frontiers | Frontiers in Blockchain

TYPE Original Research
PUBLISHED 11 November 2025
DOI 10.3389/fbloc.2025.1657110

OPEN ACCESS

EDITED BY
Barkaoui Kamel,
Conservatoire National des Arts et Métiers (CNAM), France

REVIEWED BY
Ingrid Vasiliu Feltes,
University of Miami, United States
Hewa Majeed Zangana,
University of Duhok, Iraq

*CORRESPONDENCE
Ahmad Ali Eyadat,
eyadatahmad@gmail.com

RECEIVED 30 June 2025
REVISED 10 October 2025
ACCEPTED 20 October 2025
PUBLISHED 11 November 2025

CITATION
Ali Eyadat A, Alamaren AS and Almomani SL (2025) The influence of Blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks. *Front. Blockchain* 8:1657110. doi: 10.3389/fbloc.2025.1657110

The influence of Blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks

Ahmad Ali Eyadat [1]*, Amro S. Alamaren [2] and Siwar Lutfi Almomani [3]

[1]Department of Business Intelligence & Data Analytics, Faculty of Administrative and Financial Sciences, University of Petra, Amman, Jordan, [2]Department of Banking and Finance, School of Business, Al al-Bayt University, Mafraq, Jordan, [3]Department of Business Intelligence & Data Analytics, Faculty of Administrative and Financial Sciences, Irbid National University, Irbid, Jordan

This quantitative research investigates the influence of Blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks in Jordan. It aims to determine the extent to which Blockchain technology can reduce cyber risks faced by commercial banks in Jordan. A structured questionnaire consisting of 12 items was designed based on the research question about how Blockchain technology affects and contributes to cybersecurity to check the main objective of this study. This questionnaire has been handed out to respondents who are currently employed in Jordanian commercial banks. Here, stratified sampling was used to ensure that the data collected were representative of different segments of banks, providing a more accurate analysis of the views of the various members of the banking industry. The study used TAM to determine and check the scope of factors that influence the acceptance and adoption of Blockchain technology among banking professionals. Results have been positive, showing that Blockchain technology does cut or minimize the risk of cybersecurity on financial transactions in these institutions. The findings of this study thus warrant that Jordanian commercial banks should, with immediate effect, follow the integration of Blockchain solutions into their respective systems to enhance and ensure cybersecurity. Through this, the banks are able to protect their operations and encourage the clients to trust the digital banking sector.

KEYWORDS

blockchain, cybersecurity risks, financial transactions, banking sector, decentralization

1 Introduction

The financial sector has long been a constant subject concerning security challenges, with commercial banks being at the center of cyber-attacks due to the critical nature of transactions and consumer information. Concerns pointed out by Zheng et al. (2018) suggest that organizations' conventional security practices do not suffice to address advanced threats in this era of digital transformation. The rising offering of Blockchain technology can be done with the help of its intrinsic properties, which promise improved security through decentralization and immutability. It is against this background that this study investigates the impact of Blockchain technology on reducing the cybersecurity risks of financial transactions in commercial banks. It further extends an endeavor to provide

useful insights into the potential perception of the tool in transforming and improving transaction security concerning cybersecurity in the banking sector. Sanyaolu et al. (2024) state that awareness is essential for financial institutions to protect current operations and preserve trust from clients in the rapidly digitalizing world. Ammous (2016) defines Blockchain technology as a cutting-edge database mechanism for the transparent sharing of data in a business network. In a Blockchain database, data is stored in blocks and these are chained up. Since no party involved in the network can singly delete or alter a block in the chain, it establishes the time consistency of the data. Hence, with the use of Blockchain technology, either an immutable or alterable ledger can be made for tracking orders, payments, accounts, and other transactions.

Cybersecurity risk plays an important role in every institution. Al-Alawi and Al-Bassam (2020) believe that it is the likelihood of an organization being exposed to or affected by any form of loss resulting from a cyber-attack on it or a breach of data within it. A better and more comprehensive definition is the potential loss or damage involving the technical infrastructure and usage of technology concerning an organization's reputation. Camillo (2017) asserts that with the growing reliance of entities globally on computers, networks, programs, social media, and data, organizations are highly exposed to cybersecurity threats. Kukman and Gričar, (2025) notes that blockchain technology has rapidly attracted global attention due to its potential to transform the banking ecosystem by improving security, transparency, and efficiency. Financial institutions around the world are adopting blockchain solutions to modernize transaction processes, reduce operational risks, and strengthen defenses against cyber threats. Among them, data breaches are one of the most frequent types of cyberattacks that have enormous adverse effects on businesses and are often associated with inadequate data security.

