IJCCJ
Indonesian Journal of Crime and Criminal Justice

Vol. 1 No. 1. June 2025. pp. 108-130 E-ISSN: 3108-9852 https://doi.org/10.62264/ijccj.v1i1.120

Non-Fungible Tokens and the Metaverse using Cryptocurrency in Indonesia: Money Laundering Potential and Challenges

Pujiyono Suwadi [a*], Rian Saputra [b],
[a] Prosecutor's Commission, Republic of Indonesia, Jakarta, Indonesia
[b] Faculty of Law, Universitas Slamet Riyadi, Surakarta, Indonesia
* corresponding author: pujiyonosuwadi66@gmail.com

ARTICLE INFO

Article History

Received: 09February 2025
Revised: 20 March 2025
Revised: 23 April 2025
Accepted: 22 May 2025
Available online: 01 June 2025

Keywords:

Cryptocurrency;
Metaverse;
Non-Fungible Tokens;
Money Laundering Crime

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.

1. Introduction

The rapid progression of information technology significantly facilitates the execution of daily human activities. The advancement of human civilization in science and technology, particularly regarding the intricacies of information, communication, and transportation, is global in scope and appears boundless. The pace of globalization within a nation has reached such a level that complete political, socio-cultural, economic, and legal isolation from inter-country relations is no longer feasible.[1] In the

[1] Heejin Kim, 'Globalization and Regulatory Change: The Interplay of Laws and Technologies in E-Commerce in Southeast Asia', *Computer Law & Security Review*, 35.5 (2019), 105315 <https://doi.org/https://doi.org/10.1016/j.clsr.2019.03.009>.

context of contemporary globalization, various community activities are inextricably linked to the support provided by technology. The interplay of technological advancements and the swiftly evolving commercial landscape engenders a paradigm shift, fostering many innovations that enhance the efficiency of business operations. A multitude of elements contributes to the swift advancement of technological development. The escalation of varied human requirements and the growing intricacies of threats, particularly about natural disasters, food shortages, and pandemics that afflicted the globe in early 2020. Not only did it precipitate a crisis and jeopardize the economy, but it also expedited the digitalization process across multiple dimensions since its onset.[2]

The current discourse is heavily centered around several technological advancements, notably the Metaverse, non-fungible tokens (NFTs), and cryptocurrency. The Metaverse is characterized as a virtual environment, often called MUVE (Multi-User Virtual Environment). Its framework is influenced by MMORPG (Massive Multiplayer Online Role-Playing Games). It facilitates interactions among avatars within 3D video games, integrating elements of augmented reality (AR), virtual reality (VR), and the internet. The Metaverse's emergence and accompanying technological apparatus enable individuals to experience the profound sensation of inhabiting a remarkably authentic virtual realm.[3] The concept of the 'metaverse' garnered significant public interest when Mark Zuckerberg, the CEO of Facebook, declared in 2021 that the company would rebrand itself as 'Meta' and that human activities would transition into the virtual realm. He proclaimed that "the metaverse represents the forthcoming significant advancement." The transition from Web 2.0 to Web 3.0 marked a significant evolution in the digital landscape. By 2025, projections indicate that a quarter of the global population will engage in the Metaverse for at least one hour, whether for virtual transactions or other pursuits, including professional endeavors.[4]

Beyond the Metaverse, various technological advancements are intricately

---

[2] Bart Custers and Bas Vergouw, 'Promising Policing Technologies: Experiences, Obstacles and Police Needs Regarding Law Enforcement Technologies', *Computer Law & Security Review*, 31.4 (2015), 518–26 <https://doi.org/https://doi.org/10.1016/j.clsr.2015.05.005>.

[3] Joshua Fairfield, 'Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property', *Indiana Law Journal*, 97.4 (2022), 1261–1313.

[4] Kathleen Bridget Wilson, Adam Karg, and Hadi Ghaderi, 'Prospecting Non-Fungible Tokens in the Digital Economy: Stakeholders and Ecosystem, Risk and Opportunity', *Business Horizons*, 65.5 (2022), 657–70 <https://doi.org/10.1016/j.bushor.2021.10.007>.

connected to the business realm, particularly in relation to NFTs and cryptocurrencies associated with the Metaverse. NFTs represent a category of assets that can be exchanged, and their ownership is verifiably recorded within the Metaverse. At the same time, cryptocurrency serves as a digital medium of exchange, facilitating transactions in this virtual realm. NFT is derived from 'fungibility' and 'token' concepts. NFTs are digital assets that signify unique items possessing intrinsic value that cannot be substituted or traded for something else. They extract significance from distinctiveness, scarcity, and market desire. Every NFT possesses a record of its transactions inscribed on the blockchain. This information encompasses the creator, cost, and record of ownership. From an economic perspective, a fungible asset is characterized as something that can be quantified in units akin to currency (paper or coins).[5]

The Metaverse, in essence, represents a network of three-dimensional virtual realms that emphasize social engagement. In the Metaverse, individuals engage in social and economic interactions through avatars, which serve as their virtual representations. While frequently linked to virtual reality headsets, the term encompasses not a particular technology but how individuals engage with technological systems. The primary attributes encompass virtual realms that persist independently of one's engagement, alongside augmented reality, which integrates the digital and physical domains. The Metaverse extends its influence to the digital economy, enabling users to create, purchase, and sell goods. Decentraland, a 3D virtual world game, exemplifies a platform where users can acquire virtual plots of land through cryptocurrency, craft art, and fashion items marketed as NFTs in virtual galleries and shops and interact with one another. A substantial volume of financial transactions occurs via the platform. A notable transaction in the virtual property involved a piece sold for $3.5 million. The Metaverse facilitates interactions and transactions akin to those in the physical realm, employing avatars as a medium for engagement.[6]

The evolution of the Metaverse and NFTs is intrinsically linked to cryptocurrency. Cryptocurrency serves as a medium of exchange in the acquisition and disposition of NFTs, and it is anticipated to function as a monetary instrument within business or

---

[5] Partha Pratim Ray, 'Web3: A Comprehensive Review on Background, Technologies, Applications, Zero-Trust Architectures, Challenges and Future Directions', *Internet of Things and Cyber-Physical Systems*, 3.April (2023), 213–48 <https://doi.org/10.1016/j.iotcps.2023.05.003>.

