Zohaib *et al. (IJECI)* 2024

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2024.0801188

Research Article

Vol. 8 issue 1 Jan-Apr 2024

Enhancement of Security and Privacy of Smart Contracts in Blockchain

Syed Khurram Hassan[1] and Muhammad Asif Ibrahim[2]

[1] Institute of Quality and Technology Management, University of the Punjab, Lahore, Pakistan.
[2]Department of Mathematics, The University of Lahore, Lahore.
Corresponding author: khuramshah6515@gmail.com

Received: December 29, 2023; **Accepted:** January 17, 2024; **Published:** March 15, 2024

ABSTRACT

Smart contracts, leveraging the power of blockchain technology, have revolutionized the execution and enforcement of agreements. However, their adoption also brings forth substantial challenges in terms of security and privacy. This research paper aims to identify the recent areas of focus and provide a comprehensive perspective on blockchain applications and smart contracts, highlighting their main issues and corresponding solutions. Furthermore, it seeks to address the gaps in current research and outline future avenues of investigation. The primary objective is to assess the security and privacy concerns associated with smart contracts in blockchain and propose effective measures to enhance their robustness. By conducting a thorough analysis of vulnerabilities, attack vectors, and privacy considerations, this study offers valuable insights into the risks involved in smart contracts. It also puts forth practical solutions and best practices to mitigate these risks, ensuring a more secure and privacy-preserving environment for the deployment and execution of smart contracts.

Keywords: Blockchain, privacy, security, technology, risks.

1. INTRODUCTION

The Smart contracts, driven by the innovative potential of blockchain technology, have emerged as a groundbreaking solution in the domain of decentralized digital transactions. In 2008, Satoshi Nakamoto introduced the concept of peer-to-peer cash transactions without the reliance on a centralized system. Blockchain, a digital ledger that publicly stores and verifies transactions through nodes, forms the foundation of this technology. The underlying structure of blockchain involves the validation of transactions by nodes and the security of these transactions through cryptographic hash functions. On the other hand, a smart contract represents a self-executing agreement encoded within a blockchain, enabling the automatic enforcement of contractual terms without intermediaries [1]. Essentially, it is a computer program composed of a set of rules that operate on the blockchain. By harnessing the transparent and immutable characteristics of blockchain, smart contracts provide heightened efficiency, security, and trustworthiness across various industries such as finance, supply chain management, and healthcare [2].

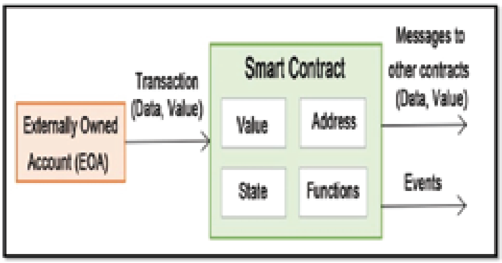
Externally Owned Account (EOA)
Transaction (Data, Value)
Smart Contract
Value
Address
State
Functions
Messages to other contracts (Data, Value)
Events

Fig 1: A basic structure of Smart Contract

The adoption of smart contracts has gained significant momentum, revolutionized traditional business processes, and enabled new forms of decentralized applications. A smart contract consists of the value, address, functions, and state. However, this rapid expansion brings forth a range of challenges and considerations, particularly in terms of security and privacy. As smart contracts increasingly handle sensitive data and control valuable assets, it becomes imperative to assess and address the security and privacy implications associated with their deployment and execution [3].

The research problem at hand revolves around the assessment of the security and privacy issues related to smart contracts in blockchain. It is crucial to identify and understand the vulnerabilities, risks, and potential attack vectors that can compromise the integrity, availability, and confidentiality of smart contracts. Furthermore, ensuring the privacy of contract participants and protecting their sensitive information from unauthorized access is of paramount importance. The objectives of this research article are twofold [4]. Firstly, it aims to conduct a comprehensive analysis of the security challenges faced by smart contracts. This analysis will encompass the identification and examination of vulnerabilities in smart contract code, potential attacks on contract execution, and governance-related risks. Additionally, it will explore the privacy concerns associated with smart contracts, including issues of identity and transaction privacy, as well as data confidentiality and access control [3].

