Journal of Social Research

P-ISSN: 2827-9832
E-ISSN: 2828-335x
http://ijsr.internationaljournallabs.com/index.php/ijsr

LAW ENFORCEMENT AGAINST CRYPTOCURRENCY ABUSE

Untung Widyatmoko[1], Romli Atmasasmita[2], Anthon F Susanto[3], Bambang Heru Purwanto[4]

Doctoral Program Students of Universitas Pasundan, Indonesia
sloriyadhncb@gmail.com

ABSTRACT

The purpose of this research is to provide knowledge and literacy on law enforcement efforts that can be taken against crimes committed through the misuse of cryptocurrencies as a means of transaction. To achieve this, the article employs a normative legal research approach, using a legal perspective to develop a concept for solving problems related to cryptocurrency misuse. This approach is supported by a legal and case-based approach, with data sourced from secondary data and primary legal materials that are binding and fundamental. The archival juridical approach method is used in this research, which prioritizes the examination of primary and secondary data, including interviews with various sources and positive legal studies, to determine how to implement them in practice in the field. The results of this research indicate that law enforcement against the misuse of cryptocurrencies requires government support in the form of clear regulations and firm legal policies on the use of cryptocurrencies. This will ensure that the law enforcement process fulfils a sense of justice for the community and the achievement of legal certainty. This research provides valuable insights into the challenges of law enforcement against the misuse of cryptocurrencies. It highlights the importance of government support in the form of clear regulations and firm legal policies to ensure that justice is served and legal certainty is achieved. The archival juridical approach method used in this study provides a useful framework for future research in this area, and the findings of this study can be used to inform policy and practice in the field of cryptocurrency law enforcement.

Keywords: *Law Enforcement; Crime; Misuse; Cryptocurrencies*

INTRODUCTION

Electronic based trading has provided major changes in society, namely encouraging people to make payment transactions that were originally offline based or cash-based instruments or cash payment instruments by meeting directly and now turning into online-based without having to meet directly between traders or known as non-cash-based instruments so as to reduce cash payment transactions using fiat money as a medium. One of the payment tools that has emerged lately is digital money (Gross et al., 2021). The use of digital money as a means of payment has given rise to new innovations from the digital financial system with the presence of new payment instruments called cryptocurrencies in the world (Dayi, 2019). Cryptocurrency as a form of technological innovation in the financial sector that develops in e-commerce activities, has become a new phenomenon in the midst of society in carrying out the process of global financial transactions. Cryptocurrencies work with a peer-to-peer model using an internet network-based operating system (Yousafzai et al., 2021), basically crypto currencies carry out their operational patterns with cryptographic techniques whose recording is carried out in a distributed ledger and is used to manage the creation of new units of cryptocurrency from the results of mining (mining) then verified when there are new transactions. This cryptographic system will ensure the security of transactions without involving other parties in the sense that there is no third party, namely the government or Central Bank in it. Users of this cryptocurrency only interact with fellow users, the technology used between users of the cryptocurrency is known as the blockchain (Priyo Amboro & Christi, 2019).

The problem is that cryptocurrencies are often misused in various fraudulent transactions, money laundering and are often used on illegal trading sites that can only be accessed through dark transaction sites called the deep web or dark web. This phenomenon certainly threatens the stability of a country's security and economy and threatens legal banking institutions in every country. Difficulties certainly arise when legal problems occur, and law enforcement officials will conduct tracing or tracing of financial sources and audits of financial transaction audits in the form of asset transfers or trade transactions. Generally, cyberspace is a safe place for cryptocurrency financial transactions. As the name suggests, cryptocurrencies are created through complex cryptographic encryption techniques with complex algorithms and are interconnected with each other between blockchains. Although cryptocurrencies are said to be safe, they are not immune to theft. Criminals carry out hacking, social engineering, and phishing scams to steal cryptocurrency from their victims, before laundering it on the blockchain. The absence of regulations and criminal sanctions in the misuse of cryptocurrencies makes it difficult for customers to hold them accountable when there are legal problems such as fraud, forgery or theft (through phishing, cracking and hacking) (Jatmiko, 2023). As for some potential crimes that are generally committed using crypto currencies can be mentioned as follows:

1. Risk to payment systems. According to Bank Indonesia, in several countries, cryptocurrencies cannot be exchanged for fiat currencies due to high volatility with local currency exchange rates. So that when crypto money customers make complaints or complaints related to exchange rates against the local Central Bank, they cannot be followed up and given solutions to the problems faced.
2. Risk of illegal activities. Cryptocurrencies have risks for money laundering, corruption and financing terrorist activities, especially transactions carried out using cryptocurrencies are difficult for legal action in the form of confiscation of evidence, freezing assets and customer accounts from cryptocurrency users.
3. Risks to financial system stability. The potential for economic bubble bursts due to the interaction between cryptocurrencies and the real economy is due to supply and demand expectations and fluctuating domestic money market situations due to various factors of global and regional economic, social and political conditions, such as wars, natural disasters, riots, state political instability, weakening people's purchasing power and so on.
4. Risk to consumer protection. Not all crypto asset trading companies and crypto exchanges are companies that are financially sound or are trusted and responsible investment companies, so the potential for escaping customer funds is very large and occurs a lot globally.

As a new phenomenon in the global financial system, cryptocurrencies demand legal certainty in Indonesia so that in the event of a cryptocurrency crime, law enforcement officials in Indonesia already have a legal basis in handling it. As it is known that it has been more than 8 (eight) years since crypto currencies were present in Indonesia (Popkova & Parakhina, 2019), there have been no concrete legal steps that can be a solution if there is misuse of the use of cryptocurrencies, this situation makes the law seem too always be present late. This has confirmed the perspective that the law is fundamentally conservative. The law is actually police that maintains "security and order" that will change when preceded by changes in values in society (Jauregui, 2018). In fact, law is always needed to be a foothold for humans from the negative influence of the impact of scientific and technological progress.

METHOD

The research conducted is normative legal research that is a legal perspective to produce new concepts in solving the problems faced, supported by a legal approach and a case approach (Christiani, 2016). The approach method used in this study is the archival juridical approach method (Cook, 2013), which is legal research that prioritizes how to examine primary and secondary data (Jauregui, 2018), in the form of interviews with various sources and positive legal studies and how to implement them in practice in the field.

RESULTS AND DISCUSSION

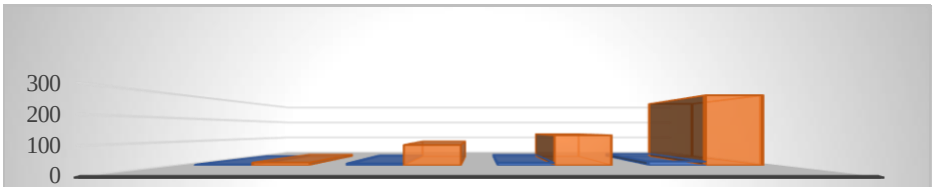
The Development of Crime in the Digital Economy Era

The rapid development of the digital economy has changed the social system and the pattern of financial system transactions has undergone very significant changes. The trade transaction system no longer requires the presence of sellers and buyers physically or face-to-face by bringing goods that are the object of buying and selling, all processes both bidding and buying virtually. Similarly, the stage of payment transactions is no longer needed by a cash system by bringing physical money as a means of payment, but payments are made through transfer methods in the form of digital numbers at the agreed nominal. This virtual pattern of trading and payments is what is referred to as the digital economy. The role of the digital economy in penetrating market access, increasing purchasing power and ease of transactions contributes greatly to the economic progress of a country, because it is considered very efficient by saving time, energy and costs (Hasan et al., 2022).