[6] Aleksandra Jordanoska, 'The Exciting World of NFTs: A Consideration of Regulatory and Financial Crime Risks', *Butterworths Journal of International Banking & Financial Law*, 36.10 (2021), 716–18.

economic endeavors in the metaverse realm, thereby establishing itself as an integral component of the ecosystem encompassing both the Metaverse and NFTs. In parallel with other dimensions of technological advancement, the developments in the Metaverse, particularly those related to technology and the internet, are not immune to the pervasive threat of diverse forms of cybercrime that may arise. Christian Laue posits that specific manifestations of criminal activity within the Metaverse realm encompass cyber crimes.[7] According to the insights of J. E. Sahetapy, there exists a significant correlation between crime and societal development; as society progresses, so too does the sophistication of criminal activity. This is also a manifestation of culture itself. This indicates that as a nation attains greater cultural sophistication and modernity, the manifestations of crime evolve correspondingly in their form, nature, and methods of execution. The interplay of science and technology in contemporary society yields both beneficial and detrimental effects, particularly regarding the discordance in their application.[8]

The progression of globalization is inherently linked to the evolution of crime; in essence, there exists a direct correlation between the anticipated growth of criminal activity and the advancement of legal frameworks. Alongside cybercrime, technological advancements intricately linked to the economy encounter the risk of facilitating money laundering. The act of money laundering represents a significant obstacle in the pursuit of a financial system characterized by integrity.[9]

Their actions contribute significantly to the deterioration of a nation's economic development and the escalation of criminal activities. It is commonly called money bleaching, panning, or legitimizing illicit income. Among the prevalent money laundering methods is the Loan Back technique, which involves borrowing one's funds. In this scenario, an individual secures a loan from a foreign entity, essentially a façade (real estate investment firm), with the individual serving as director and shareholder.[10] This arrangement operates under a 'back to loan' mechanism, where

---

[7] Sen Li and Yan Chen, 'How Nonfungible Tokens Empower Business Model Innovation', *Business Horizons*, 66.4 (2023), 543–54 <https://doi.org/10.1016/j.bushor.2022.10.006>.

[8] Hariman Satria, 'Penerapan Pidana Tambahan Dalam Pertanggungjawaban Pidana Korporasi Pada Tindak Pidana Lingkungan Hidup', *Jurnal Yudisial*, 10.2 (2017), 155 <https://doi.org/10.29123/jy.v10i2.18>.

[9] Francesca Palmiotto and Natalia Menéndez González, 'Facial Recognition Technology, Democracy and Human Rights', *Computer Law & Security Review*, 50 (2023), 105857 <https://doi.org/https://doi.org/10.1016/j.clsr.2023.105857>.

[10] Aisha Hassan Al-Emadi, 'The Financial Action Taskforce and Money Laundering: Critical Analysis of the Panama Papers and the Role of the United Kingdom', *Journal of Money Laundering Control*, 24.4 (2021), 752 – 761 <https://doi.org/10.1108/JMLC-11-2020-0129>.

the individual acquires funds from a foreign bank branch through instruments such as a 'standby letter of credit' or 'certificate of deposit' derived from illicit activities. Ultimately, the loan remains unpaid, leading to the disbursement of the bank guarantee.[11]

According to Ivan Yustiavandana, the selection of diverse methods for executing money laundering complicates the formulation of legal frameworks capable of encompassing all these potentialities. Conversely, legal provisions aimed at combating money laundering should safeguard the community, ensuring they do not obstruct labor-intensive investments. The acts of money laundering are not solely the domain of individuals; instead, they frequently involve organized crime or are driven by the motivations inherent in white-collar criminality. White-collar crime encompasses a range of offenses, including official, corporate, professional, and individual.[12]

The expansion of diverse methods in the execution of money laundering, alongside the rising volume of illicitly processed funds, is inextricably linked to the pervasive impact of globalization across all dimensions of existence. Globalization facilitates lawful and illicit economic endeavors, along with the rise of information networks, communication systems, transportation operations, and global financial intermediation. It facilitates the adoption of diverse elements of international management organization and operationalization by business actors while also permitting the utilization of detrimental practices employed by criminals.[13] The progression of blockchain technology and its role as a foundational element of the Metaverse, NFTs, and cryptocurrencies is undeniably outpacing the legal frameworks designed to govern it.

In this context, the legal instruments encompass policy matters on regulations designed to safeguard community interests alongside policies focused on crime prevention or criminal justice. In this instance, the policy surrounding criminal law encompasses proactive measures and the elimination of money laundering that employs the Metaverse, NFTs, and cryptocurrency as methods for concealing or

---

[11] Sean Lanagan and Kim-Kwang Raymond Choo, 'On the Need for AI to Triage Encrypted Data Containers in U.S. Law Enforcement Applications', *Forensic Science International: Digital Investigation*, 38 (2021), 301217 <https://doi.org/https://doi.org/10.1016/j.fsidi.2021.301217>.

[12] Fabian Teichmann, 'Recent Trends in Money Laundering', *Crime, Law and Social Change*, 73.2 (2020), 237 – 247 <https://doi.org/10.1007/s10611-019-09859-0>.

[13] Malcolm Campbell-Verduyn, 'Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance', *Crime, Law and Social Change*, 69.2 (2018), 283–305 <https://doi.org/10.1007/s10611-017-9756-5>.

obscuring the proceeds of illicit activities.

Drawing from prior research findings, there has been a notable absence of discourse surrounding the Metaverse, NFTs, and cryptocurrency. Specifically, the potential vulnerabilities of these technologies as tools for concealing the origins of assets derived from illicit activities have not been adequately explored. Furthermore, law enforcement's complexities in addressing money laundering facilitated through the Metaverse, NFTs, and cryptocurrency remain largely unexamined. It is pretty intriguing to examine the evolution of the money laundering framework and the methods employed by those engaged in such activities, as well as the potential of the Metaverse, NFTs, and cryptocurrency to serve as tools for concealing or obscuring the origins of assets derived from illicit actions or money laundering.

2. Research Method

This research activity was carried out as an effort to understand and solve problems scientifically, systematically, and logically (makes sense).[14] 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. In other words, this research not only refers to applicable legal products but also the reality that occurs in the field.[15] 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.[16] So, it could provide an overview of the reality on the object being studied objectively.

3. Results and Discussion

Crimes Issues on Non-Fungible Tokens and the Metaverse using Cryptocurrency in

[14] Hanita Mayasari, 'A Examination on Personal Data Protection in Metaverse Technology in Indonesia : A Human Rights Perspective', *Journal of Law, Environmental and Justice*, 1.1 (2023), 64–85 <https://doi.org/10.62264/jlej.v1i1.4>.

[15] Willy Naresta Hanum, Tran Thi Dieu Ha, and Nilam Firmandayu, 'Eliminating Ecological Damage in Geothermal Energy Extraction : Fulfillment of Ecological Rights by Proposing Permits Standardization', *Journal of Law, Environmental and Justice*, 2.2 (2024), 205–28 <https://doi.org/10.62264/jlej.v2i2.105>.

[16] M Yazid Fathoni and Acasio Fernandez, 'Establishment of Land Court in Indonesia : An Effort to Realise Justice Based on Pancasila', *Journal of Law, Environmental and Justice*, 1.2 (2023), 86–104 <https://doi.org/10.62264/jlej.v1i2.6>.

