Analysis of Potential Threats of NFTS (Non-Fungible Tokens) for National Security and Economic Resilience. A Case Study of Indonesia

Dany Eka SAPUTRA[1]
Nicoleta ISAC[2]
Waqar BADSHAH[3]
Cosmin DOBRIN[4]

Abstract

Technological advancements have significantly shaped global society, leading to widespread reliance on technology across various domains. This pervasive influence is particularly evident in the daily lives of individuals, who heavily depend on the digital world and internet connectivity. Crucial sectors such as finance, trade, and the creative industry have embraced the digital realm, with the emergence of Non-Fungible Tokens (NFTs) representing a novel approach for creators to acquire recognition and value for their work. However, this technological progress has also presented opportunities for criminal exploitation, as illicit activities such as money laundering and terrorism funding have transitioned to the digital landscape. This study employs a secondary research methodology to investigate the vulnerabilities associated with the use of NFTs as a medium for money laundering and terrorism funding. The study aims to highlight the potential implications for national economic resilience if these issues are not adequately addressed and securitized. By combining the constructivism theory with the concept of securitization, this work explores how the adoption of NFTs can pose a national concern, affecting both economic stability and security.

Furthermore, the research reveals that the anonymity feature inherent in NFT transactions facilitates easier execution of money laundering and terrorism funding activities, thereby posing risks to a country's national security and economic resilience.

Keywords: *NFT, technological advancements, economic resilience, cybersecurity*

JEL classification: G28, K42, O33

DOI: 10.24818/RMCI.2023.5.696

1. Introduction

Technology is constantly evolving and has taken us to new heights. Every aspect of our lives has become integrated into the digital era we depend on today.

[1] Dany Eka Saputra, Istanbul Sabahattin Zaim University, saputra.dany@std.izu.edu.tr
[2] Nicoleta Isac, Istanbul Sabahattin Zaim University, Corresponding author, nicoleta.isac@izu.edu.tr
[3] Waqar Badshah, Istanbul University, waqar.badshah@istanbul.edu.tr
[4] Cosmin Dobrin, Bucharest University of Economic Studies, cdobrin@yahoo.com

Transactions, communication, information, and even entertainment have all been digitalized, providing easy access and data processing capabilities (Scarle et al., 2012). The internet has become an essential part of our daily lives, and for modern businesses to succeed, they must embrace e-commerce and online credit card transactions or at least have a web presence. This also applies to the availability of entertainment through the internet, such as free or paid movies, games, music, and other forms of entertainment.

In the entertainment industry, fueled by technological advancements, intense competition amongst creators has emerged. Whether it's movies, games, music, or any other form of entertainment, the goal is to create captivating content that attracts market attention and generates sales. In 2022, one notable trend is the use of Non-fungible Tokens (NFTs) (Pinto-Gutiérrez et al., 2022). NFTs have the potential to jeopardize national security and expose vulnerabilities in the realm of cybercrime. These tokens, stored on blockchain, represent ownership of digital assets such as artworks, recordings, virtual real estate, and digital pets. Unlike fungible cryptocurrencies like bitcoin, NFTs are unique and cannot be exchanged for one another. This uniqueness enables NFTs to authenticate ownership of digital assets, with the blockchain, often Ethereum's, serving as a public and transparent storage for each NFT (Pinto-Gutiérrez et al., 2022).

While the convenience and access provided by the internet are undoubtedly valuable, they have also made cyberspace an attractive breeding ground for criminal activities. Cybercrimes committed using the internet pose a significant threat to international economic security. In any country, the movement of money plays a crucial role in national economic stabilization. The advent of market globalization, combined with technological advancements and innovative payment methods, has revolutionized traditional practices while introducing new avenues for money laundering (Vitvitskyi et al., 2022). The link between money laundering, financial markets, and overall human development is well-established (Šikman & Grujić, 2021). Money laundering poses a significant threat to a nation's economic resilience, with the United Nations estimating that 2% to 5% of the global GDP, equivalent to 800 billion to 2 trillion dollars, is laundered annually on a global scale (UN source). This alarming statistic highlights the correlation between money laundering, GDP, and the overall financial market, underscoring the far-reaching consequences of such illicit activities on the economic stability and growth of a nation.

2. Literature review

2.1 NFT (Non-Fungible Tokens)

NFTs, or non-fungible tokens, have gained significant popularity in the digital landscape. These unique tokens are securely stored on a blockchain, providing proof of ownership for various digital assets. Whether it's artworks, recordings, virtual real estate, or digital pets, NFTs offer a novel way to authenticate and appreciate these virtual treasures (Dowling, 2022). The functioning of NFTs relies on blockchain technology, which is commonly associated with

cryptocurrencies like Ethereum and Bitcoin. Through blockchain contracts written in specific programming languages, NFTs leverage crypto metadata to create these tokens. Unlike physical money or cryptocurrencies, NFTs possess a distinct quality that sets them apart. Each NFT carries a digital identifier that is truly one-of-a-kind, making it impossible to copy, substitute, or divide. This uniqueness is securely recorded in the blockchain, including ownership information and associated metadata. NFTs are not limited to the art world but have also made their way into the realm of gaming and the metaverse. For instance, Facebook, the largest social media company, has invested nearly 2 billion dollars in creating a digital world based on metadata and virtual reality, known as the Metaverse. The Metaverse represents a groundbreaking advancement in digitalized spaces where various activities can be carried out (Dowling, 2022). However, the flexibility and unique metadata-based nature of NFTs have also attracted the attention of criminals, who exploit them for illicit activities. This phenomenon is a consequence of the transition from the traditional era to the digital era, where criminals can operate not only in the physical realm but also in virtual environments. As the world rapidly embraces the digital era, governments, who play a crucial role in protecting and managing these digital spaces, face significant challenges and struggle to keep up with the pace of technological advancements.

2.2 Money Laundering

Money laundering is a special type of crime where criminals attempt to conceal or legitimize the proceeds of their illicit activities. With the rapid digitalization of the world, money laundering is no longer limited to traditional methods but has also evolved in the modern era (Vitvitskiy et al., 2021). Every aspect of the digital world presents opportunities and loopholes that can be exploited by those with knowledge in order to engage in criminal actions. According to a report released by the International Monetary Fund (IMF) in 1996, approximately 2% to 5% of the global economy is involved in money laundering (Gjoni et al., 2015). This report highlights the weaknesses and vulnerabilities within the system that facilitate illicit practices, posing a threat to economic stability and national security. Indonesia has undergone a transition from traditional financial systems to technology-based solutions in recent decades. Fintech now plays a significant role in the country's financial system (Anagnostopoulos, 2018). Fintech involves the use of technology to develop new financial products, services, and business models, which can greatly impact the efficiency, security, and reliability of the payment system. However, this rapid digital transformation has also exposed Fintech to various risks, including money laundering. Banks, as key players in the financial industry, have incorporated financial technology into their operations. However, they face considerable risks, with money laundering being one of the most prevalent challenges they encounter (Korejo et al., 2021). Money laundering refers to the process through which criminals attempt to disguise the origin of their illegal proceeds, making them appear legitimate. It is a crime that continues to pose a significant challenge for governments

worldwide, as their efforts to combat this illicit activity often fall short. The issue of money laundering gained widespread attention following high-profile incidents such as the Panama Papers, the Paradise Papers, and the Swiss leaks. These events exposed the sophisticated methods used by criminals to transform their illicit funds into untraceable assets or hidden bank accounts. Money laundering has become a means for individuals to conceal their illegal gains and evade detection by law enforcement agencies.

