

Application of Smart Contract in Transaction of Non-Fungible Token: Legality, Risk and Critical Evaluation Against Existing Legal Framework in Indonesia

Rahandy Rizki Prananda, Umaira Hayuning Anggayasti *,
Muhammad Febrian Syukur

Faculty of Law, Universitas Diponegoro

ABSTRAK: The emergence of Non-Fungible Tokens (NFTs) has transformed the digital economy by facilitating the ownership and transfer of distinct digital assets through blockchain technology. Smart contracts are integral to NFT transactions, as they automate processes such as ownership transfers and royalty distributions; however, they also present legal and regulatory challenges. In Indonesia, the absence of a definitive legal framework for smart contracts and NFTs raises concerns regarding their legitimacy and consumer protection. This study investigates the legality and risks associated with NFT transactions in the context of Indonesian law, emphasizing the deficiencies in current regulations, particularly regarding ownership rights and fraud prevention. The research employs a variety of legal methodologies and theoretical frameworks to scrutinize existing legislation. It concludes that the prevailing regulations are inadequate to address the requirements of NFT transactions. The paper proposes reforms, including the formal recognition of smart contracts, enhancements in consumer protection, and the establishment of explicit dispute resolution mechanisms to ensure legal clarity and foster secure digital innovation.

Keywords: Smart Contract, Non-Fungible Token, Evaluation, Legal Framework

I. INTRODUCTION

Indonesia has encounter in the digital era with increasingly sophisticated electronic technology. This instruments lead to transformation in various activities getting easier. For instance shopping does not have to be done in conventional mechanism that forces buyers to meet merchant directly or use cash. Sales and purchase able to be conducted online workable for buyers since they are unnecessary to come in person and pay in cash. All of transaction is fully take place through systems that serve online trading via the internet. The advancements of technology in the sector of e-commerce clearly bring significant shifting in many aspects of human life. This also encourages the emergence of new ways to make payments. The dependence on cash based –trade transaction shifted to cashless. Nowadays, many payments can be made paperless.¹ Utilization of digital technology encourage transaction is proceed electronically, giving rise to virtual payment.

¹ Rasji & Melia (2023). Analisis Hukum Terhadap Penggunaan Aset Kripto Sebagai Alat Pembayaran di Indonesia. Jurnal Kewarganegaraan Vol. 7 No. 2 Desember 2023 P-ISSN: 1978-0184 E-ISSN: 2723-2328

Currently, digital assets are emerging as the preferred items in the virtual realm. This results from the rising digital assets following the advent of blockchain technology. Digital assets comprise, among others, Bitcoin, Ethereum, Tether, XRP/Ripple, Bitcoin Cash, Binance Coin, Polkadot, Cardano, and Solana, along with other assets that satisfy the requirements set forth in the Commodity Futures Trading Regulatory Agency Regulation Number 7 regarding the Identification of the List of Crypto Assets eligible for Trading in the Crypto Asset Physical Market.² Dissimilar to regular digital items, a new kind of digital asset has been created that involves art variations. These art variations are often referred to as 'super rare art' due to their unique nature when an artist posts their work in an online gallery, and then a deal is made to sell the artwork on the Ethereum platform. The artist digitally signs this deal using a special kind of encryption to confirm that the artwork is real, and the sharing of the artwork happens through the Inter Planetary File System, known as IPFS. This system works like a community network, using special codes that let the artwork spread across different codes but still count as one single piece. This special item is called a Non-Fungible Token, or NFT.³ The concept of NFTs is actually rooted in a long tradition of using art as a way to enjoy beauty and show status. For instance, pieces by famous artists like Pablo Picasso, Gerhard Richter, Jean-Michel Basquiat, and Andy Warhol are often seen at high-end art auctions and have been sold for prices in the hundreds of millions of dollars. NFT can be understood as a digital asset that represents various real-world items such as artwork, videos, photos, music, tickets, and other creative works. NFT is a new digital platform that helps artists introduce their works in a simple and secure way, making it easier to use. It helps artists earn money from their works in a better way.

Non-Fungible Token (NFT) is one way of using blockchain technology, where all owners and NFT transactions are recorded in an open system, and each NFT has a different code, making each item unique. This unique NFT concept makes it different from cryptocurrencies because each cryptocurrency does not have its own unique code like NFTs, which makes them uniform and these tokens can be exchanged (fungible tokens). NFTs generally represent real-world items such as photos, videos, images, paintings, music, and other creative works.⁴ NFTs are highly sought after since those instrument provide opportunities for creators and investors to buy and sell digital objects exclusively. NFTs are often used in the fields of art, business, and entertainment. This is related to technological advancements, particularly with the existence of Smart Contracts. Smart Contracts, which can be interpreted as intelligent contracts, are self-executing contracts, or contracts on the blockchain, first proposed by Nick Szabo, a legal expert, cryptographer, and computer scientist. Nick began developing this idea in 1994.⁵

Smart contracts enable trustworthy transactions without the need for a third party. These transactions can be traced and cannot be altered. Smart contracts contain all the details about the contract terms and execute all intended processes automatically. This makes Smart contracts a good choice for online transactions, especially in buying and selling digital goods like NFTs. Due to their automatic nature, the contract contents can be carried out without interference from others.⁶ The existence of smart contracts turns users find it easier to invest, as there are no intermediaries such as banks, brokers, or the government involved in the transaction process. Through blockchain technology, which operates automatically, also ensures that transactions can be conducted securely. Smart contracts in transaction or trading processes will automate and trigger subsequent actions when the required

² Muhammad Usman Noor, "NFT (Non-Fungible Token): Masa Depan Arsip Digital? Atau Hanya Sekedar Bubble?" Pustakaloka:Jurnal Kajian Informasi dan Perpustakaan Volume 13 No. 2, Desember 2021 p. 229-230

³ Aletha, N. O. (2022). Memahami Non Fungible Tokens (NFT) Di Industri CryptoArt. Center of Digital Society. <https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2022/01/80-CfDS-Case-Study-Memahami-Non-Fungible-Tokens-NFT-di-Industri-CryptoArt.pdf>

⁴ Sulistianingsih, D., & Kinanti, A. K. (2022). Hak Karya Cipta Non-Fungible Token (Nft) Dalam Sudut Pandang Hukum Hak Kekayaan Intelektual. *Krtha Bhayangkara*, 16(1), 197-206.

⁵ Raskin, M. (2017). The Law And Legality Of Smart Contracts. *Georgetown Law Technology Review*, 1(2), 320. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166

⁶ Turk, Ž., & Klinc, R. (2017). Potentials of Blockchain Technology for Construction Management. doi: <https://doi.org/10.1016/j.proeng.2017.08.052>

conditions are met. In this way, the blockchain can record all contracts between parties from their creation to their implementation on the blockchain network. Smart contracts are a new invention, different from previous types of technology. Its mechanism are conducted entirely on-chain through blockchain platforms and use smart contract code as the contract language.⁷

Blockchain is a particular type of technology called "distributed ledger technology" or DLT, and it is changing the finance industry as well as how businesses operate. due to its capacity to significantly eliminate intermediary subjects. Blockchain represents a unique type of database that securely maintains a permanent record of past transactions. It can be readily modified for various applications and has the potential to enhance all manual processes that involve the sharing and storage of information. Owing to its resilience, this technology is frequently referred to as a "disruptive innovation" or a "foundational innovation." Furthermore, blockchain has the potential to facilitate the adoption of smart contracts, which may transform the processes of contract creation, signing, and execution. However, due to its numerous applications and complex characteristics, blockchain presents significant challenges for the government in regulating innovation and safeguarding users from potential harm.

