E-ISSN : 2686-6331
P-ISSN : 2686-6358
DINASTI INTERNATIONAL JOURNAL OF ECONOMICS, FINANCE AND ACCOUNTING (DIJEFA)
https://dinastipub.org/DIJEFA dinasti.info@gmail.com +62 811 7404 455

DOI: https://doi.org/10.38035/dijefa.v5i1
Received: 20 Maret 2024, **Revised:** 8 April 2024, **Publish:** 16 April 2024

Optimizing the Security of Letter of Credit Transactions: Application of Blockchain Technology in Reducing the Risk of Fraud in Banking

Melinda C Rantung[1], Harlyn Siagian[2], Judith Tagal Gallena Sinaga[3]
[1]Adventist University of Indonesia, Email: 2234023@unai.edu
[2]Adventist University of Indonesia, Email: siagian_unai@yahoo.co.id
[3]Adventist University of Indonesia, Email: Judith.sinaga@unai.edu

Corresponding Author: 2234023@unai.edu[1]

Abstract: Letter of Credit (LC) transactions play a vital role in facilitating international trade, but are vulnerable to various forms of fraud such as forgery of documents and manipulation of information. In the banking context, ensuring the security of LC transactions is an urgent challenge. This research aims to investigate the potential of applying blockchain technology in improving the security of LC transactions and reducing the risk of fraud in the banking sector. This research is included in descriptive quantitative research. This research was conducted at Banks in DKI Jakarta. The population in this research are customers who use Letter of Credit transactions. The sampling technique in this research is purposive sampling so that in this research the research sample was 100 customers who used letter of credit transactions. The data analysis technique in this research uses Partial Least Square (PLS). The research results show that blockchain technology has great potential to increase the security of LC transactions through aspects such as high data security, transparency and auditability, as well as automation through smart contracts. With proper implementation, blockchain technology can help reduce the risk of fraud, increase operational efficiency, and build trust in international trade. This study contributes to the understanding of the potential application of blockchain technology in the global financial context and highlights the importance of cross-sector collaboration to address transaction security challenges.

Keyword: Letter of Credit, Blockchain, Risk of Fraud

INTRODUCTION

Letter of Credit (LC) transactions play a crucial role in facilitating payments between parties involved in international trade. LC is a bank-guaranteed instrument that acts as an intermediary between importers and exporters, providing both parties with the assurance that payment will only be made upon fulfillment of the specified LC conditions (Harahap, 2018).

LC fosters trust between international trade participants, namely exporters and importers. It assures exporters of payment upon meeting obligations, while importers are

ensured that payment will occur only after satisfying LC terms (Maulana, 2020; Kriswandhany, 2014; Hendrik, 2019). Moreover, LC mitigates payment risks for both sides (Nugraha & Andraini, 2023), alleviating concerns for exporters regarding post-shipment payment and sparing importers from pre-payment prior to goods receipt or document compliance.

Compliant with International Chamber of Commerce (ICC) standards like UCP 600 (Uniform Customs and Practice for Documentary Credits), LC ensures global transactional clarity and consistency. By facilitating payment and shipment processes across parties amidst geographic, legal, or trust disparities, LC not only serves as a payment conduit but also as a fundamental pillar of international trade, instilling security, trust, and efficiency among stakeholders (Purba, 2022).

Despite its pivotal role, LC transaction security remains a primary concern due to susceptibility to varied fraud forms (Widyana, 2023; Rumengan, 2021) including document forgery, data manipulation, and other deceitful acts (Maffuadi & Khairani, 2020). The intricacy and multi-party nature often render LC a target for unscrupulous individuals aiming to exploit systemic weaknesses for personal gain.

Consequently, continuous efforts are imperative within the banking industry and international trade to enhance LC transaction security (Indriani, 2022; Mita, et al., 2018). The proposition of blockchain technology emerges as a viable solution owing to its decentralized, transparent, and tamper-resistant attributes (Pratiwi, 2022; Munir, et al., 2021). By harnessing this technology's strengths, significant fraud risk reduction is anticipated, fostering heightened trust and operational efficiency within LC transactions (Alexander & Muhammad, 2020).