Indonesia

Money laundering represents a global issue and a significant challenge. A universal consensus exists among nations regarding the characterization of money laundering as a criminal act that necessitates confrontation and elimination. Black's Law Dictionary defines money laundering as investing or transferring funds derived from racketeering, drug transactions, and other illicit sources into legitimate channels, thereby obscuring the traceability of their origins. Generally, the concept of money laundering can be defined as follows. Crime constitutes a sequence of actions involving assets that are either known or reasonably believed to stem from the proceeds of illicit activities to conceal or obscure their origin, source, location, designation, transfer of rights, or actual ownership. The objective is to legitimize funds acquired through illicit means by integrating them into the financial system, legitimate business operations, or alternative methods. Essentially, it refers to any activity intended to obscure or hide the source of funds derived from unlawful activities.[17] In contemplating the crime's essence, one must consider the subsequent facets: a. Doubt regarding the commission of a predicate offense and b. Resources derived from criminal activities

Yunus Husein noted that the global community has acknowledged the issue of money laundering for an extended period. Money laundering began to gain acknowledgment in America in 1830, as various entities utilized funds derived from illicit activities to acquire businesses. Alcapone, a notable figure among organized crime syndicates, endeavored to deceive governmental authorities by establishing a laundry business. This enterprise served as a façade to obscure the origins of illicit funds, thereby masking their criminal provenance. This subsequently gave rise to the concept known as 'money laundering.'[18]

The expression initially appeared in publications linked to the coverage of the Watergate scandal in the United States in 1973. The phrase' money laundering' appeared initially in print within articles related to the Watergate scandal in the United States in 1973. The phenomenon garnered significant attention in 1984 when Interpol investigated the money laundering activities orchestrated by the US mafia, famously referred to as the pizza connection case. This intricate operation involved the transfer of US$600 million through a labyrinth of complex financial transactions, ultimately reaching banks in

[17] Campbell-Verduyn.

[18] Mariam Aljassmi and others, 'Estimating the Magnitude of Money Laundering in the United Arab Emirates (UAE): Evidence from the Currency Demand Approach (CDA)', *Journal of Money Laundering Control*, 27.2 (2024), 332 – 347 <https://doi.org/10.1108/JMLC-02-2023-0043>.

Switzerland and Italy.[19] This case illustrates how individuals engaged in criminal activities exploit legitimate businesses to obscure the origins of illicit gains, thereby presenting them as assets obtained through lawful endeavors.

The international community, particularly the G-7 nations, undertook a significant initiative to combat and eliminate money laundering by forming The Financial Action Task Force (FATF) in 1989. The FATF is a task force dedicated to formulating international recommendations to eradicate money laundering practices. The recommendations put forth by the FATF subsequently serve as a framework for each nation in the development and establishment of regulations aimed at combating money laundering. In 1990, the FATF introduced 40 recommendations, establishing a thorough framework to eradicate money laundering offenses. This entity is structured as a policy-making body comprising legal scholars, financial analysts, and law enforcement professionals aimed at advancing national legislation and frameworks on anti-money laundering and the prevention of terrorism financing.[20] The FATF constitutes an intergovernmental entity comprised of member states engaged in policy formulation.

The establishment of Law Number 15 of 2002 on the Crime of Money Laundering signifies Indonesia's formal approach to criminalizing money laundering. Implementing the Law is undeniably a result of Indonesia's designation on the NCCT (Non-Cooperative Countries and Territories) list by the FATF. Indonesia is regarded as failing to adhere to the anti-money laundering regulations as specified in the recommendations put forth by the FATF. The Indonesian government enacted legislation to criminalize money laundering in response to this resolution. However, it was deemed less than ideal to adhere to the anti-money laundering framework established by the FATF Recommendation. Indonesia enacted Law No. 25 of 2003 to amend and enhance Law No. 15 of 2002, incorporating revisions to the provisions that criminalize money laundering. Following the establishment of the two laws, Indonesia was ultimately removed from the NCCT's list in 2005. The subsequent phase in the anti-money laundering framework was marked by the enactment of Law No. 8 of 2010, which addresses the Prevention and Eradication of the Crime of Money Laundering. This legislation aims to align with national interests and international standards, serving as a foundational legal instrument to guarantee legal certainty, enhance the efficacy of law enforcement, and facilitate the

[19] Peter Leasure, 'Asset Recovery in Corruption Cases: Comparative Analysis Identifies Serious Flaws in US Tracing Procedure', *Journal of Money Laundering Control*, 19.1 (2016), 4 – 20 <https://doi.org/10.1108/JMLC-04-2015-0010>.

[20] W Srokosz and T Kopciaski, 'Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability', *Journal of Teaching and Education*, 4.2 (2015), 619–27.

tracing and recovery of assets derived from criminal activities.

It is an irrefutable observation that, as time progresses, individuals engaged in criminal activities persist in devising or executing diverse methods to obscure or conceal the provenance of assets acquired through illicit means. These methods encompass applying more advanced methodologies or gaps within legislative frameworks. Such methods render the perpetrators of crime increasingly astute and challenging for law enforcement officials to uncover, particularly in concealing the assets derived from illicit activities.[21]

Billy Steel articulated that money laundering serves as the essential sustenance for drug dealers, fraudsters, smugglers, arms dealers, terrorists, extortionists, and tax evaders. The significance of crime proceeds in money laundering has gradually transformed law enforcement's approach, shifting from focusing on tracking the suspect to tracing the financial flows. The principle of following the financial trail underscores that the enforcement of money laundering laws is executed by tracking the movement of assets derived from illicit activities. Consequently, it is anticipated that the scope for individuals engaging in criminal activities will be significantly reduced.[22]

The evolution of money laundering law enforcement initially unfolded through a tripartite framework, encompassing the stages of placement, layering, and integration, which shaped the comprehension of the phenomenon itself. Nevertheless, they do not constitute an element; instead, they serve merely as a fundamental framework in executing money laundering activities. The banking system serves as a primary mechanism criminals employ for money laundering, predominantly through these processes. The perpetrators believe that utilizing banking services facilitates the process of money laundering, as banks not only provide a secure environment but also maintain a system of confidentiality regarding customer profiles and transaction activities that is safeguarded.[23]

Recognizing banks' vulnerability as potential conduits for money laundering by nefarious actors, the government subsequently reinforced regulations about the banking

---

[21] David U. Enweremadu, 'Nigeria's Quest to Recover Looted Assets: The Abacha Affair', *Africa Spectrum*, 48.2 (2013), 51–70 <https://doi.org/10.1177/000203971304800203>.

[22] Grat Van Den Heuvel, 'The Parliamentary Enquiry on Fraud in the Dutch Construction Industry Collusion as Concept between Corruption and State-Corporate Crime', *Crime, Law and Social Change*, 44.2 (2005), 133–51 <https://doi.org/10.1007/s10611-006-9009-5>.

