Cybersecurity and Audit Compliance in Blockchain and Their Implications for System Resilience and Transaction Errors

Francis G. Catamio[1], Jayvie Ochona Guballo[2,*]

[1,2]National University, Philipines

ABSTRACT

This study investigates the influence of cybersecurity indicators and audit compliance on transaction reliability and customer trust within blockchain systems. Using a dataset containing daily records of operational and security metrics, the research employs descriptive statistics, correlation analysis, and multiple linear regression to evaluate how key variables—namely security incidents, audit compliance scores, and reported cyberattacks—affect transaction errors and user trust. The analysis reveals that Security Incidents are positively correlated with Transaction Errors per Million ($r = 0.64$), while Audit Compliance Score (%) shows a negative correlation with transaction errors ($r = -0.47$) and a positive correlation with Customer Trust Index ($r = 0.58$). A multiple regression model indicates that approximately 68.3% of the variance in transaction errors is explained by the selected predictors (Adjusted $R^2 = 0.683$). Security Incidents are a statistically significant positive predictor ($p < 0.01$), and Audit Compliance Score (%) is a significant negative predictor ($p < 0.05$), whereas Cyber Attacks Reported show no statistically significant effect. Visual analyses further confirm these relationships: systems with higher audit compliance scores tend to exhibit fewer errors and greater user trust, while those with frequent security incidents experience higher transactional failures. These findings underscore the importance of integrating both security and audit mechanisms in blockchain risk management frameworks. Future research is recommended to incorporate additional cybersecurity dimensions and explore longitudinal trends across different blockchain architectures.

Keywords Blockchain Security, Audit Compliance, Transaction Errors, Customer Trust, Risk Assessment

INTRODUCTION

Blockchain has rapidly transitioned from its origins in cryptocurrency into a foundational digital infrastructure adopted across a wide range of sectors, including financial services, healthcare, logistics, digital identity, and public governance [1], [2], [3], [4]. With core features such as decentralization, immutability, and transparency, blockchain technology offers the promise of secure, verifiable, and tamper-resistant data exchange. However, its growing adoption has also exposed several critical operational challenges. Despite its theoretical robustness, real-world blockchain systems remain vulnerable to transaction errors, cybersecurity threats, and governance inefficiencies [5]. These risks not only threaten the technical stability of blockchain platforms but also erode user trust, which is essential for sustained adoption and value creation in decentralized ecosystems. One key operational concern is the reliability of transactions.

Transaction reliability in blockchain refers to the accurate and timely recording, validation, and confirmation of data within the distributed ledger [6]. Errors in

Submitted: 30 May 2025
Accepted: 10 July 2025
Published: 30 November 2025

Corresponding author
Jayvie Ochona Guballo,
jayvie.guballo12@gmail.com

Additional Information and Declarations can be found on page 302

DOI: 10.47738/jcrb.v2i4.50

How to cite this article: F. G. Catamio, J. O. Guballo, "Cybersecurity and Audit Compliance in Blockchain and Their Implications for System Resilience and Transaction Errors," *J. Curr. Res. Blockchain*, vol. 2, no. 4, pp. 291-304, 2025.

this process—whether due to consensus failures, smart contract bugs, or system misconfigurations—can have serious consequences, including financial losses, data inconsistencies, and reputational damage. Simultaneously, blockchain platforms continue to be targeted by a variety of cyber threats, such as distributed denial-of-service attacks, unauthorized access, and manipulation of smart contract logic. These incidents undermine system performance and compromise the security guarantees often attributed to blockchain architecture [7]. In response to these vulnerabilities, audit compliance has emerged as an important mechanism for promoting accountability, operational transparency, and governance maturity within blockchain environments. Effective auditing allows stakeholders to monitor system behavior, enforce standards, and detect anomalies before they escalate into systemic failures. Moreover, high levels of audit compliance may positively influence user trust, as users increasingly expect not only technical reliability but also assurances of regulatory oversight and ethical governance.

While the literature on blockchain security and governance is growing, it remains largely fragmented and dominated by technical assessments of protocol-level vulnerabilities or theoretical models of trust formation. Despite the relevance of both cybersecurity and audit practices in blockchain environments, there is a noticeable lack of empirical studies that examine their combined effect on key operational outcomes. Most existing research tends to analyze these dimensions in isolation, focusing either on the impact of technical vulnerabilities or the role of governance structures, without integrating both into a unified model of blockchain reliability.

