**Journal of Computer Technology and Software**

**ISSN: 2998-2383**

**Vol. 4, No. 9, 2025**

# From Distributed Consensus to Privacy-Preserving Federated Learning: Technical Advances and Open Challenges in Blockchain Systems

**Corwin Desrosiers**
University of Regina, Regina, Canada
cd9j@uregina.ca

**Abstract:** Blockchain has evolved from its initial use in cryptocurrency into a foundational infrastructure that enables secure, transparent, and decentralized applications across diverse domains such as finance, healthcare, supply chain management, and the Internet of Things (IoT). By integrating distributed ledgers, consensus protocols, and cryptographic primitives, blockchain eliminates the need for centralized intermediaries and provides tamper-resistant data sharing among untrusted participants. However, the technology faces persistent challenges, including scalability limitations, high energy consumption, privacy leakage, and a lack of interoperability among heterogeneous platforms. This survey presents a comprehensive review of blockchain technology, systematically examining the evolution of consensus mechanisms, scalability optimization strategies, and privacy-preserving frameworks. In addition, it highlights key application domains, industrial adoption trends, and the integration of blockchain with emerging paradigms such as artificial intelligence, federated learning, and edge computing. The paper further discusses open challenges related to performance, security, compliance, and socio-technical adoption, offering insights into the future research directions needed to enable secure, scalable, and sustainable decentralized systems.

**Keywords:** Blockchain technology; distributed ledger; consensus mechanisms; scalability; privacy-preserving frameworks; interoperability.

## 1. Introduction

Blockchain technology has evolved from a niche innovation enabling Bitcoin into a foundational infrastructure supporting diverse decentralized applications across finance, healthcare, supply chain, and the Internet of Things (IoT). At its core, blockchain provides a distributed ledger that guarantees immutability, transparency, and trustless coordination in networks where participants may not trust each other. Unlike traditional centralized databases, blockchain ensures that once information is recorded, it cannot be tampered with retroactively without collusion from the majority of the network. This design eliminates the need for intermediaries, reduces fraud risks, and enables programmable value transfer through smart contracts [1]. Since the release of the Bitcoin white paper in 2008, the technology has undergone several evolutionary stages: the first generation focused on cryptocurrency transactions, the second generation introduced smart contracts and decentralized applications (dApps) with Ethereum, and the third generation aims to solve scalability, interoperability, and energy inefficiency through novel architectures [2].

The disruptive potential of blockchain lies in trust decentralization and the redefinition of data ownership. Financial institutions leverage blockchain to enable cross-border settlement, stablecoins, and decentralized finance (DeFi) platforms that challenge traditional banking models [3]. Beyond payments, tokenization of real-world assets is emerging as an innovative financing mechanism, allowing fractional ownership of real estate, art, and commodities. Healthcare organizations adopt blockchain to enable secure and auditable sharing of electronic health records (EHR), ensure pharmaceutical supply chain integrity, and support data-driven clinical research without compromising patient privacy [4]. Governments experiment with digital identity, verifiable credentials, and transparent voting systems, while the IoT ecosystem utilizes blockchain to ensure data integrity among millions of autonomous devices [5]. In supply chain management, distributed ledgers provide real-time provenance tracking of goods, improving transparency and reducing fraud in industries such as agriculture, luxury goods, and electronics.

Despite its promise, blockchain faces several critical barriers to large-scale adoption. First, transaction throughput remains limited compared to centralized systems, with leading public blockchains struggling to process more than a few dozen transactions per second. Second, consensus mechanisms such as Proof of Work (PoW) have been criticized for excessive energy consumption and environmental impact. Third, privacy leakage is a major concern because transaction histories on public blockchains are permanently transparent, posing risks to individuals and enterprises. Fourth, the lack of interoperability between heterogeneous blockchain platforms prevents seamless value transfer and information exchange across ecosystems [6]. Researchers have proposed a wide range of solutions: layer-2 protocols such as the Lightning Network and rollups aim to offload transaction volume from the main chain; sharding partitions the blockchain to process transactions in parallel; zero-knowledge proofs (ZKPs) and secure multi-party

computation (SMPC) enhance privacy without sacrificing transparency; and cross-chain communication frameworks seek to enable reliable asset and data transfer between different blockchains. However, no single approach has emerged as a universal solution, and trade-offs among security, scalability, and decentralization - the so-called "blockchain trilemma" - remain unresolved [7].

