Krisnadwipayana University, Jakarta, Indonesia | 2715-243X (Print), 2962-6226 (Online)

JUSTICE Voice

Vol. 4 | No. 2 | 2025 | pp. 83-93
https://doi.org/10.37893/jv.v4i2.1204

Legal Protection for Consumers Who Lose Assets on Crypto Exchange Platforms in Indonesia: A Case Study of Hacking and Rug Pull

Dominic Imanuel Vidianto [a], Aloysius Mardiana [a], Nurul Hikmah [a], Aliif Ahmad Akbar [a,*]

[a] *Brawijaya University, Malang, Indonesia*

Keywords:

Cryptocurrency; Hacking; Rug Pull; Transaction.

Abstract: This study analyzes legal protection for consumers who experience asset loss on crypto exchange platforms in Indonesia, focusing on two main issues: hacking and rug pull practices. The study examines existing regulations, such as the Electronic Information and Transactions Law (ITE Law) and the Financial Services Authority Regulation (POJK), and reviews two specific cases: hacking of the Indodax platform and rug pull of the ASIX token. The research method used is normative juridical, with a statutory and conceptual approach. The results of the study show that although these regulations exist, the implementation of legal protection remains weak, particularly in terms of security system supervision and the accountability mechanisms of platform providers. Therefore, this study recommends strengthening cybersecurity standards and applying stricter accountability principles by crypto platform providers. There is also a need for synchronization between existing regulations and increased consumer digital literacy to minimize risks arising from illegal practices in this sector.

Article history:

Submitted : 2025-06-18
Accepted : 2025-09-02
Available online : 2025-12-31

How to cited: Vidianto, D. I., Mardiana, A., Hikmah, N., & Akbar, A. A. (2025). Legal Protection for Consumers Who Lose Assets on Crypto Exchange Platforms in Indonesia: A Case Study of Hacking and Rug Pull. *Justice Voice, 4*(2), 83–93. https://doi.org/10.37893/jv.v4i2.1204

Introduction

Cryptocurrency has become a significant innovation in the digital financial sector, facilitating cross-border transactions and decentralizing the financial system. However, legal protection for consumers involved in digital transactions through crypto exchange platforms in Indonesia remains limited, particularly concerning the risk of asset loss caused by hacking or fraudulent practices such as rug pull. This issue is becoming increasingly urgent given the high volume of crypto transactions and the lack of clarity regarding existing legal protection mechanisms (Yudistira & Yustiawan, 2025).

* ✉ corresponding author: aliifahmadakbar@student.ub.ac.id

Rug pull is a term used in the cryptocurrency world to describe a fraudulent action carried out by developers or parties involved in a crypto project. In this scenario, the developers or project owners suddenly withdraw all the funds raised from investors or users, leaving the project without further development. As a result, investors or participants in the project suffer significant financial losses (Saha Roy et al., 2024).

This practice often occurs in unregistered or unclear cryptocurrency projects, such as newly launched tokens, where developers can raise funds from investors without having to provide clear guarantees. Rug pull can occur in various types of crypto projects, such as Initial Coin Offerings (ICO), Decentralized Finance (DeFi), or tokens traded on exchanges.

The issue of responsibility for exchange platforms or cryptocurrency trading platforms has become increasingly important to address, in line with the growing popularity of cryptocurrency among the Indonesian public. According to data from BAPPEBTI, the transaction volume of cryptocurrency in Indonesia continues to show an upward trend. However, the aspect of legal protection for users still raises various questions. In practice, consumers are often faced with agreements containing standard clauses that are more favorable to platform providers, without adequate explanation regarding the compensation mechanism in the event of asset loss due to system errors or administrative negligence. This situation underscores the need for an in-depth study of the legal responsibility of crypto exchange platforms to ensure fair and balanced consumer rights protection (Yudistira & Yustiawan, 2025).

In Indonesia, crypto assets such as Bitcoin, Dogecoin, Ripple, and Litecoin are classified as virtual currencies (Siregar, 2025). According to Bank Indonesia Regulation Number 23/6/PBI/2021 on Payment Service Providers, virtual currencies have several characteristics, including: being a form of digital money issued by non-monetary authority entities, having a certain unit, utilizing cryptography technology and distributed ledger, and being used for payments or supporting economic activities. Although some types of cryptocurrency can be utilized in the economic context, it is important to emphasize that in Indonesia, the only legal payment instrument is the rupiah (Yudistira & Yustiawan, 2025).

