LEGAL BRIEF
ISSN 2722-4643 (Online) | 1979-522X (Print)
Volume 13, No. 2, 2024, pp. 267-276
Published by: IHSA Institute (Natural Resources Law Institute)

Arrangement of Blockchain Technology as an Effort to Prevent Payment Fraud via the Indonesian Standard Quick Response Code (Qris) Performed by Consumers in Electronic Transactions.

Abel Yehud Silalahi[1], Adlia Nur Zhafarina[2]

[1 2] Faculty of Economics and Social Affairs , Universites Jendral Achmad Yani , Yogyakarta, Indonesia

Abstract: This research discusses the use of blockchain technology as a solution to reduce the risk of fraud in electronic transactions using QRIS in Indonesia. With the development of information technology, cybercrime such as online fraud is increasing. However, existing regulations have not fully addressed this problem. The research method used is normative-empirical legal research, which combines literature study and interviews with QRIS users. The results show the need for better legal protection to protect consumers from fake QRIS and system vulnerabilities. The findings highlight that blockchain technology provides advantages in creating unparalleled transparency and security in electronic transactions, thus providing an effective solution in reducing the risk of fraud. Interviews with QRIS users also revealed their challenges and expectations regarding the use of QRIS, emphasizing the importance of public education on the correct use of QRIS as well as proactive law enforcement. This shows the importance of further exploration to create a fair digital transaction environment for consumers and businesses, as well as emphasizing cooperation between the government, regulatory agencies, and industry players in improving legal protection and public education regarding QRIS.

Keywords: Blockchain Technology, Electronic Transactions, Fraud, Legal Protection, QRIS

1. Introduction

Indonesia is a country of law that upholds the supremacy of law based on justice, as explained in Article 1 paragraph 3 of the 1945 Constitution. This is to create security and justice for all Indonesian people (Mukhtadir, 2022) .

Current technological developments make interaction between individuals or groups easier, increasing convenience in various aspects of life (Fitriani, 2014) . Current technological developments have become a basic need for society, especially in obtaining information via smartphones. This affects the modernization of social, cultural, economic, defense, security and law enforcement (Chumairoh, 2021) .

Information technology has become a primary need in everyday life through the use of devices such as smartphones and laptops, as well as applications such as Facebook, WhatsApp, Instagram and TikTok. The impacts are varied: positively, technology makes it easier to access information, supports education, and makes long-distance communication and online shopping easier. However, technology also has negative impacts such as increasing online crime, including online prostitution, gambling, data theft and fraud (Suhariyanto, 2012) . In Indonesia, protection of the public from technological crimes is regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (Wahyudi, 2013) .

Crime in Indonesia often occurs with varying views regarding its causes. Ineffective laws are considered to be one of the causes. Public understanding of crime needs to be improved with scientific disciplines that are appropriate to current developments, especially technology and information. Criminology is important to understand the causes and consequences of crime, such as fraud via social media (Gultom, 2022) .

Online transactions are increasingly common among people because of their con-

Correspondence:
Name: Abel Yehud Silalahi1
Email: abelyehuds@gmail.com

Received: May 25, 2024;
Revised: May 28 2024;
Accepted: Jun 07, 2024;
Published : Jun 30, 2024

venience, just by using online media such as cellphones. There are various online transaction applications that are safe and help people's activities, such as Dana, OVO, GoPay, ShopeePay, and QRIS (Admin Aptika, 2017) . QRIS is popular because of its convenience; simply scan the payment code. Its use has become widespread in stalls, supermarkets and various shops, making it easily accessible to many people.

Electronic money is a form of electronic money used for online payments via electronic devices such as smartphones. This electronic money is prepaid, meaning its value is stored in electronic media (Mahyuni & Setiawan, 2021) . Electronic payments make transactions easier without face to face. Bank Indonesia developed the QRIS standard as a single QR code for all digital transactions, accelerating digital financial inclusion in Indonesia (Tara & Sudiro, 2023) .

Even though QRIS makes things easier, the potential for fraud still exists. For example, a bakmie entrepreneur was tricked by consumers with fake QRIS, resulting in financial losses. Proof of payment turns out to be edited (Admin, 2022) . Fraud is a criminal act that must be held accountable. The perpetrator of a criminal act must fulfill the elements of the act he committed and the conditions need to be taken into account (Supriyono et al., 2022) . Electronic fraud can be reported to the Police, Bank Indonesia, OJK and other agencies. Criminal sanctions are regulated in Article 378 of the Criminal Code, with a maximum penalty of four years in prison for perpetrators who use deception to obtain unlawful profits (Mahyuni & Setiawan, 2021) .

