



International Journal of New Approaches to Law and Rationality in
Nationhood, Governance, and Rights Advocacy
Nalarnagara Journal

Vol. 1, No. 3, July 2026 pp. 1323-1332

Journal Page is available at <https://internationaljournal.lppmunsaka.ac.id/index.php/nalarnagara>



**Legal Analysis of The Immutable and Pseudonymous Nature of Crypto Asset
Blockchain in Indonesia from A Personal Data Protection Perspective**

Bagus Pekik Prasetyaji¹, Annisa Fitria², Henry Arianto³

¹²³ Universitas Esa Unggul

Email: baguspekikp@student.esaunggul.ac.id, annisa.fitria@esaunggul.ac.id, henry.arianto@esaunggul.ac.id

ABSTRACT

Technological advancements frequently create a tension between regulatory frameworks and practical realities. Law Number 27 of 2022 on Personal Data Protection (the PDP Law), which serves as the foundation for data protection regulation in Indonesia, faces various challenges, particularly regarding crypto asset trading utilizing blockchain technology. This article examines the legal issues arising from the unique characteristics of blockchain technology in crypto assets, specifically its immutable nature and pseudonymous transactions. This research employs statutory and conceptual approaches, utilizing literature review techniques for data collection. The findings reveal a contradiction that creates legal uncertainty between the immutable nature of blockchain in crypto asset trading and the right to erasure mandated by Article 8 of the PDP Law. Furthermore, it highlights the challenges surrounding law enforcement and legal protection regarding pseudonymous crypto asset transactions, which present a high risk of exploitation and cybercrime. To address these issues, this study recommends the formulation of responsive and progressive regulations specifically governing the technical aspects of crypto asset trading and blockchain. Additionally, optimizing synergy between relevant regulations and institutional bodies, implementing a hybrid on-chain/off-chain storage mechanism, and robustly applying Know Your Customer (KYC) principles can serve as comprehensive solutions to ensure legal certainty for personal data protection in Indonesia.

Keywords: Blockchain, Crypto Assets, Cyberlaw, Immutability, Personal Data Protection, Right to Erasure

INTRODUCTION

The current era is moving toward modernization that prioritizes reliability, speed, efficiency, and effectiveness in all aspects of societal life—ranging from communication and governance to financial systems. Driven by digitalization, technological innovations such as cloud computing, artificial intelligence, the Internet of Things, and cryptocurrencies have emerged. In 2008, Satoshi Nakamoto introduced blockchain-based cryptocurrency through a program designed to serve as a public ledger for various types of transactions involving a decentralized network, with its product widely known today as Bitcoin (Raharjo, 2022).

This development prompted the government to take a stance on cryptocurrency through Bank Indonesia Regulation (PBI) Number 18/40/PBI/2016 and PBI Number 19/12/PBI/2017, which explicitly prohibit the use of cryptocurrency as a payment system. Bank Indonesia's (BI) prohibition was grounded in concerns regarding volatility risks, the absence of underlying financial assets for derivative pricing, and the potential misuse related to money laundering and terrorism financing. BI also gave special attention to the lack of institutional synchronization at the time to regulate and supervise digital asset trading (Peryanto et al., 2025).

Cryptocurrency itself is defined as a digital or virtual currency developed through systematic cryptographic tools and algorithms to generate secure ciphers and codes used as a medium of exchange (Maridjan et al., 2025). In Indonesia, the Financial Services Authority (OJK) reported that as of December 2024, there were 22.9 million domestic crypto asset user accounts, with a total transaction volume reaching IDR 650.6 trillion. This figure represents a significant surge of 335.9% compared to the same period in previous years (Rizki, 2025).

It was not until 2018 that cryptocurrency obtained its legal basis through Regulation of the Minister of Trade of the Republic of Indonesia Number 99 of 2018 on General Policies for the Organization of Crypto Asset Trading, which stipulated that cryptocurrency—hereinafter referred to as crypto assets—could be qualified as commodities tradeable on the futures exchange. In this regard, the regulation also delegated supervisory authority over its operation to the Commodity Futures Trading Regulatory Agency (Bappebti).

