JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain Technology: A Technical Review of Architecture, Applications, Security and Scalability
A Structured Literature-Based Review

Ms. Sarika Kashiram Meshram
Lecturer ,Information Technology
Government Polytechnic Gondia

Mr. Nitin Gunvantrao Gulhane
Lecturer ,Information Technology
Government Polytechnic Gondia

Abstract
Blockchain has developed from the distributed ledger architecture introduced through Bitcoin into a broader technology for coordinating records, assets, identities, and automated processes among parties that may not share a single trusted administrator. This paper presents a structured literature-based review of blockchain architecture, cryptographic foundations, consensus mechanisms, smart contracts, applications, security, scalability, interoperability, and emerging integration with artificial intelligence (AI) and the Internet of Things (IoT). The review synthesizes foundational works, systematic surveys, standards-oriented guidance, and application-focused studies. A central research gap identified in the literature is the need to evaluate blockchain not only by its decentralization features but also by application-specific requirements such as trust relationships, throughput, privacy, governance, interoperability, storage, and regulatory constraints. The analysis indicates that blockchain is most appropriate where multiple parties need a shared, auditable record and where decentralization or tamper evidence provides measurable value. It is not a universal replacement for conventional databases. Future research should emphasize scalable and interoperable architectures, privacy-preserving mechanisms, secure smart contracts, efficient consensus, decentralized identity, tokenization, and responsible integration with AI and IoT.

Keywords: Blockchain, Distributed Ledger Technology, Consensus, Smart Contracts, Cryptography, Scalability, Interoperability, Blockchain Security, IoT, Artificial Intelligence

1. Introduction
Digital transformation has increased the volume and importance of electronically managed records in finance, supply chains, healthcare, education, public services, manufacturing, and connected-device ecosystems. Conventional information systems generally rely on a central database or trusted administrator. Such systems can be efficient and mature, but some multi-organization workflows require participants to share a common history without giving one organization complete control over the authoritative record. Blockchain provides an alternative distributed approach in which transactions or other records are replicated across participating nodes and linked using cryptographic mechanisms [21], [22].

The publication of Bitcoin: A Peer-to-Peer Electronic Cash System established a practical demonstration of a decentralized transaction system that could operate without a conventional financial intermediary [1]. Subsequent

research expanded blockchain concepts to smart contracts, permissioned networks, supply chains, healthcare, IoT, identity, and other application domains [2], [3], [23], [24].

However, the expansion of blockchain applications has also exposed limitations. Scalability, privacy, interoperability, smart-contract security, energy consumption, governance, storage growth, and regulatory uncertainty remain important considerations [21], [24], [25], [26], [30]. Consequently, the key research question is no longer simply whether blockchain can be used in a particular sector, but under what technical and organizational conditions it provides an advantage over conventional distributed or centralized systems.

2. Problem Statement and Research Gap

A large body of blockchain literature separately examines architecture, consensus, applications, security, and scalability. Systematic reviews have classified blockchain applications and identified broad research challenges [7], [23], [24]. Nevertheless, application studies can sometimes emphasize potential benefits without sufficiently addressing whether decentralization is necessary, how privacy should be achieved, or how performance and governance constraints affect practical deployment.

The research gap addressed in this review is therefore the need for an integrated assessment that connects blockchain's technical foundations with application suitability. In particular, the review focuses on the relationship among: (i) trust and governance requirements, (ii) consensus and performance, (iii) cryptographic security and privacy, (iv) scalability and storage, (v) interoperability, and (vi) application-specific benefits. This framing helps distinguish genuine blockchain use cases from situations in which a conventional database may remain more appropriate.

3. Objectives

- To explain the architecture and fundamental operating principles of blockchain systems.
- To examine cryptographic mechanisms used for integrity, authentication, and transaction authorization.
- To compare major consensus mechanisms including Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT).
- To review the role of smart contracts and permissioned blockchain platforms.
- To analyze blockchain applications in finance, supply chains, healthcare, education, agriculture, voting, and IoT.
- To identify security, scalability, privacy, storage, interoperability, governance, and regulatory challenges.
- To synthesize findings from representative literature and identify research gaps and future directions.
- To provide an application-oriented basis for deciding when blockchain is preferable to conventional database architectures.