QRIS has increased non-cash transactions in Indonesia since it was introduced by Bank Indonesia in February 2022. However, financial digitalization brings cyber risks, especially phishing. More than 356 thousand financial-related phishing attacks have been blocked in Indonesia since the start of this year, with the majority targeting payment systems. The increasing trend of online shopping is also attracting attention, as online stores are becoming profitable targets for cybercriminals. There have also been more than 20 thousand phishing attempts related to online banking in the country (Pramudita, 2023) .

Article 378 of the Indonesian Criminal Code does not cover online fraud in electronic transactions. The specific regulations are regulated in Law no. 19 of 2016 and Law no. 11 of 2008. The implementation of QR-Code as a payment system faces challenges in technological literacy and comprehensive regulations. Consumer rights have not been fully fulfilled, and supervision of payment service providers has not been optimal (Arsha Putra & Yustiawan, 2022; Noval et al., 2022) .

Law Number 19 of 2016 regulates information technology and electronic transactions, adapting to internet developments. Previously, cybercrime was handled using conventional law. Lack of regulation can cause losses (Kartiko, 2013) .

A gelato outlet in West Jakarta experienced a case of theft of 45 million through fake QRIS. The shop owner, Ristiana Eteng, discovered this after checking for a drop in revenue and posing as a customer to investigate. One of the employees was suspected of being the perpetrator by using his personal QRIS, even though the outlet had provided an acrylic-based QRIS (Noviansah, 2023) . This incident highlights the importance of improving the security of electronic transactions, with one proposed solution being to implement blockchain technology.

Blockchain is a distributed database technology for recording digital transactions safely and efficiently. It prevents double spending and other problems by providing a secure peer-to-peer transaction environment with low fees (Admin, 2019) .

In conventional financial transactions, a third party is needed, while QRIS is a payment tool. However, in blockchain, each transaction is recorded in a permanently linked block, increasing security because each block has a hash of the previous block (Munawar et al., 2023) . Electronic payments have positive but also negative impacts, such as increasing online fraud. An example is fake QRIS, a non-cash payment system in Indonesia, which can cause errors and harm the parties involved if intentional (Herryani, 2023) .

Blockchain improves communication efficiency and security and facilitates resource management. In financial transactions, the use of blockchain reduces the risk of fraud

and automatically records activities. As a new paradigm, blockchain offers a high level of security and supports business innovation. This research explores the use of blockchain to overcome fraud in payments via QRIS, locally and internationally, to increase understanding of blockchain solutions in reducing the risk of fraudulent electronic transactions.

With the growth of electronic transactions, the risk of fraud is also increasing, so there is a need for effective solutions to protect consumers and businesses.Blockchain technology can provide high security with transparency and non-manipulability of data, making it relevant to be applied in financial transactions.This research can help in developing measures to protect consumers and businesses in electronic transactions, which are increasingly important in today's digital era.With a deeper understanding of the regulation of blockchain technology, it can help in developing appropriate regulations to support the use of blockchain in financial transactions.

The theoretical and practical contributions of this research are to enrich the literature on electronic transactions and the application of blockchain technology in the context of transaction security and to provide guidance for related parties, such as payment technology companies and regulators, in developing policies that support the use of blockchain technology in electronic transactions.

This research has a specific objective of providing an in-depth understanding of the application of blockchain technology in preventing payment fraud through QRIS as well as a comparison with practices in several developed countries.

2. Research methods

This research uses normative-empirical legal research, examining regulations related to electronic transactions using QRIS. The relevant literature review covers consumer protection in QRIS transactions and the use of blockchain technology to prevent fraud in financial transactions. By referring to previous research, this study can provide a better understanding of efforts to counter payment fraud through QRIS using blockchain technology. This research combines normative analysis (literature review) and empirical research (interviews). Interviews were conducted directly to obtain primary data relevant to the research. The questions prepared were open-ended to allow for additional information that could support data analysis. In the interview process, information collected includes the experiences and views of business owners, cashiers, and MSME business owners regarding the use of QRIS in financial transactions. In addition, information was also collected on the challenges faced, the impact of using QRIS on businesses, as well as opinions and suggestions to improve the security of QRIS transactions and prevent fraud. Primary data was collected through structured interviews with QRIS users, including merchants, cashiers, and small and medium business owners. Secondary data includes primary, secondary, and tertiary legal documents. The analysis approach used is a qualitative approach. Data analysis is conducted by collecting relevant data from primary and secondary data sources, then analyzing it in detail. The analysis steps include data reduction or data selection, data presentation in the form of narrative text or graphs, and conclusion drawing to make accurate conclusions based on the data found. Data reduction, presentation and inference were done qualitatively based on information from primary and secondary sources.

