



DOI: <https://doi.org/10.38035/gijlss.v4i3>
<https://creativecommons.org/licenses/by/4.0/>

Police Transformation in the Crypto Era in Handling Token-Based Money Laundering in Indonesia

Indah Hartantiningrum^{1*}, Eva Achjani Zulfa², Chairul M. Setyabudi³, Ahmad Ibrahim Badry⁴

¹Universitas Indonesia, Jawa Barat, Indonesia, indah.hartantiningrum@ui.ac.id

²Universitas Indonesia, Jawa Barat, Indonesia

³Universitas Indonesia, Jawa Barat, Indonesia

⁴Universitas Indonesia, Jawa Barat, Indonesia

*Corresponding author: indah.hartantiningrum@ui.ac.id¹

Abstract: The purpose of this study is to analyze how the transformation of the police force in Indonesia can be carried out to address token-based money laundering, as well as provide policy recommendations that can improve the effectiveness of law enforcement in the context of the development of crypto technology. Adopt a post-positivism paradigm and a qualitative approach to explore the transformation of the police in handling token-based money laundering in Indonesia. The data collected will be analyzed using qualitative analysis techniques, including coding and thematic analysis, to find relevant key patterns and themes. The results of the study show that the main challenges in enforcing the law against crypto-based money laundering in Indonesia include a lack of insight into blockchain technology and cryptocurrencies, inadequate policies, and difficulties in tracking transactions due to the decentralized nature and anonymity of digital assets. To address this problem, it is necessary to increase the technological capacity of law enforcement officers, develop specially trained units, and implement stricter regulations. In addition, community empowerment through education and training for police officers is essential to improve competence in detecting suspicious transactions. With these strategic steps, it is hoped that cybersecurity can be more guaranteed and the digital asset ecosystem in Indonesia will become more transparent and responsible.

Keywords: cryptocurrency, money laundering, law enforcement, blockchain technology, policing transformation.

INTRODUCTION

Changes to the international monetary system have occurred due to the emergence of blockchain technology and digital currencies. Cryptocurrencies, as one of the main innovations in the financial world, offer various advantages, such as transaction speed, cost efficiency, and higher privacy than traditional financial systems (Sajidin, 2021). The crypto-based money laundering process has different characteristics than traditional money laundering (Nurcholis et al, 2022). The use of tokens and untraceable transactions becomes a loophole for criminals

to hide illegal sources of funds. In this context, police transformation is urgently needed so that law enforcement officials can reduce the threats that arise along with the development of this new technology. This study aims to analyze how the police transformation deals with token-based money laundering and provide recommendations to improve the prevention of this crime in Indonesia.

Cryptocurrency token-based money laundering is one of the increasingly rampant forms of financial crime (Lumaing et al, 2024). Actors can take advantage of the decentralized, anonymous, and hard-to-trace nature of cryptocurrencies to hide the origin of funds derived from illegal activities (Windani, 2023). This is a serious concern for law enforcement, especially the police, in combating and ultimately eliminating money laundering. According to data from Chainalysis, in 2021 there was a 30% increase in the volume of money laundering involving cryptocurrencies, reaching a value of around 8.6 billion US dollars (Chynalysis Team, 2022). This shows that cryptocurrency token-based money laundering has become a serious threat to global financial stability (Kepli & Zulhada, 2019).

History records several major cases involving cryptocurrencies and money laundering. In 2014, there was a theft of 850,000 Bitcoins which at the time was equivalent to 500 million US dollars from Mt (Herman et al, 2023). Gox, the largest Bitcoin trading company based in Japan. In the same year, the Islamic State of Iraq and Syria (ISIS) terrorist group announced that it was raising funds through Bitcoin for its terrorist organization and activities (US Department of Justice, 2022). These cases show how cryptocurrencies can be misused for illegal purposes, and highlight the need for stricter law enforcement.

In Indonesia, the crypto token business phenomenon is also growing, with many public figures involved in the launch of their own tokens. This creates new challenges for law enforcement authorities in supervising and regulating such activities. Although crypto assets in Indonesia are not positioned as official currencies, many other countries have recognized and legitimized cryptocurrencies as a means of payment, while developing policies to prevent misuse, especially in money laundering.

Digital transformation is a process of change and improvement in organizations, businesses, and industries through the application and utilization of digital technology (Kraus et al, 2021). The application of technology is at the core of enforcement-related digital transformations such as data processing and analysis, mobile applications, the Internet of Things (IoT), cloud computing, and blockchain technology. The importance of strengthening the role of the police through digital transformation in this era presents many new challenges for the world of security and law enforcement.

Polyfiation, as a process and practice carried out by the police in maintaining public security and order, must adapt to technological developments and the emergence of digital crime. In this context, the police must not only focus on law enforcement against conventional crimes, but also must develop strategies to deal with technology-based crimes (Jatna et al, 2024). Some important aspects of modern policing include crime prevention, law enforcement, and public service.

