International Journal of Educational Review, Law, and Social Sciences (IJERLAS)
ISSN: 2808-487X
Edition: Vol. 6 No. 4 (2026)
https://radjapublika.com/index.php/IJERLAS/index

Cryptocurrency as a Tool of Crime: An Intersectional Study of Technology, Law, and Criminology

Syamsul Hidayat*, Atika Zahra Nirmala[2], Nunung Rahmania[3]
[1,2,3]Mataram University., Indonesia
e-mail: syamsulhidayat@unram.ac.id, atikazahra@unram.ac.id, nunung_r@unram.ac.id
*syamsulhidayat@unram.ac.id

Keywords:
Cryptocurrency;
Criminology;
Money Laundering;
Law Enforcement;

Article Info:
Received:
06/05/2025
Revised:
20/05/2025
Accepted:
26/06/2025
Published:
30/07/2025

ABSTRACT

Cryptocurrency has developed as a rapidly growing financial innovation, but it also gives rise to serious challenges, particularly the increase in crimes such as money laundering. Its decentralized, pseudonymous, and borderless characteristics make it difficult for law enforcement authorities to trace illegal transactions and highlight a gap between technological advancement and regulatory readiness. Based on this issue, this study raises the following questions: (1) how is cryptocurrency used in money laundering mechanisms, (2) how is it regulated in Indonesia, and (3) how do technology, law, and criminology intersect in addressing this issue. This study aims to analyze these three aspects comprehensively. This research employs a normative juridical method with statutory, conceptual, and case approaches, utilizing primary and secondary legal materials obtained through library research and analyzed using a descriptive qualitative method. The findings show that cryptocurrency is used in money laundering through the stages of placement, layering, and integration, with increasingly complex methods based on digital technology. Addressing this issue requires an interdisciplinary synergy, where technologies such as blockchain forensics and artificial intelligence assist in tracing transactions, law provides the normative framework and enforcement mechanisms, and criminology explains offender motives and behavioral patterns. However, the regulatory framework in Indonesia remains partial and not fully adaptive to the development of digital assets. The academic contribution of this study lies in strengthening the interdisciplinary approach as a basis for more adaptive policymaking, as well as providing recommendations for regulatory improvement, enhancing law enforcement capacity, and developing more effective preventive strategies in addressing cryptocurrency-based money laundering.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)

How to cite:
DOI: https://doi.org/10.54443/ijerlas.v6i4.5647

Introduction

The development of information and communication technology has had a significant impact on various sectors, including finance and investment, particularly in the area of cryptocurrency. Cryptocurrency, as a form of digital currency, utilizes blockchain technology a digital ledger that records all transactions transparently and immutably thereby providing a high level of security (Usman et al., 2022). Cryptocurrency has emerged as a financial innovation that not only offers an alternative to traditional transactions but also creates new opportunities in investment and asset management. Blockchain technology enables greater transparency and security in transactions, which is one of the main reasons why cryptocurrency has become increasingly popular among investors and users(Dwi Lestari, 2023). One of the key characteristics of cryptocurrency is its decentralization, meaning that there is no central authority, such as a bank or government, that regulates or controls it. In addition, an important aspect of technological advancement related to cryptocurrency is the ease of access and use of digital technology. Through mobile

applications and web-based platforms, users can easily conduct cryptocurrency transactions, monitor asset values, and participate in global markets without geographical limitations.

Overall, the relationship between technological development and cryptocurrency demonstrates that technological innovation can create new opportunities in the financial sector, but also brings challenges that must be addressed, including its use as a tool for crime. The growing popularity of cryptocurrency has been directly proportional to the increase in criminal activities, where offenders use digital currencies to conceal their transaction trails (Kethineni & Cao, 2019). Numerous reports indicate that cryptocurrency is frequently used in various crimes, including money laundering (hereinafter referred to as TPPU).

In Indonesia, for instance, a report by the Financial Transaction Reports and Analysis Center (PPATK) revealed the successful uncovering of money laundering offenses conducted through crypto assets. During the period of 2022–2024, this financial intelligence agency identified suspicious crypto transactions amounting to IDR 800 billion(Rosseno Aji Nugroho, 2024). This development undoubtedly presents new challenges for law enforcement in tracing and regulating the use of such digital assets(Japinye, 2024).