Research findings by Maulani et al (2023); Susanto & Ashari (2024); Utami et al (2016); and Suryawijaya (2023) underline blockchain technology's substantial impact on information security, advocating its adoption to bolster transactional security and reliability, thereby mitigating fraud and data manipulation risks inherent in conventional processes.

Against this backdrop, this research endeavors to explore blockchain technology's potential application in optimizing LC transaction security within the banking sector. Through blockchain integration into LC transactions, a notable reduction in fraud risk is anticipated, paving the way for enhanced trust and efficiency in international trade.

By delving deeper into LC transaction challenges and blockchain technology's proposed solutions, this research aims to make valuable contributions towards cultivating a more secure, trustworthy, and efficient global financial ecosystem.

Literature Review

Letter of Credit

A documentary letter of credit (LC), referred to as a documentary credit, is a banking service utilized to facilitate product purchases, allowing buyers to defer payment for goods from the time the LC is initiated until a specified period as agreed upon (Tjung, 2022; Utami et al., 2016).

The primary function of an LC is to delay payment, serving exclusively to support sales contracts. In essence, buyers are not obliged to remit funds prior to the shipment or delivery of goods or services by the seller; instead, they are afforded the opportunity to ensure that goods or services conform to agreed specifications before settling the payment (Khoruddin, 2023).

LCs hold significant importance as financial instruments in international trade by instilling confidence in secure and reliable transactions for both parties, albeit with associated advantages and drawbacks (Herlambang, 2023). Importers and exporters can derive various advantages from adopting LC payment arrangements. For importers, benefits include the ability to select appropriate document types, certainty regarding shipment timelines, access to

import financing from the issuing bank, and enhanced transaction security and efficiency facilitated by bank guarantees and oversight. Similarly, exporters can benefit from reduced shipping-to-payment timelines, avoidance of unilateral LC cancellations, and the option to request supplementary guarantees from other banks. Exporters can mitigate transfer risks by utilizing alternative banking channels if they question the issuing bank's credibility or are concerned about political or transfer-related risks in the buyer's country. Throughout the transaction process, control over documents and goods remains shared between the bank and exporter until payment is effected by the issuing bank. In cases where the issuing bank deems the exporter compliant with LC terms, export financing facilities may be sought from alternate banking entities (Subagja, 2020).

Despite its advantages, the LC payment system is not without drawbacks. These include higher associated costs compared to alternative payment methods, challenges in canceling LC arrangements, absence of recourse in cases where goods fail to meet quality standards, and the inherent risk of non-payment, which is the responsibility of the exporter. Banks may withhold payment if submitted documents fail to satisfy LC stipulations, and additional political or transfer-related risks may arise in relation to the importing country (Ridho, 2022; Yuliyanti, 2012).

Transaction Security

Transaction security is a critical aspect across various transaction types, including within the realm of Letter of Credit (LC). The security of Letter of Credit (LC) transactions holds significant importance due to the substantial fund transfers involved among diverse parties across international borders. As defined by Safitriani et al. (2023), security pertains to the measures that companies implement to safeguard customers' personal information from cyber threats, particularly in digital environments. One effective strategy employed by businesses to protect customers' financial information during online transactions is the implementation of measures aimed at detecting and preventing suspicious activities. Customers are more likely to hold a favorable view of a business when assured of robust security measures that safeguard against the misuse of their personal information. Assuming that a company's security measures align with customer expectations, buyers will feel confident in completing their transactions.

Transaction security indicators serve as parameters or metrics used to assess the level of security within transaction processes. In the context of Letter of Credit (LC) or other financial instruments, pertinent transaction security indicators encompass identity authentication, data encryption and integrity, transaction auditing and monitoring, fraud and forgery prevention, user access control and authorization, and protection against security threats and attacks.

Through vigilant monitoring and assessment of these transaction security indicators, organizations and financial institutions can effectively identify potential risks or vulnerabilities within transaction processes and implement appropriate preventive measures to enhance the security and reliability of their transactions.

Blockchain technology

Blockchain technology is a decentralized system that enables secure and distributed data storage (Santoso et al., 2021). It functions as a digital decentralized ledger of transaction blocks that are cryptographically signed. Following verification and consensus, each block is cryptographically linked to the hash of the previous block. Once mining is complete and a new block is generated, the data contained within the previous block becomes highly resistant to alteration (Harahap et al., 2020).

