JOURNAL OF RESEARCH PERSPECTIVES IN MULTIDISCIPLINARY SCIENCE, EDUCATION AND TECHNOLOGY (RPSET)
VOL: 1, ISSUE 1, JANUARY – MARCH 2026
RCHUB PUBLISHER
ISSN: 3139-3934

A COMPREHENSIVE REVIEW OF BLOCKCHAIN TECHNOLOGY: ARCHITECTURES, PROTOCOLS, AND CROSS-DOMAIN APPLICATIONS

K.Rajasanakari
Research scholar, Department of Computer Applications,
Bharath Institute of Higher Education & Research,
Selaiyur, Chennai-600 073,
sankari.manigandan27@gmail.com
https://orcid.org/0009-0003-8178-5312

Dr.S. Silvia Priscila
Associate Professor, Department of Computer Science,
Bharath Institute of Higher Education & Research,
Selaiyur, Chennai-600 073,
silviaprisila.cbcs.cs@bharathuniv.ac.in

Abstract:

Blockchain technology has evolved from its origins as the foundational ledger for cryptocurrencies to a disruptive paradigm for decentralized, transparent, and secure data management across numerous sectors. This review paper provides a systematic analysis of core blockchain architectures, consensus protocols, and smart contract functionalities that enable its diverse applications. We examine the transition from public, permissionless networks to private and consortium models tailored for enterprise needs. The paper surveys seminal and contemporary research across key domains including decentralized finance (DeFi), supply chain provenance, healthcare data exchange, electronic voting, and the Internet of Things (IoT). By synthesizing findings from foundational protocols to cutting-edge cross-chain solutions, we identify common technical motifs and domain-specific implementations. Furthermore, the review delineates persistent challenges such as scalability trilemmas, interoperability gaps, regulatory uncertainty, and significant energy consumption. This consolidated analysis aims to serve as a reference for researchers and practitioners, highlighting both the transformative potential and the critical limitations of blockchain techniques as a trustless infrastructure for the digital age.

Keywords:

Blockchain, Decentralization, Smart Contracts, Distributed Applications, Consensus Mechanisms, Interoperability

1. Introduction:

The concept of a distributed, immutable ledger, now ubiquitously known as blockchain, emerged in 2008 through the seminal Bitcoin whitepaper published under the pseudonym Satoshi Nakamoto. Originally conceived as a peer-to-peer electronic cash system designed to operate without trusted intermediaries like banks or governments, blockchain's underlying architecture proved to be its most revolutionary contribution. At its core, a blockchain is a cryptographically secured, append-only chain of data blocks, maintained by a distributed network of nodes through a consensus mechanism. This design confers the paramount properties of decentralization, transparency, auditability, and immutability—characteristics that have ignited interest far beyond digital currencies [1]-[2].

The fundamental innovation lies in solving the Byzantine Generals' Problem in a trustless environment. By combining public-key cryptography, cryptographic hashing (e.g., SHA-256), and a consensus protocol like Proof-of-Work (PoW), blockchain creates a single source of truth that is extremely resistant to tampering and fraud. Each block contains a batch of transactions, a timestamp, a reference (hash) to the previous block, and a nonce, forming a chronologically interlinked chain [3]. Altering any piece of data in a historical block would require recomputing the hashes for that block and all subsequent blocks, an endeavor that is computationally infeasible given the honest majority control of the network's hashing power. This security model eliminates the need for a central authority to validate transactions, shifting trust from institutions to code and cryptographic proof [4].

The evolution of blockchain is marked by distinct generations. Blockchain 1.0 is epitomized by Bitcoin, focusing almost exclusively on cryptocurrency transactions. Blockchain 2.0 was ushered in by Ethereum, which introduced a Turing-complete virtual machine, enabling the deployment of self-executing *smart contracts*. These programmable scripts automatically enforce contract terms when predefined conditions are met, unlocking a vast design space for Decentralized Applications (DApps). This shift transformed blockchain from a financial ledger into a global, decentralized computing platform [5]. The ongoing exploration of Blockchain 3.0 seeks to address the scalability and interoperability limitations of earlier generations, with projects aiming for higher transaction throughput, cross-chain communication, and sustainable consensus models like Proof-of-Stake (PoS).