The role of enhancing the control of cybersecurity risks in financial transactions of Jordanian commercial banks is a clear responsibility given the increasing volume of digital services and the higher quality of cybercrime. According to Elsayed et al. (2024), breaches in cybersecurity can expose financial data to significant risks of losing integrity and confidentiality. Qasaimeh and Jaradeh (2022) affirm that cyber-attacks on financial institutions are bulging, with revelations showing that on an average day in Jordan, banks are hit by between five hundred to one thousand cyber-attacks. These incursions not only endanger sensitive customer information but also compromise the quality of financial accounting statements, which eventually result in losses including loss of finances and goodwill loss of trust from customers. The Central Bank of Jordan has formulated several guidelines and frameworks for improving cybersecurity governance within banks. However, the compliance level of banks with these guidelines ought not to be optional as it affects the renewal of operational licenses and imposition of fines. The Cybersecurity Framework developed by the Central Bank gives prominence to risk management, incident handling, and information sharing for the exploitation of the vulnerabilities of financial institutions. According to Tariq et al. (2024), trust forms the basis of banking relations. High cybersecurity measures relate to more trust by customers in terms of security when handling transactions.

Low cybersecurity results in customer churn, as customers can look for safer alternatives if they feel their financial information is at risk. Bajwa et al. (2023) state the fact that cyber incidents can cost banks a loss of money, legal responsibilities, and even higher operative charges for all the additional actions that are carried out to restore their regular operations. Banks can increase their ability to deal with investments in the security of bank information systems, which in turn increases the general financial stability of the banking sector. This can also be used as a competitive angle for the banks. Currently, they can secure their assets by deploying advanced technology and artificial intelligence to detect threats, making it attractive to customers who value the highest protection of their investments. Elsayed et al. (2024) note that a safe banking environment develops into economic growth due to the inflow of increased confidence by investors and a buoyant investment in the financial sector. As banks continue to enhance their posture toward cybersecurity, they unintentionally develop a safer environment that is inspired by economic activities for growth. The diminution of cybersecurity risks is important for sensitive data, as well as for complying with rules, maintaining the trust of customers, ensuring financial stability, attaining a competitive edge, and achieving general economic growth in the banking sector in Jordan. New cyber threats require new strategies for commercial banks to protect their undertakings and customer interests.

Several limitations are attached to the study. First, this could be a low sample size to adequately draw inferences since only a few banks in Jordan were considered. This, therefore, affects the level to which the results obtained can be generalized to all the other banks. Second, the pace of dynamism, especially in Blockchain technology and security threats, might quickly render the results irrelevant as well as outdated. The research has to be updated regularly to conform to these dynamisms in this field. Third, biases are possible in self-reported data, particularly on the differences in the level of Blockchain adoption by the banks that could cast doubt on the reliability and generality of the outcomes gleaned from the study.

The problem statement in this study is the major challenges facing financial transaction security by Jordanian banks against the increasing cyber threats. With digital banking services advancing at a breakneck pace traditional cybersecurity has been found wanting hence vulnerabilities that compromise very crucial customer data alongside financial assets to cyber-attacks. The study is expected to research how Blockchain technology can improve security measures, decrease risks, and increase trust in financial transactions. Therefore, it also makes a case for examination of the interaction between Blockchain adoption and the established frameworks of cybersecurity to minimize the risks efficaciously. By the end, the research plans to deliver useful insights that banking stakeholders can act upon in advancing their cybersecurity posture through novel technological means.

The main objective of this study is to assess whether Blockchain technology could be a remedy for enhancing cybersecurity in the banking sector. This paper thus seeks to establish whether indeed the decentralized and immutable nature of Blockchain can curtail the risk of cyber threats on data breaches and fraud, especially during financial transactions. It also identifies how Blockchain is going to enhance the security of transactions and how it protects critical financial information. The research question is: What is the impact of implementing Blockchain technology on reducing risks relating to cybersecurity in financial transactions by commercial banks? The

null hypothesis (H0) for this research question is: "The implementation of blockchain technology does not significantly reduce cybersecurity risks in commercial bank financial transactions."

