International Journal of Religion
2024
Volume: 5| Number 10 | pp. 5180 – 5190
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/yd4xeh84

The Potential of Metaverse and Non-Fungible Token Abuse by Using Cryptocurrency

Ardhian Dwiyoenanto[1], Adi Sulistiyono[2], Hartiwiningsih[3]

Abstract

The advance of Information Technology is closely related to and has a direct impact on the development of people's lives. One of the real technological advancements that plays a major role in creating evolution in the community life order is Internet progress. As time passes, the internet world continues to experience rapid development, such as Metaverse, Non-Fungible Tokens (NFTs), and Cryptocurrency. Meanwhile, the change of regulations and legal products that are not as fast as the advance of the internet and the business world raises their abuse potential as means of Money Laundering Crime. The research method used was normative juridical with analytical descriptive research specifications. Metaverse, NFTs, and Cryptocurrency are relatively new phenomena in this globalization era. The lack of regulation and the high volatility of price characteristics that are strongly influenced by public interest make them potential as means to hide or disguise the origin of assets from criminal acts. So, this research was conducted to analyse the potential use of Metaverse and Non-Fungible Tokens as means of money laundering.

Keywords: *Cryptocurrency, Metaverse, Non-Fungible Tokens, Money Laundering Crime.*

INTRODUCTION

The advancement of information technology is very fast and has implications for making it easier for humans to carry out their daily activities. The development of human civilization in the field of science and technology, especially the sophistication of information, communication, and transportation is worldwide and seems unlimited. Globalization in a country is running so fast that it is impossible for a country to isolate itself politically, socio-culturally, economically, and legally in inter-country relations (Muladi & Priyatno, 2013). Along with the development of today's globalization era, all kinds of community activities cannot be separated from technological assistance (Wahyuni & Turisno, 2019). The combination of technological advances and the rapidly growing business world create a breakthrough and all forms of innovations that can increase the ease of doing business. Many factors influence the rapid acceleration of technological progress. Increasing and diverse human needs or increasingly complex threats in terms of natural disasters, food crises and pandemics that plagued the world in early 2020. It did not only cause a crisis and threaten the economy, but accelerated the digitalization process in various aspects since it began to spread (Grover & Sabherwal, 2020).

Some technological advancements that currently become a hot topic to discuss are Metaverse, non-fungible tokens (NFTs) and cryptocurrency. Metaverse is defined as a virtual environment also known as MUVE (Multi-User Virtual Environments), which has a format derived from MMORPG (Massive Multiplayer Online Role-Playing Games) and allows everyone to meet avatars in 3D video games by combining augmented reality (AR), virtual reality (VR), and the internet. So, the existence of the Metaverse and its supporting technological devices allow users to feel the sensation of being in a very real virtual environment (Hwang & Chien, 2022). The term 'metaverse' then increasingly grabbed the public's attention when Mark Zuckerberg, CEO of Facebook, in 2021 announced that Facebook was changing its name to 'Meta' and humans would move their activities to the virtual world. He announced that "the metaverse is the next big thing" (Kraus et al., 2022). It was an internet revolution from Web 2.0 to Web 3.0 (Kim, 2021). By 2025, it is estimated that 25% of the

[1] Universitas Sebelas Maret, Surakarta. E-mail: Ardhian.dwiyoenanto4@student.uns.ac.id

[2] Universitas Sebelas Maret, Surakarta. E-mail: Adi.Sulistiyono@student.uns.ac.id, Orcid number: https://orcid.org/0000-0003-2832-1546

[3] Universitas Sebelas Maret, Surakarta. E-mail:, Hartiwingsih@staff.uns.ac.id, Orcid number: https://orcid.org/0000-0003-3761-9117

world's population will spend at least one hour in the Metaverse, either to transact in the virtual world or for other activities such as work.

In addition to the Metaverse, other aspects related to technological developments that have a direct link to the business world and are closely related to the metaverse NFTs and cryptocurrencies. NFT is a type of item that can be traded and displayed its ownership in the Metaverse world and cryptocurrency is a virtual currency used for transactions in the metaverse world.

NFT comes from the words 'fungibility' and 'token'. NFTs are digital assets that represent valuable items with value that cannot be replaced or exchanged. They derive value from uniqueness, rarity, and demand (Lawson & Gooding, 2005). Each NFT itself has transaction record data on the blockchain. This data contains the inventor, price, and ownership history (Santosa, 2023) (Santosa, 2023). From an economic point of view, it is said that a fungible asset is something that can be defined as units just like money (paper/coins). In principle, the Metaverse is a 3D virtual world network that focuses on social interaction. Within the metaverse, people can interact socially and economically using avatars (virtual representations) (Akkus et al., 2022). Although often associated with virtual reality headsets, the term does not refer to a specific type of technology, but rather how individuals interact with technology. Its main characteristics include virtual worlds that continue to exist even when one is not participating, and augmented reality that combines the digital and physical worlds. The metaverse also applies to the digital economy, where users can create, buy, and sell goods. The 3D virtual world game Decentraland is a good example, where users can buy virtual plots of land using cryptocurrency, create art and fashion items that are sold as NFTs in virtual galleries and shops, and interact with each other. Large amounts of money are traded through the platform. One of the most expensive pieces of virtual property traded in the game was sold for $3.5 million(Gorny, 2022). The Metaverse also allows people to interact and conduct transactions just like in the real-world using avatars (Davis et al., 2009).