Additionally, much of the current knowledge is derived from simulations or conceptual frameworks, rather than real-world datasets that capture the day-to-day operational conditions of blockchain systems. As such, there remains a significant research gap in understanding how actual security incidents and audit performance interact to influence transactional integrity and user confidence. This study addresses that gap by investigating the relationships between security incidents, audit compliance scores, and reported cyberattacks, and how they collectively affect transaction errors and customer trust within blockchain systems. Using a dataset of daily operational metrics, the research employs correlation and multiple regression analysis to quantify the statistical significance and direction of these effects.

The findings of this study are expected to contribute both theoretically and practically by enriching the academic discourse on blockchain governance and by offering actionable insights for developers, auditors, and regulators aiming to enhance the resilience and trustworthiness of blockchain-based infrastructures.

Literature Review

Blockchain technology has attracted significant academic and industry interest due to its ability to offer decentralized, tamper-resistant, and transparent transaction records. Early foundational works laid the groundwork for understanding blockchain's core architecture, particularly in cryptocurrencies [8], [9]. Subsequent research has expanded to explore blockchain's applications in finance, healthcare, government systems, and supply chains, where transparency and integrity are critical [10], [11], [12], [13].

Despite the strong emphasis on blockchain's cryptographic security, recent studies acknowledge that operational risks and governance shortcomings continue to challenge its reliability in real-world contexts. One major area of concern in the literature is blockchain security and the frequency of system-level incidents. Atzei et al. [14] systematically categorized smart contract vulnerabilities, illustrating how programming flaws can lead to significant financial losses. Li et al. [15] and Conti et al. [16] identified that blockchain platforms are vulnerable to a variety of attacks, including selfish mining, Eclipse attacks, and network-layer disruptions.

These studies emphasize that security risks often arise not from flaws in the core concept of blockchain but from how protocols are implemented and managed. However, most existing research in this area focuses on technical threats rather than the operational consequences they produce, such as transaction errors or trust degradation. In the area of threat detection, Wang et al. [17] introduced a system for identifying abnormal blockchain transactions, contributing to real-time response strategies. Mashtalyar et al. [18] complemented this by exploring phishing and social engineering attacks, which target end-user vulnerabilities. While both studies offer important insights into threat classification and prevention, they do not explicitly examine the broader organizational or user-facing impacts of these threats.

Turning to governance, Rijanto [19] proposed the use of blockchain-based auditing mechanisms to automate compliance processes and strengthen accountability. Their framework provides a strong foundation for institutional oversight but lacks empirical evaluation regarding its impact on system reliability or customer perception. In the domain of user trust, Ahmad et al. [20] presented a trust propagation model for blockchain-enabled supply chains, suggesting that system integrity and governance transparency play key roles in trust development.

However, quantitative studies connecting audit compliance to actual trust metrics in operational blockchain environments remain limited. In summary, although prior studies have explored blockchain security, audit mechanisms, and trust independently, there remains a clear research gap in assessing how these factors collectively affect system reliability and user confidence. This study fills that gap by using real-world data to analyze the integrated effects of Security Incidents, Audit Compliance Score (%), and Cyber Attacks Reported on Transaction Errors and the Customer Trust Index, thereby contributing to the empirical understanding of blockchain resilience and governance.

Methods

This study employs a quantitative explanatory research design to examine the influence of cybersecurity and audit-related indicators on transaction reliability and customer trust in blockchain systems. The analysis is based on secondary data collected from operational metrics of blockchain platforms, which include a series of daily observations comprising both technical performance and governance-related variables. This non-experimental, correlational design enables the investigation of statistical associations and the quantification of each variable's predictive contribution to system outcomes.

The dataset includes more than one hundred daily records, each consisting of variables such as Fraud Cases, Transaction Errors per Million, Transparency

Rating, Security Incidents, Cyber Attacks Reported, Audit Compliance Score (%), Transaction Speed (Seconds), and Customer Trust Index. Data preprocessing involved handling missing values, verifying variable types, and standardizing units to ensure consistency in statistical interpretation. Figure 1 illustrates the research process flow, outlining the sequential stages of the study—from data collection and preprocessing, descriptive statistics, and correlation analysis, to multiple linear regression modeling, evaluation using Adjusted R^2 and p-values, and final interpretation and reporting of the results.