In addition to technical evolution, blockchain research is increasingly intersecting with other emerging technologies. Integration with artificial intelligence (AI) and machine learning enables predictive analytics, fraud detection, and adaptive smart contract behavior. Federated learning over blockchain networks is being explored to train models collaboratively while preserving data privacy. Edge computing is leveraged to reduce latency in blockchain-enabled IoT scenarios, while 5G and beyond-network technologies promise to accelerate decentralized applications in real time. Regulatory frameworks and compliance mechanisms, such as privacy-enhancing technologies to meet GDPR requirements or U.S. digital asset regulations, also play a crucial role in shaping the trajectory of blockchain innovation.

This survey provides a comprehensive review of blockchain technology by synthesizing progress in consensus mechanisms, scalability optimizations, privacy-preserving frameworks, and application domains. Unlike previous surveys that are often narrowly focused - such as on cryptocurrencies or performance issues alone - this paper offers a holistic perspective by also addressing emerging research directions, including blockchain integration with artificial intelligence (AI), federated learning, and edge computing [8]. The contribution of this work lies in three aspects: (1) a systematic categorization of blockchain methodologies that drive current innovation; (2) an exploration of industrial use cases and adoption barriers in real-world deployments; and (3) a forward-looking analysis of challenges and opportunities that will shape blockchain research in the next decade. The intended audience includes both academic researchers and industry practitioners seeking to understand the evolution and potential of decentralized systems.

## 2. Related Work

The academic community has produced a large number of surveys on blockchain, each emphasizing particular perspectives, yet many fail to provide an integrated and forward-looking discussion. Zheng et al. [9] provided one of the earliest systematic overviews, covering blockchain architecture and typical applications but with limited focus on scalability and privacy. Casino et al. [10] surveyed blockchain-based trust models and their application to IoT but lacked discussion on interoperability and energy efficiency. Xu et al. [11] analyzed blockchain as a service (BaaS) frameworks, emphasizing system deployment and operational models. Meanwhile, Li et al. [12] provided a taxonomy of blockchain scalability solutions, such as layer-2 channels and sharding, but their work was completed before the rise of rollup-based scaling and hybrid consensus designs now central to Ethereum and other modern networks.

Surveys specifically on consensus algorithms have tended to be static, focusing primarily on PoW, PoS, and PBFT. For example, Mingxiao et al. [13] examined classical consensus models but did not consider energy-efficient variants like Algorand or Avalanche, nor the trend toward modular consensus frameworks. Likewise, privacy-centric reviews (e.g., Conti et al. [14]) focused on cryptographic primitives such as ring signatures and mixing services but overlooked the rapid progress of zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs), trusted execution environments (TEEs), and secure multi-party computation (MPC) that are now widely researched for privacy-preserving smart contracts [15].

Another gap lies in the emerging convergence of blockchain with AI and data governance. Some recent works explore how blockchain can support federated learning by enabling secure model aggregation without centralized coordination [16], yet few surveys contextualize this within the broader challenges of scalability, regulatory compliance (e.g., GDPR, CCPA), and real-time data analytics at the network edge. Moreover, with the proliferation of cross-chain ecosystems such as Polkadot and Cosmos, interoperability has become a central theme, but existing reviews only partially address the complexity of bridging heterogeneous consensus systems and ensuring security in inter-chain communication [17].

This paper extends prior work by (1) synthesizing the technical evolution of consensus, scalability, and privacy layers; (2) highlighting industrial deployment insights and the challenges of migrating blockchain from pilot projects to production; and (3) introducing the next-generation convergence of blockchain with AI, Internet of Vehicles (IoV), and edge-cloud collaborative systems. By integrating both well-established research and emerging directions, the survey aims to offer a cohesive and forward-thinking reference for the community.

## 3. Methodologies

Blockchain methodologies can be categorized into three foundational dimensions: consensus protocols, scalability enhancement techniques, and privacy-preserving mechanisms. Together, these layers determine the trust, efficiency, and usability of blockchain networks.