Currently, there are at least three types of variants in digital money schemes that are circulating in general in the world and have become payment instruments in global trade transactions, namely:

1. Digital money based on the value of fiat or physical money. The first variant is a form of "digitization" of the amount of money value of customers or users. Authorization is still with the banking authority because it is connected to the user's account. This digital currency is limited to the transfer of transaction vehicles, with a fixed value base using currency authorized by the government of a country. This type is used as a Card-Based Payment Instrument (APMK) which includes credit cards, debit cards, and similar cards.
2. Digital money stored in a digital wallet or E wallet which is a stored value or prepaid card. This money does not require authorization from the bank or is not linked to the user's account so that it can be used directly to transact with vendors (merchants) who have joined and approved the system of use. This type of money still uses a government-authorized currency base, stored in the form of applications in personal communication devices, cellular phones (smart phones) or in card-shaped media. In general, in Indonesia, this model is known as electronic money which has been used as a supporter of the National Non-Cash Movement.
3. The last digital money is virtual cryptocurrency. Transactions can occur between users and do not need to be known by other parties. Transactions are only recorded in computer network databases or smart phones of cryptocurrency users. The value of cryptocurrencies is not tied to any global currency.

Table 1. Crypto Asset Users & Asset Value Amount, Source: OJK



	2019	2020	2021	2022
customers	3.8	8.11	11.26	16.55
Values	12.1	86.21	127.4	296.66

Based on data collected by the Financial Services Authority (OJK), currently the number of crypto asset users registered with the Exchange Services Company (PJP) has increased every year in the number of customers and their financial value from 3.80 million customers with a gain of 12.10 T in 2019, to 8.11 million customers with an acquisition value of 86.21 T in 2020, to 11.26 million customers with an acquisition value of 127.40 T in 2021, to 16.55 million customers with an acquisition value of asset transactions cryptocurrencies reached IDR 296.66 trillion in November 2022. The data in table 1 provides a factual picture that the potential use of crypto assets in criminal acts in Indonesia can occur on a large scale (Jatmiko, 2023).

Related to the development of crime in the digital economy era, generally perpetrators of cross- border crimes or transnational crime actors never use cash in payment transactions for the predicate of the crime they committed. Conventional transfer methods are also very avoided by perpetrators of this crime, because of course it will be easy to trace financial sources (follow the money), so they change the transfer system method using the dark web that is not monitored by a country's national monetary authority system. The development of cryptocurrencies that use cryptographic technology is the latest innovation in the financial field. In addition, efforts to place assets from their crime (placement assets) and efforts to separate the proceeds of crime from the source (layering) to disguise the origin of the cryptocurrency which is the result of crime by converting to local currency (local currency) so that the proceeds of crime were originally dirty money (dirty money) into clean money (clean money) using currency conversion. Catching crypto criminals is extremely difficult due to the anonymous nature of currencies, this has made authorities face new challenges in cryptocurrency criminal investigations due to the methods and technologies used by criminals to enhance their anonymity on the blockchain. Special competence is needed for law enforcement to be able to bring criminals to justice and stop their crimes, as well as confiscate the illicit funds they generate. It must also be acknowledged that the focus of money laundering is not only efforts to avoid legitimate taxes, or avoid Bank commission fees in every transaction, but rather efforts to hide traces of crime and the consequences of criminal activities in the financial sector that they carry out on a local, regional and even global scale.

Various advantages possessed by crypto currencies are in line with their development, making criminals use them to create new types of money laundering methods (Stokes, 2012). The use of cryptocurrency as a means of payment in every criminal transaction is the main choice of criminals because the blockchain system is the best choice and is very safe from the monitoring and tracing of law enforcement officials who will have difficulty in tracing the source of their financial origins and find it difficult to follow the movement of financial transactions between parties involved in the crime. Law enforcement officials cannot ask for

information or obtain information related to the trail of money movement (follow the money) from any party to banking authorities either from the Central Bank or commercial banks.

It should be acknowledged that conventional financial instruments are very far behind the cryptocurrency system which has many advantages, and this is an expected advantage for those who commit crimes because the need for speed, security, efficiency and confidentiality of their data is more guaranteed than if financial transactions use the conventional banking system. For example, if the reference of law enforcement officials in handling trafficking is Article 1 point 4 of Law of the Republic of Indonesia No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering which reads: receipt, transfer, deposit, withdrawal, book transfer, payment, grant, donation, custody, and/or exchange of a sum of money or other actions and/or activities related to money. Of course, there will be difficulties in carrying out the investigation and investigation process because the perpetrators do not use conventional bank services as legal subjects but the subject of the law is a crypto system that is built in cyberspace and is a virtual banking product.