Indicators of blockchain technology can be instrumental in assessing the performance, security, and efficacy of implementing a blockchain system. These indicators encompass

transaction speed, consensus mechanism, decentralization, security level, scalability, transparency, adoption and utilization rates, and transaction costs.\

Blockchain has garnered substantial attention in the realms of technology and finance owing to its unique capability to enhance security, transparency, and efficiency across diverse applications. With the ongoing advancement of this technology, the aspiration is for blockchain to make a significant positive impact on numerous industries in the future. Furthermore, leveraging these indicators can facilitate the evaluation of the quality and functionality of a blockchain system, as well as enhance understanding of its implications across various utilization contexts.

Fraud risk

Fraud risk pertains to threats that compromise the reliability, honesty, and integrity of a system or process (Astika, 2017). In the context of finance and business, fraud risk encompasses various actions that contravene laws, ethical standards, or internal company policies (Chairunnisa & Ibrahim, 2019). Common forms of fraud risk include document forgery, where documents associated with financial or business transactions are falsified (e.g., invoices, contracts, certificates) to illicitly gain profits or deceive other parties involved in a transaction. Data manipulation poses a risk when critical information required for business or financial decision-making is tampered with to favor specific parties or conceal vital facts. Identity theft risk arises when someone's personal information is unlawfully used for fraudulent activities or criminal acts. Financial fraud entails deceitful or misleading financial practices, such as embezzling funds from bank accounts, engaging in credit card skimming, or participating in fraudulent investments. Asset misappropriation occurs when individuals or groups divert company funds or assets for personal gain without authorization. Corruption involves the misuse of power or authority to secure personal benefits or advantages for specific parties, such as bribery, misappropriation of public funds, or conflicts of interest in decision-making. Fraud in financial transactions occurs when individuals deliberately provide false information or exploit procedural loopholes to gain unlawful profits. Lastly, technology-related risks encompass threats to the security and integrity of information systems and technology, including cyber-attacks, malware, data breaches, and technology-enabled fraud schemes such as phishing, ransomware, or unauthorized access to customer data.

Managing fraud risk necessitates a comprehensive approach, including the establishment of robust internal controls, continuous monitoring of business activities, employee training, and the deployment of advanced security technologies. Effective prevention and detection measures can significantly mitigate fraud risk and safeguard a company's assets and reputation.

METHOD

This research falls under the category of descriptive quantitative research. According to Sugiyono (2017), research methods are fundamentally part of scientific methodologies used to collect data for specific applications. The quantitative approach is founded on this principle. Descriptive research, as defined by Sarstedt et al. (2020), involves investigations aimed at understanding a given topic through direct descriptions, interviews, or surveys conducted in the present moment. Information is gathered to test hypotheses or address questions using surveys and similar instruments. Through descriptive research, scholars aim to provide an overview of the current state of affairs.

The study is conducted in DKI Jakarta. The target population consists of individuals familiar with blockchain technology and its application in letter of credit transactions. One hundred individuals knowledgeable about blockchain technology in DKI Jakarta and neighboring areas were surveyed using random sampling methods for this research endeavor.

Partial Least Square (PLS) is employed to analyze the collected data. PLS is a system of equations used for structural equation modeling (SEM), employing variance-based or component-based methodologies. As explained by Sarstedt et al. (2020), the objective of PLS-SEM is to develop or refine theories with the aim of making predictions. PLS is utilized to ascertain the interrelationships among latent variables used for prediction. Despite the modest sample size, PLS proves to be an effective analytical method due to its independence from assumptions about data distribution or specific measurement scales (Hair et al., 2019).

Validation and Reliability Assessment

Validity and reliability testing are essential to ensure the accuracy and consistency of measurements taken. The assessment of validity and reliability includes:

Firstly, evaluating standard loading factors, which indicate the strength of the relationship between the constructs measured by each item and their scores on the item or component, is a method used to assess convergent validity. Individual reflective measures are considered strong if their correlation coefficient exceeds 0.7.

Secondly, examining the measurement model using measures and constructs of cross-loadings is important for assessing discriminant validity. This model includes reflection indices. An instrument is considered valid based on discriminant validity, determined by comparing the root mean square of variance (AVE) extracted. Values above 0.5 are considered valid.