The development of Metaverse and NFTs cannot be separated from cryptocurrency. Cryptocurrency is a payment instrument used in the buying and selling process of NFTs, and is predicted as a currency instrument in business or economic activities in the metaverse world, making itself an inseparable ecosystem from the Metaverse and NFTs. Similar to other aspects of technological progress, technological and internet advances in the metaverse field do not escape the shadow of various forms of cyber-crime that may occur. According to Christian Laue, some forms of crime that may occur in the Metaverse world are cyber-crimes (Laue, 2011). In line with what was conveyed by J. E. Sahetapy (Wahid & Labib, 2005), crime is closely related to the development of society; the more advanced the life of society, the more advanced the crime. It is also part of the result of culture itself. This means that the higher the cultural level and the more modern a nation is, the more modern the crime is in its form, nature, and method of implementation. The dynamics of science and technology in today's society not only have a positive impact, but also have a negative impact on the incompatibility of its use (Sudjito et al., 2016).

The development of globalization is accompanied by the development of crime, in other words, they should be linearly proportional to the anticipation of the development of crime through the development of the rule of law. In addition to cyber-crime, technological advances that are closely related to the economy are faced with the potential for money laundering. Money laundering itself is one of the major challenges in realizing a financial system with integrity. Its activities are the cause of the decline in a country's economic growth and high crime rates (Kostadinovic et al., 2021). It is literally also labelled money bleaching, money panning, or also called the act of legitimatising illegitimate income (N.H.T, 2005). Some common modes of money laundering include Loan Back, which is borrowing one's own money. In this mode, the person borrows money from a foreign company, but in fact the company is a shadow company (*immobilien* investment company) whose directors and shareholders are himself, in the form of 'back to loan', where the perpetrator borrows money from a foreign bank branch by 'a standby letter of credit' or 'certificate of deposit' that the money is obtained on the basis of money from crime; the loan is then not returned so that the bank guarantee is disbursed (Hibnu Nugroho, Budiyono, 2016).

As explained by Ivan Yustiavandana, the choice of various modes to commit money laundering results in the difficulty to develop legal provisions that are able to cover all these possibilities (Kostadinovic et al., 2021). On the other hand, anti-money laundering legal provisions must also protect the community, for example not hindering labour-intensive investment. The perpetrators of money laundering are not only committed by

individuals, but often, are committed by an organized crime or a crime motivated by white-collar crime. The white-collar crime includes official crime, corporate crime, professional crime, and individual crime (Suartini & Dewi, 2019).

The growth of various modes in the practice of money laundering and the increasing amount of money processed illegally are inseparable from the influence of globalization in all aspects of life. Globalization not only supports legitimate economic activities, but also illegal economic activities, and the emergence of information networks, communications, transportation activities and global financial intermediation. It does not only allow business actors to adopt various aspects of international management organization and operationalization, but also the negative ones used by criminals (Stessens, 2000). The advance of blockchain technology and its use as a pillar of the Metaverse, NFTs, and cryptocurrencies is certainly more rapid than the legal instruments that regulate it. Legal instruments in this case include policy issues related to regulations aimed at protecting the interests of the community as well as policies that are crime prevention or criminal policy. Criminal law policy in this case includes anticipatory actions and the eradication of money laundering that uses Metaverse, NFTs, and cryptocurrency as means of hiding or disguising the proceeds of criminal acts.

Based on the results of previous research, no one has discussed about Metaverse, NFTs, and cryptocurrency; how the vulnerability of Metaverse, NFTs, and cryptocurrency are, to be instruments or means to hide or disguise the origin of the assets resulted from criminal acts; and the challenges of law enforcement of laundering that uses the means of Metaverse, NFTs, and cryptocurrency. So, it is very interesting to explore how the development of the money laundering regime and the modus operandi carried out by the perpetrators of money laundering, and how the potential of Metaverse, NFTs, and cryptocurrency are, to be used as means to hide or disguise the origin of assets resulting from criminal acts or money laundering.

METHODS

This research activity was carried out as an effort to understand and solve problems scientifically, systematically, and logically (makes sense). (Amirudin & Asikin, 2018) It was initiated because of the gap between *das sollen* and *das sein*, that is between the existing theory and the reality that occurs in the field. The method used was the normative juridical approach considering the problems studied, in addition to relying on juridical aspects, such as norms, regulations, and legal theories (Diantha, 2016). In other words, this research not only refers to applicable legal products but also the reality that occurs in the field. The specification was descriptive analytical because this research is expected to obtain a clear, detailed, and systematic representation, and the data obtained were analysed for solutions to problems in accordance with applicable legal provisions. So, it could provide an overview of the reality on the object being studied objectively (Zainudin, 2019).

RESULTS AND DISCUSSION

Money laundering is an international phenomenon and challenge. All countries agree that money laundering is a criminal offense that must be faced and eradicated (Kostadinovic et al., 2021). In Black's Law Dictionary, money laundering is defined as *terms used to describe investment or other transfer of money flowing from racketeering, drug transaction and other illegal sources into legitimate channels so that its original sources cannot be traced.* In general, the definition of Money Laundering Crime is a series of actions on assets that are known or reasonably suspected of originating from the proceeds of a criminal offense with the aim of hiding or disguising the origin, source, location, designation, transfer of rights, or actual ownership. Its purpose is to legalize money gained from a criminal act by inserting it into the financial system, legal business activities, or other ways. In principle, it is any action with the aim of disguising or concealing the origin of the proceeds of a criminal offense. Considering the principle of the crime, it requires the following aspects:

a) Suspicion of Predicate Crime

b) Assets from proceeds of Crime

Yunus Husein mentioned that the problem of money laundering has long been recognized by the international world. The issue of money laundering began to be recognized in America in 1830, where many

parties used money from criminal acts to buy companies. Alcapone as one of the mafias who tried to trick the government by setting up a laundry company as a means of mixing the proceeds of crime, so that it could not be suspected that the nature of the money came from a criminal act. This is what later inspired the birth of the term 'money laundering'.

