Customary Law Journal, ICLSSEE Special Collection 2026, *Page*: 1-12

Problems of Proving and Confiscating Crypto Assets Proceeding from Money Laundering Crimes by the Prosecutor's Office in the Indonesian Criminal Justice System

Emil Brunner*, Lucky Ferdiles

Borobudur University, Jakarta, Indonesia, emilamos84@gmail.com

Borobudur University, Jakarta, Indonesia, lucky_ferdiles@borobudur.ac.id

DOI:
https://doi.org/10.47134/jcl.v3i3.1.5811
*Correspondence: Emil Brunner

Email: emilamos84@gmail.com

Received: 19/05/2026
Accepted: 13/06/2026
Published: 13/06/2026

Abstract: *This study aims to analyze the challenges of proving and confiscating crypto assets in money laundering crimes and to formulate an adaptive legal concept within the Indonesian criminal justice system. The method used is normative juridical with a statutory and conceptual approach, through a review of the Criminal Procedure Code and its updates, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes, and Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions (ITE) Law. The results show that the Indonesian criminal law evidentiary system is not yet completely able to accommodate the decentralized, pseudonymous, and cross-jurisdictional characteristics of crypto assets, resulting in difficulties in identifying ownership, validating blockchain evidence, and relying on expert testimony. Furthermore, the mechanism for confiscation and confiscation of assets is also ineffective due to limited regulations regarding private key control, digital evidence management, and technical and jurisdictional barriers. Therefore, legal reform is needed by strengthening blockchain-based electronic evidence regulations, developing adaptive asset recovery mechanisms, including non-conviction-based forfeiture, and enhancing the institutional capacity of the Attorney General's Office and international cooperation. This will enable a criminal justice system that is responsive to technological developments and effective in combating crypto-asset-based money laundering.*

Keywords: *evidence, asset confiscation, crypto assets, money laundering, Attorney General's Office, criminal justice system.*

Introduction

The crypto asset phenomenon presents a new dimension to money laundering crimes in Indonesia (Habsari & Maharani, 2025). Crypto is used as a disguise and for cross-border value transfers with a high degree of anonymity (Hasan, 2024). The development of blockchain technology, which underpins crypto assets, allows criminals to disguise the origins of criminal proceeds, making them more difficult to detect than with conventional financial instruments (Amrullah, 2024). This situation poses a serious challenge for law enforcement because crypto transactions are spread globally and are not always subject to

national jurisdiction (Nasoha, 2025). These changes demonstrate that the criminal justice system must adapt to the dynamics of digital finance.

The Attorney General's Office (AGO) holds a strategic position in addressing this challenge, as it plays a central role as public prosecutor and enforcer of court decisions (Mukhtar, 2022). The success of prosecutions and the confiscation of crypto assets depends on the prosecutor's ability to prove the assets' link to money laundering crimes (Arianto, 2024). This task requires specialized competency in digital evidence and a technical understanding of blockchain technology (Kinanti, 2024). The authority held by the Prosecutor's Office, under Law No. 11 of 2022, emphasizes the prosecutor's role not only as a prosecutor but also as an enforcer of court-ordered asset confiscation decisions. This places the Prosecutor's Office at the forefront of asset recovery efforts in the digital era.

Regulatory challenges arise from the decentralized, anonymous nature of crypto assets, which allow them to move across jurisdictions without the need for traditional financial institutions (Pujisari, 2025). National regulations face limitations when crypto transactions involve foreign parties or platforms not registered in Indonesia. Institutions such as Bappebti (Commodity Futures Trading Regulatory Agency) and the Financial Services Authority (OJK) have established provisions on crypto assets, but these are limited to trading and market supervision. Meanwhile, aspects of criminal law related to evidence and confiscation still lack technical regulations. This problem creates a gap between the needs of criminal justice practice and national regulatory readiness.