Secondly, this research article seeks to propose solutions to enhance the security and privacy of smart contracts in blockchain. By leveraging best practices, auditing approaches, and secure execution environments, we aim to mitigate the identified security risks and vulnerabilities. Similarly, through the adoption of privacy-preserving cryptographic techniques and the exploration of privacy-focused blockchain protocols, we intend to enhance the privacy of smart contract transactions and safeguard sensitive data [5]. By addressing the security and privacy challenges in smart contracts, we can foster a more trustworthy and resilient ecosystem for their deployment and execution. This not only instills confidence in stakeholders but also encourages wider adoption of smart contracts, enabling their potential to be fully realized across diverse industries. The subsequent sections of this article will delve deeper into the identified research problem, analyzing security and privacy issues, and proposing practical solutions to enhance the robustness of smart contracts in blockchain [6].

2. BACKGROUND STUDY AND RELATED WORK

The section on background study and related work presents a comprehensive overview of prior research, studies, and advancements in the realm of enhancing the security and privacy of smart contracts in blockchain. The concept of smart contracts was initially proposed by Nick Szabo in 1994 [7]. This section aims to provide the necessary context for the current research article by highlighting the existing knowledge, identifying gaps, and showcasing the contributions made by previous studies in addressing the security and privacy challenges associated with smart contracts [8].

For instance, Hiroki Watanabe et al. [9] delve into the application of smart contracts in digital rights management and propose a consensus method. Ahmed Kosba et al. introduce Hawk, a cryptographic approach to writing secure smart contracts. Joshua Ellul and Gordon J. Pace [10] describe Alkyl VM, a virtual machine tailored for creating smart contracts in Internet of Things applications. The authors of [11] and [12] explore the execution process of smart contracts and highlight specific security issues. Through an examination of various articles related to smart contracts, it becomes evident that Solidity, a high-level language, is widely used for smart contract implementation [13].

Multiple blockchain platforms, including Ethereum, Eris DB, Zeppelin, and Counterparty, employ Solidity as their development language. Ethereum, in particular, utilizes a stack-based bytecode language for writing smart contract code, which is executed in the Ethereum Virtual Machine (EVM) [14].

3. SMART CONTRACT SECURITY RESEARCH

Previous research has extensively focused on identifying vulnerabilities and security flaws in smart contract code. Studies have analyzed common coding flaws and weaknesses, such as reentrancy, integer overflow/underflow, and unchecked external calls, to highlight the potential risks and propose best practices for secure smart contract development. Researchers have also explored automated tools and formal verification techniques to improve the security of smart contracts. These advancements aim to detect and prevent vulnerabilities during the development phase and provide rigorous analysis of smart contract code for potential flaws. Auditing and testing approaches have been investigated to assess the security of deployed smart contracts. Third-party audits, bug bounties, and code review processes have been employed to identify vulnerabilities and enhance the overall security of smart contracts [15].

4. HOW SMART CONTRACT WORKS IN BLOCKCHAIN

The Smart contracts are digitized contracts that are programmed using code and implemented on blockchain networks. They facilitate the exchange of assets in a transparent and conflict-free manner without the involvement of an intermediary. Once deployed on a blockchain, a smart contract serves as an automated agent that executes the terms of an agreement between parties. The code of a smart contract contains conditional statements that reflect the terms and outcomes of the agreement. For instance, if two parties agree to trade money for property, the smart contract can automatically transfer funds from one party to the other upon the transfer of the property [14].

Self-sufficiency: Once deployed, a smart contract independently enforces an agreement between parties without human intervention. It is difficult to tamper with or terminate.