The term was first used in newspapers associated with the news about the Watergate scandal in the United States in 1973 (Sjahdeini, 2012). The term 'money laundering' was first used in newspapers associated with the news about the Watergate scandal in the United States in 1973. It gained popularity in 1984 when Interpol investigated the money laundering by US mafia, known as pizza connection case involving US$600 million, which was transferred through a series of complex financial transactions to banks in Switzerland and Italy (Harmadi, 2011). From this case, we can see that criminals actually use legal companies to launder the proceeds of crime with the aim of making it appear as assets derived from legitimate activities.

One of the steps taken by the international community, in this case the G-7 countries, in order to make efforts to prevent and eradicate money laundering was the establishment of The Financial Action Task Force (FATF) in 1989. FATF is a task force that has the task of preparing international recommendations to eradicate money laundering (Husein & Robertus, 2018). The recommendations issued by the FATF then become guidelines for each country in compiling and forming regulations related to efforts to tackle money laundering. FATF in 1990 for the first time issued 40 recommendations as a comprehensive framework for eradicating money laundering crimes. It is designed as a policy-making organization consisting of legal experts, financial experts, and law enforcement to succeed national legislation and arrangements of anti-money laundering and anti-terrorism financing. FATF is an intergovernmental organisation of member states working at the policy-making level (Husein & Robertus, 2018).

In Indonesia, the criminalization of money laundering was marked by the enactment of Law Number 15 of 2002 on the Crime of Money Laundering. The enactment of the Law cannot be denied as a consequence of Indonesia's inclusion in the NCCT's (Non-Cooperative Country and Territories) list by the FATF. Indonesia is considered not to comply with anti-money laundering regulations as outlined in the recommendations issued by the FATF. As a reaction to this determination, the Indonesian government then criminalized money laundering through this Law. But it was considered not perfect to follow the anti-money laundering system based on the FATF Recommendation. So, Indonesia formed Law No. 25 of 2003 which amended and complemented Law No. 15 of 2002, which also includes changes of article criminalizing money laundering. After the formation of the two laws, finally in 2005, Indonesia was declared out of the NCCT's list. The next step in the anti-money laundering regime was the establishment of Law No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering, in order to fulfil national interests and adjustments to international standards that are expected to become a legal basis to ensure legal certainty, effectiveness of law enforcement, and the tracing and return of assets resulting from criminal acts (Rahayuningsih, 2013).

It is undeniable that over time, criminals continue to develop or carry out various ways to hide or disguise the origin of assets resulting from criminal acts. They include the use of more sophisticated methods or the loopholes that exist in statutory provisions. Such methods make the perpetrators of crime become increasingly shrewd and difficult to detect by law enforcement officials in hiding the assets of the proceeds of crime.

Billy Steel said that money laundering is the lifeblood of drug dealers, fraudsters, Smugglers, arms dealers, terrorist, extortionist and tax evaders (Jatna & Mantovani, 2018). Such an important position of proceeds of crime in the process of money laundering has slowly changed the paradigm of law enforcement which originally focused on following the suspect to the paradigm of following the money. The concept of follow the money emphasizes that money laundering law enforcement is carried out through tracing the flow of assets resulting from criminal acts. Thus, it is expected to be able to narrow the space for the perpetrators of criminal acts.

In its development, when money laundering law enforcement was first implemented, the understanding that guided the understanding of money laundering went through three stages, namely the placement, layering, and integration processes. However, they are not an element, but only a basic pattern in conducting money

laundering. The banking system is one of the instruments mostly used by criminals to launder money, mainly by relying on those processes. The criminals assume that by using banking services, the mechanism of money laundering becomes easier to do, because in addition to being safe, bank also has a system of confidentiality (bank secrecy) related to customer profiles and transaction activities to be protected.

Realizing that bank is an easy target for money laundering by criminals, the government then tightened regulations related to the banking system mechanism, by optimizing the application of the 'know your costumer principle'. Through this application, it is easier for banks to detect if there is a flow of funds that does not match the profile of the customer concerned. Under certain conditions, if it is not sufficient to ensure the transparency of the data provided by the customer, the bank has the authority to increase profiling using the 'enhanced due diligence' mechanism. With this optimization, it will further narrow the space for criminals to use banking instruments as a means of money laundering.

Besides profiling, financial service providers, both banks and non-banks, are designated as reporting parties, or in this case have reporting obligations for any transactions required by law to be reported to the Financial Transaction Reports and Analysis Center. This reporting obligation is certainly part of the effort to narrow and complicate the space for money launderers. Money launderers who began to realize the increasingly strict banking regulations then tried other alternatives in conducting their action, no longer fully using banking services. They tried to hide the proceeds of crime through the instrument of goods and services providers. This method is considered relatively safer because the perception of criminals is that anti-money laundering regulations on goods and service providers are not as strict as those in banking regulations.

The skill of the modus operandi carried out by the perpetrators of money laundering in hiding the proceeds of crime makes the its pattern through the process of placement, layering, and integration begin to be abandoned. The perpetrators realize that it is necessary to find and develop other modus operandi that is difficult to detect by law enforcement officials. Egmont Group has released several ways or typologies of money laundering, among others:

Concealment within business structure, which is an attempt to hide criminal funds into the normal activities of the business or into an existing company controlled by the organization concerned.

