Multidisciplinary Output Research For Actual and International Issue (MORFAI Journal) ISSN (e): 2808-6635
Volumes 5 No. 6 (2025)

POLICING TRANSFORMATION IN THE CRYPTO ERA IN HANDLING TOKEN-BASED MONEY LAUNDERING IN INDONESIA

Indah Hartantiningrum[1*], Eva Achjani Zulfa[2], Chairul M. Setyabudi[3], M. Syaroni Rofii[4]
[1,2,3,4]Universitas Indonesia, Indonesia
[*]Corresponding author's email: indah.hartantiningrum@ui.ac.id

Received	: 01 October 2025	Published	: 09 December 2025
Revised	: 10 October 2025	DOI	: https://doi.org/ 10.54443/morfai.v5i6.4633
Accepted	: 25 November 2025	Publish Link	: https://radjapublika.com/index.php/MORFAI/article/view/4633

Abstract

The purpose of this study is to analyze how policing transformation in Indonesia can be carried out to address token-based money laundering, as well as to provide policy recommendations that can improve the effectiveness of law enforcement in the context of the development of crypto technology. Adopting a post-positivism paradigm and a qualitative approach to explore policing transformation 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 main patterns and themes. The results of the study indicate that the main challenges in law enforcement against crypto-based money laundering in Indonesia include a lack of insight into blockchain technology and cryptocurrency, inadequate policies, and difficulties in tracking transactions due to the decentralized nature and anonymity of digital assets. To overcome this problem, it is necessary to increase the technological capacity of law enforcement officers, develop special trained units, and implement stricter regulations. In addition, community empowerment through education and training for police officers is very important to improve competence in detecting suspicious transactions. With these strategic steps, it is hoped that cyber security can be more assured 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 resulted from the advent of blockchain technology and digital currencies. Cryptocurrencies, as one of the main innovations in the world of finance, offer various advantages, such as transaction speed, cost efficiency, and higher privacy compared to the traditional financial system (Sajidin, 2021). The crypto-based money laundering process has different characteristics from traditional money laundering (Nurcholis et al, 2022). The use of tokens and untraceable transactions become an opening for criminals to hide the source of illegal funds. In this context, policing transformation is urgently needed so that law enforcement officials can mitigate threats that arise along with the development of this new technology. This study aims to analyze how policing transformation in the face of token-based money laundering and provide recommendations for improving the prevention of this crime in Indonesia.

Cryptocurrency token-based money laundering is one form of financial crime that is increasingly rampant (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 originating from illegal activities (Windani, 2023). This is a serious concern for law enforcement, especially the police, in the fight against and eventual elimination of 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 (Chynalisis 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 that 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 (U.S. 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 these 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 their misuse, especially in money laundering. Digital transformation is a process of change and improvement in organizations, businesses, and industries through the implementation and utilization of digital technology (Kraus et al, 2021). The employment of technology is at the heart of digital transformation as it pertains to law enforcement such as data processing and analysis, mobile applications, Internet of Things (IoT), cloud computing, and blockchain technology. The importance of strengthening the role of the police through digital transformation in this era has many new challenges for the world of security and law enforcement.

Polification, 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, policing should 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 changes. By adopting new technologies, building partnerships with the community, 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 current problems need an ethical and well-considered solution if we are to keep people's rights intact.

The Transnational Organized Crime (TOC) theory refers to a form of violation that is classified as organized crime, where its definition and definition continue to evolve along with the changing times, especially in the 20th century (Miraglia et al, 2012). The UN Convention on the Eradication of TOC Crimes issued 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 transnationally. In this context, law enforcement is defined as the process of realizing the desire of the law to come true, 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 that must be carried out.

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

According to Law Number 8 of 2010 about the Prevention and Eradication of Money Laundering Crimes, some of his earlier works, such as legitimate crypto assets as digital commodities, can become unlawful when used for this purpose. Offenders can then be located and prosecuted (Sari et al, 2024). While 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 to ensure that policing remains effective and ethical in serving society (Ayu, 2023).

The study offers a new approach in understanding the transformation of policing in Indonesia, within the framework of cryptocurrency tokens used for illicit financial transactions, by highlighting the adaptation of law enforcement strategies needed to deal with the unique challenges posed by blockchain technology and the anonymous nature of crypto transactions. This research is particularly relevant given the increasing use of cryptocurrencies in Indonesia and their potential misuse for money laundering, that can endanger the stability of the economy and the banking system. By providing insights into effective policing policies and practices, this research contributes to the development of better and responsive law enforcement strategies to financial crime in the digital age. The researchers set out to examine how policing transformation in Indonesia can be carried out to deal with token-based money laundering, as well as provide policy recommendations that can increase the effectiveness of law enforcement in the context of crypto technology developments.