The applications of blockchain techniques are now profoundly diverse, driven by the technology's core value proposition: enabling verifiable and transparent interactions between mutually distrusting parties. In finance, it has spawned the entire DeFi ecosystem, encompassing lending, borrowing, and trading without traditional intermediaries. Supply chain management leverages blockchain for end-to-end provenance tracking, combating counterfeit goods and ensuring ethical sourcing. Healthcare systems explore blockchain for secure, patient-centric medical record exchange. Governments and organizations pilot blockchain-based voting systems for enhanced auditability and reduced fraud. Furthermore, it integrates with IoT to create secure machine-to-machine economies and data marketplaces [6].

However, this rapid expansion is not without significant complexity. The blockchain landscape is fragmented into various architectures—public, private, and consortium—each with distinct trade-offs between openness, control, and performance. Consensus mechanisms, from energy-intensive PoW to more efficient PoS, Delegated PoS, and Practical Byzantine Fault Tolerance (PBFT), define a network's security, decentralization, and speed. The development of DApps introduces challenges in software engineering, user experience, and legal compliance.

This review paper is structured to provide a holistic survey of this multifaceted field. Following this introduction, we present a detailed literature review of foundational and applied research across thirteen key papers. We then formalize the central problem statement, exploring the tension between blockchain's idealistic tenets and practical deployment requirements. Subsequently, we analyze the profound technical and non-technical challenges that limit wider adoption. Finally, we conclude with reflections on the trajectory of blockchain technology, assessing its role in building future decentralized infrastructures.

2. Literature Review:

Nakamoto, S., [7] This foundational paper introduced the world to blockchain technology. Nakamoto proposed a purely peer-to-peer version of electronic cash, solving the double-spending problem without a trusted authority. The core innovation was the Proof-of-Work consensus mechanism and the incentive-driven model for network security, combining timestamped transactions, cryptographic hashing, and economic game theory to create a decentralized, tamper-resistant ledger. It established the archetype for all subsequent blockchain systems.

Buterin, V., "[8] Buterin's whitepaper marked the transition to Blockchain 2.0 by proposing Ethereum, a blockchain with a built-in Turing-complete programming language. This allowed developers to create arbitrary smart contracts and decentralized applications (DApps). The introduction of the Ethereum Virtual Machine (EVM) abstracted the underlying blockchain, enabling complex logic and programmable value, thereby expanding blockchain's utility far beyond simple currency transactions.

This research moved beyond the static design of Bitcoin to analyze its dynamic behavior as a complex, incentive-driven system. It studied the interplay between miners, transaction fees, block size, and network propagation delays. The paper provided critical insights into the economic and game-theoretic forces that secure the network, highlighting potential vulnerabilities like selfish mining and the long-term sustainability of the mining reward model [9].

Wood, G., [10] The Ethereum Yellow Paper formalized the protocol's technical specification with mathematical and algorithmic precision. It detailed the state transition function, the EVM instruction set, gas mechanics, and the consensus model. This formalization was crucial for developers, security auditors, and researchers, providing a rigorous foundation for implementation, verification, and the analysis of smart contract security.

Eyal, I., & Sirer, E.G., [11] This seminal paper exposed a critical flaw in Bitcoin's incentive structure by describing the "Selfish Mining" attack. It demonstrated that a miner or pool controlling more than 25% of the network hash rate could gain a disproportionate revenue share, undermining the assumed fairness of the Nakamoto consensus. This work highlighted that blockchain security relies on rational, not just honest, participant behavior.

Zheng, Z., et al.,[12]. This early survey provided a structured taxonomy of blockchain technology. It systematically classified consensus algorithms (PoW, PoS, PBFT), compared architectural types (public, private, consortium), and outlined key challenges like scalability and privacy. It served as an essential roadmap for newcomers to the field, connecting fundamental concepts to research directions.

