Legal Liability of Digital Wallet Providers in Cases of Crypto Asset Loss: An Empirical Legal Approach

Ahmad Latief Mualim[1],

[1] *Program Pascasarjana, Law Faculty, Universitas Islam As Syafi'iyah, Jakarta-Indonesia*

Corresponding Author: Ahmad Latief Mualim, **E-mail**: ahmadmualim@gmail.com

| ABSTRACT

The rapid development of cryptocurrency in Indonesia presents significant economic opportunities while also introducing substantial security risks, particularly the loss of assets due to digital wallet hacks. This study aims to analyze legal protection for cryptocurrency owners using a normative juridical and empirical approach, examining national regulatory frameworks, the liability of digital wallet providers, cybersecurity standards, and dispute resolution mechanisms. The research methodology includes literature review, analysis of legislation, examination of service provider contracts, and interviews with hack victims. The findings indicate that Indonesian regulations still categorize cryptocurrencies as commodities, resulting in limited consumer protection, unclear legal responsibilities for wallet providers, inconsistent cybersecurity standards, and ineffective dispute resolution mechanisms. Many platforms implement contractual clauses that transfer nearly all risk to users, while most hacks occur due to system vulnerabilities rather than user negligence. This study emphasizes the need for comprehensive regulations that establish minimum security standards, independent audits, compensation mechanisms, clear dispute resolution procedures, and digital literacy education for the public. The findings are expected to provide a foundation for strengthening legal frameworks and consumer protection policies for cryptocurrency in Indonesia and contribute to the theoretical development of legal liability and digital consumer protection in the blockchain era.

| KEYWORDS

Cryptocurrency; Digital Wallet; Legal Protection; Cybersecurity Breach; Digital Consumer

I. INTRODUCTION

The development of blockchain technology over the past decade has brought about significant transformations in the world of digital finance, particularly through the emergence of crypto assets as global investment and transaction instruments. In Indonesia, crypto assets have experienced exponential growth in line with increasing public interest in financial technology, investment diversification, and the profit opportunities offered by the digital market. Digital wallets, as a medium for storing and transacting crypto assets, have become an important part of this ecosystem, as they provide high accessibility, ease of use, and flexibility compared to traditional financial systems. However, these technological advances have brought with them the consequence of increased cybercrime risks, particularly digital wallet hacking, which has resulted in the loss of large amounts of assets. Various reports indicate that cryptocurrency hacking is one of the most financially and psychologically damaging forms of cybercrime for consumers.

In Indonesia, this phenomenon is increasingly complex because crypto assets are categorized as commodities under the supervision of the Commodity Futures Trading Regulatory Agency (Bappebti), rather than as a means of payment or financial instruments such as stocks, which are under the supervision of the OJK . This difference in legal categories creates a regulatory vacuum regarding consumer protection standards, the security obligations of digital wallet service providers, and compensation mechanisms in the event of a cyberattack. This situation underscores the urgency of

research on legal protection for cryptocurrency owners, especially in the context of asset loss due to digital wallet hacking.

The core issue in this research stems from the lack of legal protection available to crypto asset owners when they suffer losses due to hacking. User losses often cannot be recovered because there are no regulations that require digital wallet providers to provide compensation or implement certain security standards. The lack of clarity regarding the legal responsibilities of platform providers further exacerbates the position of users, as many companies include risk transfer clauses in their terms and conditions of service that are difficult to negotiate . In practice, digital wallet providers can claim that hacking occurred due to user negligence, rather than due to weaknesses in the systems they manage. In addition, various reports indicate that the digital security standards implemented by digital wallet providers vary greatly, and some of them do not meet the basic principles of modern cybersecurity. As a result, users are at high risk of losing their assets without any legal instruments that can provide adequate protection.

