A Comprehensive Review of Blockchain and Smart Contracts: Foundations, Applications, and Technical Challenges

P. Shylaja[1] and J. S. Jayasudha[2]

ABSTRACT

Blockchain technology has emerged as a pivotal and transformative force, establishing transparent, secure, and decentralized frameworks for transaction management. Its core strengths include immutability, data decentralization, and consensus validation, alongside the automation provided by self-executing smart contracts. This review examines its foundational technologies, diverse applications, and associated challenges. Blockchain demonstrates profound potential across sectors like finance (e.g., Anti-Money Laundering and fraud reduction), education (credential verification), healthcare (secure record management), and the Metaverse (verifiable digital asset ownership via non-fungible tokens). However, adoption is significantly hindered by critical issues, including scalability bottlenecks, the energy inefficiency of protocols like Proof of Work, and security risks stemming from smart contract flaws, with case-based testing revealing up to 40% of public contracts have exploitable vulnerabilities. Recent advancements in high-throughput rollups and formal verification mitigate these risks. This coincides with a 2025 shift toward structured legal mandates, such as the EU's MiCA, India's VDA policy, and the U.S. GENIUS and CLARITY Acts. Therefore, future research must prioritize enhancing smart contract verification, developing energy-efficient consensus mechanisms, cross-chain interoperability, and fostering the continued alignment of supportive legal and regulatory frameworks.

Keywords: Blockchain, Consensus mechanism, Decentralization, Distributed ledger technology, Metaverse, Smart contract

[1]Department of Computer Science, Central University of Kerala & Department of IT, Kannur University, Kerala, India
[2]Department of Computer Science, Central University of Kerala, Kasaragod, India

Correspondence to:
J. S. Jayasudha,
jayasudhajs@cukerala.ac.in

Additional material is published online only. To view please visit the journal online.

Cite this as: Shylaja P and Jayasudha JS. A Comprehensive Review of Blockchain and Smart Contracts: Foundations, Applications, and Technical Challenges. Premier Journal of Science 2025;15:100257

DOI: https://doi.org/10.70389/PJS.100257

Peer Review
Received: 19 December 2025
Last revised: 5 January 2026
Accepted: 7 January 2026
Version accepted: 2
Published: 31 January 2026

Ethical approval: N/a
Consent: N/a
Funding: N/a
Conflicts of interest: N/a
Author contribution:
P. Shylaja and J. S. Jayasudha – Conceptualization, Writing – original draft, review and editing

Introduction

Blockchain, a decentralized data storage mechanism, is undergoing rapid large-scale integration within the digital economy. It ensures secure, transparent transaction management. Initially, cryptocurrencies such as Bitcoin utilized decentralized storage to mitigate the need for a centralized authority.[1–7] Various applications—such as the Internet of Things (IoT), the Metaverse, finance, education, and supply chains—leverage this technology to enhance operational transparency.[8–11] A continuous requirement for sector-specific customization drives the demand for blockchain.

By integrating with IoT, blockchain provides a robust framework for secure data transmission.[12–14] Its time-stamping property facilitates enhanced traceability.[15] Unlike centralized systems, blockchain architecture prevents single points of failure because no central authority exerts unilateral control over transactions. Furthermore, the principle of decentralization distributes data across multiple secure nodes. Data once entered into the ledger is immutable, establishing a trustworthy agreement and preventing fraud.[16–20] Blockchain technology enables users to autonomously verify records by eliminating the need for central mediators, providing a decentralized framework that is transformatively applied across diverse sectors—including agriculture, government, education, supply chain logistics, and financial services.[17,21–26]

Blockchain ecosystems are underpinned by economic models centered on cryptocurrencies and non-fungible tokens (NFTs) that establish digital asset value and verifiable ownership, alongside smart contracts that automate agreements to reduce intermediaries and enhance efficiency. Consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), further define these models by incentivizing network security and transaction validation, despite challenges like the high cost and energy inefficiency of some existing protocols.[1–6,27]

Blockchain technology integrates economic models driven by cryptocurrencies and NFTs to establish verifiable digital ownership, leveraging smart contracts for intermediary-free automation and consensus protocols like PoW or PoS for transaction security, despite persistent challenges including scalability bottlenecks and energy inefficiencies, where the immutability of flawed code can lead to critical security vulnerabilities.

At the technical core, smart contracts and consensus algorithms are central to blockchain's operation.[7–9,28] Blockchain technology, initially the backbone for cryptocurrencies, now offers secure, transparent, and decentralized frameworks that are transformatively applied across diverse industries including healthcare for secure and private record management,[1,2,6,29–37] finance for real-time transaction tracking and fraud prevention[6,38] education for robust credential verification,[7,28,39] the IoT for secure data transmission and authentication,[11,13,28,40–42] vehicular networks for improved message verification,[17,25,43,44] manufacturing industry[45] and the Metaverse for verifiable digital asset ownership and economic exchange.[3,4,14,34,46–48]

Blockchain acts as a foundational technology for emerging trends like Web3 and Decentralized Autonomous Organizations (DAOs), establishing secure, transparent, and decentralized frameworks for managing transactions and governance. Smart contracts, a core component, enable the automation of agreements, enhance efficiency, foster trust, and provide

Guarantor: J. S. Jayasudha
Provenance and peer-review: Unsolicited and externally peer-reviewed
Data availability statement: N/a

operational mechanisms for these decentralized ecosystems, including verifiable digital asset ownership in Web3 and governance within DAOs.

Public blockchains, often embodying open-source principles, face notable challenges regarding scalability and energy inefficiency, whereas private or permissioned implementations can mitigate these by assuming a degree of trust and employing hybrid consensus protocols. Nevertheless, widespread adoption across all blockchain types is consistently hindered by significant smart contract vulnerabilities, persistent regulatory ambiguity and governance issues.[7,49]

This systematic review adheres to the PRISMA 2020 reporting guidelines to synthesize literature published between 2016 and 2025, focusing on the rapid growth of blockchain and smart contract research. The methodology includes peer-reviewed journal articles, conference proceedings, and book chapters in English, specifically including studies that offer theoretical or empirical contributions to blockchain design, applications, performance, or security. Conversely, the review excludes non-peer-reviewed sources—such as blogs, white papers, and industry reports—and studies focusing strictly on cryptocurrency without technical blockchain discussion. The operational workflow involved identifying records across multiple databases, followed by the removal of duplicate records and a two-stage screening process (abstract/content screening and full-text evaluation) to ensure alignment with the predefined scope. The sources organize extracted data into a structured schema based on thematic areas, including Foundational Role and Infrastructure, Enhancing Security, and domain-specific implementations in Healthcare, Education, Finance, and the Metaverse. While a PRISMA-compliant flow diagram (Figure 1) is utilized to maintain transparency in study selection. Furthermore, the quality of evidence is evaluated through a "Critique of Evidence Quality and Contradictory Findings," which identifies critical gaps such as the "verification gap" in smart contract reliability and the "rigidity paradox" of immutable code.

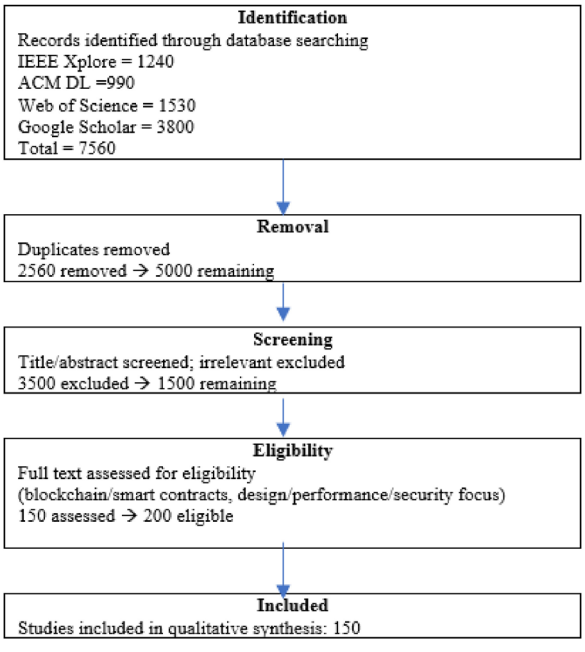

Fig 1 | PRISMA flow diagram

This comprehensive review is structured to elevate novelty by providing a focused synthesis on emerging applications and critical cross-cutting challenges, specifically integrating the rapidly developing area of the Metaverse and establishing a structured analytical synthesis of domain-specific contributions.

The second section presents the literature review in detail, followed by a summary table highlighting key contributions. It also includes discussions on major themes, explores diverse applications and associated challenges, and concludes with insights into future research directions.

Literature Review

The literature on blockchain is indeed vast and multifaceted, encompassing foundational technologies and diverse, domain-specific implementations. To provide a structured understanding of this extensive field, this review organizes the material around key thematic areas that capture the breadth and depth of current developments. The thematic subsections that follow, such as Foundational Role and Infrastructure, Enhancing Security, Interoperability, and Future Outlook in the Metaverse, Smart Contracts, and specific applications in Healthcare, Education, and Finance and IoT.

