Journal of Namibian Studies, 40 S1 (2024): 217-232 ISSN: 2197-5523 (online)

Blockchain Technology: Revolutionizing Data Security And Digital Transactions

Arwa Mohamed Bezzaouia

Umm Al-Qura University. abezzaouia@uqu.edu.sa

Summary:

This research paper explores the revolutionary impact of blockchain technology on data security and digital transactions. It provides an overview of the key concepts, types, and consensus mechanisms of blockchain, highlighting its decentralized, immutable, and transparent nature. The paper discusses the applications of blockchain in data security, such as decentralized storage, encryption, and identity management, as well as its role in digital transactions, including cryptocurrencies, smart contracts, supply chain management, and cross-border payments. It also addresses the challenges and limitations of blockchain adoption, such as scalability, regulatory issues, energy consumption, and integration with existing systems. The paper concludes by examining the future developments and potential impact of blockchain technology on various industries, predicting its evolution into a more scalable, interoperable, and user-friendly ecosystem that will reshape the global digital landscape.

Keywords: Blockchain, Data Security, Digital Transactions, Decentralization, Smart Contracts.

1. Introduction

In recent years, the rapid advancement of digital technologies has transformed the way we store, share, and transact data. However, with the increasing reliance on digital systems, concerns about data security and privacy have become more prominent. Traditional centralized systems are vulnerable to hacking, data breaches, and manipulation, leading to a growing need for more secure and transparent solutions. This is where blockchain technology comes into play.

Blockchain, first introduced as the underlying technology behind the cryptocurrency Bitcoin, has since evolved into a revolutionary tool with applications extending far beyond digital currencies. At its core, a blockchain is a decentralized, distributed ledger that records transactions across a network of computers. Each block in the chain contains a cryptographic hash of the previous block, creating an immutable and tamper-proof record of all transactions.

The decentralized nature of blockchain technology eliminates the need for intermediaries, such as banks or government institutions, to validate and verify transactions. Instead, the network participants collectively validate and record transactions through a consensus mechanism, ensuring transparency and trust within the system. This decentralization also makes the blockchain highly resistant to hacking and data tampering, as there is no single point of failure or control.

Moreover, blockchain technology enables the creation of smart contracts – self-executing contracts with the terms of the agreement directly written into code. Smart contracts automatically enforce the rules and penalties around an agreement, reducing the risk of fraud and the need for third-party involvement. This feature has the potential to streamline various processes, from financial transactions to supply chain management and beyond.

The transparency and immutability of blockchain technology make it an ideal solution for securing sensitive data and ensuring the integrity of digital transactions. By providing a tamper-proof record of all transactions and enabling secure, peer-to-peer interactions, blockchain has the potential to revolutionize the way we approach data security and digital trust.

Thesis statement: Blockchain technology is revolutionizing data security and digital transactions by providing a decentralized, transparent, and immutable system for recording and verifying transactions. This paper will explore the key concepts behind blockchain technology, its applications in data security and digital transactions, the challenges and limitations it faces, and its potential impact on various industries in the future.

1.1 Research Objectives:

The research paper does not contain an explicit section or paragraph that clearly states the research objectives. However, the overall objective of the research can be inferred from the following statement in the introduction:

"Blockchain technology is revolutionizing data security and digital transactions by providing a decentralized, transparent, and immutable system for recording and verifying transactions."

Therefore, the research aims to explore how blockchain technology is revolutionizing the fields of data security and digital transactions.

1.2 Research Importance:

Similarly, there is no specific section or paragraph that directly discusses the importance of the research. However, the significance of the research can be deduced from the introduction and conclusion, where it is highlighted that the research discusses the pivotal and transformative role of blockchain technology in reshaping the landscape of digital transactions and data security, laying the foundation for a trust-based digital economy that eliminates intermediaries.

1.3 Research Methodology:

The research paper also does not have a dedicated section explicitly outlining the research methodology. However, in general, the research employs a literature review methodology, where it reviews and discusses the concepts and applications of blockchain technology based on previous studies and research in the field, as evidenced by the references mentioned at the end of the paper.