Lastly, the assessment of composite reliability, which is a structure-based metric expressed as the coefficient of latent variables, is crucial for determining the reliability of a construction. A high level of reliability is indicated by values exceeding 0.70 on this measurement.

Additionally, Cronbach's Alpha is used to enhance the reliability of composite outcomes. A variable is considered reliable if the Cronbach's alpha value exceeds 0.7.

Instrument Testing

Instrument Test	Test used
Validity test	Convergent Validity
	AVE
Reliability Test	Cronbach Alpha
	Composite Relibility

R-Square Testing

The R-square of the dependent construct is used to analyze the influence of specific independent variables on the latent dependent variable, demonstrating the magnitude of the influence.

Inner Model Analysis

The Analysis of the Structural Model, also referred to as Structural Equation Modeling (SEM), is a technique used to forecast the relationships among variables within a model. During the comprehensive analysis of the model in Smart PLS, hypotheses are tested. This testing involves presenting probability results and T-statistics. By utilizing statistical values, hypotheses can be tested using a t-statistic of 1.96 for a significance level of 5%, and the direction of relationships between variables can be determined by examining beta coefficients. To accept or reject hypotheses, careful consideration must be given to these statistical findings.

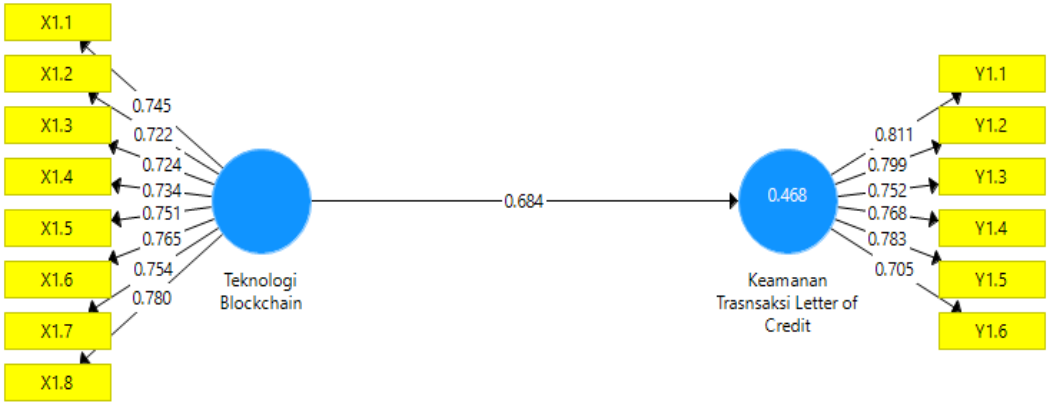
Ha: t-statistic > 1.96 with a p-value < 0.05.
H0: t-statistic < 1.96 with a p-value > 0.05.

RESULTS AND DISCUSSION

Measurement Model Evaluation (Outer Model)

The evaluation of the outer model in the research is conducted considering four criteria: Cronbach's alpha, convergent validity, discriminant validity, and composite reliability. The following diagram illustrates the research model:

Figure 2. Outer Model



Convergent Validity

External loading, also known as factor loading, is employed to assess convergent validity. An indicator is deemed to exhibit excellent convergent validity if its outer loading value exceeds 0.7. The outer loading values for each indicator on the research variables are detailed below:

Table 1
Results of Outer Loading Analysis

	Security of Letter of Credit Transactions	*Blockchain Technology*
X1.1		**0.745**
X1.2		**0.722**
X1.3		**0.724**
X1.4		**0.734**
X1.5		**0.751**
X1.6		**0.765**
X1.7		**0.754**
X1.8		**0.780**
Y1.1	**0.811**	
Y1.2	**0.799**	
Y1.3	**0.752**	
Y1.4	**0.768**	
Y1.5	**0.783**	
Y1.6	**0.705**	

Source: Processed Primary Data (2024)

Based on the outer loading measurements presented in Table 1, it is evident that all research indicators meet the criteria for use as measurement indicators, with outer loading values exceeding 0.7. Therefore, all indicators are deemed appropriate and valid for research

purposes and can be utilized for further investigation, as none of the indicators have an outer loading value below 0.7.

