Reconstructing Crypto Asset Regulation for Effective Prevention and Eradication of Money Laundering and Terrorist Financing

Garda T. Paripurna
Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia
Jl. Ir Sutami No.36, Kec. Jebres, Kota Surakarta, Jawa Tengah, Indonesia 57126
garda.paripurna@uns.ac.id

Adi Sulistiyono
Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia
Jl. Ir Sutami No.36, Kec. Jebres, Kota Surakarta, Jawa Tengah, Indonesia 57126
adisulistiyono@staff.uns.ac.id

Hartiwiningsih Hartiwiningsih
Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia
Jl. Ir Sutami No.36, Kec. Jebres, Kota Surakarta, Jawa Tengah, Indonesia 57126
hartiwiningsih@staff.uns.ac.id

Yunus Husein
Faculty of Law, Universitas Indonesia, Jakarta, Indonesia
Jl. Prof. Mr Djokosoetono, Depok, Jawa Barat, 16424
yunus.husein@gmail.com

Abstract— The rapid proliferation of crypto assets presents an urgent need to reconstruct regulatory frameworks to address the escalating challenges of money laundering (AML) and terrorist financing (TF). This abstract advocates for a strategic overhaul, emphasizing the necessity of adapting regulations to the dynamic and borderless nature of the crypto landscape. The reconstruction effort involves leveraging cutting-edge technologies, including blockchain analytics and artificial intelligence, to enhance regulatory capabilities for monitoring and tracing crypto transactions. By incorporating these tools, regulators can establish a more robust system for preventing and eradicating illicit financial activities within the crypto sphere. The abstract highlights the importance of fostering international collaboration among regulatory bodies, law enforcement agencies, and industry stakeholders. Establishing standardized global regulatory frameworks is proposed as a pivotal step to create a unified front against financial crimes, eliminating regulatory arbitrage and promoting a cohesive approach to addressing AML and TF challenges. In conclusion, this abstract underscores the exigency of reconstructing crypto asset regulation to prevent and eradicate money laundering and terrorist financing effectively. By acknowledging the distinctive features of crypto assets and embracing technological innovations, regulators can fortify the integrity of financial systems and cultivate responsible crypto asset usage on a global scale.

Keywords— crypto, regulatory, money laundering, terrorist financing.

I. INTRODUCTION

The development of the crypto asset business worldwide, including in Indonesia, showed significant progress in transaction volume and value, although it is often characterized by value volatility[1]. Based on International Monetary Funds (IMF) calculations, it is estimated that the market capitalization value of Crypto Assets in the world will be USD 1.2 trillion at the end of April 2023, which makes it an essential element in the financial sector and has de facto created a new, increasingly strategic "shadow financial system." in the world economy[2]. Meanwhile, there are 420 million known Crypto Asset owners worldwide.

Meanwhile, domestically, based on data from the Commodity Futures Trading Supervisory Agency (BAPPEBTI)[3], the development of Crypto Asset transaction value was recorded to be very significant, namely IDR 64.9 trillion in 2020, rising sharply to IDR 859.4 trillion in 2021, then decreasing to IDR 306.4 trillion in 2022. Meanwhile, registered Crypto Asset customers were 11.2 million as of December 31, 2021, increasing to 16.70 million as of December 2022 and 17.91 million customers in September 2023.

Crypto Assets are in great demand by the world community, especially Indonesia, an emerging market

A. K. Jaelani et al. (eds.), *Proceedings of the International Conference on Law, Economic & Good Governance (IC-LAW 2023)*, Advances in Social Science, Education and Humanities Research 827,
https://doi.org/10.2991/978-2-38476-218-7_25

supported by strong, dynamic, and profitable financial and capital markets. The rise and fall in the value of Crypto Assets makes them a business risk that investors must consider carefully. My second interest is because of the dangers of Money Laundering and Terrorist Financing arising from the misuse of CRYPTO ASSETS. Misuse of Crypto Assets in Money Laundering and Financing of Terrorism is a new dimension of crime modus operandi that interests criminals because of the various privileges offered. These privileges include transactions that can be carried out quickly, being able to involve significant crime proceeds through complex transactions, reaching across national borders, and having complete confidentiality with the "high levels of anonymity" feature, as well as playing in the "dark web" area which is difficult to detect.