2. Overview of Blockchain Technology

2.1. Definition and key concepts

Blockchain technology is a decentralized, distributed ledger system that records transactions across a network of computers **(Nakamoto, 2008).** The key concepts of blockchain include:

1. Decentralization: No single authority controls the blockchain; instead, it is maintained by a network of participants
2. Immutability: Once data is recorded on the blockchain, it cannot be altered or deleted.

3. Transparency: All transactions on a blockchain are visible to the network participants
4. Consensus: Network participants must agree on the validity of transactions before they are added to the blockchain **(Bach et al., 2018).**

2.2. How blockchain works

A blockchain consists of a series of blocks, each containing a list of transactions. When a new transaction occurs, it is broadcast to the network for verification. Once verified, the transaction is combined with other transactions into a new block, which is then added to the existing chain **,** Each block contains a unique cryptographic hash that links it to the previous block, creating a secure and tamper-proof chain of records **(Narayanan et al., 2016).**

2.3. Types of blockchain

There are three main types of blockchain **(Buterin, 2015).**:

1. Public blockchains: Open to anyone, allowing all participants to read, write, and audit the blockchain
2. Private blockchains: Controlled by a single organization, with restricted access and permissions
3. Consortium blockchains: Governed by a group of organizations, with varying degrees of access and permissions (e.g., R3 Corda).

2.4. Consensus mechanisms

Consensus mechanisms ensure that all participants in a blockchain network agree on the validity of transactions,The two most common consensus mechanisms are:

1. Proof of Work (PoW): Miners compete to solve complex mathematical problems to validate transactions and create new blocks**.**
2. Proof of Stake (PoS): Validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral **.**

Other consensus mechanisms include Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Authority (PoA) **(Bach et al., 2018).**

3. Applications of Blockchain in Data Security

3.1. Decentralized storage and data integrity

Blockchain technology enables decentralized storage solutions that ensure data integrity and security. Decentralized storage platforms, such as InterPlanetary File System (IPFS) and Storj, use blockchain to create a distributed network of storage nodes, making data resistant to tampering and single points of failure**,** By leveraging blockchain's immutability and consensus mechanisms, these platforms maintain data integrity and prevent unauthorized modifications

3.2. Encryption and cryptography

Blockchain technology relies heavily on advanced encryption and cryptographic techniques to secure data and ensure privacy. Public-key cryptography, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), is used to create digital signatures that verify the authenticity of transactions **(Antonopoulos, 2014).** Additionally, hashing algorithms like SHA-256 are employed to create unique, fixed-size digests of data, which serve as tamper-proof identifiers for blocks and transactions, These cryptographic primitives form the foundation of blockchain's security and immutability.

3.3. Identity management and authentication

Blockchain technology offers new possibilities for secure identity management and authentication. Decentralized identity solutions, such as Sovrin and uPort, use blockchain to create self-sovereign identities that give users control over their personal data**,** By storing identity attributes on a blockchain, these systems enable secure, privacy-preserving authentication and eliminate the need for centralized identity providers, Blockchain-based identity management has applications in various domains, including healthcare, finance, and government services.

3.4. Case studies and real-world examples

1. Estonia's e-Estonia initiative: Estonia uses blockchain technology to secure its national health records, property registries, and voting systems, ensuring data integrity and transparency **(Heller, 2017).**
2. Guardtime's Keyless Signature Infrastructure (KSI): Guardtime's KSI blockchain platform provides secure data authentication and integrity verification for various industries, including aerospace, defense, and telecommunications **.**

3. Civic's Secure Identity Platform: Civic uses blockchain to provide decentralized identity verification services, allowing users to securely share their personal information with service providers.
4. Factom's data integrity solutions: Factom leverages blockchain to provide immutable data storage and verification for applications such as land title registries, medical records, and supply chain management**.**

These case studies demonstrate the practical applications of blockchain technology in enhancing data security, integrity, and privacy across various sectors.

4. Blockchain in Digital Transactions

4.1. Cryptocurrency transactions.

Blockchain technology serves as the foundation for cryptocurrencies, enabling secure, peer-to-peer digital transactions without intermediaries. Bitcoin, the first and most well-known cryptocurrency, uses a public blockchain to record and verify transactions **.**

Ethereum, another prominent blockchain platform, introduced programmable smart contracts, expanding the possibilities for decentralized applications, Cryptocurrencies leverage blockchain's decentralized .