To date, many countries are still striving to formulate appropriate legal frameworks to regulate the use of cryptocurrency. The resulting legal uncertainty not only complicates law enforcement processes (Dhali et al., 2023), but also creates opportunities for criminals to exploit systemic weaknesses, particularly in money laundering practices. Without clear and adaptive regulations, the cross-border, fast, and relatively untraceable nature of cryptocurrency further increases the risk of its misuse as a means of disguising illicit proceeds. Therefore, the development of a comprehensive regulatory framework has become an urgent necessity to mitigate these risks (Huey, 2024).

In a global context, these challenges cannot be addressed in a partial manner. Cooperation among states and international institutions is required to develop effective strategies to prevent and combat cryptocurrency-based crimes(Uzougbo, 2024). A collaborative and integrated approach is essential to ensure that enforcement efforts are not hindered by jurisdictional differences, while also safeguarding economic stability and public security on a broader scale.

However, in many studies, discussions on cryptocurrency remain fragmented. Some view it primarily as a technological innovation, while others treat it mainly as an object of regulation. Studies that specifically examine how legal norms particularly within the anti-money laundering (TPPU) regime interact with the characteristics of cryptocurrency are still relatively limited. In fact, this is precisely where the issue becomes critical, as technological developments often outpace the legal frameworks intended to regulate them.

On the other hand, although the discourse on the importance of interdisciplinary approaches is gaining traction, the integration of technological, legal, and criminological perspectives has not been fully realized in practice. As a result, a comprehensive understanding of the patterns and mechanisms of cryptocurrency-based crimes has yet to be achieved. In reality, technology not only functions as a tool but also shapes the methods and strategies employed by offenders.

Given these conditions, an interdisciplinary approach is nec essary to examine cryptocurrency based money laundering more comprehensively. Cryptocurrency should not be viewed merely as a financial innovation, nor should money laundering be seen solely as a conventional crime; rather, both should be understood as interconnected phenomena that generate new dynamics in modern criminal practices. In this context, criminological perspectives are essential to explain the motives, rationality, and behavioral patterns of offenders who utilize cryptocurrency as a means of laundering illicit funds.

Accordingly, the analysis should not be confined to normative aspects alone, but must also consider the evolving empirical realities of crime. From this perspective, the discussion is directed toward examining the mechanisms of money laundering through cryptocurrency, while also assessing the extent to which existing regulations are capable of addressing these challenges. The integration of technology, law, and criminology is expected to provide a more comprehensive understanding, as well as a foundation for developing more adaptive, responsive, and sustainable legal policies in addressing cryptocurrency-based crimes.

Method

This study is a normative juridical research aimed at examining the use of cryptocurrency in money laundering (TPPU), the existing regulatory framework, and the interrelationship between technology, law, and criminology in understanding cryptocurrency as a means of committing TPPU. The approaches employed in this research include the statutory approach, conceptual approach, and case approach. The statutory approach is used

to analyze laws and regulations related to TPPU and cryptocurrency, while the conceptual approach is applied to examine and understand the concept of cryptocurrency-based money laundering. Meanwhile, the case approach is used to study concrete cases or legal decisions in order to understand how legal norms are applied in practice. The legal materials used in this study consist of primary and secondary sources. Primary legal materials are derived from legislation governing TPPU and cryptocurrency, whereas secondary legal materials are obtained from relevant literature, including academic writings, journal articles, and opinions of scholars and practitioners. To obtain clear and accurate information in accordance with the research questions, data collection is conducted through document study by reviewing both primary and secondary legal materials. All collected materials are then inventoried, classified, and analyzed using a descriptive analytical method. This analysis aims to explain various legal issues, thereby identifying the forms of cryptocurrency use in TPPU, the applicable regulatory framework, and the interconnection between technology, law, and criminology in understanding cryptocurrency as a means of money laundering.