The National Risk Assessment Report on Money Laundering and Terrorist Financing, released in 2021 by the Indonesian Government, places Crypto Assets as a high-risk and emerging threat that requires special attention. In FATF's 40 Recommendations, international standards require countries to mitigate risks to identify, understand, assess, and carry out strict regulation and supervision of crypto assets and crypto asset service providers.

In addition, in 2020, it was discovered from transfer records that financial criminals carried out Bitcoin transfers worth more than USD 3.5 billion involving Bitcoin accounts controlled by dark markets, ransomware criminals, hackers, and fraudsters. In 2022, the bankruptcy case of the FTX crypto exchange in the United States resulted in losses worth USD 3.1 billion belonging to its 50 largest creditors, and Sam Bankman Fried, the owner, was sentenced to 115 years in prison on seven charges including fraud, conspiracy, and money laundering.

Some transactions involving crypto assets can occur without financial intermediaries; in this case, no regulated financial institutions can implement anti-money laundering and counter-terrorist financing prevention measures, such as customer due diligence, recording, and reporting suspicious transactions. Additionally, many cryptoassets or service providers specifically incorporate technology designed to prevent transparency, such as dropping or mixing services or anonymity-enhanced coins (AEC) (Moreover, many cryptoassets or service providers specifically include technology intended to avoid transparency, such as tumbling or mixing services or anonymity-enhanced coins (AECs).

II. LITERATURE REVIEW

These Crypto Asset features align with the primary goal of Money Laundering perpetrators, namely to disguise the origin of criminal assets, including covering up personal identity so that it is difficult for financial intelligence agencies (Financial Intelligence Unit/FIU) or law enforcement officials to track them. Safeguarding the CRYPTO ASSET industry as our authority protects the financial services sector industry from perpetrators of Money Laundering and Terrorist Financing crimes and the flow of illicit money or assets resulting from corruption is maintaining and upholding the integrity of the financial system (financial system integrity) which will have a positive impact on creating system stability finance, a solid economic system and efforts to achieve prosperity and welfare of the people [4].

Misuse of Crypto Assets in Money Laundering and Financing of Terrorism is a crime with a new dimension that is of interest to criminals because of various privileges, including being able to carry out quickly, involving significant crime proceeds through complex transactions, reaching across national borders and having "high levels of anonymity," to playing in areas of the “dark web” that are difficult to detect[5]. This Crypto Asset feature is in line with the primary objective of Money Laundering and Terrorist Financing perpetrators, namely disguising the origin of criminal assets, including covering one's identity so that it is difficult for financial intelligence agencies (Financial Intelligence Unit/FIU) or law enforcement officials to track them.

Indonesia is in a transition period for the regulation and supervision of Crypto Assets after the enactment of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (PPSK) on January 12, 2023. The PPSK Law is the basis for transferring duties and authority for regulating and supervising financial assets[12]—Digital, including crypto assets, from BAPPEBTI to OJK (Article 312). The government and DPR-RI passed Law Number 4 of 2023 concerning Development and Strengthening of the Financial Sector (UU PPSK) on January 12, 2023, with the aim of, among other things, strengthening institutions and financial system stability, developing and strengthening the financial sector ecosystem; and strengthening the authority, responsibilities, duties, and functions of financial sector regulators (Article 3).

The functions, duties, and authority for regulating and supervising crypto assets (virtual assets) in the context of preventing and eradicating TPPU and TPPT after the enactment of the PPSK Law are inadequate (inadequate) to the requirements as regulated in FATF's 40 Recommendations and other standards. The PPSK Law only aims to achieve financial system stability and does not at all aim to create financial system integrity.[13]

Reconstruction of the functions, duties, and authority for the regulation and supervision of crypto assets in the framework of effective prevention and eradication of TPPU and TPPT is urgently carried out by adding the goal of achieving financial system integrity to the PPSK Law, strengthening institutional cooperation mechanisms in exchanging information and handling cases of misuse of crypto assets between

OJK and PPATK and related Ministries/Institutions.