3. Results and Discussion

3.1. Regulation of Blockchain Technology in Efforts to Prevent Payment Fraud via QRIS Committed by Consumers in Electronic Transactions

a. Regulation of Blokchain Technology According to Financial Service Authority (OJK) Regulations

OJK regulations regulate the use of blockchain in fintech financial services. Although OJK Regulations Number 13/PJOK.02/2007 and Number 37/POJK.04/2018 provide a framework, they are not sufficient as an adequate legal basis for blockchain de-

velopment in Indonesia. More comprehensive regulations are needed in accordance with national cyber law policies to ensure appropriate use and prevent misuse, taking into account societal values and the principles of legal certainty and freedom of choice of technology. (Lase et al., 2021) .

b. Regulation of Blockchain Technology According to the Criminal Code (KUHP) and the ITE Law

1) Regulation pf Blokchain Technology According to the Criminal Code Law

Blockchain technology influences criminal law in Indonesia. Although there are no specific regulations, several articles in the Criminal Code can be used. For example, Article 378 on Fraud applies to cases related to cryptocurrency, and Article 280 on Defamation to the spread of false information via blockchain. Other articles such as Articles 321, 362, 372, and 82 are also relevant in dealing with acts of network damage, embezzlement of digital assets, and abuse of power (Sofian & Pratama, 2021) .

Although there are no specific regulations for blockchain, the Criminal Code provides a legal basis for handling cases involving this technology. However, it is necessary to continue to consider and develop a more specific legal framework to respond to blockchain developments fairly and effectively.

Law Number 19 of 2016 regulates property rights in blockchain transactions, providing the relevant legal framework (Fajarianto et al., 2022) .

2) Regulation of Blockchain Technology According to the ITE Law

The Indonesian government recognizes the importance of blockchain technology in law, as reflected in the amendment to the ITE Law by Law Number 10 of 2020, providing a legal basis for the use of blockchain in contract transactions in Indonesia (Megawati et al., 2023) .

The ITE Law provides the legal basis for blockchain activities in Indonesia even though it does not directly regulate it. Several articles, such as Articles 28 and 29, can be used to deal with blockchain-related crimes. However, more specific regulations are needed to create legal certainty and consumer protection. For example, Minister of Communication and Information Regulation No. 3 of 2021 sets standards for implementing blockchain-based systems (Habiburrahman et al., 2022) .

3) Implementation of Case Studies Related to Fraudulent Acts Commited by Consumer Against Business Actors

Payments via QRIS pose a risk of fraud. This research involved three interviews with food business and shop owners, who offer QRIS services in city centers, despite being aware of risks such as fake barcodes or failed authentication (Rahmanto, 2019) .

Mrs. Onat, owner of the "Numani" food stall, experienced an incident where a consumer wanted to pay via QRIS in the amount of IDR 36,000.00 during lunch time. However, the QRIS transaction was not recorded. After several days, the consumer's girlfriend paid the previously unrecorded amount.

Using applications such as Dana for QRIS payments increases the risk of fraud due to lack of supervision from the OJK. In addition, weaknesses in the use of blockchain technology also exacerbate this problem. Developed countries are advancing blockchain systems to strengthen digital financial services and reduce the risk of fraud.

OJK must provide guidelines, regulations and training about QRIS and blockchain technology to business actors such as Mrs. Onat to prevent fraud and increase public trust in QRIS transactions.

Andre, a grocery store employee, experienced fraud via fake QRIS when a buyer paid IDR 50,000 via QRIS while Andre was standing guard at the cashier. Because he was sleepy, Andre did not check the transaction thoroughly and later discovered that the payment was not recorded. He admitted his mistake and had to compensate for the loss with his personal money.

Even though the nominal amount is small, this is an online fraud that must be handled fairly by all parties, including the government, law enforcement officials and the

community (Rahmad, 2019) . Hoefnagels quoted in (Nugroho & Yuniarlin, 2021) states that crime prevention can be done through criminal law, prevention without crime, and influencing public perception through mass media. These can be divided into criminal and non-criminal legal pathways. The criminal legal route is repressive by providing a deterrent effect, while the non-criminal legal route focuses more on prevention before an incident occurs.Dwi , owner of an MSME partner business, became a victim of fraud via QRIS when selling in front of a minimarket. The buyer used fake proof of payment, and Dwi's lack of thoroughness in checking payment notifications provided an opening for fraudsters, causing a loss of IDR 40,000. This fraud method is simple but effective because it takes advantage of the victim's negligence. Buyers may use image editing applications or screenshots of other transactions. This action violates Article 372 of the Criminal Code concerning fraud and Article 46 of the ITE Law regarding misuse of electronic information media.