4.2. Smart contracts and their applications

Smart contracts are self-executing contracts with the terms of the agreement directly written into code on a blockchain**.**

Ethereum's introduction of the Solidity programming language enabled the development of complex smart contracts **,** Smart contracts have various applications, such as:

1. Decentralized finance (DeFi): Smart contracts power decentralized lending, borrowing, and trading platforms, eliminating the need for traditional financial intermediaries **.**
2. Insurance: Smart contracts can automate the claims process, ensuring faster payouts and reducing fraud **(Hans et al., 2017)**.
3. Gaming: Blockchain-based games use smart contracts to manage in-game assets and player interactions, creating secure and transparent gaming environments.

4.3. Supply chain management and traceability

Blockchain technology can significantly improve supply chain management by providing a transparent, immutable record of transactions and product movements **(Abeyratne and Monfared, 2016).** By integrating blockchain into supply chain processes, companies can:

1. Enhance traceability: Blockchain enables the tracking of products from origin to end-consumer, ensuring authenticity and reducing counterfeiting **.**
2. Improve efficiency: Smart contracts can automate supply chain processes, such as payments and product releases, reducing manual intervention and errors **(Saberi et al., 2019).**
3. Increase transparency: Blockchain provides a shared, tamper-proof ledger of supply chain data, fostering trust and collaboration among stakeholders **(Francisco and Swanson, 2018).**

4.4. Cross-border payments and remittances

Blockchain technology has the potential to revolutionize cross-border payments and remittances by providing fast, secure, and cost-effective solutions. Traditional cross-border transactions often involve multiple intermediaries, resulting in high fees and slow processing times **(McKinsey & Company, 2016)**. Blockchain-based payment platforms, such as Ripple and Stellar, use distributed ledger technology to enable near-instant, low-cost international transactions .

By leveraging blockchain, these platforms can:

1. Reduce transaction costs: Blockchain eliminates the need for intermediaries, lowering the costs associated with cross-border payments **.**
2. Increase speed: Blockchain-based transactions can be processed in near real-time, significantly reducing settlement times compared to traditional methods **.**
3. Enhance security: Blockchain's decentralized and immutable nature makes it highly resistant to fraud and tampering, ensuring the security of cross-border transactions **(Peters and Panayi, 2016).**

The adoption of blockchain technology in digital transactions is transforming various industries, from finance to supply chain management, by providing secure, efficient, and transparent solutions

.

4.5. Cryptocurrency transactions Blockchain technology serves as the foundation for cryptocurrencies, enabling secure, peer-to-peer digital transactions without intermediaries. Bitcoin, the first and most well-known cryptocurrency, uses a public blockchain to record and verify transactions, Ethereum, another prominent blockchain platform, introduced programmable smart contracts, expanding the possibilities for decentralized applications,. Cryptocurrencies leverage blockchain's decentralized and immutable nature to ensure the integrity and transparency of financial transactions **(Yli-Huumo et al., 2016).**

4.5.1. Bitcoin and its impact on digital transactions Bitcoin, created by Satoshi Nakamoto in 2008, is the first and most widely recognized cryptocurrency. It utilizes a decentralized blockchain network to facilitate secure and transparent transactions without the need for intermediaries such as banks (Nakamoto, 2008). Bitcoin's success has paved the way for the development of numerous other cryptocurrencies and blockchain applications, revolutionizing the landscape of digital transactions **(Böhme et al., 2015).**

4.5.2. Altcoins and their role in the cryptocurrency ecosystem Altcoins, or alternative coins, are cryptocurrencies other than Bitcoin that have emerged in the wake of its success. These cryptocurrencies often aim to improve upon Bitcoin's limitations or offer additional features and functionalities (Haferkorn and Quintana Diaz, 2015). Examples of popular altcoins include Ethereum, Litecoin, and Ripple, each with their unique characteristics and use cases. Altcoins contribute to the diversity and innovation within the cryptocurrency ecosystem, providing users with a variety of options for digital transactions (Hileman and Rauchs, 2017).

