decentralization in 43% of studies confirms that these benefits are architecturally interdependent in KS contexts: transparency is only meaningful if audit records themselves cannot be selectively suppressed, which requires decentralization, which in turn depends on a secure consensus mechanism. This finding positions blockchain not merely as a technology upgrade for existing KS platforms but as a structurally superior trust architecture for knowledge-sharing systems where participant autonomy, contribution integrity, and governance fairness are foundational requirements.

VI. Discussion

A. Principal Findings

This systematic review of 77 peer-reviewed studies (2020–2025) provides the first comprehensive PRISMA-guided synthesis of blockchain consensus mechanisms as trust enablers in knowledge-sharing platforms. Four integrated findings emerge from cross-RQ analysis.

1) Blockchain trust is a multi-mechanism, co-occurring phenomenon: Blockchain consensus mechanisms enhance trust through a coherent cluster of six co-occurring mechanisms, not a single dominant property (RQ1). Distributed verification (78%), transparency (52%), and cryptographic security (39%) form the primary architectural triad, with immutability (32%), economic incentives (27%), and smart contracts (19%) providing supporting layers. Co-occurrence of distributed verification with transparency (44%) and cryptographic security (31%) confirms these operate as a system. The implication for platform design is direct: implementing blockchain for a single benefit is likely to underdeliver; maximum trust enhancement requires deploying multiple complementary mechanisms simultaneously.

2) PBFT dominates, but no single consensus protocol fits all knowledge contexts: The consensus mechanism landscape reveals domain-driven diversity rather than protocol convergence (RQ2). PBFT leads (23%) for permissioned networks requiring deterministic finality; novel and hybrid mechanisms (17%) are growing rapidly. Critically, 49% of studies did not specify a consensus mechanism, operating at the architectural level without protocol detail. Trust enhancement claims made without specifying the underlying mechanism cannot be reproduced, compared, or validated. The shift toward PoS (8%, growing from 2022) and hybrid mechanisms reflects the field's response to energy and scalability constraints: a dynamic landscape where PoW is declining, and energy-efficient alternatives are gaining ground.

3) Scalability and integration are compounding, not sequential, barriers: Blockchain knowledge sharing deployments face compounding rather than isolated barriers (RQ3). 49% of studies reported two or more concurrently. Scalability (52%) and integration complexity (30%) co-occurred in 19% of studies, creating a significant dual barrier: insufficient throughput combined with difficult legacy integration. Energy (29%), economic sustainability (26%), governance uncertainty (14%), and usability (10%) further compound these in domain-specific ways. All six challenge categories increased from 2020 to 2025, an expanding rather than contracting barrier landscape, indicating that current technical progress has not yet resolved core adoption barriers.

4) Benefits are compounding and strongly cluster around security, transparency, and decentralization: The benefit analysis reveals a powerful, cohesive value proposition (RQ4): 83% of studies documented two or more concurrent benefits, and the security-transparency-decentralization cluster co-occurred in 43% of studies. This confirms that blockchain's

value derives from simultaneously delivering multiple trust properties that centralized systems can only partially replicate. Smart contract automation (19%), economic incentives (17%), and interoperability (8%) are domain-specific amplifiers. Together, the four findings form a coherent picture: blockchain delivers multi-mechanism trust (RQ1) through protocol-diverse implementations (RQ2), overcoming compounding barriers (RQ3) to deliver compounding benefits (RQ4).

B. Practical Implications

The findings carry concrete implications for four stakeholder groups: platform designers, knowledge sharing practitioners, policymakers, and researchers.

1) For platform designers and system architects: Platform designers should treat distributed verification, transparency, and cryptographic security as a non-negotiable architectural trio; implementing one without the others weakens the overall trust model. For mechanism selection, RQ2 evidence supports PBFT or BFT variants for permissioned consortium networks with institutionally identified participants, and PoA or reputation-based hybrids for open platforms where identity verification is impractical. PoW should be reserved for high-security, low-frequency timestamping only. Layer-2 scalability solutions and legacy integration planning should be treated as first-class design constraints from the outset rather than retrofits.

2) For knowledge sharing practitioners and organisations: Organisations should temper adoption expectations: scalability affects over half of current implementations and integration complexity is the fastest-growing challenge. A hybrid approach applying blockchain selectively to the highest trust knowledge assets while retaining conventional systems for routine transactions is supported by the evidence as a pragmatic strategy. Total cost of ownership analyses should account for transaction fees, storage costs, and governance overhead before committing to deployment. The benefit evidence (Finding 4) provides a strong case for adoption where verifiable provenance, censorship resistance, and cross-organizational trust are genuine operational requirements.