Dwi's case highlights the importance of vigilance and education for business actors, especially MSMEs, in accepting payments via QRIS to prevent online fraud which can lead to financial losses. Steps such as careful checking of proof of payment and notifications are essential in preventing fraud. Business actors also need to increase their understanding of online fraud modes and report cases of fraud to the authorities for follow-up. Thus, fraud via QRIS can be prevented through education, vigilance and appropriate preventive measures. Article 28 Paragraph (1) of the ITE Law, although it does not specifically regulate fraud, regulates the occurrence of losses in electronic transactions which require the fulfillment of elements such as intent, spreading fake news, and consumer losses to be declared a violation (Fauzi & Primasari, 2018) .

4) Efforts to Overcome Payment Fraud Through QRIS Carried Out by Consumers in Elctronic Transactions

To respond to cases of fraud experienced by Ms. Onat, Andre, and Dwi , reporting is required to service providers or related institutions for fund recovery and guidelines from the OJK regarding the use of QRIS and blockchain technology. Training to increase understanding and awareness of online fraud is also important. Blockchain can increase the security of transactions without intermediaries, but regulatory and understanding challenges still need to be overcome, with the role of governments, regulators and financial institutions very crucial (Bahanan & Wahyudi, 2023) .

Andre can report the fraud to the authorities to recover funds . Training and education about checking transaction notifications can prevent future fraud. The government has issued regulations such as the Criminal Law, Consumer Protection Law, and ITE Law to tackle online fraud. Important steps include verifying site security, using a real account, and checking prices before transactions. Supervisory bodies such as Id-SIRTII/CC handle cybercrime. Consumer education, reporting, and employee training are expected to increase the security of online transactions and reduce fraud (Solim et al., 2019) .

Dwi needs to report the fraud to the authorities. MSME business actors need education about online fraud and transaction verification. Law enforcement involves both penal and non-penal policies, with constraints on resources and legal awareness. Synergy between the community, law enforcement officials and electronic transaction education is needed. Legal instruments must follow developments in information technology for a just and prosperous society (Kasiyanto & Jerri, 2017) . In Dwi's case , the first step was to report the fraud to the authorities. To prevent this, MSME business actors need to receive education about online fraud modes and how to verify transactions.

Law enforcement against online fraud needs to be strengthened through cooperation between the authorities, financial supervisory institutions and business actors. Increasing public awareness about online fraud modes and developing security technology such as blockchain is also important in reducing the risk and impact of online fraud.

Efforts to Overcome Payment Fraud Through QRIS Carried Out by Consumers in Electronic Transactions. Digitalization is renewing the way we interact, work and learn.

This enables easy and open access to information and services, and opens up limitless opportunities to connect people around the world (Nono Heryana et al., 2023) . Digitalization changes the way we interact, work, learn and carry out daily activities using digital technology. This opens up limitless new opportunities to connect people around the world and enables easy sharing of access to services and information (Wuryantai, 2013) .

The development of blockchain technology has been prominent in the digital era, especially after the introduction of Bitcoin. Awareness of its potential and benefits is increasing, with experts and business people creating digital currencies for various aspects of life. In the banking sector, blockchain has made financial transactions and the settlement of cross-border transactions easier. In the logistics sector, blockchain is used to safely and transparently record the journey of products from producer to consumer (Suryawijaya, 2023) .

Blockchain is used in various countries for secure digital identities and improving public services, such as electronic voting and humanitarian aid. The main challenge is to create regulations that support innovation while paying attention to consumer safety and protection. Increasing awareness and understanding of the potential of this technology is important for entrepreneurs, policy makers and society. Support from governments, research institutions and business people can encourage the growth of blockchain in the global digital economy. In vestment in education, progressive regulations, and collaboration between parties can bring positive changes in various aspects of global life (Pangestu, 2023) .

In Indonesia, QRIS is a popular choice for electronic transactions using QR codes. However, in other countries such as the US, China and Singapore, the trend of using cryptocurrency and blockchain technology as a payment method is increasing. As a comparison with other countries, here are the arrangements for *blockchain technology* in several developed countries:

c. Blockchain Regulations In The United States

In the US, blockchain is growing rapidly after Bitcoin's success as the first cryptocurrency to use it. This sparked interest in blockchain technology as it enables decentralized digital currencies. Developers and companies are starting to explore the potential of blockchain in various sectors, such as healthcare, digital identity, and supply chains (Gad et al., 2022) .

