Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 18 No. 21 (2024) | OPEN ACCESS

https://doi.org/10.3991/ijim.v18i21.52099

PAPER

Blockchain Technology in Mobile Payments: A Systematic Review of Security Enhancements in Mobile Commerce

Vichayanan Rattanawiboonsom[1](✉), Nohman Khan[2]

[1]Faculty of Business, Economics, and Communication, Naresuan University, Phitsanulok, Thailand

[2]Abbottabad University of Science & Technology (AUST), Abbottabad, Pakistan

vichayananr@nu.ac.th

ABSTRACT

This systematic review aims to examine how blockchain technology enhances security and trust in mobile commerce transactions, focusing on its application in mobile payments. The study employs a comprehensive methodology, utilizing the Scopus database to gather relevant literature published between 2018 and 2024. Using carefully selected keywords related to blockchain, mobile payments, and security, the initial search yielded 229 records, which were subsequently filtered using the PRISMA framework. After thorough screening, 86 studies were selected for in-depth analysis. The study utilizes VOS viewer software for bibliometric analysis, revealing a significant annual growth rate of 49.13% in publications, indicating rapidly increasing interest in this field. The results highlight four main thematic clusters: wallets, financial, blockchain, and mobile, with the blockchain cluster showing the highest centrality and frequency. Key findings demonstrate that blockchain technology addresses critical issues in mobile payments, such as high storage costs and processing latency, while significantly improving transaction throughput and security. Blockchain-based self-sovereign identity (SSI) systems are revolutionizing identity management and know your customer (KYC) processes, enhancing both efficiency and privacy. The development of secure lightweight wallets and the implementation of advanced cryptographic techniques have markedly improved the security and speed of mobile transactions. Furthermore, blockchain technology shows promise in combating financial crimes and enabling offline transactions in areas with poor connectivity. The study concludes that blockchain technology is transforming mobile commerce security, but also identifies areas for future research, including scalability solutions, regulatory frameworks, and user-friendly interfaces to encourage wider adoption.

KEYWORDS

blockchain technology, mobile payments, cybersecurity, digital wallets, financial innovation

1 INTRODUCTION

The rapid proliferation of mobile networks has fundamentally transformed the way we live, work, and communicate [1]. This digital revolution has ushered in an

Rattanawiboonsom, V., Khan, N. (2024). Blockchain Technology in Mobile Payments: A Systematic Review of Security Enhancements in Mobile Commerce. *International Journal of Interactive Mobile Technologies (iJIM)*, 18(21), pp. 134–148. https://doi.org/10.3991/ijim.v18i21.52099

Article submitted 2024-07-05. Revision uploaded 2024-08-28. Final acceptance 2024-09-05.

era of unprecedented connectivity, with mobile devices becoming an integral part of our daily lives. As the volume of data transmitted over these networks continues to grow exponentially, ensuring trust and security has become a paramount concern for organizations, governments, and individuals alike [2]. Traditional centralized systems used to manage mobile networks have faced numerous security challenges. These systems are vulnerable to various forms of cyberattacks, including hacking, man-in-the-middle attacks, and data breaches [3]. Moreover, the centralized approach creates a single point of failure, making the network susceptible to outages and disruptions [4]. As a result, there is an urgent need for innovative solutions that can address these security vulnerabilities and enhance trust in mobile networks.

Enter blockchain technology—a distributed, decentralized ledger system that has revolutionized sectors such as finance, supply chain, healthcare, and industry [5]. The unique characteristics of blockchain, including its decentralized nature and tamper-evident structure, present a compelling opportunity to bolster security and trust in mobile networks [6]. By leveraging the core features of distributed ledger, consensus mechanisms, and encryption, blockchain technology has the potential to create a more secure environment for mobile transactions and data exchange [5].

One of the primary advantages of blockchain technology in the context of mobile networks is its ability to provide a decentralized platform for recording and securing data [7]. Unlike traditional centralized systems where information is stored and managed by a single entity, a blockchain network distributes data across multiple nodes [8]. This decentralized architecture eliminates the need for intermediaries and significantly reduces the risk of a single point of failure [9]. Even if one node is compromised, the rest of the network continues to function, ensuring continuity and maintaining the integrity of the system.

Furthermore, blockchain technology offers tamper-evident records of all transactions and network activities, creating an auditable and transparent environment [10]. This feature is particularly crucial in mobile networks, where the security of sensitive user data and financial transactions is of utmost importance [11]. The immutability of blockchain records, ensured through cryptographic hashing and consensus mechanisms, makes it extremely difficult for malicious actors to alter or manipulate data without detection [12].

The integration of blockchain technology in mobile networks also presents opportunities for enhancing user authentication and identity management [13]. By providing a secure and decentralized system for storing and verifying user identities, blockchain can significantly reduce the risk of identity theft and unauthorized access to sensitive information [14]. This is especially relevant in the context of mobile commerce, where secure and reliable authentication mechanisms are essential for building trust between users and service providers [15].

The transparency offered by blockchain-based systems also contributes to building trust in mobile networks [16]. By allowing for tamper-evident record-keeping of all network transactions, blockchain technology enables easy tracing and identification of any suspicious or unauthorized activity [17]. This transparency fosters a sense of trust among network users, making the mobile network more reliable and secure [18].

However, it is important to acknowledge that the implementation of blockchain technology in mobile networks is not without challenges. Scalability remains a significant hurdle, as current blockchain systems have limitations in terms of the number of transactions they can process simultaneously [19]. The high volume of data transmitted, and the growing number of mobile users may lead to performance issues and delays in the mobile network. Additionally, the integration of blockchain with existing systems and protocols in mobile networks poses technical and operational challenges [20].