3) For policymakers and institutional decision-makers: Governance and regulatory uncertainty (14% of studies, rising to 5 in 2025) signals an urgent need for institutional frameworks. Policymakers should prioritize standards for smart contract enforceability, cross-jurisdictional data governance for blockchain knowledge records, and certification frameworks for permissioned platforms. Sustainability criteria should be embedded in institutional procurement policies, favouring PBFT and PoS over PoW-based alternatives in publicly funded knowledge infrastructure.

4) For researchers and the academic community: The most significant implication for researchers is the empirical gap identified by RQ2: 49% of studies omitted consensus mechanism specification, preventing cross-study comparison and evidence accumulation. A minimum reporting standard covering mechanism identification, selection justification, and protocol-level performance metrics is urgently needed. The underrepresentation of usability research (10% of challenge studies) relative to technical challenges also indicates a systematic bias toward engineering concerns that should be corrected through dedicated human-computer interaction research.

C. Future Research Directions

Six future research directions are identified from the cross-RQ synthesis, ordered by the strength of supporting evidence.

1) Consensus mechanism reporting standards: The most immediately actionable need is the development of minimum reporting standards for blockchain knowledge sharing studies. With 49% of studies omitting consensus mechanism specification, cumulative evidence on which mechanisms produce which outcomes in which contexts cannot be built. A reporting checklist analogous to PRISMA should specify mechanism name, version, configuration parameters, node count, fault tolerance threshold, and performance benchmarks as mandatory elements. Validating such a checklist through a Delphi study would represent a high-impact methodological contribution.

2) Scalability solutions for knowledge-intensive blockchains: Scalability constraints affect 52% of implementations yet remain unresolved after six years of research. Future work should investigate layer-2 technologies, state channels, sidechains, and rollup architectures specifically for knowledge sharing workloads, which differ from financial use cases in transaction size, frequency, and multi-party complexity. Sharding adapted to knowledge graph structures and hybrid on-chain/off-chain architectures anchoring provenance on-chain while storing content off-chain represent particularly promising directions.

3) Energy-efficient consensus for knowledge platforms: Energy consumption persisted as a challenge across all study years (29% of studies), intensified by growing sustainability reporting requirements. Future research should conduct controlled comparisons of energy consumption across consensus families (PoS, PBFT, PoA, DPoS) under knowledge sharing workloads and establish per-transaction energy benchmarks. Post-quantum cryptographic approaches to consensus offering potential security and efficiency improvements warrant early investigation given institutional adoption timescales of 10–15 years.

4) Empirical effectiveness studies with real deployments: The prevalence of simulation-based and conceptual studies highlights a critical need for empirical effectiveness research on real-world deployments. Controlled trials comparing blockchain versus traditional knowledge platforms on trust outcomes contribution rates, integrity incidents, user trust perceptions, and governance satisfaction would substantially strengthen the evidence base. Longitudinal studies are especially needed, as the 2020–2025 period captures mostly early-phase deployments where novelty effects may inflate reported benefits.

5) Cross-domain governance framework development: Governance uncertainty is the fastest-growing challenge (rising to 5 studies in 2025) yet receives the least solution-oriented attention. Future research should develop evidence-based governance frameworks addressing smart contract enforceability, cross-jurisdictional data sovereignty, stakeholder representation in decentralized governance, and dispute resolution for attribution conflicts. Comparative institutional analysis across healthcare, supply chain, and academic deployments would provide empirical grounding for such frameworks.

6) Usability and human factors research: The underrepresentation of usability research (10% of challenge studies) risks producing technically sophisticated but practically unusable platforms. Future research should apply human-computer interaction methodologies, user studies, cognitive walkthroughs, and participatory design to blockchain knowledge sharing interfaces, focusing on key management abstraction for non-expert users and progressive disclosure interfaces that communicate trust properties without requiring technical literacy, and accessibility studies examining whether blockchain knowledge platforms create or exacerbate digital exclusion for marginalized knowledge communities.

VII. Conclusion

This systematic review examined how blockchain consensus mechanisms enhance trust in knowledge sharing platforms, synthesizing evidence from peer-reviewed studies published between 2020 and 2025 across academic, corporate, and public sector contexts. The review followed PRISMA 2020 guidelines and addressed four research questions covering trust mechanisms, consensus algorithm adoption, implementation challenges, and documented benefits. The findings consistently confirm that blockchain consensus mechanisms do not operate through a single property but through a cluster of co-occurring mechanisms including distributed verification, transparency, cryptographic security, immutability, economic incentive alignment, and smart contract automation that together deliver compounding rather than marginal trust assurances. A diverse range of consensus algorithms is currently adopted, with PBFT-based variants dominant in permissioned environments and novel hybrid mechanisms growing rapidly, though a significant proportion of studies in the literature do not specify the consensus mechanism used, which represents a gap that limits cross-study comparability and reproducibility.

