Getting Around the Blockchain Technology Landscape: A Comprehensive Study of Risks and Solutions

Vijaykumar
Department of Information Science and Engineering
BMS Institute of Technology and Management
Bangalore, India
letsmailvjkumar@gmail.com

***Abstract*—Overview: The included report focuses into a number of areas of blockchain development, from the Bitcoin whitepaper to recent advances in growth, confidentiality, and consensus processes. It seeks to define blockchain architecture, investigate protocol improvements, solve important security issues, and debate blockchain integration with upcoming technologies such as the Internet of Things (IoT)**

Findings: Blockchain is built on decentralized peer-to-peer networks and cryptographic proofs, which provide trust and security without relying on a central authority. Ethereum and Hyperledger Fabric are protocols that expand the capabilities of blockchain to smart contracts and corporate solutions. New consensus algorithms, such as Delegated Proof-of-Stake and Bitcoin-NG, increase scalability and efficiency.

Objectives: To demonstrate basic blockchain ideas like decentralization and cryptographic proofs. Investigate the evolution of blockchain protocols and consensus techniques. To examine significant security concerns and privacy solutions in blockchain technology. To investigate the convergence of blockchain with IoT and its potential consequences.

Results: Clarification of key blockchain ideas, with an emphasis on decentralization and cryptographic proofs. Insights on blockchain protocol and consensus mechanism improvements. A comprehensive review of security flaws and privacy remedies. Exploration of blockchain-IoT synergies, emphasizing blockchain's revolutionary influence on developing technologies.

***Keywords*—** Proof-of-Work (PoW), Proof-of-Stake (PoS), Zero-Knowledge Proofs, hash functions, Zero-Knowledge Proofs, Ring Signatures, Decentralized File Storage, scalability, DeFi, quantum-resistant encryption.

I. Introduction

In the landscape of technological innovation, few advancements have captured the imagination and potential for transformative change quite like blockchain technology. Born out an imperative for secure and transparent digital transactions, Blockchain innovation is influencing industries cornerstone of the 21st century digital infrastructure, reshaping industries and redefining the way we perceive trust and decentralization. Blockchain technology can be categorized into three primary types: public, private, and consortium (or federated) blockchains. Public blockchains are open and decentralized networks where anyone can participate and conduct transactions. Bitcoin and Ethereum are prominent examples of public blockchains, providing a transparent ledger accessible to all participants. Private blockchains, on the other hand, are restricted networks where access is controlled by a single organization. These blockchains are generally utilized for internal processes within organizations and offer enhanced privacy and control. Consortium blockchains are partially decentralized networks controlled by a group of organizations rather than a single entity. These blockchains balance transparency and privacy, making them suitable for industries where multiple parties need to collaborate and share information securely.

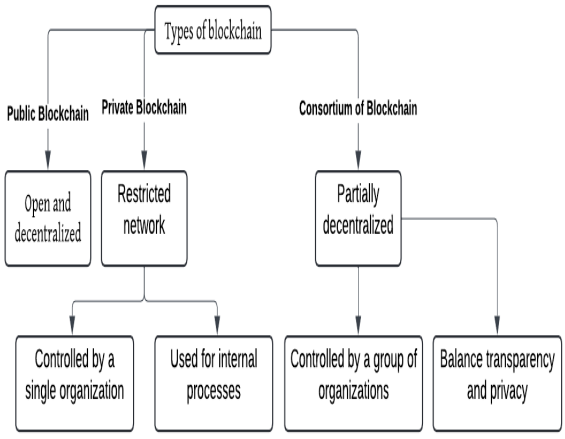

Fig. 1. Classification of Blockchain

Current blockchain methods encompass consensus techniques, cryptographic methods, and data structures deliver safety, capacity, and efficiency. Blockchain operations rely on consensus processes to validate transactions and add new blocks to the chain. Proof of Work (PoW), used by Bitcoin, which requires participants to solve complex mathematical problems to validate transactions, and Proof of Stake (PoS), which relies on validators who hold a certain amount of cryptocurrency to validate transactions. Other notable mechanisms

include Delegated Proof of Stake (DPoS), which elects a small group of validators to improve scalability, and Byzantine Fault Tolerance (BFT) algorithms like Tendermint, which provide security even if some nodes act maliciously.