Results and Discussion

Transformation of Money Laundering Schemes from Conventional to Cryptocurrency-Based

The use of cryptocurrency in money laundering (TPPU) has become a serious concern for academics and regulators across various countries. The decentralized nature and the degree of anonymity inherent in blockchain technology create strategic loopholes that are often exploited by offenders to obscure the trail of illicit funds. This phenomenon is reinforced by numerous studies indicating an increasing trend in the use of crypto assets within money laundering schemes, thereby underscoring the urgency of strengthening regulatory frameworks to prevent the misuse of digital technology for illegal purposes (Albrecht et al., 2019).

In the context of law enforcement in Indonesia, this dynamic is clearly reflected in Decision Number 2009/K/Pid.Sus/2023 in the case of Indra Kesuma, also known as Indra Kenz. The ruling reveals that cryptocurrency was not merely a supplementary instrument but a systematic component in the modus operandi of money laundering. Proceeds from binary options investment fraud were not only deposited within conventional banking systems but were also transferred to crypto asset trading platforms, consolidated across multiple digital wallets, and eventually converted back into fiat currency. The movement of funds involving personal accounts, family members, and third parties was deliberately structured to disrupt audit trails and create the illusion of legitimacy over funds that were, in fact, derived from illegal activities.

Furthermore, funds that have undergone such concealment processes are subsequently integrated into the legal economy through the acquisition of high-value assets, either under individual ownership or through formally registered business entities. This pattern demonstrates that the use of cryptocurrency in money laundering does not operate in isolation, but rather functions in a symbiotic integration with conventional financial infrastructure. The combination of transaction speed, cross-border capability, and asset conversion flexibility makes blockchain technology a reinforcing factor that enhances the effectiveness of the final stage in money laundering schemes.

Based on the above discussion, it can be concluded that although cryptocurrency-based money laundering schemes fundamentally still follow the classic stages of placement, layering, and integration, digital transformation has significantly increased their technical complexity and the challenges of investigation. Therefore, the subsequent analysis will systematically elaborate on how these three stages are operationalized within the context of crypto assets, with a particular focus on evolving modus operandi amid the dynamics of the digital economy.

Mechanism of Cryptocurrency Use in Money Laundering

a. Placement

The placement phase represents the initial stage in the money laundering scheme, in which proceeds of crime are introduced into formal or informal financial systems. In the context of cryptocurrency, placement is generally carried out by converting cash or untraceable assets into crypto assets through less-regulated exchange platforms or through cryptocurrency automated teller machines (ATMs) (Albrecht et al., 2019). Offenders also frequently utilize mixer or tumbler services that function to blend funds from multiple sources in order to obscure their origin. As noted by Antonopoulos, this mechanism is effective in concealing the identity of perpetrators while minimizing the risk of detection by financial authorities(Grabowski, 2024). A similar pattern was identified in the case of Indra Kesuma, also known as Indra Kenz, where proceeds from binary options investment fraud were placed into various bank accounts under personal and third-party names, including Bank BCA, Bank Jago, Bank Permata, Bank Mandiri, and Bank BNI. In addition to the banking system, the funds were also transferred to crypto asset trading platform accounts (Indodax) registered under the names Indra Kesuma and Nathania Kesuma. The conversion of

illicit proceeds into crypto assets through such platforms essentially constitutes a form of placement aimed at breaking the initial audit trail and complicating law enforcement tracing efforts.

b. Layering

The layering phase is the second stage, aimed at complicating the audit trail through a series of complex and layered transactions. Within the crypto asset ecosystem, this is implemented through repeated exchanges between digital assets, transferring funds to digital wallets located in jurisdictions with weak regulatory regimes, and utilizing smart contracts within blockchain networks(Mehta & Chawla, 2024). A study by Zohar confirms that blockchain architecture provides a layer of technical anonymity that allows offenders to conduct transactions without revealing their true identities, thereby making publicly recorded blockchain transactions increasingly difficult for law enforcement authorities to trace(Al-Tawil, 2022). This modus operandi is also reflected in the Indra Kesuma case, where the perpetrator concealed the origin of funds through a chain of transfers to multiple accounts belonging to family members and business associates. This structuring of funds was deliberately designed to avoid reporting thresholds and hinder forensic analysis by financial intelligence authorities. Furthermore, Indra Kesuma converted illicit proceeds into crypto assets such as Bitcoin and Ethereum, transferred them across multiple digital wallets, and later reconverted them into fiat currency through local bank accounts. This series of conversions and transfers legally fulfills the elements of the layering stage, which functions to sever the traceability chain. Additionally, part of the funds that had undergone digital obfuscation began to be directed toward the acquisition of tangible assets, such as vehicles and luxury goods, as an initial step in disguising their legal status before full integration into the formal economy.