2.3 Cybercrime and Cyberlaundering

In today's technologically advanced world, cybercrimes have become a prevalent issue (Al-Khater et al., 2020). These crimes encompass a wide range of offenses that specifically target computers or communication tools. Cybercrimes include child pornography, cyberstalking, identity theft, cyber laundering, credit card theft, cyber terrorism, drug sales, data leakage, sexually explicit content, phishing, and cyber hacking, among others. Criminals exploit vulnerabilities in computer systems to carry out these unlawful activities. The nature of cybercrimes reflects the evolution of technology itself. Criminals modify traditional crimes and incorporate computer systems as a crucial component. This has led to the emergence of the term "cyber-laundering," which refers to the practice of conducting money laundering through online platforms and transactions (Wronka, 2022). Cyber criminals increasingly target mobile devices due to the growing vulnerabilities in their security protocols. The threats on mobile devices are expanding at a faster pace compared to those encountered on personal computers. Therefore, it is imperative to establish an effective legal framework to comprehensively combat cybercrime. Cyber laundering involves perpetrators using advanced technologies to move illicitly obtained money through online accounts or digital currencies, disguising its origins (Naqvi, 2020). It is the digital version of criminals attempting to conceal their illegal funds within the cyber world. The magnitude of cybercrimes can be understood by analyzing the data. Shockingly, more than 39% of global cyber breaches in 2018 were attributed to cyber organized crime, reaching as high as 70% in 2011 and 80% in 2015 (Naqvi, 2020). Additionally, it is estimated that illegal activities accounted for 46% of Bitcoin transactions, totaling a staggering $76 billion. Furthermore, 30% of security breaches were driven by crypto mining (Naqvi, 2020). These statistics highlight the urgent need for governments worldwide to implement robust regulations targeting the exploitation of cryptocurrencies for cyber laundering purposes.

2.4 National Economy Cybersecurity

When it comes to the stability of a nation's economy, money laundering poses a significant threat. The main source of black money is corruption, which undermines the economy and hinders overall development, affecting investment rates (Jamil et al., 2021). To ensure economic stability, it is essential to focus on national economy cybersecurity, which involves safeguarding various sectors that

contribute to the country's economic well-being. These sectors include the banking system, stock exchange, critical infrastructure, and government financial systems. By ensuring the security of these components, a country can fortify its economic stability and minimize vulnerabilities. In the case of a microgrid electrical system, the infrastructure and processes involved require advanced technology to establish seamless connections among its various components. While this intelligent and automated system offers numerous benefits, it also exposes the microgrid to potential vulnerabilities. Neglecting these vulnerabilities can have catastrophic consequences for a country's critical infrastructure and economy. Therefore, it is crucial to address these vulnerabilities adequately (Jamil et al., 2021). To maintain a stable economy, it is essential for any country to minimize criminal actions that could threaten its stabilization. This is where national economy cybersecurity plays a pivotal role. By protecting a country's assets, money, and important systems from irresponsible individuals, national economy cybersecurity acts as a lock and alarm system. Just as banks have security measures in place to protect against theft, online transactions, power grids, and transportation systems should also be safeguarded against hackers.

2.5 National Economy Resilience

Economic resilience refers to how a country handles and controls the mobility of its economy and measures the strength of its defense and protection of national assets (Yuheng et al., 2023). To establish economic resilience, it is crucial to have a strong financial system in place. This not only involves preserving the economic aspects but also maintaining the country's structure and social development, as they are primary synergies for establishing national economic resilience. Various threats, such as natural disasters, economic bankruptcy, pandemics, cyber-attacks, and global crises, can pose risks to a country's economic resilience. One notable threat is cyber-attacks, which often target a country's data and need to be protected against. In the present-day cyber landscape, the convergence of money laundering and cyber-attacks is becoming increasingly prominent. To prevent such actions, a country can implement strong regulations and establish a strict monitoring system capable of detecting suspicious financial transactions accurately and in a timely manner. This requires the simultaneous collaboration of the legal sector and law enforcement agencies. By working together as a team, they can provide a robust shield for the country against these types of actions (Jamil et al., 2021). Furthermore, it is essential to strengthen financial institutions by implementing systems, filtering information, and protecting the economy. These measures contribute to enhancing the resilience of the financial sector and safeguarding against potential threats.

3. The Analysis of Cybersecurity Threats

Vulnerabilities in NFT platforms or smart contracts can be exploited by hackers, resulting in data breaches, theft, or manipulation of valuable digital assets (Al Shamsi et al., 2023). Crypto laundering has become a popular method for

individuals to transfer their illicit funds into assets that can be stored online. Cryptocurrency mixers, also known as tumblers, are tools specifically designed to enhance the privacy of digital currencies. They function by combining funds from multiple sources, making it difficult to trace the origin of the money (Avan-Nomayo, 2019). While mixers serve a legitimate purpose in protecting privacy, they have also been associated with potential misuse for illegal activities such as money laundering. The operation of mixers involves pooling funds, shuffling them between addresses, and then redistributing them to different locations, effectively creating anonymity.

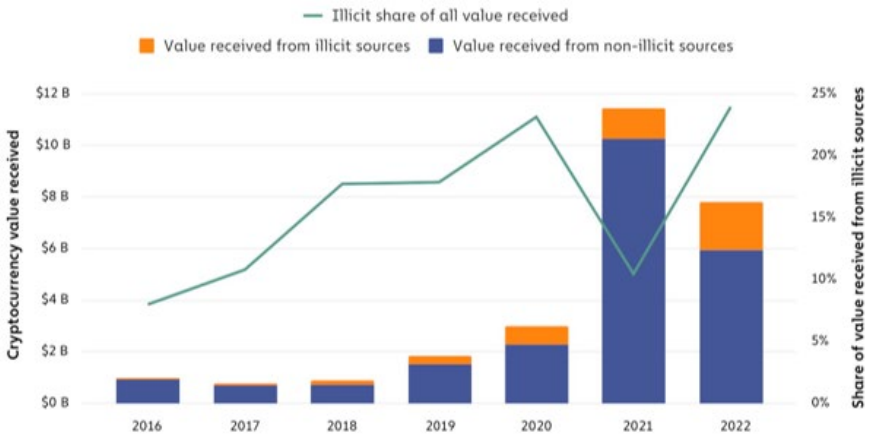

Figure 1. Yearly cryptocurrency received by mixers by source, 2016-2022
Source: https://www.chainalysis.com

As we can see in the Figure 1, in 2022 the funds received by cryptocurrency mixers totaled $7.8 billion, with approximately 24% of the value originating from illicit sources. Comparatively, in 2021, only around 10% of the funds were traced back and returned to illicit sources. This data indicates a yearly increase in the cryptocurrency received by mixers, rising from $1 billion in 2016 to $12 billion in 2022.