This study aims to systematically review and synthesize the current literature on the application of blockchain technology in mobile payments, with a specific focus on how it enhances security and trust in mobile commerce transactions. By examining blockchain's role in addressing existing security challenges and vulnerabilities, we seek to understand how this technology can revolutionize the mobile payment landscape. To systematically review and synthesize the current literature on the application of blockchain technology in mobile payments, with a specific focus on how it enhances security and trust in mobile commerce transactions. The study following the research questions.

1. How does the integration of blockchain technology in mobile payment systems address existing security challenges and vulnerabilities in mobile commerce?
2. What are the key trust-enhancing features of blockchain-based mobile payment solutions, and how do they compare to traditional mobile payment security measures in terms of data protection and user privacy?

2 RESEARCH METHODOLOGY

The current research encompasses literature from two large, reputed databases, Scopus, among researchers worldwide. We used (blockchain OR "distributed ledger" OR "decentralized ledger") AND ("mobile payment*" OR "m-payment*" OR "digital wallet*" OR "e-wallet*") AND (security OR secure OR trust* OR privacy OR encryption OR "data protection") keywords for the literature search. Initially, 229 records were obtained. The preferred reporting items for systematic reviews and meta-analyses (PRISMA) framework was used to screen the records as suggested by [21–23] and shown in Figure 1. Some critical inclusion and exclusion criteria for this review were published articles in the English language and related to fintech services. The review papers, articles, and book chapters are included in the review. Conclusive 207 studies are selected for stage 1 and used for keyword cloud and keyword occurrence. Later, a careful screening was performed for each identified classification to determine relevant records, and only 86 studies were selected to be included to synthesize the review. Figure 1 shows the overall PRISMA statement 2020 selection and rejection process of the current study in detail.

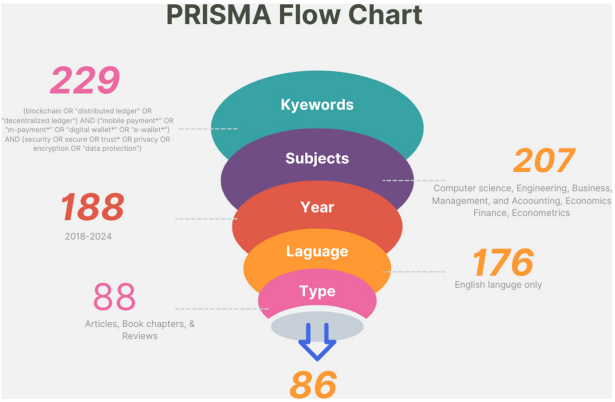

Fig. 1. PRISMA statement 2020 inclusion and exclusion criteria

3 DESCRIPTIVE

The VOSviewer software was employed to conduct the bibliometric analysis. This software is designed to construct and visualize bibliometric networks, allowing

researchers to analyze the relationships and trends within the selected literature [24]. In addition, Table 1 provides a comprehensive overview of the literature landscape on blockchain technology in mobile payments and security from 2018 to 2024. The analysis covers 86 documents from 74 sources, showing a significant annual growth rate of 49.13% in publications, indicating rapidly increasing interest in this field. The average document age of 2.03 years and 9.721 citations per document suggest that the research is both recent and impactful. The corpus includes a rich set of 294 Keywords Plus and 250 author keywords, reflecting the diverse aspects of the topic being explored. With 281 authors contributing, including 11 single-authored documents, the field shows a good balance of individual and collaborative work. The average of 3.56 co-authors per document and 24.42% international co-authorships demonstrate a strong collaborative nature in the research community, with a notable global perspective. The document types are predominantly articles (55), followed by book chapters (28) and reviews (3), providing a mix of primary research and synthesis of knowledge. This data paints a picture of a dynamic, collaborative, and rapidly evolving research area with significant scholarly attention and impact.

Table 1. Main information

Description	Results
Timespan	2018:2024
Sources (Journals, Books, etc.)	74
Documents	86
Annual Growth Rate %	49.13
Document Average Age	2.03
Average Citations Per Doc	9.721
References	4006
Keywords Plus (ID)	294
Author's Keywords (DE)	250
Authors	281
Authors of Single-Authored Docs	11
Single-Authored Docs	11
Co-Authors Per Doc	3.56
International Co-authorships %	24.42
Article	55
Book Chapter	28
Review	3

In addition, Figure 2 illustrates the annual production of articles from 2018 to 2024, showing a clear upward trend in research output over time. The graph begins with an article published in 2018, marking the initial emergence of the field. There's a significant jump to seven articles in both 2019 and 2020, indicating growing interest. From 2021 onwards, there's a steep and consistent increase, with 13 articles in 2021, 20 in 2022, and a peak of 27 articles in 2023. This rapid growth suggests a surge in research activity and interest in the topic. Interestingly, there's a slight decrease to 11 articles in 2024, though this could be due to incomplete data for the current year or a potential stabilization of research output. Overall, the graph demonstrates a robust

expansion of scholarly work in this area, particularly from 2021 to 2023, reflecting the increasing importance and relevance of the subject matter in recent years.

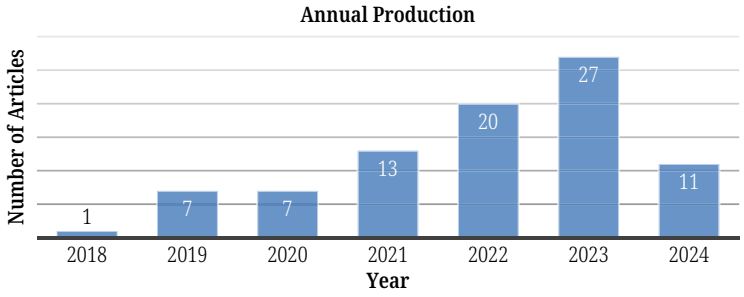

Fig. 2. Annual production of the documents

Furthermore, Figure 3 presents the major sources that have contributed publications to the current study on blockchain technology in mobile payments and security. The graph shows a variety of journals and publications across different fields, reflecting the interdisciplinary nature of the research topic.