Benet, J [13]. While not a blockchain per se, the InterPlanetary File System (IPFS) is a foundational decentralized storage protocol often integrated with blockchains. It proposes a content-addressed, peer-to-peer hypermedia protocol to make the web faster, safer, and more

open. Its integration with blockchain (e.g., for storing large data hashes) is a key enabler for DApps that require decentralized storage solutions beyond on-chain data.

Poon, J., & Dryja, T., "[14]. This whitepaper introduced the Lightning Network as a Layer-2 scaling solution for Bitcoin. It proposed off-chain payment channels that allow for near-instant, high-volume, low-fee transactions, which are later settled on the main blockchain. This work pioneered the concept of moving transactions off-chain to alleviate congestion and scalability limitations, a principle later adopted by many other blockchain networks.

Buterin, V., & Griffith, V., "[15]. This paper outlined Casper, Ethereum's transition from Proof-of-Work to a hybrid Proof-of-Stake consensus mechanism. It introduced the concept of "finality" as a safety property, where validators stake ether to participate in block validation and face slashing penalties for malicious behavior. This represented a major shift towards a more energy-efficient and arguably more secure consensus model.

Kosba, A., et al., [16]. Hawk addressed the critical privacy limitation of transparent blockchains. It proposed a framework for creating privacy-preserving smart contracts where financial transactions and contract logic are encrypted on-chain, yet remain verifiable. While relying on a manager for setup, it demonstrated that zero-knowledge cryptography could be integrated to balance privacy with public auditability.

Luu, L., et al. [17], This paper presented Elastico, one of the first provably secure sharding protocols for permissionless blockchains. Sharding partitions the network into smaller committees (shards) that process transactions in parallel, aiming to linearly increase throughput with network size. Elastico laid important groundwork for scaling blockchain transaction capacity without compromising security, a direction actively pursued by networks like Ethereum 2.0.

3. Problem Statement:

The central problem addressed by blockchain technology is the creation of reliable, verifiable consensus and immutable record-keeping in open, distributed systems where participants may not trust each other or a central coordinating authority. This fundamental problem, known as the Byzantine Generals' Problem, is exacerbated in digital environments where data can be easily replicated and altered. Traditional centralized systems rely on a trusted third party (TTP) to maintain the canonical state and validate transactions. This model introduces single points

of failure, creates opportunities for censorship and fraud, and requires users to place implicit trust in the operator's integrity and security.

Blockchain proposes a radical alternative: a decentralized network where trust is *architected* rather than *assigned*. The problem, therefore, is decomposed into achieving secure consensus on a chronological transaction history across geographically dispersed, potentially adversarial nodes, without a central referee. This encompasses several interrelated sub-problems:

1. **Consensus in Adversarial Conditions:** How can a distributed network agree on a single truth (the next valid block) when some nodes may be malicious or faulty? The solution must be resistant to Sybil attacks, where an adversary creates many fake identities.
2. **Data Immutability and Integrity:** How can the agreed-upon record be made practically tamper-proof? Any solution must ensure that modifying past records is computationally infeasible, providing a robust audit trail.
3. **Incentive Alignment:** In open, permissionless settings, why should rational participants contribute valuable resources (compute power, stake) to maintain the network? The system must provide a sustainable economic model that rewards honest behavior and penalizes malicious actions.
4. **Functional Programmability:** Beyond simple asset transfers, how can this trusted compute environment be extended to enforce complex, conditional logic (smart contracts) in a deterministic and secure manner?

The evolution of blockchain applications reveals an extended problem statement: While blockchain solves the core trust problem for simple state transitions, its naive implementation introduces new critical limitations—namely scalability, energy consumption, privacy, and interoperability—that hinder its adoption for global, high-performance, and complex multi-party applications. Thus, the contemporary problem space involves not just achieving decentralized consensus, but doing so in a way that is scalable, efficient, private, and capable of interacting with other systems (both blockchain and traditional). The tension between decentralization, security, and scalability—often called the "blockchain trilemma"—encapsulates the core engineering and research challenge facing the field today.