The use of cryptocurrencies can be classified as money laundering if the cryptocurrency comes from the proceeds of crime (criminal act) (Albrecht et al., 2019). Usually, what often happens is that crypto purchase money is the result of the circulation/sale of narcotics, then exchanged so that crypto currency will be obtained as a result of the criminal sale of narcotics (criminal process), which then the crypto currency is "laundered" in a financial transaction or invested in a legal business such as property or shares. There are several examples of "money laundering" that the author can present, as happened below:

1. In 2013, the United States Government shut down Arthur Budovsky's Liberty Reserve Money Transmitting digital currency. Where criminals through Money Transmitting service providers convert their crypto currencies derived from the sale of narcotics amounting to US $ 6 billion to conventional currencies so that the money from criminal acts from the circulation of narcotics which was originally dirty money or dirty money, turned into clean money or clean money (Mabunda, 2018).
2. In 2019 the world witnessed $2.35 billion stolen in a PlusToken Ponzi scheme. The scam offers monthly payments to cryptocurrency wallet users before leaving the scheme and withdrawing wallet funds. Until finally Chinese law enforcement officials managed to arrest 109 people related to this fraud (Zhang, 2018).
3. Another criminal case is the Darknet marketplace which is a website, hosted on the dark web as a TOR hidden service (also known as an "onion service"). They can only be accessed through TOR, thus allowing safe and anonymous browsing. This black market facilitates drug trafficking, sale of stolen data, arms trafficking, human trafficking, sale of child sexual abuse material (CSAM) and more. This form of cryptocurrency crime is a particularly concerning example of how crypto is used to profit from illicit activities and then launder money (Hamilton, 2023) (US Dept of Justice, 2022).
4. As happened in Turkey in April 2021, the Thodex crypto asset trading platform owned by Faruk Fatih Ozer fled its customers' crypto assets of US $ 2 billion (equivalent to IDR 29 trillion). Thodex Inc as a cryptocurrency exchange service company in Turkey which is also engaged in investment and capital markets reportedly has more than 400,000 customers. The Thodex company led by Faruk Fatih Ozer initially launched a massive promotion to lure investors by giving direct gifts of Tesla luxury electric cars to the first 50 (fifty) investors worth 5 million Lira (more than 2.7 billion). Istanbul-based Thodex Inc. also uses a way to sell cryptocurrencies at prices 50 percent cheaper than normal prices. But it turns out that this is just a cover for fraud to attract investors alone which leads to the flight of investor money of more than Rp 29 trillion.

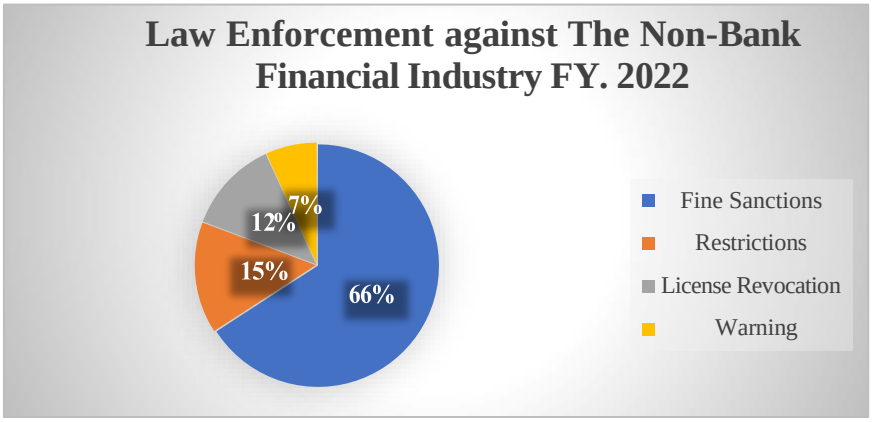
5. Black markets and scam shops accounted for more than $1.5 billion in cryptocurrency transactions in 2022, down from $3.1 billion the previous year. The decline was mainly due to the collapse of Hydra Market, the highest-revenue darknet market in 2022, which was shut down in a joint operation by law enforcement authorities of the United States and the Federal Republic of Germany in April 2022. The collapse of Hydra has left room for other markets to expand, which means authorities may now have more big players to investigate in the absence of a monopoly, as Hydra accounts for more than 93% of the darknet market value (Hamilton, 2023)
6. In May 2022, Terra USD and Luna tokens, two crypto tokens that hit highs just two months earlier, collapsed, wiping out the value of more than $40 billion of its customers' money. Many claim the currency is a Ponzi scheme, and the U.S. Security and Exchange Commission indicts the creators of the blockchain protocol for securities fraud in early 2022 (Commission., 2018).

