LEGAL PROTECTION FOR LOSSES DUE TO BUGS IN SMART CONTRACTS IN TRADE PRACTICES THROUGH ELECTRONIC SYSTEMS

Yusuf Kornelius[1*)], Surahmad[2]
[1,2]Faculty of Law, Universitas Pembangunan Nasional “Veteran” Jakarta, South Jakarta, Indonesia
2110611112@mahasiswa.upnvj.ac.id[1*)], surahmad1970@gmail.com[2]

Received 28 April 2025 • Revised 17 May 2025 • Accepted 20 May 2025

Abstract

The rapid advancement of technology has significantly impacted various aspects of society, particularly in the field of trade conducted through electronic systems. One important innovation emerging from this development is the smart contract. However, alongside these advancements, new challenges have arisen, especially technical vulnerabilities that can occur at any time. Although smart contracts offer increased efficiency and security, they remain inherently susceptible to bugs. Therefore, this study aims to analyze the potential losses caused by bugs in smart contracts within electronic trading systems, as well as to examine how existing legal instruments protect parties harmed by such bugs. This research employs a normative legal methodology, utilizing statutory and conceptual approaches, and relies on secondary data obtained through a literature review. The findings indicate that bugs in smart contracts used in electronic trading can result in both material and immaterial losses for users. Furthermore, legal protection to mitigate such losses is supported by two main pillars: preventive protection and repressive protection, both of which are guaranteed under Indonesian positive law. Thus, the findings show that although Indonesia does not yet have specific legislation explicitly regulating smart contracts, legal protection for aggrieved parties is still available through the existing legal framework, including the Electronic Information and Transactions Law (UU ITE), the Consumer Protection Law (UU PK), Government Regulation on Electronic Systems and Transactions (PP PSTE), and Government Regulation on Trading Through Electronic Systems (PP PMSE) which collectively cover protection aspects in technology-based trade transactions.

Keywords: Bug, Electronic Trading System, Legal Protection, Smart Contract

INTRODUCTION

The rapid pace of technological advancements has significantly impacted various aspects of community life, particularly in trade conducted through electronic systems. One notable example of this technological innovation is the existence of smart contracts. Smart contracts are an advanced evolution of blockchain technology (Fahlevi & Fitriana, 2024). A smart contract is a software program that functions as a digital agreement within a blockchain database system, designed to implement protocols that enable the automatic execution of agreement clauses between the parties (Adhijoso, 2019). This concept was introduced by Nick Szabo, who described smart contracts as "...a computerized transaction protocol that executes the terms of a contract" (Cieplak & Leefatt, 2017). Consequently, smart contracts in electronic trade systems are considered an ideal solution to accelerate transaction processes due to their ability to reduce reliance on third parties (Frantz & Nowostawski, 2016).

To date, the development of smart contracts has shown a positive trend, with significant advancements and applications. Smart contracts have been widely utilized in transactions/trades of digital assets such as cryptocurrencies, non-fungible tokens (NFTs), and e-commerce systems (Tanumihardjo & Putra, 2022). According to data from DappRadar, 12,779 applications are operating 226,665 smart contracts, with 1.77 million daily active users (Pintu Academy, 2023). Additionally, blockchain platforms such as Cardano have recorded significant growth in implementing smart contracts. In January 2024, the number of smart contracts on the Cardano network increased by 67%, reaching 24,050 contracts (Fakhriani, 2024). These figures indicate that smart contracts are increasingly trusted as a primary instrument in electronic trade systems.

However, these developments also pose new challenges, particularly concerning technical issues that may arise at any time. While smart contracts promise enhanced efficiency and security, they are not without risks, particularly the risk of bugs. In electronic systems, a bug refers to an error, imperfection, or defect in the software code that causes the program to behave unexpectedly (Azhar & Rochimah, 2016). Several platforms, including Opensea, SushiSwap, and Solana, have experienced concrete examples of such bugs. These three cases resulted in total losses exceeding $25 million (Marcellova, 2024; Prasasti, 2022; Zela, 2024). Such incidents demonstrate that smart contract bugs can cause financial harm and infringe on user rights. Accordingly, bugs in smart contracts create new legal dilemmas, particularly concerning the legal certainty of protection for users engaging in electronic system-based trade.