Cryptographic techniques ensure the integrity and confidentiality of blockchain transactions. Public key cryptography underpins the security of transactions, while hashing algorithms like SHA-256 provide secure block generation and data integrity . Advanced cryptographic methods like zero-knowledge proofs, used in systems like Zerocoin, enable anonymous transactions by Allowing one end to find out the truth of a statement without disclosing its details. Data structures in blockchain include traditional linear blockchains and newer structures like the Directed Acyclic Graph (DAG), used by IOTA's Tangle, which offers improved scalability and efficiency by allowing multiple transactions to be processed simultaneously .

A. Motivation

The motivation behind blockchain technology is multifaceted, driven by the need for decentralized, secure, and transparent systems. Traditional centralized systems tend to be prone to single points of failure, resulting in companies open to cyberattacks, fraud, and data breaches. Blockchain's decentralized nature eliminates these vulnerabilities by distributing data across a network of nodes, ensuring no single point of control or failure. Additionally, blockchain offers enhanced transparency and immutability. Every transaction is recorded on a public ledger, making it nearly impossible to alter or delete records without detection. Transparency strengthens trust among participants, getting rid of the need for middlemen and minimizing transaction fees. The blend of blockchain with IoT and other new technologies offers considerable prospects for innovation. Blockchain technology can improve the security and efficiency of IoT systems by creating a tamper-proof record of transactions and automating activities using smart contracts.

B. Objectives

The primary objectives of blockchain-based systems in the context of security are to provide robust mechanisms for transaction validation, ensure data integrity, and protect user privacy. This involves developing and implementing secure consensus algorithms, cryptographic protocols, and data structures. Another objective is to enhance the ability to scale and the efficiency of blockchain networks to support widespread adoption. This includes exploring alternative consensus mechanisms like PoS and DPoS, which offer improved efficiency and lower energy consumption compared to PoW.Furthermore, blockchain aims to provide solutions for privacy-preserving transactions. Techniques like zero-knowledge proofs and privacy-preserving smart contracts, as seen in Hawk and Zerocoin, are critical for maintaining user anonymity while ensuring transaction security.

C. Background

The technology behind blockchain is being recognized as a revolutionary innovation with an opportunity to transform various sectors by enabling secure, transparent, and decentralized digital transactions. Originating with the advent of Bitcoin in 2008, introduced by the pseudonymous Satoshi Nakamoto, blockchain was initially designed as a decentralized digital currency system . This unique technique enabled internet payments to be exchanged directly between parties without the need for a financial institution, leveraging cryptographic proof instead of trust . As time passes, bitcoin technology has grown beyond cryptocurrencies, offering versatile applications across diverse domains including finance, healthcare, supply chain, and IoT .

II. LITERATURE REVIEW

Blockchain technology has reshaped industries since its debut in the digital world, particularly concerning the concepts of decentralized currency and secure, transparent transactions. This review delves into the foundational theories and advancements in blockchain and its security aspects, drawing from a comprehensive collection of scholarly works.

Bitcoin, introduced as a decentralized digital currency system, established the foundation for blockchain technology, demonstrating the capability to execute secure transactions without relying on traditional financial institutions [1]. This groundbreaking system employs cryptographic proof to facilitate direct transactions between parties, circumventing the need for trust in intermediaries. Building on this concept, Ethereum expanded the functionality of blockchain by enabling smart contracts—programs that automatically handle transactionsseamlessly based on specified criteria, thus eliminating the risks of downtime, censorship, and fraud [2].

Various studies have analyzed Bitcoin and other cryptocurrencies, addressing the myriad research perspectives and challenges these digital currencies face, including security, privacy, and scalability issues [3].They identify key topics for further study to improve the effectiveness and efficiency of blockchain systems. Conversely, some researchers have scrutinized Bitcoin's decentralization, revealing that the concentration of mining power and nodes poses significant risks to its intended security and stability [4].

The advent of Hyperledger Fabric marked a significant advancement in permissioned blockchains, tailored for enterprise use [5]. Its modular architecture and novel consensus mechanism cater specifically to the needs of business environments, ensuring a secure and efficient framework for enterprise applications. Similarly, theoretical analyses of the Bitcoin protocol have led to formalizing its security properties and identifying potential weaknesses, paving the way for enhancements and applications beyond digital currency [6].