In the US, blockchain technology innovation continues to grow, with many companies and startups developing blockchain-based products for efficiency, transparency and security. Large institutions and banks are also conducting trials to increase the efficiency of financial transactions (Ali et al., 2020) . Although this technology is still relatively new in the United States and legal regulations are still being developed, some federal or state government agencies already have their own regulations governing certain aspects of blockchain technology.

1) Securities and Exchange Commission (SEC)

The Securities and Exchange Commission (SEC) oversees the US stock market, protects investors, and regulates cryptocurrencies. This determines whether a digital coin is a security, requiring registration and compliance with rules (Admin, 2024; Legge, 2024) .

2) Commodity Futures Trading Commission (CFTC)

The Commodity Futures Trading Commission (CFTC) is a US government agency that oversees and regulates commodity markets, ensuring transparency, li-

quidity and investor protection. It monitors commodity futures and financial derivatives, including cryptocurrency contracts such as Bitcoin futures (Agency, 2024; Team, 2024) .

3) Financial Crimes Enforcement Network (FinCEN)

FinCEN is a US financial agency that collects and analyzes financial data to combat money laundering and terrorist financing. It regulates cryptocurrency transactions to prevent illegal activities and ensure the integrity of the US financial system (Administrator, 2017) .

4) Internal Revenue Service (IRS)

The Internal Revenue Service (IRS) is a US government agency tasked with collecting taxes and enforcing tax regulations. They ensure transactions with crypto assets comply with tax regulations. The IRS also conducts audits of crypto transactions to ensure compliance with tax laws (LeBaube, 2024; Scott, 2023) .

5) Federal Regulations

Some parts of the United States have separate regulations on blockchain technology, so there are no uniform regulations across states. For example, in New York, there is a BitLicense regulation which is a special license for companies operating in the virtual currency industry (De Filippi et al., 2020) .

d. Blockchain Regulations In China

The Chinese government has implemented strict regulations on blockchain technology, especially regarding cryptocurrencies. It banned cryptocurrency trading and ICOs in 2017 to control market speculation and reduce financial risks. Additionally, there are regulations to monitor and regulate the use of blockchain in certain sectors such as finance, banking, and e-commerce. The government is also increasing supervision of blockchain service providers to prevent illegal activities (Wang & Chen, 2019)

e. Blockchain Regulations In Singapore

Singapore supports blockchain innovation with a progressive approach, driven by the Monetary Authority of Singapore (MAS). They issued guidelines on the use of blockchain and cryptocurrencies in 2019 and continue to monitor developments to adjust regulations (Pratama, 2024) .

f. Blockchain Setup Recommendations

Blockchain regulations vary in the US, China, Singapore and Indonesia. The US opens up, China bans crypto, Singapore supports development with strict regulations, and Indonesia balances innovation and compliance (Amiruddin et al., 2023) .

4. Conclusion

Blockchain technology enhances the security of electronic payments by preventing fraudulent QRIS transactions. It ensures transparency and tamper-proof records. Some limitations in this research method that may affect the generalizability of the findings include the limited sample size, the specific context of the study, and limited access to primary and secondary data. These limitations need to be taken into account to understand that the research findings may not be directly applicable in general to a broader population or context. Indonesian laws, including criminal law, IT law, business law, and OJK regulations, provide a legal framework for handling blockchain-related cases. Although there are no specific regulations regarding blockchain, existing laws provide a relevant legal framework. Recommendations for future research based on the results of

this study include expanding the sample size for better representativeness, in-depth study of the implementation of blockchain technology in QRIS transactions, broader interviews with various related parties, expansion of research to other industry sectors, and further study of the legal and security aspects of electronic transactions using QRIS to provide more concrete recommendations for fraud prevention. Combating fraudulent transactions can be done through criminal and non-criminal channels, with a focus on punitive and preventive measures. The contribution of this research is to provide a more in-depth understanding of the regulation of blockchain technology in payment fraud countermeasures through QRIS in electronic transactions. The implications of this research include increasing public legal awareness related to cashless banking services, strengthening legal protection in digital transactions, utilizing blockchain technology to ensure transaction integrity, as well as crime prevention efforts through concrete measures. Thus, this research can provide a foundation for further policies and actions in improving security and trust in electronic transactions using QRIS.

References

Ali, O., Ally, M., Clutterbuck, & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management*, *54*, 102199. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2020.102199

Amiruddin, Yazid, S., Anggorojati, B., Setiawan, H., & Purwoko, R. (2023). *Tinjauan strategis keamanan siber Indonesia : teknologi cloud dan tata kelola data* (D. F. Priambodo & S. U. Sunaringtyas (eds.)). Politeknik Siber dan Sandi Negara Press.

