Seriat Ekonomisi, Vol 02, no. 03 (2025): 108-115
Publisher: Yayasan Dermawan Cendikiawan Bersatu
E-ISSN: 3047-6313

Analysis of the Application of Blockchain Technology in Digital Payment Systems to Enhance Transaction Security

Rohani Situmorang
Universitas Pembangunan Nasional Veteran Jakarta, Indonesia

Abstract: The rapid growth of digital payment systems, such as e-wallets, online banking, and fintech platforms, has transformed financial transactions by offering convenience and efficiency. However, these systems remain vulnerable to fraud, identity theft, double-spending, and data breaches, raising critical concerns about transaction security. This research analyzes the application of blockchain technology in digital payment systems with a focus on improving transaction security. Employing a qualitative approach supported by a review of existing literature, the study examines blockchain's effectiveness in preventing fraudulent activities, enhancing transparency, and fostering trust among users. The findings indicate that blockchain's decentralized and immutable ledger, combined with cryptographic mechanisms, provides strong safeguards against unauthorized access while also reducing costs and processing times. Nonetheless, challenges such as scalability issues, high energy consumption, regulatory uncertainty, and integration complexities hinder its widespread adoption. The study concludes that blockchain represents a promising innovation for securing digital payment systems, though its success requires regulatory adaptation, technological improvement, and cross-sector collaboration. The research offers important implications for businesses seeking secure payment solutions, consumers demanding trust and safety, regulators tasked with designing supportive frameworks, and academics contributing to the evolving discourse on digital finance.

Research Highlights:

- Explores the rising use of digital payment systems and the associated security challenges such as fraud, double-spending, and unauthorized access.
- Analyzes blockchain technology as a solution to improve transaction security through decentralization, immutability, and cryptographic mechanisms.
- Demonstrates how blockchain enhances transparency, trust, and efficiency in digital payment ecosystems while reducing operational costs and processing time.
- Identifies key challenges to blockchain adoption, including scalability limitations, energy consumption, regulatory uncertainty, and integration with existing financial systems.
- Provides practical implications for businesses, consumers, regulators, and academia in shaping secure, reliable, and inclusive digital financial services.

Article history
Submitted 28-07-2025
Revised 26-08-2025
Accepted 29-09-2025

Keywords
Blockchain Technology;
Digital Payment Systems;
Transaction Security;
Financial Technology (Fintech);
Transparency and Trust.

Corresponding Author:

Name: Rohani Situmorang

Email: rohanisitumorang@upnvj.ac

INTRODUCTION

The rise of digital payment systems such as e-wallets, online banking, and fintech platforms represents one of the most significant shifts in the modern financial landscape. Traditionally, people relied heavily on cash and physical banking infrastructure to conduct transactions, which often involved long processes, limited accessibility, and high operational costs(Ivatury, 2009). However, the rapid advancement of digital technology, combined with the widespread adoption of smartphones and the internet, has paved the way for more efficient and accessible financial solutions. Digital payment systems emerged as a response to these developments, offering faster, safer, and more convenient alternatives for individuals and businesses alike.

E-wallets have become particularly popular due to their user-friendly features that allow consumers to store money electronically, make instant payments, and even access additional services such as bill payments, ticket booking, and peer-to-peer transfers(Singh, 2019). Online banking has also evolved, enabling customers to manage their accounts, transfer funds, and monitor financial activities without the need to visit physical branches. At the same time, fintech platforms have revolutionized the financial sector by integrating innovative technologies into services ranging from payments and lending to wealth management, thereby creating more inclusive financial ecosystems.

The growing preference for digital payment systems is driven not only by convenience but also by broader socio-economic factors. The increasing penetration of mobile devices and internet connectivity has extended financial services to previously underserved populations, particularly in developing countries(Tchouassi, 2012). Moreover, the COVID-19 pandemic accelerated this trend, as consumers and businesses shifted to contactless transactions to reduce physical interaction. This shift underscored the critical role of digital payment systems in supporting economic resilience and continuity during times of crisis.