Decentralization: Smart contracts are deployed on decentralized blockchains, so no single entity controls them. This makes them transparent and censorship-resistant.

Security: Blockchains are inherently secure due to cryptography. Hacking or tampering with a smart contract would require an enormous amount of computing power and is economically unfeasible in most cases.

Accuracy: Smart contracts are extremely precise because they are programmed using code. Vague terms in written legal contracts often lead to disputes, but smart contracts leave no room for ambiguity.

Trustlessness: Blockchains and smart contracts eliminate the need for a trusted third-party to oversee agreements and transactions. The parties do not need to know or trust each other to do business.

Immutability: Once deployed, a smart contract can never be modified or deleted. It is recorded permanently on the blockchain, ensuring the records and terms of the agreement cannot be altered [16]. While smart contracts provide many benefits, they also have some limitations. Because they cannot access data outside the blockchain, they cannot be used for agreements reliant on real-world data [17]. They also cannot be halted or reversed easily in the event of a hack or bug. Finally, current smart contract platforms lack mature, standardized programming languages [18].

5. ADVANTAGES OF SMART CONTRACTS

The use of smart contracts in blockchain technology offers several advantages. These include:

Transparency: Smart contracts are transparent, and the terms of the agreement are visible to all parties involved. This ensures that there is no room for ambiguity or misunderstanding.

Security: Smart contracts are executed automatically, and their execution is recorded on the blockchain network. This ensures that the agreement is tamper-proof, and the contract cannot be altered once it is executed.

Cost-Effective: The use of smart contracts eliminates the need for intermediaries, which reduces the cost of the transaction [19].

6. LIMITATIONS OF SMART CONTRACTS

While smart contracts offer several advantages, there are also some limitations to their use. These include:

Complexity: Smart contracts are complex, and their creation requires expertise in programming and blockchain technology.

Immutability: Once a smart contract is executed, it cannot be altered. This can be a disadvantage if there are errors in the code or if the terms of the agreement need to be changed [20].

Legal Validity: The legal validity of smart contracts is still a matter of debate, and there is no clear legal framework for their use.

In summary, smart contracts have the potential to streamline and secure many types of agreements in the future, but further progress is still required to address some of their existing limitations [21]. With continued improvement, smart contracts could transform how businesses and individuals conduct transactions and enable new blockchain-based business models [22].

7. REAL-LIFE APPLICATIONS OF BLOCKCHAIN

Blockchain technology has gained attention for its potential to revolutionize industries by providing secure, transparent, and immutable records. It enables decentralized consensus, allowing participants to trust and transact without intermediaries. While its origins lie in the realm of cryptocurrencies [18], blockchain's applications extend far beyond digital currencies. In this article, we explore real-life applications of blockchain in supply chain management, healthcare, and financial services, energy, voting, and education, intellectual property, and digital identity. Through these applications, blockchain is poised to transform industries by enabling transparency, traceability, and trust [23].

7.1. Supply Chain Management

The supply chain industry faces challenges related to transparency, traceability, and counterfeit products. Blockchain technology offers a solution by creating an auditable and immutable record of every transaction and movement within the supply chain. This ensures transparency and accountability throughout the entire process. The Food Trust initiative, a partnership between IBM and Walmart, demonstrates the potential of blockchain in enhancing food safety and traceability [24].

7.2. Healthcare

Blockchain holds promise for revolutionizing the healthcare industry by addressing issues such as data interoperability, patient privacy, and medical record management. Med Rec, developed by researchers at MIT, leverages blockchain to create a secure and auditable ledger of medical records. This approach empowers patients to control their own data while enabling secure sharing with healthcare providers. Blockchain-based medical record systems reduce errors, redundancies, and delays, leading to improved patient outcomes [24].