The use of smart contracts in Indonesia is not yet specifically regulated in legislation, but there are regulations regarding blockchain in financial technology (fintech). In Article 23 of Financial Services Authority Regulation Number 77/POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services or Fintech, it is stipulated that fintech providers may exchange data with supporting fintech service providers, which may include information technology such as big data analytics, aggregators, robo-advisors, or blockchain. Furthermore, blockchain is also explained as a financial transaction bookkeeping service based on information technology, which records and stores transaction proof data or a ledger distributed across a computer network, either privately or publicly. With the brief description above, it is illustrated that the development of blockchain's has a good potential not only spread on fintech but also expand to business sector rely on online marketplaces.

In the terms of NFT's transaction, Blockchain, which was initially only used to perform simple computing processes, such as recording transaction data, has been developed to perform more complex computing processes with smart contracts integration.⁸ The proprietor only has records and hash codes that indicate ownership of unique tokens associated with digital assets because the exclusivity of NFTs aligns with their primary purpose, which is to avoid all forms of plagiarism as a form of infringement of artists' intellectual property rights. It should be noted that its operation is still hampered in the field due to a lack of transparency, considering that NFTs are run anonymously on a blockchain system where anyone can claim digital art as its own by embedding a token on the artwork, regardless of whether they didn't create it.

The characteristics of Smart Contracts also raise legal issues that might present legal risks for those who engage in NFT transactions. First, their decentralized nature means data is not centralized in one specific location. Therefore, when fraud occurs within the system, leading to legal losses for those involved, it exacerbates the law enforcement procedure because the platform is borderless. Second, the data is immutable once recorded on the blockchain; it can only be added to the system. Third, the exclusive nature makes smart contracts separate and inaccessible to parties not involved in the network. Fourth, autonomous smart contracts contain potential weaknesses due to human error in programming, the existence of security loopholes that may be exploited, dependence on external data (oracles), transaction costs for execution, and uncertainty in legal regulations and difficulties that may arise when modifying the code after it is operational. Fifth, there is the potential for inaccuracies where errors in the code (bugs) can lead to financial losses due to their immutable nature once

⁷ Vasiliki Papadouli, Vagelis Papakonstantinou, 'A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs', (2023), 51, Computer Law & Security Review.[9].

⁸ Wax, S. (2021). A Primer on Non-Fungible Tokens and Smart Contracts. Lawyer Monthly. <https://www.lawyer-monthly.com/2021/05/a-primer-on-non-fungible-tokens-and-smart-contracts/>

integrated into the blockchain. Additional problems include reliance on "oracles" (external data) which can be a weak point, as well as legal issues caused by still insufficient regulations. Further, ambiguity and interpretation arise because the smart contract syntax is written in code, which differs from the contract language used in general contracts.

This research focuses on identifying the legal consequences of using smart contract applications in Non-Fungible Token (NFT) transactions and critiquing how Indonesian law, particularly contract law and telematics law, views the use of smart contracts in blockchain systems for Non-Fungible Token (NFT) transactions. The gap of research would be analyze utilize set principles of Contract and theory of legal protection. Additionally, this study will analyze the regulatory implementation of smart contracts in Non-Fungible Token (NFT) transactions in the Singapore and USA, aimed at providing input for a legal framework to regulate the standardization of smart contract platforms in the trade of Non-Fungible Token (NFT) commodities in Indonesia. This study deploys both primary and secondary legal resources, which are thoroughly analyzed and assessed.

II. RESEARCH METHOD

Peter Mahmud Marzuki stated that according to the views and understandings provided by many authors, legal research is able to understood as a way to discover legal regulations, legal principles, and legal doctrines with the aim of providing explanations about legal issues being faced.⁹ The set of law references as follow: regulations in Cyber space, digital economic and contract following with academic articles concerning NFTs, Smart contract and Technology law and other pertinent subjects, have been gathered and employed as the main reference materials for this study. Essentially, the research is descriptive, requiring the collection of relevant data to illustrate the phenomena being examined. The gathered data is analyzed through qualitative methods, incorporating statutory and conceptual approaches, along with comparative analysis. This allows the research to tackle existing issues and propose solutions to the identified challenges.

III. DISCUSSION AND ANALYSIS

1. MIND A GAP OF DOMESTIC REGULATORY TO RESPONSE AGAINST DISRUPT POTENTIAL AGAINST THE RIGHT OF SUBJECT

A contract is an arrangement in which one or more parties make promises to one another, establishing a legal relationship known as an obligation. Each party's obligations and rights are also involved.¹⁰ Contracts can only be deemed legally binding on the parties concerned if they are made in accordance with the law. This concept is well known as principle of *pacta sunt servanda*, states that all agreements between parties become legally binding, much like binding regulation. In contrast to the widespread use of its technology on the internet, the legal instrument to regulate remains uncertainty. This occurred since there are no clear regulations regarding NFT in general and smart contract legalities in particular. The use of smart contracts still adheres to the principles of data law, specifically paragraphs 1320 and 1338, which explain the principles of Freedom of Contract and Validity of Contract, respectively. Since both norms were created during Dutch colonial era, The absence of legal guidance has an impact on both general contract and specific contract. As of right now, the technology available is not very suitable for creating smart contracts, which have been developed very quickly compared to traditional contracts and have the ability to automatically execute obligation in case the requirement has already been violated.

Furthermore, smart contracts have a different pattern form compared to conventional contract. In literally, an agreement or contract typically consists of several parts, such as the Title, Preamble, Recitals, Premises, Body of the agreement, Conclusion, and Signatures of the involved parties.¹¹ All of this must meet the requirements for

⁹ Qamar, N, & Rezah, F.S. (2020), *Metode Penelitian Hukum Doktrinal dan Non-Doktrinal* (Makassar: CV. Social Politic Genius (SiGn), 13.

¹⁰ Munir Fuady, *Hukum Kontrak (dari Sudut Pandang Hukum Bisnis)*, (Citra Aditya Bakti, 2007),

¹¹ Salim HS> 2021. *Hukum Kontrak Elektronik E-Contract Law*. Depok: Rajagrafindo. Indonesia.

the agreement to be considered valid and in accordance with the principles of contracting. These principles include the principle of consensus, where both parties agree to create obligations; the principle of freedom of contract, which states that a contract can be formed as long as it does not violate the law, public order, and morals; the principle of pacta sunt servanda, where the agreement binds the parties as law for those who agree to it; and the principle of good faith. Next, there are several rules that stipulate that contracts must be written in Indonesian or at least in two languages. This rule is contained in Law Number 24 of 2009 concerning the National Flag, Language, symbol and National Anthem.¹²

