

INTERNET OF THINGS (IOT) AND BLOCKCHAIN ANALYSIS IN REDUCING FRAUD RISK IN BANKING INDUSTRY PURWOKERTO: TRIANGLE OF FRAUD PERSPECTIVE

Anfus Khabibillah^{1*}, Dona Primasari², Eliada Herwiyanti³, Triana Ambarsari⁴

¹⁻³ Fakultas Ekonomi dan Bisnis, Universitas Jenderal Soedirman, Indonesia
⁴ Direktorat Jenderal Perbendaharaan (DJPb), Kementerian Keuangan, Indonesia
*Email corresponding author: anfus.khabibillah@mhs.unsoed.ac.id

Abstract

The global banking industry faces significant challenges related to transaction security and the increasing risk of fraud and data theft. This study aims to analyze the role of the Internet of Things (IoT) and blockchain in reducing fraud risk within the banking industry in Purwokerto, utilizing the Triangle of Fraud perspective encompassing pressure, opportunity, and rationalization. Employing a quantitative approach with a survey method, data was collected from operational employees and system operators across five banks in Purwokerto exploring or implementing IoT and blockchain technology, with purposive sampling. This research is grounded in the Technology Acceptance Model (TAM). The findings are expected to demonstrate how IoT enhances transaction security and personalized services, while blockchain contributes to real-time transactions, transparency, smart contracts, and secure identity management, thereby optimizing fraud prevention. This study provides theoretical contributions to financial technology development and practical guidance for banking institutions in developing effective fraud and data theft prevention strategies.

Keywords: Internet of Things, Blockchain, Fraud Risk, Banking Industry, Triangle of Fraud

INTRODUCTION

The modern banking industry continues to face significant challenges related to transaction security and the increasing risk of fraud and data theft. In this digital era, the complexity of financial crimes is growing, requiring financial institutions to continue to innovate in their security systems. The latest data from the (Association of Certified Fraud Examiners (ACFE), 2024) specifically shows that the financial sector is the industry with the highest fraud cases, recording 305 cases, underscoring the urgency of mitigating this risk in order to maintain customer trust and the stability of the financial system.



This study aims to analyze in depth the role of Internet of Things (IoT) and blockchain technologies in an effort to reduce the risk of fraud in the banking industry located in Purwokerto. This analysis uses a comprehensive perspective from the Triangle of Fraud, a framework that identifies pressure, opportunity, and rationalization as factors driving fraud (Cressey, 1953), and is supported by the Technology Acceptance Model (TAM) to understand technology adoption (Davis, 1989). The novelty of this study explicitly lies in the integrated investigation between two advanced technologies, IoT and blockchain, in analyzing the risk of fraud in the specific Purwokerto banking context, which has not been widely studied simultaneously within the framework.

This research is expected to provide significant contributions, both theoretically and practically. Theoretically, this research will enrich the existing literature in the field of financial technology and fraud risk management, especially regarding the implementation and impact of IoT and blockchain in the banking context (Rantung et al., 2024). This can be a reference for further research that wants to explore similar topics. Practically, the results of this study will offer concrete guidance and suggestions for banking institutions to develop more effective fraud and data theft prevention strategies, through optimizing the use of IoT and blockchain technology (Adeyemo & Obafemi, 2024).

In general, this study is expected to show how IoT plays a role in facilitating ease of transactions, increasing security through biometric systems and Know Your Customer (KYC), and enabling more personalized services (Talib & Salman, 2022). Meanwhile, blockchain is expected to contribute to real-time transactions, data transparency, smart contract implementation, and secure identity management (Najibulloh & Rahmalia, 2024). The implication, based on the expected results, is practical advice for banks to strategically integrate IoT to improve security layers and efficiency, and implement blockchain with a focus on operational transparency and strong data authentication, while still paying attention to the Triangle of Fraud factors for comprehensive risk mitigation (Erari et al., 2024).

LITERATURE REVIEW AND HYPOTHESIS FORMULATION

A. Triangle of Fraud Theory

Triangle of Fraud is a theoretical model developed by Cressey (1953) to explain the phenomenon of fraud. This model identifies three main elements that are generally present when someone commits fraud: Pressure, Opportunity, and Rationalization. Pressure refers to the motivating factors that compel an individual to commit fraud, such as urgent financial needs, unrealistic performance targets, or personal problems. These pressures can be internal or external, which push an individual to exceed their moral boundaries. Opportunity refers to conditions or situations that allow an individual to commit fraud without detection or with low risk (Cressey, 1953).