In line with this, legal scholars have highlighted the challenges arising from the rapid advancement of technology, particularly in smart contracts. Bambang Pratama, Coordinator of the Information and Communication Technology Law Cluster at the Department of Business Law, Bina Nusantara University, in his article titled *"Legal Challenges in Facing ICT Innovation"*, emphasizes that legal polemics may arise if the rapid development of technologies such as smart contracts or blockchain is implemented without concrete legal instruments. He argues that legal regulations will continuously lag because technological products evolve in tandem with advancements in science and knowledge (Pratama, 2018). Therefore, in the context of smart contracts, legal protection is a key element that must be prioritized to ensure that users have legal certainty.

The urgency of legal protection is further reinforced by the guarantee provided in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states that "everyone shall have the right to the protection of themselves, their family, honor, dignity, and property under their possession." This principle aligns with the views of Philipus M. Hadjon in the Theory of Legal Protection, which emphasizes the importance of safeguarding human dignity, honor, and the fundamental rights of legal subjects (Wamafma et al., 2023). Therefore, the concept of protection within the context of smart contracts in trading through electronic systems becomes crucial, considering the risk of bugs caused by business actors' errors, which may lead to losses for parties engaging in such smart contracts.

In the context of the Indonesian legal system, smart contracts have received normative recognition through Law No. 19 of 2016, which amends Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Under this legal provision, smart contracts fall within the scope of "electronic contracts," as stated in Article 1 point (17), which defines an electronic contract as an agreement made by an electronic system. The electronic system itself, as defined in Article 1 point (5), refers to a set of electronic devices and procedures used to manage information. Based on this framework, smart contracts can be classified as legally valid agreements under Indonesia's positive law (Fahlevi & Fitriana, 2024). However, to date, smart contracts are not yet governed by specific technical regulations concerning protection against coding errors or bugs that may cause harm to one of the parties. When such risk results in loss, there is a pressing need for legal regulation that can ensure certainty of protection in the use of smart contracts within the electronic system trade.

Previous studies on smart contracts have not specifically addressed this issue. Gabriella Rachel Mansula (2023) highlights legal protection when transactions through smart contracts on the blockchain fail to function. Meanwhile, Hesti Ayu Wahyuni et al. (2023) discuss the application of smart contracts in e-commerce transactions from the perspective of Indonesian civil law. On the other hand, Maghfira Yuliza Fajryani (2023) focuses on legal certainty and protection for parties involved in self-executing smart contracts. However, none of these studies delve deeply into the losses caused by bugs in smart contracts or the formulation of legal protection for the parties when bugs disrupt the execution of contracts in trading through electronic systems. This indicates a research gap that requires further investigation.

This gap becomes increasingly relevant to examine, considering that coding errors in smart contracts can lead to transactional imperfections and may give rise to disputes (Giancaspro, 2017). Furthermore, bugs in smart contract code used in trading through electronic systems have the potential to cause failures in contract execution, which in turn may harm the parties involved (Christidis & Devetsikiotis, 2016). In some cases, the execution of a smart contract may not align with the intentions of either the seller or the buyer within the electronic system (Xu et al., 2016). Therefore, this study focuses on the use of smart contracts in trading through electronic systems practices, offering a new perspective by analyzing Government Regulation No. 80 of 2019 concerning Trade Through Electronic Systems (PP PMSE), which has not been addressed in the three studies.

Thus, the presence of bugs in smart contracts requires deeper examination, considering that transactional processes in trading through electronic systems are not merely agreements between two parties, but must also be grounded in legal principles that ensure fairness and certainty in transactions (Putri et al., 2024). Therefore, this research seeks to explore in more detail how potential losses may arise due to bugs in smart contracts and to describe the legal protection for parties in situations where bugs interfere with contract implementation. The results of this research will then be presented in the form of a scientific article titled “Legal Protection for Losses Due to Bugs in Smart Contracts in Trade Practices Through Electronic Systems”.