The cryptocurrency industry has faced various emerging security incidents. One significant example is the hacking of Binance, the world's largest cryptocurrency exchange platform originating from China, which on May 7, 2019, reported the loss of over 7,000 Bitcoins, worth approximately 40 million USD. The perpetrators used advanced methods such as phishing, malware, and the exploitation of user APIs to carry out their actions. In Indonesia, a similar incident occurred in September 2024, when Indodax, the largest cryptocurrency exchange in the country managed by PT Indodax Nasional Indonesia, experienced a cyber attack

that exploited security vulnerabilities in their system. Based on this background, the author is motivated to examine the legal protection aspects for consumers who experience asset loss due to hacking on cryptocurrency exchange platforms in Indonesia. (Yudistira & Yustiawan, 2025).

Methods

This research uses a normative juridical method to analyze legal protection for consumers who lose assets on crypto exchange platforms in Indonesia. A legislative approach is employed to examine regulations governing the cryptocurrency sector and consumer protection, such as the ITE Law, POJK, and Bank Indonesia regulations related to virtual currencies. Additionally, a conceptual approach is applied to explore legal theories on the platform operators' responsibility, cybersecurity, and fraudulent practices, such as rug pull.

Data was obtained through a literature review that includes legislation, journal articles, and related case reports, such as the hacking incident on the Indodax platform and the ASIX token rug pull case. This case study provides a concrete overview of the challenges faced by consumers and the weaknesses in the existing regulations.

The analysis is conducted using a normative approach to evaluate whether existing regulations sufficiently protect consumers and how the law governs the responsibilities of platform operators. A conceptual approach is used to understand the application of legal principles related to responsibility in digital transactions.

Results and Discussion

Case Analysis on the Loss of Consumer Assets in Crypto Exchange

The trading of cryptocurrency in Indonesia has grown rapidly, in line with the increasing public participation in digital investment. One of the platforms with a dominant position in this industry is PT Indodax Nasional Indonesia (Indodax). Although Indodax is registered with the Commodity Futures Trading Regulatory Agency (BAPPEBTI) and subject to regulations as an Electronic System Organizer (PSE), the alleged hacking of user accounts in 2024 revealed significant gaps in legal protection for consumers within the cryptocurrency ecosystem. In September 2024, PT Indodax Nasional Indonesia, one of the largest cryptocurrency trading platforms in Indonesia, suffered a major cyberattack, resulting in an estimated loss of around USD 22 million, or approximately IDR 280 billion. This incident is considered one of the most significant hacking cases in the history of cryptocurrency exchanges in Indonesia, not only due to the value of the losses but also because of the sophisticated social engineering methods involved in the attack (Rafie, 2024).

The cyberattack began with a modus operandi known as the 'dream job scam,' a psychological manipulation technique in which the perpetrator masquerades as a company offering high-paying jobs to an internal engineer at Indodax. During this process, the victim is asked to download and open a file claimed to be a recruitment document. The file, however, contained malware designed to exploit system vulnerabilities. Unfortunately, the device used by the engineer was a personal laptop, also used for office work, which was connected to Indodax's internal infrastructure. The malware successfully infiltrated the internal network and gradually exploited security gaps, ultimately gaining access to the main server and the hot wallet, a digital wallet used to store liquid crypto assets. Early signs of this suspicious activity were detected on September 11, 2024, by several international cybersecurity companies, including Cyvers, PeckShield, and SlowMist, which actively monitor blockchain traffic for abnormal activities. They reported significant and unusual movements of various crypto assets transferred to anonymous addresses. The stolen assets included a large amount of Bitcoin (BTC), Ethereum (ETH), TRON (TRX), Polygon (MATIC), and various other ERC-20 tokens. In response to the incident, Indodax immediately halted operational activities, suspended the withdrawal and deposit processes for digital assets, and conducted an internal audit of the security system. System recovery was successfully completed within 80 hours, and Indodax claimed that no customer funds were lost, as the company's reserve funds were used to replace the stolen assets.

Based on the results of the initial investigation and analysis of the attack patterns, it is strongly suspected that the perpetrators of this attack are the infamous North Korean hacking group, Lazarus Group, which has also been linked to various high-value digital asset theft incidents across several countries. The attack techniques and malware used show significant similarities with previous attacks traced to this group (Reddy, 2025). This hacking incident serves as a stern warning for the digital asset industry in Indonesia regarding the importance of internal risk management, the safeguarding of information technology infrastructure, and the control of personal device usage for work purposes (BYOD – Bring Your Own Device), especially in the highly vulnerable digital financial sector. From a legal perspective, this case raises an important discourse on corporate legal responsibility in maintaining the security of electronic systems, including in the context of the Information and Electronic Transactions Law, Consumer Protection, and Personal Data Protection.