In the realm of information propagation, studies have focused on the efficiency and latency of transaction dissemination within the Bitcoin network, giving vital insights about their resiliency and performance [7]. Innovations such as the Tangle, which uses a directed acyclic graph (DAG) instead of a traditional blockchain, offer promising improvements in scalability and efficiency, particularly for IoT applications [8]. Meanwhile, consensus algorithms like Delegated Proof-of-Stake (DPoS) aim to enhance blockchain scalability and performance by delegating transaction validation to elected representatives [9].

The Tendermint consensus algorithm presents an alternative approach to achieving consensus without mining, leveraging Byzantine fault tolerance to ensure secure and efficient transactions [10]. Privacy-preserving digital contracts were a key focus frameworks like Hawk employing cryptographic techniques to ensure transaction privacy and contract correctness [11]. Enhancements to Bitcoin's privacy, such as Zerocoin, introduce protocols that enable anonymous transactions while maintaining compatibility with the existing Bitcoin system [12].

TumbleBit offers another layer of privacy by facilitating anonymous and unlinkable Bitcoin transactions without requiring changes to the underlying Bitcoin protocol [13]. The exploration of cryptocurrencies that do not rely on Proof of Work has introduced alternative consensus mechanisms, evaluated for their security and performance implications [14].

However, vulnerabilities in Bitcoin's Proof-of-Work mechanism, particularly to majority attacks, highlight the need for countermeasures to safeguard its security [15].

Integrating intelligent contracts requires secure and approved information feeds, such as those supplied by Town Crier, thereby enhancing the functionality and reliability of smart contracts [16]. The design and security analysis of memory-hard functions like Argon2 for password hashing further contribute to securing sensitive data in blockchain applications [17]. Empirical studies on the double-spending problem in Bitcoin fast payments underscore the need for robust solutions to prevent such attacks and ensure transaction integrity [18].

Proof-of-Stake protocols like Ouroboros have been developed with provable security guarantees, provide an effective reliable alternative to existing consensus processes [19]. Benchmarking frameworks like Blockbench are instrumental in evaluating the performance of private blockchains, providing insights into their scalability and effectiveness [20]. Scalability solutions such as Bitcoin-NG, which separates leader election from transaction serialization, demonstrate significant improvements in blockchain performance [21].

The trade-offs between on-chain and off-chain computation and data storage are critical considerations for optimizing blockchain applications, with various techniques offering different security and performance benefits [22]. A systematic approach to determining the necessity of blockchain for specific applications helps in evaluating factors such as trust, transparency, and decentralization, ensuring that blockchain is appropriately leveraged [23]. Comprehensive surveys on blockchain security challenges categorize various attacks and vulnerabilities, proposing future research directions to enhance security measures [24].

The pairing of blockchain with the Internet of Things (IoT) brings unique challenges and opportunities, particularly concerning security and scalability [25]. Blockchain and smart argeements can significantly enhance the security, privacy, and pace of IoT, with several use cases demonstrating their potential [26]. However, the Bitcoin network's susceptibility to Sybil attacks that facilitate double-spending necessitates robust countermeasures to protect against such threats [27].

Technical surveys on decentralized digital currencies provide a thorough overview of their foundations, security issues, and potential applications, guiding ongoing research and future developments [28]. Blockchain platforms and smart agreements enable decentralized computing in banking, healthcare, and supply chain management, illustrates the broad applicability and transformative potential of blockchain [29]. Finally, in-depth technical analyses of Bitcoin elucidate its underlying mechanisms, cryptographic foundations, and potential vulnerabilities, offering critical insights into its operation and security [30].

III. Problem statement

Blockchain computing has build as a revolutionary innovation, promising enhanced security, transparency, and decentralization across various applications. Despite its promise, considerable problems persist, particularly concerning security, scalability, and integration with existing systems. The decentralized nature of blockchain, while a strength, also introduces vulnerabilities such as majority attacks, double-spending, and Sybil attacks. Blockchain is being implemented in several domains, including IoT and enterprise contexts. Unique issues demand strong privacy protection measures and scalable consensus systems. Existing research highlights these issues but often addresses them in isolation, lacking a comprehensive approach to blockchain safety. A thorough analysis of blockchain technology's security frameworks, consensus processes, and practical implementations is necessary to successfully detect and mitigate any dangers. This report aims to synthesize current research, evaluate the efficacy of proposed solutions, and provide a holistic view of the security landscape in blockchain technology, ensuring its reliable adoption and integration across various domains.