Through Bappebti Regulation Number 4 of 2023, the technical provisions for operating the physical crypto asset market were established as the primary framework for crypto asset trading. Crypto assets were formulated as digital assets that utilize cryptographic technology and peer-to-peer systems to verify and secure transactions, classified as intangible commodities (Peryanto et al., 2025). In 2023, through Law Number 4 of 2023 on the Development and Strengthening of the Financial Sector (UU P2SK), the government mandated the transfer of supervisory authority over crypto asset trading to the OJK, accompanied by a two-year transition period. To exercise its new authority and establish a more comprehensive cornerstone for crypto asset trading in Indonesia, OJK issued Financial Services Authority Regulation Number 27 of 2024 on the Operation of Digital Financial Asset Trading Including Crypto Assets (POJK 27/2024).

Alongside the development of crypto assets, fintech and e-commerce have also grown rapidly. However, in addition to positive technological developments, negative issues have also arisen, such as cybercrime and data breach incidents involving state institutions and personal data controllers. Consequently, Law Number 27 of 2022 on Personal Data Protection (the PDP Law) was enacted, serving as the legal basis for personal data protection in Indonesia.

One of the primary rationales for enacting the PDP Law is to protect the rights of personal data subjects, which include the right to obtain information, right of access, right to withdraw consent, right to rectification, right to object to processing based on specific interests, as well as the right to erasure and destruction (Maridjan et al., 2025). The protection guaranteed under the PDP Law is crucial within the crypto asset ecosystem to prevent the risk of platform exploitation by irresponsible parties. Nevertheless, significant challenges must be addressed regarding the implementation of the PDP Law in crypto asset trading. One major challenge relates to the supervision and management of crypto asset trading itself, particularly while OJK remains in its transitional phase. Another critical challenge concerns the harmony between the legal principles embedded in the PDP Law and the inherent characteristics of crypto asset blockchain platforms, which are immutable and decentralized (Maridjan et al., 2025)). These two characteristics complicate the enforcement of Article 8 of the PDP Law regarding data subjects' right to request the deletion and/or destruction of their personal data. Fundamentally, the immutable nature of blockchain aims to ensure record-keeping transparency that can be viewed and verified by all network participants, as transactions cannot be altered or deleted once recorded. Decentralization is also a crucial factor instilling confidence in blockchain security, given that altering transactions or manipulating data requires controlling more than 50% of the computers within the same blockchain network (Raharjo, 2022).

Another aspect requiring attention in the implementation of the PDP Law is the pseudonymous nature of crypto asset wallets. In cases of cybercrime such as theft via hacking, illegal transactions, or online crypto fraud, transaction flows remain traceable on the public blockchain; however, the actual identity of the user remains difficult to determine because it is not recorded on-chain. On one hand, this hampers law enforcement when violations or crimes occur; on the other hand, it constitutes an advantage of crypto assets by providing enhanced privacy and guaranteeing user privacy security.

Based on this background, the author is driven to further investigate these challenges, presented in the form of a final thesis research journal entitled “*Legal Review of the Immutable and Pseudonymous Nature of Crypto Asset Blockchain in Indonesia from a Personal Data Protection Perspective*”.

RESEARCH QUESTIONS

Based on the background outlined above, two primary research questions are formulated as follows:

1. How is personal data protection applied to crypto asset users regarding the data subject's right to erasure within an immutable or non-erasable crypto asset blockchain system?
2. How is personal data protection applied to pseudonymous crypto asset transactions within the blockchain, particularly in accommodating the tracing of personal data subjects?

RESEARCH METHOD

1. Type and Approach of Research

This study employs normative legal research (doctrinal legal research), which is a process to discover legal norms, legal principles, and legal doctrines to address the legal issues under examination (Efendi & Rijadi, 2023).

The research approaches utilized to support this normative legal research include:

- 1) Statute Approach
The statute approach is conducted by examining all laws and regulations relevant to the legal issue under study (Muhaimin, 2020).
- 2) Conceptual Approach
The conceptual approach is an analytical perspective evaluated through the lens of legal concepts or based on the norming aspects embedded within a regulation (Efendi & Rijadi, 2023).