The concept of money laundering, as regulated in Law No. Law No. 8 of 2010 provides a normative framework for how money or assets derived from criminal acts can be disguised and diverted (Riswanto, 2024). This provision provides a clear legal basis that crypto assets can be treated as money laundering objects when proven to be used to disguise the proceeds of crime (Limaatmaja, 2024). The "follow the money" theory is highly relevant in crypto cases because the primary focus of investigations is not solely on the perpetrator, but also on the flow of funds transformed into digital assets (Ginting, 2021). Asset recovery theory complements this perspective by emphasizing the importance of returning assets derived from crime to the state or victims (Panggabean, 2020). Thus, these two theories provide a strong conceptual foundation for the Prosecutor's Office to trace and confiscate crypto assets.

The evidentiary system in Indonesian criminal law remains based on the Criminal Procedure Code (KUHAP), specifically Article 184, which regulates the types of evidence (Darizta, 2023). Electronic evidence was not explicitly regulated at the time of the Criminal Procedure Code's (KUHAP) initial enactment, making the ITE Law crucial as a complement. Proving using digital evidence faces obstacles because it must be ensured that its authenticity, integrity, and relevance to the crime are ensured (Eugenia, 2024). Crypto assets, which exist solely as data within a blockchain system, require a progressive interpretation of the categories of valid evidence. Prosecutors must be able to construct legal arguments that convince judges that digital data from crypto transactions is worthy of being declared valid and relevant evidence.

The development of crypto assets as a medium for storing and transferring value has had serious consequences for the evidentiary system in money laundering cases in Indonesia. The blockchain-based, pseudo-anonymous nature of crypto and its lack of state

jurisdiction make the process of identifying wallet ownership a fundamental issue. (Atmojo, 2023) In criminal procedure law, the basis for proof remains the principle of judicial conviction, as stipulated in Article 183 of the Criminal Procedure Code (KUHAP), which requires at least two valid pieces of evidence. However, in both the old KUHAP and the new Criminal Procedure Code, the primary problem lies not in the quantity of evidence, but in the ability to connect legal subjects with crypto assets that are technically not tied to formal identities. (Hawasara, 2022) Pseudonymous wallet addresses create a gap between technological reality and the legal construction of evidence, so that ownership relationships are often only established through indirect analysis of transaction patterns.

The limitations of the evidentiary regime are also experiencing dynamics, but have not yet fully resolved the problem. In the previous Criminal Procedure Code, Article 184 limited evidence to five conventional types, while the current Criminal Procedure Code has begun to accommodate electronic evidence as valid evidence. It aligns with Law Number 1 of 2024 concerning Electronic Information and Transactions, which, through Article 5 paragraph (1), recognizes electronic information as legal evidence. (Lubis, 2025) However, this normative recognition does not automatically resolve the validity of blockchain transactions in judicial practice. While blockchain is immutable and transparent, interpreting such data still requires expertise, which in turn raises debates about the reliability of analysis methods, the chain of custody of digital evidence, and the potential for bias in interpreting transaction data. (Kusuma, 2025) Thus, although the new Criminal Procedure Code demonstrates normative progress, substantively, there are still gaps in the evidentiary standards for evidence based on decentralized technology.

The issue of proof becomes even more complex when linked to the cross-jurisdictional nature of crypto asset transactions. Tracing the flow of funds often involves various global entities, including exchanges not within Indonesian jurisdiction or even subject to anti-money laundering standards. In this regard, the provisions of Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU), particularly Articles 3, 4, and 5, which emphasize proving the origin of assets derived from criminal activity, are difficult to implement effectively. The use of technologies such as mixers, privacy coins, and decentralized finance (DeFi) further obscures transaction traces, making proving a causal relationship between the predicate offense and the assets problematic. (Aswadi, 2025) This creates tension between the principle of anonymity in technology and the evidentiary standard "beyond a reasonable doubt," which is not explicitly reformulated in the new Criminal Procedure Code to address the complexity of cross-jurisdictional digital evidence.