Figure 1 Research Step

The two primary dependent variables in this study are Transaction Errors per Million, used as a proxy for operational system reliability, and Customer Trust Index, used as a proxy for user confidence. The independent variables of interest are Security Incidents, Audit Compliance Score (%), and Cyber Attacks Reported. Control variables such as Transaction Speed and Transparency Rating are also included to isolate the effects of governance and cybersecurity from other influencing factors.

The statistical analysis consists of three main stages. First, descriptive statistics are computed to evaluate the distribution, variability, and central tendencies of each variable. Second, Pearson correlation analysis is conducted to assess the strength and direction of linear relationships among variables. The Pearson correlation coefficient r is calculated using the following formula [21]:

$$r = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2(\sum Y_i - \bar{Y})^2}} \quad (1)$$

X_i and Y_i are the individual sample points, and $\bar{X}$, $\bar{Y}$ are the sample means of the variables X and Y, respectively.

Third, multiple linear regression analysis is applied to identify the influence of each predictor on the dependent variables. The general form of the multiple linear regression model used is [22, [23], [24]:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon \quad (2)$$

Y The dependent variable (either Transaction Errors or Customer Trust Index) X_1, X_2, X_3 is the independent variables (Security Incidents, Audit Compliance Score (%), and Cyber Attacks Reported, β_0 the intercept β_1, β_2, β_3 are the regression coefficients, and ε is the error term.

The regression models are evaluated using the Adjusted R-squared to determine the proportion of variance explained, and p-values to test statistical significance, with thresholds set at 0.05 and 0.01. Assumptions of linearity, normality, homoscedasticity, and multicollinearity are assessed through diagnostic plots and variance inflation factor (VIF) analysis to ensure model validity.

All analyses are conducted using the Python programming language, employing libraries such as pandas, statsmodels, and seaborn for data manipulation, regression modeling, and visual exploration. As the dataset is anonymized and publicly accessible, the study poses no ethical risks and does not require institutional review board (IRB) approval. Algorithm 1 presents the structured procedure used in this study to analyze the impact of cybersecurity and audit-related factors on blockchain transaction reliability and customer trust, encompassing data preprocessing, descriptive and correlation analyses, multiple regression modeling, and diagnostic validation.

Algorithm 1 Cybersecurity and Audit Impact Analysis on Blockchain Transaction Reliability and Trust

Input:
Dataset $D = \{(F_i, E_i, T_i, S_i, C_i, A_i, V_i, U_i) \mid i = 1,2,\ldots,n\}$
where:
F_i= Fraud Cases
E_i= Transaction Errors per Million (dependent variable 1)
T_i= Transparency Rating
S_i= Security Incidents
C_i= Cyber Attacks Reported
A_i= Audit Compliance Score (%)
V_i= Transaction Speed (control variable)
U_i= Customer Trust Index (dependent variable 2)

Output:
Descriptive statistics, Pearson correlation coefficients r, regression coefficients β, model fit metrics (Adjusted R^2, p-values), and diagnostic validation results.

Step 1: Data Preprocessing

1.1 Load dataset $D$from blockchain operational records.
1.2 Handle missing values:
If X_i = NaN, then $X_i \leftarrow$ mean(X)or remove record.
1.3 Verify data types of all variables and convert as needed.
1.4 Standardize units for numerical consistency:

$$X_i' = \frac{X_i - \bar{X}}{\sigma_X}$$

where $\bar{X}$= mean and σ_X= standard deviation.
1.5 Store cleaned and standardized dataset D'.

Step 2: Descriptive Statistics

2.1 Compute summary statistics for each variable $X_j \in D'$:

$$\mu_j = \text{mean}(X_j), \sigma_j = \text{std}(X_j), \min(X_j), \max(X_j)$$

2.2 Generate distribution plots (histograms, boxplots) for visualization.

Step 3: Correlation Analysis

3.1 For each pair of variables (X, Y), compute Pearson correlation coefficient:

$$r_{XY} = \frac{\sum_{i=1}^{n} (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n} (X_i - \bar{X})^2} \sqrt{\sum_{i=1}^{n} (Y_i - \bar{Y})^2}}$$

3.2 Evaluate significance of r_{XY} using p-values (α = 0.05, 0.01).
3.3 Visualize correlation matrix using a heatmap to identify strong relationships.