Regulations Regarding the Use of Cryptocurrencies

The current condition is that crypto currencies have been circulating and began to be used as a means of transaction and investment in the country (Malherbe et al., 2019), but it is unfortunate that Indonesia does not have the right regulations to ensure the security of the financial industry and domestic monetary stability to face the emergence of crypto currencies. Public expectations that regulations and legal rules issued by the government are the basis for legal certainty and justice in transactions have not been achieved (Fenwick et al., 2017). The application of legal sanctions, both criminal and civil, for violations or crimes in the digital financial sector has not been clearly regulated in digital financial instruments so as to achieve legal compliance in the community. Cryptocurrency regulation itself is still a polemic and still refers to the implicit explanation that exists in the laws and regulations of institutions related to the financial and monetary sectors. This legal regulation must be firm, clear and certain, so that with clear and firm digital economy regulations in this digital economy era so that people avoid the potential emergence of various cases of crime and violations of the law in the digital service and financial sector (Bakhrul Amal, 2018), such as crimes in the insurance industry, capital markets, investment, financing, banking to financial technology (fintech).

The emergence of various problems is increasingly complex if there are not comprehensive regulations that become the rules of the game in the digital financial sectors. The use of crypto currencies as referred to in Law No.7 of 2011 concerning Currency, that crypto currencies are not issued by a country's monetary authority and are decentralized. Referring to existing regulations, it can be said that crypto currencies are currencies that are prohibited from being used in Indonesia. This is due to the characteristics of cryptocurrencies that are not managed by a country's Central Bank, pseudonymity, transactions are difficult to track and move peer to peer between users only and their value is very fluctuating so that no one is responsible if a problem occurs. In Law No. 7 of 2011 concerning Currency, it is also stated that without a managing and controlling institution, the use of digital currencies is likely to be used for unauthorized transactions and has the potential to become an entrance for financial sector crimes that can cause losses to the public, as well as the risk of disruption to the stability of the national financial system.

Table 2. LE against NBFI 2022, Source: PPATK



Meanwhile, law enforcement in the Non-Bank Financial Industry (NBFI) during 2022 has been carried out in the form of imposing fines on 164 business activities, restrictions on 37 business activities, license revocation on 31 business activities and warnings on 17 business activities.

The complex challenges experienced by the public and law enforcement in facing the phenomenon of the development of the digital financial system certainly demand the development of law both structure, content and culture to be in line with the reform of the criminal justice system as a whole. Criminal law regulations (judicial policy) play an important role as an effort to prevent crime, so it needs to be supported by government policies in an effort to prevent criminal behavior through criminal law enforcement that operates in the field by issuing a law that goes through several phases, namely:

1. The formulation phase or called legislative policy;
2. Application phase or called judicial/judicial policy;
3. Execution phase or called executive / administrative policy.

Legislation is the best legal shelter to formulate formal and material regulations, including those related to criminal penalties in law enforcement. The systematics of the formation of law is discussed in Law Number 12 of 2011 concerning the Preparation of Laws and Regulations. In addition, the legal process is also regulated in Law Number 27 of 2009 concerning MPR, DPR, DPD, and DPRD. Therefore, with the formal legal shelter that can anticipate the misuse of crypto currencies in various forms and patterns, both criminal and non-criminal, legal regulations are needed with the support of law enforcement officials who also monitor, indicate, and take action against suspected misuse of crypto currencies and anticipate potential crimes in them.