RESEARCH METHOD

This study employs a normative legal method with a statute approach and a conceptual approach. The statute approach is used to examine various legal provisions related to the topic of discussion, such as the Civil Code (KUHPerdata), the Electronic Information and Transactions Law (UU ITE), the Consumer Protection Law (UU PK), Government Regulation on Electronic Systems and Transactions (PP PSTE), and Government Regulation on Trading Through Electronic Systems (PP PMSE). Meanwhile, the conceptual approach is applied to analyze legal theories related to legal protection in smart contracts affected by bugs. These methods and approaches are utilized to analyze how written law applies in addressing issues of bugs, particularly in the context of smart contracts in trading through electronic systems. The study focuses on reviewing legal documents and existing theories to answer the formulated research questions.

This research centers on the potential losses caused by bugs in smart contracts and the legal protection available for the parties harmed. The data sources used are secondary data consisting of primary legal materials, including laws and government regulations. Secondary legal materials include books, legal journals, and research reports. Furthermore, tertiary legal materials encompass legal dictionaries, news, and other reference sources that support addressing the issues under study. The criteria for selecting literature and legal documents are based on their relevance to the legal issues being examined and the recency of data, focusing on materials published within the last five years. Data were collected through library research and analyzed using content analysis by examining the content systematically to gain a comprehensive understanding of the legal issues investigated (Nugraha, 2024).

RESULTS AND DISCUSSION

Losses Due to Bugs in Smart Contracts in Trade Practices Through Electronic Systems

In the concept of civil law, loss refers to the suffering experienced by a person as a result of the actions or negligence of another party. Such loss may arise from either a breach of contract or an unlawful act (tort). A breach of contract occurs when one party fails to fulfil its obligations as agreed upon in a contract. The regulations concerning breaches of contract are governed in Book III of the Indonesian Civil Code (KUHPerdata), specifically between Articles 1243 and 1252 (Muklis, 2023). Furthermore, an unlawful act (*Onrechtmatige daad*), as stipulated in Article 1365, refers to an act that, due to fault, causes harm to another party, in which case the party causing the harm is obliged to compensate for the resulting loss.

Furthermore, the types of losses can be classified based on the form of suffering experienced by the parties, namely material losses and immaterial losses. Material loss refers to tangible losses that can be quantified or measured, such as financial costs or damage to goods. In contrast, immaterial loss refers to losses that are difficult or impossible to measure financially, such as suffering from pain, emotional distress, reputational damage, or defamation (Febriansyah et al., 2024).

In a causal relationship, bugs in smart contracts can lead to losses, where such bugs represent errors or defects in the program code that cause the smart contract to fail to function as intended (Sayeed et al., 2020). One type of bug that can be found in trading through electronic systems is a logical error, namely an error in the program's logic that results in outcomes inconsistent with expectations (Buterin, 2014). Such bugs may arise from developers' negligence in writing the code or incorrect execution commands (Olickel, 2016).

The bug may also arise due to insufficient testing or security audits before deploying a smart contract. Such managerial failures can trigger undesired actions or create vulnerabilities that can be exploited by irresponsible actors, leading to suffering or losses borne by its users (Zhao et al., 2025). Depending on their impact, losses resulting from bugs in smart contracts can be classified into material and immaterial losses. Material losses caused by bugs in smart contracts include:

1. **Financial Losses Due to Information Mismatch**

   Bugs in smart contracts can lead to significant material losses for users of NFT trading platforms. One example is the OpenSea case. In late December 2021, a bug in the smart contract caused some users to sell their NFTs at prices far below market value. Rotem Yakir, a software developer, explained that the bug arose due to a discrepancy between the data in the NFT smart contract and the information provided by users on the OpenSea platform, which led to the failure of the smart contract to validate the sale price of the NFTs correctly. As a result, several NFTs were sold at prices lower than the market value, causing losses for the sellers, which were estimated to reach approximately $1 million (Prasasti, 2022).