c. Integration

The integration phase constitutes the final stage in the money laundering cycle, in which funds that have undergone concealment are reintroduced into the legal economy so that they appear to originate from legitimate sources. In the crypto asset ecosystem, integration is typically carried out by converting "cleaned" digital assets into fiat currency, which is then channeled into official bank accounts or invested in conventional financial instruments. To reinforce the appearance of legality, offenders often establish shell companies or utilize formally registered business entities as channels for fund distribution(Teichmann & Falker, 2020). Research by Chaum and Golle emphasizes that offenders tend to exploit blockchain-based financial infrastructure to design more structured and audit-resistant laundering mechanisms(Leuprecht et al., 2022). This pattern is empirically reflected in the Indra Kesuma case, where funds converted from crypto assets were used to acquire high-value tangible assets, such as luxury vehicles including the Tesla Model 3, Ferrari California, Toyota GR Supra, and Lamborghini Huracán. These purchases were conducted either under personal ownership or through legally operating corporate entities.

From a juridical perspective, the use of legal entities as repositories for such funds serves to sever the direct link between the perpetrator and the illicit source of funds, while simultaneously constructing a façade of legitimate economic activity before the public and supervisory authorities. Thus, the integration stage in this case does not merely involve transforming the form of assets, but also consolidates a form of pseudo-legitimacy over wealth derived from criminal acts, thereby completing the money laundering cycle as a whole.

Based on the previous discussion, there are substantive differences between money laundering (TPPU) involving cryptocurrency and conventional money laundering. These differences primarily lie in the instruments used, the complexity of the modus operandi, and the level of difficulty in tracing and law enforcement. As a basis for comparison, conventional money laundering mechanisms generally adhere to the following three classical stages:

a) Placement

The initial stage in which proceeds of crime are introduced into the formal financial system. Common methods include depositing cash into bank accounts or purchasing valuable assets (Daud & Putra Jaya, 2022). This phase carries the highest risk of detection, as unverified fund flows are vulnerable to identification through mandatory reporting systems and financial supervisory authorities(Usman & Surono, 2024) .

b) Layering

This stage involves a series of complex and layered transactions aimed at obscuring the audit trail and severing the connection between the funds and their original source(Paramitha et al., 2024). Instruments used include inter-account transfers, circulation of financial instruments, and the establishment of shell companies in foreign jurisdictions to create a façade of legitimate business activity. The use of information technology and digital banking systems at this stage plays a strategic role in accelerating fund transfers while simultaneously complicating efforts by law enforcement to reconstruct the flow of funds(Radiyah & Fithry, 2024).

c) Integration

The final phase, in which funds that have undergone concealment are reintroduced into the legal economy, making them appear to originate from legitimate sources. Offenders typically invest these funds in the property sector, commercial enterprises, or other investment instruments to consolidate wealth and disguise the illicit origin of the funds(Suparman, 2019). The success of this stage largely depends on the offender's ability to avoid early detection by anti-money laundering authorities, such as the Financial Transaction Reports and Analysis Center (PPATK), as well as competent law enforcement agencies (Adhar, 2020).

To support a more structured comparative analysis, the fundamental differences at each stage of money laundering are summarized in Table 1 below.

Table 1. Comparison of Money Laundering Mechanisms: Crypto Asset-Based vs. Conventional