4.6. Smart contracts and their applications Smart contracts are self-executing contracts with the terms of the agreement directly written into code on a blockchain, Ethereum's introduction of the Solidity programming language enabled the development of complex smart contracts, Smart contracts have various applications, such as:

4.6.1. Decentralized finance (DeFi) Decentralized finance, or DeFi, refers to the ecosystem of financial applications built on blockchain networks, particularly Ethereum. DeFi platforms utilize smart contracts to create decentralized lending, borrowing, and trading protocols, eliminating the need for traditional financial intermediaries, By leveraging blockchain technology, DeFi applications offer increased accessibility, transparency, and security in financial transactions, enabling users to retain full control over their assets.

4.6.2. Non-fungible tokens (NFTs) and their use cases Non-fungible tokens, or NFTs, are unique digital assets that represent ownership of specific items, such as artwork, collectibles, or real estate, on a blockchain network, NFTs are typically built using smart contracts, particularly on the Ethereum blockchain, and ensure the authenticity, scarcity, and provenance of digital assets. The use cases for NFTs extend beyond the art world, with potential applications in areas such as gaming, music, and intellectual property management (Dowling, 2021). As NFTs gain popularity, they are transforming the way value is created, transferred, and perceived in the digital realm.

5. Challenges and Limitations

5.1. Scalability and performance issues

One of the primary challenges facing blockchain technology is scalability. As the number of transactions on a blockchain network increases, the network's ability to process these transactions efficiently can be compromised **(Croman et al., 2016).** This issue is particularly evident in public blockchains like Bitcoin and Ethereum, where the consensus mechanisms (e.g., Proof of Work) can limit the transaction throughput **,**Various solutions have been proposed to address scalability issues, such as:

1. Sharding: Partitioning the blockchain into smaller, more manageable parts, allowing for parallel processing of transactions **(Luu et al., 2016).**
2. Off-chain transactions: Conducting some transactions outside the main blockchain, using techniques like the Lightning Network or sidechains **.**
3. Alternative consensus mechanisms: Employing more efficient consensus algorithms, such as Proof of Stake or Delegated Proof of Stake, to improve transaction throughput **(King and Nadal, 2012; Larimer, 2014).**

5.2. Regulatory and legal challenges

The decentralized and pseudonymous nature of blockchain technology poses significant regulatory and legal challenges. Governments and regulatory bodies are grappling with how to apply existing laws and regulations to blockchain-based systems **(Kakavand et al., 2017).** Key issues include:

1. Anti-money laundering (AML) and know-your-customer (KYC) compliance: Ensuring that blockchain-based financial services adhere to AML and KYC regulations.
2. Taxation: Determining how to tax transactions and assets on blockchain networks, particularly in the case of cryptocurrencies **(Bal, 2015).**
3. Jurisdictional issues: Navigating the complex legal landscape when blockchain transactions span multiple jurisdictions **(Hacker and Thomale, 2018).**

5.3. Energy consumption and environmental concerns

The energy consumption associated with some blockchain consensus mechanisms, particularly Proof of Work (PoW), has raised environmental concerns. The Bitcoin network, for example, is estimated to consume more energy than several countries, This high energy consumption contributes to greenhouse gas emissions and can have negative environmental impacts, To address these concerns, some blockchain platforms are exploring more energy-efficient consensus mechanisms, such as Proof of Stake (PoS) or Delegated Proof of Stake (DPoS) **.**

5.4. Adoption and integration with existing systems

Integrating blockchain technology with existing systems and processes can be challenging. Many organizations have legacy infrastructures that may not be compatible with blockchain-based solutions (Mendling et al., 2018). Moreover, the adoption of blockchain technology requires significant changes to business processes, organizational structures, and governance models **(Iansiti and Lakhani, 2017).** Overcoming these challenges requires:

1. Interoperability: Developing standards and protocols that enable blockchain networks to communicate and exchange data with existing systems **(Hardjono et al., 2019).**
2. Education and skills development: Providing training and resources to help organizations understand and

implement blockchain technology **(Katuwal et al., 2019).**

3. Collaborative ecosystems: Fostering partnerships and consortia to facilitate the development and adoption of blockchain solutions **(Beck et al., 2018).**

Addressing these challenges and limitations is crucial for realizing the full potential of blockchain technology in revolutionizing data security and digital transactions.

