International Journal of Recent Research and Review, Vol. XIX, Issue 2, June 2026
ISSN 2277 – 8322

COMPARATIVE ANALYSIS OF BLOCK CHAIN-BASED SMART CONTRACT FRAMEWORKS: SECURITY, EFFICIENCY, AND DEPLOYMENT CHALLENGES

Naresh poonia
M.Tech Scholar
Department of Computer Science Engineering
University of Technology
nkpoonia.naresh@gmail.com

Abstract- Blockchain technology has transformed digital transactions by introducing decentralized, transparent, and tamper-resistant systems. Smart contracts, which are self-executing programs deployed on blockchain networks, automate contractual agreements without intermediaries. Various blockchain platforms have developed distinct smart contract frameworks with different approaches to security, scalability, execution efficiency, and deployment. This analytical review compares major smart contract frameworks including Ethereum, Hyperledger Fabric, Binance Smart Chain (BNB Chain), Solana, Cardano, and Polkadot. The study evaluates their architectural designs, consensus mechanisms, security features, transaction throughput, and deployment challenges. The analysis highlights the trade-offs between decentralization, security, and performance while identifying future research directions for enhancing smart contract reliability and scalability**.**

Keywords Blockchain Technology; Smart Contracts; Ethereum; Hyperledger Fabric; Binance Smart Chain (BNB Chain); Solana; Cardano; Polkadot; Decentralized Applications

I. INTRODUCTION

Blockchain technology has emerged as one of the most transformative innovations of the twenty-first century, fundamentally changing the way digital transactions, data management, and trust mechanisms are established in distributed environments. Originally introduced as the underlying

technology for the cryptocurrency Bitcoin by Satoshi Nakamoto in 2008, blockchain has evolved far beyond digital currencies and has become a foundational technology for numerous applications across finance, healthcare, supply chain management, insurance, governance, and the Internet of Things (IoT). The core strength of blockchain lies in its decentralized architecture, which eliminates the need for centralized intermediaries by maintaining a shared and immutable ledger across multiple network participants. Through cryptographic security, consensus mechanisms, and distributed validation processes, blockchain enables transparent, secure, and tamper-resistant record keeping, thereby enhancing trust among participants operating in trust-deficient environments.

One of the most significant advancements in blockchain technology is the development of smart contracts. Smart contracts are self-executing digital agreements in which contractual terms and conditions are directly encoded into computer programs deployed on blockchain networks. These contracts automatically execute predefined actions when specified conditions are met, eliminating the need for intermediaries and reducing the possibility of human error, fraud, and delays. The concept of smart contracts was first proposed by Nick Szabo in the 1990s, but their practical implementation became feasible with the advent of blockchain platforms capable of supporting programmable logic. Smart contracts have since become a cornerstone of decentralized applications (DApps), enabling automated transactions, digital asset management, decentralized finance (DeFi), supply chain tracking, voting systems, and numerous other innovative applications.

The launch of Ethereum in 2015 marked a turning point in blockchain development by introducing a generalized platform for smart contract execution. Ethereum's Ethereum Virtual Machine (EVM) enabled developers to create decentralized applications using programmable smart contracts written primarily in Solidity. The flexibility and functionality offered by Ethereum contributed significantly to the rapid growth of blockchain ecosystems, decentralized finance protocols, and non-fungible tokens (NFTs). However, as adoption increased, limitations related to scalability, transaction throughput, network congestion, and transaction fees became increasingly evident. These

challenges motivated researchers and developers to explore alternative blockchain architectures and smart contract frameworks capable of delivering enhanced performance, security, and efficiency.

In response to the limitations of early blockchain platforms, numerous smart contract frameworks have emerged, each designed to address specific technical and operational requirements. Platforms such as Hyperledger Fabric focus on enterprise-grade applications through permissioned networks that prioritize privacy, access control, and regulatory compliance. Other platforms, including BNB Chain, emphasize low-cost transactions and compatibility with existing Ethereum-based applications. High-performance blockchain platforms such as Solana have introduced innovative consensus mechanisms to achieve significantly higher transaction throughput and reduced latency. Similarly, Cardano employs a research-driven approach emphasizing formal verification and mathematical rigor to improve smart contract security. Meanwhile, Polkadot addresses interoperability challenges by enabling communication and asset transfer among multiple blockchain networks through its parachain architecture.