Method

This study employs a descriptive qualitative approach within a post-positivist paradigm to examine policing transformation in addressing token-based cryptocurrency money laundering in Indonesia. Data were collected through in- depth, semi- structured interviews with police investigators, regulatory authorities, and blockchain experts, complemented by document analysis of relevant laws, policy reports, and scholarly publications. Data were analyzed using thematic analysis, involving coding, categorization, and identification of key analytical themes. Data validity was ensured through source triangulation and verification of emerging findings. All research procedures complied with ethical standards, including informed consent and the protection of participant confidentiality.

Result and Discussion

Transformation of Policing in Dealing with Token-Based Money Laundering

The transformation of policing in Indonesia in dealing with token-based money laundering in the crypto era faces various complex problems. First, the absence of proper knowledge and comprehension is a major obstacle regarding blockchain technology (Imelda et al, 2022) and cryptocurrencies (Kawengian, 2024). Many police members are not trained to understand how this system works, 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 have the potential to result in the loss of crucial evidence traces. Second, current regulations are still not fully adequate to tackle crimes related to cryptocurrencies. Although Indonesia has issued several regulations related to the use of digital assets, there are many legal loopholes that can still be exploited by criminals. For example, controversy about cryptocurrency's legitimacy (Firmansyah & Arifin, 2024) as a medium of exchange or asset for investment purposes (Putri et al, 2024) can lead to difficulties in law enforcement (Sholihah & Yazid, 2023).This creates challenges for the police in implementing appropriate legal action against violations that occur.

Third, the decentralized nature and anonymity inherent in cryptocurrencies (Lumaing, et al, 2024) make it very difficult to track transactions (Susanto & Afifah, 2024). Criminals can easily hide their identities and divert funds through various platforms and digital wallets, obstructing the ability of law enforcement to identify the source of money that may be under suspicion. In this context, policing needs 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 cryptocurrencies do not have an obligation to report suspicious transactions to the authorities, thus hampering prevention and enforcement efforts. Closer cooperation between the police and the involvement of the private sector is essential.to create a more transparent and responsive reporting system to potential money laundering.

The analysis of the compatibility of theories with field data in the context of token-based money laundering in Indonesia shows that various existing theories can explain this phenomenon well. First, according to money laundering theory, there are three steps to the 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. Furthermore, 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 differences in regulations in each country to launch their actions (Lampe, 2021). The data shows a lack of international cooperation in the investigation of crypto-based transactions, underscoring 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 faced in law enforcement in the crypto era.

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 members are still poorly trained in understanding blockchain technology and cryptocurrencies, leading to weak law enforcement against these crimes. This theory reinforces the argument that increased knowledge and skills among law enforcement are essential to confront 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 had an impact on the transformation of policing methods (Setiadarma et al, 2024). The data supports this theory by showing that police forces must adapt their approach to changing technological developments. This shows that policing needs to adapt in order to remain effective in dealing with increasingly complex crimes.

Finally, Social Networks 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 shows that the police need to build an intelligence system based on social network analysis to identify criminals. In addition, crypto technology facilitates cybercrime with a high degree of anonymity, and data shows that these crimes are growing as the use of digital assets in illegal transactions increases. In the rapidly evolving 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 major problem, especially those 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 can be related to illegal activities, like the funding of terrorists and the laundering of illicit funds. This unpreparedness is a loophole that cybercriminals use to hide the flow of their funds through crypto transactions that are difficult to track.

One of the factors that exacerbates this condition is the inadequate regulation of cryptocurrencies 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 causes law enforcement officials to have difficulty cracking down on criminals who use digital currencies for illegal activities. Existing regulations have not been able to accommodate the complexity of blockchain technology that is decentralized and anonymous, 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). Unlike conventional banking transactions that have a clear administrative footprint and can be overseen by financial authorities, crypto transactions take place on a global network that does not have a 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 have difficulty gathering enough evidence to uncover and take action against criminals. Additionally, the lack of collaboration between the government and the private sector further hampers 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 increase the effectiveness of suspicious activity detection.