This often arises from weaknesses in internal controls, lack of supervision, the absence of effective audits, or a lack of training and risk awareness among employees. The greater the opportunity, the more likely someone is to commit fraud (Cressey, 1953). Finally, Rationalization is the mental process by which individuals justify their fraudulent actions, thereby reducing feelings of guilt or ethical violations. Rationalization can take the form of believing that they are “just borrowing” or that the company “owes” them, being the final step that allows someone to exceed their moral boundaries (Cressey, 1953).

B. Technology Acceptance Model (TAM) Theory

Technology Acceptance Model (TAM), introduced by (Davis, 1989) as an adaptation of Theory of Reasoned Action (TRA) by (Ajzen & Fishbein, 1975), is a predictive theory regarding the acceptance and use of the latest information technology by individuals or entities (Syahronny & Dewayanto, 2024). Its main objective is to explain the adoption of accounting information technology by analyzing the relationship between perceived usefulness and ease of use on user adoption

intentions. TAM consists of four main determinants: perceived ease of use, perceived usefulness, behavioral intention to use, and actual system usage (Davis, 1989).

Perceived ease refers to the belief that technology is easy to use (Syahronny & Dewayanto, 2024), relevant to IoT which ensures data integrity, energy efficiency (Ramadhani et al., n.d.), and operational improvements such as smart ATMs (Siti Epa Hardiyanti, 2024). The perception of usefulness is related to the value of technology in improving performance and productivity (Syahronny & Dewayanto, 2024), as seen from transparency, transaction speed, blockchain data security in the IoT ecosystem, the ability to reduce fraud, and strong data integration (Arwani & Priyadi, 2024; Erari et al., 2024).

Attitudes to use reflect individual tendencies based on output and interest (Syahronny & Dewayanto, 2024), supported by the ease of IoT and the security and speed of blockchain (Waloyandari & Tyas, 2024; Arwani & Priyadi, 2024; Siti Epa Hardiyanti, 2024). Interest in use, as indicated by the number of users, indicates the success of the technology (Syahronny & Dewayanto, 2024), such as the example of BNI which uses IoT and blockchain for trade finance and remittance products, which has been proven to increase the number of customers and company profits (Bank Negara Indonesia, 2018). Thus, TAM plays a vital role as a predictor of technology adoption and fraud detection efforts, emphasizing the importance of technological innovations such as IoT and blockchain to improve services and security in the banking industry in reducing the risk of fraud (Setianingsih et al., 2024).

C. Internet of Things (IoT)

Internet of Things (IoT) is defined as a set of connected systems capable of interacting in collecting, sending, receiving, and securing data via the internet, making it widely used in everyday life including in the business world (Adianto et al., 2024). In the financial sector, the application of IoT can provide warnings and suggestions in better financial planning through collaboration with biometric sensors (Şebnem YAŞAR, n.d.).

The concept of IoT in banking includes ease of transactions with IoT-based payment protocols (Wahaballa, 2022), increased security through biometric authentication/Face ID (Talib & Salman, 2022), financial risk management based on big data analysis, and smart ATMs with real-time data. In addition, IoT enables the development of personalized customer services such as teller bots or AI-based chatbots that understand consumer needs in real-time (Arief Mulyono, 2022), as well as integration with smart contracts and algorithms for operational improvements, reduced transaction costs, and automation of financial processes that support MSMEs (Wang, 2023). This study is supported by previous studies from (Widianingsih et al., 2018; Arwani & Priyadi, 2024; (Waloyandari & Tyas, 2024); (Petratos, 2024) which also stated that IoT has a negative and significant effect on fraud risk. Based on the explanation above, the following hypothesis can be concluded.

H1: Internet of Things has a negative effect on fraud risk in the banking industry.

D. Blockchain

Blockchain is a recorded public media system that allows all parties involved to see activities in real time and secure from suspicious activities (Arwani & Priyadi, 2024). Its relationship with the Technology Acceptance Model (TAM) can be seen from the benefits and ease of use it offers, where maximum utilization of blockchain can encourage digital transformation, increase security, and accountability, although it requires understanding from customers (Erari et al., 2024).

The application of blockchain in banking can be started by implementing Triple Entry Accounting (TEA), a basic development of blockchain technology that can increase transparency, reduce the risk of fraud, and facilitate the integration of systems of various stakeholders and technologies such as Cloud Computing, AI, ERP, and supply chain, making it a basic technology for Industry 4.0 and a strong form of accounting control (Petratos, 2024). This study is supported by previous studies from (Agustin & Susilowati, 2019; Arwani & Priyadi, 2024; Setianingsih et al., 2024;

Erari et al., 2024; Petratos, 2024) which stated that Blockchain has a negative effect on fraud risk. Based on the description above, the following hypothesis can be concluded.