4. Research Methodology

This study uses a qualitative, structured literature-review methodology. The approach follows four stages: source identification, relevance screening, thematic classification, and synthesis. The paper is based on the 20 references already included in the source manuscript together with 30 additional scholarly and standards-oriented references selected to strengthen coverage of architecture, scalability, smart contracts, healthcare, supply chains, IoT, privacy, interoperability, and security [1]–[40].

4.1 Search Scope

The literature scope was organized around the following themes: blockchain architecture; distributed ledger technology; Bitcoin; consensus mechanisms; smart contracts; blockchain security; scalability; interoperability; healthcare; supply chains; IoT; privacy; and permissioned blockchain systems. Major scholarly and technical publication venues represented in the selected references include IEEE, ACM, Elsevier, PLOS ONE, NIST, and major academic publishers.

4.2 Inclusion Criteria

- Research papers, books, conference papers, systematic reviews, and standards-oriented technical publications directly relevant to blockchain.
- Sources addressing technical architecture, consensus, security, applications, or future directions.
- Foundational works that established major blockchain concepts or platforms.
- Survey and review studies useful for identifying research trends and open issues.

4.3 Exclusion Criteria

- Duplicate or substantially overlapping publications.
- Sources focused only on cryptocurrency market speculation without technical relevance.
- Unverified claims that could not be connected to an identifiable scholarly or standards source.
- Application claims unsupported by the reviewed literature.

4.4 Analysis Framework

The selected literature was grouped into five analytical dimensions: technology foundations, application domains, performance and scalability, security and privacy, and future integration. The final synthesis emphasizes both reported benefits and constraints rather than treating blockchain as inherently superior to other database technologies.

5. Literature Review

The literature shows a progression from blockchain as the infrastructure underlying Bitcoin toward a general-purpose distributed computing and coordination technology. Nakamoto introduced the original decentralized electronic cash architecture [1]. Crosby et al. discussed blockchain beyond Bitcoin [2], while Zheng et al. provided a broad survey of architecture, consensus, applications, and challenges [3], [24]. Yli-Huumo et al. systematically reviewed blockchain research and highlighted unresolved issues that shaped subsequent research [4].

Research subsequently expanded toward smart contracts and decentralized applications. Buterin described a generalized platform for programmable transactions [5], while Antonopoulos and Wood provided technical treatments of Bitcoin and Ethereum [6], [7]. Rouhani and Deters surveyed smart-contract security and performance [26], showing that programmability introduces additional software-security concerns.

Application-oriented reviews demonstrate substantial interest in finance, supply chains, healthcare, IoT, identity, and public services [23], [28], [29], [21]. At the same time, scalability and interoperability remain persistent research themes [25], [30], [31], [30], [31].

5.1 Representative Literature Review Table

Author(s) / Year	Focus	Method / Contribution	Key Finding	Relevance to This Review
Nakamoto, 2008 [1]	Bitcoin and decentralized electronic cash	Foundational protocol	Demonstrated peer-to-peer transaction consensus without a central financial institution.	Foundation of blockchain and PoW.
Crosby et al., 2016 [2]	Blockchain beyond Bitcoin	Technology overview	Identified applications beyond cryptocurrency.	Supports broader application analysis.
Zheng et al., 2017 [3]	Architecture and consensus	Survey	Classified components, consensus, applications and challenges.	Provides technical taxonomy.
Yli-Huumo et al., 2016 [4]	Blockchain research status	Systematic review	Identified research concentration and unresolved issues.	Supports research-gap formulation.