The difficulty victims face in pursuing dispute resolution mechanisms through mediation, arbitration, or litigation is also a problem in itself. Many victims find it difficult to identify the perpetrators due to the anonymous and cross-border nature of blockchain transactions, which makes law enforcement difficult . The mismatch between technological developments and regulatory readiness is the root cause of the problem underlying this study. This study aims to provide a comprehensive understanding of legal protection for crypto asset owners in cases of asset loss due to digital wallet hacking, through an empirical juridical approach. The first objective is to identify and analyze the regulatory framework related to crypto assets, digital wallet security, and consumer protection applicable in Indonesia, particularly regulations issued by Bappebti and regulations related to digital transactions.

The second objective is to analyze the legal liability of digital wallet service providers, both based on the principles of consumer protection and the theory of legal liability in contractual relationships and digital service relationships. The third objective is to assess the effectiveness of the legal protection mechanisms available to crypto asset owners in dealing with hacking cases, including dispute resolution mechanisms in the Indonesian legal system. The fourth objective is to present an empirical picture of the experiences of victims of digital wallet hacking in pursuing legal action, the obstacles they face, and the extent to which existing mechanisms are able to provide compensation for losses. Finally, this study aims to provide legal and policy recommendations that can improve security, transparency, and protection for crypto asset owners in Indonesia.

A gap analysis shows that research on crypto assets in Indonesia has developed, but most of it focuses on the legality of trading, potential abuse, and supervision in the context of digital commodities. Research discussing consumer protection aspects is still limited and focuses more on the risk of investment fraud than the risk of hacking or digital security. In addition, there have not been many studies that discuss in depth the legal responsibility of digital wallet providers when consumers experience asset loss due to platform security weaknesses. The literature on cybersecurity in the context of crypto assets discusses many technical aspects, such as encryption and private key management, but does not adequately link them to legal implications and consumer protection. In addition, empirical studies on the experiences of users who have been victims of hacking are still very limited, so there is no comprehensive picture of the real obstacles faced by the public in claiming their rights. The absence of research that combines normative and empirical legal approaches in analyzing the legal protection of crypto asset owners indicates an important gap that this research needs to fill.

This research offers important new contributions (novelty) to the development of legal science, particularly digital law, consumer protection, and crypto asset regulation. First, this research is one of the first works to examine digital wallet hacking through an empirical legal approach, namely by analyzing applicable regulations while also exploring the experiences of hacking victims directly [8]. Second, this study provides a new mapping of the legal responsibilities of digital wallet providers, which has not been widely discussed in previous studies, especially regarding contract clauses that are detrimental to consumers and security standards that should be the responsibility of the platform. Third, this study enriches the literature through an in-depth analysis of the gap between the theory of digital consumer protection and actual practice in the field. Fourth, the empirical findings provide a basis for evidence-based policy recommendations that policymakers can use to design regulations that are more adaptive and responsive to cybercrime risks in the crypto asset sector. Finally, this study supports the development of modern technology-based legal protection concepts, integrating cybersecurity principles with legal responsibilities and consumer rights, thereby contributing theoretically and practically to strengthening the crypto asset ecosystem in Indonesia. Thus, this introduction provides a strong foundation for further exploring how legal protection for crypto asset owners can be realized, especially in the face of increasing risks of digital wallet hacking that threaten public trust in blockchain-based financial systems.

II. METHODOLOGY

The research method plays a fundamental role in ensuring that the analysis of legal protection for crypto asset owners in cases of asset loss due to digital wallet hacking is carried out in a systematic, measurable, and accountable manner. This study uses an empirical juridical approach with a combination of normative juridical aspects, enabling researchers to not only examine written laws but also analyze how these laws work in social reality. This approach is in line with the characteristics of the crypto asset issue, which involves regulatory dimensions, digital technical aspects, and the behavior of users and asset storage platform providers. As explained by Soerjono Soekanto, empirical legal research seeks to understand how the law functions in society through behavioral interactions and the effectiveness of regulations.