H2: Blockchain negatively impacts fraud risk in the banking industry.

E. Pressure

Pressure in general is a situation where an individual or entity needs to commit fraud due to a need, a specific target or because of incentives (Fontanella et al., 2020). The relationship with the triangle of fraud, pressure is one of the factors that drives fraud because pressure is a condition that is definitely experienced by all workers. In general, pressure can occur due to internal and external factors, in the banking concept itself it can occur due to internal pressure in the form of financial targets or human resource pressure, or external pressure in this case includes regulatory pressure, fairly competitive targets and pressure due to market targets (Oktaviani, 2023).

This study is also supported by previous studies from (Astuti et al., 2022; Indriani et al., 2016; Flawdia Putri & Yanti, 2020; Suryandari & Pratama, 2021; Rahma & Suryani, 2019; John Tirtawirya & Riyadi, 2021; Wahidin & Asse, 2020; Fontanella et al., 2020; Marheni & Suryati, 2021) which states that pressure has a positive effect on the risk of fraud, this can occur either due to internal or external pressure such as high leverage ratios, financial pressure, work pressure on certain targets, pressure from family needs to frustration. Based on the description above, the following hypothesis can be concluded.

H3: Pressure has a positive effect on fraud risk in the banking industry.

F. Opportunity

Opportunity is a condition or an opportunity where an individual or entity knows a gap or weakness in the system so that they can commit fraud without being detected by anyone including the company system (Suryandari & Pratama, 2021). The relationship with the triangle of fraud opportunity has an important role in the occurrence of fraud because every employee involved in all company activities must understand how the flow or mechanism of the company system can run, including the advantages and disadvantages or gaps in the system. This usually happens because of a weak internal control system that makes the flow of all company activities less well controlled, especially if many individuals take advantage of this situation, it will result in habits that will harm the company as a whole. This study is also supported by previous studies from (Astuti et al., 2022; Indriani et al., 2016; Flawdia Putri & Yanti, 2020; Suryandari & Pratama, 2021; Rahma & Suryani, 2019; John Tirtawirya & Riyadi, 2021; Wahidin & Asse, 2020; Fontanella et al., 2020; Marheni & Suryati, 2021) which states that opportunity has a positive effect on fraud risk, based on the description above, the following hypothesis can be concluded.

H4: Opportunity has a positive influence on fraud risk in the banking industry.

G. Rationalization

Rationalization is an act of justifying an action that is carried out without regard to the right and wrong of the action, this is done to satisfy oneself, even though what is done cannot be justified ethically or morally and violates the law (Flawdia Putri & Yanti, 2020). The relationship between the triangle of fraud and rationalization plays an important role in encouraging fraud because it is related to the attitudes, mindsets and habits of employees, so that if this is associated with high work pressure, the potential for fraud will be even higher, and vice versa, therefore it is important to ensure that every employee has good ethical standards and codes of ethics at work, this can be realized by holding training or training on the importance of implementing morals and codes of ethics at work. This study is also supported by previous studies from (Astuti et al., 2022; Indriani et al., 2016; Flawdia Putri & Yanti, 2020; Suryandari & Pratama, 2021; Rahma & Suryani, 2019; John Tirtawirya & Riyadi, 2021; Wahidin & Asse, 2020; Fontanella et al., 2020; Marheni & Suryati, 2021) states that rationalization has a positive effect on fraud risk. Based on the description above, the following hypothesis can be concluded.

H5: Rationalization has a positive effect on the risk of fraud in the banking industry.

RESEARCH METHODS

A. Types of research

The type of research used is survey research with a quantitative approach. Survey research is research conducted with the aim of obtaining an overview of several aspects of the population through the samples studied (Maidiana, 2021). The quantitative method is called a positivist method because it is based on the philosophy of positivism. On the other hand, this method is also called a scientific method because it has fulfilled scientific principles, including concrete, objective, measurable, rational and systematic. Therefore, this method is also called discovery because it helps to discover and develop various types of new knowledge and technology, so this method is called a quantitative method because the research data is in the form of numbers or numerics and is analyzed using statistical procedures (Ali et al., 2022).

B. Research Objects and Research Subjects

The object of this research is the analysis of the Internet of Things (IoT) and blockchain in reducing the risk of fraud in the banking industry, while the subjects of the research are employees and management of several banks in Purwokerto who have experience or knowledge related to the application of IoT and blockchain technology in preventing fraud.