[23] Le Yi Koh and others, 'Willingness to Participate in Virtual Reality Technologies: Public Adoption and Policy Perspectives for Marine Conservation', *Journal of Environmental Management*, 334 (2023), 117480 <https://doi.org/https://doi.org/10.1016/j.jenvman.2023.117480>.

system's framework, emphasizing the enhancement of the 'know your customer' principle. This application facilitates the identification of any discrepancies in the flow of funds relative to the customer's established profile, thereby enhancing the banks' ability to monitor financial activities effectively. In specific circumstances, should the transparency of the data supplied by the customer prove inadequate, the bank possesses the authority to augment profiling through the mechanism of 'enhanced due diligence.' This optimization will further restrict the avenues for criminals to exploit banking instruments for money laundering.[24]

In addition to profiling, financial service providers, encompassing both banks and non-banks, are classified as reporting entities, thereby bearing the responsibility to report any transactions mandated by Law to the Financial Transaction Reports and Analysis Centre. This reporting obligation undoubtedly constrains and complicates the operational landscape for money launderers. Upon recognizing the escalating rigor of banking regulations, individuals engaged in money laundering sought alternative methods to execute their activities, thereby reducing their reliance on traditional banking services. They endeavored to obscure the ill-gotten gains by utilizing the mechanisms of goods and services providers. This approach is regarded as comparatively more secure, as it is believed that the scrutiny of criminals suggests that anti-money laundering regulations governing goods and service providers are less stringent than those applied within the banking sector.

Non-Fungible Tokens and Metaverse using Cryptocurrency: Challenges in Combating Money Laundering in Indonesia

The methodology employed by those engaged in money laundering to conceal the proceeds of illicit activities reveals a tendency to move away from the established patterns of placement, layering, and integration. The offenders acknowledge the imperative to identify and cultivate alternative methods of operation that elude detection by law enforcement authorities. The Egmont Group has published various typologies of money laundering. One notable method is the concealment within a business structure, which involves the effort to obscure illicit funds within the routine operations of a business or within an existing company that is under the control of the relevant organization. Secondly, the improper utilization of a legitimate enterprise, specifically employing an established business or company to facilitate the money laundering process, all while the entity remains oblivious to the criminal origins of the funds involved. Thirdly, fabricated

[24] Safari Kasiyanto and Mustafa R. Kilinc, 'Legal Conundrums of the Metaverse', *Journal of Central Banking Law and Institutions*, 1.2 (2022), 299–322 <https://doi.org/10.21098/jcli.v1i2.25>.

identities, documents, or intermediaries are used, such as transferring the oversight of assets obtained through illicit means to an individual unrelated to the crime by employing deceptive identities and documentation. Fourthly, the manipulation of international jurisdictional discrepancies can be done by exploiting the variations in regulations and requirements between nations, such as those on bank secrecy, identification protocols, disclosure mandates, and currency limitations.[25]

The evolution of the money laundering process is evident in its modus operandi or typology and in the classification of its perpetrators. Historically, those who committed crimes were responsible for laundering their illicit gains. In contemporary times, however, these individuals have devised methods to engage third parties who are not directly involved in the original criminal activity to facilitate the process of money laundering.[26]

The individuals engaged in money laundering often employ specific professions, including solicitors, solicitors, accountants, financial advisors, notaries, and other fiduciaries, to conceal the origins of funds derived from illicit activities. The individuals engaged in money laundering employ specific professions, including solicitors, solicitors, accountants, financial advisors, notaries, and various fiduciaries, to conceal the origins of funds derived from illicit activities. Money launderers exploit the offerings rendered by these professions to obscure the offender's identity and disseminate the gains acquired from illicit activities. Generally, the strategy involves utilizing the accounts of solicitors or solicitors to facilitate the placement and layering of funds, such as in banking institutions, by leveraging the confidentiality afforded by solicitor-client privilege.[27]

Immediate Outcome 7 FATF (IO 7) categorizes launderers into two distinct groups: self-laundering and third-party money laundering. Gabriele Bernescone (2015) articulates self-laundering as the offense perpetrated by an individual who employs, exchanges, or reallocates funds, assets, or other advantages within economic, financial, speculative, or entrepreneurial endeavors that originate from a crime they have committed, with the intent to obscure the illicit source. Third-party money laundering in this context refers to the act of laundering proceeds by an individual who did not participate in executing the underlying criminal offense. Self-laundering refers to the process by which an individual involved in the commission of a predicate offense engages in laundering the proceeds

---

[25] Jordanoska.

[26] Massimo Bartoletti and others, 'Dissecting Ponzi Schemes on Ethereum: Identification, Analysis, and Impact', *Future Generation Computer Systems*, 102 (2020), 259–77 <https://doi.org/10.1016/j.future.2019.08.014>.

[27] Erwin Rooze, 'Differentiated Use of Electronic Case Management Systems', *International Journal for Court Administration*, 3.1 (2010), 50 <https://doi.org/10.18352/ijca.53>.

derived from that offense. Upon deeper examination of the definition of 'person involved' as articulated in IO 7, it encompasses the individual who perpetrates the act, those who engage in its commission, and those who facilitate the criminal endeavor of money laundering.[28]

Money laundering constitutes a grave offense that has the potential to impact the economy at large while simultaneously obstructing the social, economic, political, and cultural advancement of communities globally. The United Nations Convention Against Illicit Traffic in Narcotics, Drugs, and Psychotropic Substances of 1988 articulates that Money Laundering involves the movement of assets obtained from serious offenses or crimes with the intent to conceal or obscure illegal property in order to evade legal repercussions or to mask the genuine nature, origin, location, and ownership rights associated with such assets. In the interim, as articulated by the FATF, money laundering constitutes the manipulation of illicit gains to obscure their unlawful origins, thereby seeking to legitimize the proceeds derived from criminal activities.[29]

The essence of the criminalisation of money laundering lies in concealing or obscuring the origins of assets derived from unlawful activities, thereby rendering these assets appear as though they are legitimate in nature. The distinction between active and passive perpetrators of money laundering offenses lies in the execution of the element of concealing or obscuring the source of illicit proceeds.

Simons posits that in specific formulations of the offense, there exists a stipulation regarding specific circumstances that must materialize post-commission of an act by an individual, where this emergence is pivotal for categorizing the individual's actions as a punishable offense. Regarding the money laundering offense, actions are deemed to satisfy the criteria of the crime if they are executed to conceal or obscure the source of an asset. The endeavor to conceal or obscure constitutes the fundamental essence of the criminalization of money laundering. According to established doctrine and jurisprudence, the term 'conceal' is characterized as an action undertaken to obscure the origin of assets from others, including failing to disclose the source of funds to the officers of Financial Service Providers. The obfuscation process involves the integration of unlawful funds with legitimate earnings, thereby creating the illusion that these illicit resources originate from lawful endeavors. This may include converting illicit funds into various currencies, among other methods. The methods employed by criminals in

[28] Andries Johannes Zoutendijk, 'Organised Crime Threat Assessments: A Critical Review', *Crime, Law and Social Change*, 54.1 (2010), 63–86 <https://doi.org/10.1007/s10611-010-9244-7>.