Reviewing discussion in the previous section, smart contracts is able to be classified into electronic contracts and innominate agreements. The definition of an electronic contract or e-contract itself is found in Article 1 paragraph 17 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, which states that it is an agreement made by the parties thru an electronic system. It is also explained in Article 18 paragraph (1) of the ITE Law that "Electronic transactions contained in Electronic Contracts are binding on the parties." In addition, electronic contracts, as part of an agreement, must be subject to the provisions of the Civil Code. In electronic contract, the provisions of Book III of the Civil Code regarding Contract Law can be applied. The Civil Code states in Article 1313 that "An agreement is an act by which one or more persons bind themselves to one or more other persons." If we refer to Article 1313 of the Civil Code, then an electronic contract can be considered a form of agreement that meets that article.¹³ Eventually, it could be concluded that smart contracts are agreements that operate using an electronic system,

Moreover, smart contracts fall under the category of new forms contracts (contracts innominati), meaning they are not yet regulated in the Civil Code and Commercial Code. According to the Civil Code, an agreement is free and not bound by a specific form, as stated in Article 1338, which reads, "All agreements made in accordance with the law are valid as law for those who make them." This article serves as the basis for the principle of freedom of contract. According to the principle of freedom of contract, everyone is free to create any contract they wish, as long as the contract meets the requirements and does not violate legal provisions, morality, or public order.¹⁴ In addition, electronic contracts, as agreements, must also adhere to the principles of contracts. which is based on the Civil Code, namely the principle of consensualism, the principle of good faith, the principle of personality, and the principle of pacta sunt servanda. It is also important to consider the principles of electronic contracts mentioned in Article 3 of the ITE Law, namely the principle of technological neutrality or the principle of freedom of technological choice, the principle of benefit, and the principle of caution.

Considering to aforementioned contractual principles inherit to smart contract should accomplish some qualifications stipulated on Article 1320 of Civil Code This article states that for a valid agreement to be formed, four conditions must be met: 1. the parties must agree to be bound by the agreement; 2. the parties must have the legal capacity to enter into an agreement; 3. there must be a specific subject matter of the agreement; and 4. the agreement must have a lawful cause. The first two conditions are subjective requirements, as they relate to the parties entering into the agreement. If any of these conditions are not met, the agreement may be revoked. This means one party can file a lawsuit to have the agreement revoked. However, if none of the parties object, the agreement will still be considered valid and binding.

The third and fourth conditions are objective requirements, as they pertain to the agreement itself or the object of the legal act. If these are not fulfilled, the agreement is considered null and void, meaning it is treated as if it never existed from the beginning.

In the context of smart contracts in NFT transactions, the status of NFTs as transactional commodities within smart contracts may lead to the failure of the fourth condition, which requires the agreement to have a lawful

¹² Muhammad Noor, "Penerapan Prinsip – Prinsip Hukum Perikatan dan Pembuatan Kontrak", Mazahib, No. 1 Vol XIV (Juni 2015), hal.92

¹³ Ridwan Romadoni & Dona Budi Kharisma. 2019. "Aspek Hukum Kontrak Elektronik (E-Contract) dalam Transaksi E-Commerce yang menggunakan Bitcoin sebagai Alat Pembayaran". Jurnal Privat Law. Vol. VII No. 1. Surakarta: Bagian Keperdataan Fakultas Hukum Universitas Sebelas Maret

¹⁴ Subekti, R. 2003. Pokok-Pokok Hukum Perdata, Jakarta: PT Intermasa

cause.

This is due to a conflict with the aforementioned legal provisions. As a result, electronic transaction agreements created using Ethereum blockchain smart contracts are considered null and void since it fail to comply against one of the objective requirements. This means the agreement is treated as if it never existed or never formed a legal obligation between the parties. Consequently, the contract should not be executed or completed at all, and all parties must return everything to its original state. However, this does not mean the use of smart contracts is prohibited in Indonesia. Smart contracts are a beneficial innovation that can greatly assist businesses in the future. Specifically, for blockchain Ethereum transactions involving smart contracts, the payment method ought use crypto asset. If in the future smart contracts is able to be utilized as a tool for transacting new types of digital commodities, then its applications ought to obey to all the requirements for a valid contract will be met, and they will not violate any legal regulations.

The rapid expansion of Non-Fungible Token transactions built upon smart contracts introduces a legal architecture that interacts imperfectly with Indonesia's existing regulatory framework. Although Indonesia possesses several foundational statutes, such as the Electronic Information and Transactions Law, the Copyright Law, the Personal Data Protection Law, the Consumer Protection Law, and the Financial Sector Development and Strengthening Law, these instruments were not drafted with the technical and conceptual complexities of blockchain in mind. The result is a fragmented regulatory environment in which the rights of subjects involved in NFT creation, ownership, or exchange are insufficiently protected. The inconsistency between the immutable, automated, and decentralized nature of blockchain and the principles embedded in Indonesian civil, administrative, and IP law becomes the central source of the regulatory gap.

A primary area of tension lies in the legal status and enforceability of smart contracts. While Indonesian law recognizes electronic documents as valid evidence, no statutory guidance clarifies how to interpret a contractual relationship governed simultaneously by human-readable text and machine-executable code. In a traditional contract, a misrepresentation, clerical error, or breach allows a party to seek annulment or renegotiation. Smart contracts, by contrast, trigger automated performance without discretionary assessment or equitable intervention, often leaving aggrieved parties without a clear remedial avenue at the moment a malfunction or coding error occurs. The absence of a statutory doctrine on the precedence between the written contract and the deployed code creates uncertainty over fault attribution, the burden of proof, and the enforceability of correction mechanisms. This ambiguity places consumers and creators at a disadvantage because irreversible transfers encoded on-chain may effectively eliminate their ability to recover digital assets through conventional civil remedies. Similar inconsistencies surface in the domain of copyright protection. Many NFT buyers mistakenly assume that purchasing an NFT grants ownership of the underlying intellectual property, even though Indonesian copyright law separates token ownership from copyright ownership.

In practice, NFT marketplaces frequently fail to incorporate standardized licensing terms, leaving too much interpretive space regarding economic rights, moral rights, or permissible downstream use. When creators encounter fraudulent "minting" of their works, existing copyright remedies are theoretically available but practically constrained by issues of extraterritorial jurisdiction, anonymity of perpetrators, and the challenge of proving provenance when metadata is incomplete or stored off-chain. Without a coherent framework governing NFT-specific licensing or verification obligations for platforms, creators' rights remain vulnerable to manipulation at scale.

The protection of personal data presents an even more structural conflict. Blockchain's immutability is in direct tension with the rights guaranteed under the Personal Data Protection Law, including the right to deletion, correction, and withdrawal of consent. A single NFT may contain metadata linking to identifiable information, wallet addresses, creative profiles, or third-party databases. Once written to the blockchain, such data becomes practically impossible to erase without compromising the integrity of the ledger. In the absence of detailed regulatory guidance on privacy-preserving blockchain design, data minimization standards, or the scope of

“erasure” in a distributed environment, data subjects face the real risk of permanent exposure far beyond the original purpose of processing. This legal vacuum disproportionately affects individuals whose identities can be inferred from blockchain activity, even when such exposure is the unintended by-product of a seemingly innocuous token transaction.

Consumer protection norms also struggle to accommodate the idiosyncratic risks of NFT markets. Although general prohibitions on misleading information and unfair business practices exist, they do not directly address structural vulnerabilities inherent in NFT ecosystems, such as price volatility, custodial risks, smart contract upgrades, or security failures of digital wallets. Consumers often participate in NFT marketplaces without adequate disclosure of risks that are technical in nature, such as compromised seed phrases or protocol-level exploits. In this landscape, asymmetries of information widen, and the lack of standardized disclosures leaves individuals exposed to fraud or permanent asset loss even when no malicious intent is involved.