Predictive Strength

The objective is to ensure that each concept of a latent variable or construct is distinct from other latent variables, which is known as discriminant validity. The HTMT values serve as the most effective current measure for this purpose. A concept is considered to exhibit excellent discriminant validity if the HTMT score is less than 0.90 (Hair Jr et al., 2021). The outcomes of the discriminant validity testing are displayed in the table below.

Table 2.
Results of Heterotrait-Monotrait Ratio (HTMT) Test

	Security of Letter of Credit Transactions	Blockchain Technology
Security of Letter of Credit Transactions		
Blockchain Technology	**0.763**	

Source: Processed Primary Data (2024)

Based on the findings presented in Table 2, it can be inferred that the HTMT ratios demonstrate excellent discriminant validity for all variable constructs, as indicated by HTMT values below 0.9 (HTMT < 0.9).

Another measure of discriminant validity is the Average Variance Extracted (AVE), which represents the square root of the average extracted variance. It is recommended that this value exceed 0.5 (Memon et al., 2021). The AVE values obtained in the study are provided in Table 3 below.

Table 3.
***Average Variance Extracted* (AVE)**

	Average Variance Extracted (AVE)
Security of Letter of Credit Transactions	**0.594**
Blockchain Technology	**0.558**

Source: Processed Primary Data (2024)

Based on the data presented in Table 3, it is observed that the AVE scores for all research variables exceed the threshold of 0.5, indicating successful outcomes for the test. Specifically, the Average Variance Extracted (AVE) values for the Blockchain Technology (X1) and Security of Letter of Credit Transactions (Y) variables are 0.558 and 0.594, respectively. Therefore, we can confidently conclude that all variables demonstrate Discriminant Validity based on their AVE values surpassing the recommended threshold of 0.5. The discriminant validity exhibited by each variable is notably robust.

Composite Reliability

Subsequently, the testing involves assessing the collective dependency of indicator blocks as a metric of construct development. If the composite reliability value exceeds 0.70, then the construct is considered reliable (Tugiman et al., 2022). Below are the results of the outer model indicating the composite reliability of each construct.

Table 4.
Composite Reliability

	Composite Reliability
Security of Letter of Credit Transactions	**0.897**

Blockchain Technology	**0.910**

Source: Processed Primary Data (2024)

Based on the findings presented in Table 4, both X1 (Blockchain Technology) and Y (Security of Letter of Credit Transactions) exhibit robust composite dependency, with values of 0.910 and 0.897, respectively. The overall dependency scores exceeding 0.70 for all components indicate the reliability of these variables. It can be concluded that all variables are highly dependable based on these results, meeting the criteria for composite dependency.

Cronbach's Alpha

The reliability assessment using composite reliability can be further supported by employing Cronbach's alpha statistics. If a variable's Cronbach's alpha value surpasses 0.7, then the variable is deemed reliable according to Cronbach's alpha (Tugiman, Herman, and Yudhana, 2022). The Cronbach's alpha values for each variable are detailed below.

Table 5.
Cronbach's Alpha

	Cronbach's Alpha
Security of Letter of Credit Transactions	**0.863**
Blockchain Technology	**0.887**

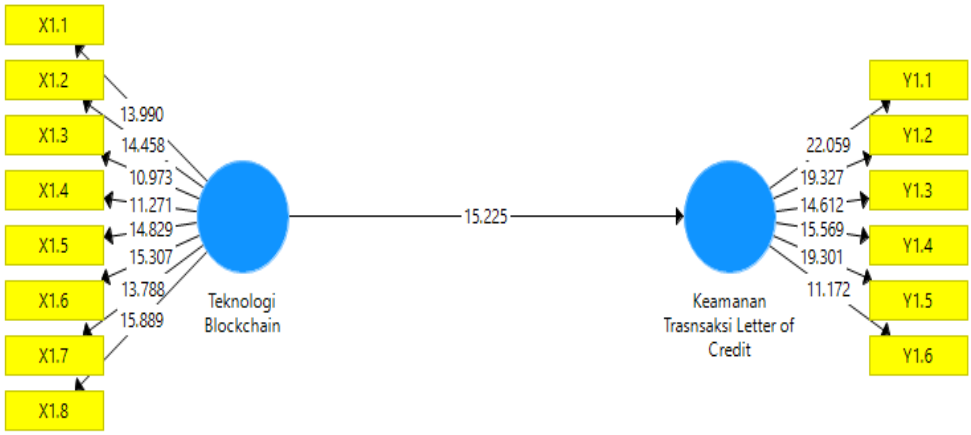
Source: Processed Primary Data (2024)

According to Table 5, all variables in the study have Cronbach's alpha values exceeding 0.7. These results suggest that all research variables exhibit a high level of reliability, meeting the established Cronbach's alpha criteria.