Despite these trust benefits, implementation remains constrained by compounding technical, economic, and governance barriers. Scalability, integration complexity, energy consumption, economic sustainability, regulatory uncertainty, and usability challenges frequently co-occur, and their prevalence has grown rather than declined as deployments have matured, indicating that current technical progress has not yet resolved the core adoption barriers. On the benefit side, enhanced data security, improved transparency, and decentralized control consistently emerge as the dominant and mutually reinforcing value proposition across all application domains and study years, with smart contract automation and economic incentive systems providing additional domain-specific value. Taken together, these findings position blockchain consensus mechanisms as a technically credible and theoretically well-grounded solution to the trust deficits of centralized knowledge sharing platforms, while acknowledging that substantial barriers to widespread institutional adoption remain.

This review has several limitations, including its restriction to three databases and English-language publications, the prevalence of simulation-based studies that limit generalizability to real-world deployments, and the significant proportion of studies that did not specify a consensus mechanism. Notwithstanding these constraints, the review makes substantive contributions by providing the first comprehensive PRISMA-guided synthesis specifically targeting consensus mechanisms in knowledge sharing contexts, establishing the multi-mechanism co-occurrence model of blockchain trust, and identifying the consensus mechanism reporting gap as a priority methodological issue. Future research should focus on developing minimum reporting standards for consensus mechanism specification, advancing scalability and energy-efficient protocol solutions, conducting empirical effectiveness studies in production deployments, and designing novel trust-weighted consensus mechanisms tailored to the specific governance and provenance requirements of knowledge sharing platforms. Addressing these priorities will advance the field toward blockchain knowledge sharing systems that are not only technically feasible but institutionally adoptable, user-accessible, and grounded in robust empirical evidence.

Acknowledgment

The authors acknowledge the use of AI-assisted tools in supporting the preparation of this manuscript. Scopus AI supported the development of preliminary conceptual maps, ChatGPT (version 5.2) assisted in constructing search strings, matrix tables, and organizing data analysis, and QuillBot was used for precise grammatical refinement and language editing. The author expresses gratitude for the financial support received from the Minister of Higher Education Malaysia under Universiti Kebangsaan Malaysia Research Grant with a Project Code: ZG-2022-010, which enabled this research to be completed.

References

[1] A. Bharadwaj, O. A. El Sawy, P. A. Pavlou, and N. Venkatraman, "Digital business strategy: Toward a next generation of insights," MIS Quarterly, vol. 37, no. 2, pp. 471–482, 2022.

[2] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application," Journal of Medical Systems, vol. 45, no. 1, pp. 1-35, 2021.

[3] N. Alkhater, R. Walters, and G. Wills, "An empirical study of factors influencing cloud adoption among private sector organisations," Telematics and Informatics, vol. 58, pp. 101537, 2021.

[4] R. Zhao, Y. Wang, X. Yao, J. Zheng, T. Chen, and C. Liu, "Exploring the large language models for knowledge graph completion," IEEE Transactions on Big Data, vol. 10, no. 1, pp. 1–14, 2023.

[5] A. A. Monrat, O. Schelen, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE Access, vol. 7, pp. 117134-117151, 2020.

[6] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Sok: Consensus in the age of blockchains," Proceedings of the 1st ACM Conference on Advances in Financial Technologies, 183–198, 2020.

[7] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, "Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities," IEEE Access, vol. 7, pp. 85727–85745, 2021.

[8] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," Expert Systems with Applications, vol. 154, pp. 113385, 2020.

[9] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology (NIST), 2021.

[10] M. Belotti, N. Bozic, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," IEEE Communications Surveys and Tutorials, vol. 21, no. 4, pp. 3796-3838, 2020.

[11] H. Zhao, X. Huang, and X. Sun, "A survey on blockchain consensus mechanisms: Recent advances and challenges," Future Generation Computer Systems, vol. 122, pp. 45-65, 2021.

[12] H. R. Hasan and K. Salah, "Blockchain-based solution for COVID-19 digital medical passports," IEEE Access, vol. 8, pp. 222093-222108, 2020.