In the case of asset seizure and confiscation, the updated Criminal Procedure Code is also not fully adapted to the nature of crypto assets. Although the new Criminal Procedure Code has begun to accommodate the concept of seizure of intangible assets, technically, the mechanism is still oriented towards physical possession or direct control over the object. However, in crypto, possession is determined by access to the private key, not the physical presence of the asset. The confiscation provisions in the old Criminal Procedure Code, such as Articles 39 and 46, do not explicitly regulate the mechanism for controlling digital assets, and the updates in the new Criminal Procedure Code do not provide clear operational procedures. Consequently, in practice, the Prosecutor's Office often encounters situations

where assets have been designated as confiscated or seized, but cannot be executed due to technical obstacles such as the inability to obtain private keys, the use of cold wallets, or storage on uncooperative foreign platforms. (Nelson, 2026)

Furthermore, the management and confiscation of crypto assets also face significant legal gaps. Although Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU) provides a legal basis for the confiscation of assets derived from crime, the regulation does not specifically address the highly volatile characteristics of digital assets. The new Criminal Procedure Code (KUHAP) also lacks technical guidelines on how confiscated crypto assets should be secured, converted, or auctioned, creating the risk of state losses due to value fluctuations. Furthermore, the conceptual distinction between confiscation and forfeiture has not been clearly adopted in the Indonesian legal system, resulting in limited legal instruments for confiscating assets without having to wait for a final and binding criminal verdict. It demonstrates that criminal procedural law reform has not yet fully integrated with the needs of modern, digital-based asset recovery. (Putra, 2025)

While the updated KUHAP demonstrates efforts to adapt to technological developments, significant normative and implementation gaps remain in the handling of crypto assets derived from money laundering. The inconsistency between the new Criminal Procedure Code (KUHAP), Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU), and Law No. 1 of 2024 concerning Electronic Information and Transactions (ITE) demonstrates that the Indonesian legal system remains partial in its response to this phenomenon. This situation not only creates obstacles in establishing evidence and confiscating assets but also has the potential to undermine the effectiveness of law enforcement and create impunity for perpetrators of technology-based financial crimes. Therefore, a comprehensive and adaptive legal formulation is needed, both in establishing evidence and asset recovery, to address the challenges posed by the development of crypto assets in the Indonesian criminal justice system.

Methodology

This research employs a normative juridical method to study positive legal norms governing the provision of evidence and confiscation of crypto assets in money laundering crimes, by positioning law as a system of norms (law in books). The approaches used include a statute approach and a conceptual approach. The statutory approach examines various relevant regulations, including the Criminal Procedure Code and its updates, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering Crimes, and Law Number 1 of 2024 concerning Electronic Information and Transactions, to identify norms, principles, and regulatory disharmony related to evidence and asset recovery in the context of crypto assets. Meanwhile, the conceptual approach analyzes legal concepts such as proof, electronic evidence, anonymity, dominus litis, and asset confiscation (confiscation and forfeiture) from a doctrinal and theoretical perspective, so that comprehensive legal arguments can be found regarding the lack of norms and inconsistencies between technological developments and existing legal constructions. Thus, this research not only examines the suitability of positive legal norms but also constructs a more adaptive legal

thinking construction in addressing the problems of proving and confiscating crypto assets in the Indonesian criminal justice system.

Result and Discussion

Problems of Proving Crypto Assets in Money Laundering Crimes from the Perspective of Indonesian Criminal Procedure Law

The problem of proving crypto assets in money laundering crimes must first be placed within the framework of the Indonesian criminal procedure law's evidentiary system, which classically relies on the principle of negative statutory proof (negatief wettelijk bewijstheorie). This principle is reflected in Article 183 of the Criminal Procedure Code, which stipulates that a judge may not impose a sentence unless, based on at least two valid pieces of evidence, he or she is convinced that a crime actually occurred and that the defendant is the perpetrator. This provision is reinforced by Article 184 of the Criminal Procedure Code, which limits evidence to five types: witness testimony, expert testimony, letters, clues, and the defendant's testimony. Although the New Criminal Procedure Code has expanded the recognition of electronic evidence, conceptually, the Indonesian evidentiary system still focuses on evidence that can be sensed and directly linked to the legal subject.