2. Data Sources

The data sources utilized in this study consist of secondary data, also referred to as legal materials. These legal materials comprise (Muhaimin, 2020):

- 1) Primary legal materials, which include binding legal materials such as laws and regulations, official decisions of authorized state institutions, international regulations, court judgments, and official state documents.
- 2) Secondary legal materials, which include legal books and academic legal journals containing underlying principles, opinions of legal scholars, and legal research findings.

- 3) Non-legal materials, which serve as non-book data sources or supporting texts relevant to this research.

3. Data Collection Technique

Data collection is conducted through a literature review technique (*library research*). This method involves gathering data from written sources and academic literature (Soekanto, 2015).

4. Data Analysis Technique

A qualitative analytical technique is selected to analyze the findings in this study. This analytical approach is executed through a research process that derives descriptive research data from written sources. The data is then thoroughly and comprehensively examined to analyze the legal issues, providing a clear and in-depth understanding of all aspects serving as the object of this research (Arbina & F Putuhena, 2022).

RESULTS AND DISCUSSION

Contradiction Between the Immutable Nature of Crypto Asset Blockchain and the Right to Erasure Under the PDP Law

The PDP Law serves as a critical regulatory foundation in Indonesia's personal data protection reform, marking a transition from a sectoral approach toward a more comprehensive and unified data protection framework. Fundamentally, the substance of the PDP Law adopts the fundamental principles of global personal data protection established by the European Union, specifically the General Data Protection Regulation (GDPR). This adoption is evident in core principles that form key pillars of the PDP Law, such as lawfulness, fairness, transparency, purpose limitation, data minimization, integrity and confidentiality, and accountability, all of which reflect well-established concepts under the GDPR (Prastia, 2025).

Both the PDP Law and the GDPR emphasize that personal data protection is not merely a legal obligation, but a cornerstone of trust within the digital ecosystem (Prastia, 2025). To foster such trust, the PDP Law regulates the enforcement of personal data subjects' rights, which are also adopted from the GDPR. There are nine primary rights guaranteed to personal data subjects: the right to information, right of access, right to withdraw consent, right to rectification, right to object to processing based on specific interests, right to erasure and destruction, right to object to automated decision-making, right to bring action and claim compensation, and the right to obtain and transfer data (Maridjan et al., 2025).

However, in its development, the PDP Law faces several challenges in fulfilling these data subjects' rights, particularly concerning crypto asset trading. Based on implementing regulations of Law No. 4 of 2023 (UU P2SK)—as amended by Law Number 4 of 2026 on the Development and Strengthening of the Financial Sector—including Government Regulation Number 49 of 2024 (PP 49/2024) and POJK 27/2024, crypto assets are defined as digital representations of value that can be traded, stored, or transferred using distributed ledger technology (such as blockchain) that guarantees transaction security and validity. Consequently, this definition indirectly shifts the paradigm of crypto assets from being categorized as commodities to being recognized as digital financial assets (Norman, 2025).

Therefore, crypto asset trading is inherently tied to distributed ledger technology known as blockchain. Blockchain technology is understood as a decentralized technology enabling transactions between two parties without involving a third party. Data within a blockchain is stored in a decentralized manner across the relevant network, making it impossible for a

single party to alter data without obtaining majority consensus from all nodes in the same network. From this explanation, blockchain serves to enhance transparency and accountability in data management (Salsabilla & Fauzi, 2026).

Thus, blockchain offers numerous advantages in crypto asset trading, particularly regarding transaction security. For instance, Article 16A and Article 16B of Law Number 1 of 2024 on Electronic Information and Transactions (UU ITE) mandate electronic system operators to maintain the security and integrity of electronic data. Blockchain fulfills this requirement through its decentralized and immutable nature by providing transparent and unalterable transaction records (Salsabilla & Fauzi, 2026). Conversely, this immutable characteristic creates a direct legal contradiction with personal data protection principles, specifically the data subject's right to erasure as stipulated in Article 8 of the PDP Law (Pinanggih et al., 2026).

The characteristics of blockchain become increasingly misaligned with existing regulations when evaluated alongside Articles 15 through 18 of the PDP Law, which mandate the fulfillment of data subject rights beyond erasure—such as rights of access, rectification, objection, and restriction of processing. Immutability complicates the direct implementation of these rights (Salsabilla & Fauzi, 2026). This contradiction between statutory regulation and the practical realities of digital advancements creates legal uncertainty regarding personal data protection, affecting users/consumers, personal data controllers, and entities within the crypto asset trading ecosystem operating their businesses.