[29] Laura Antonucci, Corrado Crocetta, and Francesco D. d'Ovidio, 'Evaluation of Italian Judicial System', *Procedia Economics and Finance*, 17.14 (2014), 121–30 <https://doi.org/10.1016/s2212-5671(14)00886-7>.

executing money laundering are in a constant state of evolution. Investigators must consider that criminals will perpetually assess methods of money laundering, particularly when one of their strategies is exposed by law enforcement authorities. [30]

Considering the distinctive attributes of the Metaverse, NFTs, and cryptocurrencies, their capacity to serve as instruments for money laundering or concealing the proceeds of illicit activities is significantly pronounced. To elucidate the potential of cryptocurrency as a vehicle for money laundering, it is imperative to first clarify the definitions of cryptocurrency, NFTs, and the Metaverse. Cryptocurrencies represent a form of digital currency meticulously developed through the application of cryptographic algorithms. These currencies are capable of being exchanged through a peer-to-peer framework. Cryptocurrency transfer between individuals can occur independently of specific financial institutions. Cryptocurrency, often called virtual currency, represents a novel advancement emerging from the evolution of digital payment systems. This innovation aligns with the broader technological advancements and the proliferation of internet networks, particularly in payment systems and contemporary digital payment solutions. The inaugural cryptocurrency, Bitcoin, has experienced remarkable growth since its inception in 2009. The progression of digital currencies has transformed the nature of cheque-cashing, credit cards, and debit cards, shifting them from physical objects that require carrying to instruments that can be managed via a smartphone.[31]

In contrast to conventional currencies, cryptocurrencies exhibit distinct advantages and characteristics. Primarily, they are irreversible; once a transfer or payment is executed, it cannot be altered or annulled. Furthermore, every transaction is subject to meticulous tracking and is permanently recorded within a digital repository known as the Blockchain. Furthermore, the system is characterized by its pseudonymity and decentralization, eliminating the need for any intermediary, such as traditional banking institutions, while ensuring that all participants maintain a degree of anonymity. Consequently, we, from the transaction data, ascertain the user's true identity. Thirdly, cryptocurrency's security and permissionless nature are upheld by the robust framework of public key cryptography and the consensus mechanisms of blockchains, rendering them challenging for malicious

[30] Ray.

[31] Ali Shahaab and others, 'Public Service Operational Efficiency and Blockchain – A Case Study of Companies House, UK', *Government Information Quarterly*, 40.1 (2023) <https://doi.org/10.1016/j.giq.2022.101759>.

actors to infiltrate.[32]

Furthermore, seeking any form of authorization or permit to use cryptocurrencies is unnecessary. Fourthly, transactions utilizing cryptocurrencies are characterized by rapidity and global reach, often concluding within minutes. Cryptocurrencies possess a global character, primarily due to their foundation on blockchain technology. This has two significant implications: firstly, individuals from any corner of the world can engage with them, and secondly, the user's geographical location minimally influences the transaction speed. Since its introduction to the public, Bitcoin has faced scrutiny due to its perceived anonymity and irreversibility. Bitcoin's anonymity has raised apprehensions among financial regulators and governments, as it is perceived to enable illicit activities, including money laundering and the financing of terrorism. The purported anonymity is said to elude regulation by central authorities, including central banks, thereby rendering it noncompliant with current legal frameworks. The extensive adoption of cryptocurrencies poses significant challenges for central banks, particularly in their efforts to regulate the money supply.[33]

The inherent anonymity of cryptocurrency presents a significant opportunity for its utilization in facilitating money laundering activities. Most contemporary cryptocurrencies are founded upon a technology known as Blockchain, which interlinks users via a sequence of blocks. Consequently, when a transaction occurs, what is revealed is a compilation of block numbers. The essence of Blockchain lies in its decentralized nature, characterized as a distributed ledger system. This implies that no individual user possesses control over the information or data contained within the Blockchain, nor is anyone responsible for ensuring its proper operation. This subsequently results in a lack of transparency regarding the ownership of cryptocurrency.[34]

According to various studies, cryptocurrencies should be a focal point for global anti-money laundering initiatives. This can be attributed to two primary factors: Anti-money laundering initiatives directly scrutinize tiny transactions that raise suspicions. This emphasis aims to counteract the efforts of offenders to integrate the gains from unlawful activities, including corruption, tax evasion, and terrorism financing, into the legitimate

---

[32] Uni Sabadina, 'Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online', *Jurnal Lex Renaissance*, 6.4 (2021), 799–814 <https://doi.org/10.20885/jlr.vol6.iss4.art11>.

[33] Muhammad Asrul and Shilla Hasmara, 'Explaining Legal Implications : Ownership Analysis Of Intellectual Property Rights On Cryptokitties Platforms', *Wacana Hukum*, 29.1 (2023), 1–13.

[34] Yudha Ramelan, 'Penerapan Saksi Pidana Korporasi Pada Bank Dan Implikasinya', *Jurnal Hukum & Pembangunan*, 48.4 (2018), 861 <https://doi.org/10.21143/jhp.vol48.no4.1806>.

financial framework. Furthermore, the significance of cryptocurrencies in global planning cannot be overstated, as they present innovative methods of employing verification practices that transcend political boundaries. These entities constitute components of digital currencies, which may either be governed by centralized institutions or operate on decentralized networks. They present a theoretical challenge to global anti-money laundering frameworks that persistently endanger financial regulators and law enforcement agencies.[35]

An examination of the banking system reveals that banks are responsible for verifying customers' identities seeking to utilize their services. Consequently, financial institutions are responsible for meticulously analyzing and verifying, or in this instance, ensuring that each transaction executed by clients is devoid of any association with illicit activities. Additionally, they must present a report to the relevant authority, in this instance, the Financial Transaction Reports and Analysis Centre (Pusat Pelaporan dan Analisis Transaksi Keuangan/PPATK), concerning transactions that are suspected to be intricately linked to criminal activities or that fall under the classifications necessitating reporting to PPATK and law enforcement entities. Furthermore, financial institutions possess the authority, and indeed the responsibility, to temporarily halt transactions or restrict access to accounts that are believed to be closely associated with criminal activities. Should the bank fail to fulfill its obligations on the anti-money laundering framework, it may face sanctions as stipulated by legal provisions.[36]

Regarding financial integrity, criminal and terrorist organizations rely on the capacity of cryptocurrencies to obscure their internal transactions. In this context, cryptocurrencies are perceived as instruments that enable money laundering, sanctions evasion, cybercrime, fraud, and the financing of terrorism, as each component of a cryptocurrency can circumvent governmental taxation. This can be interpreted as a result of a governmental body's lack of centralized oversight. In Indonesia, a notable instance of money laundering involving Bitcoin was linked to a case of corruption and financial misconduct at PT Asabri (Novina Putri Bestari: 2021).

The attributes of cryptocurrencies, which operate independently of any Financial Service Authority, lead to an absence of oversight regarding transactions between individuals. This distinguishes them from traditional currency transactions that rely on

---

[35] Susan ROSE-ACKERMAN, 'Corruption and the Criminal Law Legalization and Criminalization', *Forum on Crime and Society*, 2.1 (2002), 20.