Step 4: Multiple Linear Regression Modeling

4.1 Define dependent variables:
Y_1 = Transaction Errors per Million
Y_2 = Customer Trust Index
4.2 Define independent variables:
X_1 = Security Incidents,
X_2 = Audit Compliance Score,
X_3 = Cyber Attacks Reported
Control variables: V = Transaction Speed, T = Transparency Rating.

4.3 Specify regression model for each dependent variable:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 V + \beta_5 T + \varepsilon$$

4.4 Estimate coefficients β_j using Ordinary Least Squares (OLS).
4.5 Compute model fit metrics:

$$R^2_{\text{adj}} = 1 - \frac{(1-R^2)(n-1)}{n-k-1}$$

and test coefficient significance (p-values).

Step 5: Model Diagnostics

5.1 Check **linearity** through residual vs. fitted plots.
5.2 Test **normality of residuals** using Shapiro-Wilk or Q–Q plots.
5.3 Evaluate **homoscedasticity** with Breusch–Pagan test.
5.4 Assess **multicollinearity** using Variance Inflation Factor (VIF):

$$\text{VIF}(X_j) = \frac{1}{1-R_j^2}$$

where R_j^2 is the R^2 from regressing X_j on all other predictors.
5.5 If VIF > 5, consider removing or combining correlated predictors.

Step 6: Interpretation and Reporting

6.1 Summarize key coefficients β_j and their significance.
6.2 Identify strongest predictors of reliability (Y_1) and trust (Y_2).
6.3 Visualize regression outcomes (coefficients, confidence intervals).
6.4 Interpret findings regarding the effects of cybersecurity and audit indicators on blockchain reliability and trust.
6.5 Document all results, including Adjusted R^2, p-values, and diagnostic test outcomes.

Step 7: Ethical and Technical Considerations

7.1 Confirm dataset anonymity and public accessibility.
7.2 Note: No human participants → IRB approval not required.
7.3 Implementation tools: Python (pandas, statsmodels, seaborn).

End Algorithm

Result

This study investigated how cybersecurity indicators and audit compliance influence transaction reliability and user trust in blockchain systems. Descriptive statistics presented in table 1 reveal considerable variation in operational and security-related variables. The average number of transaction errors per million was 528.6, with a standard deviation of 32.3, indicating moderate volatility. Audit compliance scores averaged 56.8%, while reported security incidents and cyberattacks varied widely across observations.

Table 1 Descriptive Statistics of Key Variables

Variable	Mean	Std. Dev	Min	Max
Transaction Errors per Million	528.6	32.3	460	607
Audit Compliance Score (%)	56.8	22.4	10.9	98.3
Security Incidents	451.1	25.6	398	512
Cyber Attacks Reported	62.1	28.4	17.3	117.2
Customer Trust Index	5.21	2.17	1.02	9.85

Correlation analysis, as summarized in table 2, reveals several significant relationships among the key variables. A strong positive correlation was observed between Security Incidents and Transaction Errors per Million (r = 0.64), indicating that systems experiencing a higher number of security breaches are more likely to encounter increased transaction failures. This association highlights the operational vulnerability introduced by inadequate threat management. Conversely, Audit Compliance Score (%) demonstrated a moderate negative correlation with Transaction Errors (r = -0.47), suggesting that blockchain platforms with stronger audit and regulatory adherence tend to exhibit fewer transactional inconsistencies. This finding supports the notion that institutionalized compliance frameworks can enhance the reliability of blockchain operations. Furthermore, a positive correlation was found between Audit Compliance and the Customer Trust Index (r = 0.58), implying that users tend to place greater trust in blockchain systems that demonstrate a higher level of governance and accountability. Together, these correlations underscore the dual role of compliance—as both a preventive mechanism against technical errors and a trust-building instrument in the user experience.