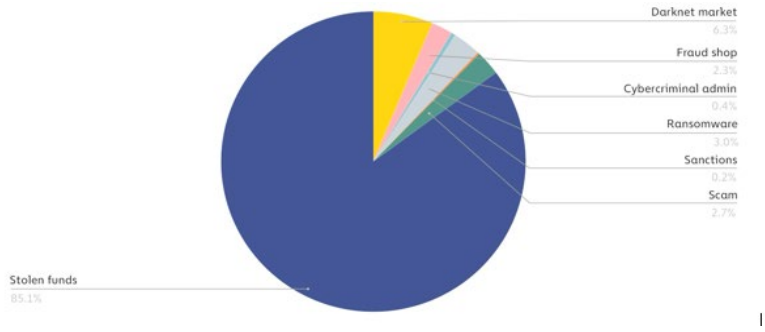

Figure 2. Sources of illicit cryptocurrency sent to mixers in 2022
Source: https://www.chainalysis.com

From the above graph, it is evident that research on money laundering, particularly in the context of cryptocurrency, reveals that illicit funds are often distributed across various types of crimes. These funds are typically transacted through key deposit addresses associated with activities such as cybercrimes, fraud, drug trafficking, terrorism financing, and other illegal actions. This understanding is crucial in developing targeted strategies to dismantle these illicit networks. Additionally, it enables the assessment of the effectiveness of current anti-money laundering (AML) policies and legislation in combating cryptocurrency laundering.

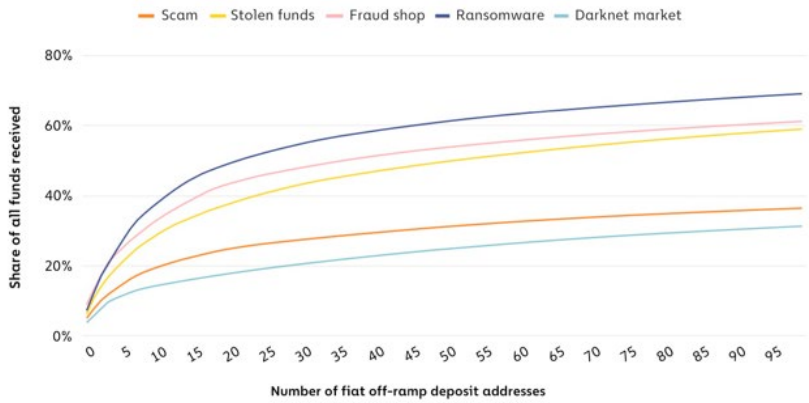

Figure 3. Money laundering concentration by crime type: share of total illicit value received by top deposit addresses in 2022
Source: https://www.chainalysis.com

As we can see in the Figure 3, it is noteworthy that only 21 deposit addresses are responsible for handling 50% of the funds from ransomware to fiat off-ramps, whereas the top 21 deposit addresses for darknet market funds manage just 18%. While there has been a decrease in overall concentration, the fact that 51% of illicit funds flow through only 542 deposit addresses across 83 exchanges still indicates a significant concentration in money laundering activities. Disrupting these individuals and groups associated with these addresses would have a substantial impact on impeding criminals attempting to launder cryptocurrency on a large scale, thereby enhancing the safety of the crypto ecosystem. This emphasizes the importance of collaboration between law enforcement and compliance teams in combating money laundering in the cryptocurrency space.

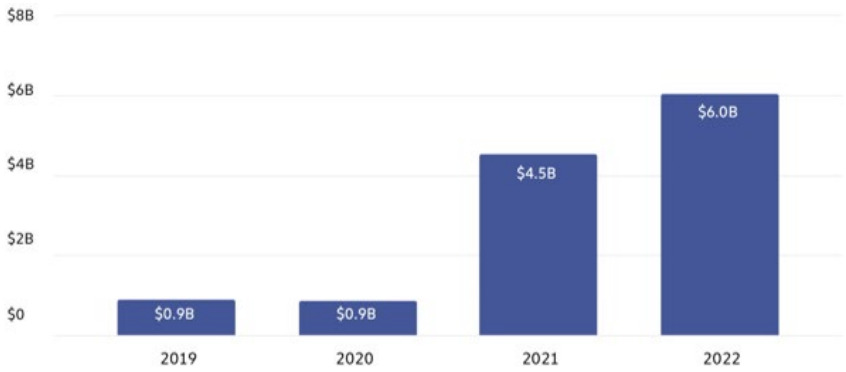

Figure 4. Total illicit value moving to suspected underground laundering services in 2019-2022
Source: https://www.chainalysis.com

Figure 4 relate that the total amount of cryptocurrency flowing into wallets associated with suspected underground laundering services has shown a significant increase in recent years, reaching $6 billion in 2022. While these figures are estimates and not all studied wallets can be confirmed as underground laundering services, their activities on the blockchain suggest their involvement. The scrutiny faced by exchanges like Garantex and Bitzlato from law enforcement may lead to a rise in the use of these underground money laundering services. It is evident that the total value of illicit funds directed towards suspected underground laundering services has experienced a substantial rise from 2019 to 2022. In 2019, the amount was $0.9 billion, but within a year, it escalated dramatically to $4.5 billion in 2021. This surge highlights a concerning trend of funneling illicit funds into these laundering services. Additionally, there has been a significant increase in the total funds received through Non-Fungible Tokens (NFTs), which raises suspicions of potential links to illicit sources. In 2022 alone, the amount surged by nearly $1.5 billion, reaching a staggering sum of approximately $6.0 billion. During 2022, there was a decrease in the amount of money held by criminals. Criminals often keep their funds in personal or associated wallets for a certain period. This may be due to increased attention from law enforcement or industry watchdogs, especially when the funds are obtained through hacking incidents. Other times, they may be waiting for the value of the cryptocurrency to rise or planning to use it for further illegal activities in the future. By monitoring the blockchain, we can observe the changes in the amount of money held by confirmed criminals throughout 2022.