The normative legal approach serves as the first analytical basis in this study. This approach examines primary, secondary, and tertiary legal materials to understand the legal framework for crypto assets in Indonesia. Primary legal materials include regulations such as Bappebti Regulation No. 8 of 2021, the Electronic Information and Transaction Law (ITE Law), and provisions related to consumer protection in the context of digital transactions. The analysis also covers legal principles, doctrines, and relevant theories such as legal protection theory, legal liability theory, cybersecurity theory, and digital consumer protection theory. This approach provides a theoretical foundation for understanding what should happen in the legal system when digital wallet users lose assets due to hacking.

Furthermore, this study integrates an empirical approach, which examines the effectiveness of the law in practice. Empirical data was obtained through semi-structured interviews with victims of digital wallet hacking, users who had experienced security breaches but did not lose assets, and parties working in the crypto asset industry, including local digital wallet service providers. This approach is used to capture social conditions and realities in the field that cannot be seen through normative studies alone. Empirical data is essential for understanding the obstacles victims face in seeking legal redress, the actual level of responsibility applied by digital wallet providers, and the gap between rules and practice.

The data collection procedure was carried out in three main stages. First, a document study, which considered official regulations, hacking incident reports, digital wallet security audit results, and court decisions related to digital asset theft cases (if available). This document study is used as a basis for comparison to measure the continuity between theory and practice. Second, in-depth interviews are conducted with at least five hacking victims and three crypto asset industry practitioners. These interviews are aimed at exploring concrete experiences that include technical and legal aspects, such as the difficulty of proving platform negligence, platform customer service responses, and obstacles in dispute resolution. Third, non-participatory observation of popular digital wallet platforms to assess whether the security standards claimed by providers are in line with proper security practices as recommended in cybersecurity theory and international recommendations such as ENISA.

To ensure the validity of the research, triangulation techniques were applied by comparing interview data with legal documents and academic references. Triangulation is important because cases of crypto asset hacking often involve complex technical issues, which need to be verified from various sources. To avoid bias, interviews were conducted with an objective approach and did not lead the interviewees, but facilitated them to explain their experiences chronologically and technically.

The data analysis technique used was descriptive qualitative analysis. Normative data was analyzed by understanding the applicable legal structure, legal principles, and consumer protection norms that should be applied. Meanwhile, empirical data was analyzed to identify patterns, trends, and obstacles experienced by the community. The results of the normative and empirical analyses were then combined to comprehensively assess the effectiveness of the law. This integrative approach enabled researchers to identify areas where the law has worked well and areas that need improvement. In modern legal research, the use of a strong theoretical framework is essential to connect empirical findings with legal analysis. Therefore, this study uses four major theories: (1) Legal protection theory, to assess the extent to which the state is present in providing certainty and justice for crypto asset owners [4]; (2) Legal liability theory, to analyze the obligations of digital wallet providers and the possibility of liability for damages [5]; (3) Cybersecurity Theory, to assess the security standards that should be required of platform providers [6]; and (4) Digital Consumer Protection Theory, to map the rights of users in the context of the digital economy. These four theories are used to construct a logical map between legal norms, industry practices, and social conditions. This research method is expected to provide a comprehensive picture of how the Indonesian legal system handles cases of crypto asset hacking and the extent to which consumer protection can be realized. The empirical juridical approach is the main basis for filling the gap in the literature, which mostly uses a purely normative approach. By understanding law as a

normative structure and social phenomenon, this study can provide realistic and implementable legal recommendations in accordance with the needs of society.

III. RESULTS AND DISCUSSION

The Legal Framework for Crypto Assets in Indonesia and the Scope of Consumer Protection