C. Research Data Collection Techniques

Data Collection Techniques The research was conducted through a questionnaire or survey distributed to respondents, namely banking employees. This questionnaire contains questions that are relevant to the object of the study, namely the role of the Internet of Things (IoT) and blockchain in reducing the risk of fraud in the banking industry, and is designed to measure respondents' perceptions of factors within the framework of the Fraud Triangle theory and the Technology Acceptance Model (TAM). A questionnaire is a data collection technique carried out by giving a set of written questions or statements to respondents to be answered (Sugiyono, 2019)

D. Multiple Regression Analysis

Multiple regression analysis is conducted to determine the relationship of dependent variables involving more than one independent variable (Sugiyono, 2019). As in this study which aims to determine the effect of the Internet of Things (IoT), Blockchain, Pressure, Opportunity and Rationalization on Fraud Risk so that the multiple linear regression equation can be written as follows:

$$Y = a + b_1X_1 + b_2X_2 + b_3X_3 + b_4X_4 + b_5X_5 + \dots + b_nX_n + \xi$$

Information:

Y = Fraud Risk

a = Constants

b₁ = Regression coefficients for the Internet of Things (IoT)

b₂ = Regression coefficient for Blockchain

b₃ = Regression coefficient for Pressure

b₄ = Regression coefficient for Chance

b₅ = Regression coefficient for Rationalization

b_n = Regression coefficient for Fraud Risk

X₁ = Internet of Things (IoT)

X₂ = Blockchain

X₃ = Pressure

X₄ = Opportunity

X₅ = Rationalization

E. Classical Assumption Test

1. Heteroscedasticity Test conducted to ensure that the residual variance is constant; the Glejser method is used, and if the significance is ≥ 0.05 then there is no heteroscedasticity (Sugiyono, 2019).
 2. Multicollinearity Test aims to detect high correlation between independent variables using VIF, where VIF values < 10 and Tolerance > 0.1 indicate the absence of multicollinearity (Sugiyono, 2019).
 3. Linearity Test used to determine the relationship between variables in the study whether they are linearly related or not. The test can be said to be linear if the significant deviation from linearity > 0.05 (Sugiyono, 2019).
- F. Coefficient of Determination (R^2)
- The coefficient of determination (R^2) is used to measure how much variation in the dependent variable can be explained by the independent variables in a regression model, with values ranging from 0 to 1. An R^2 value close to 1 indicates that the model is able to explain most of the data variability, while a low value indicates that the model's predictive ability for the dependent variable is still limited (Sugiyono, 2019).
- G. F Test
- The F test is used to test whether independent variables simultaneously have a significant effect on the dependent variable in a regression model (Sasmita et al., 2023). This test helps determine the overall significance of the model, where significant results indicate that at least one independent variable has an effect on the dependent variable, namely the Internet of Things (IoT).
1. If the significant value of $F \leq 0.05$ (α) then H_0 is rejected and H_1 is accepted. This means that all independent variables have a significant influence on the dependent variable.
 2. If the significant value $F > 0.05$ (α) then H_0 is accepted and H_1 is rejected. This means that all independent variables do not have a significant effect on the dependent variable.
- H. t Test
- The t-test is used to measure the influence of each independent variable partially on the dependent variable, by comparing the calculated t value with the t table or looking at the significance value (Sugiyono, 2019).
1. If the calculated t value $\leq t$ table then H_0 is rejected. This means that the independent variable partially affects the dependent variable.
 2. If the calculated t value $> t$ table then H_0 is accepted. This means that the independent variable partially does not affect the dependent variable.

RESULTS AND DISCUSSION

A. Classical Assumption Test

1. Based on the Glejser method, the results of the heteroscedasticity test show that the significance value (Sig.) of all independent variables is greater than 0.05. The details are: Internet of Things (IoT) with Sig. 0.449; Blockchain with Sig. 0.091; Pressure with Sig. 0.811; Opportunity with Sig. 0.575; and Rationalization with Sig. 0.655. This indicates that there is no heteroscedasticity problem in this study.
2. The results of the multicollinearity test show that all independent variables, namely Internet of Things (IoT), Blockchain, Pressure, Opportunity, and Rationalization, have a Tolerance value above 0.10 and a Variance Inflation Factor (VIF) value below 10. Specifically, the Internet of Things (IoT) has a Tolerance of 0.679 and a VIF of 1.473; Blockchain has a Tolerance of 0.542 and a VIF of 1.844; Pressure has a Tolerance of 0.977 and a VIF of 1.023; Opportunity has a Tolerance of 0.969 and a VIF of 1.032; and Rationalization has a Tolerance of 0.525 and a VIF of 1.904. Thus, it can be concluded that there are no symptoms of multicollinearity in this study.