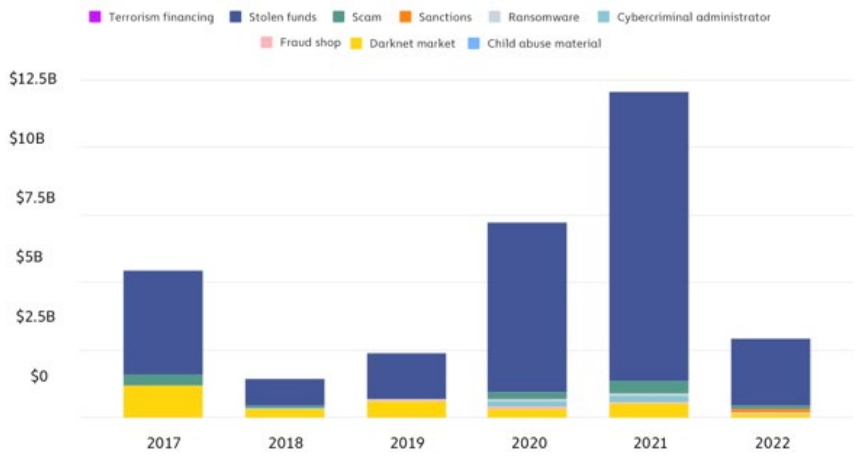

Figure 5. Year and balances of illicit addresses by crime type in 2017-2022
Source: https://www.chainalysis.com

The above figure 5 highlights two significant points. Firstly, the amount of money held by criminals experienced a substantial decline in 2022, dropping from $12.0 billion at the end of 2021 to just $2.9 billion. This decrease can be attributed to the falling prices in the current market downturn and notable seizures made by law enforcement agencies throughout the year. During 2022, investigative agencies demonstrated an increased effort in seizing cryptocurrencies. For example, the IRS Criminal Investigation Unit announced that they confiscated $7 billion worth of digital assets, more than double the amount seized in 2021. Several other notable cases of cryptocurrency seizures from criminals emerged during the year, including:

1. A record-breaking seizure of $3.6 billion from two individuals suspected of laundering funds acquired from the Bitfinex breach in 2016.

2. The seizure of $3.36 billion in Bitcoin from Silk Road, a darknet marketplace, in November 2021. This information was made public in November 2022.

3. The Lazarus Group, a North Korean hacker group, successfully seized $30 million worth of cryptocurrencies from Axie Infinity's Ronin Bridge, marking their first cryptocurrency seizure.

These instances highlight the increased efforts of law enforcement agencies in combating illicit activities involving cryptocurrencies and the significant impact they can have on disrupting criminal operations.

4. The case of Indonesia

A nation's financial system plays a critical role in its economy. It facilitates the reallocation of resources, particularly money, between surplus and underfunded units, thereby enhancing the economy's capacity to utilize money effectively (Indonesia Financial Supervisory Agency (OJK), 2017). The financial system also contributes to the distribution of money through payment system services, which

further supports economic growth (Indonesia Financial Supervisory Agency (OJK), 2017). The stability of a nation's financial system is directly correlated with the growth and stability of its economy (Indonesia Financial Supervisory Agency (OJK), 2017). Financial system stability can be viewed as the nation's ability to prevent monetary or financial crises and ensure that economic processes related to pricing, money allocation, and risk management function properly to support economic growth (Central Bank of Indonesia, 2020). The soundness of financial institutions and the stability of financial markets are interconnected. A robust capital adequacy ratio and sufficient liquidity are indicators of a stable and well-prepared financial institution. Banks often invest in government bonds to secure their funds, ensuring the safety of their assets while generating a steady income. Additionally, lower operating expenses reflect efficient management practices, which can contribute to higher profitability (Indonesia Financial Supervisory Agency (OJK), 2017). By meticulously examining these performance indicators, valuable insights can be gained into a bank's stability, risk management practices, profitability, and overall efficiency. These factors have a profound impact on Indonesia's financial landscape, shaping a vibrant and resilient economy (Indonesia Financial Supervisory Agency (OJK), 2017).

4.1 Indonesian Cybersecurity System

Indonesia, as a developing country, has been investing in IT infrastructure and witnessing an increase in smartphone and internet usage. However, the country's cybersecurity defenses have been exploited by hackers due to the weaknesses in its cybersecurity system. Consequently, there is a growing demand for cybersecurity solutions as the number of IoT connections continues to rise. Despite this demand, the Indonesian cybersecurity sector faces challenges due to a shortage of cybersecurity experts. The cybersecurity market in Indonesia can be categorized into three segments: End User (BFSI, Healthcare, Manufacturing, Government & Defense, IT and Telecommunication), Deployment (Cloud, On-premises), and Offering (Security Type and Services) (Lestari, 2021). According to the National Cyber Security Index (NCSI), Indonesia currently ranks 83rd globally and 6th among ASEAN countries in terms of cybersecurity readiness. In 2021 alone, there were nearly 2.7 million reported ransomware incidents across ASEAN countries, with an average of 1.3 million cyber security cases reported across the region.

To address cybercrime in Indonesia, the National Cyber and Encryption Agency (BSSN) has established the Cyber Threat Intelligence Programme (CTIP) in collaboration with a commercial technology business. The program aims to enhance the security of the country's infrastructure against recent threats identified in Indonesia's digital environment. The BSSN, under the Presidential mandate, is responsible for various operations related to cybersecurity, national encryption, and national cyber crisis management, including identification, detection, protection, response, recovery, and monitoring. In the financial industry, Indonesia has recently implemented new cybersecurity regulations. The Financial Services Authority

(OJK) issued specialized cybersecurity standards for banks, insurance firms, and other financial service providers. These standards cover various aspects such as risk assessments, risk management, data security, incident response planning, and staff capabilities. Furthermore, Indonesia passed its first data protection law in September 2022, demonstrating its commitment to strengthening cybersecurity regulations.

4.2 Regulatory Challenges

The rise of NFTs has posed a challenge for Indonesian authorities, as these digital assets have the potential to pose threats to national security and the economy. NFTs represent a new phenomenon that Indonesia is finding difficult to regulate and protect its citizens from. While NFTs have both positive and negative aspects, the issue lies in their relevance as tradable commodities, which currently lacks stable regulation. The awareness of the NFT phenomenon has spread widely, but the government has yet to establish a comprehensive regulatory framework to address the associated challenges. Existing regulations in Indonesia touch upon certain aspects related to NFTs, but they have not been fully transformed into preventive regulations. In terms of cybersecurity and cyber activities, there have been amendments to Indonesian laws. However, when it comes to cyber laundering involving NFTs, there is no proper law in place to effectively sanction those involved in such crimes. This legal gap makes it challenging for authorities to track and penalize cybercriminals who exploit NFTs as a medium for illicit activities. Without appropriate legislation, it becomes difficult to effectively prevent and address cybercrimes connected to NFTs. Given the potential risks and concerns associated with NFTs, it is crucial for the Indonesian government to establish clear and comprehensive regulations that address the usage, trading, and potential criminal activities related to NFTs. Such regulations would provide a legal framework for authorities to track and sanction individuals involved in cybercrimes facilitated by NFTs, enhancing national cybersecurity measures.