Casino et al., 2019 [23]	Blockchain applications	Systematic literature review	Classified applications and discussed open issues.	Supports application comparison.
Zhou et al., 2020 [25]	Scalability	Survey and classification	Low throughput and high latency remain important problems.	Supports scalability discussion.
Rouhani and Deters, 2019 [26]	Smart-contract security	Systematic survey	Smart contracts introduce security and performance concerns.	Supports smart-contract analysis.
Kshetri, 2018 [28]	Supply chains	Application analysis	Blockchain can support traceability and supply-chain objectives.	Supports supply-chain use case.
Saeed et al., 2022 [29]	Healthcare	Systematic review	Blockchain has potential for records and healthcare processes but privacy and interoperability remain important.	Supports healthcare analysis.
Ren et al., 2023 [30]	Interoperability	Survey	Interoperability is a significant challenge across blockchain systems.	Supports future-scope analysis.
Androulaki et al., 2018 [33]	Hyperledger Fabric	Platform architecture and evaluation	Permissioned blockchain can provide modular membership and consensus.	Supports enterprise/permissioned systems.
Christidis and Devetsikiotis, 2016 [37]	Blockchain and IoT	Conceptual/technical study	Smart contracts can support automated IoT interactions.	Supports IoT integration.

6. Fundamentals and Architecture of Blockchain

Blockchain is a distributed ledger architecture in which records are grouped into blocks and maintained across participating nodes. NIST characterizes blockchains as tamper-evident and tamper-resistant distributed ledgers [21]. A typical block contains transaction data, a timestamp or related metadata, and cryptographic information linking the block to earlier ledger state.

6.1 Core Components

- Transaction: A digitally authorized operation or record submitted to the network.
- Block: A collection of valid transactions and protocol metadata.
- Hash: A fixed-length cryptographic representation used to detect changes.
- Digital signature: A mechanism for proving authorization and protecting integrity.
- Peer-to-peer network: A communication layer through which nodes exchange transactions and blocks.
- Consensus mechanism: A protocol for agreeing on the next valid ledger state.
- Ledger: The ordered history of accepted records.
- Smart contract: Executable logic deployed on a blockchain platform.

6.2 Blockchain Processing Flow

A generalized workflow is: Transaction creation → digital signing → network broadcast → validation → consensus → block formation → block validation → ledger update. The exact sequence varies by protocol, but the fundamental objective is to enable participants to converge on an agreed ledger state [21], [24].

7. Cryptography and Security Foundations

7.1 Hash Functions

Cryptographic hash functions map input data to fixed-length outputs. Desired properties include deterministic computation, preimage resistance, collision resistance, and sensitivity to small input changes. Hashes are used to link blocks and support integrity verification [21], [22]. SHA-256 is strongly associated with Bitcoin's PoW system [1].

7.2 Public-Key Cryptography and Digital Signatures

Blockchain systems commonly use public-key cryptography to establish identities or addresses and to authorize transactions. The private key must remain confidential because possession of the relevant key can confer control over associated assets or permissions. Digital signatures provide evidence that a transaction was authorized by the holder of the corresponding private key [21], [32].

7.3 Security Model

Blockchain security is not limited to the ledger protocol. Wallets, applications, exchanges, smart contracts, endpoints, and identity-management systems can remain vulnerable even when the underlying consensus mechanism is robust. Consequently, end-to-end security must include both protocol-level and application-level controls [22], [26].

8. Consensus Mechanisms

8.1 Proof of Work

Proof of Work requires participants to perform computational work before proposing blocks. Bitcoin uses PoW [1]. Its principal strengths include a mature security model and suitability for open permissionless networks; its major concerns include computational resource requirements and energy consumption [21], [17].

8.2 Proof of Stake

Proof of Stake assigns block-production or validation responsibilities according to protocol-defined stake and validator rules. It can substantially reduce energy requirements compared with PoW, although validator incentives, stake concentration, governance, and protocol complexity require careful design [21], [24].

8.3 Practical Byzantine Fault Tolerance

PBFT was designed for distributed systems in which some participants may be faulty or malicious [34]. It is particularly relevant to permissioned environments with known participants. Modern enterprise platforms use modular consensus and membership mechanisms suited to organizational trust models [33].

9. Types of Blockchain Networks

Blockchain networks can be classified according to participation and governance.