[36] Hongming Cheng and L Ling, 'White Collar Crime and the Criminal Justice System: Government Response to Bank Fraud and Corruption in China', *Journal of Financial Crime*, 16.2 (2009), 166 – 179 <https://doi.org/10.1108/13590790910951849>.

banking services, making it challenging for governmental and law enforcement entities to trace or monitor the movement of cryptocurrency transactions in the same manner as more conventional currencies. The subsequent characteristic is that cryptocurrencies function independently, as the user's address remains unconnected to the owner's identity in the physical realm. Implementing anti-money laundering policies faces a significant challenge due to the inherent characteristics of anonymous cryptocurrency, which fundamentally conflict with the core principles of the anti-money laundering framework, particularly the 'Know Your Customer' principle. The concept of pseudonymity renders users indistinguishable, even as each Bitcoin transaction is meticulously documented on the Blockchain. All transaction records are accessible to every user, allowing for the identification of participants and tracing of transactions within the Bitcoin system.[37]

The concept of pseudonymity inherently undermines the transparency associated with wealth ownership, creating a conducive environment for individuals engaged in illicit activities to utilize cryptocurrencies as a mechanism for concealing or obscuring the provenance of assets derived from criminal endeavors. The advanced encryption techniques inherent in cryptocurrency render it a lucrative medium of exchange within the shadowy realms of the dark market, facilitating transactions for illicit goods such as narcotics, adult content, counterfeit documentation, arms, and munitions.[38]

NFTs serve as a vehicle for money laundering or concealing the proceeds of illicit activities, manifesting as digital assets recorded on a distributed public ledger. This ledger meticulously documents transactions, with each asset possessing a distinct identification code and unique metadata, differentiating them within the blockchain network. They embody tangible entities from the real world, including artistic paintings, animations, photographs, videos, drawings, musical compositions, signatures, tickets, and various other forms of creative expression. Every cryptocurrency is regarded as equivalent to its counterparts, allowing for the exchange of tokens, which are thus classified as fungible tokens.[39]

The realm of NFT technology remains in its nascent stages, presenting numerous

---

[37] Emanuelle Nava Smaniotto and Giacomo Balbinotto Neto, 'Speculative Trading in Bitcoin: A Brazilian Market Evidence', *Quarterly Review of Economics and Finance*, 85 (2022), 47–54 <https://doi.org/10.1016/j.qref.2020.10.024>.

[38] Lawrence Trautman, *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?*, *Richmond Journal of Law & Technology*, 2014, XX.

[39] Kee Kang and Seungduck Lee, 'Money, Cryptocurrency, and Monetary Policy', *SSRN Electronic Journal*, 2019 <https://doi.org/10.2139/ssrn.3303595>.

avenues that currently lack regulatory frameworks. Regarding the realm of Intellectual Property, NFTs serve as a tool for simplification while also representing a form of private ownership that lacks a physical manifestation, indicating that the item cannot be physically grasped yet possesses an assigned value. It is crucial to underscore that possessing NFTs does not confer upon the owner unrestricted rights to their work. Should the artist wish to convey ownership of the copyright or exclusive rights to the collector, this transaction must be executed via a smart contract. Nonetheless, the application of smart contracts within the blockchain framework remains nascent from a technical and legal perspective. NFT encompasses a comprehensive copyright framework that integrates moral and economic rights.[40]

According to the research conducted by Yosafat Caesar Sinurat, the report from Non-Fungible.com indicates that despite a decline in NFTs from 2018 to 2019, a remarkable resurgence took place in the subsequent years. Specifically, from 2019 to 2020, there was a notable increase of 97.09% in active wallets, 66.94% in the number of active buyers, 24.7% in the count of creators or sellers, and a 29% rise in the volume of monetary transactions. This case suggests that the NFT market was undergoing a swift escalation, and the report indicated that while the surge in 2021 was not particularly substantial, it remains a promising area, particularly for criminal activities.[41]

Cyber money laundering exploits online functionalities, transforming tangible currency into digital assets. Cyber Laundering represents the most recent advancement in money laundering methodologies. The velocity of the money laundering process escalates significantly when conducted through cyberspace. This is further substantiated by the absence of binding legal authority on the internet, the inherent anonymity afforded by virtual interactions devoid of physical presence, the extensive reach, and the rapid pace of transactions. Consequently, this will elevate the likelihood of an uptick in money laundering offenses perpetrated within cyberspace. The progression of technology and the business realm invariably transcends the confines of current regulations.[42]

While meticulous records of each transaction are maintained, numerous marketplaces offer an anonymity feature designed to safeguard the user's true identity. Put differently,

---

[40] Malkar Vinod Ramchandra and others, 'Assessment of the Impact of Blockchain Technology in the Banking Industry', *Materials Today: Proceedings*, 56 (2022), 2221–26 <https://doi.org/10.1016/j.matpr.2021.11.554>.

[41] Bartoletti and others.

[42] Yao Yue and others, 'How Cryptocurrency Affects Economy? A Network Analysis Using Bibliometric Methods', *International Review of Financial Analysis*, 77.71988101 (2021), 101869 <https://doi.org/10.1016/j.irfa.2021.101869>.

individuals can employ a fictitious identity to conduct transactions within the pertinent marketplace. This occurrence may arise due to the failure of numerous marketplaces to implement the 'Know Your Customer' principle, which is essential for ascertaining the user's true identity. To illustrate, when establishing an account on the OpenSea marketplace, the sole identity requirement is an email address and the wallet number of the pre-existing cryptocurrency account necessary for conducting transactions. An individual may construct a fictitious identity by establishing a counterfeit email address, subsequently utilizing this false persona to generate a cryptocurrency wallet, enabling unrestricted transactions. Creating multiple accounts for conducting transactions or engaging with independently established fictitious accounts poses significant risks.[43]

In addition to the previously discussed examples, a significant avenue for the misuse of NFTs within money laundering arises from their intrinsic lack of real value. Consequently, the valuation of an NFT is entirely contingent upon the bid presented by the subsequent purchaser. The concept referred to as 'Greater Fool Theory' suggests that an asset's value is not derived from its intrinsic qualities but rather from the presence of individuals willing to purchase it at a price exceeding that of the prior buyer, regardless of the asset's actual worth.[44]

The valuation of NFTs is intrinsically linked to the price set by subsequent purchasers, thereby presenting significant challenges regarding the potential exploitation of NFTs as instruments for money laundering. For instance, should the valuation of an NFT hinge solely on the whims of potential buyers or substantial offers, it becomes a tool susceptible to exploitation by nefarious individuals. They can execute a transaction mechanism that simulates the execution of a transaction via NFT. However, the reality is that this process involves the transfer of criminal proceeds disguised within a seemingly legitimate transaction, akin to activities surrounding the sale and purchase of NFTs.[45]

The perpetrators generate NFTs and subsequently market them on the sanctioned trading platform. The potential purchaser submits a price proposal, which is subsequently accepted by the individual who previously created the NFTs. The concern surrounding anonymity presents a significant risk, as it may facilitate the misuse of NFTs for money

---

[43] Florian Horky and others, 'Don't Miss out on NFTs?! A Sentiment-Based Analysis of the Early NFT Market', *International Review of Economics and Finance*, 2023 <https://doi.org/10.1016/j.iref.2023.07.016>.