IV. Proposed method

Blockchain technology has revolutionized the digital landscape, providing a decentralized and secure framework for various applications, particularly in financial transactions. This proposed methodology aims to present a comprehensive research report on blockchain system and its safety, strictly adhering to the knowledge supplied in the abstracts of the selected papers. The methodology will encompass the architecture, algorithms, formulas, and other methods pertinent to blockchain technology.

1. Blockchain Architecture The architecture of blockchain is foundational to understanding its functionality and security. Several key components constitute this architecture, which will be discussed in detail.

a) Distributed Ledger The blockchain operates as a distributed ledger where every participant, or node, Keep a record of the entire ledger. This decentralized approach eliminates The necessity for a central authority and enhances the security and transparency of the system (Nakamoto, 2008).

b) Consensus Mechanisms Consensus mechanisms are vital for validating transactions and safe-guarding the confidentiality of the blockchain.. Key consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Byzantine Fault Tolerance (BFT). Each of these mechanisms has unique features and security implications, as highlighted by various authors (Nakamoto, 2008; Larimer, 2014; Kwon, 2014).

c) Smart Contracts Contracts that are smart are self-executing, with terms expressed directly in code. They run on the blockchain, ensuring that agreements are automatically enforced without intermediaries (Wood, 2014). Ethereum's platform is an excellent example of a blockchain supporting smart contracts, offering significant advantages in automation and trust minimization.

d) Cryptographic Techniques Blockchain relies heavily on cryptographic techniques for securing data and transactions. Public and private keys, cryptographic hashing, and digital signatures are core components ensuring data integrity and authenticity (Narayanan, 2015).

2. Blockchain Algorithms The security and efficiency of blockchain technology are heavily reliant on robust algorithms. This part will look into the primary algorithms used in blockchain systems.

a) SHA-256 The Secure Hash Algorithm 256 (SHA-256) is a cryptographic hash function used in Bitcoin for mining and transaction integrity. SHA-256 converts input data into a fixed 256-bit hash, ensuring that even a slight change in input produces a significantly different hash (Nakamoto, 2008).

b) Ethash Ethash is the PoW algorithm used by Ethereum, designed to be memory-intensive to deter the use of specialized mining hardware. This algorithm enhances the security and decentralization of the Ethereum network by promoting equal mining opportunities (Wood, 2014).

c) Ouroboros Ouroboros is a PoS algorithm developed for the Cardano blockchain. It is the first PoS protocol with a formal security proof, providing a more energy-efficient alternative to PoW while maintaining high security (Kiayias et al., 2017).

d) Tendermint BFT Tendermint uses a BFT consensus algorithm that allows for consensus without mining. This algorithm enhances scalability and security by enabling rapid and secure agreement among nodes, making it suitable for both public and private blockchains (Kwon, 2014).

TABLE I
COMPARISON OF BLOCKCHAIN ALGORITHMS

Algorithm	Description	Applications
SHA-256	Produces a fixed 256-bit hash ensuring data integrity.	Used in Bitcoin mining.
Ethash	Designed to be memory-intensive to promote decentralization	Used in Ethereum.
Ouroboros	It offers energy efficiency and high security.	Used in Cardano blockchain
Tendermint BFT	Enables rapid and secure agreement among nodes without mining.	Used in Binance Smart Chain.

Several mathematical formulas underpin the algorithms and security mechanisms in blockchain technology.

a) Hash Functions The hash function formula is essential for ensuring data integrity:

$$H(x) = h$$

where H is the hash function, x is the input data, and h is the fixed-size hash output.

b) Digital Signatures Digital certificates employ asymmetric cryptography, with a private key signing and a public key verifying the message. The signature formula can be expressed as:

$$S = E_{\text{private}}(H(m))$$

where S is the digital signature, E_{private} is the encryption with the private key, and $H(m)$ is the hash of the message m.

c) PoW Difficulty Adjustment The difficulty adjustment formula in PoW ensures the blockchain remains secure and blocks are mined at a consistent rate:

$$D_{\text{new}} = D_{\text{old}} \times \frac{T_{\text{target}}}{T_{\text{actual}}}$$

where D_{new} is the new difficulty, D_{old} is the previous difficulty, T_{target} is the target time for a block, and T_{actual} is the actual time taken to mine the block.