Aspect	**Crypto Asset-Based Money Laundering**	**Conventional Money Laundering**
Main Instruments	Cryptocurrencies (e.g., Bitcoin, Ethereum), digital wallets, crypto asset exchange platforms, mixers/tumblers	Cash, bank accounts, traditional financial instruments (stocks, bonds), tangible assets
Transaction Characteristics	Decentralized, cross-border, pseudonymous, 24/7 transactions without bank intermediaries	Centralized through financial institutions, requires formal identification, limited to banking hours
Placement	Purchase of crypto assets through unregulated exchanges, crypto ATMs, conversion of cash into digital assets using mixers	Cash deposits into bank accounts, purchase of traveler's checks, acquisition of gold or other valuable assets
Layering	Exchange between crypto assets, transfers to digital wallets across jurisdictions, use of smart contracts, layered transactions via blockchain	Transfers between bank accounts, repeated buying and selling of financial instruments, use of shell companies abroad
Integration	Conversion of crypto assets into fiat currency, investment in digital or physical assets, purchase of luxury goods via crypto-accepting platforms	Investment in real estate, legitimate businesses, acquisition of tangible assets (vehicles, art), placement of funds in banking investment products
Level of Anonymity	High (pseudonymous via wallet addresses, although transactions are recorded on public blockchains)	Low to moderate (linked to formal identity through banking Know Your Customer/KYC systems)
Transaction Speed	Very fast (minutes to hours), without geographical limitations	Relatively slow (hours to business days), depending on clearing systems and cross-border regulations

Based on the comparative synthesis in Table 1, there is a significant structural shift between conventional money laundering modus operandi and those utilizing cryptocurrency. Conventional mechanisms rely on centralized financial infrastructure that leaves verifiable administrative trails, allowing the tracing of fund flows through banking records and standard legal procedures. In contrast, crypto-based practices optimize the characteristics of decentralization, cross-border transaction speed, and pseudonymity to complicate every stage of the laundering process.

From placement through non-regulated platforms, layering that employs techniques such as chain hopping and fund-mixing services, to integration that blurs the boundary between digital assets and the real economy, the entire process is designed to disrupt the audit trail. The direct implication of this distinction

is an escalation in tracing challenges, where authorities can no longer rely solely on financial institution reporting. Instead, they are required to develop capabilities in blockchain forensics, possess technical understanding of decentralized network architectures, and establish legal coordination mechanisms capable of keeping pace with real-time digital transactions.

The Position and Regulatory Challenges of Cryptocurrency in Indonesian Positive Law

Within the framework of Indonesian positive law, cryptocurrency occupies a dual position. From the perspective of the payment system, cryptocurrency is not recognized as a legal means of payment. This is affirmed in Law Number 7 of 2011 on Currency, which stipulates that the Rupiah is the sole legal tender within the territory of the Republic of Indonesia. This provision is further reinforced by several Bank Indonesia Regulations, including PBI Number 18/40/PBI/2016, PBI Number 19/12/PBI/2017, and PBI Number 20/6/PBI/2018, which prohibit the use of virtual currency in payment systems. However, from a trade perspective, the government recognizes cryptocurrency as a digital commodity. Through Minister of Trade Regulation Number 99 of 2018 and Bappebti Regulations Number 5 of 2019 and Number 7 of 2020, crypto assets are classified as commodities that can be traded on futures exchanges. Consequently, cryptocurrency is positioned as a legitimate investment instrument within the trading regime, although its use as a means of payment remains legally prohibited.

This dualistic regulatory framework has implications for the regime of prevention and eradication of money laundering (TPPU). In general, anti-money laundering regulation in Indonesia is based on Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering (UU PPTPPU), which serves as the primary legal foundation for preventing, detecting, and prosecuting money laundering practices. This law adopts a broad concept of "assets," which, normatively, can encompass digital assets, including cryptocurrency. Nevertheless, the UU PPTPPU does not explicitly regulate cryptocurrency as an object of money laundering offenses. The absence of specific provisions creates several challenges, particularly in terms of evidentiary processes, transaction tracing (follow the money), and asset seizure. This is largely due to the characteristics of cryptocurrency decentralized, cross-jurisdictional, and pseudonymous which do not fully align with conventional approaches within traditional financial systems.

Furthermore, the preventive mechanisms under the UU PPTPPU still rely heavily on the Know Your Customer (KYC) principle and reporting obligations imposed on financial service institutions. While this approach is relatively effective within conventional banking systems, it faces limitations when applied to the cryptocurrency ecosystem, which does not always involve centralized authorities or regulated intermediaries. On the other hand, regulations issued by Bappebti primarily focus on trading aspects and investor protection in crypto asset transactions, and thus do not comprehensively address anti-money laundering concerns. This condition creates opportunities for the misuse of cryptocurrency as a medium for disguising proceeds of crime.