The top contributors are Electronic Markets, Fintech in Islamic Financial Institutions, and IEEE Access, each with three publications. This suggests a strong interest in the topic from both financial technology and engineering perspectives. The presence of IEEE Access, a broad-scope journal, indicates the wide-ranging technical aspects of blockchain applications in mobile payments. Following these are several journals with two publications each: Accounting Perspectives, Applied Sciences, Business and Information Systems Engineering, *International Journal of Innovative Technology and Exploring Engineering*, *International Journal of Interactive Mobile Technologies*, and *Journal of Emerging Technologies in Accounting*. This diverse set of sources spans fields such as accounting, business systems, innovative technologies, and mobile technologies, underscoring the multifaceted nature of blockchain applications in mobile commerce and payments.

The variety of journals represented highlights that research on blockchain in mobile payments is not confined to a single discipline but draws interest from multiple fields, including finance, technology, engineering, and business. This interdisciplinary approach is crucial for addressing the complex challenges and opportunities presented by blockchain technology in the mobile payment ecosystem.

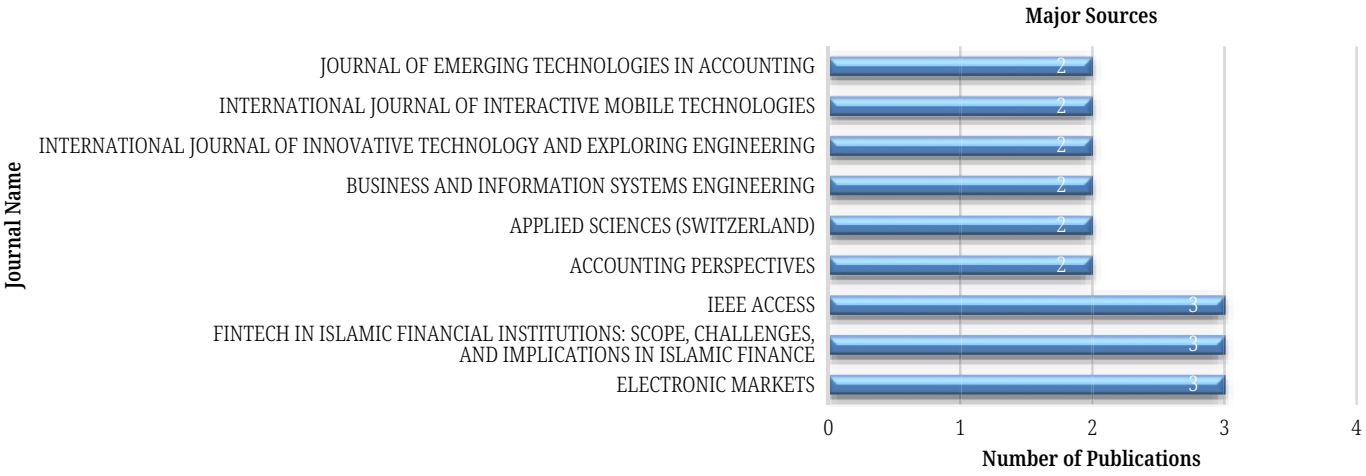

Fig. 3. Major sources inclusion

4 RESULTS

Figure 4 presents a complex network visualization of key terms and their relationships in the research corpus on blockchain technology in mobile payments and security. The visualization is color-coded, with clusters of interconnected terms represented by different hues. At the center of the network, we see prominent terms such as "blockchain," "digital," "technology," and "wallets," indicating their central role in the discourse. The red cluster on the left side emphasizes security-related concepts such as "secure," "transaction," and "wallet," highlighting the importance of safety in blockchain applications. The green cluster focuses on data and information aspects, while the blue cluster on the right side appears to be more concerned with financial and banking applications, featuring terms such as "fintech," "banking," and "financial." Purple nodes scattered throughout suggest cross-cutting themes such as "transparency" and "efficiency." The density and interconnectedness of the nodes demonstrate the multifaceted nature of blockchain research in mobile payments, encompassing technological, financial, and security dimensions. This visualization effectively captures the interdisciplinary character of the field and the complex interplay between various concepts and application areas.