2 Literature review

2.1 Theoretical framework

Through digital transformation, banking operations have become seamless with customer-centered services. According to George (2023), this might place the banks at bigger risks like cybersecurity and data breach threats. To march with the pace of technological advancement, at the same time, banks are being pressured to enhance their abilities to safeguard their systems from cyber-attacks. Now, the sector has advanced to the verge of critical development where innovation meets security in laying the future course. With financial institutions embracing technologies like Blockchain and cybersecurity, they are securing their operations as well as redefining customer experiences. A business executive is conscious that the value of a data breach is not just related to the financial results of the individual cyberattack, it might lead to many other things, such as logistical problems, court cases, loss of the company's public image, and angry clients. Al Khaldy et al. (2025) note that their study examines the application of artificial intelligence in financial risk, discusses deployment challenges, and highlights future directions, including explainable AI and federated learning. Aldweesh et al. (2023) state that their analysis focused on technical aspects, such as the implementation of blockchain in virtual worlds and the design of virtual economies.

The banking sector has significant implications for Blockchain technology. According to Abbas and David (2024), Blockchain technology, the decentralized ledger underpinning cryptocurrencies such as Bitcoin, is fast turning out to be a significant game-changer for the banking sector. The ability of Blockchain to create secure, transparent, and tamper-proof records of transactions makes it well-suited for financial transactions. With the use of Blockchain, banks are able to ramp up their securities, minimize fraud, and simplify their processes. The greatest benefit of Blockchain is in making secure and cheap cross-border payments; in most traditional banking systems, these are intermediaries, thus with delays and increased costs. But with Blockchain, banks can set up a single and secure network for any cross-border payment remittance, which works in no time and cheaply.

The Blockchain can improve cybersecurity in the banking sector. Farayola (2024) asserts that the banking sector is perennially under siege by new and sophisticated cyber threats. While retail banking arms are rolling out Blockchain frameworks to secure personal information, the jury is still out on the rules and regulations that need to be put in place for Blockchain technology. Smith and Dhillon (2020) denote that the fusion of Blockchain and cybersecurity is that force that shall change the future of banking. If banks can implement this advanced cybersecurity protocol in their banking system along with the technology of Blockchain, then a very secure and productive banking ecosystem can be created. It helps in upscaling security measures for the banks, process optimization as well as customer experience. Choithani et al. (2024) indicate that as an infrastructure technology, the decentralized architecture of Blockchain enhances cyber resilience, supported by several varied processes of consensus. No sensitive data could be accessed through a single point of vulnerability or failure. Sensitive data need multi-level validation. In addition to the other benefits, cloud-based Blockchains come up with additional security.

In the other fields, Blockchain oversees the ability of the customer to manage, by switching on a digital fingerprint, a single test so that there can not be duplication between AML and KYC checks. It also decentralizes financial transactions and this further facilitates the worldwide integration of the different ecosystems in the monetary world. Assert that the impact of Blockchain technology in the modern banking sector to exterminate the financial scams. Sukkur IBA Journal of Computing and Mathematical Sciences, 6 (2), 27–38. Blockchain systems are decentralized, permitting end-user devices and IoT systems to make their security decisions. This is a plus for banking, in the sense that end-user security is typically a weakness for most banks. Weaknesses can include passwords, trivial logins, and weaknesses related to centralized IT infrastructure. All three point to weaknesses in terms of security. Multi-party verification under Blockchain thwarts cyberattacks nearly entirely because they are made almost impossible. Aragani et al. (2024) denote that some problems, like DNS and DDoS attacks, can both be managed with Blockchain technology. It can isolate even a single node that is under attack by setting up a zero-trust network. Therefore, the rest of the system can continue working as usual.

A suitable theory for this study is the Technology Acceptance Model (TAM). It was developed by Davis et al. (1989). This model is very appropriate because it helps to understand how users come to accept and use new technologies, with a view centered on perceived ease of use and perceived usefulness. The emergence of TAM was to offer considerations on the efficiency of Jordanian commercial banks concerning technological adoption by using a developed research model. On the other hand, if the banks have favorable attitudes towards the ability of Blockchain solutions to mitigate risks relating to financial transactions, then TAM can be applied to assess the influencing factors of the banks in taking up the innovation. According to Almuhairat et al. (2025), by providing a decentralized, transparent, and tamper-proof ledger, blockchain technology significantly improves the security of commercial bank financial transactions and reduces the potential for cyberattacks and fraud. The implementation of blockchain technology enhances the integrity and trust of transactions, thereby reducing cybersecurity risks in the banking industry.