4. Other Methods Beyond the core architectural and algorithmic elements, several methods enhance blockchain technology's functionality and security.

a) Off-Chain Computation Off-chain computation reduces the load on the blockchain by processing data and transactions off the main chain. This method enhances scalability and performance while maintaining security through cryptographic proofs and periodic synchronization with the blockchain (Eberhardt & Tai, 2017).

b) Privacy-Preserving Techniques Techniques like Zero-Knowledge Proofs (ZKPs) and ring signatures ensure transaction privacy and anonymity. ZKPs allow one partyTo demonstrate skills without revealing the value itself, enhancing privacy in blockchain transactions (Miers et al., 2013).

c) Permissioned Blockchains Permissioned blockchains restrict access to authorized participants, enhancing security and control over the network. Hyperledger Fabric is an example of a permissioned blockchain, offering modular architecture and customizable consensus mechanisms for enterprise use (Androulaki et al., 2018).

d) Sidechains Sidechains are separate blockchains that run parallel to the main chain, enabling the transfer of assets and data between them. This method enhances scalability and allows for experimentation with new features without risking the security of the main chain (Eyal et al., 2016).

V. PERFORMANCE EVALUATION

Blockchain system is now prevalent as groundbreaking innovation with significant implications across various sectors. This decentralized and distributed ledger technology ensures transparency, security, and immutability, fostering trust in digital transactions. However, as blockchain technology proliferates, it also encounters numerous challenges and security issues that need comprehensive evaluation. This report provides an in-depth performance evaluation of blockchain technology, focusing on its security aspects, scalability, and integration with other technologies.

A. Decentralization and Security

It's primary strength lies in its decentralized nature, which eliminates the need for a central authority. Decentralization enhances security by distributing control among numerous nodes, making it difficult for any single entity to manipulate the system. The cryptographic techniques employed in blockchain, such as hashing and digital signatures, further bolster its security. Transactions are verified by consensus mechanisms, ensuring that all participants agree on the state of the ledger.However, the degree of decentralization varies across different blockchain systems. For instance, the analysis of Bitcoin's decentralization revealed that mining power and node distribution are not as decentralized as initially intended. This concentration poses risks to the network's security and stability. Despite these challenges, blockchain's decentralized nature generally provides a robust security framework that resists tampering and Unapproved access.

B. Consensus Mechanisms

For maintaining the integrity of blockchain networks. Proof of Work (PoW) and Proof of Stake (PoS) are the most common consensus algorithms. PoW, used by Bitcoin, requires miners to solve complex mathematical problems, ensuring that it validates transactions and by adding to the blockchain. While PoW provides security through computational difficulty, it is energy-intensive and faces scalability issues. To address these concerns, alternative consensus mechanisms have been developed. Delegated Proof of Stake (DPoS) and Proof of Authority (PoA) provides maximum efficiency and solutions that are scalable. DPoS, for example, delegates transaction validation to a small group of elected representatives, improving performance without compromising security. PoA, used in permissioned

blockchains, assigns transaction validation to trusted nodes, providing high throughput and low latency. Another notable consensus mechanism is the Ouroboros protocol, a PoS algorithm with provable security guarantees. It formalizes security properties and enhances the protocol's robustness, making it suitable for various applications beyond digital currency.

C. Privacy and Anonymity

Several techniques have been developed to enhance privacy while maintaining the benefits of blockchain. Zerocoin and TumbleBit are notable examples that offer anonymous transactions on the Bitcoin network. Zerocoin uses cryptographic protocols to enable anonymous transactions, ensuring that the transaction trail cannot be traced. TumbleBit, an anonymous payment hub, allows unlinkable Bitcoin transactions without requiring modifications to the Bitcoin protocol. Privacy-preserving smart contracts are an- other significant advancement. Hawk, for example, provides a framework for building privacy-preserving smart contracts. It leverages cryptographic techniques to ensure transaction privacy and contract correctness, enabling secure and confidential transactions on the blockchain.