Foundational Role and Infrastructure

The foundational elements of blockchain are indeed anchored in principles of decentralized consensus, transparency, and cryptographic security. These core concepts have evolved rapidly from Bitcoin's original implementation to become more sophisticated, modular, and suitable for domain-specific blockchain platforms. Early investigations into blockchain, particularly by Yli-Huumo et al.,[5] pointed to a dominant research focus on Bitcoin and its underlying consensus mechanisms, such as PoW, as well as transaction throughput. Crosby et al.[36] reinforced this foundation by detailing how blockchain integrates cryptographic hashing, distributed consensus, and time-stamping to ensure immutable transaction histories. Their work effectively laid the groundwork for more nuanced studies of blockchain architecture

Building upon the foundational elements of blockchain—decentralized consensus, transparency, and cryptographic security, Swan et al.[50] significantly extended this technical foundation by proposing a three-tiered view of blockchain's evolution, which has profoundly guided much of the conceptual framing in recent blockchain innovations. This model categorizes blockchain into Blockchain 1.0 for cryptocurrencies, Blockchain 2.0 for smart contracts, and Blockchain 3.0 for decentralized applications. For example, experimental studies showed PoS could reduce energy use by over 70%, though it required enhanced fault tolerance mechanisms.[51–54]

Collectively, this foundational work underpins the entire ecosystem of blockchain research, providing both the technical vocabulary and conceptual models that continue to profoundly influence domain-specific implementations today.[6–13,55–57] This foundational research laid the groundwork for the evolution of blockchain's infrastructure, emphasizing core components such as consensus algorithms, distributed ledger architectures,[58–62] and decentralized network design.[63] Early studies were largely driven by the operational structure of Bitcoin, which initially gained prominence as the backbone technology for Bitcoin and other cryptocurrencies, prompting researchers to meticulously investigate its inherent scalability bottlenecks and system latency.[9,12]

Review by Yli-Huumo et al.[5] notably highlighted this overwhelming early academic focus on Bitcoin and the limitations of its underlying PoW protocol, particularly concerning its consensus layer and transaction throughput. However, their review also indicated a subsequent shift in attention toward smart contracts, permissioned blockchain architectures, and domain-specific applications.Researchers have actively addressed these concerns by focusing on identity federation, cross-chain communication, and adaptive governance frameworks to meet the dynamic needs of immersive environments.[64–66]

For interoperability and cross-platform identity management, Wang et al.[67] introduced a multi-identifier resolution protocol. This system enables users to seamlessly navigate between different virtual worlds without creating redundant digital identities, thereby reducing fragmentation and strengthening trust in identity management systems. Furthermore, studies highlight cross-platform asset portability as a key benefit, allowing users to maintain a unified identity and carry their owned digital items across various virtual environments, which significantly enhances interoperability and user retention.[68]

Regarding governance frameworks, Filippi et al.[69] put forth the concept of "Lex Cryptographia". Howell et al.[63] and Etemadi et al.[70] further explored the organizational and governance challenges inherent in blockchain-based platforms. They identified stakeholder trust, regulatory ambiguity, and community-based governance as primary hurdles to adoption.[71] Etemadi et al.,[72] using Interpretive Structural Modeling (ISM), specifically concluded that legal clarity and user confidence are prerequisites for sustainable metaverse ecosystems.[3,4] These studies collectively emphasize that the future success of blockchain in the Metaverse hinges not only on technological maturity but also on social, legal, and institutional alignment, with community consensus being central to sustainable development.[69]

The immutable ledger inherent in blockchain plays a critical role in addressing security and transparency concerns in digital transactions.[71,72] It ensures that ownership and transaction histories are tamper-proof and auditable, which is vital in a space where real monetary value is associated with virtual assets.[73] Overall, the reviewed studies confirm that blockchain is not merely a supportive technology but a foundational infrastructure for the decentralized evolution of the Metaverse, indispensable for a secure and interoperable virtual ecosystem by supporting identity assurance, asset ownership, and decentralized financial interactions. However, persistent challenges include the need for user-friendly wallet interfaces, greater regulatory clarity, and a careful balance between transparency and data privacy.[74,75]

Artificial Intelligence is identified as a future direction for enhancing blockchain applications, making them easier to use and enabling advanced functionalities like AI-driven analytics and edge computing in industrial and IoT environments. This integration also extends to smart contract privacy protection, intelligent data trading modes utilizing machine learning, and safeguarding patient data-sharing through federated learning in sectors such as the Metaverse, education, and healthcare.[70,71,75]

Regulatory and legal frameworks for blockchain ecosystems are currently evolving, with regulatory ambiguity identified as a primary hurdle hindering widespread adoption across various applications like the Metaverse and education. Proposals such as "Lex Cryptographia," which aims to embed legal compliance directly into smart contracts, offer promising governance models, but their institutional adoption remains slow, underscoring the ongoing need for greater clarity and a balance between transparency and data privacy.[65,76]

The early blockchain era was a "Wild West" where users relied on their own wits and unwritten codes, new 2025 regulations represent the establishment of a formal state government. Laws like MiCA and the CLARITY Act act as the official maps and town charters, providing the clear "rules of the road" and legal safety nets that allow established commercial businesses and institutional investors to build and trade with confidence.[77,78]

Smart Contracts

Smart contracts are fundamentally self-executing programs stored on a blockchain that are designed to automatically enforce agreements once predefined conditions are met.[2,10,39,45,79] They are an integral mechanism for automating transactions, reducing the reliance on intermediaries, and ensuring contract integrity in both public and private blockchain environments.[10,75,76,80–82] These programs are crucial for enhancing working efficiency, fostering trust, and improving overall operational efficiency within digital ecosystems, as they facilitate, verify, or enforce agreements directly without requiring third-party involvement.[10]

However, a significant challenge with smart contracts is their rigidity and susceptibility to coding flaws, which consequently pose considerable security risks. Researchers have identified common vulnerabilities, particularly in Ethereum-based smart contracts, including reentrancy attacks, timestamp dependence, and unchecked external calls. This highlights a critical need for secure coding practices, comprehensive

testing, and the development of formal verification tools.[10,83] Despite recommendations for utilizing such tools and sandbox environments for rigorous testing of complex logic before deployment, their adoption remains limited or sparse.[14] Case-based testing has even revealed that up to 40% of smart contracts on public blockchains have exploitable vulnerabilities.[14,83] Furthermore, the inherent immutability of faulty smart contracts poses serious risks once they are deployed.[34]

Despite these challenges, smart contracts have been successfully applied across various sectors, demonstrating their utility and transformative potential. In education, they have been deployed in academic transcript verification systems to improve real-time validation and eliminate manual credential authentication.[7,84] For instance, Hakiki et al.[7] implemented smart contracts for issuing and validating digital diplomas, which significantly reduced the risk of fraud in this domain.[83] In supply chain management, Taherdoost et al.[10] demonstrated their value in automating logistics, ensuring transparent and tamper-resistant tracking of goods.

Furthermore, smart contracts have been utilized in healthcare to streamline medical claims processing and consent handling, aiming to reduce fraud and administrative overhead.[75,85] In finance, especially within decentralized financial infrastructures (DeFi), smart contracts contribute to real-time transaction tracking, fraud prevention, and enhanced transparency.[6,54] For the Metaverse, smart contracts are part of the underlying mechanisms that support decentralized identity (DID) systems and NFTs, which in turn enable verifiable user representation, secure asset ownership, and transparent digital economies within immersive virtual environments.[3,4,14,48]

Blockchain systems face several smart contract vulnerabilities. 2016 DAO hack stole 3.6 million ETH and 2017 Parity wallet bug froze 500,000 ETH, making the fund inaccessible.[86]

Block chain and Digital Ledger in Healthcare

Healthcare systems are currently facing significant challenges related to data privacy, interoperability, and secure record-keeping. In response, blockchain technology offers a solution by enabling the creation of decentralized, tamper-proof medical data management platforms.[70,87–89]

Several researchers have proposed and developed various blockchain-enabled Electronic Health Record (EHR) models to address these issues. For instance, Kuo et al.,[46] Oladele et al.[1] and Panwar et al.[35] have designed EHR solutions that specifically aim to tackle challenges such as data fragmentation and unauthorized access within healthcare. Despite these advantages, the full adoption of blockchain in healthcare still faces significant barriers, particularly concerning scalability and integration with legacy health systems.[28] The substantial size of medical imaging files and the computational overhead associated with blockchain consensus mechanisms present logistical difficulties.[54,57,58,65,67,90] To overcome these issues, researchers have suggested hybrid storage models, where only essential data is stored on-chain, with the remainder managed through secure off-chain solutions. These ongoing innovations affirm blockchain's transformative potential for healthcare, which is contingent upon the continued development of lightweight, privacy-preserving protocols.[91]

Smart Contracts for Education Administration

In the education sector, blockchain technology has been employed to enhance trust, transparency, and efficiency in academic credentialing.[92,93] The immutability of blockchain records ensures that once a credential is issued, it cannot be altered or falsified.[94] This feature has found strong utility in verifying degrees, transcripts, and professional certifications.[94,95]

Turkanovic et al.[96] introduced EduCTX, a global blockchain-based platform for managing student credits and qualifications. The system offers a decentralized alternative to conventional academic databases, allowing educational institutions, students, and employers to verify credentials instantly. Zou et al.[83] proposed a scalable blockchain infrastructure tailored for large universities, utilizing off-chain storage and on-chain hashes to preserve both scalability and verifiability.