2.2 Empirical studies

The following empirical studies aim to clarify the influence of Blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks. Ahakonye et al. (2024) conducted a study about tides in Blockchain in IoT Cybersecurity for Tides. This paper reviews Blockchain technology with intrusion detection systems to enhance their performance in detection. It looks into the incorporation of Blockchain technology into securing Internet of

Things (IoT) networks and proposes an extended framework that integrates Blockchain technology with Intrusion Detection Systems (IDS) to enhance IDS performance. It scrapes articles from AI, Blockchain, IDS, IoT, and Industrial IoT (IIoT) topics to present emerging trends and challenges in this field. From the analysis, various approaches to integrating AI and Blockchain prove the possibilities of integrating AI with Blockchain to change IDS. This study presents a systematic illustration used for deep assessment. The design concepts, and the Meta-Analysis (PRISMA), inspired the reviewing methodologies creatively within this work. The structure of this paper builds and develops the base for further research and also a model for the development of IDS to be accessible, scalable, transparent, immutable, and decentralized. Evidence from case studies on AI and Blockchain. Integrating shows the practicability of deploying both. The results of this study showed that, even despite resource-constraint challenges and concerns of privacy, Blockchain secures IoT networks and continues to need further innovation in the area. There is a need, therefore, for more lightweight cryptography research, efficient consensus mechanisms, and privacy-preserving techniques to unlock all the potential that Blockchain-powered cybersecurity in IoT can offer.

Prakash et al. (2022) carried out a study about Blockchain technology for cybersecurity: A text mining literature analysis. In Information Sciences 2021, Blockchain is the infrastructural technology underlying the famous digital currency Bitcoin. This can lift trust away from centralized organizations to decentralized ones with the veracity resting on some well-established mathematical basis and with the whole infrastructure being implemented through some sort of cryptographic security. It is growing at an ever-expanding pace and disrupts the way businesses function far beyond the mere aspects of digital currency. This paper presents a text-mining literature analysis of the research.

Articles are published in major digital libraries on Blockchain technology and cybersecurity. This work uses a semi-automatic literature and vulnerability analysis approach. This literature analysis employs automated text mining approaches such as topic modeling and keyphrase extraction for unearthing the themes from a vast body of literature. This analysis highlights the multidisciplinary nature of Blockchain technology within the cybersecurity domain. The findings also show the cyber threats and vulnerabilities. They show the vulnerabilities in the research community of computer security and also throws light on the future dimensions of research which is very important to design secure applications and platforms for the evolving Blockchain technology.

Moosavi and Taherdoost (2023) conducted a study on the applications of Blockchain technology in security. This is a relatively new but very popular technology among researchers. Originally introduced with digital currencies and particularly Bitcoin, as an emanation of the latter, nowadays it is used in many other areas as well. It is considered one of the most common approaches for securing networks. This research work identifies the previous works that have used Blockchain to address their security challenges. Moreover, the different aspects are examined regarding Blockchain usage, types of Blockchain categorization, consensus mechanism, smart contract usage, and integration with other software-based algorithms. Our findings support that Blockchain secures the most applications in Internet-of-Things (IoT) environments.

Rahmat et al. (2023). An exploration of using the technology of Blockchain in Cybersecurity and Data Science. Blockchain has proven to be highly effective in processing distributed transactions securely and includes many applications. B. Handling smart contacts and Bitcoin cash. Both aspects can include increased effectiveness and cost reduction because Blockchain systems enable the automatization of data exchange and thinking. This can be achieved by using contract technology as an examples of what to avoid decentralized ledgers. More than this, Blockchain technologies can boost data integrity and security, bringing greater accuracy and reliability to data analysis. Ethereum together with data science integration might simplify decentralized app creation and open new industries and income sources However, an issue of flexibility, interconnection, and complexity in the combination of Blockchain technology and data science is unsolved. To realize all its possible benefits, studies and developments in this field must endure. Blockchain applications for data science are under exploration. The paper discusses the ways of using Blockchain technology in cybersecurity and data science.