As conceptualized by Gustav Radbruch, legal certainty represents a state where the law functions as a mandatory rule to be obeyed (Halilah & Arif, 2021). This aligns with Sudikno Mertokusumo's view that legal certainty is realized when law possesses actual binding force. The existence of legal certainty establishes protection for *justiciabel* against arbitrary actions, ensuring individuals receive expected legal outcomes under specific circumstances (Julyano & Sulistyawan, 2019). Consequently, in the absence of specific regulations creating space for exercising the right to erasure within crypto asset trading, legal certainty guaranteeing data subject rights remains unfulfilled.

Blockchain algorithms and their decentralized data structures will continue to evolve, creating an experimental ecosystem that traditional regulatory approaches struggle to govern (Muflikh et al., 2025). Future blockchain technology applications are expected to expand beyond crypto asset trading into sectors such as finance, healthcare, and public administration. Thus, responsive regulations are necessary to address these unique blockchain characteristics.

This concept is aligned with Julia Black's view in her book "*Critical Reflections on Regulation*" (2002), in which she conceptualizes the idea of responsive regulation as a regulatory approach that is not static, rigid, or entirely top-down. The regulations formed are also not sufficient merely by containing formal rules, but must be capable of effectively adapting to changing field conditions, including the complexity of industry actors' behavior, the diversity of economic activities, as well as the dynamics of rapidly evolving technology (Muflikh et al., 2025).

Existing national legal frameworks—such as UU P2SK, UU ITE, the PDP Law, and Bappebti and OJK regulations—provide a foundational basis for governing electronic transactions and crypto asset trading. However, these regulations do not specifically address the unique characteristics of cross-border, volatile, intangible digital assets operating on immutable and pseudonymous blockchain technology (Muflikh et al., 2025).

Viewed through Julia Black's (2002) concept of responsive regulation, the absence of specific rules regarding crypto assets and blockchain technology demonstrates that regulators have not yet been able to adapt to respond to emerging developments and risks that may arise in the future. Existing regulations currently tend to rely on a rigid and sectoral command-and-control approach, rather than being grounded in dynamic, collaborative, and dialogue-based regulation involving all relevant stakeholders, ranging from crypto asset traders, digital wallet providers, and digital forensics analysts to individual users (Muflikh et al., 2025). From this perspective, it is expected that the government, as the regulator, can establish more specific regulations regarding crypto assets and blockchain by utilizing responsive and progressive instruments.

Then, what kind of specific regulation can bridge the contradiction between the immutable characteristic of blockchain and the data subject's right to erasure under the PDP Law? This research will propose a mechanism concept utilized under the GDPR, which simultaneously supports the principle of data minimization because the blockchain ledger (distributed ledger) does not store raw personal data of its users or owners (Pinanggih et al., 2026).

The proposed mechanism is a *hybrid on-chain/off-chain storage mechanism*. Under this framework, user personal data—such as identity, account details, risk profiles, or financial verification data—is encrypted off-chain using symmetric encryption keys. The resulting encrypted ciphertext is stored in off-chain repositories controlled by Financial Sector Technology Innovation Operators (Penyelenggara ITSK) or Crypto Asset Traders (Pinanggih et al., 2026).

As a result, the blockchain ledger no longer stores raw personal data directly; instead, it records only ciphertext hashes, data identifiers, data versions, policy identifiers, consent status, and audit logs. When data is accessed, the system re-examines the off-chain ciphertext hash and compares it with the hash stored on-chain to verify transaction legitimacy (Pinanggih et al., 2026).

In terms of its implementation, this mechanism can grant full control to personal data controller institutions over their consumers' personal data stored separately (off-chain) from the associated blockchain. Through this mechanism, it is expected that, although it does not encompass all types of data, personal data controllers can fulfill their obligations regarding the exercise of personal data subjects' rights as mandated by the PDP Law, one of which relates to the right to erasure.

In addition to the hybrid on-chain/off-chain storage mechanism, based on available literature, there remain various other technical mechanisms to support crypto asset trading operations and blockchain-related regulation. Such technical mechanisms are expected to be adapted and incorporated into specific regulations with a responsive and progressive framework to guarantee legal certainty for personal data protection in Indonesia.