Crypto asset regulations in Indonesia differ from many other jurisdictions because crypto assets are categorized as digital commodities under the supervision of the Commodity Futures Trading Regulatory Agency (Bappebti), rather than as currencies or financial instruments regulated by the Financial Services Authority. Bappebti Regulation No. 8 of 2021 establishes guidelines for the operation of physical cryptocurrency markets, including trading system operators and asset custodians [9]. However, this regulation does not specifically regulate digital wallet providers that operate as non-custodial or semi-custodial personal storage. As a result, there is a significant regulatory gap in determining the limits of digital wallet providers' liability to users in the event of a hack. In the context of digital consumer protection, Indonesia has general regulations through the Consumer Protection Law (UUPK) and the Electronic Information and Transaction Law (UU ITE). However, these two regulations are designed for digital transactions in general and do not take into account the unique characteristics of crypto assets, such as blockchain decentralization, the anonymous nature of transactions, and the control of private keys in the hands of users. Therefore, existing legal instruments tend not to provide adequate protection against the loss of crypto assets due to digital wallet security breaches. In legal protection theory, the state is obliged to provide certainty, benefit, and justice for its citizens through regulatory instruments that are capable of responding to technological developments [4]. However, normative discussions show that the applicable regulations are still partial and do not accommodate the needs of digital wallet users. This is in line with literature findings that emphasize that blockchain and cryptocurrency regulations often lag behind technological innovations [10]. Therefore, the current legal framework is still unable to provide strong protection for crypto asset users who are victims of hacking.

Digital Wallet Cybersecurity Standards and Implementation Challenges

Crypto digital wallets are a central element in crypto asset security because they store private keys, which are proof of asset ownership. Cybersecurity theory emphasizes that service providers must implement layered security principles, strong encryption, multi-factor authentication, and responsive threat detection systems. In addition, international institutions such as ENISA recommend the implementation of cold storage protocols, periodic security audits, and asset segregation to reduce the risk of hacking. However, the results of this study's observations show that many digital wallet providers in Indonesia do not optimally implement layered security standards. Some platforms only provide password-based security and email verification, without implementing multi-factor authentication or a system for monitoring suspicious activity. This type of security configuration is highly vulnerable to brute force attacks, phishing, or credential-stealing malware. In interviews with hacking victims, most incidents occurred through illegal access due to authentication weaknesses or a lack of protection against social engineering attacks. Some users also do not understand how to secure private keys or seed phrases, because service providers do not provide sufficient education. Based on the theory of digital consumer protection, service providers are required to provide clear and adequate information about the risks of using digital products. However, in practice, users are often given minimal explanations, and it is not uncommon for platforms to state that the risk of losing private keys is entirely the responsibility of the user. Digital wallet providers also tend to ignore minimum security standards such as independent security audits and penetration simulations. In fact, crypto security studies show that most digital wallet hacks occur due to weaknesses in the wallet software or the provider's backend server, not due to user negligence. This condition violates the principle of legal responsibility because service providers should provide guarantees of system feasibility and security based on industry standards. Therefore, there is a discrepancy between cybersecurity theory and actual practice in the field, which leads to a high potential for asset loss due to hacking.

Analysis of the Legal Responsibilities of Digital Wallet Providers

The legal liability of digital wallet providers is an important aspect of this study. In theory, digital service providers are required to guarantee the reliability of their systems and protect users from foreseeable risks. However, the results of this study show that most platforms include exemption clauses in their terms and conditions of service. These clauses state that providers are not liable for losses arising from hacking, unless it is proven that the attack originated from internal negligence on the part of the platform. These clauses substantially weaken the position of consumers because the burden of proving platform negligence is very heavy and difficult to do without access to server logs or system audits. In many cases, digital wallet providers do not provide sufficient technical transparency for users to prove the existence of system vulnerabilities. This contradicts the principle of consumer protection, which requires

businesses not to impose disproportionate risks on consumers. In addition, digital wallet hacking often involves cross-border attackers, making cross-jurisdictional law enforcement very difficult. Previous research shows that in cases of international cybercrime, law enforcement success rates are very low due to the complexity of digital forensics, lack of cooperation between countries, and the anonymity of perpetrators. As a result, consumers not only find it difficult to obtain compensation from platform providers but are also unable to prosecute hackers criminally. An analysis of the electronic contracts used by digital wallet providers shows that these contracts are adhesive, meaning that they do not allow room for negotiation by users. In modern contract theory, clauses that deviate from the principle of balance between rights and obligations can be considered invalid if they deprive consumers of their right to obtain adequate protection. However, to date, there has been no jurisprudence or court ruling in Indonesia that specifically assesses the validity of contract clauses in crypto digital wallet services. This condition shows that the legal liability of digital wallet providers still lacks adequate legal certainty, so that users do not have a strong instrument to claim their rights.