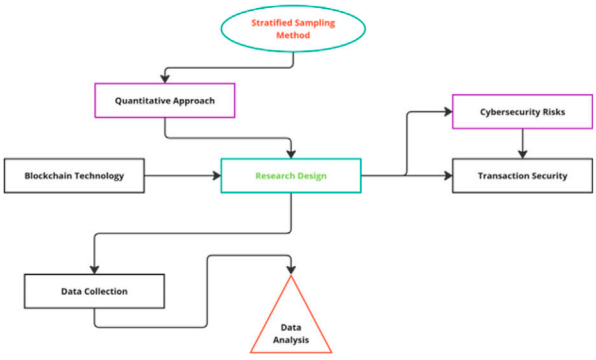
Saleh et al. (2023) carried out a study about Blockchain for Cybersecurity: A SWOT Analysis Study. In recent years, Blockchain technology has garnered an overabundance of the limelight due to its capability of being a revolutionist in manifold industries, among which is cybersecurity. While there is quite a significant volume of research in this field, there remains a requirement that is vividly put forth by the query: 'What are the possible advantages and disadvantages of implementing Blockchain technology into the already existing authentication and authorization mechanisms in cybersecurity?'. With that, the paper seeks to identify the potential and challenges of Blockchain utilization to enhance cybersecurity. The following paper gives an overview of what Blockchain technology is, as well as its principles of decentralization, immutability, and cryptographic security. How those can improve cybersecurity in creating transparent and tamper-resistant systems. The study also explores some potential uses of Blockchain technology in identity management, secure storage of data, and decentralized authentication in cybersecurity. More single points of failure in cybersecurity. The article not only discusses the promises but also the challenges and limitations of Blockchain implementation in cybersecurity. Among the major challenges that have to be overcome to make it workable integration are scalability, performance, energy consumption, and regulatory concerns. To conclude, it was a research article that provided a balanced perspective on the ability of Blockchain to be used in cybersecurity. This report strongly asserts the challenges that incredibly still need to be surmounted to make the very most of this new emergence.

Consequently, the empirical studies above provide some understanding of the transformation capacity of Blockchain within the banking industry. The studies primarily indicate that Blockchain can improve the level of security by employing decentralized and transparent means of processing transactions; this can reduce risks emanating from cyber threats and fraud. Besides, according to the Central Bank of Jordan, robust cybersecurity frameworks must accompany the implementation of Blockchain technology to create a safe financial sector where the confidence and efficiency of digital transactions are enhanced.

3 Research methodology

It includes research design, research tool, data collection, and data analysis. Thus, this study aims to the influence of Blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks in Jordan. The methodology in this study is performed using the quantitative approach. Kas et al. (2019) argued that the quantitative approach is more objective and of a deductive nature, generalizing results numerically. This is the type of methodology concerning the data or information used in the study. How is information collected to learn a specific thing, using any calculations, statistical, or mathematical techniques? Quantitative methodologies are techniques whereby mathematics is applied in the analysis of data by the use of numbers collected by researchers to answer their research questions (Warfield, 2010). This is further seen in the section on research methodology, where a lot of focus is usually on measurements and quantitative analyses. Most of the hypotheses and the bulk of the theories are tested thereby. Stress is also laid on the collection of information where numerical values are derivable, the type of statistics used in the examination of values for patterns and relationships (Long, 2014).

This study includes an independent variable (Blockchain Technology) and two dependent variables (Cybersecurity Risks and Transaction Security). Below is a diagram illustrating the research design:



The population of this study consists of all managers and administrators who are currently working in Jordanian commercial banks. The sample consists of 72 participants who are chosen according to the stratified sampling method. This study employed stratified sampling based on factors such as bank size, transaction type, and bank manager responsibilities to ensure a diverse representation of Jordanian commercial banks. Stratified sampling typically considers factors such as the number of branches, bank type (e.g., commercial, Islamic), and regional distribution. Participants from approximately 13–16 commercial banks in Jordan participated in this study, representing the total number of active commercial banks in Jordan. This stratified sampling ensured that the sample reflected the differences in managerial perspectives across banks and bank functions, allowing the findings to be generalized to a broader population of bank managers in Jordan. The sample size selected for the study is adequate to ensure statistical validity and reliability. Employing this method ensures some representation across types of commercial banks. Thus stratification helps capture diverse perspectives on the impacts of Blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks. After developing and validating the scale, it was administered to the sample by filling on a social media platform, especially WhatsApp, and e-mails. Then the data collected was analyzed using the software program SPSS. It needs several statistical tests such as The Mean, Standard Deviation, 2-tailed Significance Test, One-Sample T-Test, and others that are needed to answer the research question. After eliciting the results, an analysis was done to get the final results. A few recommendations are stated for conducting new research in the future.

3.1 Research tool

In the present study, the researcher built the questionnaire. A questionnaire of 12 items developed from this research question was judged by a set of associated professors and experts who have the same major (see Supplementary Appendix A at the end of this study). It focuses on the influence of Blockchain technology on reducing cybersecurity risks in financial transactions of commercial banks in Jordan. The questionnaire items for this research are filled by participants. Their responses are further discussed and analyzed statistically. Likert's five-point scale frames their responses as: agree, neutral, and disagree. Batterton and Hale (2017) in simple words, a Likert scale is a rating system used to measure opinions, attitudes, or behaviors. Normally, a statement is presented, followed by five response options.