Naturally, robust regulations will not be complete without effective oversight over compliance to guarantee legal certainty. As mandated by Article 58 of the PDP Law, the role of the Personal Data Protection Authority (LPPDP) as a regulator that simultaneously carries out supervisory and enforcement functions for personal data protection in Indonesia must be maximized. Just as the GDPR has specialized bodies such as Data Protection Authorities (DPAs) at the national level and the European Data Protection Board (EDPB) at the European Union level to ensure consistent regulatory enforcement across jurisdictions. In the context of this research, it is expected that the LPPDP can execute its functions together with the OJK through synergistic coordination to produce harmonious regulations and a clear division of authority.

The need for this is aligned with Maria S. W. Sumardjono's opinion regarding the concept of legal certainty, in which normatively, it can be interpreted that legal certainty needs to be grounded in sound legislative instruments that practically support the implementation of such regulations. Meanwhile, empirically, it can be interpreted that the existence of such legislation requires continuous and accountable execution by the implementing authorities (Halilah & Arif, 2021).

Pseudonymity in Crypto Asset Trading Transactions from a Personal Data Protection Perspective

Crypto asset trading built upon blockchain technology possesses another unique characteristic alongside immutability: pseudonymity. Most blockchain networks, such as *Bitcoin* and *Ethereum*, offer pseudonymity wherein users conceal their real-world identities behind a string of alphanumeric characters known as a digital wallet address. This wallet address serves as a pseudonymous identity separating financial operations from the owner's personal details (Apriliantono et al., 2026).

This pseudonymous concept is originally intended to protect user privacy through cryptographic methods while ensuring that transaction histories remain transparently and publicly recorded on the blockchain ledger. However, while this characteristic provides strong privacy for users, this identity concealment mechanism is frequently exploited by cybercriminals as a primary means to disguise illegal transactions, such as fraud, hacking, and money laundering (Apriliantono et al., 2026). Law enforcement measures by law enforcement officers, including tracing, freezing, and asset recovery, face severe hurdles when confronting cross-border, pseudonymous blockchain technology (Muflikh et al., 2025).

To address the polemic surrounding pseudonymous blockchains vulnerable to abuse and crime, Bappebti, as the regulator, enacted a series of preventive implementing regulations. Through Bappebti Regulation Number 13 of 2022 amending Regulation Number 8 of 2021, Bappebti explicitly stipulated technical and administrative provisions for business entities operating legally in Indonesia. A key aspect of this regulation is the mandatory implementation of *Anti-Money Laundering* (AML) and *Know Your Customer* (KYC) principles by crypto asset traders.

These principles are designed to offer legal protection to both business entities and consumers within the crypto asset trading ecosystem. This aligns with Muchsin's theory of legal protection, which classifies protection into two forms: preventive legal protection, which establishes government regulations to prevent violations before they occur, thereby setting legal boundaries; and repressive legal protection, which applies sanctions such as fines or imprisonment after violations take place (Salsabilla & Fauzi, 2026).

The implementation of KYC principles requires crypto service providers to identify and verify user identities prior to providing services. Data collected during this process encompasses full names, residential addresses, copies of official identity documents, personal photographs, and financial information such as bank accounts and source of funds. In practice, this creates an ecosystem where crypto exchanges rely heavily on collecting and managing user personal data (Maridjan et al., 2025).

Under the Bappebti Regulation, one of specific application of KYC principles dictates that physical crypto asset traders are permitted to open only one account per customer corresponding to a single verified identity.

Nevertheless, this Bappebti Regulation is not without flaws. The regulatory framework leans more toward market stability, trading system integrity, and financial crime prevention

rather than focusing on personal data protection and data subjects' privacy rights. This imbalance creates potential risks of data misuse if service providers fail to enforce strict data security policies aligned with personal data protection principles under the PDP Law (Maridjan et al., 2025).

Crypto asset trading in Indonesia is generally conducted through licensed exchanges such as *Indodax* or *Tokocrypto*, bound by mandatory KYC requirements, AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) provisions, and suspicious transaction reporting to the Financial Transaction Reports and Analysis Center (PPATK). Only officially registered companies can operate as crypto asset traders, and investors are required to use Indonesian Rupiah (IDR) as the transaction currency to preserve national monetary sovereignty. However, the government does not guarantee crypto asset holdings, leaving all risk of loss entirely with the investor/consumer. (Satya & Rivani, 2025).