Evaluation of the Structural Inner Model

The evaluation of the structural inner model entails assessing the relationships between latent constructs as hypothesized in this study. This evaluation involves analyzing the inner model in the following manner.

Figure 3.
Inner Model



Based on the inner model scheme, the path coefficient of 15.225 indicates the impact of blockchain technology on the security of letter of credit transactions. The positive route coefficients for the model variables are depicted by the data presented below.

Coefficient of Determination (R2)

Following the validation of the outer model, the structural model (inner model) undergoes evaluation. Analyzing the R-squared values of dependent constructs and the t-statistic values of path coefficients allows for an assessment of the inner model's predictive capability. The study's predictive power is expected to increase with higher R-squared values. In hypothesis testing, path coefficient values indicate the level of significance of relationships. Determination testing, also referred to as Analysis of Variance (R2), aims to understand the extent to which independent variables influence dependent variables. However, the use of the coefficient of determination may introduce bias based on the number of independent variables included in the model, which is a key limitation. Therefore, to select the optimal model, it is recommended to use the modified R Square (R2) approach (Edeh et al., 2023). The specific values of the coefficient of determination are presented in Table 6.

Table 6.
Coefficient of Determination (R2)

	R Square	R Square Adjusted
Security of Letter of Credit Transactions	0.468	0.463

Source: Primary data processed (2024)

Based on the R-squared value of 0.468 obtained for the Security of Letter of Credit Transactions (Table 6), the results suggest that unaccounted factors in the study model explain 53.2% of the variance in the Security of Letter of Credit Transactions, whereas Blockchain Technology accounts for 46.8% of the variance.

Statistical Testing of Hypotheses

Drawing upon the analyzed data, the research hypotheses are addressed through the examination of findings. Employing T-Statistics and P-Values, the researchers in this study tested their hypotheses. A research hypothesis is deemed valid if its associated P-Value is less than 0.05. The latent model of this research yielded the following outcomes to verify the hypotheses.

Table 7.
Research Hypothesis Testing

	Original Sample (O)	T Statistics (|O/STDEV|)	P Values
Blockchain Technology -> Security of Letter of Credit Transactions	0.684	15.225	**0.000**

Source: Primary data processed (2024)

The findings presented in Table 7 indicate the following:

Impact of Blockchain Technology on the Security of Letter of Credit Transactions : The statistical analysis reveals a significant influence of Blockchain Technology (X1) on the Security of Letter of Credit Transactions (Y), with a T-statistic of 15.225 and a P-value of 0.000. These results suggest that Blockchain Technology plays a crucial role in enhancing the security of letter of credit transactions. The T-statistic value (15.225 > 1.654) surpasses the critical T-value, and the P-value (0.000 < 0.05) falls below the standard alpha level of 5%, confirming the substantial and beneficial impact of Blockchain Technology on transaction security.

This outcome resonates with research conducted by J. Hu et al. (2018), which explored the relationship between ethical compliance and psychological safety in workplace settings. Their analysis demonstrated a significant correlation between high levels of ethical compliance and increased psychological safety among team members or individuals.

Framework

Figure 1. Framework of Thinking

H1: Blockchain technology has a significant impact on the security of letter of credit transactions in reducing fraud risks.

H0: Blockchain technology does not have a significant impact on the security of letter of credit transactions in reducing fraud risks.

CONCLUSION

Based on the research conducted on "Optimizing Letter of Credit Transaction Security: Implementing Blockchain Technology to Reduce Fraud Risks in Banking," the conclusion drawn is that Blockchain Technology exerts a positive and significant influence on the security of Letter of Credit transactions.