Turkanovic et al.[96] and Hakiki et al.[7] introduced systems like EduCTX that store and verify academic credentials, offering real-time verification and reducing fraud. These studies highlight blockchain's potential to simplify cross-border recognition of academic records, although standardization and adoption remain hurdles.

Supply Chain and Asset Tracking in IoT

Finance and the IoT are among the earliest and most mature domains for blockchain adoption. In finance, blockchain ensures tamper-proof transaction logs, enhances transparency, and supports secure peer-to-peer value exchange.[97,98] Sazu et al.,[6] Udeh et al.,[99] and Panwar et al.[35] demonstrated that blockchain enhances Anti-Money Laundering (AML) compliance, improves Know Your Customer (KYC) protocols, and reduces transaction costs and settlement times in cross-border payments.

In the IoT landscape, the integration of blockchain addresses longstanding challenges such as data integrity, device authentication, and secure communication. Dorri et al.,[34] Tyagi et al.,[11] Liu et al.,[100] and Laghari et al.[101] developed lightweight blockchain models suitable for resource-constrained environments like smart homes and precision agriculture. Their systems enhanced data authenticity and offered robust audit trails for sensor-generated information.

Lu et al.,[49] Xu et al.[102] and Yang et al.[88] applied blockchain to vehicular networks, where real-time communication and safety are paramount. Their frameworks improved message verification in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) exchanges, contributing to safer and more resilient transportation systems. As these case studies reveal, blockchain's decentralized trust model complements the distributed

DOI: https://doi.org/10.70389/PJS.100257 | Premier Journal of Science 2025;15:100257

nature of IoT and finance systems, although concerns about scalability, latency, and interoperability must still be addressed through ongoing innovation. The finance and IoT sectors are among the earliest adopters of blockchain. In finance, blockchain increases transparency, reduces fraud, and automates compliance. Sazu et al.,[6] Udeh et al.,[99] and Panwar et al.[35] demonstrated blockchain's effectiveness in anti-fraud systems, cross-border payments, and AML compliance.

In IoT, Dorri et al.,[34] Tyagi et al.,[11] Liu et al.,[100] and Laghari et al.[101] developed and evaluated blockchain applications in smart homes, agriculture, and energy monitoring. These implementations enhanced data authenticity and system resilience, thereby reinforcing the value of blockchain in distributed, autonomous networks. Blockchain solutions face significant scalability bottlenecks and latency issues in high-throughput environments like global supply chains and IoT networks, particularly due to limitations in transaction throughput and energy inefficiency of existing consensus mechanisms. To address these, researchers propose hybrid consensus protocols, multi-chain/sharded architectures, and hybrid storage models utilizing off-chain solutions to reduce latency and improve efficiency.[6–17,36,50,99,103]

Figure 2, explicitly mentioned as a pie chart extracted from the reference collected, is highly relevant for visually illustrating the core applications of blockchain today, thereby consolidating and reinforcing the diverse domain-specific applications.

Table 1 provides an overview of significant blockchain advancements and their key contributors. It systematically lists specific works or methods by various authors and their corresponding contributions to the field. These contributions cover diverse areas, such as enabling identity assurance and asset verification in the Metaverse, highlighting AML enhancements in financial systems, and improving trust and transparency in education through blockchain-based transcript validation. Table 1 provides a crucial overview of prominent blockchain contributions and their respective authors, systematically listing specific works or methods and their impact on the field, thereby illustrating the breadth of blockchain research from its fundamental technical underpinnings to highly specialized, domain-specific applications. The contributions highlighted span diverse areas, including the Metaverse, where Jin et al.[3] enabled identity assurance and asset verification through DID systems and Bhattacharjee et al.[79] ensured authenticity and interoperability of digital assets via Blockchain-NFT integration. In the financial sector, Sazu et al.[6] focused on AML enhancements, while Udeh et al.[99] reported a significant 30% reduction in fraud, and Panwar et al.[35] increased transaction speed in cross-border payments. For education administration, Hakiki et al.[7] improved trust and transparency with blockchain-based transcript validation, and Turkanovic et al.[96] developed the EduCTX system to prevent fraud and simplify international credential verification. Applications in IoT and supply chain management are also noted, with Taherdoost et al.[10] demonstrating automation with smart contracts and Dorri et al.[34] creating lightweight IoT blockchain for smart homes. The table further includes contributions to healthcare, such as Kuo et al.[46] designing secure EHR architectures and Engelhardt et al.[55] addressing interoperability challenges in EHR systems. Finally, critical areas of consensus mechanisms and governance are covered by authors like Xiao et al.[104] who evaluated trade-offs in scalability and performance, Khan et al.[105] who revealed smart contract vulnerabilities, and De Filippi et al.[69] who introduced the "Lex Cryptographia" concept for legal compliance.

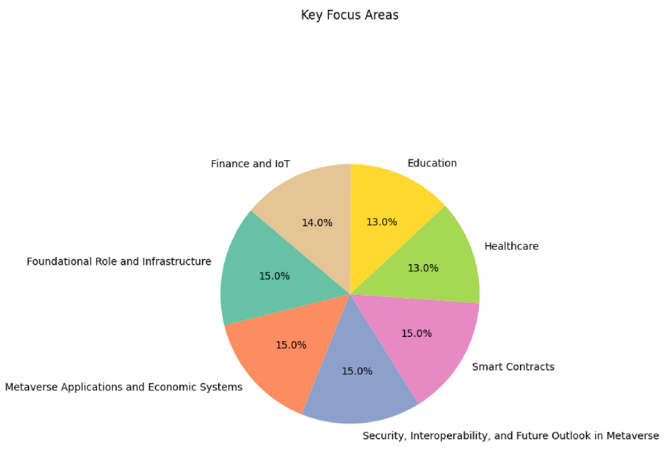

Fig 2 | Core applications of blockchain

Discussion

Blockchain technology has fundamentally evolved from a foundational infrastructure to enable diverse, domain-specific applications, leveraging its core strengths in transparency, trust, decentralization, and fraud mitigation.[106–110] While the literature confirms blockchain's immense potential, particularly in enabling secure, peer-to-peer transactions, it simultaneously uncovers recurring technical and governance limitations that hinder widespread adoption.[55,101,111]

Domain-Specific Applications and Challenges

In the Finance sector, strong maturity is evident, with blockchain significantly contributing to real-time transaction transparency, AML compliance, and automated auditing systems. Udeh et al.[99] reported a 30% reduction in fraud through real-time tracking. However, financial implementations often rely on public blockchains, exposing them to scalability bottlenecks and energy inefficiency. Educational and credentialing systems benefit from the immutability and auditability of academic records, noticeably reducing credential fraud. The primary challenge here remains system interoperability across institutions and regions. For the Metaverse, blockchain is foundational, securing virtual identity, enforcing ownership rights through NFTs, and ensuring cross-platform asset portability. Success, however, hinges on resolving evolving legal and governance frameworks and achieving regulatory clarity. In Healthcare, secure medical records are promised, but