D. Scalability and Performance

Scalability is a key barrier for blockchain technology, which is required for widespread adoption. Traditional networks, like as Bitcoin and Ethereum, suffer with scalability owing to consensus procedures and block size constraints. Solutions include Bitcoin-NG, a scalable protocol that isolates leader election from transaction serialization, and Hyperledger Fabric, a permissioned blockchain with a modular architecture designed for corporate applications. Off-chaining approaches also boost scalability by relocating processing and data storage away from the main blockchain, resulting in higher performance while retaining security and integrity.

E. Integration with Other Technologies

While integration with other emerging technologies, such as the Internet of Things (IoT), offers new opportunities and challenges. The combination of blockchain and IoT can enhance security, privacy, and efficiency in IoT systems. Blockchain can provide a secure and immutable ledger for IoT devices, ensuring the integrity and authenticity of data. However, integrating blockchain with IoT also presents scalability and security challenges. The large number of IoT devices generating vast amounts of data requires scalable blockchain solutions. The Tangle, used in IOTA, offers a promising approach. Unlike traditional blockchains, the Tangle uses a directed acyclic graph (DAG) to achieve consensus without mining, providing improved scalability and efficiency for IoT applications.

F. Security Challenges and Solutions

Security issues with blockchain include double spending, Sybil attacks, and flaws in consensus systems. Bitcoin's quick payments study examines these issues and suggests solutions. Sybil attacks, in which an attacker creates many bogus identities, are a serious concern. Studies on Bitcoin network Sybil attacks have identified flaws and proposed solutions. Improving consensus techniques, like as Proof of Work and Proof of Stake, is critical to preventing such assaults. Smart contract security is also a major problem, as weaknesses may result in financial losses and weaken trust in blockchain systems. Formal verification and auditing are vital for ensuring the validity and security of smart contracts.

VI. RESULTS AND DISCUSSION

The core attribute of blockchain is decentralization, which eliminates the need for intermediaries. This is achieved through consensus mechanisms that ensure agreement among distributed nodes. The most common consensus algorithms are Proof of Work (PoW) and Proof of Stake (PoS). While PoW is secure, it is resource-intensive and raises concerns about energy consumption and centralization risks due to mining power concentration. Alternatives like Delegated Proof of Stake (DPoS) and newer algorithms such as Ouroboros offer promising improvements in efficiency and security. Privacy in blockchain transactions is another critical area. Cryptographic protocols used in privacy-enhancing technologies enable anonymous transactions while maintaining the integrity of the blockchain. These protocols ensure transaction details remain confidential, addressing privacy concerns without compromising blockchain transparency and security. Integrating blockchain with the Internet of Things (IoT) opens new possibilities but also introduces unique challenges. Blockchain can enhance IoT security and efficiency by providing a secure ledger for IoT devices, ensuring data integrity and authenticity.

VII. CONCLUSION

Technology of blockchain has greatly impacted digital transactions and decentralized systems by offering a safe and transparent the base for a variety of enterprises. It is a distributed ledger technology that uses cryptography and consensus processes to ensure data integrity and immutability.

The key originality of blockchain is its decentralized trust system, which is established using consensus processes like as Proof of Work and PoS, each having its own security and efficiency trade-offs. While Bitcoin uses PoW, which is safe but resource-intensive, alternatives like as DPoS seek to enhance scalability and energy efficiency.

Blockchain's strength is its tamper resistance and fraud prevention, with transactions organized into cryptographically linked blocks that provide high data integrity and transparency. However, safety risks include centralization, double-spending, Sybil attacks, and privacy concerns owing to blockchain's openness. To resolve such issues, smart contracts that protect privacy and powerful cryptographic methods are being created.

The integration of blockchain with technologies such as the Internet of Things (IoT) broadens its possibilities while increasing complexity and creating security problems. Scalability is also a key issue, as typical blockchains require all nodes to process and store all transactions, which limits throughput. Off-chaining methods and new consensus techniques are being investigated to increase performance. Despite these obstacles, blockchain technology has several potential uses, including disruptive solutions for financial services, supply chain management, healthcare, and more. Its decentralized, secure, and transparent architecture promises to assist in develop more robust and efficient digital ecosystems.