[44] Andres Guadamuz, 'All Watched over by Machines of Loving Grace: A Critical Look at Smart Contracts', *Computer Law and Security Review*, 35.6 (2019), 105338 <https://doi.org/10.1016/j.clsr.2019.105338>.

[45] Huy Nghiem and others, 'Detecting Cryptocurrency Pump-and-Dump Frauds Using Market and Social Signals', *Expert Systems with Applications*, 182.November 2020 (2021), 115284 <https://doi.org/10.1016/j.eswa.2021.115284>.

laundering activities. Criminal organizations can create NFTs without revealing their identities, list them on marketplaces, and subsequently engage in transactions involving these NFTs. Initially, the case may appear to be a mere legal transaction involving two parties in a buying and selling agreement. However, upon closer examination, it reveals the potential to serve as a mechanism for concealing or obscuring the proceeds derived from illicit activities. The seller and buyer may engage in a transaction at an elevated price with a buyer identified by the individual, transferring a certain amount of funds. However, these funds are ultimately derived from illicit activities' proceeds.[46]

Recent research indicates that the prospective market within the Metaverse spans from 3.75 billion dollars to 12.46 billion dollars. Both NFTs and cryptocurrencies share certain attributes that contribute to their potential utility in concealing or obscuring the origins of illicit proceeds, highlighting the presence of pseudonymous characteristics in each. This pseudonymity stands in stark opposition to the 'Know Your Customer' principle that is prevalent in financial services systems, including both banking and non-banking sectors. It is favored by those engaged in illicit activities as it conceals the genuine identity of the proprietor.

Within the Metaverse, the notion of activity is fundamentally rooted in the occurrences of the physical world, wherein all interactions are mediated by monetary exchange. The distinction between purchasing and vending activities in the tangible realm and the Metaverse lies in the payment mechanism that employs cryptocurrency. The payment mechanism within the Metaverse necessitates the exclusive use of cryptocurrency, thereby demanding the establishment of more intricate laws and regulations. In conclusion, the advancements represented by cryptocurrencies, NFTs, and the Metaverse possess the potential for misuse by individuals engaged in illicit activities, enabling them to obscure or conceal the provenance of assets derived from unlawful actions. Cryptocurrencies and NFTs possess a pseudonymous quality that enables the concealment of the identity of the asset's owner.

4. 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

[46] Shahaab and others.

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.

5. References

Al-Emadi, Aisha Hassan, 'The Financial Action Taskforce and Money Laundering: Critical Analysis of the Panama Papers and the Role of the United Kingdom', *Journal of Money Laundering Control*, 24.4 (2021), 752 – 761 <https://doi.org/10.1108/JMLC-11-2020-0129>

Aljassmi, Mariam, Awadh Ahmed Mohammed Gamal, Norasibah Abdul Jalil, Joseph David, and K Kuperan Viswanathan, 'Estimating the Magnitude of Money Laundering in the United Arab Emirates (UAE): Evidence from the Currency Demand Approach (CDA)', *Journal of Money Laundering Control*, 27.2 (2024), 332 – 347 <https://doi.org/10.1108/JMLC-02-2023-0043>

Antonucci, Laura, Corrado Crocetta, and Francesco D. d'Ovidio, 'Evaluation of Italian Judicial System', *Procedia Economics and Finance*, 17.14 (2014), 121–30 <https://doi.org/10.1016/s2212-5671(14)00886-7>

Asrul, Muhammad, and Shilla Hasmara, 'Explaining Legal Implications : Ownership Analysis Of Intellectual Property Rights On Cryptokitties Platforms', *Wacana Hukum*, 29.1 (2023), 1–13

Bartoletti, Massimo, Salvatore Carta, Tiziana Cimoli, and Roberto Saia, 'Dissecting Ponzi Schemes on Ethereum: Identification, Analysis, and Impact', *Future Generation Computer Systems*, 102 (2020), 259–77 <https://doi.org/10.1016/j.future.2019.08.014>

Campbell-Verduyn, Malcolm, 'Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance', *Crime, Law and Social Change*, 69.2 (2018), 283–305 <https://doi.org/10.1007/s10611-017-9756-5>

Cheng, Hongming, and L Ling, 'White Collar Crime and the Criminal Justice System: Government Response to Bank Fraud and Corruption in China', *Journal of Financial Crime*, 16.2 (2009), 166 – 179 <https://doi.org/10.1108/13590790910951849>

Custers, Bart, and Bas Vergouw, 'Promising Policing Technologies: Experiences, Obstacles and Police Needs Regarding Law Enforcement Technologies', *Computer Law & Security Review*, 31.4 (2015), 518–26

<https://doi.org/https://doi.org/10.1016/j.clsr.2015.05.005>

Enweremadu, David U., 'Nigeria's Quest to Recover Looted Assets: The Abacha Affair', *Africa Spectrum*, 48.2 (2013), 51–70 <https://doi.org/10.1177/000203971304800203>

Fairfield, Joshua, 'Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property', *Indiana Law Journal*, 97.4 (2022), 1261–1313

Fathoni, M Yazid, and Acasio Fernandez, 'Establishment of Land Court in Indonesia : An Effort to Realise Justice Based on Pancasila', *Journal of Law, Environmental and Justice*, 1.2 (2023), 86–104 <https://doi.org/10.62264/jlej.v1i2.6>

Guadamuz, Andres, 'All Watched over by Machines of Loving Grace: A Critical Look at Smart Contracts', *Computer Law and Security Review*, 35.6 (2019), 105338 <https://doi.org/10.1016/j.clsr.2019.105338>

Hanum, Willy Naresta, Tran Thi Dieu Ha, and Nilam Firmandayu, 'Eliminating Ecological Damage in Geothermal Energy Extraction : Fulfillment of Ecological Rights by Proposing Permits Standardization', *Journal of Law, Environmental and Justice*, 2.2 (2024), 205–28 <https://doi.org/10.62264/jlej.v2i2.105>

Van Den Heuvel, Grat, 'The Parliamentary Enquiry on Fraud in the Dutch Construction Industry Collusion as Concept between Corruption and State-Corporate Crime', *Crime, Law and Social Change*, 44.2 (2005), 133–51 <https://doi.org/10.1007/s10611-006-9009-5>

Horky, Florian, Lili Dubbick, Franziska Rhein, and Jarko Fidrmuc, 'Don't Miss out on NFTs?! A Sentiment-Based Analysis of the Early NFT Market', *International Review of Economics and Finance*, 2023 <https://doi.org/10.1016/j.iref.2023.07.016>