2. **Loss of Assets Due to Theft**

   Malicious actors can also exploit bugs in smart contract security to commit theft. These vulnerabilities can be leveraged by ill-intentioned parties to transfer or deplete users' digital assets without authorization (Dwyer, 2020). An illustrative case occurred with SushiSwap in March 2024. ParaSwap launched a new smart contract called Augustus V6, which contained a security bug. This bug enabled unauthorized individuals to access and withdraw tokens and wallets without the rightful owner's consent. At least four user accounts were compromised, with total losses amounting to approximately $24,000 (Marcellova, 2024).

3. **Financial Losses Due to Transaction Failure**

   Bugs in smart contracts can also impede users' access to their assets. Bugs can cause discrepancies between the output and instructions, resulting in users' digital assets, such as token balances, being unable to be transferred, withdrawn, or used as intended. An example of a case that occurred is the Lido Staking case on Solana. On the Lido staking platform on the Solana network, a bug caused around $24 million worth of SOL to become locked. Users who had staked their tokens could not withdraw them because the smart contract failed to execute the function that allows the unstaking process (Zela, 2024).

In addition to material losses, bugs in smart contracts in trading through electronic systems can also bring immaterial losses. Immaterial losses experienced by users due to bugs in smart contracts may appear in the form of psychological distress. When there is a system failure that causes the loss of funds or assets, users may experience anxiety, frustration, and emotional distress, especially when the lost funds or assets have a significant value, which can affect the economic conditions for its users.

Losses due to bugs in smart contracts can create legal liability for developers and business actors involved, resulting from the concept of product liability. Product liability is a legal concept aimed at protecting consumers by freeing them from the obligation to prove errors in the production process that cause harm. This idea also emphasizes that business actors must bear responsibility for all losses caused by the products or services they produce (Shahira & Surahmad, 2022).

Legal Protection for Losses Due to Bugs in Smart Contracts in Trade Practices Through Electronic Systems

In principle, legal protection refers to the certainty or guidelines provided by legal instruments to ensure protection for legal subjects. Philipus M. Hadjon stated, "Legal protection refers to the recognition and respect for human rights, dignity, and worth possessed by legal subjects, which are protected by legal regulations to prevent arbitrary actions." Hadjon also classifies legal protection into two types, namely preventive and repressive protection (Wamafma et al., 2023). Furthermore, Soekanto also stated that legal protection aims to safeguard the rights of legal subjects by using legal instruments (Setiono, 2004).

In the context of smart contracts, parties with a self-executing mechanism must still be provided with legal protection, as errors/bugs in the programming algorithm structure are technically inevitable. This creates a need for a choice of law if it results in losses for the parties involved (Rachmadani & Rosadi, 2021). Therefore, legal protection for the parties using smart contracts on the blockchain network is necessary, and this will be explained by the author based on the theory of legal protection as follows:

1. **Preventive Legal Protection**

   Referring to the idea of Philipus M. Hadjon, legal protection in the form of prevention is a protective mechanism to minimize the potential for disputes in the future (Prayoga et al., 2023). Preventive legal protection is also intended to encourage caution in the decision-making process by legal subjects. The basis for preventive protection in the operation of smart contracts has been stated in Article 3, letters d and e of PP PMSE, which stipulates that "in conducting Electronic System Trading, the parties must adhere to the principles of trustworthiness and accountability." In this context, smart contract bugs violate the accountability and trust principles that business actors should uphold. Furthermore, preventive protection in smart contracts is also realized through the following mechanisms:

   a. **Security Standards in Electronic Systems**

      Preventive protection against losses due to bugs in smart contracts begins with electronic system operators' obligation to ensure their systems' security. Government Regulation on Electronic System and Transaction (PP PSTE), Article 8, stipulates that “Electronic System Operators must ensure that the software used meets the standards related to security and operational stability.” Furthermore, Article 13 of PP PSTE mandates that “every operator must have system governance, operational procedures, and a mechanism for regular audits.” Prevention efforts are also reinforced by the Reliability Certification mechanism as regulated in Articles 73 and 74 of PP PSTE. This certificate guarantees that the electronic system meets specific technical standards, including security-related ones. Article 21 letter e of PP PMSE even requires the organizers of trade through electronic systems to comply with technical requirements and possess such certifications. In the context of smart contracts, the system must be proven reliable before being utilized in transactions.