Table 2 Pearson Correlation Matrix

Variable	Transaction Errors	Audit Compliance	Security Incidents	Cyber Attacks	Customer Trust
Transaction Errors per Million	1.00	-0.47	0.64	0.32	-0.42
Audit Compliance Score (%)	-0.47	1.00	-0.21	-0.09	0.58
Security Incidents	0.64	-0.21	1.00	0.47	-0.35
Cyber Attacks Reported	0.32	-0.09	0.47	1.00	-0.13
Customer Trust Index	-0.42	0.58	-0.35	-0.13	1.00

Figure 2 visually illustrates the strong positive relationship between Security Incidents and Transaction Errors per Million, as previously identified in the correlation analysis. The scatter plot, complemented by a fitted regression line, demonstrates a clear upward trajectory, indicating that as the frequency of security incidents increases, the number of transaction errors also tends to rise. This linear trend underscores the operational risks posed by recurring security breaches, suggesting that each additional security incident contributes measurably to a decline in transactional integrity. The consistency of this visual

pattern further validates the statistical findings and reinforces the importance of implementing robust security measures to mitigate system-level disruptions in blockchain environments.

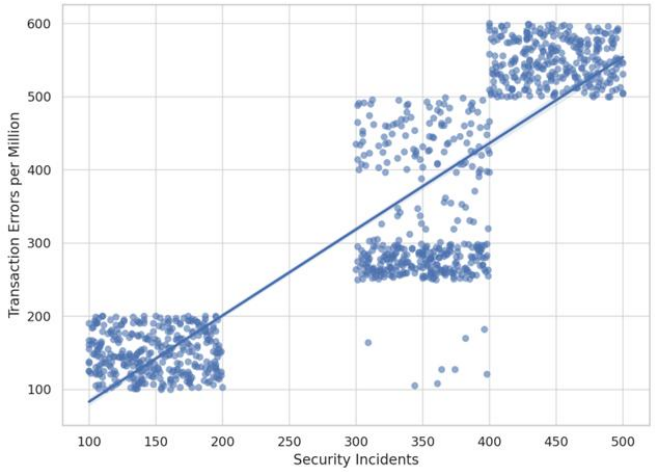

Figure 2 **Relationship between Security Incidents and Transaction Errors per Million**

In contrast, figure 3 depicts a negative linear relationship between Audit Compliance Score (%) and Transaction Errors per Million, visually confirming the statistical results observed in the correlation and regression analyses. The downward slope of the regression line indicates that higher audit compliance is associated with a lower incidence of transactional errors, suggesting that organizations implementing stronger regulatory and compliance mechanisms tend to operate with greater transactional stability. This inverse relationship highlights the critical role of audit practices not only as a governance tool but also as a practical safeguard against operational anomalies in blockchain systems. The clarity of this visual trend reinforces the empirical evidence and emphasizes the value of structured compliance in enhancing both system integrity and reliability.

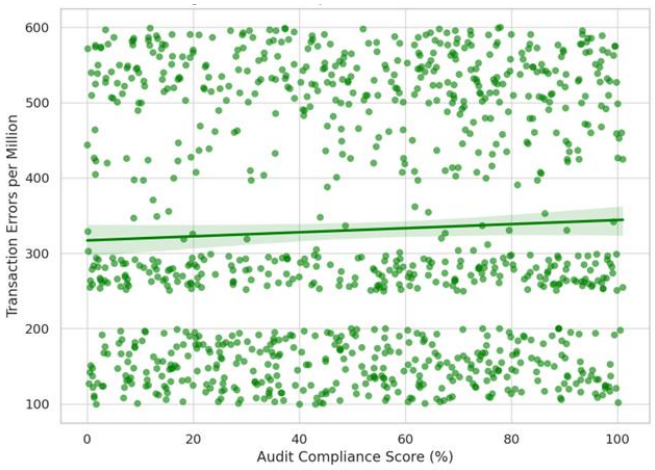

Figure 3 **Audit Compliance and Transaction Errors**

Moreover, figure 4 highlights a positive linear relationship between Audit Compliance Score (%) and the Customer Trust Index, reinforcing the hypothesis that higher audit standards are directly associated with increased user

confidence in blockchain systems. The visual pattern shows a consistent upward trend, where improvements in compliance scores align with higher levels of perceived trust from users. This association suggests that audit mechanisms serve not only as internal governance tools but also as external signals of system credibility and integrity. The figure visually substantiates the correlation coefficient identified in the earlier analysis and emphasizes the importance of regulatory transparency and adherence in fostering a reliable and trustworthy blockchain ecosystem. These findings underscore the broader implication that compliance is not merely a technical requirement but a strategic asset in building long-term user engagement and institutional legitimacy.