From the perspective of criminal law, the act of account takeover without authorization is classified as an illegal access crime as stipulated in Article 30 paragraph (1) of Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE Law) jo. Law No. 19 of 2016, which states that: "Any person intentionally and without authorization or unlawfully accesses a computer and/or

electronic system belonging to another person by any means." This provision is reinforced by Article 46 paragraph (1) of the ITE Law, which imposes a criminal penalty of up to 6 years imprisonment and/or a fine of up to IDR 600,000,000.

The legal relationship between users and Indodax is contractual and is governed by the principle of freedom of contract as stipulated in Article 1338 of the Indonesian Civil Code (*KUH Perdata*). If Indodax fails to fulfill its obligation to protect the security of users' assets and data, this can be considered a breach of contract. In the context of tort, Article 1365 of the Civil Code states that: "Every act that violates the law and causes harm to another person obliges the person who, due to their fault, causes the loss to compensate for the damage." (Subekti & Tjitrosudibio, 2017)

As a digital business entity, Indodax is required to comply with the provisions of Article 7 letter f of Law No. 8 of 1999 on Consumer Protection, which mandates compensation to consumers for losses resulting from services that do not meet the agreed terms. Law No. 27 of 2022 on Personal Data Protection also stipulates, in Article 51 paragraph (1), that any person who, due to negligence, causes personal data to be accessed unlawfully and results in damage, may be subject to administrative sanctions.

In the doctrine of civil law, the principle of strict liability is recognized, which places the responsibility on digital business operators for consumer losses without the need to prove fault. This principle aligns with the doctrine of *res ipsa loquitur*, which holds that the loss is caused by the negligence of the system itself. As explained by Subekti, a contract not only covers what is written but also what is deemed appropriate according to decency, customs, and law (Andhika, 2023). Based on the above explanation, it can be concluded that the alleged hacking of the Indosat account indicates the need for clearer technical regulations concerning the responsibility of electronic system operators (PSE), particularly regarding minimum cybersecurity standards. Synchronization between the ITE Law, PDP Law, and the Consumer Protection Law must be carried out to strengthen the legal position of consumers in digital asset transactions.

One example of a domestic cryptocurrency asset that has encountered significant issues is the ASIX token, which is a cryptocurrency product owned by public figure Anang Hermansyah. This token was first traded on March 3, 2022, at a launch price of IDR 69 per token. However, based on data as of July 5, 2023, the value of the ASIX token has drastically decreased by more than 100% from its initial value. Referring to data collected from the cryptocurrency asset tracking site CoinGecko, it was recorded that the price of the ASIX token reached only IDR 0,00009131, with a trading volume of IDR 0 on that date. This situation reflects that the ASIX token has lost its liquidity and functionality in the market, and thus, technically can be classified as an inactive asset or even one that has completely lost its value (Ali et al., 2023).

Over time, the ASIX token showed strong indications that the project contains elements of a 'rug pull', a fraudulent practice in cryptocurrency projects where developers suddenly withdraw support or funds from the project, causing harm to investors. In June 2022, Indodax, one of the cryptocurrency exchanges in Indonesia, reported that the value of the ASIX token had drastically dropped to IDR 6, from its initial price of IDR 69 when it was first traded. This sharp decline led to a perception among the public, particularly early investors, that they had become victims of manipulation (Bestari, 2022). The numerous complaints regarding these alleged losses came not only from a few individuals but also from a large number of users who had participated since the initial launch of the token. Many investors subsequently demanded accountability from the token's development team, particularly Anang Hermansyah as the public figure and main owner of the project. This situation further strengthened the perception within the cryptocurrency community that the ASIX token was suspected to be part of a 'rug pull' scheme, given the lack of transparency and the significant value drop without clear justification (Afani, 2022).

In the case of the ASIX crypto token developed by Anang Hermansyah, the project demonstrates a discrepancy between the initial plans or promises made by the developers to potential investors and the reality of its implementation. The unmet targets and the lack of significant progress in the development of the ASIX project further strengthen the perception that this initiative has stagnated or has even been de facto abandoned by its developers. This creates uncertainty and significant risk for investors (Ali et al., 2023), making the ASIX coin appear as a crypto scam scheme, where the developers only aim to attract funds from investors and then abandon the project.