4 Research results

The research question is: How does the implementation of Blockchain technology affect the reduction of cybersecurity risks in financial transactions conducted by commercial banks? Answering this question requires discussing, analyzing, and comparing the participants' responses to the 12 items of this questionnaire (See Supplementary Appendix A at the end of this study). The following table clarifies the participants' responses concerning the answers of the above research question. To investigate the participants' responses, a Descriptive Statistic Test is required to be conducted.

Table 1 shows that the average Mean of the 12 items (See Supplementary Appendix A at the end of this research) is 2.7039 with an average Standard Deviation (SD) of 0.5933. The Mean is considered high. Besides, the average percentage of the above 12 items is 78.6%. The average Range of these items is 2. According to the participants' responses, most people have been concerned that if adopted, Blockchain significantly improves the security of financial transactions in Jordanian commercial banks. The adoption of Blockchain technology can reduce the risk of cases of breach data for financial transactions taking place in banks. Since it is decentralized, Blockchain reduces the probability of a cyber-attack targeting the banking system. Security is more with smart contracts in Blockchain technology for financial transactions. Blockchain transparency raises the trust-escalation sensitivity for customers in all Jordanian banks. Implementation of Blockchain highly reduces fraudulent activities in financial transactions. There are regulatory compliance challenges that are slowing down the effectiveness of Blockchain in improving cybersecurity. The scalability of the technology is a rising issue for its adoption in all Jordanian banks. As a disruptive technology, the investment required for integrating

TABLE 1 Descriptive statistic test.

No. of items	No. of participants	The mean	Standard deviation (SD)	Frequency	Range
1	72	2.8750	0.40897	90.3%	2
2	72	2.7639	0.45943	77.5%	2
3	72	2.8194	0.48430	96.3%	2
4	72	2.8333	0.41111	77.9%	2
5	72	2.7500	0.46724	84.1%	2
6	72	2.7917	0.44207	80.8%	2
7	72	2.5694	0.64625	65.9%	2
8	72	2.6667	0.55665	70.1%	2
9	72	2.6528	0.63156	73.8%	2
10	72	2.6528	0.60885	72.5%	2
11	72	2.7222	0.58676	79.6%	2
12	72	2.7222	0.58676	73.8%	2

TABLE 2 One sample T-Test.

	No. of participants	T	Average mean	Average Std. devia-tion	Sig. (2-tailed)	Average percentage
Items: 1–12	72	21.448	2.7039	0.5933	0.000	78.6%
Total	72					

Blockchain technology is huge and is expected to act as a barrier to its implementation in small banks. Training of the staff about Blockchain technology make it more useful to reduce the risks of cyber security. Blockchain technology by itself is capable of eliminating all risks of cyber-attacks on commercial banks that exist in Jordan. Finally, continuous updates and improvements in Blockchain technology are good.

To conclude the last result of the research question, One Sample T-Test is necessary to be conducted. Table 2 clarifies this.

Since the average Mean is high (2.7039) and the Significance (2-Tailed) is 0.000, it means that implementing Blockchain technology reduces the cybersecurity risks in financial transactions conducted by Jordanian commercial banks. When Alpha is equal or less than 0.05%, it means that the influence is positive and significant (Alpha = Significance 2-Tailed).

5 Discussion

The result of this study positively denotes that Blockchain technology reduces cybersecurity risks in financial transactions of commercial banks in Jordan. It supports the study by Prakash et al. (2022), which proved that Blockchain ensures secure transactions in banking. This finding is very important because it shows that the implementation of Blockchain can make the general level of safety of financial operations better, thus addressing the very critical concerns that have been forming in the fast process of digitizing the financial position. Gangwar et al. (2025) note that quantum cryptography, which leverages the principles of quantum mechanics to create virtually unbreakable encryption, represents a significant breakthrough in the security of the banking ecosystem. Given the growing threat posed by cyberattacks, integrating quantum-resistant cryptography into existing blockchain frameworks can further secure financial transactions and better protect against future quantum attacks. The study implies that inherent characteristics in Blockchain, such as decentralization, immutability, and transparency contribute to minimizing risks associated with cyber threats in financial activities. It helps in fighting fraud and unauthorized access which in the end improves the whole security. This finding is supported by the study of Rahmat et al. (2023). They put into consideration their study about the role of Blockchain in managing efficiency and cost reduction in the banking sector of Jordan highlighting that better traceability and integrity of data could substantially reduce operational risks, including the risk of cybersecurity.