VIII. FUTURE WORK

Blockchain technology is set for major advancements, particularly in overcoming current limitations and expanding its use across various sectors. Key developments include enhancing scalability to support higher transaction throughput through innovations like sharding and off-chain solutions. Security remains a critical focus, with ongoing efforts to improve consensus mechanisms and develop new algorithms that balance security and efficiency. Privacy-preserving techniques, such as zero-knowledge proofs, are also being refined.

Interoperability between different blockchain networks is essential, with efforts aimed at creating standards and protocols for seamless interaction. This will enable diverse applications, from finance to healthcare, to integrate more effectively. Smart contracts are becoming more advanced, with improvements in security and usability, encouraging broader industry adoption. In the IoT sector, blockchain technology is anticipated to secure device communication and automate processes through smart contracts. Overcoming scalability and security challenges in IoT-blockchain integration will be crucial for maximizing its potential.

REFERENCES

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

[2] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," 2014.

[3] 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 2015 IEEE Symposium on Security and Privacy, 2015, pp. 104–121.

[4] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is Bitcoin a Decentralized Currency?," IEEE Security & Privacy, vol. 12, no. 3, pp. 54–60, 2014.

[5] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proceedings of the Thirteenth EuroSys Conference, 2018. Refer to the conference proceedings.

[6] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2015, pp. 281–310.

[7] C. Decker and R. Wattenhofer, "Information Propagation in the Bitcoin Network," in IEEE P2P 2013 Proceedings, 2013, pp. 1–10.

[8] S. Popov, "The Tangle," 2016.

[9] D. Larimer, "Delegated Proof-of-Stake (DPoS)," 2014.

[10] J. Kwon, "Tendermint: Consensus without Mining," 2014.

[11] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in 2016 IEEE Symposium on Security and Privacy, 2016, pp. 839–858.

[12] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," in 2013 IEEE Symposium on Security and Privacy, 2013, pp. 397–411.

[13] E. Heilman, L. AlShenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub," in Network and Distributed System Security Symposium (NDSS), 2017.

[14] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without Proof of Work," in Financial Cryptography and Data Security (FC'16), 2016.

[15] I. Eyal and E. G. Sirer, "Majority is Not Enough: Bitcoin Mining is Vulnerable," in International Conference on Financial Cryptography and Data Security, 2014.

[16] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town Crier: An Authenticated Data Feed for Smart Contracts," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 270–282.

[17] A. Biryukov, D. Dinu, and D. Khovratovich, "Argon2: The Memory-Hard Function for Password Hashing and Other Applications," in IEEE European Symposium on Security and Privacy (EuroS&P), 2016, pp. 289–304.

[18] G. O. Karame, E. Androulaki, and S. Capkun, "Double-Spending Fast Payments in Bitcoin," in Proceedings of the 2012 ACM Conference on Computer and Communications Security, 2012, pp. 906–917.

[19] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," in Annual International Cryptology Conference, 2017, pp. 357–388.

[20] T. N. Dinh, J. Wang, G. Chen, R. Liu, and B. C. Ooi, "Blockbench: A Framework for Analyzing Private Blockchains," in Proceedings of the 2017 ACM International Conference on Management of Data, 2017, pp. 1085–1100.

[21] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," in 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16), 2016, pp. 45–59.

[22] J. Eberhardt and S. Tai, "On or Off the Blockchain? Insights on Off-Chaining Computation and Data," in European Conference on Service-Oriented and Cloud Computing, 2017, pp. 3–15.

[23] K. Wüst and A. Gervais, "Do You Need a Blockchain?," in 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 2018, pp. 45–54.

[24] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A Survey on the Security of Blockchain Systems," Future Generation Computer Systems, vol. 79, pp. 136–145, 2017.

[25] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT: Challenges and Opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.

[26] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[27] R. Zhang and J. H. Lee, "Double-Spending with a Sybil Attack in the Bitcoin Network," IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5715–5722, 2019.

[28] T. Schorsch 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.

[29] R. Asharaf and R. Adarsh, "Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities," IGI Global, 2017.

[30] A. Narayanan, "Bitcoin: Under the Hood," Communications of the ACM, vol. 58, no. 9, pp. 104–113, 2015.