Rug pull, defined as the sudden withdrawal of funds by developers or project owners in the cryptocurrency space, can create significant financial losses and harm the integrity of the financial market (Ali et al., 2023). Rug pull can be categorized as an unlawful act (Article 1365 of the Indonesian Civil Code) as it meets the required elements. First, there is a fault in the form of deliberate actions that mislead investors with false information or unfulfilled promises. Second, there is a real loss suffered by investors who lose their invested funds. Third, there is a direct cause-and-effect relationship between the perpetrator's actions and the loss suffered by the victim. In this context, the perpetrator of the rug pull can be sued for compensation to the harmed investors, including material losses and potential immaterial losses such as stress and financial trauma. Furthermore, if there is an agreement or smart contract between the developer and the investor, a rug pull can be categorized as a breach of contract (Articles 1238-1243 of the Civil Code). Developers who commit a rug pull essentially fail to fulfill the promises made, whether it concerns project development, token distribution, or long-term commitments outlined in the project's whitepaper or roadmap.

The primary essence of the existence of the Electronic Information and Transactions Law (EIT Law) is to provide legal protection for consumers in the digital space. Therefore, the provisions in the EIT Law can still be used as a basis to hold perpetrators accountable in cases of rug pull occurring in cryptocurrency asset trading activities, even though the EIT Law does not explicitly regulate crimes related to cryptocurrency. Thus, Article 28 paragraph (1) of the EIT Law can be positioned as *lex specialis*, overriding Article 378 of the Penal Code (*lex generalis*) in the case of fraud, and can be used to prosecute online fraud perpetrators, including actions classified as rug pull practices (Ali et al., 2023).

The phenomenon of rug pull within the cryptocurrency ecosystem introduces a new layer of complexity to the legal system in Indonesia. Although, in a normative sense, provisions in civil law can serve as the basis for holding parties accountable, the effectiveness of their application is still hindered by various technical and juridical issues, including the absence of a comprehensive and specific regulatory framework. In this context, optimal legal protection can only be achieved through the synergy of enhancing investor literacy and vigilance, the creation of holistic regulations, and strengthening the capacity of law enforcement institutions to address the ever-evolving challenges of digital law. A holistic approach involving all stakeholders is necessary to create a safe and trustworthy cryptocurrency ecosystem.

Forms of Legal Protection for Consumers Who Lose Assets on Crypto Exchange Platforms

Cryptocurrency, as one of the financial innovations in the financial sector, facilitates cross-border transactions and the decentralization of the financial system. In Indonesia, digital currencies such as Bitcoin, Dogecoin, Ripple, and Litecoin are classified as virtual currencies (Siregar, 2025). According to Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment Service Providers, virtual currencies possess several distinct characteristics. These digital currencies are issued by entities outside the monetary authority and are represented in specific units, utilizing distributed ledger technology, and are used for payments or economic activities. However, the use of cryptocurrency also presents its own set of challenges, particularly concerning legal protection. Crypto exchange platforms serve as the primary intermediaries in digital asset transactions. Nevertheless, the relationship between users and platforms is often asymmetric, both in terms of access to information and the bargaining power of users as consumers. This imbalance puts consumers in a vulnerable position, exposed to various risks, including the potential loss of assets. In practice, users are often required to agree to standard clauses in service agreements, which are typically more advantageous to the platform provider. Unfortunately, these agreements often do not include clear mechanisms for compensation in the event of asset loss due to system errors or negligence on the part of the service provider.

The fundamental essence of legal protection lies in how protection is provided for the dignity, honor, and recognition of human rights (HR) inherent in legal subjects within a rule-of-law state. This protection must be based on applicable laws and regulations to prevent arbitrariness, thus leading to the conclusion that law serves the function of protecting human interests. Through BAPPEBTI, Indonesia has classified cryptocurrency assets as commodities, which are regulated under BAPPEBTI Regulation No. 5 of 2019 on the Technical Provisions for the Organization of Physical Crypto Assets Markets on Futures Exchanges. Initially, the supervision of cryptocurrency assets was carried out by BAPPEBTI (Hidayat & Sebyar, 2024).