The study by Tariq et al. (2024) highlights the fact that Jordanian banks are relatively slow in adopting Blockchain technology. High operational costs and the need for a better more comprehensive regulatory framework are some of the many factors that are posing as impediments to effective implementation46. Thus, the use of Blockchain can only be successful in reducing cybersecurity risks if such an enormous host of challenges is surmounted by integrating it with the existing systems. The findings of this paper are supported by that of Sanyaolu et al. (2024), which suggest Blockchain's potential to mitigate cybersecurity risk in the banking sector of Jordan. However, it also means much more future research and development to surmount the challenges that come along with implementing it.

The Technology Acceptance Model (TAM) fits with the research findings because of the ease with which bank employees and the systems can adopt and apply Blockchain for the security of transactions. An individual perception that the use of a particular system supports an enhancement of job performance. For example, how many bank personnel believe that Blockchain can effectively reduce cybersecurity risks to enhance the security of financial transactions? This finding implicitly reflects the Perceived Usefulness (PU) of the TAM. When bank employees and management perceive that Blockchain technology reduce cybersecurity risks (which is proved by the research), they accept and use the technology. The Jordanian commercial banks could thus make a comprehensive assessment of the applicability of Blockchain technology to their specific circumstances to improve cybersecurity in light of "Perceived Usefulness," "Perceived Ease of Use," and external factors.

6 Conclusion

The study is carried out to examine the influence of Blockchain technology in reducing cybersecurity risks in financial transactions among Jordanian commercial banks. The respondents were issued with questionnaires, which had 12 items, and they were currently working in commercial banks. A stratified sampling method was used in data collection for this study. This study was based on the framework provided by the Technology Acceptance Model (TAM). The findings showed that Blockchain technology significantly reduces cybersecurity risks associated with financial transactions in commercial banks in Jordan.

6.1 Recommendations

The study suggests that banks should continue collaborating with technology companies to ensure the effective exploitation of the capabilities that Blockchain harbors. With the changing trends in the financial sector, Jordanian banks must adopt new technologies, such as Blockchain, to protect their activities and gain the trust of the customers. The study should be followed by another research that develops both theoretical and practical frameworks for the effective implementation of Blockchain solutions, taking into account both regulatory and operational issues. This work finally adds to the emergent understanding of the place of Blockchain in the cybersecurity of financial movements, with clear import for those in policy and banking in Jordan and further afield.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics statement

The studies involving humans were approved by The study was approved by the Institutional Review Board of the Faculty of Administrative and Financial Sciences, Irbid National University, Jordan. The studies were conducted in accordance with the local legislation and institutional requirements. The participants provided their written informed consent to participate in this study.

Author contributions

AE: Visualization, Validation, Data curation, Resources, Formal Analysis, Conceptualization, Project administration, Investigation, Writing – review and editing, Methodology, Software, Supervision, Writing – original draft. AA: Methodology, Formal Analysis, Validation, Data curation, Software, Writing – original draft, Resources, Writing – review and editing. SA: Writing – review and editing, Writing – original draft, Conceptualization, Resources, Validation, Methodology, Visualization, Investigation.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fbloc.2025.1657110/full#supplementary-material

References

Abbas, G., and David, J. (2024). Artificial intelligence and blockchain: a combined approach for predicting and preventing cyber attacks in financial institutions.

Ahakonye, L. A. C., Nwakanma, C. I., and Kim, D. S. (2024). Tides of blockchain in IoT cybersecurity. *Sensors* 24 (10), 3111. doi:10.3390/s24103111

Al Khaldy, M., Al-Qerem, A., Aldweesh, A., Alkasassbeh, M., Almomani, A., and Alauthman, M. (2025). Artificial intelligence for financial risk management and analysis. *Artif. Intell. Financial Risk Manag. Analysis*, 499–524. doi:10.4018/979-8-3373-1200-2.ch024

Al-Alawi, A. I., and Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *J. Xidian Univ.* 14 (7), 1523–1536. doi:10.37896/jxu14.7/174

Aldweesh, A., Alauthman, M., Al Khaldy, M., Ishtaiwi, A., Al-Qerem, A., Almoman, A., et al. (2023). The meta-fusion: a cloud-integrated study on blockchain technology enabling secure and efficient virtual worlds. *Int. J. Cloud Appl. Comput. (IJCAC)* 13 (1), 1–24. doi:10.4018/IJCAC.331752

Almuhairat, A., Alti, A., and Annane, B. (2025). Unified central bank blockchain for improving accounting bank performance in Jordan. *Secur. Priv.* 8 (2), e70022. doi:10.1002/spy2.70022

Ammous, S. (2016). Blockchain technology: what is it good for?