NFT as Nano Technology in Money Laundering Crimes

Despite the meticulous recording of transactions in NFT marketplaces, there are concerns regarding the ease of engaging in transactions using false identities. The lack of robust Know Your Customer (KYC) procedures in these platforms allows users to create fake email addresses and cryptocurrency wallets, enabling transactions without genuine identification. This anonymity feature contributes to a new aspect of money laundering known as the "nano nature," facilitating smaller-scale illicit activities (Sina Osivand, 2021). Tracing illegal money becomes more complex when transactions occur in auction markets using cryptocurrencies instead of official currencies. Data from Chainalysis, a prominent blockchain analysis company, indicates a significant increase in funds associated with criminal activities in 2021, coinciding with the rise of NFTs. Criminals are sending substantial amounts of stolen funds and fraud-related funds from blockchain addresses to the NFT market. In the fourth quarter of 2021 alone, Chainalysis detected approximately

$284,000 worth of suspicious transactions sent to NFT marketplaces. Money laundering through NFTs is not limited to criminal activities but can also facilitate other financial crimes, including tax evasion and embezzlement. The unique characteristics of NFT transactions, combined with their anonymity feature, make tracking and tracing these activities nearly impossible. Moreover, encryption implemented by certain virtual transaction service providers further complicates accessing information, even for the service providers themselves. Let's take a look at the following example.

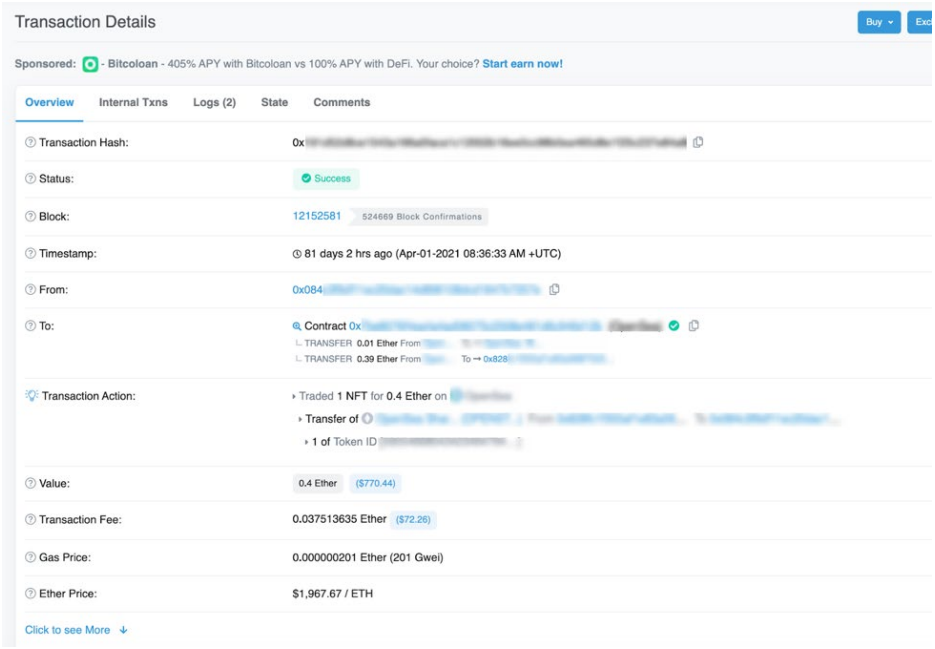

Figure 6. Transaction details of NFT purchased
Source: https://www.chainalysis.com

Everything appears normal at first glance; however, the Reactor graph below indicates that address 0x828 sent 0.45 Ethereum to address 0x084 shortly before the sale.

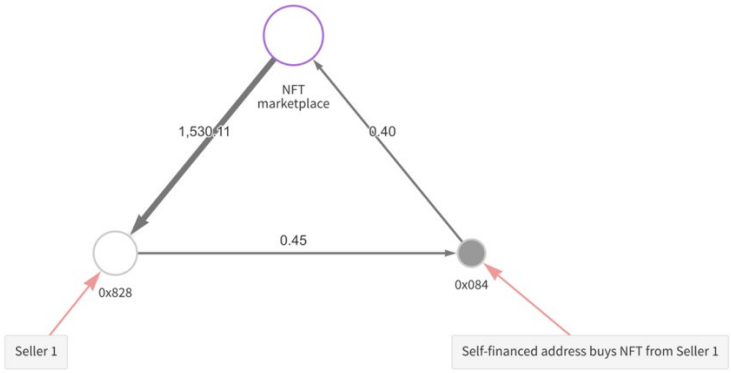

Figure 7. Self-financed Address buys NFT from seller A
Source: https://medium.com/@AMLCrypto/how-to-launder-money-with-nfts-97dce7f2d6a

As shown figure 7, this activity aligns with a pattern observed for Seller 1. The Reactor graph below illustrates similar relationships between Seller 1 and numerous other addresses to which they have sold NFTs. However, an intriguing narrative unfolds: while the majority of NFT wash traders have not been profitable, a select group of 262 traders have achieved substantial profits. Their success has been so significant that this group has collectively generated immense profits overall.

Wash Trader Group Table

Table 1

Wash Trader Group	Number of Addresses	Profits from wash trading
Profitable wash traders	110	$8,875,315
Unptofitable wash traders	152	-$416,984
All	262	$8,458331

Source: author conception

In the third quarter of 2021, there was a significant surge in the value sent to NFT marketplaces from illicit addresses, surpassing $1 million worth of cryptocurrency (Dyntu & Dykyi, 2019). This figure further increased in the fourth quarter, reaching just under $1.4 million. During both quarters, a major portion of this activity originated from addresses associated with scams, which sent funds to NFT marketplaces for purchases. Additionally, substantial amounts of stolen funds were also sent to these marketplaces during the same periods. Of particular concern is the fact that in the fourth quarter, around $284,000 worth of cryptocurrency was sent to NFT marketplaces from addresses with sanctions risk. Notably, these transactions were traced back to the P2P exchange Chatex, which was added to the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals (SDN) list last year (Day, 2021). We can observe instances of various types of criminals purchasing NFTs in the Reactor graph provided below.

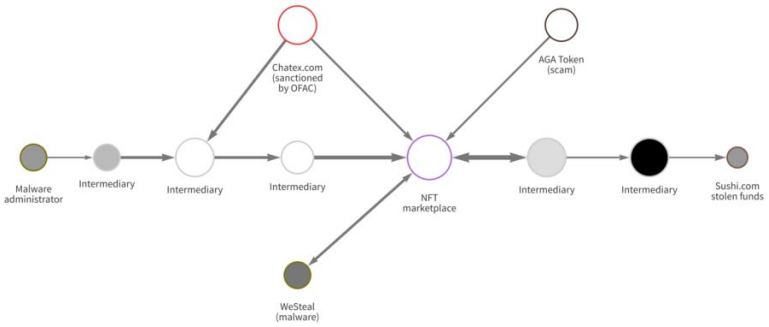

Figure 8. Reactor Graph

Source: https://medium.com/@AMLCrypto/how-to-launder-money-with-nfts-97dce7f2d6a

Here, in the Figure 8, we can identify addresses linked to various types of cybercriminals engaging with a well-known NFT marketplace. These include entities involved in activities such as malware operations, scams, and the P2P exchange Chatex.