Table 1 | Overview of prominent block chain contributions

Area	Author(s)	Work/Method	Contribution
Metaverse, Identity and Digital Assets	Jin et al.[3]	DID systems in the Metaverse	Enabled identity assurance and asset verification
	Mourtzis et al.[4]	Blockchain in industrial metaverse	Improved collaboration in virtual prototyping
	Wang et al.[14]	Multi-identifier resolution framework	Proposed cross-chain identity linking solution
	Bhattacharjee et al.[79]	Blockchain-NFT integration	Ensured authenticity and interoperability of digital assets
Foundational Concepts and Review	Yli-Huumo et al.[5]	Systematic mapping study	Identified Bitcoin's dominance in early blockchain research
	Crosby et al.[36]	Technical overview of blockchain	Highlighted decentralization and cryptographic security
	Swan et al.[50]	Theoretical extrapolation of blockchain applications	Predicted future role in governance, identity, and education
Consensus and Scalability	Xiao et al.[104]	Consensus comparison (PoW, PoS, PBFT)	Evaluated trade-offs in scalability, performance, and energy
	Nguyen et al.[106]	Survey of consensus algorithms	Identified gaps in throughput and security
	Abreu et al.[107]	Stress-testing blockchain configurations	Supported hybrid consensus adoption
Smart Contract Security and Governance	Khan et al.[105]	Smart contract vulnerabilities	Revealed critical flaws in Ethereum contracts
	De Filippi et al.[69]	Lex Cryptographia concept	Embedded legal compliance into smart contracts
	Howell et al.[63]	Blockchain governance analysis	Identified adoption challenges and stakeholder conflicts
	Etemadi et al.[70]	Blockchain adoption barriers	Used ISM to rank trust, cost, and expertise as top issues
Finance and Fraud Reduction	Sazu et al.[6]	Financial systems review	Highlighted AML enhancements through blockchain
	Udeh et al.[99]	Nigerian bank blockchain case	Reported 30% fraud reduction via real-time tracking
	Panwar et al.[35]	Cross-border payment automation	Increased transaction speed and reduced errors
Education Administration	Hakiki et al.[7]	Blockchain-based transcript validation	Improved trust and transparency in education
	Turkanovic et al.[96]	EduCTX credit record system	Prevented fraud and simplified international verification
	Zou et al.[108]	Scalable educational blockchain	Hybrid storage to handle large academic datasets
Healthcare and EHR Systems	Kuo et al.[46]	Blockchain EHR architecture	Enabled secure and patient-centric health records
	Panwar et al.[109]	Health data on IBM blockchain	Integrated patient privacy with cloud storage
	Engelhardt et al.[55]	Review of EHR blockchain systems	Addressed interoperability challenges
	Bazel et al.[110]	Blockchain for claim processing	Reduced insurance fraud and delays
IoT, Supply Chain and Vehicular Networks	Taherdoost et al.[10]	Supply chain automation with smart contracts	Reduced transaction time and manual verification
	Dorri et al.[34]	Lightweight IoT blockchain	Enabled access control in smart homes
	Tyagi et al.[11]	Agricultural blockchain system	Improved data trust and traceability
	Lu et al.[17]	Blockchain-based vehicular trust	Improved message integrity in VANETs
	Laghari et al.	Blockchain in smart metering	Prevented billing fraud and enhanced transparency

barriers persist with the scalability of large data and the underutilization of privacy-enhancing techniques like zero-knowledge proofs.

Consensus Algorithms Comparison

Blockchain's reliance on trustlessness and security results in quantitative trade-offs regarding efficiency and performance. Consensus mechanisms like PoW and PoS present significant trade-offs.

PoW ensures immutable transaction histories but is known for its limitations in transaction throughput and energy inefficiency. Early academic research was dominated by its study.[62,63,104] PoS offers a more energy-efficient alternative, with experimental studies showing it could reduce energy use by over 70% compared to PoW, although it requires enhanced fault tolerance mechanisms.[104] Xiao et al.[104] specifically evaluated trade-offs in scalability, performance, and energy across various algorithms. The trend points toward hybrid or application-specific consensus protocols in permissioned environments to address scalability bottlenecks and high costs. Other distributed ledger technologies (DLTs), such as Directed Acyclic Graph (DAG)-based systems, aim for higher throughput, scalability, and improved energy efficiency compared to traditional blockchain. Table 2 compares different consensus algorithms.

Critique of Evidence Quality and Contradictory Findings

The evidence suggests a critical gap between theoretical security and practical implementation quality. The security landscape reveals a duality: while immutability generally enhances security, the immutability of faulty smart contracts poses serious risks.[14,83]

Evidence Critique (Vulnerability): Case-based testing has shown that up to 40% of smart contracts on public blockchains have exploitable vulnerabilities,

DOI: https://doi.org/10.70389/PJS.100257 | Premier Journal of Science 2025;15:100257

Table 2 | Consensus algorithms comparison[62,63,104]

Algorithm Class	Throughput/Latency	Energy Efficiency	Fault Tolerance/Security Profile
PoW	Low/Limited: Transaction bottlenecks and high latency.	Very Low: Known for high operational costs and inefficiency.	High: Dominates early research; ensures immutable histories through massive hashing.
PoS	Higher/Scalable: Addresses PoW's throughput limitations.	High: Experimental studies show over 70% reduction in energy use.	Moderate: Requires "enhanced fault tolerance" mechanisms to maintain security.
Hybrid/ Sharded (e.g., OmniLedger)	Very High: Optimized for high-throughput environments like global supply chains.	Variable: Aims to mitigate the high costs of public protocols.	Assumed Trust: Often used in permissioned chains where a degree of trust is assumed.

including reentrancy attacks and coding flaws. This high rate reveals a significant deficit in current development and quality assurance practices.[9,10,14,69,83,105]

Evidence Critique (Verification Gap): Despite consensus among researchers recommending formal verification tools and sandbox environments for rigorous testing, their adoption remains limited or sparse.[14,83]

Contradictory Findings (Governance): The goal of seamless, automated legal compliance through models like "Lex Cryptographia" is promising, yet institutional adoption remains slow. This is primarily due to persistent legal and regulatory ambiguity and the lack of standardization required for enforcement across jurisdictions.[69]

Contradictory Findings (Decentralization): Public blockchains embody open-source and full decentralization. However, to overcome their inherent scalability and energy inefficiency, many enterprises adopt private or permissioned implementations utilizing hybrid consensus, which assumes a degree of trust, contradicting the core promise of trustfulness. Table 3 lists implementation challenges while using block chain.

Between 2023 and 2025, blockchain systems have seen major practical advances in scalability, consensus, interoperability, and correctness assurance: Layer-2 rollups—especially zk-rollups and zkEVMs such as Polygon zkEVM and zkSync Era—have enabled thousands of transactions per second with lower fees and faster finality while retaining Ethereum compatibility; modern BFT-PoS consensus mechanisms like Tendermint (Cosmos), HotStuff (enterprise and permissioned chains), and Algorand's Pure Proof-of-Stake have delivered deterministic finality, high throughput, and energy efficiency in production networks; interoperability has matured through the Inter-Blockchain Communication (IBC) protocol, allowing secure, trust-minimized asset and data transfer across sovereign blockchains, supported by real-world multichain ecosystems; and formal verification tools such as Certora Prover, Solidity's SMTChecker, and protocol-level verification frameworks have been widely adopted by high-value DeFi and blockchain platforms to mathematically prove safety and correctness properties, demonstrably reducing critical bugs and smart-contract vulnerabilities—together showing measurable gains in performance, security, and reliability across deployed blockchain systems.[86,112]

Future research must focus on overcoming the persistent challenges to enable wider, safer adoption. Priority areas include:

1. Smart Contract Reliability: Research must focus on developing adequate protocols and enhancing the reliability of smart contract verification to mitigate the risk posed by exploitable coding flaws.[113–117]
2. Technological Efficiency: Focus on energy-efficient consensus mechanisms and cross-chain interoperability. This includes developing lightweight protocols for resource-constrained IoT devices.
3. Governance and Legal Clarity: Efforts must be made to increase the accessibility of regulatory frameworks and foster supportive legal and governance frameworks to resolve ambiguity.
4. Integration and System Design: Research should explore the integration of IoT and AI (AI-driven analytics, federated learning for data sharing) and address specific needs like secure patient data sharing in healthcare, provenance tracking in supply chains, and exploring blockchain-based voting systems.[118–121]

Challenges

The existing consensus mechanisms are very expensive that a common application cannot work with. Exchange of data from one platform to another is a hindrance. Wang et al.[14] and Howell et al.[63] proposed multi-identifier resolution systems and governance models to improve cross-chain integration, but technical complexity and lack of standardization remain barriers.[122–128]

Security vulnerabilities, particularly in smart contracts, represent an ongoing concern. Khan et al.[105] found that a significant number of smart contracts on Ethereum suffer from flaws like reentrancy bugs and logic errors. Wang et al.[14] recommended more comprehensive verification tools, but adoption remains limited.[129]

Table 3 | Practical implementation challenges of block chain[9,10,14,69,83,105]

Area of Contradiction	Blockchain Promise/Theoretical Benefit	Practical Reality/Contradictory Finding
Security and Immutability	Blockchain's immutability ensures tamper-proof transaction histories and data integrity.	The immutability of faulty smart contracts poses serious risks, with high rates of exploitable coding flaws (up to 40% vulnerability).
Governance and Trust	Blockchain fosters trust and enables autonomous, intermediary-free agreements.	Institutional adoption of robust governance models like "Lex Cryptographia" remains slow due to persistent regulatory ambiguity and lack of standardization.
Decentralization vs. Efficiency	Public blockchains embody open-source and full decentralization.	Public blockchains face notable challenges regarding scalability and energy inefficiency. To mitigate these issues, many implementations rely on private or permissioned chains using hybrid consensus, which assumes a degree of trust and sacrifices pure decentralization.