Despite substantial technological advancements, the widespread adoption of blockchain-based smart contracts continues to face significant challenges. Security vulnerabilities remain one of the most critical concerns in smart contract deployment. Unlike traditional software applications that can be easily updated or modified, smart contracts often become immutable once deployed on blockchain networks. Consequently, coding errors, logical flaws, and security vulnerabilities can result in severe financial losses and system compromises. Several high-profile attacks involving reentrancy vulnerabilities, access control weaknesses, integer overflow errors, and oracle manipulation have demonstrated the importance of robust security practices in smart contract development. As blockchain ecosystems continue to expand, ensuring the reliability and resilience of smart contracts has become a primary research and industry focus.

Scalability represents another major challenge confronting blockchain-based smart contract frameworks. Public blockchain networks often experience performance bottlenecks due to limitations in transaction processing capacity and consensus mechanisms. As the

number of users and applications increases, network congestion can lead to delayed transaction confirmations and elevated transaction costs. These issues are particularly evident in highly utilized blockchain platforms where demand frequently exceeds available network resources. To address scalability concerns, researchers have proposed various solutions including sharding, sidechains, Layer-2 scaling protocols, rollups, and alternative consensus algorithms. However, achieving scalability without compromising security and decentralization remains a complex and ongoing challenge commonly referred to as the "blockchain trilemma."

Interoperability is another important aspect influencing the effectiveness of smart contract frameworks. The blockchain ecosystem consists of numerous independent networks that often operate in isolation, limiting seamless communication and data exchange. The inability of different blockchain platforms to interact efficiently creates barriers to cross-chain asset transfers, decentralized application integration, and collaborative ecosystem development. To overcome these limitations, modern blockchain frameworks increasingly incorporate interoperability protocols and cross-chain communication mechanisms. Such developments aim to create interconnected blockchain ecosystems capable of supporting more sophisticated and scalable decentralized services.

II. OVERVIEW OF SMART CONTRACT FRAMEWORKS

The rapid evolution of blockchain technology has resulted in the development of numerous smart contract frameworks, each designed to address specific challenges associated with security, scalability, interoperability, and transaction efficiency. Smart contract platforms serve as the foundation for decentralized applications (DApps), enabling automated execution of contractual agreements without the need for intermediaries. While all smart contract frameworks share the common objective of facilitating secure and transparent digital transactions, they differ significantly in terms of consensus mechanisms, governance structures, programming environments, and deployment models. Understanding the characteristics, strengths, and limitations of major smart contract frameworks is essential for selecting the most suitable platform for a particular application. This section provides

an overview of six prominent blockchain-based smart contract frameworks: Ethereum, Hyperledger Fabric, BNB Chain, Solana, Cardano, and Polkadot.

2.1 Ethereum

Ethereum is widely recognized as the pioneer and most extensively adopted smart contract platform in the blockchain ecosystem. Introduced in 2015 by Vitalik Buterin and his development team, Ethereum expanded the capabilities of blockchain technology beyond simple cryptocurrency transactions by enabling programmable smart contracts and decentralized applications. The platform operates through the Ethereum Virtual Machine (EVM), a decentralized computational environment capable of executing smart contract code across a distributed network of nodes.

Ethereum primarily supports programming languages such as Solidity and Vyper, allowing developers to create complex decentralized applications in sectors including finance, healthcare, gaming, digital identity management, and supply chain systems. One of Ethereum's most significant milestones was its transition from the energy-intensive Proof-of-Work (PoW) consensus mechanism to the more sustainable Proof-of-Stake (PoS) mechanism through "The Merge." This transition substantially reduced energy consumption while improving network sustainability and security.