Misuse of legitimate business, i.e., using an existing business or established company to carry out the money laundering process without the company's awareness of the crime that is the source of the funds.

Use of false identities, documents, or straw men, i.e., by handing over the management of assets derived from crime to someone who has nothing to do with the crime by using false identities and documents.

Exploitation of international jurisdictional issues by manipulating the differences in regulations and requirements that apply between one country and another, for example regarding bank secrecy, identification requirements, disclosure requirements, and currency restrictions.

Not only in modus operandi or typology, the development of the money laundering process has also developed in the categorization of the perpetrators. If in the past the perpetrators of crime laundered the proceeds of crime themselves, today the perpetrators of crime make it possible to involve other parties who are not participated in the predicate crime to carry out money laundering.

The perpetrators of money laundering utilize certain professions, such as solicitors or attorneys, accountant's financial advisors, notaries, and other fiduciaries to obscure the origin of money that actually comes from a criminal act (Husein & Robertus, 2018). The perpetrators of money laundering utilize certain professions, such as solicitors or attorneys, accountant's financial advisors, notaries, and other fiduciaries to obscure the origin of money that actually comes from a criminal act. The services provided by these professions are manipulated by money launderers to hide the identity of the perpetrator and distribute the profits obtained from criminal acts. Typically, the trick is to use the accounts of solicitors or attorneys to place funds through the placement and layering stages, for example in banks, by offering offers the anonymity of the solicitor-client privilege in the same relationship with accountant lawyers to establish fake companies to build increasingly complex and complicated networks with the intention of hiding or obscuring the origin and proceeds of crime and at the same time hiding the identity of the parties involved.

Immediate Outcome 7 FATF (IO 7) divides the classification of launderers into self-laundering and third-party money laundering. Gabriele Bernescone (2015) defines self-laundering as the crime committed by the person who uses, substitutes, or transfers money, goods or other benefits in or to economic, financial, speculative or entrepreneurial activities deriving from a crime committed by himself in order to hide their criminal origin. Third party money laundering in the provision is defined as the laundering of proceeds by a person who was not involved in the commission of the predicate offense. Self-laundering is defined as the laundering of proceeds by a person who was involved in the commission of the predicate offense. If interpreted further to the definition of 'person involved' as mentioned in IO 7, it includes the person who commits, the person who participates in committing and the person who assists the criminal act of money laundering.

Money laundering is a 'serious crime' that can affect the economy as a whole, as well as hinder the social, economic, political, and cultural development of communities around the world (Yusuf, 2014). The United Nations Convention Against Illicit Traffic in Narcotics, Drugs and Psychotropic Substances of 1988 defines Money Laundering as the transfer of property derived from the proceeds of serious offenses or crimes with the aim of hiding or disguising illegal property to avoid the legal consequences of its actions; or disguising the true nature, source, location, rights relating to the ownership of such property. Meanwhile, according to FATF, money laundering is the processing of criminal proceeds to disguise their illegal origin to legitimize the ill-gotten profit of crime.

Basically, the core of the criminalization of money laundering is the act of hiding or disguising the origin of assets resulting from criminal acts, so that the assets appear as if they are legitimate assets. The fulfilment of the element of hiding or disguising the origin of the proceeds of crime is what then becomes the difference between active perpetrators and passive perpetrators of money laundering offense.According to Simons, in some formulations of the offense, we can find a requirement in the form of certain circumstances that must arise after an act is committed by a person, where the emergence is decisive, so that the person's actions can be called a punishable act. In relation to the crime of money laundering, actions are considered to fulfil the formulation of the offense if the action is carried out with the aim of hiding or disguising the origin of an asset. The effort or purpose to 'hide or disguise' is what becomes *bestandelen delichten* or the core offense of criminalization of money laundering. Based on doctrine and jurisprudence, in general, the phrase 'conceal' is defined as an activity carried out in an effort, so that other people will not know the origin of the assets, including not informing the Financial Service Provider officers about the source of funds. The act of disguising is the act of mixing illicit money with halal money, so that illicit money appears as if it comes from legitimate activities, exchanging illicit money for other currencies, and so on. So, the modus operandi of criminals in committing money laundering continues to evolve. Investigators should think that criminals will constantly evaluate techniques in laundering money when one of their modes can be revealed by law enforcement officials (Garnasih, 2017).

Judging from the special characteristics of the Metaverse, NFTs, and cryptocurrencies, their potential to be used as a means to commit money laundering or hide the proceeds of crime is very big. To identify how the potential of Cryptocurrency abuse as a means of money laundering, the first thing that then needs to be explained is what is meant by cryptocurrency, NFTs, and Metaverse. Cryptocurrencies are electronic currencies created with cryptographic algorithms. These currencies can be exchanged on a peer-to-peer basis. In other words, sending cryptocurrency from one person to another can be done without having to pass through certain financial authorities (Chatterjee, 2015). Cryptocurrency or virtual currency is a new innovation resulting from developments in the world of digital payments in line with the development of the world of technology and internet networks, especially in payment systems and digital payment facilities that exist today. The first cryptocurrency product is known as Bitcoin which has grown rapidly since it was created in 2009 (Amboro, 2019). The evolution of digital currencies has impacted cheque cash, credit cards, and debit cards from being something that has to be carried around to something that can be controlled through a smart phone (Berger, 2014).

Compared to traditional currencies, cryptocurrencies have the following advantages and characteristics:

Irreversible - transfer and payment process cannot be changed or cancelled. In addition, all transactions can be tracked and permanently stored in a digital database named block chain.