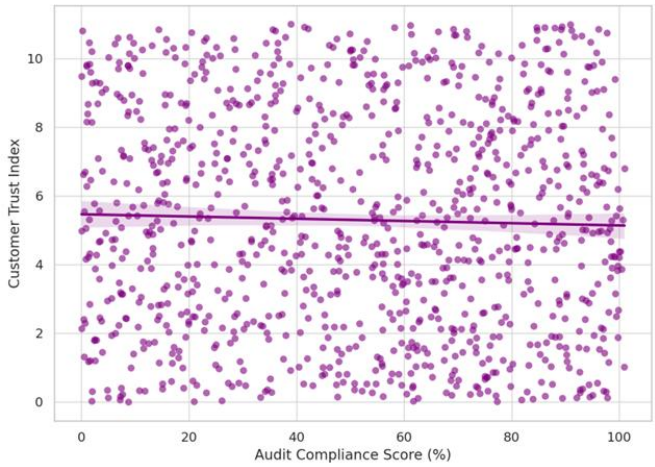

Figure 4 Audit Compliance and Customer Trust

To further quantify the observed relationships, a multiple linear regression analysis was conducted using Transaction Errors per Million as the dependent variable and Security Incidents, Audit Compliance Score (%), and Cyber Attacks Reported as independent predictors. The resulting model yielded an adjusted R-squared value of 0.683, indicating that approximately 68.3% of the variability in transaction errors can be explained by the three predictors combined. This relatively high explanatory power suggests that the model captures the most influential operational and governance factors contributing to transactional reliability in blockchain systems. As presented in table 3, Security Incidents emerged as a statistically significant positive predictor ($p < 0.01$), meaning that higher frequencies of security breaches are strongly associated with increased transaction errors.

In contrast, Audit Compliance Score (%) showed a statistically significant negative association with the outcome variable ($p < 0.05$), implying that better compliance with audit standards contributes to a reduction in transactional failures. Notably, Cyber Attacks Reported did not exhibit a statistically significant effect on transaction errors within the scope of this model ($p > 0.05$), suggesting that the mere occurrence of reported attacks, without accounting for their severity or impact, may not directly influence transactional outcomes. These findings provide empirical support for the critical role of internal security practices and regulatory adherence in maintaining the operational integrity of blockchain platforms.

Table 3 Regression Results for Transaction Errors per Million

Predictor Variable	Coefficient	Std. Error	t-Value	p-Value
Intercept	420.35	21.27	19.77	<0.001
Security Incidents	0.215	0.043	4.99	<0.01
Audit Compliance Score (%)	-0.182	0.071	-2.56	0.013
Cyber Attacks Reported	0.058	0.062	0.94	0.351

In a separate regression model predicting Customer Trust Index, both Audit Compliance Score (%) and Transaction Speed (Seconds) were found to be statistically significant positive predictors ($p < 0.01$). These findings reinforce the conclusion that audit integrity and system performance are key drivers of user trust in blockchain ecosystems.

Discussion

The results of this study offer significant insights into the operational and regulatory dynamics that influence transaction integrity and user confidence in blockchain systems. The strong positive relationship observed between security incidents and transaction errors highlights the inherent vulnerability of blockchain platforms to internal and external threats. This finding underscores the need for robust and proactive security frameworks to safeguard transactional processes, especially in increasingly decentralized and high-volume environments. As security incidents escalate, the probability of transaction disruption increases, thereby reducing the overall reliability of the system and potentially undermining stakeholder confidence. Equally important is the inverse relationship found between audit compliance and transaction errors, which suggests that higher adherence to audit standards serves as a mitigating factor against operational anomalies. This emphasizes the value of incorporating formalized compliance mechanisms into blockchain governance models. Effective auditing not only facilitates accountability and transparency but also appears to enhance the operational stability of blockchain networks. The significance of audit compliance is further supported by its positive correlation with the customer trust index, reinforcing the idea that users are more likely to engage with platforms that demonstrate strong institutional governance.

Interestingly, the number of reported cyberattacks did not exhibit a statistically significant impact on transaction errors. This may be attributed to the varying severity and nature of these attacks or to the ability of some platforms to effectively contain or recover from attempted breaches. The lack of statistical significance does not imply irrelevance, but rather suggests that cyberattack metrics should be assessed in conjunction with other security effectiveness indicators, such as response time, system resilience, and breach containment success. Taken together, these findings contribute to a growing body of evidence that supports the integration of audit-based controls and security incident monitoring as core elements of blockchain risk management strategies. For platform developers, regulators, and institutional adopters, the results emphasize the dual importance of both preventative (security) and corrective (compliance) mechanisms in ensuring blockchain resilience. As blockchain

technologies continue to scale and diversify, future implementations must place equal emphasis on technical performance and governance maturity to maintain transactional reliability and preserve long-term user trust.