Additional challenges arise in the area of law enforcement, particularly regarding the seizure and management of crypto assets. To date, there are no detailed technical guidelines concerning the safeguarding of private keys, storage mechanisms, or procedures for auctioning crypto assets. This regulatory gap has the potential to generate legal uncertainty in practice. Therefore, while the regulation of cryptocurrency use in money laundering in Indonesia is generally grounded in the UU PPTPPU, it remains normative and lacks specificity. Existing sectoral regulations also tend to be fragmented across monetary, trade, and law enforcement regimes. Accordingly, regulatory harmonization and strengthening are required to specifically accommodate the characteristics of cryptocurrency, so that efforts to prevent and combat money laundering can be carried out more effectively.

The Intersection of Technology, Law, and Criminology in Addressing Cryptocurrency-Based Money Laundering

a. Technological Perspective

The use of technology, particularly cryptocurrency, has become a critical concern in global efforts to combat money laundering (TPPU). The decentralized and pseudonymous nature of cryptocurrency often makes it difficult for law enforcement authorities to trace the source and movement of illicit funds. This condition highlights the need for more advanced monitoring systems as well as legal frameworks capable of adapting to technological developments (Kurniawan et al., 2024). One emerging approach is blockchain forensics, which involves analyzing transactions within blockchain networks to trace the flow of funds.

Through this technique, investigators can map the transfer of assets from one wallet to another, ultimately leading to the identification of involved parties(Narasimhan & Kala, 2025). Furthermore, Regina (Regina, 2025)proposes a framework that integrates on-chain and off-chain analysis to ensure that investigative processes maintain legal legitimacy.

In addition, the use of artificial intelligence (AI) and machine learning further enhances the effectiveness of investigations. Intelligent algorithms are capable of detecting suspicious transaction patterns, analyzing large volumes of data, and identifying anomalies that are often overlooked by conventional methods, thereby accelerating the detection of cryptocurrency-based money laundering practices (Ruiz & Angelis, 2021). Nevertheless, Indonesia still faces challenges in terms of human resources in enforcing technology-based financial crimes. The availability of experts in digital forensics remains limited, while the complexity of crimes involving digital technologies, including cryptocurrency, continues to grow. This condition reflects a capacity gap among law enforcement authorities in conducting tracking, evidentiary processes, and the safeguarding of digital assets. Therefore, capacity building through competency development and technical training is essential to ensure that anti-money laundering enforcement can adapt to the dynamics of modern financial crime.

b. Legal Perspective

Law functions as a normative framework that not only interprets and regulates, but also provides the basis of legitimacy for addressing crimes related to the use of cryptocurrency. In the Indonesian context, the regulation of money laundering (TPPU) is grounded in Law Number 8 of 2010 on the Prevention and Eradication of Money Laundering, which serves as the primary instrument for both prevention and enforcement. Although this law provides a broad legal foundation through the concept of "assets," the regulation of cryptocurrency as both a means and an object of money laundering has not yet been explicitly and comprehensively formulated. The absence of specific provisions creates legal uncertainty in addressing cyber laundering, namely money laundering practices that utilize crypto assets to disguise the origin of illicit funds.

Furthermore, Law Number 8 of 2010 does not explicitly regulate crucial technical aspects, such as mechanisms for transaction tracing, procedures for the seizure of digital assets, and the management and recovery of assets derived from cryptocurrency-based crimes. This regulatory gap directly affects law enforcement practices, particularly in evidentiary processes and execution, which often encounter obstacles due to the complex and cross-jurisdictional nature of the technology. Therefore, although the existing legal framework provides a general normative basis, there remains a need to strengthen regulations in a more specific and operational manner to effectively respond to the dynamics of cryptocurrency-based financial crimes. Without such regulatory development, the law risks lagging behind technological advancements that are increasingly exploited by offenders.