Meanwhile, the financial regulatory landscape remains unsettled. Indonesia has shifted the supervision of digital assets to the Financial Services Authority (OJK) under the 2023 financial reform statute, yet the classification of NFTs, whether as investment instruments, commodities, digital collectibles, or hybrid assets, remains unresolved. This ambiguity affects taxation, anti-money-laundering enforcement, reporting obligations, and the scope of licensing for platforms facilitating NFT sales. The lacuna encourages regulatory arbitrage, where actors exploit inconsistencies between jurisdictions or between domestic supervisory mandates. Without a coherent classification, both the state and market participants operate in a climate of legal uncertainty that complicates compliance and weakens accountability.

The gaps described above underscore the need for a structured reform pathway. Before Indonesia adopts a fully comprehensive statutory approach, targeted regulatory interventions can reduce legal ambiguity while preserving space for innovation. Conceptually, Indonesia could embrace a model that recognizes smart contracts as binding only when accompanied by a human-readable contract that prevails in case of contradiction, a principle adopted in several comparative jurisdictions. Likewise, a standardized NFT licensing taxonomy, privacy-by-design guidelines for blockchain applications, mandatory risk disclosures, and a definitive asset classification policy under OJK would provide a robust transitional architecture. Such reforms would strengthen the protection of creators, consumers, and data subjects while aligning domestic law with the technological realities of decentralized systems.

Table 1. Principal Regulatory Gaps and Their Impact on Subject Rights

Regulatory Area	Key Gap	Impact on Rights
Smart Contract Governance	No statutory rule on the hierarchy between written text and code; absent interpretive doctrine	Irreversible loss of assets; difficulty seeking annulment or correction; unclear fault attribution
Copyright Protection	No standardized NFT licensing; weak provenance verification	Misunderstanding of rights; increased piracy; challenges proving ownership in cross-border disputes
Personal Data Protection	Immutable blockchain incompatible with statutory rights to deletion and correction	Permanent exposure of personal data; lack of effective remedies for data subjects
Consumer Protection	Generic rules not tailored to technical risk of NFTs	Asymmetrical information; heightened vulnerability to fraud and asset loss
Financial Regulation	Lack of definitive classification under OJK	Regulatory arbitrage; uncertain taxation; weak AML safeguards

Altogether, the findings demonstrate that Indonesia's regulatory landscape is not yet capable of fully addressing the disruptive potential of smart-contract-based NFT transactions. The law's reactive posture contrasts sharply with the technological determinism of blockchain systems. Without a deliberate reform agenda, the asymmetry between technological innovation and legal safeguards will continue to widen, placing creators, consumers, and data subjects in a persistently vulnerable position. By acknowledging the structural nature of these challenges and embracing a forward-looking regulatory strategy, Indonesia can construct a legal environment that protects rights without stifling creativity or technological experimentation. The existence of Ethereum smart contracts in Indonesia is legally recognized under the ITE Law and the PSTE Regulation, and is regulated under the supervision of the Financial Services Authority (OJK) thru digital financial innovation (OJK Regulation 13/2018) and is currently more detailed in the trading of crypto assets thru OJK Regulation No. 27 of 2024 concerning the Implementation of Digital Financial Asset Trading (which includes crypto). OJK regulations emphasize security, transparency, and consumer protection, ensuring that platforms utilizing this technology (such as NFTs or DeFi) operate legally, but cannot be used for daily transactions (not official payment instruments like the Rupiah). This provision is intended to protect market integrity and ensure that only assets meeting eligibility standards are accessible to retail investors. The latest POJK also introduces a more transparent framework regarding the trading of digital financial asset derivatives. This derivative instrument is permitted as an additional investment option for consumers, but it remains strictly regulated thru the principles of prudence and consumer protection. Exchanges wishing to begin derivatives trading must apply for approval from the OJK. Meanwhile, traders can conduct Digital Asset derivatives transactions at the request of consumers on exchanges that have been licensed, without requiring additional approval from the OJK, as long as there is a cooperation agreement between the two parties. However, this POJK regulation does not stipulate security and suitability standards for blockchain systems, such as audit mechanisms and external access to the system for inspection purposes in the event of a violation of consumer rights.

The lack of resilience providing a clear and specific definition of smart contracts means that transactions must be executed according to general contract principles. In this context, we refer back to the Civil Code and the Electronic Information and Transactions Law (EIT Law) regarding electronic transactions, specifically Articles 40 and 43 of that law. Furthermore, the Electronic Transactions Law (ETL) only focuses on protecting electronic transactions, particularly in articles 41, 49, 50, and 90 regarding the government's role. In addition to the provisions mentioned earlier, this depends on the good faith of the parties involved in the transaction. Existing rules to protect smart contract transactions in NFT products are not working well. This is due to the false protection provided to NFT transaction users. This incident is caused by the very broad meaning of the article and the lack of implementation of an NFT registry that has passed qualification tests and is proven safe for transactions. Additionally, there is a difference points in specific context among between electronic contracts and smart contracts.

An interview with Thelvia Vennianata, Head of Tokomall (an NFT & Crypto e-commerce platform in Indonesia), explains that smart contracts within blockchain technology in general and NFTs in particular are not just a series of words. Rather, it's a series of algorithms and coding within a computer system that connects the parties and is linked to the blockchain system.¹⁵ The smart contract that has been created cannot be deleted, which means that transactions already recorded in the smart contract will always be stored on the blockchain. This confirms that Smart Contracts are not the same as Electronic Contracts in general. Smart contracts are not language or words, but code whose execution is created and adapted from the services or products made within the platform. This type of smart contract makes fraud almost impossible, but on the other hand, cheating caused of intention the parties who designed the smart contract. Despite this, there are no specific provisions regarding the use of smart contracts in Indonesia's legal system, so legal protection for their users is also not yet optimal.

¹⁵ Interview with Thelvia Vennianata, Head of Tokomall in 30 August 2022

Referring to beyond clarification, Based on the previous discussion, it has been clearly explained that smart contracts are vastly different from electronic contracts and are two distinct concepts. This adds to the reasons for the ineffectiveness of existing regulations in closing potential loopholes in NFT transactions using smart contracts. The main aspects that need to be protected in smart contract transactions for NFTs are network security and the use of automated contracts. The security of the network on e-commerce platforms is essentially already regulated, as previously explained, especially regarding electronic transactions and personal data protection. As for more details, the ITE Law in articles 45-52 has provided criminal sanctions in the form of fines for platforms or electronic system and transaction organizers. However, the government has not yet provided clear certification regarding the security of each platform. While there are some basic requirements that have been met for registration, there is no assessment or testing body for the protection of these electronic systems. It leads to the ineffectiveness of enforcing regulations regarding smart contracts in NFT transactions. Most platforms, especially crypto e-commerce platforms, still use certification bodies outside the territory of the Republic of Indonesia, which offer expertise and the ability to conduct security audits and certifications. This contradicts Article 73 paragraph (2) of the PP PSE which. Although contradictory, this is not against the law because there is no provision prohibiting crypto e-commerce platforms from using certification bodies outside the territory of the Republic of Indonesia to make the platform more trustworthy to consumers. Although not against the law, the lack of preparedness in the regulations and the absence of a certification body that consumers can trust to assess the safety of domestic e-commerce crypto platforms have hindered the implementation of the legislation. These circumstances carried hesitation on effectiveness of enforcement, especially the legal protection of the services used by users.