4. Challenges and Limitations:

Despite its transformative potential, blockchain technology faces profound challenges that span technical, governance, economic, and regulatory domains, limiting its widespread and efficient adoption.

1. The Scalability Trilemma: Articulated by Vitalik Buterin, this posits that a blockchain system can only optimally deliver two of the three following properties: **Decentralization** (many nodes participate in consensus), **Security** (resistance to attack), and **Scalability** (high transaction throughput). Bitcoin and Ethereum 1.0 prioritize decentralization and security, resulting in low transaction throughput (e.g., 7 TPS for Bitcoin) and high latency. Efforts to scale, such as increasing block size, can compromise decentralization by raising hardware requirements for node operators. Solutions like sharding and Layer-2 networks are promising but add complexity and may introduce new security assumptions or centralization pressures.

2. Energy Consumption and Environmental Impact: Proof-of-Work consensus, used by Bitcoin and previously by Ethereum, is notoriously energy-intensive. The "hash rate" security model directly correlates to massive electricity consumption, raising serious environmental, social, and governance (ESG) concerns. While a transition to Proof-of-Stake (as with Ethereum's Merge) dramatically reduces energy use, PoS introduces potential risks related to wealth concentration and different attack vectors like long-range attacks. The sustainability of consensus mechanisms remains a critical design choice.

3. Interoperability and Fragmentation: The blockchain ecosystem is increasingly fragmented into thousands of isolated networks ("silos") with their own rules, assets, and communities. Transferring value or data between these chains is complex and risky, relying on centralized custodians or decentralized bridges that have become major attack targets, with billions lost to bridge hacks. The lack of seamless interoperability hinders user experience and the development of truly cross-chain applications.

4. Privacy and Confidentiality: The transparency of most public blockchains is a double-edged sword. While it enables auditability, it also exposes all transaction details (amounts, participants) to anyone. This is unacceptable for enterprise and many personal use cases. Privacy-enhancing technologies (PETs) like zero-knowledge proofs (ZKPs) and confidential

transactions exist but are often computationally expensive, complex to implement correctly, and can complicate regulatory compliance.

5. Regulatory Uncertainty and Compliance: The decentralized and global nature of public blockchains creates a significant clash with traditional, jurisdictionally bound legal and regulatory frameworks. Issues around the legal status of digital assets, securities law, anti-money laundering (AML), know-your-customer (KYC) requirements, and taxation are unresolved and evolving unevenly across the globe. This uncertainty stifles institutional adoption and innovation.

6. Smart Contract Security and Formal Verification: Smart contracts are immutable once deployed, making vulnerabilities catastrophic. High-profile exploits of flawed contract logic have led to enormous financial losses. The field of smart contract auditing and formal verification—mathematically proving a contract behaves as specified—is advancing but remains a specialized, resource-intensive process. Developing secure DApps requires a level of expertise that is still scarce.

7. User Experience and Key Management: Blockchain applications often have steep learning curves. Users must manage private keys—the sole proof of ownership for their assets—with no recourse if keys are lost or stolen. Concepts like gas fees, seed phrases, and wallet addresses are alien to mainstream users. Improving UX without compromising self-custody and decentralization is a major hurdle.

8. On-Chain and Off-Chain Data Oracle Problem: Smart contracts cannot natively access data from outside their blockchain (e.g., stock prices, weather data). They rely on oracles—third-party services—to feed this information on-chain. This reintroduces a point of trust and potential failure/ manipulation. Creating decentralized, reliable, and tamper-proof oracles is an ongoing challenge.