One of the efforts to prevent and overcome cryptocurrency crime can be done by establishing standard legal definitions and inviting countries in the world to adopt more uniform legal regulations. In this method, law uses its traditional aspects through rules to achieve a specific goal or policy. If in Law Number 7 of 2011 concerning Currency which is the basis for Bank Indonesia to reject crypto currencies because there are criminal provisions regulated in article 33 which reads," Everyone who does not use Rupiah in:

1. Every transaction that has the purpose of payment,
2. Settlement of other obligations that must be fulfilled with money and/or,
3. Other financial transactions. As referred to in article 21 paragraph 1, it shall be punished with a maximum imprisonment of one year and a maximum fine of Rp200 million."

Based on the phenomenon of the presence of crypto currencies as one of the results of technological innovation in the digital financial sector which is developing very rapidly in the

world, the author argues that a futuristic, responsive and integral financial sector regulation is needed with the renewal and harmonization of regulations in the financial sector by policymakers in the financial sector. Based on the above, the author examines the idea of revising or amending Law No. 7 of 2011 concerning Currency so that with the new law, it is hoped that legal regulations on the use of crypto currencies can prevent and overcome cryptocurrency crime in Indonesia, by forming special regulations governing the use and circulation of cryptocurrencies in Indonesia along with the increasing number of users and the value of currency transactions cryptocurrencies in Indonesia. The author has an idea for regulation of cryptocurrencies by requiring customer identity (Know Your Customer) and Bank Indonesia as the Central Bank is given the opportunity to issue Rupiah crypto currency which makes crypto currencies legal to use in Indonesia. So that the Indonesian people have certainty over the legal policies carried out by the government in the use of crypto currencies and are protected from potential crimes contained therein. This is as the purpose of the state is to protect all Indonesian people and Indonesian bloodshed and provide welfare for its people. The Indonesian government must certainly follow changes in the world's economic order and digital transaction system if it does not want to be left behind and ostracized by other countries in the global economy.

The Role of LE Officials in the Digital Financial Industry

Cryptocurrencies as part of the global financial industry, have a very complicated transaction scheme and are often carried out by perpetrators of Money Laundering (TPPU) because they know that law enforcement officials and global financial transaction supervisors will have many difficulties to track the movement of cryptocurrencies due to their pseudonymity, in addition to other difficulties arise when crypto currencies have been converted into local currencies (Dollars or Euros) There will be obstacles in tracking financial resources (follow the money). Law enforcement officials in the financial sector in Indonesia understand the recommendation of the Financial Action Task Force (FATF) Number 15 which stipulates that each country is required to make comprehensive regulations regarding New Payment Methods (NPM) including Internet Based Payment Services (FATF 2015). Therefore, it is necessary to have a risk assessment and risk management by considering government policies, so that appropriate policies can be formulated to minimize crime in the use of cryptocurrency.

That the FATF advises a country's national authorities to create a proactive coordination mechanism of information sharing in a way that promotes a deeper understanding of the risks of money laundering in the Cryptocurrency Ecosystem (EC). Furthermore, with a risk-based approach, the FATF will advise national authorities and their law enforcement officials to target specific 'nodes' that are most likely to be at the forefront of money laundering and whose activities intersect with the fiat currency financial system that has been regulated by the Central Bank of a country. Generally, in money laundering investigation activities carried out by law enforcement officials, the main strategy carried out by law enforcement officials is to follow the journey of money (follow the money), so that the predicate crime is known, which means that the journey of money still adheres to the centralized banking system.

The challenge for law enforcement officials is not easy, given the decentralized financial transaction system used by cryptocurrencies. In this system, the details of all cryptocurrency transactions are distributed to all account holders in a main report, analysis of transaction flows and the amount of value against the time of commission of the crime should allow law enforcement officials to find the pseudonyms of cryptocurrency users involved in criminal acts by following their transaction history, but this is not easy. Based on this, the increasing scale of illegal financial transactions seems to have motivated countries to see more serious risks from the impact of money laundering itself, by seeing the high risks presented in the use of

cryptocurrencies, some countries are trying to prepare regulations related to cryptocurrencies and increase the competence of law enforcement resources to be able to prevent and overcome crime cryptocurrencies.