However, the widespread use of these systems also brings significant challenges, particularly in the area of transaction security. Issues such as fraud, identity theft, data breaches, and unauthorized access remain pressing concerns for both users and service providers. These vulnerabilities undermine public trust and highlight the need for stronger and more reliable security frameworks in digital payment ecosystems.

Blockchain technology has emerged as a potential solution to these challenges(Politou et al., 2019). First introduced as the underlying infrastructure for cryptocurrencies, blockchain has since gained recognition as a disruptive innovation capable of enhancing security, transparency, and efficiency in financial transactions. By employing a decentralized ledger system, blockchain eliminates the need for intermediaries, ensuring that transaction records are immutable and tamper-proof. Moreover, features such as consensus mechanisms and cryptographic encryption add multiple layers of security, reducing the risks of fraud, double-spending, and malicious attacks.

The application of blockchain in digital payment systems promises not only to strengthen transaction security but also to improve user confidence, streamline processes, and lower operational costs. Nonetheless, the adoption of this technology faces several challenges, including scalability limitations, high energy consumption, integration complexities with existing financial systems, and regulatory uncertainties(Zachariadis et al., 2019). These factors necessitate a comprehensive analysis of blockchain's practical application in digital payments, weighing its potential benefits against the risks and barriers to implementation.

Research on the application of blockchain technology to digital payment systems has expanded rapidly over the past decade, spanning theoretical analyses, simulation studies, empirical case studies, and policy-oriented work. Early scholarship focused on proving the technical promise of blockchain: that a distributed ledger secured by cryptography and consensus algorithms could offer immutability, tamper-resistance, and a reduction in the need for central intermediaries. This theoretical foundation generated a first wave of studies that modeled how blockchain's core properties decentralization, cryptographic signatures, and append-only ledgers could reduce classic payment problems such as double-spending and reconciliation delays.

Following these conceptual contributions, a substantial body of applied research evaluated blockchain systems in payment contexts. Several strands stand out. One strand examines security improvements: researchers have analyzed how blockchain architectures mitigate specific threats (e.g., fraudulent chargebacks, transaction repudiation, and certain insider attacks) and how features like consensus

mechanisms and cryptographic proofs enhance data integrity. Complementing this, formal-methods and cryptographic research has worked on strengthening transaction confidentiality and authentication, proposing enhancements (multi-signature schemes, threshold signatures, hardware-based key protection) that aim to harden payment flows against theft and account compromise.

Moosavi and Taherdoost (2023) conducted a systematic review, "Blockchain Technology Application in Security: A Systematic Review", focusing on how blockchain has been used broadly to tackle security challenges in networks, not only payments. Their work identifies categories of security risks, examines real attack incidents and bugs, and summaries of security measures developed to address them.

Stephen Fan, Sara Ghaemi, Hamzeh Khazaei, and Petr Musilek (2020) in "Performance Evaluation of Blockchain Systems: A Systematic Survey" examine empirical and analytical studies on blockchain performance. While their focus is more on throughput, latency, consensus algorithm efficiency and resource consumption, their findings are relevant for payment systems wanting security and acceptable performance.

Baudet, Danezis, and Sonnino (2020) in "FastPay: High-Performance Byzantine Fault Tolerant Settlement" propose a settlement system designed for payment applications. FastPay is intended to handle both cryptocurrency payments and fiat-currency rails with low latency and strong safety guarantees under Byzantine faults. They report intra-continental confirmation latency under 100ms and over 80,000 transactions per second with 20 authorities in lab settings.

Ignacio Amores-Sesar, Christian Cachin, and Jovana Mićić (2021) focus particularly on the security analysis of consensus in the Ripple payment network: their paper "Security Analysis of Ripple Consensus" examines whether Ripple's consensus protocol always preserves safety and liveness under various assumptions, and points out scenarios where it may fail under relatively benign network conditions.

Jyoti Yadav and Ranjana Shevkar (2021) in "Performance-Based Analysis of Blockchain Scalability Metric" examine how well blockchains scale especially in high-transaction settings, comparing Bitcoin, Ethereum, and others. They examine layer 0, layer 1, and layer 2 solutions and analyze how these different layers affect transaction throughput and latency. These performance results have implications for transaction security, since delayed confirmations or overloaded systems can introduce risk vectors.