[13] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on platforms and challenges," Computer Networks, vol. 176, pp. 107287, 2020.

[14] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352-375, 2020.

[15] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," Healthcare, vol. 9, no. 1, pp. 56, 2021.

[16] A. Pal, C. K. Tiwari, and S. Behal, "Blockchain technology: Security issues, healthcare applications, challenges, and future trends," Electronics, vol. 10, no. 16, pp. 2022, 2021.

[17] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," IEEE Access, vol. 7, pp. 10127-10149, 2020.

[18] M. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, "Eductx: A blockchain-based higher education credit platform," IEEE Access, vol. 6, pp. 5112-5127, 2020.

[19] M. Xu, X. Chen, and G. Kou, "A systematic review of blockchain," Financial Innovation, vol. 5, pp. 27, 2021.

[20] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," Information Processing & Management, vol. 58, no. 1, pp. 102397, 2021.

[21] B. Kitchenham, "Guidelines for performing systematic literature reviews in software engineering," Technical Report EBSE 2007-001, Keele University, 2007.

[22] T. Long and M. Godfrey, "An evaluation tool to assess the quality of qualitative research studies," International Journal of Social Research Methodology, vol. 7, no. 2, pp. 181–196, 2004.

[23] C. Lockwood, Z. Munn, and K. Porritt, "Qualitative research synthesis: Methodological guidance for systematic reviewers utilising meta-aggregation," International Journal of Evidence-Based Healthcare, vol. 13, no. 3, pp. 179–187, 2015.

[24] K. Shahzad, L. Xiaofeng, F. Shahzad, and S. Riaz, "Internal determinants of knowledge sharing: A systematic review of ten years empirical research (2008–2017)," Journal of Information Science, vol. 45, no. 2, pp. 247–268, 2021.

[25] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications," Telematics and Informatics, vol. 36, pp. 55-81, 2020.

[26] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, and D. Moher, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," BMJ, 372, n71, 2021.

[27] J. Popay, H. Roberts, A. Sowden, M. Petticrew, L. Arai, M. Rodgers, and N. Britten, "Guidance on the conduct of narrative synthesis in systematic reviews," ESRC Methods Program, 2006.

[28] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Computing Surveys, vol. 52, no. 3, pp. 1–34, 2022.

[29] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, vol. 107, pp. 841–853, 2023.

[30] J. Song, F. H. Bai, Y. Zhu, T. Shen, and A. K. Xie, "An improved-poa consensus algorithm for blockchain-empowered data sharing system," ACM International Conference Proceeding Series, 2022.

[31] L. Chen, X. Zhang, and Z. X. Sun, "Blockchain data sharing query scheme based on threshold secret sharing," Security and Communication Networks, 2022.

[32] T. Alladi, V. Chamola, R. M. Parizi, and K. K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," IEEE Access, vol. 7, pp. 176935–176951, 2022.

[33] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," Journal of Medical Systems, vol. 42, no. 8, pp. 136, 2023.

[34] K. Hao, J. C. Xin, Z. Q. Wang, Z. M. Yao, and G. R. Wang, "Efficient and secure data sharing scheme on interoperable blockchain database," IEEE Transactions on Big Data, 2023.

[35] K. P. Zheng, L. J. Zheng, J. Gauthier, L. Y. Zhou, Y. G. Xu, A. Behl, and J. Z. Zhang, "Blockchain technology for enterprise credit information sharing in supply chain finance," Journal of Innovation and Knowledge, 2022.

[36] A. Khan, S. Bourouis, G. Aldehim, S. S. Alotaibi, M. A. Alohali, and Z. Hamad, "Blockchain-based privacy-preserving healthcare data sharing using federated learning," Computers in Biology and Medicine, vol. 169, pp. 107857, 2025.

[37] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K. K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," Journal of Network and Computer Applications, vol. 149, pp. 102471, 2025.

[38] A. M. Boljam, S. G. R. Bojja, V. Saini, V. R. R. Alluri, and H. U. H. Mohammed, "Optimizing AI algorithms using blockchain for secure and transparent data sharing," 2025 International Conference on Computing Technologies and Data Communication, ICCTDC 2025, 2025.

[39] J. Rachana, S. M. Naik, and R. V. Sampangi, "Blockchain-enabled intellectual property management for collaborative knowledge ecosystems," Journal of Intellectual Property Law & Practice, vol. 20, no. 1, pp. 45–62, 2025.