The next challenge faced by law enforcement officials in efforts to prevent and combat cryptocurrency crime is to connect pseudonyms with real people, as already mentioned that the decentralized nature of cryptocurrencies makes it very difficult to trace financial sources. Cryptocurrencies are often widely used to commit crimes, because they know that they are not yet fully on the radar of criminal justice, many countries do not have clear regulations in regulating cryptocurrencies so that it is difficult to enforce the law. Whatever the case, cryptocurrencies already pose significant risks or are a potential threat that lies ahead. So, it is an obligation of law enforcement officials to ensure that the risks that exist or potential crimes of using crypto currencies can be widely understood to be minimized.

In the context of law enforcement of criminal problems that occur in the national digital financial industry, it seems that law enforcement officials in Indonesia can use 2 (two) methods of approach in their law enforcement efforts, namely through prosecuting mechanisms and non-prosecuting mechanisms in the financial sector which means litigation or non-litigation in solving violations or crimes in the financial sector. When using the prosecuting mechanism, the legal action will be based on Article 5 paragraph (1) of Law of the Republic of Indonesia Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering stated that "any person who receives or controls the placement, transfer, payment, grant, donation, custody, exchange, or use of assets that he knows or reasonably suspects is the result of a criminal act as referred to in Article 2 paragraph (1) shall be punished with a maximum imprisonment of 5 (five) years and a maximum fine of IDR 1,000,000,000.00 (one billion rupiah)."

Meanwhile, when using a non-prosecuting mechanism, the legal action will base a sense of justice, in deciding whether a case will proceed to the investigation stage or not proceed to the investigation stage, henceforth law enforcement officials apply the provisions of the una via and non-prosecution mechanism using parameters:

1. The value of the transaction and/or the value of losses for violations;
2. The presence or absence of settlement for losses arising from criminal acts;
3. Impact on the industry and/or the interests of customers, investors, and/or the public;
4. For the capital market, there are also considerations regarding as a result of criminal acts on securities offering and/or trading activities as a whole.

If it has fulfilled the elements of the occurrence of money laundering prosecuting mechanism, of course, it is clear that law enforcement officials can continue it as a criminal report and will be processed criminally to court. Meanwhile, the idea of non-prosecuting mechanism arises from the need for law enforcement against criminal acts in business activities that require law enforcement officials to pay attention to the nature of economic activities that not only intersect with aspects of criminal law, but also aspects of administrative law and civil rights.

So that the need for law enforcement in the financial sector plays a very significant role in providing a sense of security which is expected to trigger national economic growth and act as a locomotive of growth in the real economic sector through capital accumulation and technological innovation to create a variety of business models and financial products and services. Furthermore, if the problem is considered to be resolved by non-litigation mechanisms, the case is stopped and not continued to the investigation stage.

The spirit of applying the principles of non-litigation una via, non-prosecuting mechanism, and disgorgement is a manifestation of the restorative justice system. The goal in general is that criminal offenders are responsible for repairing losses caused by their mistakes. In terms of the financial services industry, this law enforcement model is expected to efficiently solve

problems fairly, quickly, and efficiently so that financial industry activities can continue to run and the integrity of financial markets is maintained.

This mechanism links the authority of law enforcement to prosecute corporate and business crimes and to delay or not prosecute with the condition that the perpetrator is willing to meet the terms and conditions (recovery of losses) set by law enforcement. The settlement will be made by damages sought through means of remedies that require the party who profited from the illegal or wrongful act to surrender any profits they gained as a result of the illegal act, offense, or crime (disgorgement). The non-prosecution mechanism is applied through the principle of una via as a principle that gives authority to authorities representing the public interest to choose whether to take action on criminal violations by taking administrative legal channels or criminal law channels to be subsequently transferred to the court.

A similar hybrid approach to criminal law enforcement in business activities is not new and has been implemented in several countries. In the end, law enforcement carried out in any sector is still aimed at accommodating people's sense of justice and realizing legal certainty, while being able to provide benefits for the interests of the nation and state as a whole. Efforts to achieve these three legal objectives simultaneously are expected to realize sustainable justice

CONCLUSION

Amendments to several laws governing the national financial industry by taxing the inclusion of customer identity with the intention of clearly knowing the ownership of crypto money and traceability if a criminal act occurs in it, as well as obtaining space for Bank Indonesia as the Central Bank to create a new digital currency also called Digital Rupiah or e-Rupiah or technology-based Crypto Rupiah blockchain. Enforcement measures and legal certainty that continue to be strengthened in financial institutions that have authority by preparing human resources in the form of competent personnel in the field of digital financial investigation through education and training programs in the form of collaboration between law enforcement institutions in Indonesia. This means that an education and training process is carried out for investigators who serve in the financial industry as an effort to fulfil the readiness of investigators in financial crimes who serve in the national financial sector and are able to implement litigation or non-litigation policies on legal problems that occur.