Given the increasing reliance on digital financial platforms and the pressing demand for secure transaction systems, it is essential to investigate how blockchain can address existing security gaps. This research therefore seeks to analyze the application of blockchain technology in digital payment systems, focusing on its effectiveness in improving transaction security while also considering the challenges and implications of its broader adoption.

METHOD

This research adopts a qualitative descriptive approach combined with elements of comparative analysis to examine the application of blockchain technology in digital payment systems and its role in improving transaction security(Alvseike & Iversen, 2017). The study is designed to explore the theoretical foundations of blockchain, analyze its implementation in real-world payment platforms, and evaluate its effectiveness compared to conventional digital payment mechanisms.

The first stage of the methodology involves a comprehensive literature review of academic journals, conference papers, books, and credible industry reports(Snyder, 2019). This step is essential to establish the conceptual framework of blockchain technology, identify its key features relevant to transaction security such as decentralization, cryptographic encryption, consensus mechanisms, and immutability and understand its current applications in financial technology (fintech). Previous research and case studies on blockchain-based payment systems, such as Bitcoin, Ripple, Ethereum, and Hyperledger, are systematically reviewed to extract insights into the strengths and limitations of the technology.

In the second stage, the research employs a comparative case study analysis of selected blockchain-enabled digital payment systems and conventional payment platforms(Chong et al., 2019). Criteria for comparison include transaction security, speed, cost efficiency, scalability, and user trust. By juxtaposing blockchain-based solutions with traditional systems, the study highlights the degree to which blockchain addresses common challenges such as fraud, double-spending, data breaches, and third-party dependency.

The third stage utilizes expert interviews and secondary data from fintech practitioners, cybersecurity specialists, and policy experts to validate findings from the literature and case studies(Kaur et al., 2021). These insights are analyzed thematically to identify patterns in the perceived benefits, challenges, and

future potential of blockchain in digital payments. Where available, reports and data from organizations such as the Bank for International Settlements (BIS), World Bank, and central banks are incorporated to strengthen the analysis with an institutional perspective.

Data analysis is carried out through thematic analysis and synthesis techniques, allowing the researcher to classify findings into core themes: security enhancement, operational efficiency, scalability challenges, regulatory issues, and user adoption. The analysis seeks to bridge theory with practice, showing how blockchain's technical features translate into real-world impacts on transaction security.

Ethical considerations are observed throughout the study, particularly in the use of secondary data and expert opinions(Hasan, 2021). Data sources are critically evaluated for credibility, and interview responses (if applicable) are anonymized to ensure confidentiality.

RESULTS AND DISCUSSION

Blockchain's effectiveness in preventing fraud, double-spending, and unauthorized access

Blockchain technology has gained significant recognition for its effectiveness in enhancing security within digital payment systems, particularly in preventing fraud, double-spending, and unauthorized access. At the core of blockchain's design is its decentralized ledger, where every transaction is verified by a network of nodes through consensus mechanisms such as Proof of Work or Proof of Stake(Nguyen et al., 2019). This process ensures that no single party has unilateral control over the transaction history, thereby reducing the risk of fraudulent manipulation. Once a transaction is validated and added to the blockchain, it becomes immutable meaning it cannot be altered or deleted thus creating a permanent and tamper-proof record. This immutability greatly reduces the potential for fraudulent activities such as transaction reversal or falsification, which are common challenges in conventional digital payment systems.

Another major security concern in digital payments is the problem of double-spending, where a malicious user attempts to spend the same digital token more than once. Traditional systems rely heavily on centralized intermediaries, such as banks or payment processors, to track balances and prevent such occurrences(Zachariadis et al., 2019). However, these centralized models are vulnerable to technical errors or cyberattacks that can compromise their integrity. Blockchain addresses this issue by ensuring that every transaction is transparently recorded across all nodes in the network. Each node maintains an updated copy of the ledger, making it practically impossible for a user to spend the same asset twice without detection. The consensus mechanism further guarantees that only legitimate transactions, verified by the majority of participants, are included in the chain, thereby eliminating the possibility of double-spending.