- Public blockchain: Generally open participation and typically designed for permissionless operation, such as Bitcoin and Ethereum.
- Private blockchain: Controlled by a single organization with restricted participation.
- Consortium blockchain: Governed by a group of organizations sharing responsibility for the network.
- Hybrid blockchain: Combines selected public and permissioned characteristics.

Permissioned platforms such as Hyperledger Fabric illustrate how membership, smart contracts, and consensus can be modularized for enterprise use [33].

10. Smart Contracts and Decentralized Applications

Smart contracts are programs deployed on blockchain infrastructure that execute according to predefined conditions. They can automate payments, asset transfers, business rules, insurance processes, and other multi-step workflows [5], [26], [35]. Their principal advantage is deterministic automation among parties that share the same execution environment. Their major risk is that programming defects can become operational or financial vulnerabilities. Secure development, testing, auditing, access control, and careful handling of external data are therefore essential [26].

11. Applications of Blockchain Technology

11.1 Finance and Banking

Blockchain has been investigated for cross-border payments, settlement, digital assets, trade finance, tokenization, and transaction tracking. Its value is strongest where multiple institutions need a shared transaction history and where reconciliation between independent databases is costly [2], [23], [24].

11.2 Supply Chain Management

Supply-chain applications can record product movement across manufacturers, distributors, warehouses, retailers, and customers. The principal proposed benefits are traceability, shared visibility, auditing, and improved provenance [28]. However, blockchain cannot by itself guarantee that information entered at the source is truthful; trusted data capture remains necessary. [33], [38].

11.3 Healthcare

Potential healthcare uses include medical-record sharing, consent management, credential verification, and pharmaceutical supply-chain tracking [29]. Healthcare deployments must prioritize privacy, access control, interoperability, and regulatory compliance. Sensitive clinical data may therefore be better maintained off-chain with blockchain storing proofs, permissions, or references.

11.4 Education

Blockchain can support digital certificates and academic credential verification by creating an auditable record that employers or institutions can independently validate [23]. The architecture should minimize unnecessary disclosure of personal information. [35].

11.5 Voting

Blockchain has been proposed for auditable electronic voting, but blockchain alone does not solve voter privacy, endpoint security, coercion resistance, identity management, accessibility, or election governance. Therefore, claims of blockchain-enabled voting should be treated as conditional rather than as a complete security solution. [37].

11.6 Agriculture

Agricultural supply chains may use distributed ledgers to record farm origin, production, transportation, storage, certification, and distribution. The principal objective is improved traceability and provenance. [39], [40].

11.7 Internet of Things

IoT systems generate large volumes of events and may involve devices that need decentralized coordination. Blockchain and smart contracts can support trusted event recording, identity, and automated interactions [27], [21]. Because many IoT devices have limited resources and produce high data volumes, hybrid on-chain/off-chain architectures are generally more practical than storing all sensor data directly on-chain.

12. Advantages and Application Suitability

- Shared auditability: Participants can independently verify an agreed history.
- Tamper evidence: Cryptographic linking makes unauthorized historical modification detectable.

- Reduced reconciliation: A shared ledger can reduce repeated reconciliation between organizational databases.
- Programmable processes: Smart contracts can automate predefined workflows.
- Traceability: Transaction history can support provenance and auditing.
- Reduced dependence on a single administrator: Appropriate in selected multi-party trust environments.

These advantages should be evaluated against actual application requirements. Blockchain is most defensible when several independent parties need a shared ledger and no single party should have unilateral control over the authoritative record [21], [23].

13. Limitations and Challenges

13.1 Scalability and Performance

Scalability remains a major challenge because some blockchain architectures have limited throughput, transaction latency, and growing storage requirements [25]. Layer-2 approaches, sharding, alternative consensus mechanisms, sidechains, and other scaling techniques continue to be investigated.

13.2 Energy Consumption

Energy concerns are particularly associated with PoW systems. Alternative consensus mechanisms such as PoS can reduce computational requirements, but their security and governance properties must be evaluated in context [21], [24].