However, since the enactment of Law Number 4 of 2023 on the Development and Strengthening of the Financial Sector (hereinafter referred to as Law 4/2023), the oversight of cryptocurrencies has been transferred to the Financial Services Authority (OJK). Following this transfer, OJK then comprehensively regulated cryptocurrencies in the Financial Services Authority Regulation Number 27 of 2024 on the Organization of Digital Financial Asset Trading (POJK 27/2024). The scope of the regulation in this POJK includes the parties involved in cryptocurrency transactions, the buying and selling mechanisms, oversight, rights and obligations, criteria for digital financial assets, the duties and authorities of the relevant institutions, and the forms of administrative sanctions. In POJK 27/2024, preventive protection can be seen in the regulation of the criteria for cryptocurrency assets, both in general (Article 4) and specifically (Article 8). The purpose of regulating these criteria is to ensure the quality of traded digital financial assets and cryptocurrencies, as well as to protect consumers from cryptocurrencies that are high-risk or even illegal.

In the regulation of crypto transactions, this repressive protection can be seen in the Financial Services Authority Regulation Number 22 of 2023 on Consumer and Public Protection in the Financial Services Sector (POJK 22/2023). The scope of this regulation includes the obligations of Financial Services Business Actors (PUJK), the rights and obligations of consumers, complaint mechanisms, as well as sanctions and supervision. As a form of consumer protection, the provisions in POJK 22/2023 can be found in Article 10, paragraph (1), which states:

> "PUJK shall be liable for consumer losses caused by errors, negligence, and acts that contravene the provisions of laws and regulations in the financial services sector and/or agreements, whether committed by the Board of Directors, Board of Commissioners, Employees, or by third parties representing or working for the benefit of the PUJK."

Based on the provisions in the article, it can be understood that Financial Services Business Actors (PUJK) are obligated to be responsible for losses suffered by consumers, whether arising from mistakes, negligence, or actions that violate laws and regulations in the financial services sector and/or agreements. Although the form of

this liability is not explained in detail in the article, an explanation can be found in the Explanation of Article 10, paragraph (1), which states that the PUJK's responsibility for consumer losses may be realized in the form of compensation. Furthermore, the regulation regarding crypto exchanges is also addressed in POJK 27/2024.

In this context, exchanges are conducted by business entities acting as traders, which are business organizations that engage in trading or buying and selling digital financial assets, either in their own name or in their capacity as facilitators for the benefit of consumers. In facilitating these transactions, traders inevitably store the assets being traded on behalf of the consumers. Article 85 paragraph (1) letter b of POJK 27/2024 stipulates that, essentially, when consumers engage in buying and selling assets, they must first place the assets being used into a wallet owned by the trader. However, this regulation does not prevent the possibility of asset loss due to actions by the trader that violate the provisions of the applicable laws and regulations. Regarding the issue of consumer asset loss, this is explicitly regulated in Article 91 paragraph (1) of POJK 27/2024, which states: "Traders must ensure security and are responsible for any loss of Digital Financial Assets owned by Consumers that are stored by the Trader."

The provision of the article mentions the obligation of traders to be responsible if the consumer's assets stored by the trader are lost. Furthermore, according to Article 139, paragraph (1) of POJK 27/2024, which states:

> "Digital Asset Trading Organizers must comply with the following provisions: a) Governance; b) Personal data protection; and c) Consumer protection, within a period of 6 (six) months from the enactment of this Financial Services Authority Regulation."

This article regulates the obligation of organizers concerning consumer protection. Based on the provision of this article, the consumer protection regulation refers to the provisions in POJK 20/2023, which states that the form of accountability for consumers who lose assets due to the crypto exchange activities is by providing compensation.

Conclusion

The shift in the oversight of cryptocurrency assets in Indonesia, which was previously under BAPPEBTI and has now been transferred to the Financial Services Authority (OJK) through Law No. 4 of 2023, has significant implications for regulation and consumer protection in the digital asset trading sector. Further provisions in POJK Number 27 of 2024 and POJK Number 22 of 2023 clarify the responsibilities of operators in safeguarding assets and protecting consumer rights. These two regulations outline the obligation to compensate consumers who suffer losses due to negligence or legal violations by platform operators, providing a stronger legal foundation for consumers involved in digital asset transactions.

The hacking incident on the Indodax platform and the alleged rug pull on the ASIX token highlight two dangerous aspects of vulnerabilities in the cryptocurrency trading ecosystem in Indonesia. The hacking incident at Indodax, which involved advanced social engineering techniques, underscores the importance of implementing stricter cybersecurity standards by cryptocurrency platform operators. This case also demonstrates the need for better system security and more diligent internal risk management in an industry vulnerable to cyberattacks. Additionally, the use of personal devices for work-related purposes (BYOD) must be strictly regulated to prevent potential illegal access to internal systems.