See further on the very broad definition and the lack of uniformity in regulations between state institutions and ministries will make the bureaucracy's push for the use of smart contracts in NFT transactions ineffective. This condition underscores the need for at least a uniform understanding of the institutions that serve as regulators and supervisors in NFT transactions so that user rights can be protected to the maximum extent without overlapping authority.

IV. NAVIGATING THE DAMAGE POTENTIAL OF SMART CONTRACT FOR SECURING NFT'S TRANSACTION IN INDONESIA

4.1. Policy Regulation of Smart Contract for NFT Transaction in Singapore and United States of America

Singapore, as a nation bordering Indonesia, was quicker to respond in preparing regulations regarding electronic transactions. This is evidenced by the enactment of the Electronic Transactions Act ("ETA") in 1998, which was 10 years earlier than Indonesia's Law Number 11 of 2008 concerning Information and Electronic Transactions. likewise, Singapore is also more adaptable to the development of electronic transaction law in its country, adopting the United Nations Convention on the Use of Electronic Communications in International Contracts in 2010 and updating the ETA to the Electronic Transactions Act 2010. Additionally, Singapore was the first country in Asia to adopt the UNCITRAL Model Law on Electronic Commerce.

The ETA serves as the primary regulatory basis for electronic commerce. The regulations contained within are intended to facilitate electronic commerce by removing obstacles arising from uncertainty about written requirements and by promoting the development of legal and business infrastructure to secure electronic commerce. Therefore, information is considered undeniable due to its legal nature, validity, or enforceability based on its electronic form, as stipulated in Article 3, Paragraph (b) of the ETA. This provision promotes the principle of freedom of contract (party autonomy), which is explicitly regulated in Article 5 of the ETA. However, this is limited by exceptions for information required by law to be in written form and with binding legal consequences. In an attempt to ensure a transaction conducted electronically, a contract is required to meet basic elements, namely the presence of an offer and acceptance clearly stated thru electronic communication, as well as other elements

such as consideration, intention to create legal relations, and capacity of the parties.¹⁶ This does not rule out the possibility that a contract can be formed from the interaction between automated systems and individuals.

Smart Contracts, as agreements that run automatically within the ETA, could be categorized under Chapter II of the ETA, "Use of automated message systems for contract formation." Where in Article 2 paragraph (1) the Automated Message system is defined as: "... means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the program or electronic or other means."

This highlights that the Automated Message System exhibits the characteristics of a smart contract, which is a computer program that automatically executes electronic contracts from data (code) without individual intervention in an electronic information system. Further in Chapter II, Article 15, regarding the usefulness of the automated message system, it states: "A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, is not to be denied validity or enforceability solely on the ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

Article 16 of the ETA explains that the regulations regarding errors in the creation of automated messaging systems refer to the initial agreement made when the deal was concluded, meaning the contract or agreement executed must have an information balance between both parties. If an error occurs, the party responsible is the one who made the mistake in the automated message. The provisions regarding compensation and losses due to the fault of a certain party are not the responsibility of the other party, provided that they comply with paragraph 2 of Article 16 of the ETA and paragraph 3 of this regulation, which further clarifies the provisions previously outlined.

In addition to being regulated by the ETA, provisions regarding smart contracts and their application must also comply with the PDPA, which is the Personal Data Protection Act enacted in Singapore in 2012. This law is designed to regulate the collection, use, and disclosure of personal data by organizations in a manner that respects individuals' right to protect their personal data, as well as the organizations' requirement to gather, use, or disclose personal data for purposes considered reasonable in the circumstances. The PDPA contains detailed provisions regarding the types of data that organizations, companies, or data service providers can collect about Singapore residents' personal data. The main focus of this law is the protection of personal data of Singaporean citizens, as well as criminal sanctions, especially fines, in case of a data breach or misuse of data beyond its intended function without the consent or knowledge of the service user.

Regarding smart contracts in the execution of NFT transactions, the connection lies in the application of the rules. The parties involved in NFT transactions utilize the services of a third party, in this case, a Crypto NFT e-commerce platform that has service guidelines and collects personal data from each party. The provisions regarding this are contained in Chapters IV and V of the PDPA concerning the collection, use, and disclosure of personal data, and access to and correction of personal data. In Chapter IV, Consent is mentioned, which means agreement or awareness. Articles 13 to 16 list the criteria for Consent, starting with:

"An organisation must not, on or after 2 July 2014, collect, use or disclose personal data about an individual unless :

(a) the individual gives, or is deemed to have given, his or her consent under this Act to the collection, use or disclosure, as the case may be; or

¹⁶ Eureka Inola Kadly, et all. 2021. Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura. LPPM Universitas Jambi : Jurnal Sains Sosio Humaniora Volume 5 Nomor 1 Juni 2021

(b) the collection, use or disclosure (as the case may be) without the individual's consent is required or authorised under this Act or any other written law.

This article states that, outside of the provisions of Article 13 and subsequent articles, personal data collected without consent or in violation of the provisions of this law constitutes a violation of this law. Where violations are committed, sanctions will be imposed in accordance with the provisions of Chapter X of Singapore's PDPA, specifically Articles 51 and 52 of this law. The sanctions listed can be fines or imprisonment, depending on the court process and the evidence of the violation committed. Generally speaking, the penalties received range from \$5,000 (five thousand Singapore dollars) to 00,000 (one hundred thousand Singapore dollars), with a maximum prison sentence of 6 (six) months to 3 (three) years.

The paragraph that follows explains how the role and obligation of crypto NFT e-commerce is to implement appropriate regulations for the protection of its consumers' personal data. Both buyers and NFT's creator use the services of that e-commerce platform. If there is a violation of consent, then the creator of the smart contract (crypto NFT e-commerce) or if there is a data breach, the e-commerce platform must be responsible for the resulting losses and be penalized for it.

Meanwhile, United States of America arrange a contract or agreement to be recognized as legal, it must comply with two regulations: the Uniform Commercial Code, which contains all comprehensive regulations regarding all commercial transactions in America, and the statute of frauds, which is state law requiring agreements to be written and agreed upon by the parties without coercion.⁵The UCC and the statute of frauds state that not all agreements must be executed in writing. Only a few agreements meet the following criteria to be made in written form: (i) contracts for the sale of goods with a price of \$500 (Five Hundred US Dollars) or more; (ii) lease contracts related to personal property that require total payments of 1,000 (One Thousand US Dollars) or more;⁵² and (iii) certain agreements that create security issues.

Under the Statute of Frauds, an agreement must be in writing if (i) it relates to executorship, suretyship, or marriage; (ii) performance is to be undertaken over one or more years after the agreement's execution; and (iii) it involves the sale of an interest in land.¹⁷ According to Salim HS., an agreement is generally valid in America if it meets the following elements:¹⁸ 1) There is an offer and acceptance; 2) Consideration exists; 3) The parties have the legal capacity to act and the subject matter is legal; 4) There is mutual assent or a meeting of the minds.

in the U.C.C itself and the statute of frauds, both state that a written agreement does not have to be in a specific language comprehensively. The U.C.C specifies that this is intended in the type of "intentional reduction to tangible form".¹⁹ This is in accordance with the U.C.C. policy that the writing requirement is intended to ensure that the parties' intentions are realized. Thus, the court has jurisdiction to handle the cases. The smart contracts in question are not significantly different from general contract requirements, although they are in code form. Smart contracts under the U.C.C still meet the existing contract requirements, especially since the embedded code guaranties the execution of the agreed-upon terms.