Currently, until two years into the enactment of the 2025 PPSK Law, the authority to issue permits, regulate and supervise Virtual Assets as Commodities and Virtual Assets Service Providers (VASPs) rests with the Commodity Futures Trading Supervisory Agency (BAPPEBTI).[14] In the framework of Anti-Money Laundering and Prevention of Terrorism Financing (APU-PPT), Bappebti has issued Commodity Futures Trading Supervisory Agency Regulation Number 6 of 2019 concerning the Implementation of Anti-Money Laundering and Prevention of Terrorism Financing (APU and PPT) Programs Regarding the Implementation of Physical Markets for Futures Exchange Commodities. This Bappebti regulation requires the submission of Virtual Assets Service Providers (VASPs) reports, including Suspicious Financial Transaction Reports to PPATK, in addition to other obligations such as implementing Customer Due Diligence (CDD) and a Risk-Based approach within the APU and PPT framework.[15]

Apart from that, OJK and Bank Indonesia are in the process of making Virtual Assets and VASPs objects of supervision. The risks posed by Virtual Assets include high volatility in investment value, which has the potential to disrupt the financial system's stability, so macroprudential management by Bank Indonesia is necessary to prevent systemic risks from occurring. Apart from that, PPATK, as the primary guardian of anti-money laundering, also has yet to explicitly supervise crypto asset transactions and fund flows, so the detection and monitoring of suspicious financial transactions has practically not been carried out optimally by any of the Ministries and Institutions.

Article 93 of the Anti-Money Laundering Law opens up opportunities for the adoption of international provisions and standards into statutory regulations; Article 93 reads, "If there is the development of international conventions or international recommendations in the field of preventing and eradicating criminal acts of money laundering and terrorist financing, PPATK and the relevant agencies can implement these provisions by the provisions of the laws and regulations." Based on the domestic need to increase supervision of Virtual Assets and Virtual Assets Service Providers (VASPs) to mitigate the risk of their misuse in TPPU crimes, the Government, together with relevant Ministries and Institutions, needs to jointly reformulate the TPPU Prevention and Eradication Policy with a modus operandi for abuse of Virtual Assets and Virtual Assets Providers.[16]

To mitigate the risk of TPPU, policymakers must focus their attention on the "emerging risk" posed by Virtual Assets which serious criminals misuse, both individuals and organized criminal groups, and closely monitor the organizers or Virtual Asset Service Providers (VASPs), including targeting unlicensed or illegal Virtual Assets organizers who operate underground.

Several points related to the basic principles of Crypto Asset regulation and law. Basic Principles of Crypto Regulation As Set Out in International Standards (quoted in part). BIS is of the view that although countries set different criteria in categorizing crypto assets, most competent authorities in several countries agree on the application of the basic principle of "same business, same rules, same risks, same rules) for crypto assets. Regulation and supervision depend on the risks faced, and the Government/Authority carries out the assessment.

III. METHOD

This normative or doctrinal legal research methodology is normative juridical legal research or normative legal research which is basically an activity that will examine the internal aspects of positive law. Normative legal research focuses more on the scope of legal conceptions, legal principles and legal rules. It can be concluded based on existing doctrine, that normative legal research is a type of legal research methodology that bases its analysis on applicable laws and regulations that are relevant to the legal issues that are the focus of the research.

IV. RESULT AND DISCUSSION

Cases of Money Laundering and Terrorist Financing with the typology of abuse of Crypto Assets (crypto assets or Virtual Assets) have occurred in many countries, such as the United States and Japan, and Indonesia is no exception[6]. In 2017, the case of "The 'Wannacry' Ransomware" in the United States revealed that victims paid a ransom in Bitcoin amounting to USD 8 million for hacker attacks on thousands of government computer systems and private companies controlled by the perpetrators. Fraud using Cryptocurrencies was the biggest crime in the United States in 2019 and 2020[7]. With Ponzi Schemes carried out by organized syndicates causing losses of USD 2.9 billion and USD 1.9 billion, this amount is the largest in recorded history of crimes using Cryptocurrencies. in the United States.