The platform benefits from a large and active developer community, extensive documentation, robust development tools, and a mature ecosystem of decentralized applications. Ethereum serves as the foundation for numerous decentralized finance (DeFi) protocols and non-fungible token (NFT) marketplaces. Its high degree of decentralization and strong security mechanisms have contributed to its widespread adoption across industries.

Despite these advantages, Ethereum faces several challenges. The platform often experiences network congestion during periods of high demand, leading to increased transaction processing times and elevated gas fees. Scalability limitations remain a concern, although ongoing developments such as Layer-2 scaling solutions and sharding aim to address these issues. Consequently, Ethereum represents a highly secure and mature platform but continues to balance the trade-offs between decentralization, scalability, and transaction efficiency.

2.2 Hyperledger Fabric

Hyperledger Fabric is an open-source, permissioned blockchain framework developed under the Hyperledger project hosted by the Linux Foundation. Unlike public blockchain networks, Hyperledger Fabric is specifically designed for enterprise and business applications where privacy, regulatory compliance, and access control are critical requirements.

One of the distinguishing characteristics of Hyperledger Fabric is its permissioned architecture, which restricts participation to verified and authorized organizations. This approach enables enterprises to maintain greater control over network participants while ensuring confidentiality of sensitive business information. Hyperledger Fabric employs a modular design that allows organizations to customize consensus protocols, identity management systems, and communication mechanisms according to their operational requirements.

Smart contracts within Hyperledger Fabric are referred to as chaincode and can be developed using programming languages such as Go, Java, and Node.js. The platform supports private channels and confidential transactions, making it particularly suitable for industries such as banking, healthcare, logistics, insurance, and government services.

The framework offers several advantages, including high transaction throughput, strong privacy controls, flexible architecture, and efficient resource utilization. However, Hyperledger Fabric also presents certain limitations. The restricted participation model reduces decentralization compared to public blockchain platforms. Additionally, configuring and maintaining the network infrastructure can be complex, requiring specialized expertise and organizational coordination. Despite these challenges, Hyperledger Fabric remains one of the most widely adopted enterprise blockchain solutions due to its ability to satisfy strict security and regulatory requirements.

2.3 Binance Smart Chain (BNB Chain)

BNB Chain was developed to provide a high-performance and cost-effective alternative to Ethereum while maintaining compatibility with Ethereum-based applications. The platform utilizes a Proof-of-Staked Authority (PoSA) consensus mechanism, which combines elements of delegated staking and validator authority to achieve rapid

transaction confirmation and low operational costs.

One of the primary strengths of BNB Chain is its compatibility with the Ethereum Virtual Machine. This compatibility enables developers to migrate Ethereum-based decentralized applications with minimal modifications, thereby reducing development complexity and facilitating ecosystem expansion. The platform supports smart contracts written in Solidity and utilizes many of the same development tools available within the Ethereum ecosystem.

BNB Chain has gained significant popularity among decentralized finance projects due to its low transaction fees and high transaction processing speed. Compared to Ethereum, users can execute transactions more efficiently and at a fraction of the cost, making the platform attractive for applications involving frequent interactions and microtransactions.

However, BNB Chain has been criticized for its relatively lower degree of decentralization. The limited number of validators participating in consensus creates concerns regarding validator concentration and potential governance centralization. While this architecture improves efficiency and performance, it may introduce security and trust concerns when compared to more decentralized blockchain networks. Nevertheless, BNB Chain continues to play a major role in expanding blockchain adoption through affordable and accessible smart contract deployment.

2.4 Solana

Solana is a next-generation blockchain platform designed to address scalability challenges through innovative consensus mechanisms and high-performance infrastructure. Solana combines Proof-of-History (PoH) with Proof-of-Stake (PoS) to achieve exceptional transaction throughput while maintaining network security and decentralization.

Proof-of-History serves as a cryptographic clock that establishes the chronological order of transactions before they enter the consensus process. This innovation significantly reduces communication overhead among validators and enables parallel transaction processing. As a result, Solana is capable of processing tens of thousands of transactions per second while maintaining extremely low transaction fees.