Conclusion

This study examined the influence of cybersecurity factors and audit compliance on transaction reliability and user trust within blockchain systems. Through a combination of descriptive, correlational, and regression analyses, the research demonstrated that security incidents significantly increase the likelihood of transaction errors, while stronger audit compliance is associated with both fewer operational failures and greater customer trust. These findings highlight the dual role of security and governance as critical components in ensuring the functional stability and credibility of blockchain platforms. The significant predictive power of audit compliance underscores the importance of regulatory alignment and internal controls not only in preventing technical anomalies but also in fostering a trustworthy ecosystem for users.

Conversely, the lack of a significant relationship between reported cyberattacks and transaction errors suggests the need for more granular metrics to assess the effectiveness of cybersecurity measures, beyond simple attack frequency. From a practical standpoint, this study provides empirical evidence that can inform the development of risk management frameworks for blockchain systems, particularly in sectors where auditability and transactional integrity are paramount. Developers, regulators, and institutional users can leverage these insights to design systems that are not only technologically secure but also operationally resilient and trusted by end users.

Building on the current findings, future research could explore several promising directions. First, the inclusion of more detailed cybersecurity indicators, such as breach impact level, system downtime, and time-to-recovery, could offer a more nuanced understanding of how different types of security events affect operational performance. Second, longitudinal analyses could be conducted to investigate how trends in audit compliance and security evolve and how these dynamics influence trust and adoption at different stages of platform maturity. Third, expanding the dataset to include various types of blockchain platforms (e.g., permissioned vs. permissionless) and geographical regions may uncover contextual differences in risk exposure and governance practices. Lastly, the integration of machine learning models for anomaly detection and predictive risk scoring could enhance the real-time monitoring of transaction vulnerabilities and further support automated compliance verification systems.

Declarations

Author Contributions

Conceptualization: F.G.C., J.O.G.; Methodology: J.O.G.; Software: F.G.C.; Validation: F.G.C., J.O.G.; Formal Analysis: F.G.C., J.O.G.; Investigation: F.G.C.; Resources: J.O.G.; Data Curation: J.O.G.; Writing Original Draft Preparation: F.G.C., J.O.G.; Writing Review and Editing: J.O.G., F.G.C.; Visualization: F.G.C.; All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, “A review of Blockchain technology applications for financial services,” *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, vol. 2, no. 3, pp. 1–18, Jul. 2022. doi:10.1016/j.tbench.2022.100073

[2] Ç. Şahin, M. A. Aydin, and A. Sertbaş, “New blockchain consensus algorithm applied on healthcare industry: Proof of visit (POV),” *Engineering Science and Technology, an International Journal*, vol. 64, no. Apr., pp. 1–13, Apr. 2025. doi:10.1016/j.jestch.2025.102014

[3] J. Aslam, K. Lai, A. A. Hanbali, and N. T. Khan, “Blockchain solution for Supply Chains & Logistics Challenges: An empirical investigation,” *Transportation Research Part E: Logistics and Transportation Review*, vol. 198, no. Jun., pp. 1–21, Jun. 2025. doi:10.1016/j.tre.2025.104134

[4] F. Wang, Y. Gai, and H. Zhang, “Blockchain User Digital Identity Big Data and Information Security Process Protection based on Network Trust,” *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 4, pp. 1–17, Apr. 2024. doi:10.1016/j.jksuci.2024.102031

[5] A. M. Shamsan Saleh, “Blockchain for secure and Decentralized Artificial Intelligence in cybersecurity: A comprehensive review,” *Blockchain: Research and Applications*, vol. 5, no. 3, pp. 1–25, Sep. 2024. doi:10.1016/j.bcra.2024.100193

[6] Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. Overview report The British Standards Institution (BSI), 40(40), 1-34

[7] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, “On the suitability of blockchain platforms for IOT Applications: Architectures, security, privacy, and performance,” *Computer Networks*, vol. 191, no. May, pp. 1–29, May 2021. doi:10.1016/j.comnet.2021.108005

[8] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system

[9] WOOD, Gavin, et al. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 2014, 151.2014: 1-32.