Furthermore, this also applies to the statute of frauds, as long as its application is the same as the elements fulfilled in U.C.C. The presence of consideration in an agreement provides a high level of background and authentication, especially in electronic contracts. Without consideration, an agreement is not considered to exist. In addition to the elements mentioned above, especially those of agreements covered by the U.C.C. and the Statute of Frauds, there are several new provisions that provide legality for transactions using smart contracts. This is stated in the provisions of US law called UETA and E-SIGN. UETA stands for the Uniform Electronic Transactions Act, while

¹⁷ Stuart Levi, et all. 2020. Legal issues surrounding the use of smart contracts, global legal insight : blockchain & cryptocurrenncy regulation second edition.

¹⁸ Salim H.S. (2019). Hukum Kontrak: Teori & Teknis Penyusunan Kontrak. Jakarta: Penerbit Sinar Grafika

¹⁹ Stuart Levi, et all. 2020. Op Cit p. 157

E-SIGN stands for Electronic Signatures in Global National Commerce. In brief, both UETA and E-SIGN contain provisions regarding electronic contracts. In both of these legal sources, electronic records and electronic signatures used in interstate or international commercial transactions generally cannot be denied solely because of their electronic form. This provision is already in effect in 47 US states, including Columbia, Puerto Rico, and the Virgin Islands.

Both of these legal sources adopt the concept of automation or "enforcement," which is a hallmark of smart contracts. Based on this provision, an agreement cannot be legally revoked because the parties utilized an "electronic agent" whose every action is defined as including "computer programs or other electronic or automated means used independently to initiate actions or respond to electronic records or performances in whole or in part, without review or action by an individual." Smart Contracts that execute code agreed upon by the contracting parties and implemented thru electronic information systems fall under this definition. In the UETA Commentary, the possibility that electronic agents could transact with other electronic agents or independently is also discussed, which could manifest as smart contracts and evolving artificial intelligence.

In order to obtain the mentioned UETA protection, both parties must first agree in writing (not electronically) that they will conduct all or part of the transaction electronically. Therefore, one party cannot execute a smart contract without the written consent of the other party. Similarly, if written documents must be provided to consumers using services, E-SIGN emphasizes the importance of explicit consumer consent before electronic documents or transactions can be utilized, and that such consent can be revoked at any time. The consumer's right to withdraw consent at any time under the E-SIGN Act can create a dilemma because it introduces operational complexity, given the self-executing nature of many smart contracts. As mentioned, only 47 states have adopted UETA. Illinois (through the state's Electronic Commerce Security Act), New York (through the state's Electronic Signatures and Records Act), and Washington (although state laws recognizing the E-SIGN Act apply to state and local transactions) have each implemented distinct electronic signature laws instead of laws based on UETA. These three states adopted comprehensive definitions of electronic records and electronic signatures, but none provided greater protection for electronic agents, such as smart contracts, than the 47 states that have enacted UETA.

Following this situation, the United States, in preparing to face potential legal issues arising from advancements in information and communication technology, particularly regarding the use of automated contracts executed thru computers, has extensively interpreted legal instruments such as the U.C.C. and UETA. Although some entities like the Uniform Law Commission state that there is no legal relationship between "Smart contracts" and "Contracts,"²⁰ this is due to the unique characteristics of smart contracts in their execution and form, meaning not all smart contracts have legal ties to contracts. Only smart contracts with legal consequences and executed in trade or transactions between parties on electronic information systems or in accordance with the provisions of UETA, E-SIGN, and U.C.C. can be considered contracts and have binding elements.

Even if a consensus isn't reached, actions taken by a smart contract may be deemed adequate to hold the members of a DAO accountable for breaches of securities regulations. In *Samuels v. Lido DAO*, No.23-cv-06492-VC, 2024 WL 4815022, at *4 (N.D. Cal. Nov. 18, 2024),²¹ the question was whether DAO members could be considered a legal entity liable to legal action. A DAO is a type of organization that is regulated by code, typically functioning without centralized authority, with rules integrated and upheld by smart contracts. The court in *Samuels* determined that the DAO, which jointly made governance decisions and had a substantial market effect, might be held accountable under specific legal theories. Notably, despite the DAO functioning through autonomous code,

²⁰ Uniform, T., Commission, L., Committee, E., & Note, G. (2019). The Uniform Law Commission Executive Committee approved the Guidance Note at its January 2019 midyear meeting. Hlm. 4-5

²¹ *Samuels v. Lido Dao*, No.23-cv-06492-VC, 2024 WL 4815022, at *4, *11, *12 (N.D. Cal. Nov. 18, 2024).

the court highlighted that human participants within the DAO played a role in decision-making—thereby obscuring the distinction between automated code and conventional agency or corporate responsibility.

A crucial difference arising in legal rulings is the separation between mutable and immutable smart contracts. The Fifth Circuit Court of Appeals examined this matter in *Van Loon v. Department of the Treasury*, 122 F.4th 549 (5th Cir. (2024), a case stemming from the federal government's sanctions on Tornado Cash—a decentralized protocol employing smart contracts to enable private cryptocurrency transactions.²² In *Van Loon*, the court emphasized a critical legal issue: can immutable smart contracts—those that are not owned, managed, or changeable by any individual or organization—be classified as “property” under federal law for sanctions? The court investigated the difference between mutable contracts, which can be revised or managed by one party, and immutable contracts, which operate independently and cannot be altered once implemented.

The Fifth Circuit concluded that the immutable smart contracts of Tornado Cash did not qualify as “property” according to the applicable sanctions laws, as they cannot be owned or controlled by any specific entity. This differentiation has significant consequences: if smart contracts cannot be associated with a legal person or organization, enforcement—whether private or regulatory—becomes challenging or unfeasible.²³ This case demonstrates the legal ambiguity associated with decentralized technologies. Mutable smart contracts can meet standard contract requirements (e.g., control, agreement, alteration), whereas immutable contracts question basic principles of contract law and ownership, including the identity of the party executing the actions, if any.

4.2. Reconstructing Domestic Policy Framework for Covering Right of Subjects and Ease Doing Business in Technology Sector

Law is an essential element in social life that plays a role in maintaining order, justice, and balance among individuals in society. In the Latin adage “ubi societas ibi ius,” it is stated that “where there is society, there is law,” which indicates that law arises from social needs.²⁴ Beside serving as a tool for control, law also reflects values, norms, and desires. a community that is constantly advancing.²⁵ In this context, regulations not only play a role in maintaining the status quo but can also be drivers of social change. The concept of law as a means of social engineering (social regulation serves as an instrument for social engineering) was introduced by Roscoe Pound thru a sociological legal theory approach. Pound stated that law needs to adapt to societal progress and play a role in balancing various societal interests.²⁶ Law must not only be enforced textually, but also needs to be able to restructure unbalanced social order.²⁷ In his view, the law should promote social balance thru structured and gradual change.