13.3 Privacy

Transparency can conflict with confidentiality. Publicly visible transaction patterns may reveal information even when real-world identities are not directly recorded. Privacy-preserving designs, selective disclosure, encryption, zero-knowledge techniques, and off-chain data storage are therefore important research directions [36].

13.4 Interoperability

Different blockchain networks may use incompatible data models, consensus protocols, identity systems, and smart-contract environments. Interoperability research therefore seeks mechanisms for reliable cross-chain communication and asset or information transfer [30], [31], [30], [31].

13.5 Storage and Data Management

Replicating complete ledger histories can increase storage requirements. Large files and sensor streams are generally unsuitable for direct on-chain storage. Hybrid architectures that retain large data off-chain while anchoring hashes, proofs, or metadata on-chain can reduce this burden.

13.6 Smart-Contract Vulnerabilities

Smart contracts introduce software risks including logic errors, access-control defects, re-entrancy-style vulnerabilities, and unsafe interactions with external data. Formal analysis, testing, auditing, and secure development practices are therefore essential [26].

13.7 Governance and Regulation

Blockchain deployments involve technical and organizational governance questions: who can validate transactions, modify protocol rules, resolve disputes, manage identities, and respond to legal requirements? Financial and digital-asset applications may also be affected by evolving regulatory frameworks [21], [24].

14. Blockchain Security Threats

- 51% attack: In some permissionless systems, majority control of relevant consensus power can permit manipulation of transaction ordering or confirmations [24], [17].
- Sybil attack: An adversary creates multiple identities to influence network behavior [21], [32].

- Private-key compromise: Theft or loss of a private key can result in loss of control over associated assets or permissions [21].
- Smart-contract attack: Vulnerable code can be exploited despite the integrity of the underlying ledger [26].
- Phishing and social engineering: Users can be tricked into revealing credentials or authorizing malicious transactions.
- Endpoint compromise: Wallets, applications, exchanges, and connected devices can provide attack paths outside the consensus layer [22].

15. Blockchain and Artificial Intelligence

Blockchain and AI can complement each other when provenance, auditability, and distributed data coordination are important. Blockchain can provide a record of data origin, model-related events, permissions, or transactions, while AI can provide prediction, classification, anomaly detection, and pattern recognition. Potential applications include fraud detection, supply-chain intelligence, decentralized data or model marketplaces, healthcare data management, and smart manufacturing. The combined architecture also introduces additional requirements for data quality, privacy, computational cost, and scalability.

16. Blockchain and Internet of Things

A representative architecture is: IoT devices → gateway → blockchain network → smart contract → application. Blockchain can provide shared event histories and decentralized coordination, while smart contracts can automate responses to trusted device events [27], [21]. The principal design challenge is that IoT systems can generate data at rates and volumes that are unsuitable for direct blockchain storage. Edge computing, gateways, off-chain databases, and selective on-chain anchoring can therefore be used to balance trust and performance.

17. Comparative Analysis: Traditional Database vs. Blockchain

Criterion	Traditional Database	Blockchain
Primary control	Usually centralized or administratively controlled	Distributed or shared according to network design
Performance	Generally high for conventional transactional workloads	Depends on consensus, network, and architecture
Historical modification	Authorized administrators can update records	Historical records are designed to be tamper-evident
Trust model	Trust in database administrator or organization	Trust distributed across protocol and participating nodes
Auditability	Depends on logging and database design	Strong shared transaction history in appropriate designs
Privacy	Can be tightly controlled by administrator	Varies; public systems may expose transaction metadata
Consensus	Usually not required across independent organizations	Required in many blockchain architectures
Intermediaries	Often relies on a central administrator	Can reduce dependence on a single intermediary in selected workflows
Best fit	High-performance centralized applications	Multi-party shared-record problems with meaningful decentralization or tamper-evidence requirements

18. Discussion

The literature indicates that blockchain's strongest contribution is not simply decentralization but the ability to create a shared, auditable state among parties that may have different organizational interests. This property can reduce

reconciliation and provide traceability in multi-party processes [23], [24]. However, the same literature shows that blockchain introduces trade-offs in performance, privacy, storage, governance, and complexity [21], [25].