4.3 Cyberlaundering and Indonesia Economic Resilience

Cyberlaundering refers to the illicit transfer of funds acquired through criminal activities into the digital realm, utilizing online financial services and platforms that deal with virtual currencies. In recent years, cyber laundering has emerged as a cutting-edge technique in the field of money laundering. The allure of cyber laundering lies in its anonymity, the absence of physical contact required, the speed of transactions, and the broader reach within internet services (Wojciech Filipkowski, 2008). Among the various methods employed for cyber laundering, Non-Fungible Tokens (NFTs) have gained significant prominence. NFTs offer a unique avenue for money launderers to digitally transact and store their unlawfully obtained funds. Platforms like OpenSea and Binance serve as auction platforms for NFT transactions. Unlike spending money on cryptocurrencies, which can be relatively easier to trace and locate, using NFTs allows launderers to divide their funds into different digital assets, effectively creating an untraceable collection.

In 2022, the global fascination with NFTs extended to Indonesia. One notable example is the case of Ghozali, a renowned creator who sold his NFT collection for a remarkable sum of 1 million USD. By uploading his face selfies for 256 consecutive days, Ghozali amassed a total of 933 self-portraits. NFTs have gained significant popularity among the Indonesian community, with many individuals participating in NFT hype and believing that NFTs can be a lucrative means of generating wealth. However, with the rapid growth and hype surrounding NFTs, concerns have arisen regarding the potential for NFTs to be utilized as an alternative method for money laundering. NFTs possess a unique structure in which blockchain data is transparent, but the decentralized nature of the blockchain makes it challenging to identify the individuals involved in the transaction history. Unlike

traditional transactions where the buyer and seller can be identified through KYC (Know Your Customer) procedures, decentralized blockchain transactions are complex and fast-moving, making it difficult to verify the parties involved. The volume of the NFT marketplace can be observed in the graph below, encompassing multiple platforms used by individuals to trade and sell their NFTs, including Opensea, X2Y2, Bur, Looksrare, Rarible, and Sudoswap.

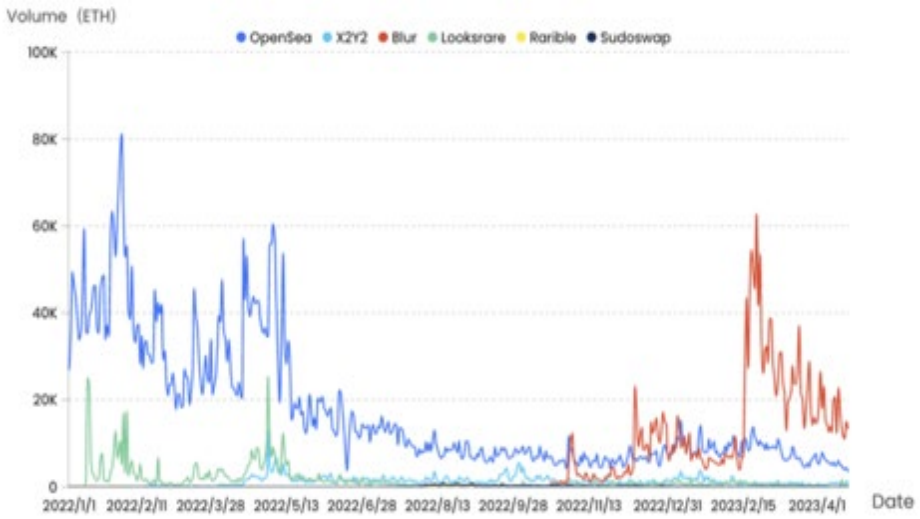

Figure 9. NFT marketplace volume comparison
Source: https://coinmarketcap.com/academy/article/2023-nft-market-analysis:-an-insider-look

The chart presented above depicts a significant surge in Blur's trading volume following its airdrop on February 15. Cumulative trading volume data from January to April of this year reveals that Blur has outperformed OpenSea by 120%. However, it is worth noting that the number of independent traders on OpenSea is approximately three times higher than that of Blur, which has around 590,000 traders. This indicates that the majority of traders on Blur are professional traders who engage in high-frequency trading and conduct trades with larger average amounts. In terms of the number of addresses, OpenSea has only experienced a 12% growth. Moreover, NFTGo offers GoTrading solutions, which can assist in the swift and easy creation of your own NFT marketplace aggregator. While the OJK (Indonesian Financial Services Authority) provides statistics on the performance of banks throughout the year, the graph below showcases the trend of NFTs.

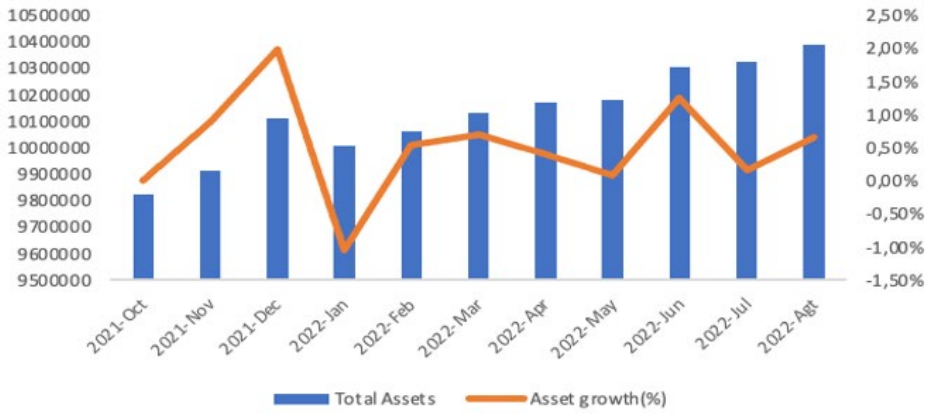

Figure 10. Indonesian Bank Asset Growth
Source: https://www.qeios.com/read/CSTTYQ.2

Bank assets exhibit an overall upward trend from October 2021 to August 2022, as depicted in Figure 10. However, the growth of assets shows high variability, which highlights the inherent risks associated with bank asset acquisition and management. The graph indicates that the performance of bank asset growth has been positive, suggesting an increase in customer assets deposited with banks. This growth can indicate the potential for risk in managing these assets. In terms of market growth in Indonesia, the revenue of the NFT market is expected to experience a rapid rise according to industry research. It is projected to reach an impressive value of 33.66 million USD by 2027. This significant figure demonstrates the increasing interest and acceptance of NFTs in the country, making Indonesia an appealing destination for NFT-related firms. NFTs are being utilized across a broad range of industries in Indonesia, including art, music, real estate, and gaming.