Another challenge in enforcing KYC principles involves maintaining high compliance standards and mature risk management mechanisms necessary for successful execution (Prastia, 2025). Effective coordination between the OJK—as the primary supervisor of crypto asset trading in Indonesia—and trading platform operators is essential. The OJK and platform providers must ensure that pseudonymous transactions are linked to legally verified identities, enabling transactions to be traced back to their respective owners and held accountable.

As the financial authority safeguarding market integrity and consumer protection, the OJK must continually adapt to evolving ground realities, given that regulatory success relies heavily on policy clarity and institutional readiness to manage the digital asset ecosystem comprehensively (Norman, 2025). Several supervisory challenges in Indonesian crypto asset trading require immediate, specific, and responsive regulation. For instance, implementing the Travel Rule—which mandates the exchange of originator and beneficiary information in cross-border crypto transactions—is closely linked to tracing illegal funds (AML/CFT) and recovering criminal assets.

CONCLUSION

The Personal Data Protection Law (PDP Law) serves as an important regulatory foundation in Indonesia's personal data protection regulatory reform toward a more comprehensive and unified legal framework. However, in its development, the PDP Law faces a number of challenges, one of which relates to crypto asset trading with its blockchain technology. Although blockchain offers many advantages, such as transparency and high accountability, its immutable nature creates a contradiction with personal data protection principles regarding the right to data deletion (right to erasure) as mandated by Article 8 of the PDP Law. This contradiction causes legal uncertainty regarding the rights of personal data subjects, between existing regulations and the reality occurring in the field.

To bridge this contradiction, the results of this research recommend the formulation of specific regulations regarding crypto asset blockchain technology that are responsive and progressive toward technological developments, by utilizing responsive instruments to strengthen the legal framework of existing national regulations. In addition, technical mechanisms such as hybrid on-chain/off-chain storage that is separate from the blockchain can serve as a technical solution to this issue. This mechanism can grant personal data controllers full authority over their consumers' personal data stored separately (*off-chain*) from the associated blockchain. Through this mechanism, it is expected that space will be created for personal data controllers to fulfill their obligations regarding the exercise of personal data subjects' rights as mandated by the PDP Law, without sacrificing security and privacy factors.

Another issue that arises relates to the characteristic of crypto asset blockchain trading, which is pseudonymous. Most blockchain networks offer pseudonymity wherein users can conceal their real identities behind alphanumeric characters (wallet address). Although this characteristic provides strong privacy for entity users, identity concealment mechanisms are frequently abused by cybercriminals as a primary means to disguise illegal transactions, such as fraud, hacking, and money laundering.

Regulations that prioritize the *Know Your Customer* (KYC) principle can serve as a recommendation in response to this issue. However, the implementation of KYC requires high compliance standards and mature risk management mechanisms. Effective coordination is required between the OJK and crypto asset trading platform operators. The OJK and crypto asset trading operators must ensure that every pseudonymous transaction taking place is linked to a legally verified identity.