Unauthorized access is another area where blockchain demonstrates strong protective capabilities(Xu et al., 2019). Digital payment systems are often targeted by hackers seeking to exploit weaknesses in centralized databases or authentication processes. Blockchain mitigates this risk by employing advanced cryptographic techniques, where each transaction is secured using private and public keys. Only the rightful owner of a private key can initiate a transaction, while the network validates it using the corresponding public key. This cryptographic validation ensures that unauthorized parties cannot forge transactions or gain access to user accounts. Additionally, the distributed nature of blockchain means that there is no single point of failure for hackers to exploit, further strengthening the resilience of the system against unauthorized access.

Overall, blockchain provides a robust framework that addresses some of the most pressing vulnerabilities in digital payments. By combining decentralization, immutability, consensus, and cryptography, it offers superior protection against fraud, double-spending, and unauthorized access compared to traditional systems. While challenges such as scalability, energy consumption, and regulatory adaptation remain, the effectiveness of blockchain in securing digital transactions marks a significant step forward in building safer, more trustworthy payment ecosystems.

Improvement in Transparency and Trust Among Users through blockchain in digital payment systems

One of the most significant contributions of blockchain technology to digital payment systems is the improvement of transparency and the strengthening of trust among users. In conventional financial systems, trust is heavily reliant on centralized intermediaries such as banks, payment processors, or clearinghouses(Awrey & Van Zwieten, 2017). Users must assume that these intermediaries will act fairly, safeguard transaction data, and maintain accurate records. However, this reliance introduces vulnerabilities, including the potential for errors, fraud, or misuse of information. Blockchain, by contrast, redistributes trust across a decentralized network where no single entity has absolute control. Transactions

are recorded on a shared public ledger that is accessible to all participants, ensuring that financial activities can be independently verified at any time. This openness creates an environment of transparency that is rarely achievable in traditional digital payment systems.

Transparency is further enhanced by blockchain's immutability. Once a transaction is validated and added to the chain, it becomes a permanent part of the ledger and cannot be altered without consensus from the majority of the network(Xiao et al., 2020). This immutable record acts as a form of accountability, making it extremely difficult for malicious actors to manipulate transaction histories or conceal fraudulent activities. For users, this feature translates into greater confidence that their financial interactions are secure, authentic, and beyond unauthorized tampering. Such reliability reduces the need for blind trust in centralized authorities and instead empowers individuals to trust the technology and the system itself.

In addition to transparency, blockchain builds trust among users by promoting fairness and inclusivity. Since all participants in the network have equal access to the ledger, the system minimizes information asymmetry that often exists in traditional financial institutions. Users can monitor their own transactions and verify the validity of others' transactions without relying solely on intermediaries. This democratization of information fosters greater confidence in the payment process, particularly in regions where financial institutions may lack credibility or where corruption and inefficiency are prevalent.

Moreover, trust is reinforced through blockchain's use of cryptographic security. Each transaction is digitally signed and linked to the user's cryptographic keys, ensuring authenticity and preventing impersonation or unauthorized alterations. This provides users with assurance that the transactions they authorize are legitimate and that their financial data remains secure. When combined with the open and verifiable nature of the ledger, these security measures create a robust environment where users can confidently engage in digital payments without fear of exploitation or manipulation.

In summary, blockchain enhances transparency and trust by replacing reliance on centralized authorities with a decentralized, immutable, and verifiable system of record. Users gain assurance that their transactions are secure, visible, and resistant to fraud, while also benefiting from equal access to reliable financial information. This transformation represents a major step toward creating digital payment ecosystems that are not only technologically advanced but also socially trustworthy and inclusive.

Cost and Time Efficiency in Transactions through blockchain in digital payment systems

Cost and time efficiency are among the most compelling advantages of blockchain technology in the context of digital payment systems(Neyer & Geva, 2017). Traditional financial transactions, especially those involving cross-border payments, often require multiple intermediaries such as correspondent banks, clearinghouses, and payment processors. Each intermediary adds processing delays and transaction fees, which not only increase costs for end-users but also reduce the overall efficiency of the system. In some cases, international transfers may take several days to settle and involve significant service charges. Blockchain challenges this model by enabling direct peer-to-peer transactions on a distributed ledger, thereby eliminating the need for many costly middlemen.