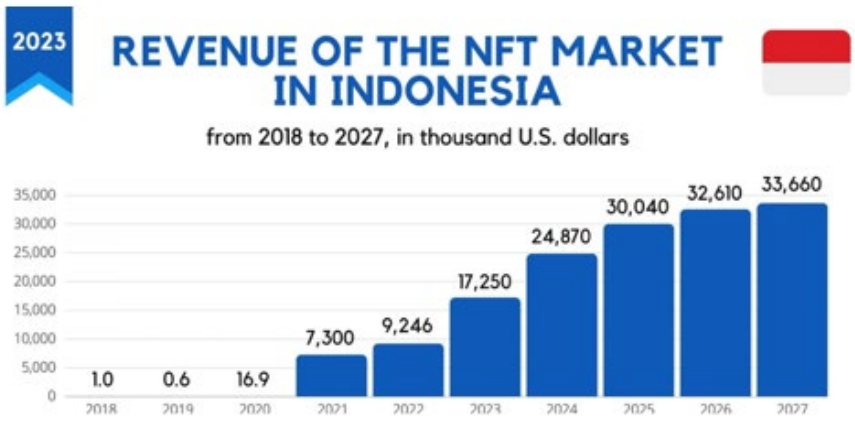

Figure 11. NFT Market Growth in Indonesia
Source: https://www.ajmarketing.io/post/the-ultimate-guide-to-nft-marketing-in-indonesia

According with Figure 11, the revenue market of NFTs in Indonesia is surprisingly experiencing growth, even though NFTs may not be as popular as before. This trend can potentially indicate that NFTs are still being utilized as a medium for money laundering. The projected increase in revenue until 2027 suggests that NFTs continue to hold value in the market ("Prospecting Consumers' Interest for Fashion NFT in Indonesia," 2022). In Indonesia, NFTs have gained significant popularity, with individuals attempting to capitalize on the trend by selling various types of NFTs, ranging from selfies to digital art. The availability of diverse NFT options allows anyone to participate in this activity, opening opportunities for criminals to create their own NFTs and potentially withdraw funds. Criminals can leverage NFT platforms to monetize their illicit financial flows and exercise full control over their activities. Regarding the cybersecurity index in Indonesia, assessing the strength of cybersecurity is crucial when considering the factors contributing to cyber laundering in the country. Below are some facts that highlight the level of security in Indonesia's cybersecurity index compared to other ASEAN countries.

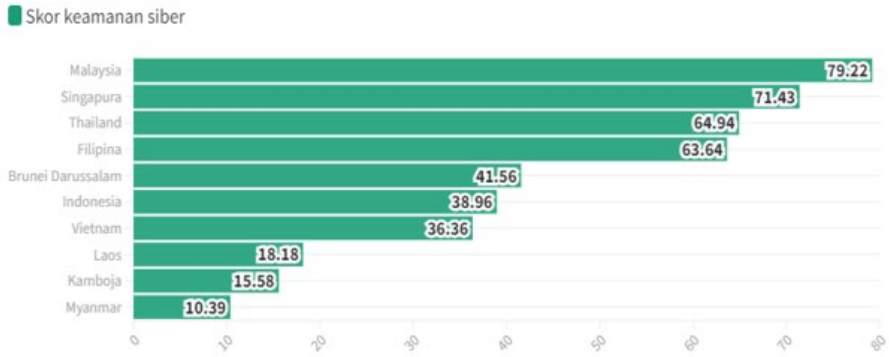

Figure 12. ASEAN Cybersecurity Index 2022
Source: https://data.goodstats.id/statistic/agneszefanyayonatan/indonesia-jadi-salah-satu-negara-dengan-keamanan-siber-terbaik-di-asean-8KhrD

From the graph, it is evident that Indonesia ranks 6th among the ASEAN countries in terms of the strength of its cybersecurity, with a score of 38.96 points. This ranking suggests that Indonesia still requires further improvements in its cybersecurity systems. It is important to note that Indonesia holds a substantial amount of personal data for its population, surpassing 200 million individuals. The potential consequences of data breaches and the misuse of this data for malicious purposes could be disastrous. Therefore, enhancing cybersecurity measures and protecting sensitive data should be a priority for Indonesia.

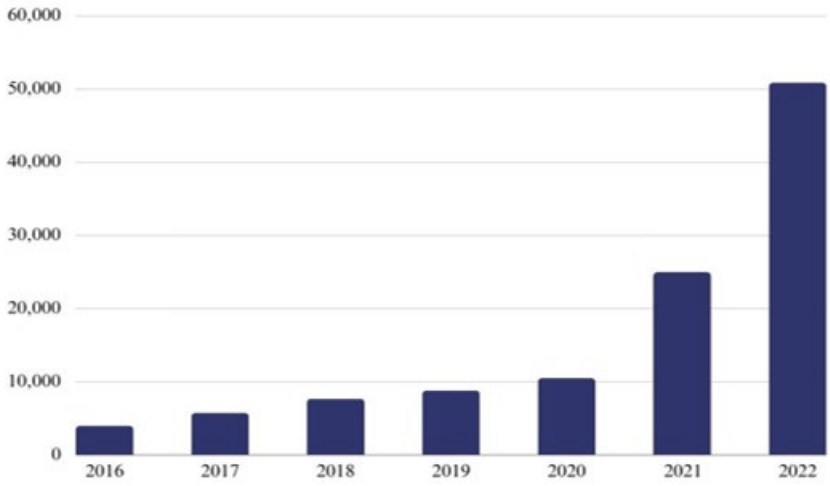

Figure 13. Total Cryptocurrency Laundered by 2015-2022in Indonesia
Source: https://www.chainalysis.com

In 2022, roughly $23.8 billion worth of cryptocurrency was sent from illicit addresses, indicating a substantial 68.0% increase compared to the previous year. As mentioned earlier, NFTs have been identified as a potential avenue for cyber laundering, allowing criminals to transfer and hide unlawfully obtained funds. The revenue market of NFTs in Indonesia has been growing, indicating continued interest and usage despite potential risks. It is worth noting the significance of major centralized exchanges in the cryptocurrency ecosystem. These exchanges typically receive the largest share of illicit cryptocurrency, accounting for nearly half of all funds originating from illicit sources. This is noteworthy because centralized exchanges are expected to have systems in place to detect and address such activities. Moreover, these exchanges serve as pathways for converting illicit cryptocurrency into cash, acting as fiat off-ramps. Thus, the link between NFTs, cyber laundering, and the role of centralized exchanges highlights the need for robust cybersecurity measures and effective regulatory frameworks to combat illicit activities in the digital realm. Protecting personal data and enhancing cybersecurity in Indonesia's context becomes even more crucial considering the potential risks associated with the increasing use of NFTs and the significant amount of personal data held by the country.

Conclusion

Non-fungible tokens (NFTs) have gained significant relevance in various industrial applications, particularly within blockchain and the metaverse. They offer new opportunities for business innovation and entrepreneurship. However, there is a lack of comprehensive studies examining the key aspects of NFT success, trends, and challenges.

While NFTs have become a major trend in the digital space, it is important to recognize the potential risks associated with advanced technology. Money laundering and terrorism funding have moved beyond traditional methods and have infiltrated the digital realm. Criminals exploit vulnerabilities in the use of NFTs as a medium for conducting these illicit activities, posing a national threat if not adequately addressed.