The platform has attracted considerable attention from decentralized finance, gaming, and NFT projects due to its ability to support large-scale applications with minimal latency. Developers typically utilize the Rust programming language to build smart contracts on the Solana network, benefiting from Rust's memory safety and performance characteristics.

Despite its impressive performance capabilities, Solana faces several operational challenges. The network has experienced occasional outages and service disruptions, raising concerns regarding reliability and resilience. Additionally, the platform's development environment can be more complex than those of EVM-compatible networks, requiring developers to acquire specialized knowledge. Validator participation also demands substantial hardware resources, which may limit accessibility for smaller participants. Nonetheless, Solana remains one of the fastest and most scalable blockchain platforms currently available.

2.5 Cardano

Cardano is a blockchain platform developed using a research-driven methodology emphasizing scientific rigor, peer-reviewed academic research, and formal verification techniques. The platform operates using the Ouroboros Proof-of-Stake consensus protocol, which provides energy-efficient transaction validation while maintaining strong security guarantees.

A distinguishing feature of Cardano is its focus on formal methods and mathematical verification. Smart contracts are developed using Plutus, a language based on Haskell that facilitates rigorous testing and verification of contract behavior. This approach reduces the likelihood of programming errors and vulnerabilities, making Cardano particularly attractive for applications requiring high levels of reliability and security.

The platform emphasizes sustainability, scalability, and interoperability through a layered architectural design that separates transaction processing from smart contract execution. Cardano also seeks to address governance challenges by incorporating community-driven decision-making mechanisms and treasury systems for ecosystem development.

Although Cardano offers strong security and academic credibility, its ecosystem growth

has been relatively slower compared to platforms such as Ethereum and Solana. The specialized programming languages and development tools may also present a steeper learning curve for developers unfamiliar with functional programming concepts. Despite these limitations, Cardano is widely regarded as one of the most secure and scientifically grounded blockchain platforms.

2.6 Polkadot

Polkadot is a blockchain framework specifically designed to enable interoperability among multiple blockchain networks. Developed by Gavin Wood, one of Ethereum's co-founders, Polkadot addresses the challenge of isolated blockchain ecosystems through an innovative architecture consisting of a central relay chain and multiple specialized parachains.

The relay chain provides shared security and consensus services, while parachains operate independently to support specific applications and use cases. This architecture allows multiple blockchain networks to communicate, exchange data, and transfer digital assets securely and efficiently. By enabling parallel transaction processing across multiple chains, Polkadot significantly enhances scalability and network performance.

One of Polkadot's key advantages is its shared security model, which allows smaller parachains to benefit from the security infrastructure of the relay chain. The platform also supports cross-chain communication, making it highly suitable for decentralized ecosystems requiring interoperability among diverse blockchain networks.

However, Polkadot's sophisticated architecture introduces complexity in development, deployment, and governance. Managing parachains, governance mechanisms, and network upgrades requires substantial technical expertise and coordination among stakeholders. Despite these challenges, Polkadot represents one of the most promising solutions for achieving blockchain interoperability and creating a truly interconnected decentralized ecosystem.