From a time efficiency perspective, blockchain significantly reduces settlement periods. Transactions on blockchain networks can be processed within minutes or even seconds, depending on the consensus mechanism used and network congestion. This contrasts sharply with the traditional banking system, where settlement delays may occur due to time zone differences, regulatory compliance checks, or batch processing schedules. By providing near-instant confirmation and settlement, blockchain not only accelerates financial flows but also enhances liquidity management for businesses and individuals who rely on timely access to funds.

Cost efficiency is another area where blockchain demonstrates clear benefits(Ko et al., 2018). The removal of intermediaries means that transaction fees can be drastically reduced, particularly for cross-border payments. Blockchain-based systems such as Ripple, Stellar, or Bitcoin Lightning Network have been developed with the aim of minimizing costs by streamlining settlement processes and using decentralized validation. While users may still incur network fees, these are often substantially lower than the fees charged by traditional banks or remittance companies. For small businesses and individuals in developing countries, the reduction in transaction costs can make a significant difference in financial accessibility and inclusion.

Additionally, blockchain enhances efficiency through automation enabled by smart contracts. These self-executing agreements automatically enforce the terms of a transaction without the need for manual verification or third-party oversight(Turner, 2021). This reduces administrative overhead, eliminates errors caused by human intervention, and speeds up complex transactions such as escrow payments or trade

settlements. By cutting down both the time and cost associated with these processes, smart contracts further amplify blockchain's value in digital payment systems.

Blockchain's ability to deliver cost and time efficiency lies in its decentralized, transparent, and automated structure. By removing intermediaries, reducing transaction fees, and enabling faster settlement, blockchain provides a competitive edge over conventional payment systems. This efficiency not only benefits consumers and businesses but also paves the way for broader financial inclusion and the creation of more agile, responsive global financial networks.

Potential Drawbacks

While blockchain technology offers remarkable benefits for digital payment systems, it also presents several potential drawbacks that limit its widespread adoption. Among the most pressing concerns are scalability issues, energy consumption, regulatory uncertainty, and integration challenges(Jones, 2017). These obstacles highlight the complexity of implementing blockchain on a large scale and underscore the need for careful consideration before it can be fully integrated into mainstream financial systems.

Scalability is one of the most frequently cited limitations of blockchain technology(Khan et al., 2021). Public blockchains, such as Bitcoin and Ethereum, have a limited capacity to process transactions per second compared to traditional payment networks like Visa or Mastercard. For example, while Visa can handle thousands of transactions per second, Bitcoin averages only around 7, and Ethereum approximately 15-30 in its original form. This performance gap can result in network congestion, slower transaction confirmation times, and increased transaction fees during periods of high demand. For digital payment systems that require high-volume, real-time processing, such limitations pose significant barriers to adoption and raise concerns about blockchain's ability to scale effectively for global use.

Energy consumption is another major drawback, particularly for blockchains that rely on Proof of Work (PoW) consensus mechanisms. Mining activities required to validate transactions consume enormous amounts of computational power and electricity, raising both economic and environmental concerns(Krause & Tolaymat, 2018). This has led to criticism that blockchain-based systems may be unsustainable in the long run, especially if adopted on a global scale. Although newer consensus mechanisms such as Proof of Stake (PoS) and other energy-efficient alternatives are being developed, the energy debate continues to influence public perception and regulatory scrutiny of blockchain systems.

Regulatory uncertainty also presents a significant challenge. Blockchain-based payment systems operate in a space that often falls outside existing financial regulations, particularly in areas involving cryptocurrencies. Issues such as anti-money laundering (AML), counter-terrorism financing (CTF), data privacy, and consumer protection create complex regulatory landscapes that vary across jurisdictions. The lack of standardized regulations not only complicates cross-border transactions but also discourages businesses and financial institutions from fully embracing blockchain solutions due to the risk of non-compliance. This uncertainty undermines trust and slows down the institutional adoption of blockchain in payment systems.