Jordanoska, Aleksandra, 'The Exciting World of NFTs: A Consideration of Regulatory and Financial Crime Risks', *Butterworths Journal of International Banking & Financial Law*, 36.10 (2021), 716–18

Kang, Kee, and Seungduck Lee, 'Money, Cryptocurrency, and Monetary Policy', *SSRN Electronic Journal*, 2019 <https://doi.org/10.2139/ssrn.3303595>

Kasiyanto, Safari, and Mustafa R. Kilinc, 'Legal Conundrums of the Metaverse', *Journal of Central Banking Law and Institutions*, 1.2 (2022), 299–322 <https://doi.org/10.21098/jcli.v1i2.25>

Kim, Heejin, 'Globalization and Regulatory Change: The Interplay of Laws and Technologies in E-Commerce in Southeast Asia', *Computer Law & Security Review*, 35.5 (2019), 105315 <https://doi.org/https://doi.org/10.1016/j.clsr.2019.03.009>

Koh, Le Yi, Min Wu, Xueqin Wang, and Kum Fai Yuen, 'Willingness to Participate in

Virtual Reality Technologies: Public Adoption and Policy Perspectives for Marine Conservation', *Journal of Environmental Management*, 334 (2023), 117480 <https://doi.org/https://doi.org/10.1016/j.jenvman.2023.117480>

Lanagan, Sean, and Kim-Kwang Raymond Choo, 'On the Need for AI to Triage Encrypted Data Containers in U.S. Law Enforcement Applications', *Forensic Science International: Digital Investigation*, 38 (2021), 301217 <https://doi.org/https://doi.org/10.1016/j.fsidi.2021.301217>

Leasure, Peter, 'Asset Recovery in Corruption Cases: Comparative Analysis Identifies Serious Flaws in US Tracing Procedure', *Journal of Money Laundering Control*, 19.1 (2016), 4 – 20 <https://doi.org/10.1108/JMLC-04-2015-0010>

Li, Sen, and Yan Chen, 'How Nonfungible Tokens Empower Business Model Innovation', *Business Horizons*, 66.4 (2023), 543–54 <https://doi.org/10.1016/j.bushor.2022.10.006>

Mayasari, Hanita, 'A Examination on Personal Data Protection in Metaverse Technology in Indonesia : A Human Rights Perspective', *Journal of Law, Environmental and Justice*, 1.1 (2023), 64–85 <https://doi.org/10.62264/jlej.v1i1.4>

Nghiem, Huy, Goran Muric, Fred Morstatter, and Emilio Ferrara, 'Detecting Cryptocurrency Pump-and-Dump Frauds Using Market and Social Signals', *Expert Systems with Applications*, 182.November 2020 (2021), 115284 <https://doi.org/10.1016/j.eswa.2021.115284>

Palmiotto, Francesca, and Natalia Menéndez González, 'Facial Recognition Technology, Democracy and Human Rights', *Computer Law & Security Review*, 50 (2023), 105857 <https://doi.org/https://doi.org/10.1016/j.clsr.2023.105857>

Ramelan, Yudha, 'Penerapan Saksi Pidana Korporasi Pada Bank Dan Implikasinya', *Jurnal Hukum & Pembangunan*, 48.4 (2018), 861 <https://doi.org/10.21143/jhp.vol48.no4.1806>

Ray, Partha Pratim, 'Web3: A Comprehensive Review on Background, Technologies, Applications, Zero-Trust Architectures, Challenges and Future Directions', *Internet of Things and Cyber-Physical Systems*, 3.April (2023), 213–48 <https://doi.org/10.1016/j.iotcps.2023.05.003>

Rooze, Erwin, 'Differentiated Use of Electronic Case Management Systems', *International Journal for Court Administration*, 3.1 (2010), 50 <https://doi.org/10.18352/ijca.53>

ROSE-ACKERMAN, Susan, 'Corruption and the Criminal Law Legalization and Criminalization', *Forum on Crime and Society*, 2.1 (2002), 20

Sabadina, Uni, 'Politik Hukum Pidana Penanggulangan Kejahatan Teknologi Informasi Terkait Kebocoran Data Pribadi Oleh Korporasi Berbasis Online', *Jurnal Lex Renaissance*, 6.4 (2021), 799–814 <https://doi.org/10.20885/jlr.vol6.iss4.art11>

Satria, Hariman, 'Penerapan Pidana Tambahan Dalam Pertanggungjawaban Pidana Korporasi Pada Tindak Pidana Lingkungan Hidup', *Jurnal Yudisial*, 10.2 (2017), 155 <https://doi.org/10.29123/jy.v10i2.18>

Shahaab, Ali, Imtiaz A. Khan, Ross Maude, Chaminda Hewage, and Yingli Wang, 'Public Service Operational Efficiency and Blockchain – A Case Study of Companies House, UK', *Government Information Quarterly*, 40.1 (2023) <https://doi.org/10.1016/j.giq.2022.101759>

Smaniotto, Emanuelle Nava, and Giacomo Balbinotto Neto, 'Speculative Trading in Bitcoin: A Brazilian Market Evidence', *Quarterly Review of Economics and Finance*, 85 (2022), 47–54 <https://doi.org/10.1016/j.qref.2020.10.024>

Srokosz, W, and T Kopciaski, 'Legal and Economic Analysis of the Cryptocurrencies Impact on the Financial System Stability', *Journal of Teaching and Education*, 4.2 (2015), 619–27

Teichmann, Fabian, 'Recent Trends in Money Laundering', *Crime, Law and Social Change*, 73.2 (2020), 237 – 247 <https://doi.org/10.1007/s10611-019-09859-0>

Trautman, Lawrence, *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?*, *Richmond Journal of Law & Technology*, 2014, XX

Vinod Ramchandra, Malkar, Krishan Kumar, Abhijit Sarkar, Samrat Kr. Mukherjee, and Kirti Agarwal, 'Assessment of the Impact of Blockchain Technology in the Banking Industry', *Materials Today: Proceedings*, 56 (2022), 2221–26 <https://doi.org/10.1016/j.matpr.2021.11.554>

Wilson, Kathleen Bridget, Adam Karg, and Hadi Ghaderi, 'Prospecting Non-Fungible Tokens in the Digital Economy: Stakeholders and Ecosystem, Risk and Opportunity', *Business Horizons*, 65.5 (2022), 657–70 <https://doi.org/10.1016/j.bushor.2021.10.007>

Yue, Yao, Xuerong Li, Dingxuan Zhang, and Shouyang Wang, 'How Cryptocurrency Affects Economy? A Network Analysis Using Bibliometric Methods', *International Review of Financial Analysis*, 77.71988101 (2021), 101869 <https://doi.org/10.1016/j.irfa.2021.101869>

Zoutendijk, Andries Johannes, 'Organised Crime Threat Assessments: A Critical Review',

Crime, Law and Social Change, 54.1 (2010), 63–86 <https://doi.org/10.1007/s10611-010-9244-7>