REFERENCES

Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. *Journal of Money Laundering Control*, *22*(2), 210–216.

Bakhrul Amal. (2018). Law & Society: History, Politics and Development,. *Thafa Media, Yogyakarta,*.

Christiani, T. A. (2016). Normative and empirical research methods: Their usefulness and relevance in the study of law as an object. *Procedia-Social and Behavioral Sciences*, *219*, 201–207.

Commission., S. and E. (2018). *The SAGE Encyclopedia of Surveillance, Security, and Privacy*. https://doi.org/https://doi.org/10.4135/9781483359922.n383

Cook, T. (2013). Evidence, memory, identity, and community: four shifting archival paradigms. *Archival Science*, *13*, 95–120.

Dayi, F. (2019). *The Global Financial System's New Tool: Digital Money BT - Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age* (U. Hacioglu (ed.); pp. 17–39). Springer International Publishing. https://doi.org/10.1007/978-3-030-25275-5_2

Fenwick, M., Siems, M., & Wrbka, S. (2017). *The shifting meaning of legal certainty in*

comparative and transnational law. Bloomsbury Publishing.

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., & Schellinger, B. (2021). Designing a central bank digital currency with support for cash-like privacy. *Available at SSRN 3891121*.

Hamilton, G. (2023). Department of Justice. *Foreword by Kevin D. Roberts, PhD Edited by Paul Dans and Steven Groves*.

Hasan, Z., Jayanti, E. D., Azlina, N., Lestari, R., & Muslim, M. (2022). Prospect of Islamic Electronic Money in Indonesia: Case Study on the LinkAja Application. *JESI (Jurnal Ekonomi Syariah Indonesia)*, *12*(1), 1–13.

Jatmiko, B. (2023). Bambang Jatmiko, BNI Presents MSME Flagship Products at ASEAN Summit. *Kompas Newspaper, May 12, 2023.*

Jauregui, B. (2018). Police Unions and the politics of democratic security and order in postcolonial India. *Qualitative Sociology*, *41*, 145–172.

Mabunda, S. (2018). Cryptocurrency: The New Face of Cyber Money Laundering. *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (IcABCD)*, 1–6. https://doi.org/10.1109/ICABCD.2018.8465467

Malherbe, L., Montalban, M., Bédu, N., & Granier, C. (2019). Cryptocurrencies and blockchain: Opportunities and limits of a new monetary regime. *International Journal of Political Economy*, *48*(2), 127–152.

Popkova, E. G., & Parakhina, V. N. (2019). Managing the global financial system on the basis of artificial intelligence: possibilities and limitations. *The Future of the Global Financial System: Downfall or Harmony 6*, 939–946.

Priyo Amboro, Y., & Christi, A. (2019). Prospek Pengaturan Cryptocurrency sebagai Mata Uang Virtual di Indonesia (Studi Perbandingan Hukum Jepang Dan Singapura). *Journal of Judicial Review*, 21(02), 14–40. https://doi.org/https://doi.org/10.37253/jjr.v21i2.665

Stokes, R. (2012). Virtual money laundering: the case of Bitcoin and the Linden dollar. *Information & Communications Technology Law*, *21*(3), 221–236.

US Dept of Justice. (2022). *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace*.

Yousafzai, A., Kumar, P. M., & Hong, C. S. (2021). CROWD-CDN: A cryptocurrency incentivized crowdsourced peer-to-peer content delivery framework. *Computer Communications*, *179*, 260–271.

Zhang, J. (2018). Public governance and corporate fraud: Evidence from the recent anti-corruption campaign in China. *Journal of Business Ethics*, *148*(2), 375–396.