Consensus Mechanisms. Consensus ensures that nodes in a distributed network agree on a single ledger state even under adversarial conditions. The Proof of Work (PoW) paradigm, introduced by Bitcoin, provides strong security but is computationally expensive and environmentally unsustainable [18]. Proof of Stake (PoS) mitigates energy costs by allowing participants to validate blocks proportional to their stake; Ethereum's transition to PoS through the Merge illustrates industry-wide movement toward sustainability [19]. Further developments include Delegated Proof of Stake (DPoS), adopted by EOS and TRON, where stakeholders elect a limited set of validators to achieve faster confirmation times. Byzantine Fault Tolerant (BFT) protocols such as PBFT and Tendermint underpin many permissioned networks like Hyperledger Fabric, offering low-latency consensus in controlled environments [20]. Hybrid consensus schemes that combine PoS with BFT or PoW with verifiable delay functions

(VDF) are increasingly popular, aiming to balance security and performance [21].

Scalability and Performance Enhancements. The scalability trilemma - balancing decentralization, security, and throughput - remains a core challenge. Solutions can be categorized into on-chain and off-chain techniques. On-chain methods include sharding, which partitions the blockchain state and transaction processing across subsets of nodes to increase parallelism [22]. Off-chain or Layer-2 protocols such as payment/state channels (e.g., Lightning Network) and rollups (Optimistic Rollup, zkRollup) batch transactions before committing proofs to the base chain, drastically increasing throughput [23]. Novel data structures like Directed Acyclic Graphs (DAGs), employed in IOTA and Fantom, attempt to bypass traditional linear blockchain constraints to achieve high scalability and asynchronous consensus [24]. These innovations enable blockchain systems to approach enterprise-grade transaction speeds without sacrificing decentralization.

Privacy-Preserving Frameworks. While transparency is a strength of blockchain, it conflicts with the need for data confidentiality in many applications. Privacy solutions range from lightweight mixing protocols like CoinJoin to advanced cryptography such as zero-knowledge proofs (ZKPs), which allow users to prove knowledge of a secret or validity of a transaction without revealing details [25]. Projects such as Zcash implement zk-SNARKs to provide shielded transactions, while Ethereum research explores zk-STARKs for scalable privacy [26]. Other methods include secure multi-party computation (MPC), which allows multiple parties to jointly compute functions without revealing private inputs, and trusted execution environments (TEEs) like Intel SGX to execute smart contracts confidentially [27]. Combining these with regulatory compliance frameworks (e.g., GDPR-friendly selective disclosure) represents a critical step for real-world adoption in regulated sectors such as finance and healthcare [28].

## 4. Challenges and Future Directions

Despite considerable progress, blockchain technology faces a series of persistent challenges that must be addressed for mass adoption. Scalability remains the most pressing issue, as even advanced Layer-2 solutions and sharding introduce complexity in security guarantees and user experience. Achieving low-latency finality without compromising decentralization is an active area of research; hybrid consensus models and asynchronous BFT protocols show promise but require further standardization and rigorous security analysis [29]. Another major concern is energy efficiency: although PoS significantly reduces energy consumption compared to PoW, large-scale validator networks still require computational resources, and incentive models for maintaining decentralization under PoS remain debated [30].

Privacy and compliance present another crucial research frontier. The rise of privacy-enhancing technologies (PETs) such as ZKPs, MPC, and homomorphic encryption allows private transactions and confidential smart contracts, yet they introduce computational overhead and complex cryptographic assumptions. Balancing privacy with regulatory transparency - such as anti-money laundering (AML) and know-your-customer (KYC) requirements - is challenging [31]. Future systems may need to integrate selective disclosure and auditable privacy frameworks to comply with legal requirements without undermining user confidentiality.

Interoperability across heterogeneous blockchains remains fragmented. Cross-chain bridges, sidechains, and interoperability frameworks (e.g., Polkadot, Cosmos IBC) aim to allow asset and data transfer between platforms, but they are vulnerable to security exploits, as evidenced by numerous bridge attacks resulting in billions of dollars in losses [32]. Developing formal verification techniques and standardized security protocols for inter-chain communication is vital for the multi-chain future. Moreover, as enterprise blockchains increasingly integrate with public networks, hybrid architectures that combine permissioned governance with public verifiability will be essential.