Modern policing practices have evolved in response to the proliferation of information and communication technologies. Policing in the context of digital crime requires significant institutional change. By adopting new technologies, building partnerships with communities, and developing specialized units to deal with cybercrime, the police can be more effective in maintaining security and order in the digital age (Setyawan et al, 2024). But today's problems require ethical solutions and are carefully considered if we are to keep people's rights intact.

The Transnational Organized Crime (TOC) theory refers to a form of offense classified as organized crime, where its definition and definition continue to evolve with the changing times, especially in the 20th century (Miraglia et al, 2012). The UN Convention on the Eradication of Crime TOC published in 2003 emphasizes the importance of defining organized

criminal groups to facilitate law enforcement, provided that the group consists of three or more people operating across countries. In this context, law enforcement is defined as the process of realizing the will of the law to become a reality, where law enforcement is expected to uphold the values of truth and justice. Legal obedience, which is closely related to legal awareness, reflects the relationship between awareness and obedience, where legal obedience is an obligation to be carried out.

Social transformation, which involves changes in social structures and norms, also contributes significantly to our knowledge of how police operate in the crypto age, where information and communication technologies create interconnected societies. To combat crimes such as token-based money laundering, which is more common in this era of the fourth industrial revolution, contemporary policing must embrace new technologies such as artificial intelligence and the internet of things (Bower & Johson, 2024). The theory of social networks by Castells highlights the importance of social interaction mediated by information technology, which is the basis for community policing in the face of crime challenges in the digital age (Sulliva, 2023).

According to Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes, some of its early works, such as legal crypto assets as digital commodities, can become illegal if used for this purpose. Offenders can then be found and prosecuted (Sari et al, 2024). Although big data-based predictive policing models can improve crime prevention, challenges such as environmental stigmatization, personal data protection, and community privacy policies need to be addressed in order for police to remain effective and ethical in serving the community (Ayu, 2023).

This research contributes to the development of a study of the transformation of the police in Indonesia in dealing with money laundering based on crypto assets, especially transactions that utilize tokens and blockchain technology. The contribution of research lies in the integration of technological, institutional, regulatory, and law enforcement capacity aspects into the Indonesian context. Different from studies that generally discuss cyber policing strategies in general, this study contextualizes the need for police transformation to the characteristics of crypto transactions that are cross-border, pseudonymous, and based on blockchain technology. Based on this approach, the study formulated recommendations that include increasing investigator capacity, strengthening inter-agency coordination, utilizing blockchain analysis technology, and adjusting the regulatory framework. Thus, this study does not claim to create an entirely new model of policing, but offers an integrative framework that can be the basis for strengthening the Indonesian police's response to crypto asset-based money laundering.

METHOD

Police Transformation in Handling Token-Based Money Laundering

The transformation of the police in Indonesia in dealing with token-based money laundering in the crypto era faces various complex problems. First, the lack of proper knowledge and understanding is a major obstacle related to blockchain technology (Imelda et al, 2022) and cryptocurrencies (Kawengian, 2024). Many police officers are not trained to understand how these systems work, making it difficult for them to detect and investigate money laundering cases involving digital assets. Without a deep understanding, law enforcement efforts become less effective and potentially lead to the loss of important evidence trails. Second, current regulations are still not fully adequate to deal with cryptocurrency-related crimes. Although Indonesia has issued several regulations related to the use of digital assets, there are still many legal loopholes that can still be exploited by criminals. For example, controversy over the legitimacy of cryptocurrencies (Firmansyah & Arifin, 2024) as a medium of exchange or assets for investment purposes (Putri et al, 2024) can cause difficulties in law

enforcement (Sholihah & Yazid, 2023). This creates challenges for the police in carrying out appropriate legal action against violations that occur.

Third, the decentralized nature and anonymity inherent in cryptocurrencies (Lumaing, et al, 2024) make tracking transactions extremely difficult (Susanto & Afifah, 2024). Criminals can easily hide their identities and divert funds through various platforms and digital wallets, thus hampering law enforcement's ability to identify possible sources of money. In this context, the police need to develop new methods and technologies to effectively monitor and analyze cryptocurrency transactions. Fourth, the lack of collaboration between law enforcement agencies and the private sector, including cryptocurrency service providers, is also a problem (Aini & Lubis, 2024; Munajat & Yusuf, 2024). Many companies engaged in cryptocurrency have no obligation to report suspicious transactions to the authorities, thus hampering prevention and enforcement efforts. Closer cooperation between the police and private sector involvement essential to create a more transparent and responsive reporting system to potential money laundering.