Meanwhile, the ASIX case highlights the weaknesses of regulations concerning domestic crypto projects, which are vulnerable to rug pull practices, where developers suddenly withdraw funds or cease project development. The drastic decline in token value, coupled with the lack of transparency and accountability from developers, underscores the need for stricter oversight of local crypto projects. Without clear regulations and firm implementation, consumers become highly vulnerable to such fraudulent schemes.

To ensure optimal legal protection for consumers, the crypto asset trading sector requires a more comprehensive and integrated approach. In addition to enhancing digital literacy for consumers, there needs to be stronger regulation covering more detailed cybersecurity standards, more effective oversight, and clear compensation mechanisms for consumers harmed by the negligence of operators. As a recommendation, there should be alignment between regulations related to the Personal Data Protection Act (PDP Law), consumer protection regulations, and the Information and Electronic Transactions Law (ITE Law), in order to create a safe and transparent ecosystem in the crypto sector. Moving forward, strengthening the capacity of law enforcement in addressing digital legal challenges will be crucial to prevent illegal practices and enhance consumer trust in crypto exchange platforms in Indonesia.

References

Afani, A. (2022). Anang Hermansyah Diminta Tanggung Jawab oleh Investor karena Harga Token Asix Anjlok. *haibunda.com*. https://www.haibunda.com/trending/20220323185610-93-269716/anang-hermansyah-diminta-tanggung-jawab-oleh-investor-karena-harga-token-asix-anjlok

Ali, M. F., Imran, S. Y., & Apripari, A. (2023). Penegakan Hukum Pidana Terhadap Praktek Rugpull Ditinjau dari Hukum Positif Indonesia. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *1*(4), 317–328. https://journal.stekom.ac.id/index.php/Hakim/article/view/1478

Andhika, A. (2023). Kelemahan Regulasi Perlindungan Konsumen di Platform Digital. *Jurnal Hukum & Teknologi*, *8*(1), 89–105.

Bestari, N. P. (2022). Gimana Nih Mas Anang Hermansyah, Nasib Token Kripto ASIX? *CNBC Indonesia*. https://www.cnbcindonesia.com/tech/20220607094521-37-344872/gimana-nih-mas-anang-hermansyah-nasib-token-kripto-asix

Hidayat, B. D., & Sebyar, M. H. (2024). Implikasi Hukum Perpindahan Pengawasan Aset Kripto dari Bappebti ke OJK terhadap Pelaku Industri dan Investor: (A Comparative Study). *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 888–899. https://journal.stekom.ac.id/index.php/Hakim/article/view/2206

Rafie, B. T. (2024). Indodax Diretas dengan Kerugian Capai Rp 280 Miliar, Pelaku Diduga Hacker Korea Utara. *Kontan.Co.Id*. https://internasional.kontan.co.id/news/indodax-diretas-dengan-kerugian-capai-rp-280-miliar-pelaku-diduga-hacker-korea-utara

Reddy, S. (2025). North Korea's Lazarus Group Linked to $11.5M theft from Taiwan Crypto Exchange. *Nknews.Org*. https://www.nknews.org/2025/06/north-koreas-lazarus-group-linked-to-11-5m-theft-from-taiwan-crypto-exchange/

Saha Roy, S., Das, D., Bose, P., Kruegel, C., Vigna, G., & Nilizadeh, S. (2024). Unveiling the Risks of NFT Promotion Scams. *Proceedings of the International AAAI Conference on Web and Social Media*, *18*, 1367–1380. https://doi.org/10.1609/icwsm.v18i1.31395

Siregar, D. (2025). Legal Protection for Investors in Bitcoin Transactions on Exchange Platforms. *Binamulia Hukum*, *14*(1), 53–68. https://doi.org/10.37893/jbh.v14i1.1012

Subekti, R., & Tjitrosudibio, R. (Eds). (2017). *Kitab Undang-Undang Hukum Perdata: Burgerlijk Wetboek Dengan Tambahan Undang-Undang Pokok Agraria dan Undang-Undang Perkawinan*. Balai Pustaka.

Yudistira, K., & Yustiawan, D. G. P. (2025). Pertanggungjawaban Exchange Kripto Terhadap Hilangnya Aset Konsumen. *Kertha Desa*, *12*(11), 4873–4884. https://ojs.unud.ac.id/index.php/kerthadesa/article/view/120442