The convergence of blockchain with AI and edge computing represents a promising but underexplored frontier. Blockchain can enhance federated learning by providing auditable model aggregation and incentive mechanisms for data contribution [33]. Conversely, AI can optimize blockchain performance by predicting network congestion, adapting gas fees, or automating governance decisions through intelligent agents [34]. The rise of Decentralized Autonomous Organizations (DAOs) suggests a future where AI-driven governance could manage complex ecosystems, but robust security, interpretability, and accountability frameworks will be needed to avoid systemic risks.

Lastly, sustainability and socio-economic adoption must be considered. Governments and regulators are shaping the trajectory of blockchain adoption through policy frameworks on digital assets, stablecoins, and privacy-preserving identity systems. Standardization efforts by bodies such as ISO/TC 307 and IEEE P2418 will play a crucial role in fostering interoperability and trust [35]. Understanding the interaction between technological advances and socio-legal constraints will define the pace at which blockchain transforms industries.

## 5. Conclusion and Future Directions

Blockchain has transitioned from serving solely as the backbone of cryptocurrencies to becoming a versatile and foundational infrastructure supporting a broad range of decentralized applications. This transformation has been driven by continuous innovations in consensus algorithms, scalability solutions, and privacy-preserving frameworks, which together have significantly improved the performance, security, and usability of blockchain systems. Modern consensus mechanisms - from Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) to Byzantine Fault Tolerance (BFT)-based protocols and hybrid models - aim to reduce energy consumption, improve finality, and support higher throughput compared to the energy-intensive Proof of Work (PoW) paradigm. Scalability solutions such as sharding, layer-2 rollups, and state channels have been introduced to overcome throughput bottlenecks, enabling blockchains to process a

growing volume of transactions efficiently. Meanwhile, privacy technologies such as zero-knowledge proofs (ZKPs), ring signatures, homomorphic encryption, and secure multi-party computation (SMPC) have emerged to protect sensitive data while maintaining verifiability and compliance with increasingly strict regulatory requirements.

Despite these advances, blockchain still faces several systemic challenges that hinder mainstream adoption. Interoperability remains a critical barrier, as existing blockchain networks operate in isolated silos with limited capacity for seamless asset and data transfer. Energy efficiency, though improved in newer consensus models, continues to be a concern for large-scale networks, particularly those transitioning from PoW. Privacy compliance and regulatory alignment pose additional complexity, as enterprises must balance the transparency of distributed ledgers with data protection mandates such as the General Data Protection Regulation (GDPR) and emerging digital asset regulations across jurisdictions. Furthermore, large-scale deployment challenges persist due to latency issues, storage overhead, and the difficulty of integrating blockchain systems with heterogeneous legacy infrastructures.

Emerging trends suggest that the next decade of blockchain research and development will be shaped by the convergence of distributed ledger technology with other transformative paradigms. AI-enhanced blockchain networks are being explored to optimize consensus efficiency, predict network congestion, and enable adaptive smart contract execution. Federated learning over blockchain is gaining traction as a privacy-preserving approach to training machine learning models across decentralized participants while maintaining data sovereignty. Edge-cloud integration promises to reduce latency and support real-time decentralized applications, particularly in the Internet of Things (IoT) and autonomous systems. At the same time, standardized cross-chain protocols and interoperability frameworks are advancing to create unified ecosystems that bridge currently fragmented networks, allowing assets and data to move securely across diverse platforms.

By synthesizing the state of the art and systematically identifying these emerging directions, this survey seeks to guide both scholars and practitioners in designing the next generation of blockchain-based systems. Specifically, it aims to illuminate the key design trade-offs among scalability, security, privacy, and energy efficiency while offering a forward-looking perspective on how to achieve secure, scalable, and sustainable decentralized infrastructures. These insights will be essential for enabling future digital ecosystems - ranging from finance and supply chain to healthcare, IoT, and smart cities - where trustless, transparent, and high-performance distributed systems form the backbone of innovation and global connectivity.

## References


[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014.

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

[4] G. Liang, M. Zhao, and S. Shetty, "Integrating blockchain with healthcare: A systematic review," IEEE Access, vol. 9, pp. 137447–137458, 2021.