3. The results of the linearity test show that the significance value (Sig.) for all independent variables is greater than α (0.05). In detail, the Internet of Things (IoT) has a Sig. of 0.919; Blockchain has a Sig. of 0.922; Pressure has a Sig. of 0.951; Opportunity has a Sig. of 0.326; and Rationalization has a Sig. of 0.989. Thus, it can be said that the independent variables in this study have a linear relationship with the dependent variable Fraud Risk.

B. Multiple Regression Analysis

The research was conducted to analyze the influence of independent variables on dependent variables. The following are the results of multiple regression analysis in this study:

No	Variables	Regression coefficient	count	ttable
1.	Internet of Things (IoT)	-1,716	-16,157	1,67
2.	Blockchain	0,178	2,29	1,67
3.	Pressure	0,045	0,789	1,67
4.	Opportunity	0,817	2,344	1,67
5.	Rationalization	-0,854	-7,438	1,67

Source: Data processed, SPSS 25

Constants = 36,256

Coefficient of determination = 0,807

F_{count} = 55,365

Based on the table above, it can be concluded that the multiple regression analysis equation is:

$$Y = 36,256 - 1,716 X_1 + 0,178 X_2 + 0,045 X_3 + 0,817 X_4 - 0,854 X_5$$

1. The risk of fraud will be 36,256 if IoT, Blockchain, Pressure, Opportunity and rationalization are 0 due to the constant of 36,256.
2. The coefficient of -1.716 can be said that the Internet of Things (IoT) variable has a negative influence on fraud risk and it can also be said that if the Internet of Things (IoT) increases, the fraud risk will decrease.
3. The coefficient of 0.178 can be said that the Blockchain variable has a positive influence on fraud risk and it can also be said that if Blockchain increases, the risk of fraud will increase.
4. With a coefficient of 0.045, it can be said that the pressure variable has a positive influence on the risk of fraud and it can also be said that if pressure increases, the risk of fraud will increase.
5. The coefficient of 0.817 can be said that the Opportunity variable has a positive influence on the risk of fraud and it can also be said that if the Opportunity increases, the risk of fraud will increase.
6. The coefficient of -0.854 can be said that the Rationalization variable has a negative influence on the risk of fraud and it can also be said that if Rationalization increases, the risk of fraud will decrease.

C. Coefficient of Determination (R^2)

The results of the multiple regression analysis show a determination coefficient (R^2) of 0.807 and it can be said that 81% of the changes in fraud risk can be explained by changes in the Internet of Things (IoT), Blockchain, Pressure, Opportunity and Rationalization variables. And 19% can be explained by changes in fraud risk due to variables that were not studied.

D. F Test

Based on the results of multiple regression analysis, this study obtained F_{count} of 55.365 with F_{table} 2.368 and significance of $0.000 < 0.05$. So it can be concluded that the Internet of Things (IoT), Blockchain, Pressure, Opportunity and Rationalization have a significant influence on turnover intention and it can also be said that the study is said to be appropriate with the research data (goodness of fit).

E. t Test

1. In the multiple regression analysis test of the relationship between the Internet of Things (IoT) variable and the Risk of fraud, there is a t_{count} result $> t_{table}$ with a result of $-16.157 > 1.670$, with a significance level of $< \alpha$ (0.05) which is $0.00 < 0.05$ and the results of the F_{count} test $> F_{table}$, it can be concluded that the regression results are good (good of fit). It can be interpreted that the Internet of Things (IoT) has a significant negative effect on the Risk of fraud, so H_1 the Internet of Things (IoT) variable has a negative effect on the Risk of fraud is accepted.
2. In the multiple regression analysis test of the relationship between the Blockchain variable and the Risk of fraud, there is a result of $t_{count} > t_{table}$ with a result of $2.290 > 1.670$, with a significance level of $< \alpha$ (0.05) which is $0.026 < 0.05$ and the results of the $F_{count} > F_{table}$ test, it can be concluded that the regression results are good (good of fit). It can be interpreted that Blockchain has a significant positive effect on the Risk of fraud, so H_2 the Blockchain variable has a positive effect on the Risk of fraud is accepted.
3. In the multiple regression analysis test of the relationship between the Pressure variable and the Risk of fraud, there is a result of $t_{count} > t_{table}$ with a result of $0.789 < 1.670$, with a significance level of $> \alpha$ (0.05) which is $0.433 > 0.05$ and the results of the $F_{count} < F_{table}$ test, it can be concluded that the regression results are not good. It can be interpreted that Pressure has a significant positive effect on the Risk of fraud, so that H_3 the Pressure variable has a positive effect on the Risk of fraud is rejected.
4. In the multiple regression analysis test of the relationship between the Opportunity variable and the Risk of fraud, there is a result of $t_{count} > t_{table}$ with a result of $2.344 > 1.670$, with a significance level of $< \alpha$ (0.05) which is $0.022 < 0.05$ and the results of the F_{count} test $> F_{table}$, it can be concluded that the regression results are good (good of fit). It can be interpreted that Opportunity has a significant positive effect on the Risk of fraud, so that H_4 the Opportunity variable has a positive effect on the Risk of fraud is accepted.
5. In the multiple regression analysis test of the relationship between the Rationalization variable and the Risk of fraud, there is a result of $t_{count} > t_{table}$ with a result of $-7.438 > 1.670$, with a significance level of $< \alpha$ (0.05) which is $0.00 < 0.05$ and the results of the F_{count} test $> F_{table}$, it can be concluded that the regression results are good (good of fit). It can be interpreted that Rationalization has a significant negative effect on the Risk of fraud, so that H_5 the Rationalization variable has a negative effect on the Risk of fraud is accepted.