An analysis of the compatibility of the theory with field data in the context of token-based money laundering in Indonesia shows that various theories can explain this phenomenon well. First, according to money laundering theory, there are three steps in this process: placement, layering, and integration (Jaya, et al, 2020; Pase, et al, 2020). Field data shows that token-based money laundering practices in Indonesia follow this pattern, where blockchain technology and the anonymity of crypto transactions make the laundering process more difficult to trace. This is in line with the fact that the police face difficulties in detecting illegal sources of funds that have gone through various stages of laundering in the digital system.

In addition, the Transnational Organized Crime Theory is also proven to be in accordance with existing data. Money launderers often use global networks and take advantage of regulatory differences in each country to launch their actions (Lampe, 2021). The data shows a lack of international cooperation in the investigation of crypto-based transactions, confirming the importance of a cross-border approach in tackling digital crime. This theory supports the need for closer collaboration between countries to address the challenges facing law enforcement in the crypto age.

Law Enforcement Theory highlights the importance of training (Makogon et al, 2020) and capacity building for law enforcement officials (Violanti et al, 2019). Field data shows that many police officers are still undertrained in understanding blockchain technology and cryptocurrencies, so law enforcement against these crimes is weak. This theory reinforces the argument that increased knowledge and skills among law enforcement are essential to deal with the challenges posed by digital crime. In this regard, the Social Transformation Theory is also relevant, as the adoption of cryptocurrencies has changed the way financial transactions are conducted, which has an impact on the transformation of policing methods (Setiadarma et al, 2024). The data supports this theory by showing that police must adapt their approach to changing technological developments. This shows that the police need to adapt to remain effective in handling increasingly complex crimes.

Finally, Social Network Theory and Cybercrime Theory also provide important insights (Ashady, 2024; Harianto, 2019). Token-based money laundering crimes are often carried out through complex social networks, and field data suggests that police need to build intelligence systems based on social network analysis to identify criminals. Additionally, crypto technology facilitates cybercrime with a high level of anonymity, and data shows that these crimes are on the rise as the use of digital assets in illegal transactions increases.

In the rapidly growing digital era, technology-based crimes are increasingly sophisticated and difficult to identify. The inability of law enforcement officers in Indonesia to keep up with technological developments is a big problem, especially related to blockchain and cryptocurrencies (Setiawan et al, 2023). Many members of the police force do not have a deep

understanding of this technology, so they have difficulty detecting suspicious transactions that could be linked to illegal activities, such as terrorist financing and illegal money laundering. This unpreparedness is a loophole that cybercriminals use to hide their fund flows through hard-to-trace crypto transactions.

One of the factors that exacerbates this condition is inadequate cryptocurrency regulation in Indonesia (Widjaja, 2019). Although the government has issued various policies related to digital assets, there are still many legal loopholes that can be exploited by irresponsible parties. The lack of clear rules on how crypto transactions should be monitored and reported has made it difficult for law enforcement officials to crack down on criminals who use digital currencies for illegal activities. Existing regulations have not been able to accommodate the complexity of decentralized and anonymous blockchain technology, so many cases of crimes involving cryptocurrencies cannot be effectively acted upon.

The decentralized and anonymous nature of cryptocurrency transactions is another challenge in law enforcement efforts (Widyatmoko, 2024). In contrast to conventional banking transactions that have a clear administrative footprint and can be supervised by financial authorities, crypto transactions take place on a global network that has no central authority. This makes it very difficult to track the flow of funds, especially when criminals use techniques such as mixing services or privacy coins designed to obscure the origin of funds (Putri et al, 2023). Without adequate technical skills and tools, law enforcement officials struggle to gather enough evidence to uncover and take action against criminals. Additionally, the lack of collaboration between the government and the private sector further hampered law enforcement efforts in dealing with crimes involving cryptocurrencies. Cryptocurrency service providers in Indonesia, such as digital asset exchanges and crypto wallet providers, do not have a clear obligation to report suspicious transactions to the authorities. As a result, law enforcement officials often do not have enough information to conduct a comprehensive investigation. In fact, collaboration with the private sector is essential to create stricter surveillance mechanisms and improve the effectiveness of suspicious activity detection.

To overcome these challenges, strategic steps involving various parties are needed. First, increasing the capacity and understanding of technology among law enforcement officials must be a top priority. Training programs and collaborations with experts in the field of blockchain technology can help them understand how cryptocurrencies work as well as the methods that can be used to track suspicious transactions (Albshaier et al, 2024). With better knowledge, police officers will be better prepared to deal with digital-based crime.

Second, regulations related to cryptocurrencies should be strengthened to better accommodate technological developments and prevent the misuse of digital assets for illegal activities. Governments need to develop stricter policies regarding reporting obligations for cryptocurrency service providers as well as set higher security standards for digital asset transactions. With clearer and more comprehensive regulation, existing legal loopholes can be minimized, reducing the opportunities for criminals to abuse the system (Falk & Hammer, 2023).