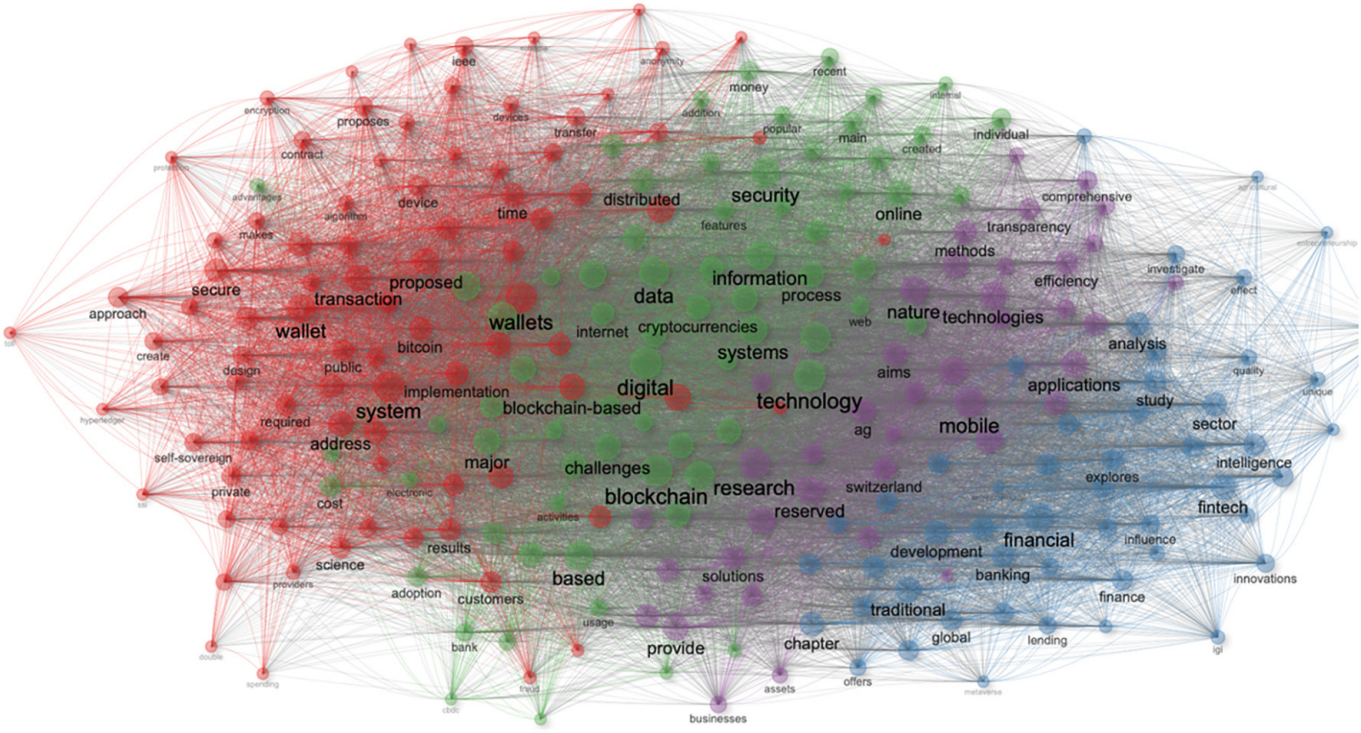

Fig. 4. Key term occurrences

In addition, Table 2 presents a compelling overview of the thematic clusters identified in the research on blockchain technology in mobile payments and security. The table uses two key metrics, callon centrality and callon density, to characterize four main clusters: wallets, financial, blockchain, and mobile. The blockchain cluster shows the highest callon centrality (81.665) and the second-highest callon density (64.645), indicating its central role and well-developed nature in the research field. It also has the highest cluster frequency (924), underscoring its prominence in the literature. The wallets cluster, while ranking third in centrality, has the highest density (92.317), suggesting a highly focused and internally cohesive research area.

The financial cluster ranks second in both centrality and density, reflecting its significant role and well-established research base. Interestingly, the mobile cluster, despite having the lowest centrality and density scores, ranks first in both categories, possibly indicating its foundational role or broad relevance across the field. This cluster analysis provides valuable insights into the structure and focus areas of research in blockchain-based mobile payments and security, highlighting the interplay between technological, financial, and user-interface aspects of the field.

Table 2. Thematic clusters on block chain technology and mobile payments

Cluster	Callon Centrality	Callon Density	Rank Centrality	Rank Density	Cluster Frequency
Wallets	54.001	92.317	3	4	694
Financial	53.647	71.738	2	3	453
Blockchain	81.665	64.645	4	2	924
Mobile	47.96	41.487	1	1	475

Furthermore, the thematic map presented in Figure 5 provides a visual representation of the key themes in blockchain research for mobile payments and security, organized along two axes: relevance degree (centrality) and development degree (density). The map is divided into four quadrants, each representing different stages of thematic development. In the upper right quadrant, labeled "Motor Themes," we find the highly developed and central topics of "wallets," "system," and "wallet," indicating their mature and driving role in the field. The upper left quadrant, "Niche Themes," contains "financial," "fintech," and "traditional," suggesting these are well-developed but somewhat specialized areas. The lower right quadrant, "Basic Themes," includes "blockchain," "digital," and "technology," representing fundamental concepts with high centrality but lower density, likely due to their broad applicability. In the lower left, "Emerging or Declining Themes," we see "mobile," "research," and "services," which may be either emerging areas of study or topics losing relevance. This map effectively illustrates the current landscape of research themes, highlighting both established core concepts and potential areas for future development in the field of blockchain-based mobile payments and security.