To overcome these challenges, strategic steps involving various parties are needed. First, increasing capacity and understanding of technology among law enforcement officials must be a top priority. Training programs and collaboration 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 crimes.

Second, regulations regarding cryptocurrencies must be strengthened to better accommodate technological developments and prevent the misuse of digital assets for illegal activities. The government needs 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 opportunities for criminals to abuse the system (Falk & Hammer, 2023).

Third, crypto transaction tracking 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 specialized software capable of detecting suspicious transaction patterns as well as identifying relationships between various crypto wallet addresses. Indonesia also needs to develop or adopt similar technologies so that law enforcement officials can work more effectively in tracking suspicious money flows.

Fourth, cooperation with the private sector should be increased 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 face of the ever-evolving digital era, law enforcement officials in Indonesia must be able to adapt to technological changes in order to maintain security and order in cyberspace. By improving understanding of technology, strengthening regulations, adopting more advanced tracking technologies, and building closer cooperation with the private sector, challenges in enforcement related to cryptocurrencies can be overcome

more effectively. These measures will not only help in eradicating digital crime, but will also strengthen the digital asset ecosystem in Indonesia to be more transparent and accountable. The challenge in handling 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. Regulations regarding cryptocurrencies 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 investigation efforts and detection of suspicious transactions. In addition, the utilize of AI-based analysis technology and big data must be increased to help the authorities in automatically recognizing suspicious transaction patterns and conducting more in-depth analysis of digital crime activities.

Policies and Strategies

A. Law Enforcement Policy

Emerging threats in the realm of law enforcement have been posed by blockchain technology and cryptocurrencies in the past few years, especially in efforts to handle crypto-based money laundering cases in Indonesia. Amidst the widespread use of cryptocurrency, effective regulation is very important so that the use of this technology is not misused for illegal activities. Therefore, a strong and structured law enforcement policy is needed to overcome the threat of money laundering through digital assets.

Clear and comprehensive regulations are the first step that must be taken. The government needs to establish policies that regulate 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 appropriate authorities. This step not only aims to prevent the misuse of crypto assets in money laundering crimes, but also to create 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 this technology-based crime. Therefore, the establishment of a special unit within the police force that focuses on cybercrime (Anggraeny et al, 2022) and money laundering is an urgent need. 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, this special unit will be able to detect and investigate suspicious transactions more effectively, thereby reducing the number of crimes that utilize 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 insights and the best strategies in handling money laundering cases involving cryptocurrencies. By building a global partnership (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 tackling crypto-based money laundering depend not only on strict regulation and increased capacity of law enforcement officials, but also on synergies 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.

B. Community Empowerment Strategy

Community empowerment is one of the key strategies in efforts to prevent crypto-based money laundering. In this context, the police have an important role to actively involve the community in fighting this crime. One step that can be taken is to provide comprehensive literacy (Aarvik, 2020) about the risks and signs of money laundering using cryptocurrencies. Through socialization and counseling programs, the police can hold seminars, workshops, and social media campaigns that aim to increase public awareness. In these activities, the public will be taught how to recognize suspicious activities that may be related to money laundering, as well as the importance of reporting such findings to the authorities.

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

C. Use of Technology in Law Enforcement

In the increasingly advanced digital era, the use of technology has become a crucial element in law enforcement, particularly when dealing with cases of illicitly obtained funds. The police are now required to utilize data analysis technology and artificial intelligence (AI) as a tool to detect suspicious transaction patterns (Santoso et al, 2023; Sari, 2021). With advanced analytical capabilities, this technology can assist law enforcement officials in identifying transactions that are potentially related to money laundering activities, which are often difficult to track with traditional methods. The technology-based monitoring system allows the police to monitor and analyze financial transactions in real-time, so they can respond immediately if suspicious activity is detected. In addition, greater accountability and openness are further benefits of implementing blockchain technology into 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 auditable. By integrating technology in law enforcement, the police can not only improve efficiency and effectiveness in detecting and dealing with crimes, 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 harmful financial crimes. In this context, the use of technology is not just a tool, but also a strategic step to create a safer and more secure environment.