In Japan, the Japanese National Police announced that in 2018 there were more than 7,000 cases of money laundering related to cryptocurrency, a 10-fold increase compared to the previous year, 2017. Cryptoasset theft also worried investors in Japan after discovering the disappearance of 58 billion Yen in cryptocurrency from Coincheck in January 2018. Even though the public trauma has not disappeared since

the tragedy of the loss of USD 435 million Bitcoin in 2014, which caused the bankruptcy of Mt. Gox, the world's largest cryptocurrency exchange company based in Shibuya, Tokyo, controls more than 70% of the value of Bitcoin transactions worldwide[8].

In Indonesia, there are at least 2 cases of money laundering using Bitcoin, namely those allegedly carried out by three suspects in the mega corruption scandal at PT. ASABRI in 2021 is estimated to cause state losses of IDR 23.7 trillion, and the E-Dinar Coin Cash (EDCCASH) investment fraud case in the same year, which appears to be trading in Cryptocurrencies which has lost 57 thousand investors, is estimated at more than IDR 5, 8 trillion. In 2015, these Virtual Assets also attracted the interest of terrorist crime perpetrators, such as what happened in the bomb tragedy at Alam Sutera Mall, South Tangerang, where the perpetrator named Leopard Wisnu Kumala, carried out extortion by asking for 100 Bitcoins from the management of Alam Sutera Mall Management as a threat. before the bomb detonated. This bomb tragedy, although it later turned out to be carried out by a single perpetrator who was not related to a particular terrorist network (lone wolf), has encouraged awareness of the misuse of Crypto Assets (Cryptoassets or Virtual Assets) in criminal acts.

Various regulatory and supervisory policy steps in preventing Money Laundering and Terrorist Financing crimes with the misuse of Crypto Assets (Crypto assets or Virtual Assets) have been carried out through various international forums. Ministers of Finance and Governors of Central Banks from G20 countries in 2019 urged the FATF as a standard-setting organization in the field of Anti-Money Laundering and Prevention of Terrorist Financing in the world to encourage countries to tighten regulations and increase supervision over the use of Crypto Assets (Cryptoassets or Virtual Assets), in line with growing abuse in several countries[9].

Several countries, such as China and India, prohibit the use of Virtual Assets. Some countries, such as Australia, France, Germany, the United States, Italy, Japan, and Switzerland, strictly regulate and supervise providers or exchangers within the framework of anti-money laundering and preventing the financing of terrorism. In contrast, several other countries, such as South Korea, Saudi Arabia, Russia, Canada, and the EU, have prepared laws and regulations. Indonesia is one country that prohibits using Virtual Assets in payment and transaction settlement systems as per Bank Indonesia policy. OJK prohibits financial services under its rule and supervision from using, trading, providing loans, or producing Virtual Assets—however, the Ministry of Trade cq. The Commodity Futures Trading Supervisory Agency (Bappebti) has licensing, regulatory, and supervisory authority over the trading of Virtual Assets as an investment vehicle on commodity exchanges and Virtual Assets Service Providers (VSAPs)[10].

As mentioned above, the disparity in regulation and supervision of Crypto Assets and physical Crypto Asset trading companies is visible among the G20 countries, of which Indonesia is one of the members. Even with this, as the FATF explains, most countries still need to adequately regulate or supervise crypto assets. Hence, gaps in the global regulatory system create significant loopholes that money laundering and terrorist financing actors can misuse.