7.3. Financial Services

Financial services are among the early adopters of blockchain technology. Blockchain offers secure, transparent, and efficient solutions for transactions, identity management, and smart contracts. Ripple, a blockchain-based payment protocol, facilitates fast and low-cost cross-border transactions, bypassing intermediariesClick or tap here to enter text.. This technology reduces transaction fees, enhances speed, and increases financial inclusion, transforming traditional financial systems [25].

7.4. Blockchain in Energy

The energy sector can leverage blockchain to improve efficiency, transparency, and decentralized energy trading. Blockchain-based platforms enable peer-to-peer energy transactions, optimizing energy usage and reducing reliance on centralized authorities. The Brooklyn Microgrid project is an example of blockchain-powered energy trading, where participants can buy and sell excess solar energy in a secure and transparent manner [26].

7.5. Blockchain in Voting

Blockchain can introduce transparency, security, and trust in the voting process. By leveraging blockchain technology, the voting process can become tamper-proof, ensuring the integrity of the electoral system. Agora, a blockchain voting platform, successfully conducted a pilot project in Sierra Leone, allowing citizens to verify their votes and ensuring transparency in the electoral process [22].

7.6. Blockchain in Education

Blockchain technology can revolutionize the education sector by enabling secure and verified credentials, preventing fraud, and ensuring lifelong learner records. Blockchain-based platforms can authenticate degrees, certifications, and achievements, allowing individuals to have a portable and immutable record of their educational qualifications [24].

7.7. Blockchain in Intellectual Property

Blockchain provides a decentralized and transparent platform for protecting intellectual property rights. By recording transactions and ownership on a blockchain, creators can establish proof of ownership and protect their creations from infringement. The IP Chain project in Russia is an example of blockchain application in intellectual property management, streamlining the registration and protection of patents, trademarks, and copyrights [25].

7.8. Blockchain in Digital Identity

Blockchain technology can enhance digital identity management by providing secure, decentralized, and verifiable identities. Self-sovereign identity solutions allow individuals to control and manage their digital identities, reducing the risk of identity theft and enhancing privacy. Port, a blockchain-based identity platform, enables individuals to create and manage their digital identities, facilitating secure interactions in the digital world [26].

8. CHALLENGES AND LIMITA TIONS OF BLOCKCHAIN

Blockchain technology has gained significant attention as a decentralized, secure, and transparent system for managing digital transactions. However, the technology still faces several limitations and challenges that limit its widespread adoption. In this paper, we explore some of the key challenges and limitations of blockchain technology.

8.1. Scalability Limitations

The traditional proof-of-work consensus algorithm used by many blockchains limits their transaction processing capacity to a few dozen transactions per second. This is far below the processing capacity of centralized payment systems such as Visa or Mastercard. Several solutions have been proposed to address this issue, such as sharding and off-chain transactions. However, these solutions require consensus among the network participants and may compromise the security and decentralization of the blockchain [27].

8.2. Security and Privacy Concerns

Security and privacy concerns remain a significant challenge for blockchain adoption. Despite the use of cryptographic techniques to secure the blockchain, hackers have exploited vulnerabilities in smart contracts, wallets, and exchanges to steal millions of dollars' worth of cryptocurrencies. The lack of standardized security protocols and regulations also exposes blockchain users to legal and regulatory risks

[28].

9. INTEROPERABILITY AND GOVERNANCE CHALLENGES

The interoperability and governance of blockchain technology pose significant challenges. Different blockchains have different standards, protocols, and rules that limit their compatibility and coordination. The decentralized and distributed nature of blockchain technology also makes it difficult to establish a unified governance framework and ensure the accountability and transparency of its stakeholders [29].

9.1. Organizational Challenges

Lack of awareness and understanding about blockchain technology. Resistance to change and cultural barriers within organizations. High implementation costs and the need for specialized expertise. The requirement for large storage systems and increased computational power [28].

9.2. Governmental Challenges

Lack of laws and regulations addressing technical disputes and smart contracts. The need for standardization in blockchain applications. The importance of government support and regulatory frameworks for blockchain adoption [30].