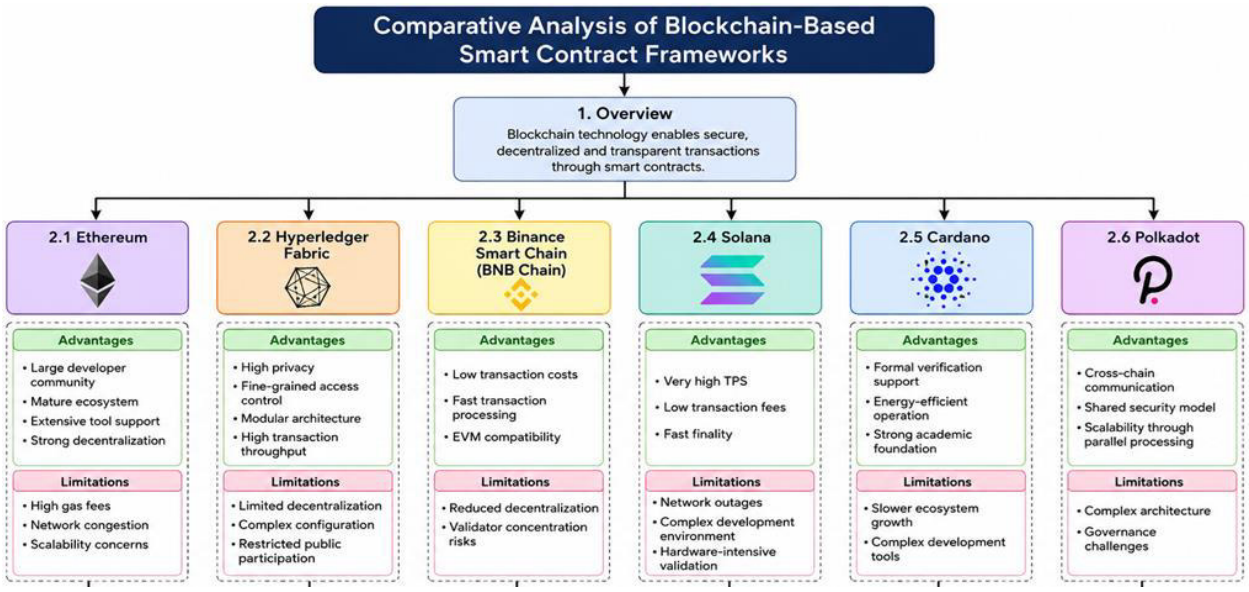

Figure 1. Comparative Framework Analysis of Major Blockchain-Based Smart Contract Platforms

III. SECURITY ANALYSIS

Security is a fundamental aspect of smart contract deployment, as vulnerabilities can lead to financial losses, unauthorized access, and system failures. Evaluating the security features of different blockchain frameworks helps ensure reliable, transparent, and secure smart contract execution.

Table.1.Common Smart Contract Vulnerabilities

Vulnerability	**Description**
Reentrancy Attack	Recursive contract calls enabling fund theft
Integer Overflow	Arithmetic errors causing unexpected behavior
Front-Running	Manipulation of transaction ordering
Access Control Flaws	Unauthorized access to contract functions
Logic Bugs	Errors in contract implementation

Table.2.Security Comparison

Framework	**Security Features**	**Formal Verification**
Ethereum	Auditing tools, OpenZeppelin libraries	Partial
Hyperledger Fabric	Permissioned access control	Moderate
BNB Chain	EVM-based security tools	Limited
Solana	Rust memory safety	Moderate
Cardano	Formal methods and Haskell-based design	Strong
Polkadot	Shared security architecture	Moderate

The security comparison table evaluates the security features and formal verification capabilities of major blockchain platforms. Ethereum provides strong security through extensive auditing tools and OpenZeppelin libraries, although formal verification is only partially implemented. Hyperledger Fabric offers enhanced security through permissioned access control and identity management systems, making it suitable for enterprise applications. BNB Chain utilizes Ethereum-compatible security tools but has limited formal verification and faces concerns regarding validator concentration. Solana improves security through the Rust programming language, which offers memory safety and reduces common coding vulnerabilities. Cardano demonstrates the strongest security approach by employing formal verification methods and Haskell-based smart contract development, enabling mathematical proof of contract correctness. Polkadot utilizes a shared security architecture in which multiple parachains benefit from the security provided by a central relay chain, offering moderate formal verification and secure interoperability.

IV. EFFICIENCY ANALYSIS

Efficiency is evaluated based on transaction throughput, latency, and operational cost.