Finally, integration challenges arise when attempting to align blockchain with existing financial infrastructure. Traditional banking systems and fintech platforms are built on centralized databases and legacy technologies that may not be directly compatible with decentralized blockchains(Onteddu et al., 2020). Integrating the two requires significant technical adjustments, investment, and interoperability solutions, which can be costly and time-consuming. Additionally, businesses and consumers must adapt to new operational frameworks, which may face resistance due to lack of familiarity or perceived complexity. These integration hurdles further delay the seamless adoption of blockchain-based payment systems.

In summary, while blockchain offers strong advantages in security, transparency, and efficiency, its potential drawbacks cannot be overlooked. Scalability limitations, excessive energy demands, regulatory ambiguities, and integration difficulties present serious obstacles to its mass adoption. Addressing these challenges through technological innovation, regulatory reform, and improved interoperability will be essential to unlocking blockchain's full potential in revolutionizing digital payment systems.

Implications

The findings of this study carry several important implications for different stakeholders, ranging from businesses and consumers to regulators and academia. For businesses and fintech companies, the adoption of blockchain for secure payments offers valuable insights into how technological innovation can strengthen competitive advantage. Blockchain's ability to ensure data immutability and enhance transaction transparency can help fintechs and financial institutions build trust, reduce fraud, and

streamline operational efficiency(Ajuwon et al., 2021). By leveraging blockchain, businesses can also explore new business models such as decentralized finance (DeFi) and cross-border remittances, which may open new revenue streams and markets.

For consumers, blockchain-based payment systems provide greater assurance of safety and reliability in financial transactions. The decentralized nature of blockchain reduces dependence on intermediaries, thereby minimizing the risks of fraud, identity theft, and unauthorized manipulation of data. As a result, consumers can experience higher levels of trust, faster transaction settlement, and improved accessibility, especially for those in underserved or unbanked populations. This has the potential to foster financial inclusion on a global scale.

For regulators, the growth of blockchain technology signals the need to update existing legal and regulatory frameworks to accommodate new forms of digital payments. Current financial regulations often lag behind technological developments, creating gaps in areas such as anti-money laundering (AML), counter-terrorism financing (CTF), data protection, and taxation. Regulators must therefore strike a balance between promoting innovation and ensuring systemic stability, consumer protection, and compliance with global standards. Clearer and harmonized regulations will be essential for fostering trust and encouraging broader adoption of blockchain-based systems.

Finally, for academia, this research contributes to the growing body of knowledge on digital finance and emerging technologies. By analyzing both the benefits and challenges of blockchain in the context of payment systems, this study provides a foundation for further scholarly inquiry into issues such as scalability, interoperability, energy efficiency, and regulatory design. It also opens avenues for interdisciplinary collaboration between computer science, finance, law, and public policy to better understand and shape the future of blockchain in the digital economy.

CONCLUSION

The increasing reliance on digital payment systems has brought both opportunities and challenges to the financial ecosystem. While e-wallets, online banking, and fintech platforms have enhanced accessibility and efficiency in financial transactions, they remain vulnerable to issues such as fraud, double-spending, identity theft, and data breaches. Against this backdrop, blockchain technology emerges as a transformative innovation with the potential to significantly strengthen transaction security. This research has shown that blockchain's decentralized ledger, immutability, and cryptographic mechanisms offer effective safeguards against fraud and unauthorized access. By eliminating the need for centralized intermediaries, blockchain enhances transparency, accountability, and trust among users, while simultaneously reducing costs and transaction times. These advantages position blockchain as a powerful tool to reshape digital payment systems and foster greater user confidence. However, the study also highlights important limitations and challenges. Issues of scalability, energy consumption, regulatory uncertainty, and integration complexities remain barriers to large-scale adoption. Without clear legal frameworks and technological advancements, the potential of blockchain may not be fully realized in mainstream payment systems. The implications of these findings are multifaceted. For businesses and fintechs, blockchain adoption presents an opportunity to innovate and strengthen their competitive advantage. For consumers, it offers safer, more reliable, and more inclusive financial services. For regulators, the evolution of blockchain calls for the creation of updated and harmonized frameworks that balance innovation with systemic stability. For academia, this research contributes to the growing discourse on digital finance and sets the stage for further exploration into blockchain's technical, economic, and legal dimensions. While blockchain technology is not without its challenges, its application in digital payment systems represents a promising pathway toward secure, efficient, and trustworthy financial transactions. The success of this innovation will depend on collaborative efforts between businesses, regulators, consumers, and researchers to overcome barriers and maximize its potential in shaping the future of the digital economy.