[40] A. Garg, H. Makhija, V. Biswas, P. Varma, Z. Homavazir, A. Wunnava, and K. Tejesh, "Blockchain-based health informatics systems for secure patient data sharing and interoperability; [sistemas informáticos sanitarios basados en blockchain para compartir datos de pacientes de forma segura e interoperable]," Seminars in Medical Writing and Education, 2024.

[41] M. A. Yuman, R. W. Ahmad, A. A. Almazroi, and K. Salah, "Blockchain-based patient-centric health data management," Journal of Biomedical Informatics, vol. 141, pp. 104373, 2025.

[42] Y. Teng, S. J. Ma, Q. Qian, and G. Wang, "Seir-diffusion modeling and stability analysis of supply chain finance based on blockchain technology," Heliyon, 2024.

[43] G. Y. Zhu, Z. Y. Gu, and Y. H. Dai, "Construction of a human resource sharing system based on blockchain technology," Information (Switzerland), 2023.

[44] C. Z. Lai, Z. Ma, R. Guo, and D. Zheng, "Secure medical data sharing scheme based on traceable ring signature and blockchain," Peer-to-Peer Networking and Applications, 2022.

[45] F. J. Shang and X. X. Deng, "A data sharing scheme based on blockchain for privacy protection certification of internet of vehicles," Vehicular Communications, 2025.

[46] M. Mukhedkar, P. Kote, M. Zonde, O. Jadhav, V. Bhasme, and N. A. Dawande, "Advanced and secure data sharing scheme with blockchain and IPFS: A brief review," 2024 15th International Conference on Computing Communication and Networking Technologies, ICCCNT 2024, 2024.

[47] A. Liu, X. B. Chen, G. Xu, Z. Wang, Y. Sun, Y. H. Wang, and H. M. Feng, "Qbiov: A secure data sharing scheme for the internet of vehicles based on quantum-enabled blockchain," Quantum Information Processing, 2024.

[48] J. T. Fu, L. P. Zhang, L. X. Wang, and F. Q. Li, "Bct: An efficient and fault tolerance blockchain consensus transform mechanism for IoT," IEEE Internet of Things Journal, 2023.

[49] Q. Dang, W. Shang, L. Yan, and X. Liu, "Power business data sharing system based on blockchain and cryptography technology," Proceedings - 2021 International Conference on Networking, Communications and Information Technology, NetCIT 2021, 2021.

[50] L. Cai, A. J. Liu, and Y. C. Yan, "Blockchain consensus algorithm for supply chain information security sharing based on convolutional neural networks," Scientific Reports, 2025.

[51] L. P. F. Wu, W. S. Lu, R. Zhao, J. Y. Xu, X. Li, and F. Xue, "Using blockchain to improve information sharing accuracy in the onsite assembly of modular construction," Journal of Management in Engineering, 2022.

[52] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "Blockchain integration to enhance trust in supply chain sharing platforms: A systematic review," International Journal of Production Economics, vol. 255, pp. 108712, 2023.

[53] G. X. Du, Y. J. Cao, J. Li, Y. Zhuang, X. F. Chen, Y. B. Li, and J. H. Chen, "A blockchain-based trust-value management approach for secure information sharing in internet of vehicles," IEEE Internet of Things Journal, 2024.

[54] K. Yan, W. P. Ma, Q. Yang, S. H. Sun, and W. W. Wang, "Info-chain: Reputation-based blockchain for secure information sharing in 6g intelligent transportation systems," IEEE Internet of Things Journal, 2024.

[55] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," Sensors, vol. 18, no. 11, pp. 3894, 2022.

[56] F. Bai, T. Shen, Z. Yu, K. Zeng, and B. Gong, "Trustworthy blockchain-empowered collaborative edge computing-as-a-service scheduling and data sharing in the IIoE," IEEE Internet of Things Journal, 2022.

[57] E. Sun, K. Meng, R. Yang, Y. Zhang, and M. Li, "Research on distributed data sharing system based on internet of things and blockchain," Journal of Systems Science and Information, 2021.

[58] A. Cholke, V. V. Mandhare, and P. S. Vikhe, "A review of security and information control in blockchain-integrated IoT applications," 2024 IEEE International Conference on Blockchain and Distributed Systems Security, ICBDS 2024, 2024.

[59] S. D. Okegbile, J. Cai, and A. S. Alfa, "Practical byzantine fault tolerance-enhanced blockchain-enabled data sharing system: Latency and age of data package analysis," IEEE Transactions on Mobile Computing, 2024.

[60] H. Wang, Y. Wang, Z. Cao, Z. Li, and G. Xiong, "An overview of blockchain security analysis," Cybersecurity, vol. 4, no. 1, pp. 34, 2025.