Third, tracking crypto transactions should be strengthened by leveraging more advanced technologies, such as blockchain analytics (Javaid et al, 2023) and artificial intelligence (Tairov & Stefanova, 2024). Some countries have adopted special software that is capable of detecting suspicious transaction patterns as well as identifying relationships between different crypto wallet addresses. Indonesia also needs to develop or adopt similar technology so that law enforcement officials can work more effectively in tracking suspicious money flows.

Fourth, cooperation with the private sector should be enhanced through regulations that require cryptocurrency service providers to report suspicious activity to the authorities. With stricter reporting mechanisms, law enforcement officials will have faster access to information that can help in the investigation process. In addition, this collaboration can also create a safer

ecosystem for digital asset users, reduce the risk of fraud, and increase public trust in blockchain technology. In the midst of an ever-growing digital era, law enforcement officials in Indonesia must be able to adapt to technological changes to maintain security and order in cyberspace. By improving technology understanding, strengthening regulations, adopting more advanced tracking technologies, and building closer cooperation with the private sector, cryptocurrency-related law enforcement challenges can be addressed more effectively. These measures will not only help eradicate digital crime, but also strengthen the digital asset ecosystem in Indonesia to be more transparent and responsible.

The challenge in dealing with cryptocurrency-based money laundering in Indonesia requires strengthening the capacity of law enforcement officials through intensive training on blockchain systems and crypto asset tracking mechanisms, so that they can be more effective in detecting illegal activities. Cryptocurrency-related regulations need to be updated to provide legal certainty and narrow loopholes for criminals, while increased international cooperation and collaboration with the private sector, such as cryptocurrency exchange platforms, are essential to strengthen efforts to investigate and detect suspicious transactions. In addition, the use of AI-based analytics technology and big data should be improved to help authorities automatically recognize suspicious transaction patterns and conduct more in-depth analysis of digital crime activities.

Policies and Strategies

Law Enforcement Policy

Emerging threats in the field of law enforcement have been presented by blockchain technology and cryptocurrencies in recent years, especially in an effort to deal with crypto-based money laundering cases in Indonesia. Amid the widespread use of cryptocurrencies, effective regulation is essential so that the use of this technology is not misused for illegal activities. Therefore, strong and structured law enforcement policies are needed to address the threat of money laundering through digital assets.

Clear and comprehensive regulation is the first step to take. The government needs to establish policies that govern the use of cryptocurrencies (Taudaa et al, 2023) including registration procedures and supervision of digital asset service providers. With strict regulations, these industry players are required to meet certain security standards and report suspicious transactions to the competent authorities. This step not only aims to prevent the misuse of crypto assets in money laundering crimes, but also creates a safer and more transparent investment environment for the public.

In addition to strict regulations, law enforcement officials must also have adequate capacity to deal with these technology-based crimes. This unit must be equipped with experts who understand blockchain technology, smart contracts, as well as advanced data analysis techniques. With trained human resources and adequate infrastructure, these specialized units will be able to detect and investigate suspicious transactions more effectively, thereby reducing the number of crimes that leverage digital assets.

However, given the transnational nature of crypto-based money laundering crimes, law enforcement efforts at the national level alone are not enough. Close cooperation between Indonesia and other countries is needed to strengthen the monitoring mechanism and exchange of information related to cross-border transactions. Partnerships with international law enforcement agencies will allow Indonesia to gain the best insights and strategies in handling money laundering cases involving cryptocurrencies. By building global partnerships (Khan, 2024). Indonesia can be more effective in anticipating and cracking down on criminals who take advantage of loopholes in the digital financial system.

Ultimately, effective law enforcement policies in dealing with crypto-based money laundering depend not only on strict regulation and capacity building of law enforcement

officials, but also on synergy between governments, the tech industry, and the global community. With coordinated measures and a well-thought-out strategy, Indonesia can ensure that the development of blockchain and cryptocurrency technology does not become a loophole for crime, but can be used positively to support safer and more sustainable economic growth.

Community Empowerment Strategy

Community empowerment is a crypto-based money laundering prevention strategy that focuses on increasing public knowledge, awareness, and participation. In this context, the police play a role as facilitators by providing comprehensive legal and digital literacy regarding the risks, modes, and signs of money laundering through cryptocurrency (Aarvik, 2020). Community empowerment needs to be distinguished from institutional capacity building and professional training of the police. Institutional capacity building is concerned with strengthening institutions, technology, inter-agency coordination, and law enforcement mechanisms, while professional training is aimed at improving the competence of police personnel in detecting and dealing with blockchain-based crimes. With this distinction, community empowerment in this study specifically refers to efforts to increase community capacity to recognize, prevent, and report the potential for crypto-based money laundering.

Through socialization and counseling programs, the police can hold seminars, workshops, and social media campaigns aimed at raising public awareness. In this activity, the public will be taught how to recognize suspicious activity that may be related to money laundering, as well as the importance of reporting these findings to the authorities.