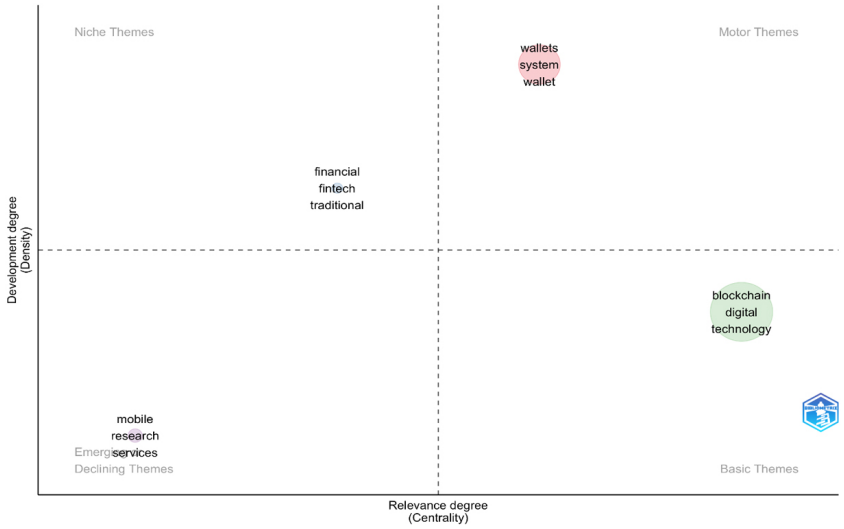

Fig. 5. Thematic map

5 BLOCKCHAIN TECHNOLOGY AND EXISTING SECURITY CHALLENGES IN MOBILE COMMERCE

Blockchain technology emerges as a pivotal area of research in the realm of digital finance, particularly in its applications to mobile payments, digital identities, and security enhancements [25]. At the core of the blockchain cluster is its ability to enhance security and efficiency in financial transactions. [26] proposed solutions to address the critical issues of high storage costs and payment processing latency in mobile cryptocurrency payments, laying the groundwork for more efficient blockchain-based mobile payment systems. Building on this foundation, [27] developed a Deep Reinforcement Learning-based Payment Channel Rebalancing algorithm, which significantly improved transaction throughput and success rates in blockchain-based payment networks, further advancing the efficiency of cryptocurrency transactions.

In addition, the cluster also showcases blockchain's potential in revolutionizing identity management and verification processes. [28] demonstrated how blockchain-based self-sovereign identity (SSI) can enhance the efficiency and privacy of know your customer (KYC) processes, a crucial aspect of financial services. This concept of SSI was further explored by [29], who highlighted its capacity to enable secure and privacy-preserving management of digital identities and credentials. The application of SSI extends beyond financial services, as evidenced by [30], who applied this technology to event ticketing systems, improving secondary market control and enhancing privacy for users.

However, security remains a paramount concern in blockchain applications [31] contributed to this aspect by developing a trustzone-based secure lightweight wallet for hyperledger fabric, which showed improved performance and security compared to traditional bitcoin wallets. Similarly, [32] demonstrated through security testing that Ethereum transactions utilizing Merkle Hash Tree are both faster and more secure than conventional transactions, further solidifying the security advantages of blockchain in financial applications.

The blockchain cluster also addresses complex financial processes. [33] proposed a novel approach of recording transactions on the blockchain before populating enterprise resource planning (ERP) systems, potentially streamlining reconciliation processes and reducing associated costs and time. This approach could have significant implications for improving efficiency in multi-stakeholder financial operations. Furthermore, to provide a structured understanding of blockchain systems, [34] developed a comprehensive taxonomy that includes components such as digital wallets and tokens. This framework offers valuable insights for researchers and practitioners in conceptualizing and developing blockchain-based solutions. Additionally, the cluster demonstrates blockchain's potential in combating financial crimes. [35] introduced a self-supervised graph neural network framework for detecting illicit transactions in bitcoin, outperforming existing methods in anti-money laundering efforts. This advancement showcases how blockchain technology, combined with advanced analytics, can enhance the integrity and security of cryptocurrency transactions. Table 3 of block chain technology for security challenges in mobile commerce illustrates the details of authors, research settings, and major outcomes of the studies.

Table 3. Block chain technology and security challenges in mobile commerce

Authors	Settings	Outcomes
Schlatt et al. (2022)	KYC processes	Blockchain-based SSI improves KYC efficiency and privacy.
Xu et al. (2020)	Mobile cryptocurrency payment	Addressed storage cost and latency issues in mobile payments.
Sedlmeir et al. (2021)	Digital identities	Enables secure, privacy-preserving identity management.
Feulner et al. (2022)	Event ticketing	SSI improves secondary market control and privacy.
Chen et al. (2024)	Payment channel networks	DRL algorithm improves transaction throughput and success.
Dai et al. (2021)	Hyperledger Fabric wallet	Developed secure lightweight wallet with improved performance.
Bosamia and Patel (2022)	Ethereum security testing	Ethereum with Merkle hash tree is faster and more secure.
Gomaa et al. (2023)	Multi-stakeholder reconciliation	Blockchain-first approach may reduce reconciliation time and costs.
Alzhrani et al. (2022)	Blockchain system taxonomy	Comprehensive framework including digital wallets and tokens.
Lo et al. (2023)	Bitcoin anti-money laundering	GNN framework outperforms in detecting illicit transactions.

In conclusion, the Blockchain Cluster represents a dynamic and rapidly evolving area of research, with implications spanning from enhancing the efficiency and security of financial transactions to revolutionizing identity management and combating financial crimes. The interrelated nature of these studies demonstrates how advancements in one area of blockchain technology can have far-reaching effects across multiple domains of digital finance and identity management.

6 BLOCKCHAIN-BASED MOBILE WALLETS

The mobile wallets cluster represents a significant area of research and innovation in the realm of digital finance, showcasing the evolving landscape of payment technologies and their integration with blockchain systems [36]. [37] proposed an innovative blockchain-based mobile wallet that enables offline transactions using Bluetooth and digital signatures, addressing the challenge of transactions in areas with poor internet connectivity. This offline capability is further explored by [38], who developed the Pure Wallet system for blockchain-based offline transactions, demonstrating the industry's push towards more flexible and accessible payment solutions. According to [39], the role of blockchain in providing multi-level authentication for secure mobile electronic payment transactions. Building on this security focus, [40] conducted a comprehensive assessment of security measures in cryptocurrency wallets, offering insights into future improvement prospects.