Pseudonymized and decentralized - there is no third party (central management such as banks) involved in the entire cryptocurrency system, and all users are also pseudonymous. Therefore, based on the transaction information we cannot obtain the real identity of the user.

Secure and permissionless - cryptocurrency security is guaranteed by public key cryptography and blockchains consensus mechanism which is difficult for criminals to break into. Moreover, there is no need to apply for any authority or license to use cryptocurrencies.

Fast and global - transactions with cryptocurrencies can be completed in just a few minutes. Cryptocurrencies are also global in nature as they are largely based on blockchains which has two implications, firstly anyone in the world can use them and secondly the geographical location of the user has little effect on the speed of the transaction (Grover & Sabherwal, 2020).

Since introduced to the public, Bitcoin has been under suspicion because it is considered anonymous and irreversible. It has sparked concern among financial regulators and governments because Bitcoin's anonymity is considered to facilitate crimes, such as money laundering and terrorism financing. The anonymity allegedly cannot be controlled by central entities such as central banks, so it does not comply with existing regulations (Jatna & Mantovani, 2018). The widespread use of cryptocurrencies will make it difficult for central banks, especially in controlling the supply of money (Kang & Lee, 2019).

This anonymity of crypto is then a great potential to be used as a means to commit money laundering. That most cryptocurrencies today are based on a technology called blockchain that connects users to each other through a series of blocks, so that when a transaction is made, what appears is a collection of block numbers (Jabotinsky, 2020). Blockchain itself is decentralized because it is a distributed ledger system, meaning that no single user controls the information or data on the blockchain, and no one is responsible for maintaining its proper functioning (Schrepel, 2019). It then causes anonymity in cryptocurrency ownership. Based on some researches, cryptocurrencies should be one of the entities that global anti-money laundering programs pay attention to. This is for two reasons; firstly, anti-money laundering programs focus attention on suspicious transactions. This focus seeks to combat the attempts by perpetrators to place the proceeds of illegal activities such as corruption tax evasion terrorism financing into the legitimate financial system. Secondly, cryptocurrencies need to be a focus of global planning because they offer new ways of using verification practices that virtually cross political boundaries. They are parts of digital currencies, which may have centralized institutions or be based on decentralized networks (Trautman, 2014). They, theoretically, give a challenge to global anti-money laundering regimes that consistently pose a threat to financial regulators and law enforcement (Campbell-Verduyn, 2018).

If we look at how the banking system works, banks are charged with the obligation to profile the identity of customers who want to use their services. Then, banks have an obligation to analyse verify or in this case ensure that every transaction carried out by customers is not a transaction related to a criminal act. They also have to submit a report to the party that has the authority or in this case, for example, the Financial Transaction Reports and Analysis Center (*Pusat Pelaporan dan Analisis Transaksi Keuangan*/PPATK) relating to the transactions suspected of being closely related to a criminal act or meeting the classifications as transactions that are required to be reported to PPATK and law enforcement officials. Besides, banks have the authority or even the obligation to temporarily suspend transactions or block accounts that are suspected of having a strong link to a criminal offense. If the bank does not carry out obligations related to the anti-money laundering regime, it is possible that the bank will be sanctioned in accordance with what has been determined by law.

In terms of financial integrity, criminal and terrorist organizations trust the integrity of cryptocurrencies in disguising their internal transactions. Here, cryptocurrencies are seen to facilitate money laundering, sanctions evasion, cybercrime, fraud, and terrorism financing, as each element of a cryptocurrency can evade taxation by governments. This can be understood as a consequence of the absence of centralized regulation from a government agency. In Indonesia, one of the money laundering cases using Bitcoin as a means of money laundering was a case of corruption and money laundering that occurred at PT Asabri (Novina Putri Bestari: 2021).

The characteristics of cryptocurrencies, in which their use does not go through any Financial Service Authority, result in a lack of supervision of traffic between one individual to another, so it's unlike the flow of currency transactions that use banking services, both the government and law enforcement officials will have difficulty tracking or monitoring the flow of cryptocurrency transactions like other commonly used currencies. The next characteristic is that cryptocurrencies operate singularly as the user's address cannot be linked to the identity of the owner in the real world. It becomes the biggest challenge in efforts to implement anti-money laundering policies, because the characteristics of anonymous crypto contradict the essence of the anti-money laundering regime program, that is the application of the 'Know Your Customer' principle. Pseudonymity makes users unrecognizable at the same time every Bitcoin transaction is recorded on the Blockchain. All transaction records can be seen by all users, so in the Bitcoin system, users can be recognized and transactions can be traced (Budhi, 2021).

Pseudonomity itself contradicts the transparency of wealth ownership, so this condition is an easy space for criminals to be able to use cryptocurrencies as a means to hide or disguise the origin of assets resulting from criminal acts. Due to the sophisticated encryption methods in cryptocurrency, it can then be used as a profitable means of payment on the dark market (Dark Web or Darknet), such as to pay for drugs, pornography, fake documents, weapons, and ammunition (Srokosz & Kopciaski, 2015).

As a means of money laundering or hiding the proceeds of crime, NFTs become asset in digital form that is stored on a distributed public ledger that records transactions and has a unique identification code and metadata that is different from each other on the blockchain network. They represent real-world objects such as artwork paintings, animations, photos, videos, drawings, music, signatures, tickets, and other creative works. Each cryptocurrency is considered equal to the others, so the tokens can be exchanged or called fungible tokens (Sulistianingsih & Khomsa Kinanti, 2022).