9.3. Technical Challenges

Complexity of blockchain technology, making it difficult for users to understand. The increasing size of the blockchain, leading to performance degradation. Demands for substantial storage and computational resources, resulting in environmental concerns. Latency issues in adding verified blocks to the ledger. Integration challenges with legacy systems and the interoperability of different blockchains [31].

9.4. Energy Consumption

Bitcoin and other cryptocurrencies use blockchain technology for transactions. To validate transactions, a process called mining is performed using specialized hardware. However, this mining process consumes a lot of energy, leading to a significant carbon footprint. For example, Bitcoin mining consumes about 125 TWh of energy annually. This raises concerns about the environmental impact of cryptocurrencies. Efforts are being made to find energy-efficient solutions for blockchain technology [32].

9.5. Selfish Mining

In a selfish mining attack, an individual or group aims to maximize their own rewards by exploiting the mining process and causing other miners to waste their resources. Here's how it works in simpler terms: The attacker mines a block but keeps it private instead of sharing it with the network. This means that other miners are unaware of this block's existence. Meanwhile, the honest miners continue their efforts to validate a block, unaware that the attacker has already found one. This leads to a waste of their time and resources. The attacker continues to work on their private chain, trying to build a longer chain than the public one known to the rest of the network. By withholding their discovered blocks and secretly building their own chain, the attacker gains an advantage over honest miners. They can release their private chain at a strategic moment, causing the honest miners' efforts to go to waste, and potentially reaping more rewards for them. In essence, the selfish mining attack is a strategy where an individual or group manipulates the mining process to their advantage, causing other miners to waste resources while they maximize their own profits [31].

9.6. Personal Identifiable Information (PII)

There is a misconception surrounding the use of blockchain for identity management. Many believe that blockchain provides an ideal decentralized alternative to store Personal Identifiable Information (PII), replacing centralized databases. However, the reality is that blockchain can be used in two ways for PII: either by directly storing PII on the blockchain or by creating attestations on the blockchain that point to off-chain storage for PII. Elmagharaby and Losavio have delved into the concept of PII, specifically focusing on communication and location privacy [33].

10. FUTURE OF BLOCKCHAIN

Blockchain technology is a revolutionary way to securely record and store information. Initially introduced through the digital currency Bitcoin, blockchain has evolved to offer various applications beyond cryptocurrencies. This technology operates as a decentralized digital ledger that records transactions or information. Instead of being controlled by a single authority, such as a bank or government, it is maintained by a network of computers [34].

In blockchain, each transaction or piece of information is stored in a "block" and linked together in a "chain" of blocks, forming a complete record of all the transactions. The blockchain platform provides a distributed ledger that is scalable, secure, tamper-proof, and accessible by each peer on the network. Bitcoin, which operates on the blockchain, was created as a digital currency by an anonymous individual or group known as Satoshi Nakamoto [35]. Transactions on the Bitcoin blockchain are verified by network participants called "miners," who use powerful computers to solve complex mathematical problems [34]. The blockchain platform utilizes Public Key Cryptography Asymmetric Encryption algorithms, which involve public and private keys to encrypt and decrypt data. Public keys are used to encrypt messages, and private keys are necessary to decrypt them. Conversely, private keys are used to encrypt messages, and public keys are required for decryption [36].

Blockchain technology offers numerous benefits. It ensures transparency, as anyone can view the blockchain and verify transactions. The information stored on the blockchain is encrypted and resistant to alteration, enhancing security. Additionally, blockchain enables faster and more efficient transactions by eliminating the need for intermediaries. The potential of blockchain extends beyond Bitcoin. It can revolutionize various industries by increasing transparency and accountability. Blockchain's decentralized nature enhances security and transparency, making it valuable in supply chain management. It can track goods from manufacturers to end-users, ensuring authenticity and ethical production conditions.