In light of this conclusion, several recommendations can be proposed. Firstly, the integration of Blockchain Technology in Letter of Credit transactions could serve as an effective solution to bolster the security and dependability of the transaction process, thereby mitigating the risks associated with fraud and data manipulation prevalent in conventional approaches. Secondly, enterprises and institutions engaged in Letter of Credit transactions should contemplate adopting Blockchain Technology within their systems to enhance security and streamline transaction efficiency. Thirdly, further investigation is warranted to gain deeper insights into the optimal deployment of Blockchain Technology within the framework of Letter of Credit transactions and its potential ramifications on overall efficiency and security. Lastly, the formulation of regulations supportive of Blockchain Technology's use in Letter of Credit transactions can facilitate its adoption within the financial sector. By implementing these recommendations, it is anticipated that the security and efficiency of Letter of Credit transactions will be fortified while minimizing the likelihood of fraudulent activities.

REFERENCES

Alexander Sugiharto, S. H., & Muhammad Yusuf Musa, M. B. A. (2020). *Blockchain & Cryptocurrency Dalam Perspektif Hukum Di Indonesia Dan Dunia* (Vol. 1). Indonesian Legal Study for Crypto Asset and Blockchain.

Astika, A. D. (2017). *Peranan Pengendalian Internal Terhadap Pencegahan Kecurangan (Fraud) (Studi Kasus pada Koperasi Indra Dana Kabupaten Bandung)* (Doctoral dissertation, Universitas Widyatama).

Chairunnisa, C., & Ibrahim, M. (2019). Evaluasi Penerapan Strategi Antifraud dalam Mengelola Risiko Kecurangan pada PT X. *Jurnal Riset Akuntansi dan Keuangan*, *7*(3), 465-476.

Creswell, J. W. (2018). Penelitian kualitatif dan desain riset.

Harahap, M. Y. (2018). *Letter Of Credit* Sebagai Jaminan Pembayaran Perdagangan Internasional Di Indonesia (Tinjauan Tentang Perdegangan Mekanisme Dan Penerapannya). *Islamic Bussiness Law Review*, *1*(1).

Harahap, E. P., Aini, Q., & Anam, R. K. (2020). Pemanfaatan teknologi *blockchain* pada platform crowdfunding. *Technomedia Journal*, *4*(2 Februari), 199-210.

Hendrik, K. G. B. (2019). Kajian Yuridis Penggunaan *Letter of Credit* (L/C) Dalam Transaksi Perdagangan Internasional. *Lex Et Societatis*, *7*(3).

HERLAMBANG, F. S. (2023). *Analisis Perbandingan Antara Letter Of Credit Dan Telegraphic Transfer* Dalam Transaksi Perdagangan Internasional Pada PT Kayu Lima Utama (Doctoral dissertation, Universitas Diponegoro).

Indriani, P. (2022). Analisis *Letter of Credit* Sebagai Alat Jaminan Pembayaran Guna Mengurangi Risiko Kerugian Transaksi Ekspor Batubara Pada PT. Bukit Asam (Persero) Tbk. Analisis *Letter of Credit* Sebagai Alat Jaminan Pembayaran Guna Mengurangi Risiko Kerugian Transaksi Ekspor Baubara Pada PT. Bukit Asam (Persero) Tbk.

Khoiruddin, K. (2023). Studi Atas Fatwa Dsn-mui Terhadap Akad-akad Dalam *Letter of Credit* (L/c) Impor Dan Ekspor Syariah. *ASAS: Jurnal Hukum Ekonomi Syariah*, *3*(2).

Kriswandhany, N. (2014). *Analisis Perlindungan Hukum Bagi Para Pihak Dalam Transaksi Expor-Impor Dengan Menggunakan L/C (Letter Of Credit) Sebagai Alat Pembayaran* (Doctoral dissertation, University of Muhammadiyah Malang).

Maffuadi, M., & Khairani, K. (2020). Tinjauan Yuridis Terhadap Penggunaan *Letter of Credit* (L/C) Dalam Pelakasanaan Ekspor Impor Barang Di Indonesia. *Jurnal Ilmiah Mahasiswa Bidang Hukum Keperdataan*, *4*(2), 304-313.

Maulana, I. (2020). Aplikasi Akad Wakalah dalam *Letter of Credit* Bank Syariah Mandiri. *Jurnal Asy-Syukriyyah*, *21*(02), 175-193.