In the case of decentralized technology-based crypto assets, this orientation is problematic because the relationship between the perpetrator and the asset cannot always be proven through conventional, direct evidence (Habsari & Maharani, 2025). The status of electronic evidence has indeed gained stronger normative legitimacy through Law Number 1 of 2024 concerning the Second Amendment to the ITE Law, specifically Article 5 paragraphs (1) and (2), which affirm that electronic information and/or electronic documents and their printouts constitute valid legal evidence and constitute an extension of the evidence recognized in Indonesian procedural law. However, this normative recognition does not automatically resolve the problems in the practice of providing evidence for crypto assets. Blockchain transactions are recorded permanently and are immutable, but this data only shows the flow of value between addresses without explicitly revealing the owner's identity (Harun, 2025). Therefore, even though electronic evidence has been legally recognized, the main challenge remains how to convincingly link this digital data to the defendant's legal identity within the framework of criminal evidence.

The validity and evidentiary power of blockchain transactions also pose unique challenges in judicial practice. Technically, blockchain provides full transparency of transaction history, but this transparency is pseudonymous and requires interpretation based on specialized analysis. In this case, blockchain evidence does not stand alone as perfect evidence, but must be constructed as part of "indicative" evidence as stipulated in Article 188 of the Criminal Procedure Code, or supported by expert testimony. Problems arise when evidence becomes heavily reliant on digital forensics and blockchain analytics experts, whose methodologies are not always uniform and whose scientific validity can be disputed in court (Antari, 2026). It may create legal uncertainty, as the strength of the

evidence becomes highly dependent on the judge's subjective assessment of the expert testimony.

A more fundamental problem lies in identifying crypto asset ownership, particularly in distinguishing between beneficial owners and mere address controllers. In the practice of money laundering crimes, as stipulated in Articles 3, 4, and 5 of Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU), evidence requires a link between the perpetrator and the assets derived from the crime. However, in the crypto ecosystem, an individual can control multiple wallets without formal identification or use third parties and technologies such as mixing services to disguise the origin of funds. As a result, proving ownership becomes extremely complex and is often based solely on transaction correlations, rather than direct evidence of ownership. It makes it vulnerable to challenges within the framework of criminal evidence, which demands certainty and cannot be based solely on assumptions (Rachmahdani, 2023).

In these circumstances, the role of digital forensics and blockchain analytics experts is crucial, yet problematic. On the one hand, this expertise is necessary to trace the flow of funds and link addresses to specific entities. However, on the other hand, heavy reliance on experts has the potential to shift the principle of proof from evidence-based to expert-based. Furthermore, operational standards and blockchain analysis methodologies have not been standardized nationally in the Indonesian justice system, leaving room for differing interpretations among experts. It contradicts the need for legal certainty in criminal evidence, especially when faced with the principle of "beyond a reasonable doubt," which requires the absence of reasonable doubt in criminal convictions (Hermanto, 2025).

It can be concluded that despite normative developments through updates to the Criminal Procedure Code (KUHAP) and the strengthening of the recognition of electronic evidence in Law Number 1 of 2024 concerning the Second Amendment to the ITE Law, the Indonesian criminal law evidentiary system is fundamentally not fully adaptive to the characteristics of crypto assets. The gap between legal constructions still based on conventional evidence and the decentralized and anonymous nature of technology has led to structural weaknesses in proving evidence in crypto-based money laundering (TPPU) cases. Therefore, it is necessary to reformulate the evidentiary system that not only formally recognizes electronic evidence but also develops evidentiary standards to accommodate the complexity of blockchain technology substantively and consistently in criminal justice practice.