Pound saw law as shaping and renewing society. Smart contracts are a new technology that can revolutionize the way transactions are conducted, speed up processes, and reduce costs, which aligns with Pound's goal of social progress. Furthermore, Pound divides interests into individual (transactional profit), public (system security), and social (data protection, fairness). Smart contract regulation needs to balance these interests, for example, personal data security (individual/public) versus automation efficiency (social). Although automated, smart contracts must still be based on good faith and fulfill promises. Regulations ensure that automatically running code continues to reflect fairness and does not cause undue harm, as outlined in Pound's theory of contract integrity. Pound's principle, “Law must be stable, and yet it cannot stand still,” is very suitable. Traditional (written) contract law

²² *Van Loon*, 122 F.4th at 555.

²³ *Van Loon*, 122 F.4th at 550.

²⁴ Satjipto Rahardjo, *Ilmu Hukum*, Citra Aditya Bakti, Bandung, 2012, p

²⁵ Shidarta, *Refleksi tentang Struktur Ilmu Hukum*, Mandar Maju, Bandung, 2006, p.25

²⁶ Roscoe Pound, *Law and Morals*, Macmillan, New York, 1910, 29.

²⁷ M. Diab, *Social Engineering and the Legal System: A Global Perspective*, Al Nahda Press, Cairo, 2014, 17.

needs to adapt to the dynamics of smart contracts that run automatically on the blockchain, requiring new regulations to remain relevant and function to protect society.

Apart the existence of regulation stipulates the context of smart contract in general, it would necessary to control further in particular relating the technical matter on Cyberspace. We have identified on the uniqueness characteristic of smart contract which is immutable easily, then to secure it resilience and safety in sustain period, it requires an audit of system by independent entity and determine a certification standart for the qualification of system as additional stipulation.

The primary goals of a regulation that enables the certification of smart contracts should be to safeguard customers, specifically the users of DeFi services, and to enhance trust in DeFi. This regulation would not pertain to smart contracts utilized (i) for non-financial objectives, such as smart contracts delivering NFTs, or (ii) in the context of activities that are already overseen (for instance, under MiCA regarding stablecoin regulation).²⁸ For effectiveness, this type of regulation must at minimum be implemented at the Domestic level .Additionally, Ministry of Communication and Digitalization can coordinate with the Financial Services Authority and the Central Bank of Indonesia in overseeing activities related to crypto assets and digital transactions within the blockchain platform, considering limitations on authority and duties. As an application, the Ministry of Communication and Digitalization can issue a Ministry Regulation to clarify the rules related to blockchain, in accordance with the main duties and functions of the Ministry of Communication and Information in the field of communication and information.

Blockchain certification standards include international professional credentials such as Certified Blockchain Expert (CBE) and Certified Ethereum Developer for technical expertise, as well as security standards like ISO/TC 307 for distributed ledger technology. In Indonesia, the qualification standard of smart contract is embodied inside Government Regulation 28/2025 which recognizes blockchain and requires a Standard Certificate thru OSS for business legality, ensuring quality and compliance, and building a safe and trusted digital ecosystem. The classification of standard encompass ISO/TC 307: International Standards Committee for Blockchain and Distributed Ledger Technology (DLT). ISO 27001: Information Security Management System (ISMS) standard relevant for crypto exchanges and blockchain companies to protect data and enhance trust. Certification would be evaluated at the activity level, thus encompassing protocols in their entirety. (i.e. it would take into account the setup of smart contracts that allow the service to be delivered through a protocol). The standard's three elements (security, governance, compliance) would pertain to the protocol, with the approval of each smart contract in the protocol being awarded based on the foundation of security components solely. A certification registry would provide details on those protocols that have received certification for public accessibility.

In the terms of security aspect, the NFT's issuers on Blockchain, must undergo Independent code audits periodically, penetration testing and security certification issued by authorized institution. Considering on vulnerabilities of Blockchain system are identifiable before its deployment through systematic auditing tools.²⁹ Proportionality measures might be implemented to adjust the requirements' level (light, standard, or high) based on the risk associated with each protocol. The criteria for evaluating this risk may include, based on the situation: Total Value Locked (TVL), transaction volume, transaction count, or user count. Among the three potential regulatory frameworks: (i) voluntary certification, (ii) compulsory certification for all smart contracts, and (iii) compulsory certification with proportionality measures, the third option may offer the greatest assurance for users and investors while not excessively hindering innovation.³⁰ Mandatory certification would entail banning

²⁸ Forum Fintech Acpr-Amf . (2024) Report of the Working group on Smart Contract Certification p. 30-35.

²⁹ Yang, Shuo et al. Definition and Detection of Defects in NFT Smart Contracts. Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis, Seattle, WA, USA, Jul. 2023, pp. 373-384. <https://doi.org/10.1145/3597926.3598063>

³⁰ Op Cit.

all intermediaries in Indonesia from dealing with uncertified smart contracts. Among the three potential methods for organizing certification, ex-ante certification granted by a public authority that accredits a collective of third-party auditors offers numerous theoretical advantages. Nevertheless, if the quantity of certifications to be issued was substantial, prior certification provided directly by accredited auditors would seem like a more feasible option.

Three scenarios need to be differentiated here: (i) the primary certification audit, meaning the first examination of a smart contract or protocol; (ii) the renewal audit post-certification expiration (with no changes made to the smart contract); and (iii) the renewed certification audit after alterations have been made to the smart contract or protocol. This part addresses concerns on three circumstances. The expense of certification, differing based on the complexity of protocols, should mainly be absorbed by the smart contract producer, who is theoretically the party most invested in seeking certification. The proposed regulatory framework should provide public authorities with the necessary powers to monitor the “products” available in the market. Public authorities ought to be capable of formulating or verifying the fundamental principles of the standard, choosing evaluators, and deciding whether to grant a certification.

Furthermore, The Government of Indonesia must establish a statutory definition by revising the ITE Law. Explicitly, Indonesian ITE Law must see the Smart Contract is self –executing electronic agreement operating through digital ledger technology and capable of generating legally unforceable obligation. This definition would eliminate uncertainty on legal recognition. Drafting a legal definition for smart contracts while establishing regulatory principles for them prompts the inquiry into what factors should be considered when identifying and overseeing smart contracts. As a more straightforward approach to blockchain decentralization, the principles used for regulating blockchain technology are also applicable to smart contracts. This examination is concluded in the preceding entries and relies on the primary legal alteration in Indonesia, particularly concerning the electronic legal framework that facilitates the use of smart contracts. Drawing from this understanding, the key principles vital for regulating smart contract usage are:³¹

- a) **Clarity or transparency** of smart contracts that aids in evaluating the quality of an agreement embedded in a smart contract. The legal framework governing smart contracts should also mandate an informative document.
- b) **Verifiability**, specifically smart contracts that ensure all executing smart contracts are legitimate and can be verified as transactions that are carried out automatically or semi-automatically through a validated transaction platform as a medium.
- c) **Trust and compliance**, which emphasizes the necessity for the platform provider of smart contract transaction services to earn users' trust by offering safe, reliable, and secure transaction services concerning security, encompassing both legal and regulatory aspect.