To effectively combat these issues, governments must consider contemporary technological advancements and cross-border regulations when formulating new anti-money laundering policies that encompass cyberspace. Collaboration among law enforcement agencies, regulatory bodies, and the private sector is crucial in developing effective measures to prevent and detect online financial crimes. Striking a balance between national security and the benefits of emerging technologies is essential.

It is important to recognize that the ramifications of NFTs as a means of money laundering and terrorism funding go beyond typical national security concerns, encompassing cyber security and economic security. Several governments have already implemented legislation to oversee cryptocurrency and NFT transactions, aiming to reduce risks and promote national security. Failing to address the transactional vulnerabilities associated with NFTs could pose a significant threat to national security, especially considering their increasing importance.

Taking action to protect the economic security of Indonesia and other countries involves addressing the potential dangers posed by the exploitation of NFTs. Safeguarding against these risks is crucial for maintaining a secure and stable financial environment.

References

1. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrimedetection techniques. IEEE Access, 8, 137293-137311. *(PDF) Types of Cybercrime and Approaches to Detection*. Available from: https://www.researchgate.net/publication/356815301_Types_of_Cybercrime_and_Approaches_to_Detection
2. Al Shamsi, M., Smith, D., & Gleason, K. (2023). Space transition and the vulnerabilities of the NFT market to financial crime. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-09-2022-0218
3. Anagnostopoulos, I. (2018). Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business*, *100*, 7-25. https://doi.org/10.1016/j.jeconbus.2018.07.003
4. Avan-Nomayo, O. (2019). *Cryptocurrency Mixers and Why Governments May Want to Shut Them Down*. Cointelegraph. https://cointelegraph.com/news/cryptocurrency-mixers-and-why-governments-may-want-to-shut-them-down
5. Day, M. Y. (2021). Artificial intelligence for knowledge graphs of cryptocurrency anti-money laundering in fintech. *Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2021*. https://doi.org/10.1145/3487351.3488415

6. Dowling, M. (2022). Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters*, *44*. https://doi.org/10.1016/j.frl.2021.102097
7. Dyntu, V. & Dykyi, O. (2019). CRYPTOCURRENCY IN THE SYSTEM OF MONEY LAUNDERING. *Baltic Journal of Economic Studies*, *4*(5). https://doi.org/10.30525/2256-0742/2018-4-5-75-81
8. Gjoni, M., Gjoni, A. (Karameta), & Kora, H. (Bako). (2015). *Money Laundering Effects*. *UBT International Conference*. https://knowledgecenter.ubt-uni.net/conference/2015/all-events/16 , https://doi.org/10.33107/ubt-ic.2015.16
9. Jamil, N., Qassim, Q. S., Bohani, F. A., Mansor, M., & Ramachandaramurthy, V. K. (2021). Cybersecurity of microgrid: State-of-the-art review and possible directions of future research. In *Applied Sciences (Switzerland)* (Vol. 11, Issue 21). https://doi.org/10.3390/app11219812
10. Korejo, M. S., Rajamanickam, R., & Muhamad, M. H. (2021). The concept of money laundering: a quest for legal definition. *Journal of Money Laundering Control*, *24*(4). https://doi.org/10.1108/JMLC-05-2020-0045
11. Lagutin, V., Boiko, A., & Shkuropadska, D. (2020). Institutional Conditions for Ensuring Resilience of National Economy: The Example of Ukraine. *Baltic Journal of Economic Studies*, *6*(3). https://doi.org/10.30525/2256-0742/2020-6-3-76-86
12. Lestari, E.A.P. (2021). Complex Interdependence Between Indonesia-Australia Through Cybersecurity Cooperation Post-Indonesia-Australia Cyberwar in 2013. *Jurnal Hubungan Internasional*, *9*(2). https://doi.org/10.18196/jhi.v9i2.10522
13. Naqvi, N. (2020). Conference Proceedings of 2nd Blockchain International Scientific Conference ISC2020. In *The Journal of the British Blockchain Association*.
14. Pinto-Gutiérrez, C., Gaitán, S., Jaramillo, D., & Velasquez, S. (2022). The NFT Hype: What Draws Attention to Non-Fungible Tokens? *Mathematics*, *10*(3). https://doi.org/10.3390/math10030335
15. Prospecting Consumers' Interest for Fashion NFT in Indonesia. (2022). *International Journal of Business and Technology Management*. https://doi.org/10.55057 /ijbtm.2022.4.3.8
16. Scarle, S., Arnab, S., Dunwell, I., Petridis, P., Protopsaltis, A., & de Freitas, S. (2012). E-commerce transactions in a virtual environment: Virtual transactions. *Electronic Commerce Research*, *12*(3). https://doi.org/10.1007/s10660-012-9098-4
17. Šikman, M., & Grujić, M. (2021). Relationship of Anti-Money Laundering Index with GDP, financial market development, and Human Development Index. *Nauka, Bezbednost, Policija*, *26*(1). https://doi.org/10.5937/nabepo26-29725
18. Sina Osivand. (2021). Smart collectibles; use case of NFT tokens. *Open Access Research Journal of Engineering and Technology*, *1*(2). https://doi.org/10. 53022/oarjet.2021.1.2.0113
19. Vitvitskiy, S. S., Kurakin, O. N., Pokataev, P. S., Skriabin, O. M., & Sanakoiev, D. B. (2021). Formation of a new paradigm of anti-money laundering: The experience of Ukraine. *Problems and Perspectives in Management*, *19*(1). https://doi.org/ 10.21511/ppm.19(1).2021.30
20. Vitvitskyi, S., Syzonenko, A., & Titochka, T. (2022). DEFINITION OF CRIMINAL AND ILLEGAL ACTIVITIES IN THE ECONOMIC SPHERE. *Baltic Journal of Economic Studies*, *8*(4). https://doi.org/10.30525/2256-0742/2022-8-4-34-39
21. Wojciech Filipkowski. (2008). Cyber Laundering: An Analysis of Typology and Tecniques. *International Journal of Criminal Justice Sciences*, 15-17.

22. Wronka, C. (2022a), “Cyber-laundering: the change of money laundering in the digital age”, *Journal of Money Laundering Control*, Vol. 25 No. 2, pp. 330-344, 10.1108/JMLC-04-2021-0035.
23. Yuheng, L., Cheng, W. & Xiao, W. (2023) Measuring national economic resilience to the SARS and COVID-19 pandemics, *Applied Economics*, 10.1080/00036846.2023.2274304

Internet sources

https://www.chainalysis.com
https://coinmarketcap.com/academy/article/2023-nft-market-analysis:-an-insider-look
https://medium.com/@AMLCrypto/how-to-launder-money-with-nfts-97dce7f2d6a

Authorized files sources

National Cyber and Encryption Agency (BSSN)
Cyber Threat Intelligence Programme (CTIP)
Financial Services Authority's (OJK)