Problems of Confiscation and Confiscation of Crypto Assets by the Prosecutor's Office in the Indonesian Criminal Justice System

The problem of confiscation and seizure of crypto assets in the Indonesian criminal justice system is fundamentally rooted in the inconsistency between conventional criminal procedural law and the non-physical, cryptographic-technology-based nature of digital assets. The confiscation mechanism in the Criminal Procedure Code, specifically Article 39 paragraph (1), stipulates that objects subject to confiscation include objects or bills suspected of being obtained from a crime or used to commit a crime. However, this norm is based on the assumption that the object of confiscation is in a form that can be physically controlled

or at least is under the direct control of law enforcement officials. In the context of crypto assets, such control is determined not by physical presence but by access to the private key, making the physical-based confiscation approach irrelevant and ineffective.

The New Criminal Procedure Code (KUHAP) has indeed attempted to expand the scope of confiscation to include intangible objects, but this regulation remains normative and lacks a clear operational mechanism for taking control of digital assets. There are no explicit provisions governing the procedures for law enforcement officials, particularly the Prosecutor's Office, to obtain, secure, and manage private keys, the primary instrument for controlling crypto assets. Consequently, in practice, situations often arise where assets have been designated as confiscated but are not actually under state control, thus failing to achieve the purpose of confiscation, which aims to secure evidence and enforce the law.

Regarding asset confiscation, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (AML) provides a strong legal basis, particularly through Articles 67 and 69, which allow for the confiscation of assets known or reasonably suspected to be the proceeds of crime. However, these provisions do not specifically address the highly volatile and cross-jurisdictional characteristics of crypto assets. Furthermore, the confiscation regime in the Money Laundering Law still relies heavily on legally binding court decisions, thus failing to fully adopt the non-conviction-based forfeiture mechanism, which, in international practice, has proven more effective in pursuing easily transferable digital assets quickly and anonymously.

Technical obstacles are also a crucial factor in the ineffectiveness of asset recovery efforts for crypto assets. Asset control relies heavily on access to private keys, which are often unknown or not provided by suspects. The use of cold wallets that are not connected to the internet, as well as the storage of assets on foreign exchanges not subject to Indonesian jurisdiction, further complicates the seizure and confiscation process. Under these circumstances, even though assets have been legally designated as objects of confiscation, the state lacks the capacity to enforce the decision. It indicates a gap between legal norms and technical realities, which impacts the ineffectiveness of law enforcement.

The Prosecutor's Office, as the institution with dominus litis authority in the criminal justice system, plays a central role in the prosecution and execution of decisions, including the implementation of asset confiscation. However, this authority is not matched by adequate technical capacity and a regulatory framework for handling crypto assets. The absence of standard operating procedures (SOPs) specifically governing the management of crypto evidence, including aspects of secure storage, value conversion, and volatility risk mitigation, creates potential state losses. Furthermore, coordination with other institutions, such as the Financial Transaction Reports and Analysis Center (PPATK) and international authorities, continues to face legal and technical challenges, hindering the optimal asset recovery process.

This situation demonstrates that existing legal mechanisms are unable to effectively accommodate the need for asset recovery for crypto assets. The limited provisions in the Criminal Procedure Code and its updates, as well as the lack of adaptation of Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU) to

developments in digital technology, create structural weaknesses in the asset forfeiture system. As a result, although there is a legal basis for seizure and confiscation, in practice, these mechanisms are often ineffective. It underscores the inability of the current legal system to address the challenges of crypto-based asset recovery, necessitating a more comprehensive and adaptive legal reformulation to technological developments.