CONCLUSION

A. Conclusion

1. The Internet of Things (IoT) has a negative and very significant impact on the risk of fraud in the banking industry in Purwokerto, this means that the more reliable (sophisticated) and massive the implementation of IoT, the lower the level of fraud risk in the banking industry in Purwokerto.
2. Blockchain has a positive and significant effect on the risk of fraud in the banking industry in Purwokerto, this means that the more massive the implementation of Blockchain, the higher the level of fraud risk in the banking industry in Purwokerto, and vice versa.
3. Pressure has a positive effect on the risk of fraud in the banking industry in Purwokerto, this means that the higher the pressure in the work environment, the higher the level of fraud risk in the banking industry in Purwokerto, and vice versa.

4. Opportunity has a positive and very significant effect on the risk of fraud in the banking industry in Purwokerto, this means that the higher the opportunity obtained or known, the higher the level of fraud risk in the banking industry in Purwokerto, and vice versa.
5. Rationalization has a negative and very significant effect on the risk of fraud in the banking industry in Purwokerto, this means that the more rational the employee thinks, the lower the level of fraud risk in the banking industry in Purwokerto.

B. Implications

The banking industry in Purwokerto is advised to continue investing in the development and implementation of more sophisticated Internet of Things (IoT) technology to improve security, reduce potential fraud, and accelerate threat detection. On the other hand, Blockchain implementation needs to be carried out more carefully, accompanied by tight control and mitigation of loopholes that can be exploited by fraudsters. In addition, it is important for banks to focus on stress management and creating a healthy work environment to reduce the potential for fraud due to pressure.

Strict internal controls, stronger transaction monitoring policies, and the use of sophisticated technologies such as automated audit systems are also crucial to minimize fraud opportunities. Finally, fostering a culture of ethics and integrity among employees through training, a clear reward/sanction system, and understanding the consequences of fraudulent actions can significantly reduce the potential for fraud by encouraging rational and ethical thinking.

C. Research Limitations

The limitations of this study include, among others, it was only conducted in the banking industry in Purwokerto, so that for further research it is expected to expand the scope of the area and research objects regarding the Internet of Things (IoT), Blockchain, Pressure, Opportunity, Rationalization, and Fraud Risk. In addition, this study also faces limitations because there are still few articles or journals that specifically discuss the topic of analyzing the influence of IoT and Blockchain in reducing the risk of fraud in the banking industry, especially those that focus on Blockchain technology.

BIBLIOGRAPHY

- Adeyemo, K., & Obafemi, F. J. (2024). A Survey on the Role of Technological Innovation in Nigerian Deposit Money Bank Fraud Prevention. *South Asian Journal of Social Studies and Economics*, 21(3), 133–150. <https://doi.org/10.9734/sajsse/2024/v21i3790>
- Adianto, Wiedartini, Rachmadita, R., Erawati, I., Budiawati, R., Utari, D., & Ardliyana, T. (2024). Pengenalan Sistem IoT Pada Pemanfaatan Kebutuhan Sehari-Hari. *Jurnal Cakrawala Maritim*, 7. <http://jcm.ppns.ac.id>
- Agustin, R., & Susilowati, D. (2019). Preventing Corruption With Blockchain Technology (Case Study Of Indonesian Public Procurement). *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, 8(09). www.ijstr.org
- Ajzen, I., & Fishbein, M. (1975). A Bayesian analysis of attribution processes. *Psychological Bulletin*, 82(2), 261–277. <https://doi.org/10.1037/h0076477>
- Ali, M. M., Hariyati, T., Pratiwi, M., & Afifah, S. (2022). Metodologi Penelitian Kuantitatif Dan Penerapan Nya Dalam Penelitian. *Education Journal*.2022, 2(2).
- Arief Mulyono, J. (2022). Evaluation of Customer Satisfaction on Indonesian Banking Chatbot Services During the COVID-19 Pandemic. *CommIT Journal*, 16(1).
- Arwani, A., & Priyadi, U. (2024). Eksplorasi Peran Teknologi Blockchain dalam Meningkatkan Transparansi dan Akuntabilitas dalam Keuangan Islam: Tinjauan Sistematis. *JURNAL EKONOMI BISNIS DAN MANAJEMEN*, 2(2), 23–37. <https://doi.org/10.59024/jise.v2i2.653>
- Association of Certified Fraud Examiners (ACFE). (2024). *Penipuan di Tempat Kerja 2024: Laporan untuk Negara-negara*.