c. Criminological Perspective

Criminology plays an important role in providing an understanding of the motives, patterns, and behavior of perpetrators of money laundering (TPPU) who utilize cryptocurrency. The selection of crypto assets by offenders is generally based on their characteristics, which offer a certain level of anonymity, ease in the layering process, and limited oversight. In this context, theoretical approaches such as Rational Choice Theory (RCT) and Routine Activity Theory (RAT) can be used to analyze these tendencies, so that countermeasures are not merely technical, but also address the behavioral and motivational aspects of offenders. RCT explains that individuals make decisions based on rational considerations of costs and benefits(Mehlkop & Graeff, 2010). Sastrawati (Sastrawati, 2020) emphasizes that every social action, including economic activities, is influenced by subjective evaluations of gains and costs. In the context of cryptocurrency, this theory helps explain investment and transaction decisions based on considerations of risk, cost, and potential profit (Abdeldayem & Aldulaimi, 2023). In addition, such decisions are also influenced by behavioral, financial, and social factors. Through the Technology Acceptance Model (TAM), individuals assess the benefits of using cryptocurrency compared to other instruments, reflecting a rational dimension as explained in RCT (Liaqut & Siddiqui, 2021). Nevertheless, some criticisms argue that RCT tends to oversimplify the complexity of human behavior, and therefore should be combined with social and institutional factors to achieve a more comprehensive analysis(Radovanović, 2019). Despite this, RCT remains relevant in explaining individual decision-making processes in the use and investment of cryptocurrency.

As an empirical illustration, the case of Indra Kesuma alias Indra Kenz in Decision Number 2009/K/Pid.Sus/2023 demonstrates the relevance of RCT in explaining cryptocurrency-based money laundering. The use of cryptocurrency in this case was not incidental, but rather part of an integrated strategy within the laundering scheme. The selection of crypto assets reflects the offender's awareness of blockchain technology characteristics, such as transaction speed, cross-border flexibility, and relative anonymity. From the perspective of RCT, this action indicates a rational calculation between potential economic gains and legal risks. The offender exploited perceived weak oversight and limited enforcement capacity as part of this rational consideration. The pattern of conduct also reflects the classical stages of money laundering, where illicit funds are transferred, fragmented, and converted into crypto assets to complicate tracing. This layering stage was carried out through digital platforms that do not fully implement strict monitoring standards, illustrating the exploitation of regulatory gaps as part of the criminal strategy.

On the other hand, RAT emphasizes that crime occurs due to the convergence of three elements: a motivated offender, a suitable target, and weak guardianship (Drawve et al., 2017). In cryptocurrency-based money laundering practices, offenders are driven by high potential profits with relatively low risk, while taking advantage of anonymity and ease of cross-platform transactions without central authority involvement(Jackon, 2024). Activities such as using platforms with weak oversight, conducting repeated small-value transactions to avoid detection, and utilizing certain networks create opportunities for crime. By understanding these patterns, RAT can serve as a basis for formulating more effective prevention strategies, particularly through strengthening supervision and regulation. From the perspective of RAT, the Indra Kenz case also demonstrates the presence of these three elements: a motivated offender seeking substantial profit, a suitable target in the form of illicit funds easily convertible into crypto assets, and weak oversight due to regulatory limitations and the characteristics of cryptocurrency technology. This situation creates a conducive environment for cryptocurrency-based money laundering. It further confirms that the use of cryptocurrency is not merely a technological issue, but also reflects the adaptive behavior of offenders in response to the dynamics of law enforcement.

Based on the foregoing, the intersection of technology, law, and criminology in addressing cryptocurrency-based money laundering (TPPU) should not be understood merely as a complementary relationship, but rather as an integrated system that operates simultaneously and in an interlocking manner. Each component has a distinct function, yet each also determines the effectiveness of the others. From a technological perspective, capabilities such as blockchain forensics and artificial intelligence based analysis provide data and digital traces that form the initial foundation for uncovering criminal activities. However, such data holds no legal significance unless it can be translated into admissible standards of proof. At this point, law functions as a mechanism of legitimacy, determining whether the results of technological analysis can be recognized as evidence and used for asset seizure.