NFT technology is still relatively new, so there are many scopes of NFTs that do not yet have regulations. In terms of Intellectual Property, NFTs can be considered a simplifying tool as well as private property that has no form, meaning that the item cannot be held or touched but has a certain level of value assigned to the item. In this case, it needs to be emphasized that ownership of NFTs does not make the owner have unlimited rights to his work. If the artist wants to transfer his ownership of the copyright or exclusive rights to the collector, it must be done through a smart contract. However, the use of smart contracts on the blockchain is still premature in both technical and legal terms (Sadiku et al., 2018). NFT is a rich copyright that includes moral rights and economic rights.

Based on Yosafat Caesar Sinurat's research, the report from Non-Fungible.com states that although NFTs experienced a downturn from 2018 to 2019, a surge occurred in the following years, from 2019 to 2020, there was an increase of 97.09% in active wallets, 66.94% in the number of active buyers, 24.7% in the number of creators or sellers, and an increase of 29% in the amount of money rotating (Siregar & Sinurat, 2019). This case leads to a conclusion that the NFT market was experiencing a very rapid surge, and in the report, it was also mentioned that in 2021 there was a surge, although not significant, it will still be a fertile field, especially when it comes to crime (Fairfield, 2022).

Cyber money laundering uses features provided on the internet, and converts real-world money into virtual currency. Cyber Laundering is the latest in money laundering techniques (Marley, 2022). When it is done through cyberspace, the speed of the money laundering process increases rapidly. This is also supported by the internet's lack of binding legal power, the anonymity of the internet without physical contact, the wide reach, and the fast speed of transactions. Thus, it will rise the probability of an increase in money laundering crimes committed through cyberspace (Sinurat et al., 2022). It is undeniable that the advancement of technology and business world always exceeds the boundaries of existing regulations.

Although every detail of every transaction is recorded, there is an anonymity feature provided by many marketplaces to protect the real identity of the user. In other words, anyone can use a fake identity to make transactions on the relevant marketplace. It can happen because many marketplaces do not apply the 'Know Your Customer' principle to get the real identity of the user. For example, if we want to create an account on the OpenSea marketplace, the identity required is only an email address, as well as the wallet number of the

cryptocurrency that has been previously created to make transactions. A user can falsify their identity by creating a fake email address, and use a fake identity to create a cryptocurrency wallet, and then they can transact freely. It can be dangerous if a person creates multiple accounts to perform transactions, or even transactions with other fake accounts created independently.

Apart from the examples mentioned, one of the great potentials for NFT abuse in the money laundering mechanism is because NFTs basically have no real value, so the price of the NFT depends solely on how much the offer is given by the next buyer. It is known as 'Greater Fool Theory', which means that something is basically valued not because it has intrinsic value but many stupid people who want to buy the asset at a higher price than the previous buyer.

Because the value of the NFTs depends solely on how much it is offered by the next buyer, there is a big challenge from the potential abuse of NFTs as means of money laundering. As an illustration, if the NFT price is only based on the desire or a large offer from the next buyer, the criminals will use this instrument. They can carry out a transaction mechanism as if the transaction is carried out by NFT. But in fact, the process is a process of handing over the transfer of criminal proceeds wrapped in a legitimate underlying transaction, as if it were NFT sale and purchase activity.

The criminals create NFTs then sell them on the official trading platform. The prospective buyer provides a price offer and the criminal who previously made the NFTs accepts it. The issue of anonymity is also vulnerable to causing NFTs to be misused for money laundering practices by means of criminal groups creating NFTs anonymously, registering them to the market-place and then transacting the NFTs themselves (Jordanoska, 2021). At first glance, the case is only a legal event where there are two parties who bind themselves in the form of buying and selling, but in fact, it has the potential to be an attempt to hide or disguise the proceeds of criminal acts. The seller and buyer can sell at a high price with a buyer who has been determined by the person, then there will be a delivery of a number of funds (money), but in the end, the money is the property of the proceeds of criminal acts.

Recent studies show that the potential market in Metaverse ranges from 3.75 billion dollars to 12.46 billion dollars (Safari Kasiyanto, Mustafa R. Kilinc: 2022). Both NFTs and cryptocurrencies have similarities of why the two instruments have great potential to be used as means to hide or disguise the origin of proceeds of crime, so there are characteristics of pseudonomity in both. This pseudonymity is very contrary to the 'Know Your Customer' principle applied to financial services systems such as banking and non-banking. It is preferred by criminals because it will cover the true identity of the owner.

In Metaverse, the concept of activity is based on what happens in the real world itself, where everything uses money. The difference between buying and selling activities in the real world and the metaverse world is the payment system that uses cryptocurrency (Marley, 2022). Because the payment mechanism in the metaverse is only possible when using cryptocurrency, it requires the implementation of more complex laws and regulations (Kasiyanto & Kilinc, 2022). To sum up, cryptocurrencies, NFTs, and metaverse as a series of technological advances can be abused by criminals to hide or disguise the origin of assets resulting from criminal acts. It can be seen that, in principle, cryptocurrencies and NFTs have a pseudonymous characteristic which makes it possible to hide the identity of who is the owner of the asset.