[61] M. Y. Hou, T. Y. Kang, and L. Guo, "A blockchain based architecture for IoT data sharing systems," 2020 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2020, 2020.

[62] C. Cao and X. Zhu, "Credit evaluation and blockchain consensus for supply chain," 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics, ICCCBDA 2021, 2021.

[63] E. Lee, Y. Yoon, G. M. Lee, and T. W. Um, "Blockchain-based perfect sharing project platform based on the proof of atomicity consensus algorithm," Tehnicki Vjesnik, 2020.

[64] X. X. Zhang, X. R. Zhu, and I. Ali, "Performance analysis of IOTA tangle and a new consensus algorithm for smart grids," IEEE Internet of Things Journal, 2024.

[65] X. Bu, J. Wu, and G. Li, "Repshardchain: A reputation-based sharding blockchain system in smart city," 2022 2nd International Conference on Intelligent Technology and Embedded Systems, ICITES 2022, 2022.

[66] T. E. Zheng, J. H. Wu, and G. S. Li, "Iov data sharing scheme based on the hybrid architecture of blockchain and cloud-edge computing," Journal of Cloud Computing, 2023.

[67] J. Cui, F. Q. Ouyang, Z. B. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," IEEE Transactions on Intelligent Transportation Systems, 2022.

[68] P. V. K. Reddy, R. K. Murugesan, and M. S. Elayidom, "A framework for blockchain-based secure and transparent pharmaceutical supply chain," Journal of Pharmaceutical Sciences, vol. 113, no. 3, pp. 845–856, 2024.

[69] A. Ural, K. K. R. Choo, and A. Dehghantanha, "A blockchain-based trusted decentralized data sharing system for the internet of things," Future Generation Computer Systems, vol. 141, pp. 286–298, 2023.

[70] A. Bouzegag, D. Tandjaoui, and I. Romdhani, "Blockchain-based trust management for IoT systems: Challenges and solutions," Journal of Network and Computer Applications, vol. 199, pp. 103304, 2022.

[71] F. Erfan, M. Bellaiche, and T. Halabi, "Game-theoretic designs for blockchain-based IoT: Taxonomy and research directions," Proceedings - 4th IEEE International Conference on Decentralized Applications and Infrastructures, DAPPS 2022, 2022.

[72] H. J. Ju, X. L. Zhang, H. Y. Jia, X. Zhang, E. Zhu, K. Yan, and J. Guo, "A survey on efficient consensus mechanism for electricity information acquisition system," 9th International Conference on Smart Grid, icSmartGrid 2021, 2021.

[73] Y. C. Zhu, "Research on evolutionary game of digital twin data information sharing based on blockchain technology," Measurement and Control (United Kingdom), 2025.

[74] B. Cao, L. Zhang, D. Li, D. Feng, and W. Cao, "Intelligent offloading in multi-access edge computing: A state-of-the-art review and framework," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1709–1727, 2022.

[75] Z. H. Wang, Y. H. Xu, J. H. Liu, Z. Y. Li, Z. M. H. Li, H. Y. Jia, and D. H. Wang, "An efficient data sharing scheme for privacy protection based on blockchain and edge intelligence in 6g-vanet," Wireless Communications and Mobile Computing, 2022.

[76] T. Zhang, Y. Wang, L. Huang, and T. Zhou, "Enabling trust in cross-organizational data sharing for EMU maintenance: A double-blockchain solution," Journal of Information and Knowledge Sharing, 2023.

[77] M. A. Nasab, M. Shojafar, Z. Pooranian, M. Conti, and R. Tafazolli, "Btem: Belief based trust evaluation mechanism for wireless sensor networks," Future Generation Computer Systems, vol. 96, pp. 605–616, 2022.

[78] A. Jabbar, P. Iqbal, and P. Bhatt, "Blockchain for supply chain management: A strategic perspective for sustainable development," International Journal of Production Research, vol. 58, no. 7, pp. 2063–2081, 2022.

[79] H. Seike, Y. Aoki, and N. Koshizuka, "Quantitative analysis of blockchain consensus effects on dataspace transaction latency," 2025 IEEE International Conference on Big Data (BigData), 2025.

[80] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," IEEE Communications Surveys and Tutorials, 2022.

[81] P. N. Bathula and M. Sreenivasulu, "An integrated blockchain framework for secure data sharing in IoT fog computing," Tsinghua Science and Technology, 2025.