Aragani, V. M., Maroju, P. K., and Raju, L. N. (2024). Enhancing cybersecurity in banking: best practices and solutions for securing the digital supply chain. *J. Comput. Analysis Appl.* 33 (8). Available online at: https://eudoxuspress.com/index.php/pub/article/view/1515.

Bajwa, I. A., Ahmad, S., Mahmud, M., and Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. *Inf. & Comput. Secur.* 31 (5), 635–654. doi:10.1108/ics-11-2022-0179

Batterton, K. A., and Hale, K. N. (2017). The likert scale what it is and how to use it. *Phalanx* 50 (2), 32–39. Available online at: https://www.jstor.org/stable/26296382.

Camillo, M. (2017). Cybersecurity: risks and management of risks for global banks and financial institutions. *J. Risk Manag. Financial Institutions* 10 (2), 196–200. doi:10.69554/epyv4777

Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., and Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. *Ann. Data Sci.* 11 (1), 103–135. doi:10.1007/s40745-022-00433-5

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1989). Technology acceptance model. *J. Manag. Sci.* 35 (8), 982–1003. doi:10.1287/mnsc.35.8.982

Elsayed, D. H., Ismail, T. H., and Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region. *Future Bus. J.* 10 (1), 115. doi:10.1186/s43093-024-00402-9

Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Account. Res. J.* 6 (4), 501–514. doi:10.51594/farj.v6i4.990

Gangwar, M., Mantri, S., and Sarkar, A. (2025). Quantum-resilient banking: strategies for a secure transition.

George, A. S. (2023). Securing the future of finance: how AI, blockchain, and machine learning safeguard emerging neobank technology against evolving cyber threats. *Partners Univers. Innovative Res. Publ.* 1 (1), 54–66.

Kas, M. J., Penninx, B., Sommer, B., Serretti, A., Arango, C., and Marston, H. (2019). A quantitative approach to neuropsychiatry: the why and the how. *Neurosci. & Bio-Behavioral Rev.* 97, 3–9. doi:10.1016/j.neubiorev.2017.12.008

Kukman, T., and Gričar, S. (2025). Blockchain for quality: advancing security, efficiency, and transparency in financial systems. *FinTech* 4 (1), 7. doi:10.3390/fintech4010007

Long, H. (2014). An empirical review of research methodologies and methods in creativity.

Moosavi, N., and Taherdoost, H. (2023). Blockchain technology application in security: a systematic review. *Blockchains* 1 (2), 58–72. doi:10.3390/blockchains1020005

Prakash, R., Anoop, V. S., and Asharaf, S. (2022). Blockchain technology for cybersecurity: a text mining literature analysis. *Int. J. Inf. Manag. Data Insights* 2 (2), 100112. doi:10.1016/j.jjimei.2022.100112

Qasaimeh, G. M., and Jaradeh, H. E. (2022). The impact of artificial intelligence on the effective applying of cyber governance in jordanian commercial banks. *Int. J. Technol. Innovation Manag. (IJTIM)* 2 (1). doi:10.54489/ijtim.v2i1.61

Rahmat, R., Abbas, M. S., Nordin, M., Yunus, Y., Muhammad, S., and Ismail, A. F. (2023). "Exploring the use of blockchain technology in cybersecurity and data science," in *2023 3rd international conference on advance computing and innovative technologies in engineering (ICACITE)* (IEEE), 1094–1098.

Saleh, M. A., Amanzholova, S. T., Sagymbekova, A. O., Zaurbek, A., and Almisreb, A. A. (2023). "How can blockchain strengthen cybersecurity? Unravelling the promises and challenges," in *DTESI (workshops, short papers)*.

Sanyaolu, T. O., Adeleke, A. G., Azubuko, C. F., and Osundare, O. S. (2024). Harnessing blockchain technology in banking to enhance financial inclusion, security, and transaction efficiency. *Int. J. Sch. Res. Sci. Technol. August* 5 (01), 035–053.

Smith, K. J., and Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. *Manag. Finance* 46 (6), 833–848. doi:10.1108/mf-06-2019-0314

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E., Alzboun, N., Al-Hawary, S., et al. (2024). How cybersecurity influences fraud prevention: an empirical study on Jordanian commercial banks. *Int. J. Data Netw. Sci.* 8 (1), 69–76. doi:10.5267/j.ijdns.2023.10.016

Warfield, D. (2010). Is/It research: a research methodologies review. *J. Theoretical& Appl. Inf. Technol.* 13.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: a survey. *Int. J. Web Grid Serv.* 14 (4), 352–375. doi:10.1504/ijwgs.2018.095647