To address the multifaceted challenges of blockchain technology, researchers have identified specific technological, developmental, and regulatory pathways focused on enhancing system optimization and security.[55,130–135] Technological scalability and energy efficiency can be significantly improved by migrating from PoW to PoS, which experimental studies indicate can reduce energy consumption by over 70%, or by implementing sharded architectures like OmniLedger and Estuary to mitigate throughput bottlenecks. Furthermore, the high prevalence of smart contract vulnerabilities—affecting up to 40% of public contracts—requires the rigorous adoption of formal verification tools, sandbox testing environments, and secure coding practices to resolve the "rigidity paradox," where the immutability of flawed code creates permanent security risks.[101,111] In data-intensive sectors such as healthcare and education, pathways for resolution include the use of hybrid storage models that store essential cryptographic hashes on-chain while managing larger datasets off-chain, combined with the development of lightweight protocols specifically for resource-constrained IoT devices. Finally, overcoming regulatory ambiguity and fragmentation involves the implementation of "Lex Cryptographia"—embedding legal compliance directly into smart contract logic—and utilizing multi-identifier resolution protocols to facilitate seamless cross-chain interoperability and secure identity management.[9,69,136–140]

Conclusion

This comprehensive review provides a structured understanding of blockchain technology and smart contracts, encompassing foundational concepts, diverse applications, challenges, and future directions, based on peer-reviewed literature published from 2016–2025.[141,142] As a DLT, blockchain ensures secure, transparent transactions and is fundamental to emerging areas like the Metaverse and various sectors including finance, healthcare, and education. Smart contracts, while crucial for automation and efficiency, present a significant risk, as case-based testing shows up to 40% on public blockchains have exploitable vulnerabilities due to the limited or sparse adoption of formal verification tools.[143–145] Adoption is further hindered by scalability bottlenecks, the high energy inefficiency of PoW protocols—though PoS can reduce energy use by over 70%—and persistent regulatory ambiguity, despite the proposal of governance models like "Lex Cryptographia". Future blockchain research should focus on core technological advancements like energy-efficient consensus, cross-chain interoperability, and privacy-preserving mechanisms, while addressing sector-specific needs such as secure patient data sharing in healthcare, provenance tracking in supply chains, decentralized credential verification in education, and lightweight protocols for resource-constrained IoT devices.[146–149] Additionally, research must develop more reliable smart contract verification, foster supportive legal and governance frameworks, and explore blockchain-based voting systems to ensure transparent and secure public services.

Abbreviations

AML: Anti-Money Laundering
DAO: Decentralized Autonomous Organization
IoT: Internet of Things
NFT: Non-Fungible Token
PoW: Proof of Work
PoS: Proof of Stake
DLT: Distributed Ledger Technology

References

1 Oladele JK, Ojugo AA, Odiakaose CC, Emordi FU, Abere RA, Nwozor B, et al. BEHeDaS: a blockchain electronic health data system for secure medical records exchange. J Comput Theor Appl. 2024;1(3):231–42. https://doi.org/10.62411/jcta.9509
2 Khan SN, Loukil F, Guegan CG, Benkhelifa E, Bani Hani A. Blockchain smart contracts: applications, challenges, and future trends. Peer Peer Netw Appl. 2021;14(5):2901–25. https://doi.org/10.1007/s12083-021-01127-0
3 Jin B, Kuang H, Li X. Blockchain application in metaverse: a review. arXiv. 2025. arXiv:2504.11730. https://doi.org/10.48550/arXiv.2504.11730
4 Mourtzis D, Angelopoulos J, Panopoulos N. Blockchain integration in the era of industrial metaverse. Appl Sci. 2023;13(3):1353. https://doi.org/10.3390/app13031353
5 Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on blockchain technology?—A systematic review. PLoS One. 2016;11(10):e0163477. https://doi.org/10.1371/journal.pone.0163477
6 Sazu MH, Jahan SA. Impact of blockchain-enabled analytics as a tool to revolutionize the banking industry. Data Sci Finance Econ. 2022;2(3):275–93. http://doi.org/10.3934/DSFE.2022014
7 Hakiki M, Fadli R, Sabir A, Prihatmojo A, Hidayah Y, Irwandi. The impact of blockchain technology effectiveness in Indonesia's learning system. Int J Online Biomed Eng. 2024;20(7):47675. https://doi.org/10.3991/ijoe.v20i07.47675
8 Fartitchou M, Lamaakal I, El Makkaoui KE, El Allali ZE, Maleh Y. BlockMEDC: blockchain smart contracts for securing Moroccan higher education digital certificates. IEEE Access. 2025;13:39152–75. https://doi.org/10.1109/ACCESS.2025.3546177
9 Sari HB, Thalib EF, Meinarni NPS. Implementation of smart contracts in Indonesia: an analysis of financial regulation, taxation, and consumer protection. Notariil J Kenotariatan. 2024;9(2):65–70. https://doi.org/10.22225/jn.9.2.2024.65-70
10 Taherdoost H. Smart contracts in blockchain technology: a critical review. Information. 2023;14(2):117. https://doi.org/10.3390/info14020117
11 Tyagi AK, Ojugo AA, Agarwal D, Ahmed HFT. Blockchain—Internet of Things applications: opportunities and challenges for industry 4.0 and society 5.0. Sensors. 2023;23(2):947. https://doi.org/10.3390/s23020947
12 Ramachandran A, Kantarcioglu M. Using blockchain and smart contracts for secure data provenance management; 2017. https://doi.org/10.48550/arXiv.1709.10000
13 Tapscott D, Tapscott A. Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world. New York, NY: Penguin Random House; 2016.
14 Wang H, Ning H, Lin Y, Wang W, Dhelim S, Farha F, et al. MIS: a multi-identifier management and resolution system in the metaverse. ACM Trans Multimed Comput Commun Appl. 2024;20(7):1–25. https://doi.org/10.1145/3597641
15 Zamani M, Movahedi M, Raykova M. RapidChain: scaling blockchain via full sharding. In: Proceedings of the 2018 ACM SIGSAC conference computer and communications security; 2018. p. 1–16. https://doi.org/10.1145/3243734.3243798
16 Nanayakkara S, Perera S, Senaratne S, Weerasuriya GT, Bandara HMND. Blockchain and smart contracts: a solution for payment issues in construction supply chains. Informatics. 2021;8(1):36. https://doi.org/10.3390/informatics8020036
17 Lu Z, Qu G, Liu Z. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans Intell Transp Syst. 2018:1–17. https://doi.org/10.1109/TITS.2018.2874762O
18 jugo AA, Eboka AO. Evolutionary model for virus propagation on networks. Autom Control Intell Syst. 2015;3(4):56–63. https://doi.org/10.11648/j.acis.20150304.12

19 Akazue MI, Debekeme IA, Edje AE, Asuai C, Osame UJ. Unmasking fraudsters: ensemble feature selection to enhance random forest fraud detection. J Comput Theor Appl. 2023;1(2):201–11. https://doi.org/10.33633/jcta.v1i2.9462

20 Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: benefits, challenges, applications, and integration with cloud computing. Future Internet. 2022;14(11):341. https://doi.org/10.3390/fi14110341

21 Wang H, Ning H, Lin Y, Wang W, Dhelim S, Farha F, et al. A survey on the metaverse: the state-of-the-art, technologies, applications, and challenges. IEEE Internet Things J. 2023;10(16):14671–88. http://doi.org/10.1109/JIOT.2023.3278329

22 Wang J, Zhang T, Sebe N, Shen HT A survey on learning to hash. IEEE Trans Pattern Anal Mach Intell. 2017;40(4):769–90. http://doi.org/10.1109/TPAMI.2017.2699960

23 Liang X, Shetty S, Tosh D, Kamhoua C, Kwait K, Njilla L. ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing (CCGRID); 2017. p. 468–77. http://doi.org/10.1109/CCGRID.2017.8

24 Jia D, Lu K, Wang J, Zhang X, Shen X. A survey on platoon-based vehicular cyber-physical systems. IEEE Commun Surv Tutor. 2016;18(1):263–84. http://doi.org/10.1109/COMST.2015.2410831

25 Lyu Z. State-of-the-art human–computer interaction in metaverse. Int J Hum Comput Interact. 2024;40(21):6690–708. https://doi.org/10.1080/10447318.2023.2248833

26 Shin D. The actualization of meta affordances: conceptualizing affordance actualization in the metaverse games. Comput Hum Behav. 2022;133:107292. https://doi.org/10.1016/j.chb.2022.107292

27 Dang H, Dinh TTA, Loghin D, Chang EC, Lin Q, Ooi BC. Towards scaling blockchain systems via sharding. In: Proceedings of the international conference on data management; 2019. p. 123–40. https://doi.org/10.1145/3299869.3319889

28 Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In: Proceedings of the IEEE international conference on high performance computing & communications, data science & systems; 2016. p. 1392–3. http://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