By raising public awareness and knowledge, the creation of a safer and more profitable environment is the desired outcome. People who are sensitive to potential crime will be better able to identify and report suspicious activity, reducing the chances for criminals to commit money laundering. In the long run, community empowerment will not only strengthen law enforcement efforts, but also build trust between police and communities, creating more effective collaboration in maintaining security and order.

The Use of Technology in Law Enforcement

In the increasingly advanced digital era, the use of technology has become an important element in law enforcement, especially in dealing with cases of illegally obtained funds. The police are now required to use data analysis and artificial intelligence (AI) technology as tools to detect suspicious transaction patterns (Santoso et al, 2023; Sari, 2021). With advanced analytics capabilities, this technology can help law enforcement officials identify transactions potentially related to money laundering activities, which are often difficult to track with traditional methods.

This technology-based monitoring system allows police to monitor and analyze financial transactions in real-time, so they can respond immediately if suspicious activity is detected. Additionally, greater accountability and openness are additional benefits of applying blockchain technology to the financial sector. With its decentralized and immutable nature, blockchain can be an effective tool in preventing money laundering, as every transaction is permanently recorded and can be audited. By integrating technology in law enforcement, police can not only improve efficiency and effectiveness in detecting and dealing with crime, but also build public trust in the legal system. The public will feel safer knowing that advanced technology is being used to protect them from adverse financial crimes. In this context, the use of technology is not only a tool, but also a strategic step to create a safer and more secure environment.

Human Resource Training and Development

Training and development of human resources in the police force is a very important aspect that cannot be ignored, especially in the face of the increasingly complex challenges of technology-based crime (Stuart & Scott, 2024; Inaray et al., 2024). Therefore, the police need to provide adequate training to their members on blockchain technology, cryptocurrencies, and cybercrime investigation techniques. By improving the competence of police members through structured and ongoing training, it is hoped that they will be better prepared and responsive to the various challenges posed by digital crime. In-depth knowledge of the technologies used in these crimes will allow them to conduct more effective and efficient investigations, as well as identify patterns that may not be seen with traditional approaches. However, this training is not only limited to the technical aspect. It is also important to include elements of ethics and human rights protection in the training curriculum. Thus, members of the police force will be trained to carry out their duties fairly and equally, respect individual rights, and avoid abuse of authority.

With this comprehensive approach, the police will not only improve the technical capabilities of their members, but also build public trust in law enforcement agencies. The public will feel safer and more secure, knowing that the police are equipped with the knowledge and skills necessary to deal with modern crime ethically and professionally.

In dealing with crypto-based money laundering, there are several significant challenges that must be faced by law enforcement officials. One of the main challenges is the anonymous and decentralized nature of blockchain technology. Transactions made with cryptocurrencies are often difficult to trace, as the identity of the perpetrator is not always revealed in the transaction records. This makes it difficult for police to identify and arrest criminals, so they can easily hide their illegal activities behind the layer of anonymity offered by this technology. In addition, in Indonesia, regulations related to cryptocurrencies are still in the development stage. The lack of clarity in this regulation creates a legal loophole that can be exploited by criminals to commit money laundering without fear of legal consequences. Without a clear and comprehensive legal framework, law enforcement becomes increasingly difficult, and criminals feel freer to operate. Therefore, it is crucial to accelerate the development of regulations that can regulate the use of cryptocurrencies and provide clear guidelines for law enforcement officials.

Limited resources are also equally important challenges. In terms of both budget and expertise, the police often face obstacles that hinder their efforts in tackling crypto-based money laundering crimes. Without adequate support, both financially and expertly, law enforcement efforts will be less effective. Therefore, governments and their institutions must provide the necessary support so that the police can better carry out their duties in the face of the ever-evolving challenges of crime in this digital age.

Some suggestions on how Indonesian police can better combat crypto-based money laundering come from the results of this study including accelerating the development of clear and comprehensive regulations on cryptocurrencies, as well as the establishment of special units within the police force focused on cybercrime and money laundering with adequate training. In addition, it is important to increase international cooperation with law enforcement agencies in other countries to strengthen investigative efforts, implement outreach programs to raise public awareness of the risks of money laundering, and utilize data analytics and artificial intelligence technologies to detect suspicious transactions. Finally, the development of human resources through blockchain technology training and cybercrime investigation techniques is essential to prepare police members to face the challenges of the digital age.