[82] W. Bouzegag, L. Belaiche, L. Kahloul, and H. Bennoui, "Leveraging formal methods to blockchain consensus protocols: A scoping literature review," 2022 International Symposium on iNnovative Informatics of Biskra, ISNIB 2022, 2022.

[83] H. Cao, H. Cao, and G. Liang, "Data mining model of internet of things based on blockchain technology," ACM International Conference Proceeding Series, 2022.

[84] P. G. Chen, F. H. Bai, T. Shen, B. Gong, L. Zhang, L. Huang, and M. Waqas, "Scca: A slicing-and coding-based consensus algorithm for optimizing storage in blockchain-based IoT data sharing," Peer-to-Peer Networking and Applications, 2022.

[85] P. Y. Chen, Y. L. Chen, C. Y. Tan, Y. X. Yang, B. Li, and J. C. Huang, "Slicing PBFT consensus algorithm based on VRF," Proceedings - 2024 IEEE International Conference on Blockchain, Blockchain 2024, 2024.

[86] Y. W. Chen, B. W. Hu, H. J. Yu, Z. M. Duan, and J. X. Huang, "A threshold proxy re-encryption scheme for secure iot data sharing based on blockchain," Electronics (Switzerland), 2021.

[87] Q. Fan, Y. Xin, B. Jia, Y. Zhang, and P. X. Wang, "Cobats: A novel consortium blockchain-based trust model for data sharing in vehicular

networks," IEEE Transactions on Intelligent Transportation Systems, 2023.

[88] J. Fu, W. Zhou, and J. Xu, "Design of improved PBFT algorithm based on aggregate signature and node reputation," Intelligent and Converged Networks, 2023.

[89] X. Fu, H. M. Wang, P. C. Shi, and X. H. Zhang, "Teegraph: A blockchain consensus algorithm based on TEE and DAG for data sharing in IoT," Journal of Systems Architecture, 2022.

[90] A. R. Harish, X. L. Liu, X. Wang, S. L. Pan, H. N. Dai, M. Li, and G. Q. Huang, "Blockchain FOR LOGISTICS 4.0: A SYSTEMATIC REVIEW AND PROSPECTS," Transportation Research Part E: Logistics and Transportation Review, 2025.

[91] R. Jabbar, E. Dhib, A. B. Said, M. Krichen, N. Fetais, E. Zaidan, and K. Barkaoui, "Blockchain technology for intelligent transportation systems: A systematic literature review," IEEE Access, 2022.

[92] X. D. Jia, X. M. Song, and M. Sohail, "Effective consensus-based distributed auction scheme for secure data sharing in internet of things," Symmetry, 2022.

[93] S. A. Khan, S. Balusamy, M. P. A. Saviour, S. Bojjawar, C. M. Chidambaranathan, and D. S. Sofia, "Integrating blockchain technology with artificial intelligence to create scalable, reliable, and open decision support systems," 2025 Global Conference in Emerging Technology, GINOTECH 2025, 2025.

[94] Z. Li, J. Li, F. Nie, B. Zhang, and J. Guo, "Optimization of blockchain consensus mechanism based on DPOS," Proceedings of SPIE - The International Society for Optical Engineering, 2023.

[95] A. Liu, Q. Zhang, S. W. Xu, H. M. 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, 2024.

[96] Y. Liu, J. Gao, Y. Lu, R. Cao, L. Yao, Y. Xia, and D. Han, "Lightweight blockchain-enabled secure data sharing in dynamic and resource-limited UAV networks," IEEE Network, 2024.

[97] Z. Ma, F. Richard Yu, X. Jiang, and A. Boukerche, "Trustworthy traffic information sharing secured via blockchain in VANETs," DIVANet 2020 - Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, 2020.

[98] Y. Meng, "Research on trusted exchange and data traceability mechanism of health information system integrating blockchain and internet of things," 2025 Asia Conference on Energy Conversion Systems and Power Electronics (AECSPE), 2025.

[99] S. S. F. Nasab, D. Bahrepour, and S. R. K. Tabbakh, "A review on secure data storage and data sharing technics in blockchain-based IoT healthcare systems," 2022 12th International Conference on Computer and Knowledge Engineering, ICCKE 2022, 2022.

[100] R. G. Reddy, P. S. Pateja, A. Patel, G. Palaniappan, and B. Rajendran, "Identifying sybil attacks in blockchain networks through behavioral analysis and zero knowledge proof implementations," 2024 1st International Conference on Data, Computation and Communication, ICDCC 2024, 2024.

[101] F. Ren and Z. Liang, "A data sharing privacy protection model based on federated learning and blockchain technology," International Journal of Advanced Computer Science and Applications, 2024.