- Astuti, P., Maghfiroh, S., Ramadhanti, W., Pku, R. S., & Gombong, M. (2022). Sistem pengendalian internal berbasis COSO untuk pencegahan fraud di Rumah Sakit Muhammadiyah / Aisyiyah Wilayah Jawa Tengah. *Jurnal Ilmiah Akuntansi Dan Keuangan*, 5(1), 2022. <https://journal.ikopin.ac.id/index.php/fairvalue>
- Bank Negara Indonesia. (2018, May 11). Manfaatkan Teknologi Blockchain, BNI Tingkatkan Bisnis Trade Finance dan Remittance. *Www.Bni.Co.Id*.
- Cressey, D. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Free Press. <https://psycnet.apa.org/record/1954-06293-000>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*, 13(3), 319–339. <https://doi.org/10.2307/249008>
- Erari, A., Hartono, P., Surahman, B., Mahdi, & Kraugusteeliana, K. (2024). PENGARUH TEKNOLOGI BLOKCHAIN TERHADAP EFISIENSI DAN KEAMANAN TRANSAKSI KEUANGAN: STUDI KASUS PADA INDUSTRI PERBANKAN DI INDONESIA. *Edunomika*, 8(2).
- Flawdia Putri, C., & Yanti, H. B. (2020). *PENGARUH FRAUD DIAMOND TERHADAP TINDAK PIDANA KORUPSI*. <https://doi.org/https://doi.org/10.25105/pakar.v0i0.6916>
- Fontanella, A., Sukartini, S., Chandra, N., & Sriyuniati, F. (2020). Kecurangan Akademis Mahasiswa: Kenapa Terjadi dan Apa yang Harus Dilakukan? *Jurnal ASET (Akuntansi Riset)*, 12(1), 155–164. <https://doi.org/10.17509/jaset.v12i1.22378>
- Indriani, I., Suroso, A., & Maghfiroh, S. (2016). *PENERAPAN KONSEP FRAUD DIAMOND THEORY DALAM MENDETEKSI PERILAKU FRAUD*.
- John Tirtawirya, M., & Riyadi, S. (2021). Pengaruh Segitiga Kecurangan untuk Mengidentifikasi Kecurangan Laporan Keuangan Menggunakan Variabel Moderasi Penerapan Integrasi Teknologi Industri. *Jurnal Akuntansi, Keuangan, Dan Manajemen*, 2(3), 179–194. <https://doi.org/10.35912/jakman.v2i3.108>
- Maidiana. (2021). Penelitian Survey. *ALACRITY : Journal Of Education*, 1(2).
- Marheni, D. K., & Suryati, S. (2021). Analysis of Financial Stability Factors, Financial Targets, External Pressure, Inefficient Monitoring and Rationalization of the Financial Statements Fraud. *Almana : Jurnal Manajemen Dan Bisnis*, 5(2), 241–248. <https://doi.org/10.36555/almana.v5i2.1626>
- Najibulloh, K., & Rahmalia, L. (2024). Penerapan Teknologi Blockchain dalam Industri Keuangan Syariah: Tantangan dan Peluang. *Jurnal Ekonomi Dan Bisnis Islam*, 03(01). <https://ejournal.stais.ac.id/index.php/j-ebi/index>
- Petratos, P. (2024). Triple-Entry Accounting and System Integration. *Journal of Risk and Financial Management*, 17(2). <https://doi.org/10.3390/jrfm17020045>
- Rahma, D. V., & Suryani, E. (2019). Pengaruh Faktor-Faktor Fraud Triangle Terhadap Financial Statement Fraud. *Jurnal ASET (Akuntansi Riset)*, 11(2), 301–314. <https://doi.org/10.17509/jaset.v11i2.17926>
- Ramadhani, R., Gultom, H., Ramadhan, I. F., Salsabila, S., & Herdiyanto, O. (n.d.). PENGAMANAN DATA SENSOR IOT DENGAN TEKNOLOGI BLOCKCHAIN UNTUK SMART HOME. *Journal Education and Technology (JUTECH)*.
- Rantung, M. C., Siagian, H., Tagal, J., & Sinaga, G. (2024). Optimizing the Security of Letter of Credit Transactions: Application of Blockchain Technology in Reducing the Risk of Fraud in Banking. *DINASTI INTERNATIONAL JOURNAL OF ECONOMICS FINANCE AND ACCOUNTING (DIJEFA)*, 5(1). <https://doi.org/10.38035/dijefa.v5i1>
- Şebnem YAŞAR, R. (n.d.). A Critical Overview of the Geometry of Fraud and a Model Proposal within the Framework of Situational Action Theory *. *The Journal of Accounting and Finance*.
- Setianingsih, R., Negeri, U. I., & Utara, S. (2024). Analisis Teknologi Blockchain Berperan dalam Meningkatkan Keamanan dan Data Privasi di Sektor Keuangan Terhadap Implementasi. *Jurnal Ilmiah Nusantara (JINU)*, 1(4), 3047–9673. <https://doi.org/10.61722/jinu.v1i4.1841>