D. 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 increasingly complex technology-based crime challenges (Fitriyanti & Sinaga, 2024; Inaray et al., 2024). For this reason, the police need to provide adequate training to its members on blockchain technology, cryptocurrency, and cybercrime investigation techniques. By improving the competence of police members through structured and continuous training, it is hoped that they will be more prepared and responsive in facing the various challenges posed by digital crime. An in-depth knowledge of the technology used in these crimes will allow them to conduct more effective and efficient investigations, as well as identify patterns that may not be visible with traditional approaches. However, this training is not only limited to technical aspects. 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 in a fair and equitable manner, respect the rights of individuals, 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 institutions. 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 in an ethical and professional manner. In handling 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 apprehend criminals, so they can easily hide their illegal activities behind the layers of anonymity offered by this technology. In addition, in Indonesia, regulations regarding cryptocurrencies are still in the development stage. This lack of clarity in regulations creates loopholes 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 more free 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 an equally important challenge. Both in terms of budget and expertise, police often face obstacles that hinder their efforts in tackling crypto-based money laundering crimes. Without adequate support, both in terms of finance and expertise, law enforcement efforts will be less effective. Hence, the

government and its agencies must offer the required backing so that the police can better carry out their duties in the face of the ever-evolving crime challenges in this digital era. Several suggestions for how the Indonesian police may better combat crypto-based money laundering were derived from the results of the study include accelerating the development of clear and comprehensive regulations on cryptocurrencies, as well as the establishment of a special unit in the police force that focuses 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 investigation efforts, implement outreach programs to raise public awareness of money laundering risks, and utilize data analysis technology and artificial intelligence to detect suspicious transactions. Finally, the development of human resources through training on blockchain technology and cybercrime investigation techniques is essential to prepare police members for the challenges of the digital age.

Conclusion

In the rapidly evolving digital era, the main challenges faced by law enforcement officials in Indonesia are a lack of understanding of blockchain and cryptocurrency, inadequate regulations, 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 utilize cryptocurrencies for illegal activities. The lack of cooperation between the government and the private sector is further hampering law enforcement, as cryptocurrency service providers do not yet have a clear obligation to report suspicious transactions. To overcome this, it is necessary to increase the technological capacity of law enforcement, stricter regulations, the use of blockchain analysis technology, and close collaboration with the private sector. With these strategic measures, cyber security can be more guaranteed, digital crime can be suppressed, and the digital asset ecosystem in Indonesia becomes more transparent and responsible. An effective law enforcement policy 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 for information sharing. In addition, community empowerment through education about the risks of money laundering and the use of data analysis technology and artificial intelligence is essential to detect suspicious transactions. Training and development of human resources in the police force is essential for enhancing members' ability to tackle technology-based crime. Challenges include the anonymous and decentralized nature of blockchain, lack of clear regulation, and limited resources, which require recommendations to accelerate regulatory development, establish specialized units, increase international cooperation, and implement socialization and counseling programs.

REFERENCES

Aarvik, Per. (2020). Blockchain as an Anticorruption Tool: Case Examples and Introduction to the 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). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. *Judge: Jurnal Hukum*, *5*(02), 55–63

Albshaier, Latifa, Almarri, S. & Rahman, M.M.H. (2024). A Review of Blockchain's Role 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). Pengembangan Sumber Daya Manusia di Satuan Polisi Pamong Praja Balikpapan dalam Melaksanakan Tugas Penertiban Masyarakat. *Journal of Management and Creative Business*, *2*(3), 301–313 DOI: https://doi.org/10.30640/jmcbus.v2i3.2910

Anggraeny, Isdian and others. (2022). The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department. *KnE Social Science*, 3rd International Conference on Law Reform (3rd INCLAR), 349-359 DOI: 10.18502/kss.v7i15.12107

Ashady, S. Januar. (2024). Cybercrime sebagai Kejahatan Dunia Maya dalam Perspektif Hukum dan Masyarakat. *Juridische: Jurnal Penelitian Hukum*, *1*(2), 34–46.

Bower, Kate & Shane Jhonson, Shane. (2024). Facing the Future of Crime: A Framework for Police Use of Technology, *The Political Quartelrly*, 95(3), 480-488 https://doi.org/10.1111/1467-923X.13426

Chainalysis Team, DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still

Dominate, 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. *The University of Pennsylvania Journal of Business Law*, 25(2) http://dx.doi.org/10.2139/ssrn.4245285

Firmansyah, Ade Lukman & Arifin, Tajul. (2024). Cryptocurrency Dalam Perspektif Permendag No. 99 Th. 2018 Dan Hukum Islam. *Tashdiq: Jurnal Kajian Agama Dan Dakwah*, *4*(3), 21–30 https://doi.org/10.4236/tashdiq.v4i3.3686

Fitriyanti, A., & Sinaga, O. S. (2024). Pengembangan Sumber Daya Manusia di Satuan Polisi Pamong Praja Balikpapan dalam Melaksanakan Tugas Penertiban Masyarakat. *Journal of Management and Creative Business*, 2(3), 301–313.