CONCLUSION

In the rapidly growing digital era, the main challenges faced by law enforcement officials in Indonesia are the lack of understanding of blockchain and cryptocurrencies, inadequate regulation, and difficulty tracking transactions due to the decentralized nature and anonymity of digital assets. Many members of the police force have difficulty detecting suspicious transactions, while legal loopholes allow criminals to use cryptocurrencies for illegal activities. The lack of cooperation between the government and the private sector further hampered law enforcement, as cryptocurrency service providers did not yet have a clear obligation to report suspicious transactions. To address this, it is necessary to increase the capacity of law enforcement technology, stricter regulations, the use of blockchain analytics technology, and close collaboration with the private sector. With these strategic measures, cybersecurity can be more guaranteed, digital crime can be suppressed, and the digital asset ecosystem in Indonesia becomes more transparent and accountable. Effective law enforcement policies in dealing with crypto-based money laundering in Indonesia should include clear regulations regarding the use of cryptocurrencies, the development of specialized units in the police force trained in blockchain technology and data analysis, and international cooperation to share information. In addition, community empowerment through education about the risks of money laundering as well as the use of data analysis and artificial intelligence technologies is essential to detect suspicious transactions. Training and development of human resources in the police force is essential to improve members' ability to deal with technology-based crime. Challenges include the anonymous and decentralized nature of blockchains, lack of clear regulation, and limited resources that require recommendations to accelerate regulatory development, establish special units, increase international cooperation, and implement socialization and counseling programs.

REFERENCES

- Aarvik, Per. (2020). Blockchain as an Anti-Corruption Tool: Case Examples and Introduction to Technology. Norway: CMI, U4, 4. Retrieved from: <https://www.u4.no/publications/are-blockchain-technologies-efficient-in-combatting-corruption.pdf>
- Aini, Nurul & Fauziah Lubis, Fauziah. (2024). Challenges of Proof in Cybercrime Cases. *Judge: Journal of Law*, 5(02), 55–63
- Albshaier, Latifa, Almarri, S. & Rahman, M.M.H. (2024). Review of the Role of Blockchain in E-Commerce Transactions: Open Challenges, and Future Research Directions, *Computers*, 13(27) <https://doi.org/10.3390/computers13010027>
- Amanda, Fitriyanti & Sinaga, Ovigeria Subroto (2024). Human Resources Development in the Balikpapan Civil Service Police Unit in Carrying out Community Control Duties. *Journal of Management and Creative Business*, 2(3), 301–313 DOI: <https://doi.org/10.30640/jmcmbus.v2i3.2910>
- Anggraeny, Isdian, and others. (2022). The urgency of establishing guidelines for handling cybercrime cases in the Indonesian National Police. *Social Sciences KnE*, 3rd International Conference on Legal Reform (3rd INCLAR), 349-359 DOI: <https://doi.org/10.18502/kss.v7i15.12107>
- Ashady, S. Januar. (2024). Cybercrime as Cybercrime in the Perspective of Law and Society. *Juridische: Journal of Legal Research*, 1(2), 34–46.
- Bower, Kate & Shane Johnson, Shane. (2024). Facing the Future of Crime: A Framework for the Use of Technology by the Police, *The Political Quarterly*, 95(3), 480-488 <https://doi.org/10.1111/1467-923X.13426>
- Chainalysis Team, DeFi Takes Bigger Role in Money Laundering Yet Small Group of Centralized Services Still Dominates, Retrieved from:

- <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/>
- Falk, Brett Hemenway & Hammer, Sarah. (2023). A Comprehensive Approach to Crypto Regulation. *University of Pennsylvania Journal of Business Law*, 25(2) <http://dx.doi.org/10.2139/ssrn.4245285>
- Firmansyah, Ade Lukman & Arifin, Tajul. (2024). Cryptocurrency in the Perspective of Permendag No. 99 Th. 2018 and Islamic Law. *Tashdiq: Journal of Religious Studies and Da'wah*, 4(3), 21–30 <https://doi.org/10.4236/tashdiq.v4i3.3686>
- Fitriyanti, A., & Sinaga, O. S. (2024). Human Resources Development in the Balikpapan Civil Service Police Unit in Carrying out Community Control Duties. *Journal of Creative Management and Business*, 2(3), 301–313.
- Hendrawan, Herman, Haris, O.K., Hidayat, S., Sinapoy, M.S. Hendrawan. (2023). Criminal Liability for the Use of Bitcoin in Money Laundering Crimes. *Halu Oleo Legal Research*, 5(2), 675–691 DOI <https://doi.org/10.33772/holresch.v5i2.235>
- Inaray, F.Q., Pratiknjo, M.H., Londa, V.Y. (2024). Analysis of Human Resource Development of Investigators at Sub-Directorate II of Harda Bangtah General Criminal Investigation at the North Sulawesi Regional Police. *Innovative: Journal Of Social Science Research*, 4(4), 2573–2587 DOI: <https://doi.org/10.31004/innovative.v4i4.13115>
- Jatna, R.N., Manthovani, R. & Hasbullah, H., (2024). The role of disruptive artificial intelligence technology in fighting crime in Indonesia. *Beijing Law Review*, 15, 1668-1711. doi: 10.4236/blr.2024.153097.
- Javaid, Mohd, and others. (2022). An Overview of Blockchain Technology Applications for Financial Services. *BenchCouncil Transactions on Benchmarks, Standards, and Evaluations*, 2, 100073 <https://doi.org/10.1016/j.tbench.2022.100073>
- By Violeta Michiko. (2024). Legal review of the role of central banks in the use of blockchain technology in financial transactions in Indonesia. *Lex Privatum*, 14(2)
- Kepli, M.Y.b.Z. and Zulhuda, S. (2019). Cryptocurrencies and Anti-Money Laundering Acts: The Need for an Integrated Approach. Oseni, U.A., Hassan, M.K. and Hassan, R. (ed.) *New Issues in Islamic Financial Law and Practice in Malaysia*, Emerald Publishing Limited, Leeds, 247-263. <https://doi.org/10.1108/978-1-78973-545-120191020>
- Khan, Azfer A. (2024). Reconceptualizing Policing for Cybercrime: Perspectives from Singapore, MPDI, *Laws*, 13(4), 44 <https://doi.org/10.3390/laws13040044>
- Kraus, Sacha, Jones, Paul & Tierno, N.R. (2021). Digital Transformation: An Overview of the Current State of the Research Arts. *Journal of Wisdom*, 11(3) <https://doi.org/10.1177/21582440211047576>
- Lampe, K. Von. (2021). Transnational Organized Crime Practices. In *the Routledge handbook on transnational organized crime*, 200–214
- Lumaing, Engelina Yuliana, Purba, Casthro, Moga, J.V., Metusalach, W., Legi, R., Dakhi, Robin (2024). Juridical Review of Money Laundering Crimes in Digital Transactions of Cryptocurrencies. *Journal of Social Science*, 12(2), 155–161
- Makogon, Borris V, Aristov, E.V., A Chaban, E.A., Fedorov, M.V. (2020). Law enforcement as a policy and legal process. *International Journal of Criminology and Sociology*, 9, 1918–1921 DOI: <https://doi.org/10.6000/1929-4409.2020.09.223>
- Miraglia, P., Ochoa, R. & Briscoe, L. (2012). Transnational Organized Crime and Fragile Countries. *OECD Development Working Paper*, Paris: OECD Publishing, 5 <https://doi.org/10.1787/5k49dfg88s40-en>.
- Munajat, Andi Ahmad & Yusuf, Hudi. (2024). The role of information technology in the prevention and disclosure of specific economic crimes: A study of digital-based financial crimes. *Journal of Intellectual Property Management*, 1(9), 4853–4865.
- Nurcholis, Manggala Rizal, Suarda, I Gede Widhiana, Prihatmini, Sapti. (2021). Law

- Enforcement of Money Laundering Crimes in Crypto Asset Investment Abuse. *Journal of Anti-Corruption*, 11(2) DOI: <https://doi.org/10.19184/jak.v3i2.26765>
- Pase, Ana Tasia, Royani, Ferawati, Fitra, Feby Ilham. (2020). Judicial Review of Law Enforcement against Money Laundering Crimes in accordance with Article 3 of Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes (Case Study of Money Laundering at the Bengkulu District Court). *Sehasen Journal of Law*, 6(2), 45–50 DOI: <https://doi.org/10.37676/jhs.v6i2.2040>
- Son, Dwi Jaya, Timur, Widya, Supindi, Elpin. (2020). A Judicial Study of Police Members as Legal Advisors. *Sehasen Journal of Law*, 6(2), 51–54 DOI: <https://doi.org/10.37676/jhs.v6i2.2037>
- Putri, Lisa Angelie & Tarina, Dwi Desi Y. (2024). Legal Certainty of Fiduciary Guarantees on Cryptocurrencies as Intangible Digital Assets in Credit Agreements in Indonesia. *Indonesian Legal Media (MHI)*, 2(4), 437–444 DOI: <https://doi.org/10.5281/zenodo.14208715>
- Putri, Tiara, and others. (2023). Insufficient Regulation of Cryptocurrency and Money Laundering in Indonesia (US and German Comparative Law). *Yustisia Journal of Law*, 12(2), 129-152, <https://doi.org/10.20961/yustisia.v12i2.71835>
- Sajidin, Syahrul. (2021). The Legality of the Use of Cryptocurrency as a Means of Payment in Indonesia. *Legal Arena*, 14(2), 245–267 <https://doi.org/10.21776/ub.arenahukum.2021.01402.3>
- Santoso, Gunawan, Karim, A.A., Maftuh, B., Sapriya, Murod, M. (2023). A Study of Law Enforcement in Indonesia to Form Peace in Bhinneka Tunggal Ika Indonesia in the 21st Century. *Journal of Transformative Education*, 2(1), 210–223 DOI: <https://doi.org/10.9000/jupetra.v2i1.143>
- Sari, Adinda Melinia, Mandiana, Sari, Paula, P. (2024). Analysis of Criminal Liability for the Use of Crypto Assets as a Means of Money Laundering Crimes. *Alliance: Journal of Law, Education and Social Humanities*, 1(2), 115–126 DOI: <https://doi.org/10.62383/aliansi.v1i2.85>
- Sari, U.I.P. (2021). Law enforcement policies in efforts to handle cyber crime carried out by the Virtual Police in Indonesia. *Journal of Studia Legalia*, 2(01), 58–77.
- Setiadarma, Aan, Abdullah, Ahmad Zaki, Sadjijo, Priyono, Firmansyah, Dwi (2024). Literature Review of Social Transformation in the Virtual Era. *Equator: Journal of Educational and Social Humanities*, 4(1), 232–244 DOI: <https://doi.org/10.55606/khatulistiwa.v4i1.2930>
- Setiawan, Jeremiah, Peter & Jennifer. (2023). Characteristics of Cryptoasset-Related Crimes and Convergence-Based Law Enforcement Policies. *Journal of Legal Dynamics*, 23(2), 305-324 <https://doi.org/10.20884/1.jdh.2023.23.2.3478>
- Setyawan, Novan Eka and others. (2024). The Impact of Digital Technology on Criminal Law Enforcement: An Analysis of Cybercrime and Its Handling. *Mawaddah Journal of Islamic Family Law*, 2(2) <https://doi.org/10.52496/mjhki.v2i2.169>
- Sholihah, Sitti Rofiatus & Yazid, Muhammad. (2023). A review of contemporary Islamic scholars' thinking on Bitcoin in the context of ḥifẓ al-Māl; Implications and Perspectives. *Falah: Journal of Sharia Economic Law*, 5(2), 11–24 DOI: <https://doi.org/10.55510/fjhes.v5i2.229>
- Sulliva, John P. (2023). The Information Age: Transnational Organized Crime, Networks, and Illegal Markets, *Journal of Strategic Security*, 16(1), 51-71 DOI: <https://doi.org/10.5038/1944-0472.16.1.2049>
- Suryawijaya, Tito Wira Eka. (2023). Strengthening Data Security through Blockchain Technology: Exploring Successful Implementation in Digital Transformation in Indonesia. *Journal of Public Policy Studies*, 2(1), 55–68 DOI:

- <https://doi.org/10.21787/jskip.2.2023.55-68>
- Susanto, Asmara Nova & Afifah, Wiwik. (2024). The Role of Institutions Supporting the Search for Evidence of Money Laundering Crimes Using Cryptocurrency. *Media Legal Indonesia (MHI)*, 2(4), 271-283 <https://doi.org/10.5281/zenodo.14181850>
- Wardani, Andhira Alya, Ali, Mahrus, Barkhuizen, Jaco. (2022). Money Laundering through Cryptocurrencies and Regulations in Money Laundering Acts, *Lex Publica*, 9(2), 49-66 <https://doi.org/10.58829/lp.9.2.2022.49-66>
- Tairov, Iskren & Stefanova, N. (2024). The Collapse of Cryptocurrencies—An Analysis of Artificial Intelligence Applications to Counter Coin Value Fluctuations in the Crypto Market, *TEM Journal*, 13(3), 1905-1915 <https://doi.org/10.18421/TEM133-18U34T>
- Taudaa, Gunawan A., Omarab, Andy, Arnonec, G., (2023). Cryptocurrencies: Highlighting Approaches, Regulation, and Protection in Indonesia and the European Union, *Bestuur*, 11(1), 1-25 <https://dx.doi.org/10.20961/bestuur.v11i1.67125>
- Trinita Imelda Bandoso, Trinita Imelda, Randa, F., & Mongan, F.F.A.. (2022). Blockchain Technology: How to Deal With It?—In an Accounting Perspective. *Journal of the Accounting Profession (APAJI)*, 4(2), 97–115 DOI: <https://doi.org/10.35593/apaji.v4i2.55>
- U.S. Department of Justice, "Global Disruption to Three Terror-Financing-Backed Cyber Campaigns," Retrieved from: <https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>
- Violanti, J.M., Owens, S.L., McCanlies, E., Fekedulegn, D. and Andrew, M.E. (2019). Law Enforcement Suicide: A Review. *Policing: International Journal*, 42(2), 141-164 <https://doi.org/10.1108/PIJPSM-05-2017-0061>
- Widjaja, Gunawan. (2019). Cryptocurrency Legality in Indonesia, *Advances in Business Research International Journal*, 5(22), 76 DOI:10.24191/abrij.v5i2.9997
- Widyatmoko, Untung, and others. (2024). Law Enforcement Against Cryptocurrency Misuse. *Journal of Social Research*, 3(2), 347-357 <https://doi.org/10.55324/josr.v3i2>
- Windani, Cynthia Ayu. (2023). Strategies and Challenges of Predictive Policing in the Era of Big Data for Modern Society. *Deviance Journal of Criminology*, 7(2), 101–120 <https://doi.org/10.36080/djk.2385>