Dispute Resolution Mechanisms and Barriers to Their Implementation

In the Indonesian legal system, disputes over digital transactions can be resolved through mediation, arbitration, or litigation. However, research shows that most victims of crypto asset hacking face significant difficulties in pursuing any form of dispute resolution. Through empirical interviews, it was found that most victims choose to report to the service provider first. However, the response from service providers is often limited to requesting documentation of the incident and is not followed by an in-depth technical investigation. Many victims receive a standard response stating that "the attack did not originate from the internal system" even though no independent audit has been conducted. This shows an imbalance of information between users and platform providers. Bappebti, as the supervisory authority for digital commodities, does not have a specific mechanism for handling complaints related to digital wallet hacking. Bappebti only supervises crypto asset trading service providers, not independent digital wallet providers. Thus, victims who lose assets in non-custodial wallets are outside the scope of Bappebti's administrative protection [9]. Litigation in district courts is also not easy to pursue. The main challenge is digital evidence, especially in determining the point of entry for the hack, the identity of the perpetrator, and whether the platform was negligent in maintaining security. This is in line with international reports showing that cyber litigation is very complex because it requires a high level of technical evidence and often involves more than one jurisdiction. Meanwhile, online mediation or arbitration is rarely used because digital wallet providers do not provide formal channels for dispute resolution through third parties. Some platforms even state that their internal decisions are final and cannot be contested. Thus, the existing dispute resolution mechanisms have proven to be unable to provide effective, fast, and fair solutions for digital wallet users who have lost their assets.

The Effectiveness of Legal Protection in Practice: An Integrative Analysis

Based on normative analysis and empirical findings, legal protection for crypto asset owners who experience digital wallet hacking is still ineffective. The main weaknesses of legal protection can be seen in four aspects. First, the regulatory framework is not comprehensive because it only focuses on asset trading, not on storage security aspects. The dominance of the commodity approach has led to the neglect of consumer protection aspects. Second, the legal responsibility of digital wallet providers is unclear, and contract clauses are more favorable to the platform. This ambiguity weakens the position of consumers, who ultimately bear the full risk of asset loss. Third, platform security standards are inadequate, allowing for hacking attacks that could be avoided if service providers strictly implemented cybersecurity principles. Fourth, dispute resolution mechanisms are ineffective, whether through administrative channels, litigation, or alternative mechanisms. The existing regulatory structure does not provide a clear path to recovery for users. The combination of these four factors creates a vulnerable legal environment in which consumers are not adequately protected, while technological risks are increasing.

IV. CONCLUSION

This study shows that legal protection for crypto asset owners who experience asset loss due to digital wallet hacking in Indonesia is still in its early stages of development and does not yet provide adequate legal certainty. Based on normative and empirical legal analysis through literature studies, regulations, interviews, and case studies, it was found that the existing legal structure is not yet able to accommodate the characteristics of blockchain technology and the rapidly growing security risks of digital wallets. First, from a regulatory perspective, Indonesia still classifies crypto assets as commodities under the authority of Bappebti. This framework causes regulators to focus more on asset trading activities rather than on asset storage security, which should be a key element in digital consumer protection. The absence of specific regulations regarding security standards for digital wallet providers, compensation mechanisms for victims, audit requirements, and dispute resolution systems reveals a serious regulatory gap. Compared to global trends such as the MiCA regulation in the European Union, the Payment Services Act in

Singapore, and the Financial Services Act in Japan, the position of crypto consumer protection in Indonesia is relatively far behind.