A practical deployment decision should therefore begin with the trust and governance problem rather than with the technology. If one trusted organization can efficiently operate the database and participants do not require independent validation, a conventional database may be simpler and faster. If several parties need a shared record and no single party should control the authoritative history, a blockchain or permissioned distributed ledger may be justified [21], [33].

The literature also suggests that future systems will increasingly be hybrid. Sensitive or high-volume data can remain off-chain while blockchain stores proofs, permissions, identities, or transaction summaries. Similarly, interoperability mechanisms may connect specialized blockchain networks rather than requiring every application to operate on one universal chain [30], [31].

19. Future Research Directions

- Interoperable blockchain protocols and reliable cross-chain communication [30], [31], [30], [31].
- Layer-2 and other scaling mechanisms that improve throughput and reduce transaction costs [25].
- Privacy-preserving blockchain architectures and selective disclosure [36].
- Secure smart-contract development, formal verification, and automated vulnerability analysis [26].
- Energy-efficient consensus and sustainable blockchain infrastructure [21], [24].
- Decentralized identity and verifiable credentials.
- Tokenization of digital and selected real-world assets.
- Blockchain-supported government services such as credential, document, and land-record verification.
- Hybrid blockchain–AI architectures for provenance and intelligent decision support.
- Blockchain–IoT architectures using edge computing and off-chain storage.
- Application-specific governance models that address accountability, upgrades, dispute resolution, and regulatory compliance.

20. Conclusion

Blockchain has progressed from its original cryptocurrency application into a family of distributed ledger architectures with potential applications in finance, supply chains, healthcare, education, agriculture, IoT, identity, and public services. Its principal technical foundations are distributed storage, cryptography, digital signatures, consensus, and, in many platforms, programmable smart contracts [1], [21].

The literature reviewed in this paper shows that blockchain offers meaningful benefits when independent parties need a shared, auditable record and when decentralization or tamper evidence provides a concrete advantage. At the same time, scalability, privacy, security, interoperability, storage, governance, energy consumption, and regulatory requirements can limit practical deployment [24]–[26], [30].

The main research implication is that blockchain should be selected because it solves a specific trust and coordination problem, not because it is technologically fashionable. Future work should emphasize interoperable, scalable, privacy-aware, energy-efficient, and application-specific architectures, including hybrid designs that combine blockchain with conventional databases, cloud/edge systems, AI, and IoT. Responsible implementation and evidence-based evaluation will determine the long-term value of blockchain across different sectors.

21. References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” Applied Innovation Review, no. 2, 2016.

[3] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in Proc. IEEE Int. Congress on Big Data, 2017.

[4] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where Is Current Research on Blockchain Technology?—A Systematic Review,” PLOS ONE, vol. 11, no. 10, 2016.

[5] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2014.

[6] A. M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain. O’Reilly Media, 2017.

[7] A. M. Antonopoulos and G. Wood, Mastering Ethereum: Building Smart Contracts and DApps. O’Reilly Media, 2018.

[8] D. Yaga, P. Mell, N. Roby, and K. Scarfone, Blockchain Technology Overview, NISTIR 8202, National Institute of Standards and Technology, 2018, doi: 10.6028/NIST.IR.8202.

[9] M. Swan, Blockchain: Blueprint for a New Economy. O’Reilly Media, 2015.

[10] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies. Princeton University Press, 2016.

[11] M. Iansiti and K. R. Lakhani, “The Truth About Blockchain,” Harvard Business Review, vol. 95, no. 1, pp. 118–127, 2017.

[12] K. Wüst and A. Gervais, “Do you Need a Blockchain?” in Proc. Crypto Valley Conf. Blockchain Technology (CVCBT), 2018, pp. 45–54, doi: 10.1109/CVCBT.2018.00011.

[13] M. Pilkington, “Blockchain technology: principles and applications,” in Research Handbook on Digital Transformations, 2016, doi: 10.4337/9781784717766.00019.