CONCLUSION

Criminals at present are more and more careful to utilize technological advances to avoid themselves from the criminal activities they carry out and the profits they earn using digital banks and electronic money transfer systems. It allows them to buy, sell, and exchange goods without the need for physical interaction. Globalization presents technological advances that can be used by criminals to find new modes of stealing money, including the use of blockchain technology, such as cryptocurrency/Bitcoin NFTs and Metaverse as means to hide the proceeds of crime. Cryptocurrencies and NFTs have the anonymity characteristics, that can provide secrecy in transactions, of course, this is in contrast with the principle of 'Know Your Customer' or 'customer due diligence' which are means of anticipating money laundering. Consequently, many criminals

choose them because their identity is not revealed and they can still use money from the proceeds of crime through the use of cryptocurrency and NFTs.

REFERENCES

Akkus, H. T., Gursoy, S., Dogan, M., & Demir, A. B. (2022). Metaverse and metaverse cryptocurrencies (meta coins): bubbles or future. *Pressacademia*. https://doi.org/10.17261/Pressacademia.2022.1542

Amboro, F. Y. P. (2019). Prospek Pengaturan Cryptocurrency sebagai Mata Uang Virtual di Indonesia (Studi Perbandingan Hukum Jepang Dan Singapura). *Journal of Judicial Review*, *XXI*(2), 14–40.

Amirudin, & Asikin, Z. (2018). *Pengantar metode penelitian hukum* (Cetakan ke). Rajawali Press.

Berger, W. (2014). Bitcoin and the internet of money. *Wall Street Journal.*, *12*(8), 67–81.

Budhi, I. G. K. (2021). *Bitcoin* (Pertama). Radjawali Pers.

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, *69*(2), 283–305. https://doi.org/10.1007/s10611-017-9756-5

Chatterjee, C. (2015). Legal aspects of trade finance. In *Legal Aspects of Trade Finance* (1st ed.). https://doi.org/10.4324/9781315707969

Davis, A., Murphy, J., Owens, D., Khazanchi, D., & Zigurs, I. (2009). Avatars, people, and virtual worlds: Foundations for research in metaverses. *Journal of the Association for Information Systems*, *10*(2), 90–117. https://doi.org/10.17705/1jais.00183

Diantha, I. made pasek. (2016). *Metode Penelitian Hukum Normatif dalam Justifikasi Teori Hukum* (Winatsari (ed.); I). PT Interfajar Pramatama Mandiri.

Fairfield, J. (2022). Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property. *Indiana Law Journal*, *97*(4), 1261–1313. https://papers.ssrn.com/abstract=3821102%0Ahttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=3821102

Garnasih, Y. (2017). *Penegakan hukum anti pencucian uang dan permasalahannya di Indonesi* (Cetakan ke). Rajawali Pers.

Gorny, T. J. (2022). *AML Regulations and the Metaverse*. Sanctions.Io. https://www.sanctions.io/blog/aml-regulations-and-the-metaverse

Grover, V., & Sabherwal, R. (2020). Making sense of the confusing mix of digitalization, pandemics and economics. *International Journal of Information Management*, *55*(1), 102234. https://doi.org/10.1016/j.ijinfomgt.2020.102234

Harmadi, H. (2011). *Kejahatan Pencucian Uang, Modus-modus pencucian uang di Indonesia (money laundering)* (Pertama). Setara Press.

Hibnu Nugroho, Budiyono, P. (2016). Penyidikan Tindak Pidanan Pencucian Uang Dalam Upaya Penarikan Asset. *Jurnal Penelitian Hukum De Jure*, *16*(1), 1–2.

Husein, Y., & Robertus, K. (2018). *Tipologi dan Perkembangan Tindak Pidana Pencucian Uang* (Revisi). Radjawali Pers.

Hwang, G.-J., & Chien, S.-Y. (2022). Definition, roles, and potential research issues of the metaverse in education: An artificial intelligence perspective. *Computers and Education: Artificial Intelligence*, *3*, 100082. https://doi.org/10.1016/j.caeai.2022.100082

Jabotinsky, H. Y. (2020). Fordham Intellectual Property , Media and Entertainment Law The Regulation of Cryptocurrencies : Between a Currency and a Financial Product The Regulation of Cryptocurrencies : Between a Currency and a Financial Product. *Fordham Intellectual Property, Media and Entertainment Law Journal Volume*, *31*(1), 118–165.

Jatna, N., & Mantovani, R. (2018). *Rezim Anti Pencucian uang dan Perolehan Hasil Kejahatan di Indonesia* (Cetakan II). UAI Press.

Jordanoska, A. (2021). The exciting world of NFTs: A consideration of regulatory and financial crime risks. *Butterworths Journal of International Banking & Financial Law*, *36*(10), 716–718.

Kang, K., & Lee, S. (2019). Money, Cryptocurrency, and Monetary Policy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3303595

Kasiyanto, S., & Kilinc, M. R. (2022). Legal Conundrums of the Metaverse. *Journal of Central Banking Law and Institutions*, *1*(2), 299–322. https://doi.org/10.21098/jcli.v1i2.25

Kim, J. (2021). Advertising in the Metaverse: Research Agenda. *Journal of Interactive Advertising*, *21*(3), 141–144. https://doi.org/10.1080/15252019.2021.2001273

Kostadinovic, S., Kostadinovic, I., & Krasic, D. (2021). Brand and Legal Protection as a Perequisite for Successful Business. *Ekonomiski Signali*, *16*(2), 023–038.