29 Kishigami J, Fujimura S, Watanabe H, Nakadaira A, Akutsu A. The blockchain-based digital content distribution system. In: Proceedings of the IEEE 5th international conference big data cloud computing (BDCloud); 2015. p. 1–6. https://doi.org/10.1109/BDCloud.2015.35

30 Chen J, Micali S. Algorand. 2016. Available from: https://algorand.foundation/

31 Novikov SP, Kazakov OD, Kulagina NA, Azarenko NY. Blockchain and smart contracts in a decentralized health infrastructure. In: Proceedings of the IEEE international conference quality management, transport and information security, information technologies (IT&QM&IS); 2018. p. 1–5. http://doi.org/10.1109/ITMQIS.2018.8524970

32 Ojugo A, Eboka AO. Assessing users satisfaction and experience on academic websites: a case of selected Nigerian universities websites. Int J Inf Technol Comput Sci. 2018;10(10):53–61. https://doi.org/10.5815/ijitcs.2018.10.07

33 Udeze L, Eteng IE, Ibor AE. Application of machine learning and resampling techniques to credit card fraud detection. J Niger Soc Phys Sci. 2022;4(3):769. https://doi.org/10.46481/jnsps.2022.769

34 Dorri A, Kanhere SS, Jurdak R. Blockchain for IoT security and privacy: the case study of a smart home. In: Proceedings of the IEEE international conference on pervasive computing and communications workshops (PerCom Workshops); 2017. p. 618–23. http://doi.org/10.1109/PERCOMW.2017.7917634

35 Panwar A, Bhatnagar V. Distributed ledger technology (DLT): the beginning of a technological revolution for blockchain. In: Proceedings of the 2nd international conference on data, engineering and applications (IDEA); 2020. p. 1–6. https://doi.org/10.1109/IDEA50346.2020.9311342

36 Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: beyond Bitcoin. Appl Innov Rev. 2016;2:71–85.

37 Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of the IEEE symposium on security and privacy; 2016. p. 839–58. https://doi.org/10.1109/SP.2016.55

38 Khalid MI, Ehsan I, Al-Ani AK, Iqbal J, Hussain S. A comprehensive survey on blockchain-based decentralized storage networks. IEEE Access. 2023;11:10995–1015. https://doi.org/10.1109/ACCESS.2023.3240237

39 Verma G, Pathak N, Sharma N. A secure framework for health record management using blockchain in cloud environment. J Phys Conf Ser. 2021;1998(1):012019. https://doi.org/10.1088/1742-6596/1998/1/012019

40 Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016;4:2292–303. https://doi.org/10.1109/ACCESS.2016.2566339

41 Li S, Chen Y. Governing decentralized autonomous organizations as digital commons. J Bus Venturing Insights. 2024;21:e00450. https://doi.org/10.1016/j.jbvi.2024.e00450

42 Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Syta E, Ford B. OmniLedger: a secure, scale-out, decentralized ledger via sharding. In: Proceedings of the IEEE symposium on security and privacy; 2018. p. 583–98. http://doi.org/10.1109/SP.2018.000-5

43 Wright A, De Filippi P. Decentralized blockchain technology and the rise of Lex Cryptographia. SSRN Electron J. 2015. https://doi.org/10.2139/ssrn.2580664

44 Fan K, Xie Q, Zhang H, Li X. Dredas: decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. Future Gener Comput Syst. 2020;110:665–74. https://doi.org/10.1016/j.future.2019.10.014

45 Debe M, Salah K, Rehman MHU, Svetinovic D. Monetization of services provided by public fog nodes using blockchain and smart contracts. IEEE Access. 2020;8:20118–28. https://doi.org/10.1109/ACCESS.2020.2968573

46 Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc. 2017;24(6):1211–20. https://doi.org/10.1093/jamia/ocx068

47 Elsadig M, Alohali MA, Ibrahim AO, Abulfaraj AW. Roles of blockchain in the metaverse: concepts, taxonomy, recent advances, enabling technologies, and open research issues. IEEE Access; 2024. http://doi.org/10.1109/ACCESS.2024.3367014

48 Xiao Y, Li W, Liu J, Zhang H. A survey of distributed consensus protocols for blockchain networks. IEEE Commun Surv Tutor. 2020;22(2):1432–65. https://doi.org/10.1109/COMST.2020.2969706

49 Jabbar R, Ali S, Ahmed R. Blockchain technology for intelligent transportation systems: a systematic literature review. IEEE Access. 2022;10:20995–1031.

50 Swan M. Blockchain: blueprint for a new economy. Sebastopol, CA: O'Reilly Media; 2015.

51 Islam MN, Kundu S. Enabling IC traceability via blockchain pegged to embedded PUF. ACM Trans Des Autom Electron Syst. 2019;24(3):1–23. https://doi.org/10.1145/3315669

52 Novo O. Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. 2018;5(2):1184–95. https://doi.org/10.1109/JIOT.2018.2812239

53 Panja S, Bag S, Hao F, Roy B. A smart contract system for decentralized Borda count voting. IEEE Trans Eng Manag. 2020;67(4):1323–39. https://doi.org/10.1109/TEM.2020.2986371

54 Yu K, Tan L, Shang X, Huang J, Srivastava G, Chatterjee P. Efficient and privacy-preserving medical research support platform against COVID-19: a blockchain-based approach. IEEE Consum Electron Mag. 2020;9(3):23–9.

55 Engelhardt MA. Hitching healthcare to the blockchain: a privacy-preserving and integrative framework. IEEE Access. 2017;5:3836–54. https://doi.org/10.1109/ACCESS.2017.2685630

56 Xiong W, Xiong L. Smart contract based data trading mode using blockchain and machine learning. IEEE Access. 2019;7:102331–44. http://doi.org/10.1109/ACCESS.2019.2928325

57 Mondragon AEC, Coronado CEC, Coronado ES. Investigating the applicability of distributed ledger/blockchain technology in manufacturing and perishable goods supply chains. In: Proceedings of the IEEE conference on industrial electronics and