Reformulation of the Law on Evidence and Confiscation of Crypto Assets in Money Laundering Crimes

Reformulation of the law on evidence and confiscation of crypto assets in money laundering crimes must begin with a renewal of the paradigm of criminal procedural law, which has so far focused on physical objects and conventional evidence. In this context, although the New Criminal Procedure Code (KUHAP) has begun to accommodate electronic evidence and intangible objects, strengthening norms that explicitly recognize the characteristics of blockchain technology as a stand-alone source of evidence is necessary. This reformulation can be realized by adding provisions confirming that blockchain data, including transaction hashes, wallet addresses, and ledger records, constitutes valid evidence with certain evidentiary strength as long as it can be cryptographically verified. Furthermore, it is necessary to formulate specific evidentiary standards for crypto assets that accommodate the use of circumstantial evidence based on digital transaction analysis, so that judges do not rely solely on direct evidence, which in many cases is unavailable.

The reformulation must also address the harmonization of Law Number 1 of 2024 concerning the Second Amendment to the ITE Law, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU), and criminal procedural law. In this regard, concrete steps are needed in the form of drafting implementing regulations (for example, Supreme Court Regulations or Attorney General Regulations) that provide technical guidelines for the acceptance, examination, and evaluation of blockchain-based electronic evidence in court. These guidelines should include chain-of-custody standards for digital evidence, transaction verification methods, and the qualifications and competency standards for digital forensic experts. Without such standardization, the normative recognition of electronic evidence will remain formalistic and lack certainty in judicial practice.

Regarding asset confiscation, legal reform should be directed at strengthening asset recovery mechanisms that are more adaptive to the characteristics of crypto assets. Although Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU) already regulates asset confiscation, further development is needed by adopting the concept of non-conviction-based asset forfeiture more explicitly in national law. Concrete steps that can be taken include revising or adding provisions that allow for the confiscation of crypto assets without having to wait for a final and binding criminal decision, as long as there is sufficient evidence that the assets originated from a criminal act. Furthermore, a freezing order mechanism should be established that allows for the immediate blocking of crypto assets during the investigation stage to prevent the transfer or disappearance of assets.

The reformation must also address the technical aspects of the seizure and management of crypto assets by law enforcement officials, particularly the Attorney General's Office. In this regard, the establishment of national standard operating procedures (SOPs) governing the procedures for confiscating crypto assets is necessary, including the mechanism for taking over private keys, the use of state-owned custodial wallets, and procedures for securing digital assets. Furthermore, an urgent concrete step is the establishment of a dedicated digital asset recovery unit within the Attorney General's Office, equipped with technical capabilities in blockchain analytics and digital forensics. This unit must also be supported by adequate technological infrastructure to securely store and manage crypto assets, thereby minimizing the risk of loss or misuse of seized assets.

At the institutional and international cooperation level, legal reformation must encourage strengthened coordination between the Attorney General's Office, the Financial Transaction Reports and Analysis Center (PPATK), the National Police, and international authorities. Given the cross-jurisdictional nature of crypto assets, a concrete step that needs to be taken is to expand international cooperation agreements regarding financial data exchange and law enforcement regarding digital assets, including cooperation with global cryptocurrency exchanges. In addition, Indonesia needs to adopt international standards such as those developed by the Financial Action Task Force (FATF) regarding virtual asset service providers (VASPs), so that the process of tracking and confiscating assets can be carried out more effectively and coordinated across countries.

Reformulation of the law on evidence and confiscation of crypto assets must be directed towards building an adaptive, integrative, and technology-based legal system. Concrete steps that can be taken include a more comprehensive revision of the Criminal Procedure Code (KUHAP), the establishment of specific regulations regarding digital assets in criminal law, the development of technical guidelines for law enforcement officials, and strengthening institutional capacity through training and technology investment. Without such systemic and implementable reforms, the Indonesian criminal justice system will continue to face difficulties in proving and confiscating crypto assets derived from money laundering, which will ultimately weaken the effectiveness of law enforcement and significantly harm state interests.