Aptika. (2017, June 29). *Sistem e-Commerce dan Perlindungan Konsumen*. Direktorat Jendral Aplikasi Informatika. https://aptika.kominfo.go.id/2017/06/sistem-e-commerce-dan-perlindungan-konsumen/

Arsha Putra, I. P. R., & Yustiawan, D. G. P. (2022). Aspek Perlindungan Hukum Terhadap Nasanah Atas Penyelenggaraan E-Payment Berbasis QR-Code. *KERTHA WICAKSANA*, *16*(2), 99–107. https://doi.org/10.22225/kw.16.2.2022.99-107

Azmi, M. U., Sunarmi, S., Azwar, T. K. D., & Sutiarnoto, S. (2023). Risiko Hukum Penggunaan Smart Contract pada Ethereum di Indonesia. *Locus Journal of Academic Literature Review*, *2*(3), 235–242. https://doi.org/10.56128/ljoalr.v2i3.140

Bahanan, M., & Wahyudi, M. (2023). Analisis Pengaruh Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Pada Perbankan Syariah. *I'THISOM : Jurnal Ekonomi Syariah*, *2*(1), 43–54. https://ejournal.staialutsmani.ac.id/index.php/ithisom/article/view/42

Chumairoh, I. N. (2021). *Tinjauan Pasal 28 Uu Ite Dan Hukum Pidana Islam Terhadap Penipuan Arisan Online*. Universitas Islam Negeri Walisongo.

CNN Indonesia. (2019, August 15). *Blokchain Disebut Bisa Jadi Solusi Masalah Perbankan*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20190815093816-185-421509/blockchain-disebut-bisa-jadi-solusi-masalah-perbanka

CNN Indonesia. (2022, July 21). *Pengusaha Bakmi Jadi Korban Modus Penipuan QRIS*. CNN Indonesia. https://www.cnnindonesia.com/ekonomi/20220721180653-78-824540/pengusaha-bakmi-jadi-korban-modus-penipuan-qris/amp

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*, 101284. https://doi.org/https://doi.org/10.1016/j.techsoc.2020.101284

Fajarianto, E. R., Zulfikar, P., & Mulyadi, E. (2022). Tinjauan Yuridis Penggunaan Blockchain-Smart Contract Dalam Transaksi Non-Fungible Token (Nft) Pada Pt. Saga Riung Investama. *Jurnal Pemandhu*, *3*(2), 84–97. https://ejournal.unis.ac.id/index.php/JM/article/view/2997

Fauzi, S. N., & Primasari, L. (2018). Tindak Pidana Penipuan dalam Transaksi di Situs Jual Beli Online (E-Commerce). *Jurnal Recidive* , *7*(3), 250–261. https://jurnal.uns.ac.id/recidive/article/view/40603

Federal Register. (2024). *Commodity Futures Trading Commission*. Federal Register. https://www.federalregister.gov/agencies/commodity-futures-trading-commission

FinCEN. (2017, August 22). *Advisory to Financial Institutions and Real Estate Firms and Professionals*. Financial Crimes Enforcement

Network. https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a003

Fitriani. (2014). *Perkembangan Teknologi, Informasi, dan Komunikasi*. Pemerintah Aceh. https://acehprov.go.id/berita/kategori/serba-serbi/80-perkembangan-teknologi-informasi-dan-komunikasi

Gad, A. G., Mosa, D. T., Abualigah, L., & Abohany, A. A. (2022). Emerging Trends in Blockchain Technology and Applications: A Review and Outlook. *Journal of King Saud University - Computer and Information Sciences*, *34*(9), 6719–6742. https://doi.org/10.1016/j.jksuci.2022.03.007

Gultom, K. F. (2022). Analisis Kriminologi Terhadap Pelaku Tindak Pidana Penipuan Dengan Modus Arisan Online (Studi Pada Kepolisian Resor Kota Besar Medan). *Jurnal Ilmiah Mahasiswa Hukum [JIMHUM]*, *2*(1), 1–17. https://jurnalmahasiswa.umsu.ac.id/index.php/jimhum/article/view/1180

Habiburrahman, M., Muhaimin, & Atsar, A. (2022). Perlindungan Hukum Bagi Pengguna Transaksi Cryptocurrency Di Indonesia. *Jurnal Education And Development*, *10*(2), 697–706. https://journal.ipts.ac.id/index.php/ED/article/view/3896

Herryani, M. R. T. R. (2023). Enhancing Legal Protection for Digital Transactions: Addressing Fraudulent QRIS System in Indonesia. *Rechtsidee*, *11*(1), 1–12. https://doi.org/10.21070/jihr.v12i1.990

HSB. (2024). *Securities and Exchange Commission*. HSB Invest in Time. www.hsb.co.id/glosarium/s/securities-and-exchange-commission

Indah, S. C. M. (2014). *Perlindungan Korban (Suatu Perspektif Viktimologi dan Kriminologi* . Kencana.