The future of blockchain technology is promising. Beyond cryptocurrencies, blockchain can facilitate smart contracts, which are self-executing agreements with predefined conditions. It also enables secure transfer and storage of digital assets like property deeds and intellectual property rights. However, it is worth noting that public blockchain networks with a large number of nodes can experience limitations in transaction throughput and high latency, resulting in slower propagation of transactions and blocks [37].

11. CONCLUSION

Blockchain technology has evolved beyond cryptocurrencies, finding applications in various sectors. The examples discussed in this article illustrate how blockchain enhances transparency, security, and efficiency in supply chain management, healthcare, financial services, energy, government, and education. As blockchain continues to advance, it holds the potential to reshape industries, enabling trust, and transforming the way we conduct business and manage data. A number of endeavors have been made to improve consensus algorithms in blockchain, such as Peer Census, Kickstarter, and Chepurnoyet al.'s new consensus algorithm. Peer Census decouples block creation and transaction confirmation, while Kickstarter proposes the Greedy Heaviest-Observed Sub-Tree (GHOST) chain selection rule. Chepurnoyet al. proposed a new consensus algorithm for peer-to-peer blockchain systems where anyone who provides non-interactive proofs of retrievability is agreed to generate the block. The traditional proof-of-work consensus algorithm used by many blockchains limits their transaction processing capacity to a few dozen transactions per second. Security and privacy concerns remain a significant challenge for blockchain adoption, as hackers have exploited vulnerabilities in smart contracts, wallets, and exchanges to steal millions of dollars’ worth of cryptocurrencies. The interoperability and governance of blockchain technology pose significant challenges, such as lack of awareness and understanding, resistance to change, high implementation costs, lack of laws and regulations, need for standardization, government support and regulatory frameworks, complexity of blockchain technology, increasing size of the blockchain, environmental concerns, and integration challenges with legacy systems.

In conclusion, blockchain technology has several limitations and challenges that hinder its widespread adoption. The scalability limitations, security and privacy concerns, interoperability and governance challenges, organizational challenges, governmental challenges, technical challenges, energy consumption, selfish mining, and the management of personal identifiable information are significant barriers to the adoption of blockchain technology. Addressing these challenges and developing innovative solutions are essential to realize the full potential of blockchain technology. Blockchain technology, introduced through Bitcoin, offers a decentralized and secure way to record and store information. Its potential applications are vast, and it holds promise for transforming various industries. As we look to the future, it's important to explore how blockchain can improve efficiency, transparency, and security while addressing challenges related to scalability and regulatory frameworks. Please note that this explanation is simplified to provide a basic understanding of blockchain technology and Bitcoin. There are many technical and complex aspects involved in these topics, but this overview should give you a general idea of how they work.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus,

and Future Trends," Proceedings - 2017 IEEE 6th International Congress on Big Data, Big Data Congress 2017, pp. 557-564, 2017.

[2] M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," SSRN Electronic Journal, 2015.

[3] A. Bahga and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," Journal of Software Engineering and Applications, vol. 9, pp. 533-546, 2016.

[4] C. Delgado-Von-eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, "Blockchain Applications in Education: A Systematic Literature Review," Applied Sciences, vol. 11, no. 24, p. 11-18, 2021.

[5] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A Secure Sharding Protocol for Open Blockchains," 2016.

[6] G. Zyskind and A. Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy," New Solutions for Cybersecurity, pp. 425-456, 2019.

[7] N. Szabo, "Formalizing and Securing Relationships on Public Networks," First Monday, vol. 2, no. 9, 1997.

[8] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," 2016 IEEE International Conference on Consumer Electronics, ICCE 2016, pp. 467-468, 2016.

[9] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", 2015.

[10] T. Dickerson, P. Gazzillo, M. Herlihy, and E. Koskinen, "Adding Concurrency to Smart Contracts," Distrib Comput, vol. 33, no. 3–4, pp. 209–225, 2017.

[11] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?," Future Internet vol. 10, no. 2, pp. 20-23, 2018.