With the support of the G20, FATF has issued several guidelines needed to prevent the misuse of Crypto Assets in money laundering and terrorist financing crimes, including in October 2021, FATF issued FATF's Updated Guidance for Risk Based Approach which regulates procedures and matters relating to supervision risk-based against physical Crypto Asset trading companies (Virtual Asset Service Providers (VASPs). Its FATF's Report on Virtual Assets Red Flags Indicators of Money Laundering and Terrorist Financing (September 2020), which compiles case study reports from countries in the period 2017 to 2020, reveals trends in the misuse of Virtual Assets related to money laundering crimes and predicate crimes.[11]

Meanwhile, the Bank for International Settlements (BIS) – Financial Stability Institute (FSI) published Insights on Supervising Cryptoassets for Anti-Money Laundering in April 2021, which includes, among other things, recommendations for supervisors to conduct an open dialogue with the private sector and provide a transition period for physical Crypto Asset trading companies (VASPs) operating, completing regulations regarding Crypto Assets and physical Crypto Asset trading companies (VASPs), and carrying out national risk assessments for Anti-Money Laundering (National Risk Assessment) as well as law enforcement/regulatory actions.

Apart from that, BAPPEBTI's 2022 Performance Report states that the Crypto Asset Physical Market Trading ecosystem has yet to be formed. Bappebti has issued regulations for implementing the Physical Crypto Asset Market on the Futures Exchange to protect the public who trade Crypto Assets. However, the required institutions, namely the Crypto Asset Futures Exchange, Futures Clearing House, and Depository Manager, still need to be fully formed. To optimize Crypto Asset Physical Market Trading, it is necessary to improve regulations and strengthen the supervision of Crypto Asset business actors. It is also required to prepare a trading ecosystem, such as forming a cryptocurrency exchange.

Several points related to the basic principles of Crypto Asset regulation and law. Basic Principles of Crypto Regulation As Set Out in International Standards (quoted in part). BIS is of the view that although countries set different criteria in categorizing crypto assets, most competent authorities in several countries

agree on the application of the basic principle of "same business, same rules, same risks, same rules) for crypto assets. Regulation and supervision depend on the risks faced, and the Government/Authority carries out the assessment.

The question, in turn, depends on the risk assessment carried out by the government or competent authority regarding what risks are posed by Virtual Assets (VA) and the activities of related Virtual Assets Service Providers (VASPs), which must be regulated in statutory regulations and are there legal loopholes or lacunae that need to be closed with legislation. How do FATF 40 Recommendations handle law enforcement issues regarding misuse of VA and VASPs? What is the purpose of law enforcement? Enforcement actions remain limited in number and have been carried out by very few authorities in a country (jurisdiction); this certainly leaves room for improvement. This is partly due to the novelty of the regulations in most jurisdictions.

Based on the information in the survey results, in jurisdictions where law enforcement measures have been taken, the behavior subject to sanctions often includes fraud or unregistered activity. Given the importance of public and transparent enforcement actions to demonstrate the authorities' commitment to implementing regulations and the role these actions play in helping the overall AML/CFT system mature, further attention is needed in this area.

Therefore, many jurisdictions expect more enforcement actions as supervisory frameworks mature. The Travel Rule is a binding FATF obligation, but most jurisdictions must implement it effectively. The Travel Rule is a binding FATF obligation, but most jurisdictions must implement it effectively. Several jurisdictions question whether they can reasonably impose travel rules on CSPs until technological solutions are available to make compliance less onerous, as SWIFT does for correspondent banking.

Surveyed authorities also raised concerns that compliance with travel regulations will only be manageable if these technological solutions are generally accepted or inoperable. However, other jurisdictions are implementing the rule now because it is feasible, although challenging. Those who have implemented these requirements can provide an example for those who have not. P2P transactions pose risk challenges, etc.

P2P transactions pose challenges, but views differ on their magnitude. Some jurisdictions consider these transactions equivalent to cash exchanges and believe that the risks they involve fall within the risk tolerances of FATF standards and national regulations. This is especially the case when authorities expect P2P transactions to remain limited in number, with most of these assets passing through CSPs before they can be used. The availability of ledger analytics tools to track these assets has also partly raised concerns among some authorities regarding P2P transactions, as it suggests transparency can be achieved. However, others believe that the comparison with cash is inappropriate and have concerns regarding the possible disintermediation of P2P transactions.