Table.3.Performance Comparison

Framework	**Consensus Mechanism**	**TPS**	**Average Fee**

Ethereum	PoS	15–30	High
Hyperledger Fabric	PBFT Variants	3000+	Low
BNB Chain	PoSA	100–300	Low
Solana	PoH + PoS	50,000+	Very Low
Cardano	Ouroboros PoS	250–1000	Low
Polkadot	Nominated PoS	1000+	Low

The performance comparison table evaluates the efficiency of different smart contract frameworks based on their consensus mechanisms, transaction throughput (TPS), and transaction fees. Ethereum offers strong decentralization and security but processes relatively fewer transactions (15–30 TPS) with high transaction fees. Hyperledger Fabric achieves very high throughput (3000+ TPS) and low fees, making it suitable for enterprise applications. BNB Chain provides moderate throughput with low transaction costs, making it efficient for decentralized applications. Solana demonstrates the highest performance, processing over 50,000 TPS with very low fees due to its Proof-of-History and Proof-of-Stake architecture. Cardano balances security and performance by offering 250–1000 TPS with low fees, while Polkadot achieves scalability through its parachain architecture, supporting over 1000 TPS at low operational costs.

V. DEPLOYMENT CHALLENGES

5.1 Smart Contract Development Complexity

Table.4.Different frameworks require distinct programming languages and development environments.

Platform	**Primary Language**
Ethereum	Solidity
Hyperledger Fabric	Go, Java, Node.js
BNB Chain	Solidity
Solana	Rust
Cardano	Haskell, Plutus
Polkadot	Rust

Developers often face steep learning curves, particularly when transitioning from traditional software engineering environments.

Table 5. Comparative Evaluation of Smart Contract Frameworks

Criterion	**Best Performing Framework**	**Key Strength**
Security	Cardano	Formal verification and research-driven development
Decentralization	Ethereum	Large decentralized network and strong community support
Enterprise Adoption	Hyperledger Fabric	Permissioned architecture with privacy and access control
Throughput	Solana	Extremely high transaction processing capacity
Low-Cost Transactions	BNB Chain	Fast transactions with minimal fees
Interoperability	Polkadot	Seamless cross-chain communication through parachains

The development complexity table highlights the primary programming languages used by each smart contract platform. Ethereum and BNB Chain use Solidity, which is widely adopted and supported by extensive development tools. Hyperledger Fabric supports multiple programming languages such as Go, Java, and Node.js, providing flexibility for enterprise developers. Solana and Polkadot primarily use Rust, a powerful language known for security and performance but requiring specialized expertise. Cardano utilizes Haskell and Plutus, which offer strong formal verification capabilities but present a steeper learning curve. As a result, developers often face challenges when adapting to different programming environments and blockchain-specific development frameworks.

The comparative analysis indicates that each smart contract framework possesses unique strengths and is optimized for specific use cases. No single platform performs best across all evaluation criteria. While Cardano emphasizes security through formal verification, Ethereum remains the leader in decentralization and ecosystem maturity. Hyperledger Fabric is preferred for

enterprise applications due to its privacy and permissioned architecture, whereas Solana delivers exceptional transaction throughput. BNB Chain offers cost-effective transactions, and Polkadot excels in blockchain interoperability through its parachain framework. Therefore, the selection of a smart contract platform should be based on the specific requirements of the intended application, including security, scalability, cost, privacy, and interoperability needs.

VI. FUTURE RESEARCH DIRECTIONS

Future research in blockchain-based smart contract frameworks should focus on addressing existing limitations related to security, scalability, interoperability, and sustainability. One promising area is the development of Artificial Intelligence (AI)-assisted smart contract auditing**,** which can enhance the identification of coding errors, security vulnerabilities, and logical flaws before deployment. Similarly, automated vulnerability detection systems powered by machine learning can continuously monitor smart contracts and detect potential threats in real time, thereby improving overall network security. Another important research direction involves establishing cross-chain interoperability standards to enable seamless communication and asset transfer between different blockchain networks, reducing ecosystem fragmentation and promoting broader adoption. As advancements in quantum computing continue, the development of quantum-resistant cryptographic mechanisms will become essential to protect blockchain networks from future computational threats. Researchers are also exploring energy-efficient consensus algorithms that can maintain security and decentralization while significantly reducing computational power consumption and environmental impact. Furthermore, the implementation of formal verification frameworks for large-scale decentralized applications can provide mathematical assurance of smart contract correctness, minimizing the risk of vulnerabilities and operational failures. Finally, the integration of blockchain technology with emerging fields such as the Internet of Things (IoT) and Artificial Intelligence (AI) has the potential to create intelligent, autonomous, and secure ecosystems capable of supporting advanced applications in healthcare, supply chain management, smart cities, and industrial

automation. These research advancements are expected to enhance the reliability, scalability, and practical adoption of blockchain-based smart contract systems in the coming years.