Kartiko, G. (2013). Pengaturan Terhadap Yurisdiksi Cyber Crime Ditinjau dari Hukum Internasional. *Rechtidee*, *8*(2), 136–153. https://doi.org/10.21107/ri.v8i2.695

Kasiyanto, A., & Jerri, T. (2017). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Yang Dilakukan Melalui Media Elektronik. *De Facto* , *4*(2), 64–86. https://jurnal.pascasarjana.uniba-bpn.ac.id/index.php/jurnaldefacto/article/view/51

Lase, S. M. N., Adinda, A., & Yuliantika, R. D. (2021). Kerangka Hukum Teknologi Blockchain berdasarkan Hukum Siber di Indonesia. *Padjadjaran Law Review*, *9*(1), 1–20. https://jurnal.fh.unpad.ac.id/index.php/plr/article/view/500

LeBaube, R. A. (2024). *9 Assisting Taxpayers in Meeting Their Obligations Under the Law*. IMF ELibrary. https://www.elibrary.imf.org/configurable/content/book$002f9781557753175$002fch009.xml?t:ac=book%24002f9781557753175%24002fch009.xml

Legge, M. (2024, February 12). *SEC & Crypto: How Does The SEC Regulate Crypto?* Koinly. https://koinly.io/blog/sec-crypto/

Mahyuni, L. P., & Setiawan, I. W. A. (2021). Bagaimana QRIS menarik minat UMKM? sebuah model untuk memahani intensi UMKM menggunakan QRIS. *Forum Ekonomi*, *23*(4), 735–747. https://journal.feb.unmul.ac.id/index.php/FORUMEKONOMI/article/view/10158

Megawati, L., Wiharma, C., & Hasanudin, A. (2023). Peran Teknologi Blockchain Dalam Meningkatkan Keamanan Dan Kepastian Hukum Dalam Transaksi Kontrak Di Indonesia. *Jurnal Hukum Mimbar Justitia*, *9*(2), 410–435. https://doi.org/10.35194/jhmj.v9i2.3856

Mukhtadir, M. A. (2022). *Analisis Hukum Terhadap Penerapan Sanksi Tindak Pidana Penipuan Arisan Online Di Kota Makassar* [Universitas Bosowa]. https://repository.unibos.ac.id/xmlui/bitstream/handle/123456789/2721/2022 MUH AWALUL MUKHTADIR 4518060142.pdf?sequence=1&isAllowed=y

Munawar, Z., Putri, N. I., Iswanto, & Widhiantoro, D. (2023). Analisis Keamanan Pada Teknologi Blockchain. *Infotronik*, *8*(2), 67–79. https://doi.org/10.32897/infotronik.2023.8.2.2062

Nono Heryana, M. K., Dr. Muhammad Fuad, S. E. M. M., Dr. Titi Nugraheni, S. E. M. M. M. S., Darnilawati, S. E. M. S., Meida Rachmawati, S. E. M. M. M. H., Fadli Agus Triansyah, S. P., Adhi Susano, M. K., Dr. Siska Yulia Defitri, S. E. M. S., Dr. M. Subhan Iswahyudi, M. E. P. C. C. A., & Puteri Syarifah Al-Sakinah, S. E. M. M. (2023). *UMKM Dalam Digitalisasi Nasional*. Cendikia Mulia Mandiri. https://books.google.co.id/books?id=SijJEAAAQBAJ

Noval, M., Nofrial, R., & Nyrkhotijah, S. (2022). Analisis Yuridis Proses Penyelesaian Tindak Pidana Terhadap Pelaku Penipuan Melalui Pembayaran Elektronik Untuk Mewujudkan Perlindungan Hukum. *Ilmiah Hukum Dan Hak Asasi Manusia (HAM)*, *2*(1), 29–37. https://doi.org/https://doi.org/10.35912/jihham.v2i1.1579

Noviansah, W. (2023, October 11). *Viral Karyawan Gelato Tilap Duit Toko Rp 45 Juta Bermodal QRIS Palsu*. DetikNews. https://news.detik.com/berita/d-6977199/viral-karyawan-gelato-tilap-duit-toko-rp-45-juta-bermodal-qris-palsu

Nugroho, R. A., & Yuniarlin, P. (2021). Pelaksanaan Jual Beli Secara Online Berdasarkan Perspektif Hukum Perdata. *Media of Law and Sharia*, *2*(2), 190–206. https://doi.org/10.18196/mls.v2i2.11488

Pangestu, D. A. (2023). *Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Syariah*. Universitas Islam Indonesia.