Additionally, there is a distinct risk that P2P transactions will proliferate in scale, especially as crypto assets become more widely accepted. The potential dangers posed by P2P transactions indicate that additional mitigation measures may be necessary. However, many jurisdictions need more explicit risk assessments to guide their decisions. There is an opportunity to adopt new approaches that take advantage of the inherently data-rich nature of the cryptoasset sector. The authorities are committed to supporting responsible financial innovation while ensuring adequate oversight: new Surveillance Methods And Suptech Applications. New monitoring methods and Suptech applications can help pursue this balance and maximize its resources. That should allow them to use data and technology tools such as blockchain analytics to increase the effectiveness of their surveillance frameworks.

International cooperation to monitor the sector effectively is critical. The inherently cross-border nature of crypto assets and the uneven application of global international standards in this area make international cooperation a crucial component for adequate supervision. This is especially true considering how new the sector is. The watchdog appears to have the necessary legal authority and channels for international cooperation, but its actual use is another area requiring improvement. New crypto asset business models may pose financial crime, consumer/investor, market integrity, and financial stability risks that still need to be captured by existing regulatory frameworks, presenting challenges in adapting regulations to meet new needs. This is the case, for example, of the financial crime risks posed by new market participants such as crypto asset issuers, exchange and wallet providers, or the financial stability risks posed by global stablecoin arrangements.

Globally, international standard-setting bodies (SSBs) have expanded the scope of their standards and recommendations (e.g., FATF), have revised them (e.g. FSB), or are in the process of assessing the adequacy of their measures (e.g. Basel Committee on Banking Supervision, Payments and Infrastructure Committee Markets and International Organization of Securities Commissions) to capture a range of risks to the global financial system posed by crypto assets and related activities not previously covered within their framework. This study focuses on "positive legal norms within the legislative system" and employs a normative legal research methodology. The present study provides evidence that the research methodology utilized in this legal study is a hybrid of statutory and conceptual approaches. Document study, a legal material collection

technique, was used in this research. Data was gathered from various scholarly sources, including laws and regulations, books, journals, articles, reports by previous researchers, and other pertinent documents about the examined subjects.[17]

V. CONCLUSION

Indonesia is currently in a transition period for the regulation and supervision of Crypto Assets after the enactment of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (PPSK). The functions, duties, and authority for regulating and supervising crypto assets must be revised to the requirements in FATF's 40 Recommendations and other standards. To improve supervision of Virtual Assets and Virtual Assets Service Providers (VASPs) to mitigate the risk of their misuse in TPPU crimes, the Government and relevant Ministries and Institutions need to jointly reformulate the TPPU Prevention and Eradication Policy with a modus operandi for abuse of Virtual Assets and Virtual Assets Providers. Crypto asset regulation and law are based on the basic principles of "same business, same rules, same risks, same rules" as set out in international standards. Governments and authorities apply these principles to regulate and supervise crypto assets, assessing risks and addressing legal loopholes. Enforcement actions are limited and have been carried out by few rules in a country, leaving room for improvement.

VI. REFERENCES

[1] S. Y. Choi, “Entry into the Crypto Assets Business by Global Financial Services Firms,” SSRN Electron. J., 2023, doi: 10.2139/ssrn.4343323.

[2] D. D. S. Ningsih, D. H. Achmad, E. K. Dewi, and Y. A. P. Purnami, “Crypto Asset as a Transaction Tool in the Perspective of Economic Analysis of Law: Legal Consequences and Ius Constituendum,” Rechtsidee, vol. 10, Jun. 2022, doi: 10.21070/jihr.v10i0.787.

[3] T. Morozova, R. Akhmadeev, L. Lehoux, A. Yumashev, G. V. Meshkova, and M. Lukiyanova, “Crypto asset assessment models in financial reporting content typologies,” Entrep. Sustain. Issues, vol. 7, no. 3, pp. 2196–2212, Mar. 2020, doi 10.9770/jesi.2020.7.3(49).

[4] M. A. Amrullah, “The Countermeasure Of Criminal Act Of Terrorism Financing Through Money Laundering,” Pattimura Law J., vol. 6, no. 2, p. 49, Mar. 2022, doi: 10.47268/palau.v6i2.949.