   b. **Supervision Efforts by the Government and Society**

      Supervision is important in preventing losses due to bugs in smart contracts. Based on Articles 76 and 78 of PP PMSE, the Minister has the authority to supervise and provide guidance to Electronic System Operators, including compliance with technical standards. This supervision includes evaluating business actors, both domestic and foreign, to minimize the negative impacts of cross-border digital transactions. The role of society is also recognized in Article 41 of the Electronic Information and Transactions Law (UU ITE), where the public can establish institutions that perform consultation and mediation functions related to the implementation of electronic systems. This mechanism opens up space for social supervision of system operators who are not transparent or negligent in maintaining the reliability of their platforms. This involvement is further reinforced by the Consumer Protection Law (UU PK) through Article 30, which provides opportunities for active public participation.

   The study results indicate that the legal system in Indonesia already contains legal instruments that can be utilized as preventive protection against bugs in smart contracts. This protection comes in the form of implementing security standards, such as periodic audits and system certification, as well as layered supervision from both the government and society. Although there are no explicit regulations specifically addressing bugs in smart contracts, the existing legal framework provides preventive protection through technical approaches and oversight of electronic system operations. The establishment of security standards and supervisory efforts is a crucial step in minimizing the negative impacts or losses that may arise from the risks of bugs in trading through electronic systems practices.

2. **Repressive Legal Protection**

   Repressive legal protection refers to the efforts made after a violation or loss. The purpose of this protection in the context of smart contracts is to impose sanctions or restore the rights of the party harmed by issues arising from digital transactions. Philip M. Hadjon states that repressive legal protection addresses disputes or problems that have already occurred (Tampubolon, 2016). Repressive legal protection is typically manifested through civil law mechanisms, where the affected party can file a lawsuit to obtain compensation for damages. This provision aligns with Article 72, paragraph (1) of PP PMSE, which states that trading through electronic systems transactions can be resolved through judicial proceedings or other alternative dispute resolution methods. Thus, there are several mechanisms for obtaining repressive protection when losses occur due to bugs in smart contracts, including:

a. **Litigation Mechanism**

One way to resolve smart contract disputes is through litigation in court. The court can make a decision that has legal consequences and is legally binding on all parties involved in the dispute. Article 72 paragraph (3) of PP PMSE stipulates that if the disputing party is a consumer, the consumer can file a lawsuit against the business actor through the Consumer Dispute Settlement Agency (BPSK) or bring the case to a court located in the consumer's jurisdiction. However, suppose the dispute involves an Indonesian consumer and a foreign business actor. In that case, the consumer can resolve the dispute through general courts based on the regulations in the field of consumer protection, as stipulated in Article 75, letter b of PP PMSE.

b. **Non-Litigation Mechanisms**

Furthermore, dispute resolution mechanisms outside of the judiciary, such as consultation, negotiation, conciliation, mediation, or arbitration, become alternative methods that can be used to resolve disputes related to smart contracts. Furthermore, through Article 72 paragraph (2) of PP PMSE, the government offers dispute resolution through ODR or Online Dispute Resolution (Barkatullah & Syahrida, 2019). ODR introduces a new concept of resolving disputes via the internet, which provides quick, efficient, and practical solutions (Chandra, 2014). The types of resolution offered by ODR features include online dispute resolution, online mediation, online negotiation, and online arbitration (Aziz & Hidayah, 2020).