In addition, the integration of blockchain technology with mobile wallets is a recurring theme in this cluster. [31] developed a secure lightweight wallet for Hyperledger Fabric, showcasing improved performance compared to traditional blockchain wallets. This advancement in blockchain-based wallets is complemented by the work of [41],

who proposed the H2CT protocol for efficient and secure key management in wallets, addressing the crucial aspect of cryptographic key security in blockchain environments. Also, privacy and anonymity in mobile payments are also significant concerns addressed within this cluster. [42] proposed the SATP system for strong anonymity in mobile payments, specifically designed to protect user privacy against curious third-party providers. This focus on privacy aligns with the broader trend of enhancing user trust and security in digital financial transactions. Table 4 depicts the outcomes of the studies discussed about mobile wallets in the context of blockchain technology.

Table 4. Blockchain based digital wallets

Authors	Settings	Outcomes
Rasheed et al. (2023)	Blockchain mobile wallet	Proposed offline transactions using Bluetooth and digital signatures.
Mohamed (2023)	Mobile electronic payment system	Blockchain provides multi-level authentication for secure transactions.
Kersic et al. (2023)	Digital wallets for identity management	Proposed orchestration solution for on- and off-chain wallets.
Nowroozi et al. (2023)	Cryptocurrency wallets	Assessed security measures and future improvement prospects.
Dai et al. (2021)	Hyperledger Fabric wallet	Developed secure lightweight wallet with improved performance.
Cao and Zhu (2019)	Anonymous mobile payment	Proposed SATP for strong anonymity against curious third-party providers.
Igboanusi et al. (2021)	Offline transaction architecture	Developed Pure Wallet for blockchain-based offline transactions.
Li et al. (2024)	e-CNY adoption in China	Identified factors influencing willingness to use central bank digital currency.
Hoess et al. (2024)	Mobility-as-a-Service	Digital wallets enable seamless multimodal mobility services.
Xiang et al. (2024)	Distributed key generation	Proposed H2CT protocol for efficient and secure key management in wallets.

Furthermore, [43] investigated factors influencing the willingness to use e-CNY, China's central bank digital currency, providing valuable insights into the adoption of state-backed digital currencies. Similarly, [44] examined how digital wallets can enable seamless multimodal mobility services, illustrating the potential of mobile wallets beyond traditional financial transactions. An interesting development in this cluster is the convergence of identity management with mobile wallets. [45] proposed an orchestration solution for on- and off-chain wallets in the context of digital identity management. This study highlights the expanding role of mobile wallets as not just financial tools but also as potential carriers of digital identities and credentials.

The mobile wallets demonstrate the dynamic and multifaceted nature of research in this field. From enhancing security and privacy to enabling offline transactions and supporting diverse applications such as digital identity management and mobility services, mobile wallets are at the forefront of digital finance innovation [46]. The interconnected nature of these studies shows how advancements in one aspect of mobile wallet technology, such as security or offline capabilities, can have far-reaching implications for the entire ecosystem of digital payments and beyond.

7 CONCLUSION

The review of blockchain technology in mobile payments reveals a transformative impact on security and trust in mobile commerce transactions. Blockchain's decentralized architecture fundamentally enhances security by eliminating single points of failure and providing tamper-evident records. The technology addresses critical issues in mobile payments, such as high storage costs and processing latency [26], while significantly improving transaction throughput and success rates through advanced algorithms [47]. Blockchain-based SSI systems are revolutionizing identity management and KYC processes, enhancing both efficiency and privacy. The development of secure lightweight wallets [31] and the implementation of Merkle Hash Trees in Ethereum transactions have markedly improved the security and speed of mobile transactions. Furthermore, blockchain technology is proving invaluable in combating financial crimes, with advanced analytics detecting illicit transactions more effectively. Innovations in offline transaction capabilities are extending the reach of secure mobile payments to areas with poor connectivity, while systems such as SATP enhance user privacy against third-party intrusions. The integration of blockchain with central bank digital currencies and its application in non-financial sectors such as mobility services and digital identity management underscore its versatility and far-reaching impact.

Looking to the future, several recommendations emerge from this review. First, there is a need for continued research into scalability solutions to address the high volume of transactions in mobile networks. Second, efforts should be directed towards seamless integration of blockchain with existing mobile payment infrastructure to ensure widespread adoption. Third, regulatory frameworks need to evolve to accommodate blockchain-based financial innovations while ensuring consumer protection. Fourth, further exploration of blockchain's potential in enhancing cross-border mobile payments could significantly benefit global commerce. Fifth, research into improving the energy efficiency of blockchain systems for mobile applications is crucial for sustainability. Sixth, developing user-friendly interfaces for blockchain-based mobile wallets is essential to encourage wider adoption among non-technical users. Finally, ongoing studies into the long-term economic and social impacts of blockchain-enabled mobile payments will be vital for informed policy-making and industry development. These recommendations aim to address current limitations and exploit the full potential of blockchain technology in revolutionizing mobile commerce security and trust.

8 REFERENCES

[1] S. E. Vadakkethil Somanathan Pillai and P. Pawar, "Blockchain technology for enhancing trust and security in mobile networks," in *Proceedings of the 2nd IEEE International Conference on Networking and Communications*, 2024, pp. 1–6. https://doi.org/10.1109/ICNWC60771.2024.10537290

[2] S. Sarker, M. Ahuja, S. Sarker, and K. M. Bullock, "Mobile technologies and work–life conflict," in *Navigating Work and Life Boundaries*, 2021, pp. 117–142. https://doi.org/10.1007/978-3-030-72759-8_5

[3] K. K. Stephens, "Mobile work, mobility, and mobile devices: Responding to a societal shift," *Mobile Media & Communication*, vol. 11, no. 1, pp. 118–124, 2023. https://doi.org/10.1177/20501579221126956

[4] L. Xia, D. T. Semirumi, and R. Rezaei, "A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy," *Sustain. Cities. Soc.*, vol. 98, p. 104771, 2023. https://doi.org/10.1016/j.scs.2023.104771