[5] C. P. Buttigieg, C. Efthymiopoulos, A. Attard, and S. Cuyle, “Anti-money laundering regulation of crypto assets in Europe’s smallest member state,” Law Finance. Mark. Rev., vol. 13, no. 4, pp. 211–227, Oct. 2019, doi: 10.1080/17521440.2019.1663996.

[6] M. I. Inozemtsev, “Digital Assets in the United States: Legal Aspects,” 2021, pp. 514–522. doi: 10.1007/978-3-030-53277-2_61.

[7] M. Kutera, “Cryptocurrencies as a subject of financial fraud,” J. Entrep. Manag. Innov., vol. 18, no. 4, pp. 45–77, 2022, doi: 10.7341/20221842.

[8] M. A. García-Ramos Lucero and R. Rejas Muslera, “Análisis del desarrollo normativo de las criptomonedas en las principales jurisdicciones: Europa, Estados Unidos y Japón,” IDP Rev. Internet Derecho y Política, no. 35, pp. 1–13, Jan. 2022, doi: 10.7238/idp.v0i35.391466.

[9] N. M. Artemov, L. L. Arzumanova, A. A. Sitnik, Y. L. Smirnikova, and S. Zenin, “The legal regulatory model of virtual currency circulation: A socio-legal study,” JURÍDICAS CUC, vol. 16, no. 1, Feb. 2020, doi: 10.17981/juridcuc.16.1.2020.05.

[10] D. Irma, S. Maemunah, S. Zuhri, and N. Juhandi, “The future of cryptocurrency legality in Indonesia,” J. Econ. Bus. Lett., vol. 1, no. 1, pp. 20–23, Jun. 2021, doi: 10.55942/jebl.v1i1.87.

[11] M. Tatar and K. Martynenko, “SYSTEM ANALYSIS OF SUBJECTS CRYPTOCURRENCIES OPERATIONS IN THE CONDITIONS OF GLOBAL CHALLENGES,” Model. Dev. Econ. Syst., no. 4, pp. 100–108, Dec. 2022, doi 10.31891/mdes/2022-6-13.

[12] A. Simbolon and D. I. G. Sinaga, “The Legality of Cryptocurrency Transactions in Indonesia,” J. Daulat Huk., vol. 5, no. 3, p. 196, Oct. 2022, doi: 10.30659/jdh.v5i3.26722.

[13] V. Taniady, S. P. Permatasari, and R. W. Nugraha, “Crypto Asset-Trade Resilience During The Covid-19 Pandemic In Indonesia,” J. Jurisprud., vol. 11, no. 1, pp. 31–43, Jan. 2022, doi: 10.23917/jurisprudence.v11i1.13340.

[14] Iriansyah, R. Febrina, and Irfansyah, “THE IMPLEMENTATION OF COMMODITY FUTURES TRADING LAW AND THE AUTHORITY OF THE COMMODITY FUTURES TRADING SUPERVISORY AGENCY (BAPPEBTI),” Russ. J. Agric. Socio-Economic Sci., vol. 139, no. 7, pp. 48–55, Jul. 2023, doi: 10.18551/rjoas.2023-07.06.

[15] K. Christiani, A. Wibisono, and G. H. TW, “Perlindungan Hukum Terhadap Nasabah Cryptocurrency

Di Indonesia," SALAM J. Sos. dan Budaya Syar-i, vol. 9, no. 5, pp. 1541−1556, Aug. 2022, doi: 10.15408/sjsbs.v9i5.27644.

[16] M. A. Murizqy and R. Dirkareshza, "Peninjauan Aspek Keamanan Dan Perlindungan Hukum Terhadap Investor Crpytocurrency," J. Ius Const., vol. 7, no. 2, p. 277, Oct. 2022, doi: 10.26623/jic.v7i2.4067.

[17] H. Rahma, A. Fauzi, B. Juanda, and B. Widjojanto, "Development of a Composite Measure of Regional Sustainable Development in Indonesia," pp. 1–16, 2019.