The findings indicate that the Indonesian legal system also provides repressive legal protection for consumers who suffer losses due to bugs in smart contracts, which may be pursued through both litigation and non-litigation mechanisms. This form of protection includes dispute resolution through court proceedings by filing a legal claim, or through out-of-court forums such as the Consumer Dispute Settlement Agency (BPSK), as well as alternative means including mediation, arbitration, and Online Dispute Resolution (ODR). The existing legal framework grants consumers the right to claim compensation or hold the responsible party liable for any losses suffered, whether material or immaterial, as a form of legal protection against the adverse impacts or damages arising from the use of smart contracts in trading through electronic systems practices.

CONCLUSION

Bugs in smart contracts constitute coding errors that may result in losses for involved parties, both materially, such as asset and financial losses, and immaterially, including psychological distress. This condition highlights the importance of both preventive and repressive legal protections as a legal safeguard, particularly in the context of smart contracts used in trading through electronic systems. The current legal framework provides for such protections: preventive protection includes the obligation for electronic system operators to ensure system reliability by conducting regular code audits and supervising the practical use of smart contracts in trading through electronic systems. Meanwhile, repressive protection involves dispute resolution, either through litigation or alternative non-litigation methods such as consultation, negotiation, conciliation, mediation, arbitration, and Online Dispute Resolution (ODR).

These findings underscore the necessity for developers and electronic system operators to understand their legal obligations and to integrate consumer protection considerations from the design phase of smart contracts, in order to mitigate potential harm during implementation. Furthermore, considering that this technology is still relatively new, the public or users of smart contracts should be made aware of the importance of applying the precautionary principle before using smart contract technology to avoid unwanted risks. On the other hand, the government, as a policymaker, must continue to develop and adapt legal regulations to keep pace with the social changes brought about by technological advancement. In this regard, there is a pressing need for specific legal provisions governing smart contracts as part of a progressive legal development that aligns with technological innovation, ensuring their effective implementation within society.

ACKNOWLEDGMENTS

In writing this article, the author would like to express gratitude to the Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta, for providing the opportunity to present the results of this

analysis as an academic article. This gratitude is also dedicated to the supervising lecturers, Surahmad, S.H., M.H., as well as the author's colleagues who have provided support in preparing this academic article.

REFERENCES

Abel, F., Rachmadani, S., Sinta, D., & Rosadi, D. (2021). Tinjauan Yuridis Terhadap Perbuatan Melawan Hukum Pada Smart Contract Ditinjau Dari Hukum Positif Di Indonesia. *Jurnal Sains Sosio Humaniora P-ISSN*, *5*, 2580–1244.

Adhijoso, B. D. (2019). Legalitas Penerapan Smart Contract Dalam Asuransi Pertanian di Indonesia. *Jurist-Diction*, *2*(2), 395–414.

Azhar, N. F., & Rochimah, S. (2016). Memprediksi Waktu Memperbaiki Bug dari Laporan Bug Menggunakan Klasifikasi Random Forest. *Jurnal Sistem dan Informatika*, *11*(1), 156–164. http://www.jsi.stikom-bali.ac.id/index.php/jsi/article/view/99%0Ahttps://www.jsi.stikom-bali.ac.id/index.php/jsi/article/download/99/101.

Aziz, M. F., & Hidayah, M. A. (2020). Perlunya Pengaturan Khusus Online Dispute Resolution (Odr) Di Indonesia Untuk Fasilitasi Penyelesaian Sengketa E-Commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 275.

Barkatullah, A. H. & Syahrida. (2019). *Sengketa Transaksi E-Commerce Internasional: Pengertian, Sebab Kemunculan, dan Cara Penyelesaian*. Banjarmasin: Fakultas Hukum Universitas Lambung Mangkurat Press.

Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. *Whitepaper*, 1–36. https://ethereum.org/en/whitepaper.