Kraus, S., Kanbach, D. K., Krysta, P. M., Steinhoff, M. M., & Tomini, N. (2022). Facebook and the creation of the metaverse: radical business model innovation or incremental transformation? *International Journal of Entrepreneurial Behavior & Research*, *28*(9), 52–77. https://doi.org/10.1108/IJEBR-12-2021-0984

Laue, C. (2011). Virtual Worlds and Criminality. In *Virtual Worlds and Criminality* (Issue August 2011). https://doi.org/10.1007/978-3-642-20823-2

Lawson, A., & Gooding, C. (2005). The Dog that Didn't Bark : The Issue of Access to Rights under the European Convention on Human Rights by Disabled People. *Disability Rights in Europe : From Theory to Practice*, *7*. https://doi.org/10.5040/9781472563323.ch-003

Marley, R. (2022). *METAVERSE AND MONEY LAUNDERING – HOW SHUFTI PRO'S AML SCREENING HELPS*. Shufti Pro. https://shuftipro.com/blog/metaverse-and-money-laundering-how-shufti-pros-aml-screening-helps/

Muladi, M., & Priyatno, D. (2013). *Pertanggungjawaban Pidana Korporasi* (Cetakan Ke). Kencana Pernamedia Group.

N.H.T, S. (2005). *Pencucian uang dan Kejahatan Perbankan* (Perdana). Pustaka Sinar Harapan.

Rahayuningsih, T. (2013). ANALISIS PERAN PPATK SEBAGAI SALAH SATU LEMBAGA DALAM MENANGGULANGI MONEY LAUNDERING DI INDONESIA. *Yuridika*, *28*(3), 314–330. https://doi.org/10.20473/ydk.v28i3.349

Sadiku, M. N. O., Eze, K. G., & Musa, S. M. (2018). Smart Contracts: A Primer. *Journal of Scientific and Engineering Research*, *5*(5), 538–541.

Santosa, A. B. (2023). *Apa Itu NFT (Non-Fungible Token)?* PT. Pintu Kemana Saja. https://pintu.co.id/academy/post/nft-adalah#apa-itu-non-fungible-token-nft

Schrepel, T. (2019). Collusion by blockchain and smart contracts Volume 22, Number 1 Fall 2008. *Harvard Journal of Law & Technology*, *22*(1). https://jolt.law.harvard.edu/assets/articlePDFs/v33/03-Schrepel.pdf

Sinurat, Y. C., Putranti, I. R., & Hanura, M. (2022). The Deception of Art : Analisis Potensi Ancaman NFTs (Non-Fungible Tokens) Terhadap Keamanan Nasional Indonesia. *Journal of International Relations*, *8*, 280–288. http://ejournal-s1.undip.ac.id/index.php/jihiWebsite:http://www.fisip.undip.ac.id

Siregar, E. S., & Sinurat, L. (2019). Perlindungan Haki Dan Dampaknya Terhadap Perekonomian Indonesia Di Era Pasar Bebas: Pendekatan Kepustakaan. *Niagawan*, *8*(2), 75. https://doi.org/10.24114/niaga.v8i2.14255

Sjahdeini, S. R. (2012). *Pencucian Uang: Pengertian, Sejarah, Faktor-Faktor Penyebab Dan Dampaknya Bagi Masyarakat* (Pertama). Jurnal Hukum Bisnis Press.

Srokosz, W., & Kopciaski, T. (2015). Legal and economic analysis of the cryptocurrencies impact on the financial system stability. *Journal of Teaching and Education*, *4*(2), 619–627. http://www.universitypublications.net/jte/0402/pdf/F5N180.pdf%0Ahttp://universitypublications.net/jte/0402/index.html

Stessens, G. (2000). *Money Laundering A New International Law Enforcement Model* (First Edit). University Press.

Suartini, N. W., & Dewi, A. A. I. A. A. (2019). Aspek Kriminologis White Collar Crime dalam Tindak Pidana Korupsi di BUMN. *Jurnal Kertha Wicara*, *8*(8), 1–16. https://ojs.unud.ac.id/index.php/kerthawicara/article/view/57270

Sudjito, B., Majid, A., Sulistio, F., & Ruslijanto, P. A. (2016). Tindak Pidana Pornografi dalam Era Siber di Indonesia. *Wacana, Jurnal Sosial Dan Humaniora*, *19*(02), 66–72. https://doi.org/10.21776/ub.wacana.2016.019.02.1

Sulistianingsih, D., & Khomsa Kinanti, A. (2022). Hak Karya Cipta Non-Fungible Token (NFT) Dalam Sudut Pandang Hukum Hak Kekayaan Intelektual. *Krtha Bhayangkara*, *16*(1), 197–206. https://doi.org/10.31599/krtha.v16i1.1077

Trautman, L. (2014). Richmond Journal of Law and Technology Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox? VIRTUAL CURRENCIES; BITCOIN & WHAT NOW AFTER LIBERTY RESERVE, SILK ROAD, AND MT. GOX? In *Richmond Journal of Law & Technology* (Vol. 20, Issue 4). http://scholarship.richmond.edu/jolt%0Ahttp://scholarship.richmond.edu/jolt/vol20/iss4/3

Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara* (Pertaama). Refika Aditama.

Wahyuni, R. A. E., & Turisno, B. E. (2019). Praktik Finansial Teknologi Ilegal Dalam Bentuk Pinjaman Online Ditinjau Dari Etika Bisnis. *Jurnal Pembangunan Hukum Indonesia*, *1*(3), 379–391. https://doi.org/10.14710/jphi.v1i3.379-391

Yusuf, M. (2014). *Mengenal, Mencegah, Memberantas Tindak Pidana Pencucian Uang* (Pertama). Pustaka Juanda Tigalima.

Zainudin, M. (2019). *Pemahaman Metode Penelitian Hukum (Pengertian, Paradigma, dan Susunan Pembentukan* (Pertama). CV. Istana Agency.