[10] D. Yermack, “Corporate governance and blockchains,” *Review of Finance*, vol. 21, no. 1, pp. 7–31, Jan. 2017. doi:10.1093/rof/rfw074

[11] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain technology in Healthcare: A systematic review,” *Healthcare*, vol. 7, no. 2, p. 56, Apr. 2019. doi:10.3390/healthcare7020056

[12] S. Ølnes, J. Ubacht, and M. Janssen, “Blockchain in government: Benefits and implications of Distributed Ledger Technology for Information sharing,” *Government Information Quarterly*, vol. 34, no. 3, pp. 355–364, Sep. 2017. doi:10.1016/j.giq.2017.09.007

[13] N. Kshetri, “1 blockchain’s roles in Meeting Key Supply Chain Management Objectives,” *International Journal of Information Management*, vol. 39, no. Apr., pp. 80–89, Apr. 2018. doi:10.1016/j.ijinfomgt.2017.12.005

[14] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on Ethereum Smart Contracts (SOK),” *Lecture Notes in Computer Science*, no. Mar., pp. 164–186, Mar. 2017. doi:10.1007/978-3-662-54455-6_8

[15] K. Li, J.-Y. Lee, and A. Gharehgozli, “Blockchain in food supply chains: A literature review and synthesis analysis of platforms, benefits and challenges,” *International Journal of Production Research*, vol. 61, no. 11, pp. 3527–3546, Sep. 2021. doi:10.1080/00207543.2021.1970849

[16] M. Conti, E. Sandeep Kumar, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416-3452, Fourthquarter 2018, doi: 10.1109/COMST.2018.2842460.

[17] J. Wang, H. Jin, J. Chen, J. Tan, and K. Zhong, “Anomaly detection in internet of medical things with blockchain from the perspective of Deep Neural Network,” *Information Sciences*, vol. 617, no. Dec., pp. 133–149, Dec. 2022. doi:10.1016/j.ins.2022.10.060

[18] N. Mashtalyar, U. N. Ntaganzwa, T. Santos, S. Hakak, and S. Ray, “Social engineering attacks: Recent advances and challenges,” *Lecture Notes in Computer Science*, no. Jul., pp. 417–431, Jul. 2021. doi:10.1007/978-3-030-77392-2_27

[19] A. Rijanto, “Blockchain technology roles to overcome accounting, accountability and assurance barriers in supply chain finance,” *Asian Review of Accounting*, vol. 32, no. 5, pp. 728–758, Jan. 2024. doi:10.1108/ara-03-2023-0090

[20] A. Y. A. B. Ahmad, N. Verma, N. M. Sarhan, E. M. Awwad, A. Arora and V. O. Nyangaresi, "An IoT and Blockchain-Based Secure and Transparent Supply Chain

Management Framework in Smart Cities Using Optimal Queue Model," in *IEEE Access*, vol. 12, pp. 51752-51771, 2024, doi: 10.1109/ACCESS.2024.3376605

[21] P. Stoica and P. Babu, “Pearson–Matthews correlation coefficients for binary and multinary classification,” *Signal Processing*, vol. 222, no. Sep., pp. 1–9, Sep. 2024. doi:10.1016/j.sigpro.2024.109511

[22] Y. Altork, “Comparative analysis of machine learning models for wind speed forecasting: Support Vector Machines, fine tree, and linear regression approaches,” *International Journal of Thermofluids*, no. Apr., pp. 1–23, Apr. 2025. doi:10.1016/j.ijft.2025.101217

[23] A. S. Paramita and J. Jusak, “Predicting Player Performance in Valorant E-Sports using Random Forest Algorithm: A Data Mining Approach for Analyzing Match and Agent Data in Virtual Environments”, *Int. J. Res. Metav.*, vol. 2, no. 4, pp. 292–311, Nov. 2025.

[24] M. Javadi, D. Sugianto, and Sarmini, “Sentiment Analysis of User Reviews on Cryptocurrency Trading Platforms Using Pre-Trained Language Models for Evaluating User Satisfaction”, *J. Digit. Mark. Digit. Curr.*, vol. 2, no. 4, pp. 408–433, Nov. 2025.