applications (ICIEA); 2019. p. 143–8. http://doi.org/10.1109/IEA.2019.8715005
58 Yuan H. Distributed ledger of blockchain enhance API supply chain social economical resilience. In: Proceedings of the international conference on economic management and green development; 2024. p. 1–10. http://doi.org/10.54254/2754-1169/104/2024ED0078
59 Kim S, Sarin A. Distributed ledger and blockchain technology: framework and use cases. J Invest Manag. 2018;16(4):45–61.
60 Liu X, Chen Y, Zhang W, Li X. Blockchain in digital cultural heritage resources: technological integration, consensus mechanisms, and future directions. NPJ Herit Sci. 2025;13(1):1–11. https://doi.org/10.1038/s41529-025-00215-0
61 Howell BE, Potgieter PH, Sadowski BM. Governance of blockchain and distributed ledger technology projects. ITS Aswan Conference Paper; 2019.
62 Li Y, Chen X, Liu J, Wang P. A blockchain-based decentralized federated learning framework with committee consensus. IEEE Netw. 2020;35(1):234–41. https://doi.org/10.1109/MNET.011.2000263
63 Zhu N, Li Y, Wang X, Chen Q. Toward designing highly effective and efficient consensus mechanisms for blockchain-based applications. Cluster Comput. 2024;27(5):5677–98. https://doi.org/10.1007/s10586-023-04244-y
64 Marwah K, Sharma P, Gupta R. Revolutionizing education: the role of AI and blockchain. In: Idrees SM, Jameel R, Nowostawski M, editors. Blockchain and machine learning innovations. Cham: Springer; 2025. p. 231–47. https://doi.org/10.1007/978-3-031-88095-7_12
65 Wang S, Zhang J, Li X, Sun Y. Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans Syst Man Cybern Syst. 2019;49(11):2266–77. https://doi.org/10.1109/TSMC.2019.2895123
66 Platt M, Salinas D, Müller T. The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In: Proceedings of the IEEE 21st international conference on software quality, reliability and security companion; 2021. p. 98–105. https://doi.org/10.1109/QRS-C52525.2021.00020
67 Yuan Y, Wang FY. Blockchain and cryptocurrencies: model, techniques, and applications. IEEE Trans Syst Man Cybern Syst. 2018;48(9):1421–8. https://doi.org/10.1109/TSMC.2018.2854904
68 De Filippi P, Mannan M, Reijers W. Blockchain technology and the rule of code: regulation via governance. Geo Wash Law Rev. 2024;92:1229–60.
69 Fernando P, Li X, Zhang Q. Distributed-proof-of-sense: blockchain consensus mechanisms for detecting spectrum access violations. IEEE Trans Cogn Commun Netw. 2023;9(5):1110–25. https://doi.org/10.1109/TCCN.2023.3291366
70 André M, Margarida J, Garcia H, Dante A. Complexities of blockchain technology and distributed ledger technologies: a detailed inspection. Fusion Multidiscip Res. 2021;2(1):1–18.
71 Lin Y, Chen Z, Li H, Zhou X. Blockchain-based efficient and trustworthy AIGC services in metaverse. IEEE Trans Serv Comput. 2024. https://doi.org/10.1109/TSC.2024.3420987
72 Singh A, Gupta R, Kumar S. Blockchain-based lightweight authentication protocol for next-generation trustworthy Internet of Vehicles communication. IEEE Trans Consum Electron. 2024;70(2):4898–907.
73 Myrzashova R, Zhang L, Wang Y. Safeguarding patient data-sharing: blockchain-enabled federated learning in medical diagnostics. IEEE Trans Sustain Comput. 2024. https://doi.org/10.1109/TCE.2024.3351221
74 Li R, Zhao Q, Chen M. Efficient blockchain-assisted distributed identity-based signature scheme for integrating consumer electronics in metaverse. IEEE Trans Consum Electron. 2024. https://doi.org/10.1109/TCE.2024.3420789
75 Jia L, Wang H, Zhang X. Estuary: a low cross-shard blockchain sharding protocol based on state splitting. IEEE Trans Parallel Distrib Syst. 2024;35(3):405–20. https://doi.org/10.1109/TPDS.2024.3351632
76 Biswas S, Muthukkumarasamy V, Wu M. A scalable blockchain framework for secure transactions in IoT. IEEE Internet Things J. 2018;6(3):4650–9. https://doi.org/10.1109/JIOT.2018.2874095
77 European Parliament, Council of the European Union. Markets in Crypto-Assets Regulation (EU) 2023/1114. 2023.
78 CoinLaw. SEC and CFTC regulations on cryptocurrencies: enforcement statistics and trends in 2025. 2025.
79 Bhattacharjee P, Sharma S, Singh R. DigiBlock: digital self-sovereign identity on distributed ledger based on blockchain. In: Proceedings of the international conference on advancements in smart, secure and intelligent computing (ASSIC); 2022. p. 1–6.
80 Dimakis AG, Prabhakaran V, Ramchandran K. Decentralized erasure codes for distributed networked storage. IEEE Trans Inf Theory. 2006;52(6):2809–16. https://doi.org/10.1109/TIT.2006.874535
81 Franks PC. Implications of blockchain distributed ledger technology for records management and information governance programs. Rec Manag J. 2020;30(3):287–99. https://doi.org/10.1108/RMJ-08-2019-0047
82 Alzahab NA, D'Angelo G, Di Paolo C, Marchesi M. Decentralized biometric authentication based on blockchain and fuzzy commitment schemes. IEEE Access. 2023. https://doi.org/10.1109/ACCESS.2023.3289574
83 Bu B, Chen Y, Li X. A man–vehicle e-passport system using biometric blockchain towards automated border control. Front Blockchain. 2025;8:1596567. https://doi.org/10.3389/fbloc.2025.1596567
84 Paea S, Sharma B, Bulivou G, Katsanos C. Emergency remote teaching in higher education institutes: a taxonomy of challenges faced by first-year mathematics students in the Pacific region. IEEE Access. 2024;12:6339–55. https://doi.org/10.1109/ACCESS.2024.3351098
85 Xiong W, Xiong L. Data trading certification based on consortium blockchain and smart contracts. IEEE Access. 2020;8:225916–27. https://doi.org/10.1109/ACCESS.2020.3041533
86 Xiao M, Xu Y, Zhang Y, Yang K, Yan S, Cen L. Formal verification of Solidity smart contracts via automata theory. Symmetry. 2025;17(8):1275. https://doi.org/10.3390/sym17081275
87 Yang Q, Liu J, Wang Y, Li H. Fusing blockchain and AI with metaverse: a survey. IEEE Open J Comput Soc. 2022;3:122–36. https://doi.org/10.1109/OJCS.2022.3178962
88 Etemadi N, Van Gelder P, Strozzi F. An ISM modeling of barriers for blockchain/distributed ledger technology adoption in supply chains towards cybersecurity. Sustainability. 2021;13(9):4672. https://doi.org/10.3390/su13094672
89 Yadav AS, Singh N, Kushwaha DS. Evolution of blockchain and consensus mechanisms and its real-world applications. Multimed Tools Appl. 2023;82(22):34363–408. https://doi.org/10.1007/s11042-023-14624-6
90 Benčić FM, Podnar Žarko I. Distributed ledger technology: blockchain compared to directed acyclic graph. Zagreb: University of Zagreb, Faculty of Electrical Engineering and Computing.
91 Laghari AA, Khan AA, Alkanhel R, Elmannai H, Bourouis S. Lightweight-BIoV: blockchain distributed ledger technology for Internet of Vehicles. Electronics. 2023;12(3):677. https://doi.org/10.3390/electronics12030677
92 Kim HM, Laskowski M. Toward an ontology-driven blockchain design for supply-chain provenance. Intell Syst Account Finance Manag. 2018;25(1):18–27. https://doi.org/10.1002/isaf.1424
93 Yang Z, Zheng K, Yang K, Leung VCM. A blockchain-based decentralized trust management system in vehicular networks. IEEE Trans Veh Technol. 2018;67(10):9789–801. https://doi.org/10.1109/TVT.2018.2869979
94 Rajput AR, Li Q, Taleby Ahvanooey M, Masood I. EACMS: emergency access control management system for personal health record based on blockchain. IEEE Access. 2019;7:84304–17. https://doi.org/10.1109/ACCESS.2019.2917976
95 Kotzer A, Gandelman D, Rottenstreich O. SoK: applications of sketches and rollups in blockchain networks. IEEE Trans Netw Serv Manag. 2024;21(3):3194–208. https://doi.org/10.1109/TNSM.2024.3372604
96 Turkanovic M, Hölbl M, Košic K, Heričko M, Kamišalić A. EduCTX: a blockchain-based higher education credit platform. IEEE Access. 2018;6:5112–27. https://doi.org/10.1109/ACCESS.2018.2789929
97 Polge J, Robert J, Le Traon Y. Permissioned blockchain frameworks in the industry: a comparison. ICT Express. 2021;7(2):229–33. https://doi.org/10.1016/j.icte.2020.09.002
98 Valenta M, Sandner P. Comparison of Ethereum, Hyperledger fabric and corda. Frankfurt School Blockchain Center; 2018. Available from: http://www.fs-blockchain.de
99 Bazel MA, Al-Fuqaha A, Al-Sarawi S. Blockchain technology adoption in healthcare: an integrated model. Sci Rep.