[14] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” Business & Information Systems Engineering, vol. 59, no. 3, pp. 183–187, 2017, doi: 10.1007/s12599-017-0467-3.

[15] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[16] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies,” in Proc. IEEE Symp. Security and Privacy, 2015, pp. 104–121.

[17] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of Proof of Work blockchains,” in Proc. ACM SIGSAC Conf. Computer and Communications Security, 2016, pp. 3–16, doi: 10.1145/2976749.2978341.

[18] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in Proc. 3rd Symp. Operating Systems Design and Implementation (OSDI), 1999, pp. 173–186.

[19] E. Androulaki et al., “Hyperledger Fabric: A distributed operating system for permissioned blockchains,” in Proc. 13th EuroSys Conf., 2018, pp. 1–15.

[20] A. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in Proc. IEEE Security and Privacy Workshops, 2015, pp. 180–184.

[21] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[22] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proc. IEEE Int. Conf. Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.

[23] N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," International Journal of Information Management, vol. 39, pp. 80–89, 2018, doi: 10.1016/j.ijinfomgt.2017.12.005.

[24] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, vol. 36, pp. 55–81, 2019, doi: 10.1016/j.tele.2018.11.006.

[25] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[26] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," IEEE Access, vol. 8, pp. 16440–16455, 2020, doi: 10.1109/ACCESS.2020.2967218.

[27] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," IEEE Access, vol. 7, pp. 50759–50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[28] M. N. M. Bhutta et al., "A survey on blockchain technology: Evolution, architecture and security," IEEE Access, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[29] H. Saeed et al., "Blockchain technology in healthcare: A systematic review," PLOS ONE, vol. 17, no. 4, e0266462, 2022, doi: 10.1371/journal.pone.0266462.

[30] K. Ren, N.-M. Ho, D. Loghin, T.-T. Nguyen, B. C. Ooi, Q.-T. Ta, and F. Zhu, "Interoperability in blockchain: A survey," IEEE Transactions on Knowledge and Data Engineering, vol. 35, no. 12, pp. 12750–12769, 2023, doi: 10.1109/TKDE.2023.3275220.

[31] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," ACM Computing Surveys, vol. 54, no. 8, pp. 1–41, 2021, doi: 10.1145/3471140.

[32] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," Renewable and Sustainable Energy Reviews, vol. 100, pp. 143–174, 2019, doi: 10.1016/j.rser.2018.10.014.

[33] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: A systematic literature review and research agenda," Supply Chain Management: An International Journal, vol. 24, no. 1, pp. 62–84, 2019, doi: 10.1108/SCM-03-2018-0148.

[34] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. 2nd Int. Conf. Open and Big Data (OBD), 2016, pp. 25–30.

[35] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," Applied Sciences, vol. 9, no. 12, Art. no. 2400, 2019, doi: 10.3390/app9122400.

[36] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," Journal of Network and Computer Applications, vol. 166, Art. no. 102731, 2020, doi: 10.1016/j.jnca.2020.102731.

[37] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for e-voting," Symmetry, vol. 12, no. 8, Art. no. 1328, 2020, doi: 10.3390/sym12081328.

[38] U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain technology for secure supply chain management: A comprehensive review," IEEE Access, vol. 10, pp. 85493–85517, 2022, doi: 10.1109/ACCESS.2022.3194319.

[39] W. Liu, X.-F. Shao, C.-H. Wu, and P. Qiao, "A systematic literature review on applications of information and communication technologies and blockchain technologies for precision agriculture development," Journal of Cleaner Production, vol. 298, Art. no. 126763, 2021, doi: 10.1016/j.jclepro.2021.126763.

[40] M. Giganti, M. Borrello, P. M. Falcone, and L. Cembalo, "The impact of blockchain technology on enhancing sustainability in the agri-food sector: A scoping review," Journal of Cleaner Production, vol. 456, Art. no. 142379, 2024, doi: 10.1016/j.jclepro.2024.142379.