[12] B. Nissen, L. Pschetz, D. Murray-Rust, H. Mehrpouya, S. Oosthuizen, and C. Speed, "GeoCoin: Supporting ideation and collaborative design with smart contracts," Conference on Human Factors in Computing Systems - Proceedings, vol. 2, 2018.

[13] M. Shurman, A. A. R. Obeidat, and S. A. D. Al-Shurman, "Blockchain and Smart Contract for IoT," 2020 11th International Conference on Information and Communication Systems, ICICS 2020, pp. 361-366, 2020.

[14] T. Feng, X. Yu, Y. Chai, and Y. Liu, "Smart contract model for complex reality transaction," International Journal of Crowd Science, vol. 3, no. 2, pp. 184–197, 2019.

[15] M. Alharby and A. van Moorsel, "Block-

chain-based Smart Contracts: A Systematic Mapping Study," pp. 125-140, 2017.

[16] I. Eyal and E. G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," Commun ACM, vol. 61, no. 7, pp. 95-102, 2013.

[17] Y. Yue, X. Li, D. Zhang, and S. Wang, "How cryptocurrency affects economy? A network analysis using bibliometric methods," International Review of Financial Analysis, vol. 77, 2021.

[18] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", Accessed: Feb. 23, 2024.

[19] "Blockchain Enigma. Paradox. Opportunity". vol. 9, no. 2, pp. 39-41, 2016.

[20] D. Kraft, "Difficulty control for blockchain-based consensus systems," Peer Peer Netw Appl, vol. 9, no. 2, pp. 397-413, 2016.

[21] Y. Sompolinsky and A. Zohar, "Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains," Cryptology ePrint Archive, 2013.

[22] A. Chepurnoy, M. Larangeira, and A. Ojiganov, "A Prunable Blockchain Consensus Protocol Based on Non-Interactive Proofs of Past States Retrievability," arXiv.org, 2016.

[23] A. Chandratre and A. Pathak, "Blockchain Based Intellectual Property Management," SSRN Electronic Journal, 2019.

[24] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, and T. Vieira, "A Case Study for Blockchain in Healthcare: 'MedRec' prototype for electronic health records and medical research data White Paper MedRec: Using Blockchain for Medical Data Access and Permission Management IEEE," 2016.

[25] K. Rarhi, "Melanie Swan Blockchain blueprint for a new economy." Infosec, 2023.

[26] Z. Gao, L. Xu, L. Chen, N. Shah, Y. Lu, and W. Shi, "Scalable blockchain based smart contract execution," Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS, vol. 6, pp. 352-359, 2017.

[29] D. J. Daluwathumullagamage and A. Sims, "Blockchain-Enabled Corporate Governance and Regulation," International Journal of Financial Studies 2020, vol. 8, no. 2, p. 36-44, 2020.

[30] M. Pilkington, "Blockchain Technology: Principles and Applications." vol. 2, pp. 23-31, 2024.

[31] D. Meva, "Issues and Challenges with Blockchain a Survey," International Journal of Computer Sciences and Engineering, vol. 6, no. 12, pp. 488-491, 2018.

[32] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin Meets Strong Consistency," vol. 4, pp. 31-34, 2016.

[34] H. Hellani, "On Blockchain Technology: Overview of Bitcoin and Future

Insights". pp. 41-45. 2019.

[35] F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, "Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review," Sensors, vol. 20, no. 4, p. 71-76, 2020.

[36] W. Zhang, X. Zeng, H. Liang, Y. Xue, and X. Cao, "Understanding How Organizational Culture Affects Innovation Performance: A Management Context Perspective," Sustainability, vol. 15, no. 8, p. 60-64, 2023.

[37] M. Attaran and A. Gunasekaran, "Blockchain-enabled technology: The emerging technology set to reshape and decentralise many industries," International Journal of Applied Decision Sciences, vol. 12, no. 4, pp. 424-444, 2019.