9. Governance and Protocol Upgrades: Decentralized networks face the meta-challenge of governing themselves. How are decisions about protocol upgrades made? Processes range from informal core developer consensus (Bitcoin) to on-chain governance (Tezos, MakerDAO). All models struggle with voter apathy, plutocratic tendencies (vote weight based on stake), and the difficulty of coordinating diverse stakeholders, potentially leading to contentious hard forks.

5. Conclusion:

Blockchain technology has undeniably established itself as a foundational innovation for the digital era, offering a novel paradigm for trustless coordination and verifiable data management. This review has traced its journey from a niche cryptographic experiment to a multi-faceted ecosystem underpinning cryptocurrencies, decentralized finance, transparent supply chains, and beyond. The core architectural principles of decentralization, cryptographic security, and immutability provide compelling solutions to longstanding problems of intermediary trust and data integrity.

However, the path to mainstream adoption is paved with significant obstacles. The scalability trilemma, energy consumption concerns, interoperability gaps, regulatory complexities, and user experience barriers collectively represent a formidable set of challenges that the field must overcome. Current research and development are vigorously targeting these limitations through layered scaling solutions, efficient consensus mechanisms, cross-chain communication protocols, privacy-preserving cryptography, and improved governance models.

The future of blockchain likely lies not in a single, dominant chain but in a heterogeneous, interconnected ecosystem of specialized networks. Success will depend on the technology's ability to integrate seamlessly with existing systems (legacy and digital), operate sustainably, and navigate the evolving global regulatory landscape. As foundational infrastructure, blockchain’s ultimate value may become most visible when it is largely invisible—serving as a reliable, open-standard backend for identity, asset ownership, and secure data exchange. While it is not a panacea for all problems of trust and efficiency, blockchain techniques offer a powerful new toolkit for re-architecting socio-economic systems in a more transparent, participatory, and resilient manner.

References:

[1.] Li, L., Wu, J., & Cui, W. (2023). A review of blockchain cross-chain technology. *IET Blockchain*, *3*(3), 149-158.

[2.] Ezawa, Y., Kakei, S., Shiraishi, Y., Mohri, M., & Morii, M. (2023). Blockchain-based cross-domain authorization system for user-centric resource sharing. *Blockchain: Research and Applications*, *4*(2), 100126.

[3.] Wang, W., Hu, N., & Liu, X. (2018, June). BlockCAM: A blockchain-based cross-domain authentication model. In *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)* (pp. 896-901). IEEE.

[4.] Hao, X., Ren, W., Fei, Y., Zhu, T., & Choo, K. K. R. (2022). A blockchain-based cross-domain and autonomous access control scheme for internet of things. *IEEE Transactions on Services Computing*, *16*(2), 773-786.

[5.] Huang, C., Xue, L., Liu, D., Shen, X., Zhuang, W., Sun, R., & Ying, B. (2022). Blockchain-assisted transparent cross-domain authorization and authentication for smart city. *IEEE Internet of Things Journal*, *9*(18), 17194-17209.

[6.] Singh, P., Masud, M., Hossain, M. S., & Kaur, A. (2021). Cross-domain secure data sharing using blockchain for industrial IoT. *Journal of Parallel and Distributed Computing*, *156*, 176-184.

[7.] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, *4*(2), 15.

[8.] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*, *3*(37), 2-1.

[9.] Zhang, H., Chen, X., Lan, X., Jin, H., & Cao, Q. (2020). BTCAS: A blockchain-based thoroughly cross-domain authentication scheme. *Journal of Information Security and Applications*, *55*, 102538.

[10.] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, *151*(2014), 1-32.

[11.] Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, *61*(7), 95-102.

[12.] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). Ieee.

[13.] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*.

[14.] Poon, J., & Dryja, T. (2016, January). *The bitcoin lightning network: Scalable off-chain instant payments*.

[15.] Buterin, V., & Griffith, V. (2017). Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437*.

[16.] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: the blockchain model of cryptography and privacy- preserving smart con- tracts. In *2016 IEEE Symposium on Security and Pri- vacy (SP), San Jose, CA. New York, USA: IEEE*.

[17.] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 17-30).