VII. CONCLUSION

Blockchain-based smart contract frameworks have revolutionized digital transactions by enabling decentralized, transparent, and automated execution of agreements. This comparative analysis shows that each platform offers unique strengths and limitations in terms of security, efficiency, scalability, interoperability, and deployment. Ethereum leads in decentralization and ecosystem maturity, Hyperledger Fabric is well-suited for enterprise applications, Solana excels in transaction throughput, Cardano emphasizes security through formal verification, BNB Chain provides cost-effective transactions, and Polkadot enhances interoperability across blockchain networks.

Despite these advancements, challenges such as security vulnerabilities, scalability constraints, interoperability issues, and deployment complexity continue to affect widespread adoption. Therefore, the choice of a smart contract framework depends on the specific requirements of the application. Future developments in AI-assisted auditing, quantum-resistant cryptography, energy-efficient consensus mechanisms, and cross-chain communication are expected to further improve the security, efficiency, and reliability of blockchain-based smart contract ecosystems. Overall, smart contract technologies will continue to play a crucial role in the growth of decentralized applications and digital transformation across industries.

References

[1] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., ... Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*, 1–15. https://doi.org/10.1145/3190508.3190538

[2] Antonopoulos, A. M., & Wood, G. (2018). *Mastering Ethereum: Building smart contracts and DApps*. O'Reilly Media.

[3] Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. Ethereum White Paper.

[4] Cardano Foundation. (2024). *Cardano documentation and developer resources*. Cardano Foundation. https://cardano.org

[5] Chen, Y., Bellavitis, C., & Hao, H. (2022). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights, 18*, e00339. https://doi.org/10.1016/j.jbvi.2022.e00339

[6] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

[7] Dannen, C. (2017). *Introducing Ethereum and Solidity: Foundations of cryptocurrency and blockchain programming for beginners*. Apress.

[8] Ethereum Foundation. (2024). *Ethereum developer documentation*. Ethereum Foundation. https://ethereum.org

[9] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 3–16. https://doi.org/10.1145/2976749.2978341

[10] Hileman, G., & Rauchs, M. (2017). *Global blockchain benchmarking study*. Cambridge Centre for Alternative Finance.

[11] Hyperledger Foundation. (2024). *Hyperledger Fabric documentation*. Hyperledger Foundation. https://hyperledger.org

[12] Liu, Y., Zhang, X., Wang, J., & Luo, Y. (2022). Security analysis and vulnerability detection in blockchain smart contracts: A survey. *IEEE Access, 10*, 89744–89767. https://doi.org/10.1109/ACCESS.2022.3200424

[13] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

[14] Parizi, R. M., Dehghantanha, A., Choo, K. K. R., & Singh, A. (2018). Empirical vulnerability analysis of automated smart contracts security testing on blockchains. *Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering*, 103–113.

[15] Polkadot Foundation. (2024). *Polkadot whitepaper and developer documentation*. Polkadot Foundation. https://polkadot.network

[16] Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering, 62*(6), 599–608. https://doi.org/10.1007/s12599-020-00656-x

[17] Solana Foundation. (2024). *Solana developer documentation*. Solana Foundation. https://solana.com

[18] Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday, 2*(9). https://doi.org/10.5210/fm.v2i9.548

[19] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A survey on consensus mechanisms and mining management in blockchain networks. *IEEE Access, 7*, 22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108

[20] Wood, G. (2016). *Polkadot: Vision for a heterogeneous multi-chain framework*. Web3 Foundation.

[21] Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer. https://doi.org/10.1007/978-3-030-03035-3