Additionally, the rules of contract in Indonesia must adopting a hybrid model whereby: Traditional legal contract and executable blockchain code. Enlargement of contract's variants able to secure enforceable legal obligation even though the code face malfunction. In temporary, the accommodation hybrid system into regulation considerably compatible in Contract law instead pure code-based agreement.

V. CONCLUSION

Legal certainty regarding the use of smart contracts for Non-Fungible Token transactions in Indonesia is regulated in the ITE Law. This is because the ITE Law adopts the Principle of Technological Neutrality, where regulations concerning electronic transactions in Indonesia are not focused on a specific technology, but rather on the utilization of that technology. This principle results in the regulation of technology use being done generally and considered valid as long as it does not conflict with applicable laws, both within the ITE Law and outside of it, such as in the

³¹ Amato F, Cozzolino G, M. F. (2021). A model for verification and validation of law compliance of smart contracts in IoT environment. IEEE Transactions

Civil Code and other provisions. Conversely, legal protection for smart contract users in NFT transactions is regulated in Article 37 of PP PSE, and structurally, NFT e-commerce offering services falls under the definition of Article 2 paragraph 5 letter b of PP PSTE, which is classified as a Private Electronic System Operator. This has legal consequences: legal protection for NFT transactions thru smart contracts does not create a legal vacuum, but the regulations are still too general and NFTs have not gained any legal status other than that recognized in Article 499 of the Civil Code as digital assets.

The risks of smart contracts in NFT transactions include legal, economic, and governance issues, in addition to technical flaws. While they improve efficiency, they also bring problems like coding errors and misunderstandings about ownership. Indonesia's regulations are not adequate, as they were made for regular electronic transactions. To address these issues, Indonesia should create a smart contract framework that includes legal recognition, audits, consumer protection, dispute resolution, and digital property rights to strengthen its digital economy. Hereinafter, the existing rules define the context and application of smart contract in vary point of view and not detail. This situation turns into uncertainty for enforcing and impose sanction against the perpetrator. To solvent gap of regulation particularly mitigate and secure the ledger system whether it is agile or improper to be operated. Therefore the Government of Indonesia should design the specific rules to check and examine the reliability of ledger through certification from The Ministry of Communication & Digitalization and audit by independence IT auditor.

REFERENCES

- [1.] Aletha, N. O. (2022). Memahami Non Fungible Tokens (NFT) Di Industri CryptoArt. Center of Digital Society. <https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2022/01/80-CfDS-Case-Study-Memahami-Non-Fungible-Tokens-NFT-di-Industri-CryptoArt.pdf>;
- [2.] Amato F, Cozzolino G, M. F. (2021). A model for verification and validation of law compliance of smart contracts in IoT environment. IEEE Transactions;
- [3.] Eureka Inola Kadly, et all. 2021. Keabsahan Blockchain-Smart Contract Dalam Transaksi Elektronik: Indonesia, Amerika Dan Singapura. LPPM Universitas Jambi : Jurnal Sains Sosio Humaniora Volume 5 Nomor 1 Juni;
- [4.] Forum Fintech Acpr-Amf . (2024) Report of the Working group on Smart Contract Certification p. 30-35.
- [5.] M. Diab, Social Engineering and the Legal System: A Global Perspective , Al Nahda Press,Cairo, 2014 , 17;
- [6.] Munir Fuady, Hukum Kontrak (dari Sudut Pandang Hukum Bisnis), (Citra Aditya Bakti, 2007),
- [7.] Muhammad Noor, “Penerapan Prinsip – Prinsip Hukum Perikatan dan Pembuatan Kontrak”,Mazahib, No. 1Vol XIV (Juni 2015);
- [8.] Muhammad Usman Noor, “NFT (Non-Fungible Token): Masa Depan Arsip Digital? Atau Hanya Sekedar Bubble?” Pustakaloka:Jurnal Kajian Informasi dan Perpustakaan Volume 13 No. 2, Desember 2021 p. 229-230
- [9.] Qamar, N, & Rezah, F.S. (2020), Metode Penelitian Hukum Doktrinal dan Non-Doktrinal (Makassar: CV. Social Politic Genius (SiGn), 13;
- [10.] Rasji & Melia (2023). Analisis Hukum Terhadap Penggunaan Aset Kripto Sebagai Alat Pembayaran di Indonesia. Jurnal KewarganegaraanVol. 7 No. 2 Desember 2023 P-ISSN: 1978-0184 E-ISSN: 2723-2328

- [11.] Raskin, M. (2017). The Law And Legality Of Smart Contracts. Georgetown Law Technology Review, 1(2), 320. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166
- [12.] Ridwan Romadoni & Dona Budi Kharisma. 2019. “Aspek Hukum Kontrak Elektronik (E-Contract) dalam Transaksi E-Commerce yang menggunakan Bitcoin sebagai Alat Pembayaran”. Jurnal Privat Law. Vol. VII No. 1. Surakarta: Bagian Keperdataan Fakultas Hukum Universitas Sebelas Maret;
- [13.] Roscoe Pound, Law and Morals , Macmillan, New York, 1910 , 29;
- [14.] Salim H.S. (2019). Hukum Kontrak: Teori & Teknis Penyusunan Kontrak. Jakarta: Penerbit Sinar Grafika.
- [15.] Salim HS> 2021. Hukum Kontrak Elektronik E-Contract Law. Depok: Rajagrafindo. Indonesia.
- [16.] Samuels v. Lido Dao, No.23-cv-06492-VC, 2024 WL 4815022, at *4, *11, *12 (N.D. Cal. Nov. 18, 2024).
- [17.] Satjipto Rahardjo, Ilmu Hukum , Citra Aditya Bakti, Bandung, 2012;
- [18.] Shidarta, Refleksi tentang Struktur Ilmu Hukum , Mandar Maju, Bandung, 2006;
- [19.] Stuart Levi, et all. 2020. Legal issues surrounding the use of smart contracts, global legal insight : blockchain & cryptocurrenncy regulation second edition;
- [20.] Subekti, R. 2003. Pokok-Pokok Hukum Perdata, Jakarta: PT Intermasa;
- [21.] Sulistianingsih, D., & Kinanti, A. K. (2022). Hak Karya Cipta Non-Fungible Token (Nft) Dalam Sudut Pandang Hukum Hak Kekayaan Intelektual. Krtha Bhayangkara, 16(1), 197-206.
- [23.] Turk, Ž., & Klinc, R. (2017). Potentials of Blockchain Technology for Construction Management. doi: <https://doi.org/10.1016/j.proeng.2017.08.052>
- [24.] Uniform, T., Commission, L., Committee, E., & Note, G. (2019). The Uniform Law Commission Executive Committee approved the Guidance Note at its January 2019 midyear meeting.
- [25.] Vasiliki Papadouli, Vagelis Papakonstantinou, ‘A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs’, (2023), 51, Computer Law & Security Review.[9].
- [26.] Wax, S. (2021). A Primer on Non-Fungible Tokens and Smart Contracts. Lawyer Monthly. <https://www.lawyer-monthly.com/2021/05/a-primer-on-non-fungible-tokens-and-smart-contracts/>
- [27.] Yang, Shuo et al. Definition and Detection of Defects in NFT Smart Contracts. Proceedings of the 32nd ACM SIGSOFT International Symposium on Software Testing and Analysis, Seattle, WA, USA, Jul. 2023, pp. 373-384. <https://doi.org/10.1145/3597926.3598063>