Maulani, I. E., Herdianto, T., Syawaludin, D. F., & Laksana, M. O. (2023). Penerapan Teknologi *Blockchain* Pada Sistem Keamanan Informasi. *Jurnal Sosial dan Teknologi*, *3*(2), 99-102.

Mita, D., Makhsun, A., & Pentiana, D. (2018). Tinjauan Atas Pelaksanaan Prosedur Penjualan Ekspor Dengan Menggunakan Sistem Pembayaran *Letter of Credit*. *Karya Ilmiah Mahasiswa*.

Munir, Y. F., Azahra, W. Y., & Putri, D. M. (2021, June). Kajian Kausal Teknologi *Blockchain* Dalam Auditpada Era Revolusi Industri 4.0. In *Prosiding National Seminar on Accounting, Finance, and Economics (NSAFE)* (Vol. 1, No. 2).

Nugraha, B. A., & Andraini, F. (2023). Perlindungan Hukum Terhadap Eksportir dan Importir dalam Transaksi Ekspor Impor Barang dengan Menggunakan L/C (*Letter of Credit*) Sebagai Alat Pembayaran. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam*, *5*(2), 1627-1646.

Pratiwi, L. L. (2022). Implementasi *Blockchain* Pada Akuntansi dan Audit di Indonesia. *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan*, *4*(6), 2185-2203.

Purba, E. L. (2022). Perlindungan Hukum Transaksi Bisnis Internasional dalam Perdagangan Ikan Kemasan dalam Proses Pembayaran *Letter of Credit* (Studi pada PT. Medan Tropical Canning & Frozen Industries).

Ridho, B. (2022). *Pengaruh Pembiayaan Letter Of Credit Terhadap Pendapatan Bank Syariah Mandiri Tahun 2015-2019* (Doctoral dissertation, UIN Raden Intan Lampung).

Rumengan, R. V. (2021). Perlindungan Hukum Bagi Para Pihak Terhadap Penggunaan *Letter of Credit* (L/C) Dalam Transaksi Perdagangan Internasional. *Lex Privatum*, *9*(3).

Safitriani, M., Abdurahman, N. H., Setiawan, I., & Abdullah, F. D. (2023). Penerapan Konsep Hybrid Contracts dalam Operasional Transaksi *Letter of Credit* Perdagangan Internasional di Bank Muamalat Indonesia. *Nuansa*, *16*(2), 131-141.

Santoso, N. P. L., Durachman, Y., Watini, S., & Millah, S. (2021). Manajemen Kontrol Akses Berbasis *Blockchain* untuk Pendidikan Online Terdesentralisasi. *Technomedia Journal*, *6*(1 Agustus), 111-123.

Subagja, A. D. (2020). *Letter of Credit* (L/C) Sebagai Cara Pembayaran yang Paling Aman dalam Transaksi Pembayaran Perdagangan Internasional/Ekspor-Impor.(Studi Kasus pada PT. San San Saudaratex Jaya). *International Journal of Demos*, *2*(1), 78-89.

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55-68.

Susanto, P. W., & Ashari, W. M. (2024). Penerapan Teknologi *Blockchain* pada Transaksi Online Shop. *Al Qalam: Jurnal Ilmiah Keagamaan dan Kemasyarakatan*, *18*(1), 654-670.

Tjung, Y. F. R. (2022). Kasus L/C Fiktif Bni: Penyalahgunaan *Letter Of Credit* Dalam Perdagangan Ekspor Impor Dalam Perspektif Tindak Pidana Pencucian Uang. *JISIP (Jurnal Ilmu Sosial dan Pendidikan)*, *6*(3).

Utami, I. P. A., Djuwityastuti, D., & Adiastuti, A. (2016). *Letter of Credit* (L/c) Sebagai Cara Pembayaran Transaksi Perdagangan Internasional Dalam Kerangka ASEAN Economic Community. *Privat Law*, *4*(1), 164496.

Widyana, I. G. K. P. (2023). *Tinjauan Yuridis Mengenai Pelaksanaan Ekspor Impor Yang Menggunakan Letter Or Credit* (Doctoral dissertation, Universitas Tadulako).

Yuliyanti, D. (2012). Sistem pembayaran *letter of credit* pada transaksi Ekspor tekstil pt. Dan liris Di Sukoharjo.