- Siti Epa Hardiyanti. (2024). Inovasi dalam Layanan Perbankan Berbasis Internet of Things (IOT) Peluang dan Tantangan di Era Digital. *Maeswara: Jurnal Riset Ilmu Manajemen Dan Kewirausahaan*, 2(3), 361–372. <https://doi.org/10.61132/maeswara.v2i3.1041>
- Sugiyono. (2019). 'Pengertian Uji Instrumen Penelitian.' <https://repository.unja.ac.id/24060/6/BAB%20III.pdf>
- Suryandari, E., & Pratama, L. V. (2021). Determinan Fraud Dana Desa: Pengujian Elemen Fraud Hexagon, Machiavellian, dan Love of Money. *Reviu Akuntansi Dan Bisnis Indonesia*, 5(1), 55–78. <https://doi.org/10.18196/rabin.v5i1.11688>
- Syahronny, M. R., & Dewayanto, T. (2024). PENERAPAN TEKNOLOGI ARTIFICIAL INTELLIGENCE DAN BLOCKCHAIN DALAM MENDETEKSI FRAUD PADA PROSES AUDIT: SYSTEMATIC LITERATURE REVIEW. *DIPONEGORO JOURNAL OF ACCOUNTING*, 13(3), 1–14. <http://ejournal-s1.undip.ac.id/index.php/accounting>
- Talib, A. A., & Salman, A. D. (2022). Design and develop authentication in electronic payment systems based on IoT and biometric. *Telkomnika (Telecommunication Computing Electronics and Control)*, 20(6), 1297–1306. <https://doi.org/10.12928/TELKOMNIKA.v20i6.22157>
- Wahaballa, A. (2022). *Lightweight and Secure IoT-based Payment Protocols from an Identity-Based Signature Scheme*. <https://doi.org/10.20944/preprints202210.0331.v1>
- Wahidin, A., & Asse, A. (2020). PENGARUH DIMENSI FRAUD TRIANGLE TERHADAP PERILAKU KECURANGAN AKADEMIK DENGAN AKHLAK SEBAGAI VARIABEL MODERASI PADA MAHASISWA AKUNTANSI UIN ALAUDDIN MAKASSAR. *ISAFIR: Islamic Accounting and Finance Review*, 01. <https://doi.org/https://doi.org/10.24252/isafir.v1i1.18323>
- Waloyandari, M. J., & Tyas, A. M. (2024). Pengaruh Teknologi Blockchain Terhadap Kepercayaan Investor dalam Pengambilan Keputusan Investasi. *R2J*, 6(5). <https://doi.org/10.38035/rrj.v6i5>
- Wang, R. (2023). Blockchain and Bank Lending Behavior: A Theoretical Analysis. *SAGE Open*, 13(1). <https://doi.org/10.1177/21582440231164597>
- Widianingsih, R., Maghfiroh, S., Sunarmo, A., Ekonomi, F., Bisnis, D., & Soedirman, U. J. (2018). PENGARUH TEKNOLOGI INFORMASI DAN ACCOUNTING REPORTING TERHADAP PENCEGAHAN FRAUD. *KOMPARTEMEN: JURNAL ILMIAH AKUNTANSI*, XVII(2), 110–123. <http://jurnalnasional.ump.ac.id/index.php/kompartemen/>