Conclusion

The conclusion of this study indicates that the Indonesian criminal procedure system is not yet fully adaptive to addressing the challenges of proving and confiscating crypto assets in money laundering crimes. Despite normative developments through the New Criminal Procedure Code (KUHAP) and the strengthening of the recognition of electronic evidence in Law Number 1 of 2024 concerning the Second Amendment to the ITE Law, substantively, there are still weaknesses in accommodating the decentralized, pseudonymous, and cross-jurisdictional nature of crypto assets. Limitations in identifying wallet ownership, reliance on expert testimony in proving blockchain transactions, and the lack of standardized standards for assessing digital evidence indicate a gap between legal norms and technological developments. Furthermore, the asset seizure and confiscation

mechanisms stipulated in the Criminal Procedure Code and Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU) are also ineffective in reaching crypto assets, primarily due to technical constraints such as private key control, the use of cold wallets, and limited jurisdiction over foreign platforms. This situation demonstrates the structural inability of the current legal system to support digital technology-based asset recovery.

Based on these findings, a comprehensive and implementable legal reformulation is recommended to improve the effectiveness of evidence collection and confiscation of crypto assets. Concrete steps that need to be taken include improving the provisions in the New Criminal Procedure Code by including specific provisions regarding blockchain-based evidence and digital asset confiscation, as well as harmonizing them with Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law and Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU). Furthermore, it is necessary to establish technical guidelines governing digital evidence standards, crypto evidence management, and more flexible confiscation mechanisms, including the development of the concept of non-conviction-based asset forfeiture. From an institutional perspective, the Attorney General's Office needs to strengthen its capacity by establishing a special unit for handling digital assets, improving human resource competency, and strengthening international cooperation in asset tracking and recovery. With these steps, it is hoped that the Indonesian criminal justice system will be able to adapt effectively to technological developments and increase the success of law enforcement against crypto-asset-based money laundering crimes.

The study argues that improving the Attorney General’s Office capacity in handling crypto assets requires broader institutional reform beyond establishing a specialized unit. This includes integrated procedures for crypto asset tracing, seizure, storage, and liquidation, supported by inter-agency coordination mechanisms. In addition, adequate technological infrastructure such as blockchain forensic tools, secure digital wallets, and transaction monitoring systems is necessary. Prosecutors must also develop competencies in blockchain technology, digital forensics, crypto asset valuation, and cross-border asset recovery to ensure effective and legally certain digital asset management.

References

Amrullah, M. A. (2024). Inovasi Digital dalam Bentuk Aset Kripto Sebagai Sarana untuk Melakukan Tindak Pidana Pencucian Uang. MLJ Merdeka Law Journal, 5(2), 113-125.

Antari, Y. (2026). Konstruksi Hukum Pembalikan Beban Pembuktian dalam Tindak Pidana Pencucian Uang di Era Digital. Al-Zayn: Jurnal Ilmu Sosial & Hukum, 7221-7234.

Arianto, A. F. (2024). Peran Lembaga Penegak Hukum Dalam Proses Perampasan Aset. Jurnal USM Law Review, 7(3), 1601-1615.

Aswadi, K. a. (2025). Perlindungan Hukum Aset Kripto Sebagai Objek Jaminan Berdasarkan Perspektif Hukum Jaminan. Diversi: Jurnal Hukum, 424-456.

Atmojo, R. N. (2023). Upaya perlindungan hukum bagi para konsumen pemegang aset kripto di Indonesia. Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat, 254-276.

Darizta, F. S. (2023). Barang Bukti dalam Hukum Pembuktian di Indonesia. Lex Stricta: Jurnal Ilmu Hukum, 2(2), 91-102.

Eugenia, F. L. (2024). Tantangan Praktis dalam Proses Pembuktian Perkara Pidana: Kredibilitas Saksi dan Validitas Bukti Elektronik. Iuris Studia: Jurnal Kajian Hukum, 5(2), 492-503.

Ginting, Y. P. (2021). Pemberantasan Pencucian Uang dengan Pendekatan Follow the Money dan Follow the Suspect. Mulawarman Law Review, 6(2), 105-114.