[5] K. Salah et al., "Blockchain for IoT security and privacy: The case study of smart grid," IEEE Communications Magazine, vol. 57, no. 10, pp. 68–73, 2019.

[6] J. Poon and T. Dryja, "The Bitcoin lightning network: Scalable off-chain instant payments," 2016.

[7] Y. Zhang and R. Xue, "Security and privacy on blockchain," ACM Computing Surveys, vol. 52, no. 3, pp. 1–34, 2020.

[8] M. Crosby et al., "Blockchain technology: Beyond bitcoin," Applied Innovation Review, vol. 2, pp. 6–10, 2016.

[9] Z. Zheng et al., "An overview of blockchain technology: Architecture, consensus, and future trends," IEEE International Congress on Big Data, pp. 557–564, 2017.

[10] 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.

[11] X. Xu et al., "A taxonomy of blockchain-based systems: From architecture to governance," Future Generation Computer Systems, vol. 107, pp. 605–618, 2020.

[12] C. Li et al., "Scaling blockchain systems via sharding: A survey," IEEE Access, vol. 8, pp. 14155–14181, 2020.

[13] M. Mingxiao et al., "A review of consensus algorithms in blockchain," IEEE International Conference on Systems, Man, and Cybernetics, pp. 2567–2572, 2017.

[14] M. Conti et al., "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[15] A. Kosba et al., "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," IEEE Symposium on Security and Privacy, pp. 839–858, 2016.

[16] Q. Lu et al., "Blockchain-enabled federated learning: A survey," IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12472–12491, 2021.

[17] G. Zyskind et al., "Enigma: Decentralized computation platform with guaranteed privacy," arXiv:1506.03471, 2015.

[18] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," 2012.

[19] T. Ruffing et al., "Coinshuffle: Practical decentralized coin mixing for bitcoin," ESORICS, pp. 345–364, 2014.

[20] E. Buchman, "Tendermint: Byzantine fault tolerance in the age of blockchains," M.S. thesis, Univ. of Guelph, 2016.

[21] Y. Gilad et al., "Algorand: Scaling byzantine agreements for cryptocurrencies," ACM Symposium on Operating Systems Principles, pp. 51–68, 2017.

[22] J. Wang et al., "SoK: Sharding on blockchain," IEEE Security & Privacy Workshops, pp. 95–100, 2019.

[23] V. Buterin, "An incomplete guide to rollups," Ethereum Foundation Blog, 2021.

[24] S. Popov, "The Tangle: IOTA white paper," 2018.

[25] E. Ben-Sasson et al., "Zerocash: Decentralized anonymous payments from bitcoin," IEEE Symposium on Security and Privacy, pp. 459–474, 2014.

[26] E. Ben-Sasson et al., "Scalable zero knowledge via recursive proofs," Advances in Cryptology, pp. 108–136, 2021.

[27] F. Brasser et al., "TEE-based smart contracts: Trust and privacy on blockchains," arXiv:1612.06813, 2016.

[28] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," 2015.

[29] E. Kokoris-Kogias et al., "OmniLedger: A secure, scale-out, decentralized ledger via sharding," IEEE Symposium on Security and Privacy, pp. 583–598, 2018.

[30] L. Luu et al., "Power of stake: Energy-efficient consensus in blockchains," Proceedings of the 2019 IEEE Symposium on Security and Privacy Workshops, pp. 115–122, 2019.

[31] D. Das, M. S. Rahman, and M. S. Rahman, "Privacy-preserving blockchain frameworks: A comprehensive survey," Future Generation Computer Systems, vol. 136, pp. 238–254, 2022.

[32] L. Qin et al., "Cross-chain technology in blockchain: A survey," IEEE Access, vol. 8, pp. 62078–62094, 2020.

[33] Y. Kang et al., "Incentive design for federated learning: A blockchain-based approach," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5833–5849, 2021.

[34] H. Kim et al., "Artificial intelligence-enabled blockchain: A survey," IEEE Access, vol. 9, pp. 61080–61099, 2021.

[35] IEEE Standards Association, "IEEE P2418: Standard for the Framework of Blockchain Use in the Internet of Things."