6. Future Developments and Potential Impact

6.1. Emerging trends and innovations in blockchain technology

As blockchain technology continues to evolve, several emerging trends and innovations are expected to shape its future development. One such trend is the convergence of blockchain with other cutting-edge technologies, such as artificial intelligence (AI), Internet of Things (IoT), and big data analytics **(Salah et al., 2019)**. This integration can unlock new opportunities for data security, process automation, and decision-making. Another notable trend is the development of more advanced smart contract languages and frameworks, which will enable the creation of sophisticated decentralized applications (dApps) and enhance the programmability of blockchain networks **(Cai et al., 2018).**

Furthermore, research into quantum-resistant cryptography is gaining traction as quantum computing advances pose potential threats to the security of current blockchain systems, The development of quantum-secure blockchain platforms will be crucial in ensuring the long-term resilience of blockchain-based data security and digital transactions.

6.2. Potential impact on various industries (finance, healthcare, government, etc).

Blockchain technology has the potential to revolutionize various industries by providing secure, transparent, and efficient solutions. In the financial sector, blockchain-based systems can streamline processes, reduce costs, and enable new business models, such as decentralized finance (DeFi) **(Schär, 2021).** In healthcare, blockchain can enhance the security and privacy of patient data, facilitate secure data sharing among healthcare providers, and improve the transparency of supply chains for pharmaceuticals and medical devices**.**

In the government sector, blockchain technology can be applied to various use cases, such as secure identity management, transparent voting systems, and efficient land registry management **(Ølnes et al., 2017).** Moreover, blockchain can play a crucial role in fostering trust and accountability in public services and reducing corruption.

6.3. Predictions for the future of blockchain and its role in data security and digital transactions

As blockchain technology matures and gains wider adoption, it is expected to become an integral part of the global digital infrastructure. The future of blockchain will likely see the emergence of more scalable, interoperable, and user-friendly platforms that cater to the needs of various industries and use cases **(Lu, 2019).** Blockchain-based data security solutions will become more sophisticated, leveraging advanced cryptography and privacy-enhancing techniques to protect sensitive information and ensure compliance with data protection regulations.

In the realm of digital transactions, blockchain technology will continue to transform the way value is exchanged and assets are managed. The rise of central bank digital currencies (CBDCs) and the increasing adoption of blockchain-based payment systems will reshape the global financial landscape **(Dashkevich et al., 2020).** Furthermore, the convergence of blockchain with IoT and AI will enable new forms of machine-to-machine transactions and autonomous economic agents, paving the way for a more interconnected and efficient digital economy.

As blockchain technology continues to evolve and mature, its impact on data security and digital transactions will become increasingly significant. The future of blockchain holds immense promise for creating a more secure, transparent, and efficient digital world.

7. Conclusion

Blockchain technology stands at the forefront of a digital revolution, redefining the paradigms of data security and digital transactions. This paper has traversed the expansive landscape of blockchain, elucidating its core principles, diverse applications, inherent challenges, and the boundless potential it harbors for the future. As we recapitulate the main points, it's imperative to underscore the foundational elements of blockchain—decentralization, immutability, transparency, and consensus—that collectively fortify its position as a bastion of digital trust and security.

Blockchain's architecture dismantles the traditional centralized frameworks, mitigating the risks of data breaches, manipulation, and single points of failure. Its immutable ledger ensures that once a transaction is recorded, it becomes an indelible part of the digital tapestry, visible to all participants and beyond the reach of tampering. This transparency, underpinned by robust consensus mechanisms, fosters an environment of trust and cooperation, eschewing the need for intermediaries and heralding a new era of peer-to-peer transactions.

The applications of blockchain technology extend far beyond the realms of cryptocurrency, infiltrating sectors such as healthcare, finance, supply chain management, and government, among others. Through decentralized storage, enhanced encryption, and blockchain-based identity solutions, it offers a secure harbor for sensitive data, protecting it from the ubiquitous threats of the digital age. Smart contracts, with their self-executing and autonomous nature, promise to streamline complex processes, embedding efficiency and transparency into the fabric of digital contracts.