[5] O. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023. https://doi.org/10.3390/electronics12061333

[6] M. Tornatore *et al.*, "A survey on network resiliency methodologies against weather-based disruptions," in *Proceedings of 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, 2016, pp. 23–34. https://doi.org/10.1109/RNDM.2016.7608264

[7] A. Thakur, "A comprehensive study of the trends and analysis of distributed ledger technology and blockchain technology in the healthcare industry," *Frontiers in Blockchain*, vol. 5, 2022. https://doi.org/10.3389/fbloc.2022.844834

[8] H. S. Musa, M. Krichen, A. A. Altun, and M. Ammi, "Survey on blockchain-based data storage security for android mobile applications," *Sensors*, vol. 23, no. 21, p. 8749, 2023. https://doi.org/10.3390/s23218749

[9] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review," *Sensors*, vol. 23, no. 2, p. 788, 2023. https://doi.org/10.3390/s23020788

[10] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Future Internet*, vol. 14, no. 11, p. 341, 2022. https://doi.org/10.3390/fi14110341

[11] Z. Xiong, Y. Zhang, N. C. Luong, D. Niyato, P. Wang, and N. Guizani, "The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things," *IEEE Netw.*, vol. 34, no. 1, pp. 166–173, 2020. https://doi.org/10.1109/MNET.001.1900095

[12] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of Things: benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications*, vol. 10, no. 6, pp. 40–48, 2018. https://doi.org/10.5815/ijisa.2018.06.05

[13] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, and E. Bartocci, "A roadmap toward the resilient Internet of Things for cyber-physical systems," *IEEE Access*, vol. 7, pp. 13260–13283, 2019. https://doi.org/10.1109/ACCESS.2019.2891969

[14] A. Prakash, "Blockchain technology for supply chain management: Enhancing transparency and efficiency," *International Journal for Global Academic & Scientific Research*, vol. 3, no. 2, pp. 1–11, 2024. https://doi.org/10.55938/ijgasr.v3i2.73

[15] C. Gupta *et al.*, "A systematic review on machine learning and deep learning models for electronic information security in mobile networks," *Sensors*, vol. 22, no. 5, p. 2017, 2022. https://doi.org/10.3390/s22052017

[16] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects," *Journal of Network and Computer Applications*, vol. 163, p. 102635, 2020. https://doi.org/10.1016/j.jnca.2020.102635

[17] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K. K. Raymond Choo, "Blockchain-based identity management systems: A review," *Journal of Network and Computer Applications*, vol. 166, p. 102731, 2020. https://doi.org/10.1016/j.jnca.2020.102731

[18] M. Kang and V. L. Lemieux, "A decentralized identity-based blockchain solution for privacy-preserving licensing of individual-controlled data to prevent unauthorized secondary data usage," *Ledger*, vol. 6, 2021. https://doi.org/10.5195/ledger.2021.239

[19] A. A. El-Saleh, A. Alhammadi, I. Shayea, W. H. Hassan, M. S. Honnurvali, and Y. I. Daradkeh, "Measurement analysis and performance evaluation of mobile broadband cellular networks in a populated city," *Alexandria Engineering Journal*, vol. 66, pp. 927–946, 2023. https://doi.org/10.1016/j.aej.2022.10.052

[20] A. Dhar Dwivedi, R. Singh, K. Kaushik, R. Rao Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, p. e4329, 2021. https://doi.org/10.1002/ett.4329

[21] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and TPG, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PloS Med.*, vol. 6, no. 7, p. e1000097, 2009. https://doi.org/10.1371/journal.pmed.1000097

[22] N. Khan and M. I. Qureshi, "A systematic literature review on online medical services in Malaysia," *International Journal of Online and Biomedical Engineering*, vol. 16, no. 6, pp. 107–118, 2020. https://doi.org/10.3991/ijoe.v16i06.13573

[23] M. I. Qureshi and N. Khan, "Editorial: Business disruptions and innovations beyond COVID-19," *Foresight*, vol. 24, nos. 3–4, pp. 297–300, 2022. https://doi.org/10.1108/FS-06-2022-227

[24] N. E. Nomalisa and R. Widowati, "A bibliometric analysis using the VOS Viewer: Green marketing, repurchase intention, and correlations," *Multidisciplinary Reviews*, vol. 7, no. 6, p. 2024119, 2024. https://doi.org/10.31893/multirev.2024119

[25] E. Ducas and A. Wilner, "The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada," *International Journal*, vol. 72, no. 4, pp. 538–562, 2017. https://doi.org/10.1177/0020702017741909

[26] L. Xu *et al.*, "Supporting blockchain-based cryptocurrency mobile payment with smart devices," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 26–33, 2020. https://doi.org/10.1109/MCE.2019.2953734

[27] W. Chen, X. Qiu, Z. Cai, B. Tang, L. Du, and Z. Zheng, "Graph neural network-enhanced reinforcement learning for payment channel rebalancing," *IEEE Transactions on Mobile Computing*, vol. 23, no. 6, pp. 7066–7083, 2024. https://doi.org/10.1109/TMC.2023.3328473

[28] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity," *Information & Management*, vol. 59, no. 7, p. 103553, 2022. https://doi.org/10.1016/j.im.2021.103553

[29] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," *Business and Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021. https://doi.org/10.1007/s12599-021-00722-y

[30] S. Feulner, J. Sedlmeir, V. Schlatt, and N. Urbach, "Exploring the use of self-sovereign identity for event ticketing systems," *Electronic Markets*, vol. 32, no. 3, pp. 1759–1777, 2022. https://doi.org/10.1007/s12525-022-00573-9