Second, an analysis of legal liability theory shows that digital wallet providers do not yet have clear legal obligations in the event of a hack that results in consumer losses. Many platforms use adhesion contracts with exemption clauses that, in practice, transfer almost all of the risk to users. This condition contradicts the basic principles of consumer protection and contractual justice. The lack of jurisprudence in Indonesia regarding crypto asset disputes exacerbates the uncertainty of users' position in claiming their rights. Third, from a cybersecurity perspective, literature reviews and field findings show that many hacks occur due to weaknesses in security implementation, both on the part of wallet providers and users. However, the finding that most attacks exploit system vulnerabilities and are not solely due to user negligence indicates that digital wallet providers have a significant responsibility to provide secure, transparent, and regularly audited systems in accordance with the principle of layered security. The absence of minimum-security standards mandated by regulators highlights the weakness of preventive legal protection.

Fourth, the dispute resolution mechanism related to crypto asset hacking is not yet effective. Victims often experience difficulties in digital evidence, lack of transparency in internal platform investigations, and weak access to administrative and litigation mechanisms. Without a clear, fast, and fair dispute resolution system, consumers' legal efforts are not maximized. From these findings, it can be concluded that legal protection for crypto asset owners in the context of digital wallet hacking in Indonesia is still ineffective and requires comprehensive legal reform. This study makes an important contribution through mapping regulations, legal theory, technical risks, and empirical analysis that can serve as a basis for developing a stronger regulatory framework. This study proposes that in the future, the following are needed: 1) the establishment of specific regulations for crypto assets that include digital wallet security standards; 2) a consumer-friendly compensation mechanism; 3) mandatory independent security audits; 4) structured dispute resolution procedures; and 5) digital security literacy programs for the public. These efforts are important steps in ensuring that the development of the digital economy can take place safely, fairly, and provide optimal protection for cryptocurrency users in Indonesia.

REFERENCES

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

[2] Bappebti, *Peraturan Kepala Bappebti No. 5 Tahun 2019 tentang Pedoman Fisik Aset Kripto sebagai Komoditas Berjangka*, Jakarta: Bappebti, 2019.

[3] Hadjon, P.M., (2001) *Perlindungan Hukum bagi Rakyat*, Jakarta: Universitas Indonesia Press.

[4] Al-Bassam, M., (2021). *Blockchain Security and Cryptography: A Survey*, Journal of Information Security, vol. 12, no. 3, pp. 45–67/

[5] OECD, (2020). *Consumer Protection in the Digital Age*, OECD Publishing, Paris.

[6] European, Parliament(2023). *Regulation of Markets in Crypto-assets (MiCA)*, Official Journal of the European Union, 2023.

[7] Singapura Financial Authority (MAS), (2019). *Payment Services Act 2019*, Singapore.

[8] Japanese Financial Services Agency, (2020). *Regulation on Cryptocurrency Exchanges*, Tokyo..

[9] Chainalysis, (*2023) Crypto Crime Report*, New York: Chainalysis Research.

[10] ENISA, (2022). *Blockchain Threat Landscape Report*, European Union Agency for Cybersecurity

[11] FinCEN, (2021). *Guidance on Virtual Currencies*, U.S. Department of the Treasury.

[12] SEC, (2022). *Investor Alert: Crypto Asset Risks*, U.S. Securities and Exchange Commission.

[13] Fatf-Gafi, (2021). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Paris.

[14] UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), Indonesia.

[15] Komisi Nasional Konsumen, (2020). *Pedoman Perlindungan Konsumen Digital*, Jakarta: KNK.

[16] M. Swan, (2015). *Blockchain: Blueprint for a New Economy*, Sebastopol: O'Reilly Media.

[17] Zohar, A., (2015). *Bitcoin: Under the Hood*, Communications of the ACM, vol. 58, no. 9, pp. 104–113.

[18] Tapscott, D., & Tapscott, A., (2016). *Blockchain Revolution*, New York: Penguin.

[19] Kshetri, N., *(2018). Blockchain's Roles in Meeting Key Supply Chain Management Objectives*, International Journal of Information Management, vol. 39, pp. 80–89.

[20] Hardjono, T., Lipton, A., & Pentland, A., (2019). *Towards a Design Philosophy for Interoperable Blockchain Systems*, MIT Connection Science, 2019.