Results:

- Blockchain technology provides a decentralized, immutable, and transparent system for recording and verifying transactions, enhancing data security and digital trust.
- The applications of blockchain extend beyond cryptocurrencies, with potential use cases in various industries, such as healthcare, finance, supply chain management, and government.
- Smart contracts and decentralized applications (dApps) built on blockchain platforms enable automated, secure, and efficient execution of digital agreements and processes.
- Blockchain faces challenges related to scalability, regulatory compliance, energy consumption, and integration with existing systems, which need to be addressed for widespread adoption.
- The convergence of blockchain with other technologies, such as AI, IoT, and big data analytics, opens up new

possibilities for secure, automated, and data-driven solutions.

Recommendations:

- Foster collaboration among researchers, technologists, policymakers, and industry leaders to address the limitations and explore new avenues for blockchain application.
- Develop more scalable, environmentally sustainable, and quantum-resistant consensus mechanisms to ensure the long-term viability and security of blockchain networks.
- Establish clear regulatory frameworks and global standards to guide the development and adoption of blockchain technology across industries.
- Invest in education and skills development to build a workforce capable of understanding, implementing, and leveraging blockchain solutions.
- Encourage the creation of collaborative ecosystems and partnerships to facilitate the development, testing, and deployment of blockchain-based applications and services.

References:

1. Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger. International Journal of Research in Engineering and Technology, 5(9), 1-10.
2. Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc.
3. Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. Journal of the Association for Information Systems, 19(10), 1020-1034.
4. Benet, J. (2014). IPFS-content addressed, versioned, P2P file system. arXiv preprint arXiv:1407.3561.
5. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. White paper, 3(37).
6. Buterin, V. (2015). On public and private blockchains. Ethereum blog, 7.
7. Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. (2018). Decentralized applications: The blockchain-empowered software system. IEEE Access, 6, 53019-53033.
8. Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Song, D. (2016, February). On scaling decentralized blockchains. In International conference on financial cryptography and data security (pp. 106-125). Springer, Berlin, Heidelberg.
9. Dashkevich, N., Counsell, S., & Destefanis, G. (2020). Blockchain application for central banks: A systematic mapping study. IEEE Access, 8, 139918-139952.

10. Francisco, K., & Swanson, D. (2018). The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics, 2(1), 2.
11. Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. European Company and Financial Law Review, 15(4), 645-696.
12. Hans, R., Zuber, H., Rizk, A., & Steinmetz, R. (2017). Blockchain and smart contracts: Disruptive technologies for the insurance market. In 23rd Americas Conference on Information Systems (AMCIS) (pp. 1-10).
13. Hardjono, T., Lipton, A., & Pentland, A. (2019). Towards a design philosophy for interoperable blockchain systems. arXiv preprint arXiv:1805.05934.
14. Heller, N. (2017). Estonia, the digital republic. The New Yorker, 18, 1-19.
15. Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.
16. Kakavand, H., De Sevres, N. K., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. Available at SSRN 2849251.
17. Katuwal, G. J., Pandey, S., Hennessey, M., & Lamichhane, B. (2019). Applications of blockchain in healthcare: current landscape & challenges. arXiv preprint arXiv:1812.02776.
18. King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19.
19. Larimer, D. (2014). Delegated proof-of-stake (dpos). Bitshare whitepaper.
20. Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 15, 80-90.
21. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 17-30.(
22. McKinsey & Company. (2016). Global payments 2016: Strong fundamentals despite uncertain times.
23. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.
24. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.
25. Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed

ledger technology for information sharing. Government Information Quarterly, 34(3), 355-364.

26. Peters, G. W., & Panayi, E. (2016). Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In Banking beyond banks and money (pp. 239-278). Springer, Cham.
27. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135.
28. Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127-10149.
29. Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. FRB of St. Louis Review.
30. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-38.
31. Dowling, M. (2021). Fertile LAND: Pricing non-fungible tokens. Finance Research Letters, 44, 102096.
32. Haferkorn, M., & Quintana Diaz, J. M. (2015). Seasonality and interconnectivity within cryptocurrencies-an analysis on the basis of Bitcoin, Litecoin and Namecoin. In International Workshop on Enterprise Applications and Services in the Finance Industry (pp. 106-120). Springer, Cham.
33. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.