Chandra, A. (2014). Penyelesaian Sengketa Perdagangan melalui sistem elektronik Melalui Online Dispute Resolution (ODR) Kaitan Dengan UU Informasi Dan Perdagangan melalui sistem elektronik no . 11 tahun 2008. *Jurnal Ilmu Komputer*, *10*(2), 80–89.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*, 2292–2303.

Cieplak, J., & Leefatt, S. (2017). Smart Contracts: A Smart Way to Automate Performance. *Georgetown Law Technology Review*, *1:2*, 417–427.

Dwyer, K. (2020, September 26). *Batasan penggunaan smart contracts*. EMURGO. https://www.emurgo.io/press-news/apa-itu-smart-contracts-part2/

Fahlevi, S., F., & Fitriana, M., Z. (2024). Keabsahan Smart Contract Sebagai Solusi Penyelenggaraan Manipulasi Kontrak Di Indonesia. *Kabillah: Journal of Social Community*, *9*(14), 243–255.

Fajryani, M. Y. (2023). *Kepastian Hukum Eksistensi Self-executing dan Perlindungan Hukum bagi Para Pihak Pada Smart Contract dalam Jaringan Blockchain* (Doctoral dissertation). Universitas Islam Indonesia.

Fakhriani, Z. (2024, Januari 25). *Jumlah Smart Contract di Jaringan Cardano Naik 67% selama Januari 2024*. BeinCrypto Indonesia. https://id.beincrypto.com/jumlah-smart-contract-di-jaringan-cardano-ada-naik-67-persen-januari-2024/

Febriansyah, R., Kurniawan, Z. A., Syahladin, F. R., & Amanda, G. (2024). Perbuatan Melawan Hukum (PMH) Sebagai Perikatan Yang Lahir Karena Undang-Undang: Implikasi Terhadap Penentuan Ganti Rugi. *Media Hukum Indonesia*, *2*(4), 597–604.

Filippi, D. P. (2018). *Blockchain & the Law: The Rule of Code*. Cambridge: Harvard University Press.

Frantz, C. K., & Nowostawski, M. (2016). From institutions to code: Towards automated generation of smart contracts. *Proceedings - IEEE 1st International Workshops on Foundations and Applications of Self-Systems, FAS-W 2016*, (September 2016), 210–215.

Giancaspro, M. (2017). Is a ‘smart contract’ really a smart idea? Insights from a legal perspective. *Computer Law and Security Review*, *33*(6), 825–835.

Kurniawan. (2011). *Hukum Perlindungan Konsumen (Problematika Kedudukan Dan Kekuatan Putusan Badan Penyelesaian Sengketa Konsumen (BPSK))*. Malang: UB Press.

Marcellova, K. (2024, Maret 26). *Kebocoran Besar di Dunia Crypto: ParaSwap Berhasil Pulihkan Dana Pengguna!*. Pintu News. https://pintu.co.id/news/78254-paraswap-pulihkan-dana-setelah-kebocoran-kontrak-pintar

Muklis. (2023). Analisis Ganti Kerugian Berdasarkan Perspektif Hukum Perdata. *Iuris Studia: Jurnal Kajian Hukum*, *4*(1), 6–10. http://jurnal.bundamediagrup.co.id/index.php/iuris/article/view/326

Nugraha, S. (2024). *Metode Penelitian Hukum*. Banjar: Ruang Karya.

Olickel, H. (2016, June 21). *Why smart contracts fail: Undiscovered bugs and what we can do about them*. Medium. https://hrishiolickel.medium.com/why-smart-contracts-fail-undiscovered-bugs-and-what-we-can-do-about-them-119aa2843007

Pemerintah Republik Indonesia. (1999). *Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen* [Law of the Republic of Indonesia Number 8 of 1999 concerning Consumer Protection]. *Lembaran Negara Republik Indonesia Tahun 1999 Nomor 20*, *Tambahan Lembaran Negara Republik Indonesia Nomor 3821*.

Pemerintah Republik Indonesia. (2008). *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* [Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions]. *Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58*, *Tambahan Lembaran Negara Republik Indonesia Nomor 4843*.