[31] W. Dai, Q. Wang, Z. Wang, X. Lin, D. Zou, and H. Jin, "Trustzone-based secure lightweight wallet for hyperledger fabric," *J Parallel Distrib Comput*, vol. 149, pp. 66–75, 2021. https://doi.org/10.1016/j.jpdc.2020.11.001

[32] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," NISTIR 8202, U.S. Department of Commerce, 2019. https://doi.org/10.6028/NIST.IR.8202

[33] A. A. Gomaa, M. I. Gomaa, S. L. Boumediene, and M. S. Farag, "The creation of one truth: Single-ledger entries for multiple stakeholders using blockchain technology to address the reconciliation problem," *Journal of Emerging Technologies in Accounting*, vol. 20, no. 1, pp. 59–75, 2023. https://doi.org/10.2308/JETA-19-06-01-28

[34] F. E. Alzhrani, K. A. Saeedi, and L. Zhao, "A taxonomy for characterizing blockchain systems," *IEEE Access*, vol. 10, pp. 110568–110589, 2022. https://doi.org/10.1109/ACCESS.2022.3214837

[35] W. W. Lo, G. K. Kulatilleke, M. Sarhan, S. Layeghy, and M. Portmann, "Inspection-L: Self-supervised GNN node embeddings for money laundering detection in bitcoin," *Applied Intelligence*, vol. 53, pp. 19406–19417, 2023. https://doi.org/10.1007/s10489-023-04504-9

[36] A. A. Mohammed, A. Monem, S. Rahma, and H. B. Abdulwahab, "A comprehensive review of exploring the dynamic evolution of digital wallets and currencies in the face of challenges, innovation, and the future landscape from 2008 to 2023," *J Electrical Systems*, vol. 20, no. 4s, pp. 2194–2209, 2024. https://doi.org/10.52783/jes.2388

[37] R. S. Rasheed, K. H. A. Al-Shqeerat, A. S. Ghorab, F. S. AbuOwaimer, and A. A. AbuSamra, "Blockchain mobile wallet with secure offline transactions," *Computers, Materials & Continua*, vol. 75, no. 2, pp. 2905–2919, 2023. https://doi.org/10.32604/cmc.2023.036691

[38] I. S. Igboanusi, K. P. Dirgantoro, J. M. Lee, and D. S. Kim, "Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture," *ICT Express*, vol. 7, no. 3, pp. 327–334, 2021. https://doi.org/10.1016/j.icte.2021.08.004

[39] A. O. Y. Mohamed, "Intelligent blockchain-based secure framework for transaction in mobile electronic payment system," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 4, pp. 37–46, 2023. https://doi.org/10.3991/ijim.v17i04.37671

[40] E. Nowroozi, S. Seyedshoari, Y. Mekdad, E. Savaş, and M. Conti, "Cryptocurrency wallets: Assessment and security," *Advances in Information Security*, vol. 102, pp. 1–19, 2022. https://doi.org/10.1007/978-3-031-25506-9_1

[41] A. Xiang, H. Gao, Y. Tian, J. Xiong, L. Wang, and V. Peng, "H2CT: Asynchronous distributed key generation with high computational efficiency and threshold security in blockchain network," *IEEE Internet Things Journal*, vol. 11, no. 20, pp. 33758–33772, 2024. https://doi.org/10.1109/JIOT.2024.3431554

[42] C. Cao and X. Zhu, "Strong anonymous mobile payment against curious third-party provider," *Electronic Commerce Research*, vol. 19, pp. 501–520, 2019. https://doi.org/10.1007/s10660-018-9302-2

[43] Y. Li, T. Wareewanich, and T. Chankoson, "A study on influencing factors of willingness to use E-CNY based on logistic model," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 18, no. 4, pp. 112–23, 2024. https://doi.org/10.3991/ijim.v18i04.47117

[44] A. Hoess, J. Lautenschlager, J. Sedlmeir, G. Fridgen, V. Schlatt, and N. Urbach, "Toward seamless mobility-as-a-service: Providing multimodal mobility through digital wallets," *Business and Information Systems Engineering*, 2024. https://doi.org/10.1007/s12599-024-00856-9

[45] V. Kersic, U. Vidovic, A. Vrecko, M. Domajnko, and M. Turkanovic, "Orchestrating digital wallets for on- and off-chain decentralized identity management," *IEEE Access*, vol. 11, pp. 78135–78151, 2023. https://doi.org/10.1109/ACCESS.2023.3299047

[46] Y. Maleh, S. Lakkineni, L. Tawalbeh, and A. A. AbdEl-Latif, "Blockchain for cyber-physical systems: Challenges and applications," in *Advances in Blockchain Technology for Cyber Physical Systems. Internet of Things*, Y. Maleh, L. Tawalbeh, S. Motahhir, and A. S. Hafid, Eds., Springer, Cham, 2022, pp. 11–59. https://doi.org/10.1007/978-3-030-93646-4_2

[47] R. Chen, Y. D. Lee, and C. H. Wang, "Total quality management and sustainable competitive advantage: Serial mediation of transformational leadership and executive ability," *Total Quality Management & Business Excellence*, vol. 31, nos. 5–6, pp. 451–468, 2020. https://doi.org/10.1080/14783363.2018.1476132

9 AUTHORS

Vichayanan Rattanawiboonsom is with the Faculty of Business, Economics, and Communication, Naresuan University, Thaplo, Muang, Phitsanulok 65000, Thailand (E-mail: vichayananr@nu.ac.th).

Nohman Khan is with the Abbottabad University of Science & Technology (AUST), Abbottabad, khybe, Havelian Havelian, Abbottabad, 22500, Pakistan.