REFERENCES

- Apriliantono, N., Hermawan, O. C., Primasary, S. E., & Halim, T. (2026). Penggunaan Cryptocurrency Sebagai Pencucian Uang oleh Pelaku Korupsi. *Jurnal Wacana Sosial Nusantara*, 2(7), 1–17. <https://doi.org/https://doi.org/10.5281/zenodo.21224296>
- Arbina, M., & F Putuhena, M. I. (2022). Tata Kelola Pembentukan Regulasi Terkait Perdagangan Mata Uang Kripto (Cryptocurrency) sebagai Aset Kripto (Crypto Asset). *Mahadi: Indonesia Journal of Law*, 1(1), 33–57. <https://doi.org/10.32734/mah.v1i1.8314>
- Efendi, J., & Rijadi, P. (2023). *Metode Penelitian Hukum Normatif dan Empiris* (6th ed.). Kencana.
- Halilah, S., & Arif, Mhd. F. (2021). Asas Kepastian Hukum Menurut Para Ahli. *Siyasah: Jurnal Hukum Tata Negara*, 4(II), 56–65. <https://ejournal.an-nadwah.ac.id/index.php/Siyasah/article/view/334>
- Julyano, M., & Sulistyawan, A. Y. (2019). Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum. *CREPIDO*, 1(1), 13–22. <https://doi.org/10.14710/crepido.1.1.13-22>
- Maridjan, Y. I. M., Mamengko, R., & Gerungan, C. A. (2025). Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dalam Transaksi Cryptocurrency. *Lex Crimen Jurnal Fakultas Hukum UNSRAT*, 13(2). <https://doi.org/10.31933/unesrev.v7i1>
- Muflikh, A. A. M., Ramadan, D. R. C., Silalahi, B. B. S., Martitah, & Sulistianingsih, D. (2025). Analisis Perlindungan Hukum Konsumen pada Perjanjian Transaksi E-Commerce terkait Investasi Kripto Ilegal via Media Sosial. *Book Chapter Hukum dan Politik dalam Berbagai Perspektif Unnes*, 4, 106–133. <https://doi.org/10.15294/hp.v4i.609>
- Muhaimin. (2020). *Metode Penelitian Hukum*. Mataram University Press.
- Norman, C. A. (2025). Transformasi Hukum Aset Kripto di Indonesia: Analisis Komparatif dengan Malaysia Mengenai Pergeseran dari Komoditas ke Instrumen Keuangan. *Padjadjaran Law Review*, 13(1), 100–113. <https://doi.org/10.24198/plr.v13i1.2214>
- Peryanto, J., Napitupulu, D. R. W., & Saragi, P. (2025). Perlindungan Hukum Bagi Pengguna Cryptocurrency Menurut UU No. 4 Tahun 2023 Tentang P2SK. *Jurnal Kolaboratif Sains*, 8(5), 2432–2446. <https://doi.org/10.56338/jks.v8i5.7576>

- Pinanggih, A. R., Mardiana, N., Pratama, F. Y., Desvia, Y. F., & Maulana, A. (2026). Pengembangan Sistem Keamanan Data Berbasis Blockchain untuk Perlindungan Informasi Sensitif di Sektor Keuangan. *Jurnal Penelitian Sistem Informasi*, 4(2), 71–103. <https://doi.org/10.54066/jpsi.v4i.3880>
- Prastia, Y. (2025). Keseimbangan Inovasi dan Kepatuhan: Implementasi Pelindungan Data Pribadi dalam Ekosistem Finansial Teknologi dan Aset Digital. *Journal of Financial Sector Law & Policy*, 1(2), 262–302. <https://jurnal.hkhsk.id/index.php/jfslp/article/view/127>
- Raharjo, B. (2022). *Uang Masa Depan: Blockchain, Bitcoin, Cryptocurrencies* (M. C. Wibowo, Ed.; 1st ed.). Yayasan Prima Agus Teknik. <https://digi-lib.stekom.ac.id/ebook/view/uang-masa-depan--blockchain-bitcoin-cryptocurrencies>
- Rizki, M. J. (2025, February 11). *Investor Kripto Indonesia 3 Besar Dunia! OJK Perketat Pengawasan*. <https://www.hukumonline.com/berita/a/investor-kripto-indonesia-3-besar-dunia-ojk-perketat-pengawasan-lt67ab385fd68/?Page=1>.
- Salsabilla, & Fauzi, E. (2026). Pengaturan Hukum Teknologi Blockchain Dan Penerapannya Dalam Transaksi Bisnis Di Indonesia. *Jurnal Kajian Hukum dan Kebijakan Publik*, 3(2), 609–617. <https://doi.org/https://doi.org/10.62379/6se9ay66>
- Satya, V. E., & Rivani, E. (2025). Parliamentary Review: Tantangan Regulasi dan Perdagangan Aset Kripto Di Indonesia dalam Mewujudkan Stabilitas Sistem Keuangan Nasional. *Parliamentary Review Badan Keahlian DPR RI*, VII(4), 189–197. <https://pusaka.dpr.go.id/en/produk/parliamentary-review>
- Soekanto, S. (2015). *Pengantar Penelitian Hukum*. Penerbit Universitas Indonesia (UI Press).