Hendrawan, Herman, Haris, O.K, Hidayat, S., Sinapoy, M.S. Hendrawan. (2023). Pertanggungjawaban Pidana Penggunaan Bitcoin dalam Kejahatan Tindak Pidana Pencucian Uang. *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). Analisis Pengembangan Sumber Daya Manusia Penyidik pada Subdit II Harda Bangtah Reserse Kriminal Umum di Kepolisian Daerah Sulawesi Utara. *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 Combating Crime in Indonesia. *Beijing Law Review*, 15, 1668-1711. doi: 10.4236/blr.2024.153097.

Javaid, Mohd and others. (2022). A Review 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

Kawengian, Violeta Michiko. (2024). Tinjauan Hukum Peran Bank Sentral Terhadap Penggunaan Teknologi Blockchain Dalam Transaksi Keuangan Di Indonesia. *Lex Privatum*, *14*(2)

Kepli, M.Y.b.Z. and Zulhuda, S. (2019). Cryptocurrencies and Anti-money Laundering Laws: The Need for an Integrated Approach. Oseni, U.A., Hassan, M.K. and Hassan, R. (Ed.) Emerging Issues in Islamic Finance 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: Perspective 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 Art of Research. *Sage Journals*, 11(3) https://doi.org/10.1177/21582440211047576

Lampe, K. Von. (2021). The Practice of Transnational Organized Crime. In *Routledge handbook of transnational organized crime*, 200–214

Lumaing, Engelina Yuliana, Purba, Casthro, Moga, J.V., Metusalach, W., Legi, R., Dakhi, Robin (2024). Tinjauan Yuridis Tindak Pidana Pencucian Uang pada Transaksi Digital Cryptocurrenncy. *Jurnal Social Science*, *12*(2), 155–161

Makogon, Borris V, Aristov, E.V, A Chaban, E.A., Fedorov, M.V. (2020). Law Enforcement as Discretion and Legal Process. *International Journal of Criminology and Sociology*, *9*, 1918–1921 DOI:10.6000/1929-4409.2020.09.223

Miraglia, P., Ochoa R. & Briscoe, L. (2012). Transnational Organised Crime and Fragile States. *OECD Development Co-operation Working Papers*, Paris: OECD Publishing, 5 https://doi.org/10.1787/5k49dfg88s40-en.

Munajat, Andi Ahmad & Yusuf, Hudi. (2024). Peran teknologi informasi dalam pencegahan dan pengungkapan tindak pidana ekonomi khusus: Studi tentang kejahatan keuangan berbasis digital. *Jurnal Intelek Insan Cendikia*, *1*(9), 4853–4865.

Nurcholis, Manggala Rizal, Suarda, I Gede Widhiana, Prihatmini, Sapti. (2021). Penegakan Hukum Tindak Pidana Pencucian Uang dalam Penyalahgunaan Investasi Aset Kripto. *Jurnal Anti Korupsi*, 11(2) DOI: https://doi.org/10.19184/jak.v3i2.26765

Pase, Ana Tasia, Royani, Ferawati, Fitra, Feby Ilham. (2020). Juridical Review of Law Enforcement against the Crime of Money Laundering According to Article 3 of Law Number 8 of 2010 concerning Prevention and Eradication of the Crime of Money Laundering (Case Study of Money Laundering at the Bengkulu District Court). *Jurnal Hukum Sehasen*, *6*(2), 45–50 DOI: https://doi.org/10.37676/jhs.v6i2.2040

Putra, Dwi Jaya, Timur, Widya, Supindi, Elpin. (2020). Juridical Study of Police Members as Legal Advisors. *Jurnal Hukum Sehasen*, *6*(2), 51–54 DOI: https://doi.org/10.37676/jhs.v6i2.2037

Putri, Lisa Angelie & Tarina, Dwi Desi Y. (2024). Kepastian Hukum Jaminan Fidusia atas Cryptocurrency Sebagai

Aset Digital Tidak Berwujud dalam Perjanjian Kredit di Indonesia. *Media Hukum Indonesia (MHI)*, *2*(4), 437–444 DOI: https://doi.org/10.5281/zenodo.14208715