Pemerintah Republik Indonesia. (2019a). *Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik* [Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions]. *Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185*, *Tambahan Lembaran Negara Republik Indonesia Nomor 6400*.

Pemerintah Republik Indonesia. (2019b). *Peraturan Pemerintah Republik Indonesia Nomor 80 Tahun 2019 tentang Perdagangan Melalui Sistem Elektronik* [Government Regulation of the Republic of Indonesia Number 80 of 2019 concerning Trade through Electronic Systems]. *Lembaran Negara Republik Indonesia Tahun 2019 Nomor 222*, *Tambahan Lembaran Negara Republik Indonesia Nomor 6420*.

Pintu Academy. (2022, November 25). *Mengenal Teknologi Smart Contract*. Pintu Academy. https://pintu.co.id/academy/post/apa-itu-dapps-dan-smart-contract

Prasasti, G. D. (2022, Januari 26). *Ada bug di OpenSea, bikin NFT bisa dibeli jauh lebih murah*. Liputan6.com. https://www.liputan6.com/tekno/read/4869939/ada-bug-di-opensea-bikin-nft-bisa-dibeli-jauh-lebih-murah

Prayoga, D. A., Husodo, J. A., Elok, A., & Maharani, P. (2023). Perlindungan Hukum Terhadap Hak Warga Negara Dengan Berlakunya Undang-Undang Nomor 23 Tahun 2019 Tentang Pengelolaan Sumber Daya Nasional. *Souvereignty : Jurnal Demokrasi dan Ketahanan Nasional*, *2*(2), 188–200. https://journal.uns.ac.id/Souvereignty/article/view/865.

Putri, A. S., Kirani, M., Sadi, M. F., & Setiawan, R. Q. (2024). Analisis Kewajiban dan Perlindungan Konsumen Dalam Kontrak Jual Beli. *Media Hukum Indonesia (MHI)*, *2*(4), 505–514.

Safira, V. (2021, Maret 26). *Keabsahan Smart Contract Sebagai Perjanjian yang Mengikat Para Pihak*. HK & Associates Law Office. https://hkalawoffice.com/keabsahan-smart-contract-sebagai-perjanjian-yang-mengikat-para-pihak/

Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020). Smart Contract: Attacks and Protections. *IEEE Access*, *8*, 24416–24427.

Setiono. (2004). *Rule of Law (Supremasi Hukum)*. Surakarta: Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret.

Shahira, R., & Surahmad. (2023). Perlindungan Konsumen Dalam Jual Beli Properti (Studi Kasus PT Developer Properti Indoland). *Al-Mashlahah Jurnal Hukum Islam dan Pranata Sosial*, *10*(001 SE-Articles). https://jurnal.staialhidayahbogor.ac.id/index.php/am/article/view/3585.

Tampubolon, S. W. (2016). Upaya Perlindungan Hukum Bagi Konsumen Ditinjau Dari Undang Undang Perlindungan Konsumen. *Jurnal Ilmiah Advokasi*, *4*(1), 684–686.

Tanumihardjo, G. K., & Putra, A. P. M. (2022). Penggunaan Smart Contract Di Indonesia. *Jurnal Kertha Wicara*, *11*(2), 437–447.

Wamafma, F. et al. (2024). *Perlindungan Hukum Bagi Konsumen Dalam Transaksi E-Commerce*. Banyumas: Amerta Media.

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain as a software connector. *Proceedings - 2016 13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016*, (April), 182–191.

Zela, D. (2024, April 4). *Terjebak di Lido: $24 juta SOL kandas karena bug smart contract!* Pintu. https://pintu.co.id/news/79905-24juta-sol-bug-smart-contract

Zhao, B., Lin, X., Tian, Y., Zonouz, S., Ruan, N., Li, J., Beyah, R., & Ji, S. (2025). Detecting Functional Bugs in Smart Contracts through LLM-Powered and Bug-Oriented Composite Analysis. *arXiv preprint arXiv:2503.23718*.