2025;15(1):14111. https://doi.org/10.1038/s41598-025-95253-x
100 Liu H, Zhang Y, Zheng S, Li Y. Electric vehicle power trading mechanism based on blockchain and smart contract in V2G network. IEEE Access. 2019;7:160546–58. https://doi.org/10.1109/ACCESS.2019.2951057
101 Skiba DJ. The blockchain and distributed ledgers: implications for nursing. Nurs Educ Perspect. 2017;38(4):221–2. https://doi.org/10.1097/01.NEP.0000000000000163
102 Khan AA, Khan F, Ahmad I, Ullah S. Internet of Things security with blockchain technology: a state-of-the-art review. IEEE Access. 2022;10:122679–95. https://doi.org/10.1109/ACCESS.2022.3223370
103 Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. Gaithersburg, MD: National Institute of Standards and Technology; 2019. NISTIR 8202. https://doi.org/10.6028/NIST.IR.8202
104 Nguyen CT, Pathirana PN, Ding M, Seneviratne A, Sherratt RS. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access. 2019;7:85727–45. https://doi.org/10.1109/ACCESS.2019.2925012
105 Zoughbi D, Venkatachalam K. Mitigating cloud vulnerabilities using a blockchain platform. Front Blockchain. 2025;8:1567417. https://doi.org/10.3389/fbloc.2025.1567417
106 Gupta R, Tanwar S, Al-Turjman F, Italiya P, Nauman A, Kim SW. Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. IEEE Access. 2020;8:24746–72. https://doi.org/10.1109/ACCESS.2020.2970576
107 Abreu AWS, Coutinho EF, Bezerra CIM. Performance evaluation of data transactions in blockchain. IEEE Lat Am Trans. 2022;20(3):409–16. https://doi.org/10.1109/TLA.2022.9667139
108 Zou W, Lo D, Kochhar PS, Le XBD, Xia X, Feng Y, Chen Z, Xu B. Smart contract development: challenges and opportunities. IEEE Trans Softw Eng. 2019;47(10):2084–106. https://doi.org/10.1109/TSE.2019.2942301
109 Panwar V, Bhatnagar M, Khari A, Salehi AW, Gupta G. A blockchain framework to secure personal health record (PHR) in IBM cloud-based data lake. Comput Intell Neurosci. 2022:1–19. https://doi.org/10.1155/2022/3045107
110 Udeh EO, Amajuoyi P, Adeusi KB, Scott AO. Blockchain-driven communication in banking: enhancing transparency and trust with distributed ledger technology. Finance Account Res J. 2024;6(6):1–15.
111 Kumar A, Singh M, Sharma R. A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. Sensors. 2022;22(15):5921. https://doi.org/10.3390/s22155921
112 BlockchainTechs.io. Top 10 ZK rollup projects in 2025. 2025. Available from: BlockchainTechs.io.
113 Čeke D, Kunosić S. Smart contracts as a diploma anti-forgery system in higher education—a pilot project. In: Proceedings of the 43rd international convention on information, communication and electronic technology (MIPRO); 2020. p. 1–6. http://doi.org/10.23919/MIPRO48935.2020.9245391
114 Li Z, Xiao B, Guo S, Yang Y. Securing deployed smart contracts and DeFi with distributed TEE cluster. IEEE Trans Parallel Distrib Syst. 2022;34(3):828–42. https://doi.org/10.1109/TPDS.2022.3232548
115 Zheng Z, Liu Y, Wang X, Chen J. Turn the rudder: a beacon of reentrancy detection for smart contracts on Ethereum. In: Proceedings of the IEEE/ACM 45th international conference on software engineering (ICSE); 2023. p. 1–12. https://doi.org/10.1109/ICSE54865.2023.00024
116 Zhang Z, Li H, Xu M, Chen S. Demystifying exploitable bugs in smart contracts. In: Proceedings of the IEEE/ACM 45th international conference on software engineering (ICSE); 2023. p. 615–27. https://doi.org/10.1109/ICSE54865.2023.00070
117 Rajput R, Li Q, Taleby Ahvanooey M, Masood I. EACMS: emergency access control management system for personal health record based on blockchain. IEEE Access. 2019;7:84304–17. https://doi.org/10.1109/ACCESS.2019.2917976
118 Damoska SJ, Erceg A. Blockchain technology toward creating a smart local food supply chain. Computers. 2022;11(6):95. https://doi.org/10.3390/computers11060095
119 Gier RE, Eves C, Green P. Evaluation of the therapeutic effect of levamisole in treatment of recurrent aphthous stomatitis. J Oral Pathol. 1978;7(6):405–13. https://doi.org/10.1111/j.1600-0714.1978.tb01610.x
120 Quamara S, Singh AK. An in-depth security and performance investigation in Hyperledger Fabric-configured distributed computing systems. Blockchain Model. 2023;1(1):12–24.
121 Singh S, Jadhav S, Roopashree M. Factors to overcoming barriers affecting electronic medical record usage by physicians. Indian J Community Med. 2020;45(2):168. https://doi.org/10.4103/ijcm.IJCM_478_19
122 Al Mamun S, Azam S, Gritti C. Blockchain-based electronic health records management: a comprehensive review and future research direction. IEEE Access. 2022;10:5768–89. https://doi.org/10.1109/ACCESS.2022.3141079
123 Murthy VNUB, Shri ML, Kadry S, Lim S. Blockchain based cloud computing: architecture and research challenges. IEEE Access. 2020;8:205190–205. https://doi.org/10.1109/ACCESS.2020.3036812
124 Sharma T, Singh R, Verma P. Unpacking how decentralized autonomous organizations (DAOs) work in practice. In: Proceedings of the IEEE international conference on blockchain and cryptocurrency (ICBC); 2024. p. 1–8. https://doi.org/10.1109/ICBC56789.2024.00011
125 Tyagi AK. Decentralized everything: practical use of blockchain technology in future applications. In: Distributed computing to blockchain. Cambridge, MA: Academic Press; 2023. p. 19–38. https://doi.org/10.1016/B978-0-12-824308-1.00002-1
126 Yang G, Lee K, Lee K, Yoo Y, Lee H, Yoo C. Resource analysis of blockchain consensus algorithms in hyperledger fabric. IEEE Access. 2022;10:74902–20. https://doi.org/10.1109/ACCESS.2022.3190979
127 Du J, Li W, Zhang X, Zhang Y. Secure task offloading in blockchain-enabled MEC networks with improved PBFT consensus. IEEE Trans Cogn Commun Netw. 2024. https://doi.org/10.1109/TCCN.2024.3167852
128 Zyskind G, Nathan O, Pentland A. Decentralizing privacy: using blockchain to protect personal data. In: Proceedings of the IEEE security and privacy workshops; 2015. p. 180–4. https://doi.org/10.1109/SPW.2015.27
129 Rantos K, Drosatos G, Kritsas A, Ilioudis C, Papanikolaou A, Filippidis AP. A blockchain-based platform for consent management of personal data processing in the IoT ecosystem. Secur Commun Netw. 2019:1–15. https://doi.org/10.1155/2019/1431578
130 Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification, and open issues. Telemat Inform. 2019;36:55–81. https://doi.org/10.1016/j.tele.2018.11.006
131 Ihama E, Akazue MI, Omede EU, Ojie DV. A framework for smart city model enabled by Internet of Things (IoT). Int J Comput Appl. 2023;185(6):6–11. https://doi.org/10.5120/ijca2023922685
132 Alrubei SM, Ball EA, Rigelsford JM, Willis CA. Latency and performance analyses of real-world wireless IoT-blockchain application. IEEE Sens J. 2020;20(13):7372–83. https://doi.org/10.1109/JSEN.2020.2979031
133 Meng T, Zhao Y, Wolter K, Xu CZ. On consortium blockchain consistency: a queueing network model approach. IEEE Trans Parallel Distrib Syst. 2021;32(6):1369–82. https://doi.org/10.1109/TPDS.2021.3049915
134 Peng Z, Chen X, Li M, Wang Y. BU-trace: a permissionless mobile system for privacy-preserving intelligent contact tracing. In: Proceedings of the international conference on database systems for advanced applications; 2021. p. 204–18. https://doi.org/10.1007/978-3-030-75756-4_14
135 Linoy S, Stakhanova N, Matyukhina A. Exploring Ethereum's blockchain anonymity using smart contract code attribution. In: Proceedings of the 15th international conference on network and service management (CNSM); 2019. p. 1–9. https://doi.org/10.23919/CNSM46954.2019.9012681
136 Bhuvana R, Aithal PS. RBI distributed ledger technology and blockchain: a future of decentralized India. Int J Manage Technol Soc Sci. 2020;5(1):227–37. http://doi.org/10.47992/IJMTS.2581.6012.0091
137 Mukherjee AA, Vaidya M, Chatterjee P. Application of blockchain technology for sustainability development in agricultural supply chain: justification framework. Oper Manag Res. 2022;15(1):46–61. https://doi.org/10.1007/s12063-022-00231-0

138 Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Trans Ind Inform. 2019;16(7):4177–86. https://doi.org/10.1109/TII.2019.2919935
139 Hasan HR, Salah K. Proof of delivery of digital assets using blockchain and smart contracts. IEEE Access. 2018;6:46781–93. https://doi.org/10.1109/ACCESS.2018.2876971
140 Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: a data processing view of blockchain systems. IEEE Trans Knowl Data Eng. 2018;30(7):1366–85. https://doi.org/10.1109/TKDE.2017.2781227
141 Zou Y, Meng T, Zhang P, Zhang W, Li H. Focus on blockchain: a comprehensive survey on academic and application. IEEE Access. 2020;8:187182–201. https://doi.org/10.1109/ACCESS.2020.3030491
142 Lu Y, Wang J, Zhang H, Zhao Q. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles. IEEE Trans Veh Technol. 2020;69(4):4298–311. https://doi.org/10.1109/TVT.2020.2973651
143 Wan J, Li D, Liu X. A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Trans Ind Inform. 2019;15(6):3652–60. https://doi.org/10.1109/TII.2019.2894573
144 Cao Q, Li J, Zhang W. Has the fan economy affected the price of non-fungible tokens? SSRN. 2023. https://doi.org/10.2139/ssrn.4404748
145 Mohammed Uveise SA, Fathima SMHS. Efficient lightweight blockchain with hybridized consensus algorithm for IoT networks. IETE J Res. 2024;70(12):8527–37. https://doi.org/10.1080/03772063.2024.2400599
146 Xie J, Liu Y, Zhang X, Wang L. A survey of blockchain technology applied to smart cities: research issues and challenges. IEEE Commun Surv Tutor. 2019;21(3):2794–830. https://doi.org/10.1109/COMST.2019.2899617
147 Joseph S, Pandeeswari N. Secured IoT data transmission with enhanced integrated encryption techniques with blockchain technology. IETE J Res. 2025;71(4):1156–75. http://doi.org/10.1080/03772063.2025.2458609
148 Abdullah AAH, Kumar P, Singh R. Blockchain adoption and its impact on sustainability of accounting education. Environ Dev Sustain. 2024:1–21. https://doi.org/10.1007/s10668-024-02911-x
149 Scharfman J. Decentralized autonomous organization fraud, hacks, and controversies. In: The cryptocurrency and digital asset fraud casebook. Vol. II. Cham: Springer Nature; 2024. p. 65–106.