Putri, Tiara and others. (2023). Inadequate Cryptocurrency and Money Laundering Regulations in Indonesia (Comparative Law of US and Germany). *Yustisia Jurnal Hukum*, 12(2), 129-152, DoI:10.20961/yustisia.v12i2.71835

Sajidin, Syahrul. (2021). Legalitas Penggunaan Cryptocurrency Sebagai Alat Pembayaran di Indonesia. *Arena Hukum*, *14*(2), 245–267 DOI:10.21776/ub.arenahukum.2021.01402.3

Santoso, Gunawan, Karim, A.A., Maftuh, B., Sapriya, Murod, M. (2023). Kajian Penegakan Hukum di Indonesia untuk Membentuk Perdamian dalam Bhinneka Tunggal Ika Indonesia Abad 21. *Jurnal Pendidikan Transformatif*, *2*(1), 210–223 DOI: https://doi.org/10.9000/jupetra.v2i1.143

Sari, Adinda Melinia, Mandiana, Sari, Paula, P. (2024). Analisa Pertanggungjawaban Pidana Atas Penggunaan Aset Kripto Sebagai Sarana Tindak Pidana Pencucian Uang. *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, *1*(2), 115–126 DOI: https://doi.org/10.62383/aliansi.v1i2.85

Sari, U.I.P. (2021). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58–77.

Setiadarma, Aan, Abdullah, Ahmad Zaki, Sadjijo, Priyono, Firmansyah, Dwi (2024). Tinjauan Literatur Transformasi Sosial dalam Era Virtual. *Khatulistiwa: Jurnal Pendidikan Dan Sosial Humaniora*, *4*(1), 232–244 DOI: https://doi.org/10.55606/khatulistiwa.v4i1.2930

Setiawan, Jeremiah, Peter & Jennifer. (2023). Characterictics of Cryptoassset-Related Crime and Convergence-Basde Law Enforcement Policies. *Jurnal Dinamika Hukum*, 23(2), 305-324 DOI: 10.20884/1.jdh.2023.23.2.3478

Setyawan, Novan Eka and others. (2024). The Effect of Digital Technology on Criminal Law Enforcement: An Analysis of Cybercrime and Its Handling. *Mawaddah Jurnal Hukum Keluarga Islam*, 2(2) https://doi.org/10.52496/mjhki.v2i2.169

Sholihah, Sitti Rofiatus & Yazid, Muhammad. (2023). Tinjauan Pemikiran Cendekiawan Islam Kontemporer Mengenai Bitcoin dalam Konteks Ḥīfẓū Al-Māl; Implikasi dan Perspektif. *Falah: Jurnal Hukum Ekonomi Syariah*, *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 Illicit 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). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68 DOI: https://doi.org/10.21787/jskp.2.2023.55-68

Susanto, Asmara Nova & Afifah, Wiwik. (2024). Peran Lembaga yang Mendukung Penelusuran Alat Bukti Tindak Pidana Pencucian Uang yang Menggunakan Cryptocurrency. *Media Hukum Indonesia (MHI)*, *2*(4), 271-283 https://doi.org/10.5281/zenodo.14181850

Wardani, Andhira Alya, Ali, Mahrus, Barkhuizen, Jaco. (2022). Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act, *Lex Publica*, 9(2), 49-66 https://doi.org/10.58829/lp.9.2.2022.49-66

Tairov, Iskren & Stefanova, N. (2024). Cryptocurrencies Collapse–Analysis of Artificial Intelligence Applications for Countering 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). Cryptocurrency: Highlighting the Approach, Regulations, and Protection in Indonesia and 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: Bagaimana Menghadapinya?–Dalam Perspektif Akuntansi. *Accounting Profession Journal (APAJI)*, *4*(2), 97–115 DOI: https://doi.org/10.35593/apaji.v4i2.55

U.S. Department of Justice, "Global Disruption of Three Terror Finance Cyber-Enabled 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: An International Journal*, 42(2), 141-164 https://doi.org/10.1108/PIJPSM-05-2017-0061

Widjaja, Gunawan. (2019). Legality of Cryptocurrency 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 Abuse. *Journal of Social*

Research, 3(2), 347-357 https://doi.org/10.55324/josr.v3i2
Windani, Cynthia Ayu. (2023). Strategi dan Tantangan Predictive Policing di Era Big Data bagi Masyarakat Modern. Deviance Jurnal Kriminologi, 7(2), 101–120 DOI: 10.36080/djk.2385