[102] J. Ryu, Y. Lee, and Y. Yoon, "Blockchain model for reliable consensus algorithm on the autonomous driving data management," Digest of Technical Papers - IEEE International Conference on Consumer Electronics, 2024.

[103] A. Sarfaraz, R. K. Chakrabortty, and D. L. Essam, "The implications of blockchain-coordinated information sharing within a supply chain: A simulation study," Blockchain: Research and Applications, 2023.

[104] A. Shrivastava, R. Praveen, M. MuhsnHasan, S. Bansal, S. P. Dwivedi, and V, A, "Blockchain-powered secure data sharing in AI driven smart cities," 2025 International Conference on Computing and Communications (COMPUTINGCON), 2025.

[105] K. Singh, A. S. Rajawat, S. B. Goyal, and H. N. Waked, "A blockchain-based intelligent framework for secure and sustainable knowledge sharing in organizational systems," Procedia Computer Science, 2025.

[106] O. Ural and K. Yoshigoe, "Survey on blockchain-enhanced machine learning," IEEE Access, 2023.

[107] S. van Engelenburg, B. Rukanova, W. Hofman, J. Ubacht, Y. H. Tan, and M. Janssen, "Aligning stakeholder interests, governance requirements and blockchain design in business and government information sharing," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020.

[108] H. H. Wang, C. P. Wang, K. Zhou, D. Y. Liu, X. L. Zhang, and H. B. Cheng, "Tebchain: A trusted and efficient blockchain-based data sharing scheme in UAV-Assisted IoV for disaster rescue," IEEE Transactions on Network and Service Management, 2024.

[109] H. Wang, D. Mao, Z. Chen, H. Rao, and Z. Li, "Blockchain-based decentralized federated learning model," 2023 4th International Conference on Information Science, Parallel and Distributed Systems, ISPDS 2023, 2023.

[110] Q. Wang, Z. Wu, and Y. Lu, "A multi-layer secure sharing framework for aviation big data based on blockchain," Future Internet, 2025.

[111] W. Z. Wang, D. X. Tian, X. T. Duan, and J. S. Zhou, "Rpbft: A scalable consensus mechanism for large blockchain systems," Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 2024.

[112] Y. Wang and X. H. Zhao, "Ig-pgft: A secure and efficient intelligent grouping PBFT consensus algorithm for the industrial internet of things," Cluster Computing, 2025.

[113] Z. Wang, B. Wen, and Z. Luo, "Towards on blockchain data privacy protection with cryptography and software architecture approach," Communications in Computer and Information Science, 2020.

[114] F. Y. Xu, S. H. Hu, Y. Sun, X. X. Hu, J. Qi, Y. F. Sun, and Z. J. Dong, "Fdss: Flight data sharing scheme based on blockchain with dynamic, secure and efficient consensus algorithm," Computer Networks, 2025.

[115] Y. Yuman, S. B. Goyal, A. S. Rajawat, M. Kumar, A. Shankar, F. Alhayan, and S. Basheer, "A blockchain-based solution for enhancing the efficiency and security of healthcare knowledge sharing systems in the era of industry 4.0," Wireless Networks, 2025.

[116] S. F. Zhang, Y. Liu, and X. R. Chen, "Bit problem: Is there a trade-off in the performances of blockchain systems?," Communications in Computer and Information Science, 2020.

[117] X. F. Zhang, W. B. Xia, Q. M. Cui, X. F. Tao, and R. P. Liu, "Efficient and trusted data sharing in a sharding-enabled vehicular blockchain," IEEE Network, 2023.

[118] X. Zhang, Q. Guo, X. Pan, D. Bai, X. Pan, and J. Lv, "Study on the development status and prospect of blockchain technology in the energy field," ACM International Conference Proceeding Series, 2022.

[119] X. Zhang, M. Xue, and X. Miao, "A consensus algorithm based on risk assessment model for permissioned blockchain," Wireless Communications and Mobile Computing, 2022.

[120] Y. H. Zhang, Y. T. Wu, T. Li, H. Zhou, and Y. L. Chen, "Vertical federated learning based on consortium blockchain for data sharing in mobile edge computing," CMES - Computer Modeling in Engineering and Sciences, 2023.

[121] X. K. Zhou, W. Huang, W. Liang, Z. Yan, J. H. Ma, Y. Pan, and K. I. K. Wang, "Federated distillation and blockchain empowered secure knowledge sharing for internet of medical things," Information Sciences, 2024.