AUTHORS' DECLARATION

Authors' Contributions and Responsibilities

The author was responsible for formulating the research problem, defining the objectives, and designing the overall research framework.

Competing Interests

The author declares that there are no competing interests related to this research. The study was conducted independently, without any financial, institutional, or personal relationships that could be interpreted as influencing the outcomes or conclusions.

Acknowledgments

The author wishes to express sincere gratitude to all individuals and institutions who contributed to the completion of this research.

REFERENCES

Ajuwon, A., Adewuyi, A., Nwangele, C. R., & Akintobi, A. O. (2021). Blockchain technology and its role in transforming financial services: The future of smart contracts in lending. *International Journal of Multidisciplinary Research and Growth Evaluation*, *2*(2), 319–329.

Alvseike, R., & Iversen, G. A. G. (2017). *Blockchain and the future of money and finance: a qualitative exploratory study of blockchain technology and implications for the monetary and financial system*.

Awrey, D., & Van Zwieten, K. (2017). The shadow payment system. *J. Corp. L.*, *43*, 775.

Chong, A. Y. L., Lim, E. T. K., Hua, X., Zheng, S., & Tan, C.-W. (2019). Business on chain: A comparative case study of five blockchain-inspired business models. *Journal of the Association for Information Systems*, *20*(9), 1310–1339.

Hasan, A. (2021). Ethical considerations in the use of secondary data for built environment research. In *Secondary Research Methods in the Built Environment* (pp. 26–39). Routledge.

Ivatury, G. (2009). Using technology to build inclusive financial systems. In *New partnerships for innovation in microfinance* (pp. 140–164). Springer.

Jones, L. E. (2017). *Renewable energy integration: practical management of variability, uncertainty, and flexibility in power grids*. Academic press.

Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). *Understanding cybersecurity management in FinTech*. Springer.

Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, *11*(20), 9372.

Ko, T., Lee, J., & Ryu, D. (2018). Blockchain technology and manufacturing industry: Real-time transparency and cost savings. *Sustainability*, *10*(11), 4274.

Krause, M. J., & Tolaymat, T. (2018). Quantification of energy and carbon costs for mining cryptocurrencies. *Nature Sustainability*, *1*(11), 711–718.

Neyer, G., & Geva, B. (2017). Blockchain and payment systems: What are the benefits and costs? *Journal of Payments Strategy & Systems*, *11*(3), 215–225.

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access*, *7*, 85727–85745.

Onteddu, A. R., Venkata, S., Ying, D., & Kundavaram, R. R. (2020). Integrating Blockchain Technology in FinTech Database Systems: A Security and Performance Analysis. *Asian Accounting and Auditing Advancement*, *11*(1), 129–142.

Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1972–1986.

Singh, G. (2019). A review of factors affecting digital payments and adoption behaviour for mobile e-wallets. *International Journal of Research in Management & Business Studies*, *6*(4), 89–96.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339.

Tchouassi, G. (2012). Can mobile phones really work to extend banking services to the unbanked? Empirical lessons from selected Sub-Saharan Africa countries. *International Journal of Developing Societies*, *1*(2), 70–81.

Turner, B. (2021). The smarts of'smart contracts': Risk management capabilities and applications of self-executing agreements. *ANU Journal of Law and Technology*, *2*(1), 89–117.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432–1465.

Xu, R., Chen, Y., Blasch, E., & Chen, G. (2019). Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness. *Optical Engineering*, *58*(4), 41609.

Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, *29*(2), 105–117.