Pemerintah Indonesia. (1999). *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen*.

Pramudita, B. (2023, April 11). *Penipu Manfaatkan QRIS, Indonesia Catat Ratusan Ribu Kasus Pada Tahun 2022*. Arketeers. https://www.marketeers.com/penipu-manfaatkan-qris-indonesia-catat-ratusan-ribu-kasus-pada-tahun-2022/

Pratama, Y. A. (2024). *Legalitas Hukum Coin Cryptocurrency Sebagai Alat Pembayaran Di Indonesia*. Universitas Islam Indonesia.

Rahmad, N. (2019). Kajian Hukum terhadap Tindak Pidana Penipuan Secara Online. *J-HES: Jurnal Hukum Ekonomi Syariah*, *3*(2), 103–117. https://journal.unismuh.ac.id/index.php/jhes/article/view/2419

Rahmanto, T. Y. (2019). Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. *Jurnal Penelitian Hukum De Jure*, *19*(1), 31–52. https://doi.org/10.30641/dejure.2019.V19.31-52

Rohid, D. (2024). Implikasi Hukum Dari Penggunaan Teknologi Blockchain Dalam Bisnis Di Indonesia. *Tugas Mahasiswa Hukum*, *1*(2), 1–13. https://coursework.uma.ac.id/index.php/fakum/article/view/685

Scott, M. P. (2023, August 16). *What's Wrong With the American Tax System?* Investopedia. https://www.investopedia.com/articles/personal- finance/082415/whats-wrong-american-tax-system.asp

Sofian, A., & Pratama, B. (2021). Tindak Pidana Mata Uang dalam Konteks Hukum Pidana dan Hukum Siber. *Jurnal Hukum Pidana Dan Kriminologi*, *2*(2), 49–63. https://doi.org/10.51370/jhpk.v2i2.56

Solim, J., Rumapea, M. S., Agung Wijaya, Manurung, B. M., & Lionggodinata, W. (2019). Upaya Penanggulangan Tindak Pidana Penipuan Situs Jual Beli Online Di Indonesia. *Jurnal Hukum Samudra Keadilan*, *14*(1), 97–110. https://doi.org/10.33059/jhsk.v14i1.1157

Suhariyanto, B. (2012). *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi Pengaturan Dan Celaan Hukumnya*. Pt Raja grafindo Perseda.

Supriyono, Sholichah, V., & Irawan, A. D. (2022). Urgensi Pemenuhan Hak-Hak Konstitusional Warga Negara Era Pandemi Covid-19 di Indonesia (The Urgency of Fulfilling the Constitutional Rights of Citizens in the Era of the Covid-19 Pandemic in Indonesian). *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia (Jihham)*, *1*(2), 55–66. https://doi.org/10.35912/JIHHAM.v1i2.909

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. https://doi.org/10.21787/jskp.2.2023.55-68

Tara, I. K. K. B., & Sudiro, A. (2023). Perlindungan Hukum Konsumen Terhadap Pengguna Qris dan Penanganan Penipuan dalam Bertransaksi. *UNES Law Review*, *6*(2), 4581–4588. https://review-unes.com/index.php/law/article/view/1498

Team. (2024). *The Commission*. CFTTC: Commodity Futures Trading Commission. https://www.cftc.gov/About/AboutTheCommission

Wahyudi, D. (2013). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime di Indonesia. *Jurnal Ilmu Hukum Jambi*, *4*(1), 98–113. https://media.neliti.com/media/publications/43295-ID-perlindungan-hukum-terhadap-korban-kejahatan-cyber-crime-di-indonesia.pdf

Wang, J., & Chen, L. (2019). Regulating Smart Contracts and Digital Platforms: A Chinese Perspective. In L. A. DiMatteo, M. Cannarsa, & C. Poncibò (Eds.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (pp. 183–210). Cambridge University Press. https://doi.org/DOI: 10.1017/9781108592239.010

Wuryantai, A. E. W. (2013). Digitalisasi Masyarakat: Menilik Kekuatan dan Kelemahan Dinamika Era Informasi Digital dan Masyarakat Informasi. *Jurnal ILMU KOMUNIKASI*, *1*(2), 131–142. https://doi.org/10.24002/jik.v1i2.163