Habsari, H. T., & Maharani, N. (2025). Kripto Dalam Pusaran Tindak Pidana Pencucian Uang dan Perampasan Aset di Indonesia. Jurnal Fundamental Justice, 6(1), 51-68.

Harun, M. N. (2025). Crypto Crime: Rekonstruksi Kualifikasi Tindak Pidana Pencucian Uang dalam Era Digital Hukum Indonesia. Al-Zayn: Jurnal Ilmu Sosial & Hukum , 9520-9537.

Hasan, Z. W. (2024). Regulasi Penggunaan Teknologi Blockchain Dan Mata Uang Kripto Sebagai Tantangan Di Masa Depan Dalam Hukum Siber. Birokrasi: Jurnal Ilmu Hukum Dan Tata Negara, 2(2), 55-69.

Hawasara, W. R. (2022). Penerapan dan Kecenderungan Sistem Pembuktian yang dianut dalam KUHAP. Aksara: Jurnal Ilmu Pendidikan Nonformal, 587-594.

Hermanto, H. a. (2025). Pengaturan Penyitaan Aset Kripto sebagai Hasil Tindak Pidana Pencucian Uang di Indonesia. Jurnal Hukum Lex Generalis, 67.

Kinanti, P. M. (2024). Melintasi Era Digital Dengan Menganalisis Hukum Cryptocurrency dan Blokchain Dalam Yurisprudensi Modern. Innovative: Journal Of Social Science Research, 4(1), 920-932.

Kusuma, A. P. (2025). Validitas Digital Signature Dalam Smart Contract Terhadap Jual Beli Produk Hasil Pertanian Digital. Acten Journal Law Review, 99-116.

Limaatmaja, P. J. (2024). Aspek Pidana Terhadap Transaksi Mata Uang Kripto Yang Berpotensi Sebagai Tempat Pencucian Uang. Lex Positivis, 2(4), 511-532.

Lubis, F. K. (2025). Analisis hukum bukti elektronik sebagai alat bukti dalam pemeriksaan hukum acara perdata. JISPENDIORA Jurnal Ilmu Sosial Pendidikan Dan Humaniora, 614-626.

Mukhtar, A., Hafidz, M. R., & Said, M. F. (2022). Kedudukan Jaksa Selaku Pelaksana Mewakili Negara Dalam Sistem Peradilan Pidana. Journal of Lex Generalis (JLG), 3(4), 828-845.

Nasoha, A. M. (2025). Blockchain Kripto dan Pancasila: Kajian Hukum Internasional terhadap Perdagangan Elektronik. JDHI: Jurnal Dinamika Hukum Indonesia, 1(1), 39-48.

Nelson, J., Soekorini, N., Cornelis, V. I., & Paramitha, V. N. (2026). Aturan Legalitas Dan Kerangka Pengaturan Perlindungan Investor Aset Kripto Di Indonesia: Studi Komparasi Pengaturan Bappebti Dan Otoritas Jasa Keuangan (Ojk). COURT REVIEW: Jurnal Penelitian Hukum, 21-34.

Panggabean, D. H. (2020). Pemulihan Aset Tindak Pidana Korupsi Teori-Praktik dan Yurisprudensi di Indonesia. Jakarta: Bhuana Ilmu Populer.

Pujisari, Y. K. (2025). Pengaruh Perceived Security Dan Desentralisasi Terhadap Manfaat Finansial Pada Aset Kripto. Jurnal Ekonomi dan Bisnis, 19(2), 171-181.

Putra, R. T. (2025). Analisa pertanggungjawaban pidana atas penggunaan aset kripto sebagai sarana tindak pidana pencucian uang. PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora, 6538-6552.

Rachmahdani, J. N. (2023). Pertanggungjawaban Pidana Pelaku Pencucian Uang melalui Aset Kripto. Jurist-Diction, 64.

Riswanto, R. R. (2024). Legal Aspects In Handling Money Laundering Cases In Indonesia. Asian Journal of Social and Humanities, 2(8), 1818-1823.