Conversely, legal frameworks that are not supported by technology face serious limitations, particularly in dealing with the complex, pseudonymous, and cross-jurisdictional nature of cryptocurrency transactions. In such circumstances, legal norms risk becoming operationally ineffective, as they are unable to keep pace with the evolving modalities of digital crime. Meanwhile, the criminological perspective through Rational Choice Theory (RCT) and Routine Activity Theory (RAT) adds a deeper dimension by explaining why and how offenders utilize cryptocurrency. This analysis is crucial, because without understanding the rationality and behavioral patterns of offenders, law enforcement efforts remain merely reactive. Criminology enables a shift from a repressive approach toward risk-based preventive strategies, such as identifying vulnerable nodes within the crypto transaction ecosystem.

Thus, an ideal interdisciplinary synthesis is not merely integrative, but functionally synchronized:

a. Technology acts as the enabler of detection (identification and tracing);
b. Law serves as the enforcer of legitimacy (normative grounding and enforcement);
c. Criminology functions as the predictor of behavior (pattern recognition and crime prevention).

When these three elements are not aligned, imbalances emerge: technology without legal backing produces unusable evidence; law without technological support becomes ineffective; and both, without criminological insight, fail to anticipate the evolution of crime. Therefore, the policy direction for addressing cryptocurrency-based money laundering must move toward an adaptive integration model that not only strengthens regulatory frameworks and technical capacity, but also develops criminology-based intelligence approaches. This model enables the state not only to respond to crimes that have already occurred, but also to anticipate and prevent them in line with the evolving dynamics of digital financial technology.

Conclusion

The use of cryptocurrency in money laundering (TPPU) presents new challenges due to its decentralized, pseudonymous, and cross-border nature. Although it still follows the classic stages of placement, layering, and integration, cryptocurrency-based money laundering is more complex as it leverages technologies such as blockchain, mixers, and decentralized exchanges to obscure the origin of illicit funds. The regulatory framework in Indonesia, including the Anti-Money Laundering Law, Bank Indonesia regulations, and Bappebti policies, remains fragmented and not fully adaptive to the development of digital assets. This condition is further exacerbated by limited law enforcement capacity and the cross-jurisdictional nature of crypto transactions. Therefore, addressing cryptocurrency-based money laundering requires an integrated and adaptive approach. From a technological perspective, the use of blockchain forensics, artificial intelligence, and machine learning plays a crucial role in detecting and tracing illicit financial flows. From a legal perspective, regulatory strengthening is necessary to explicitly accommodate digital assets, including mechanisms for tracing, seizure, and asset management. Meanwhile, from a criminological perspective, understanding offender motives and behavioral patterns through Rational Choice Theory and Routine Activity Theory enables the formulation of more targeted prevention strategies.Thus, the intersection of technology, law, and criminology becomes essential in building an effective anti-money laundering framework. This approach not only strengthens repressive law enforcement measures but also promotes preventive strategies capable of anticipating the evolving nature of cryptocurrency-based financial crimes in a sustainable manner.

Acknowledgement

The author expresses sincere appreciation and gratitude to the Institute for Research and Community Service of the University of Mataram (LPPM UNRAM) for the financial support provided through the PNBP grant, which enabled this research to be conducted successfully. This support has been instrumental in facilitating the entire research process and the completion of this publication.

Author Contributions Statement

SH served as the principal investigator and research chair, responsible for conceptualization, research design, supervision, and final approval of the manuscript. AZN contributed to data collection, literature review, data analysis, and drafting of the manuscript. NR contributed to data analysis, literature review, and manuscript editing. All authors have read and approved the final version of the manuscript and agree to be accountable for all aspects of the work

AI Usage Statement

The authors declare that Artificial Intelligence (AI) tools were used solely for language editing, grammar checking, translation, and improving clarity and readability of the manuscript. AI was not used to generate research ideas, conduct data analysis, interpret findings, or draw conclusions. All intellectual content, analysis, and academic arguments remain the full responsibility of the authors. The authors confirm that the manuscript complies with academic integrity standards, and AI tools are not listed as authors or contributors.

Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

References

Abdeldayem, M. M., & Aldulaimi, S. H. (2023). Investment Decisions Determinants in the GCC Cryptocurrency Market: A Behavioural Finance Perspective. *International Journal of Organizational Analysis*. https://doi.org/10.1108/ijoa-02-2023-3623

Adhar, A. (2020). Analisis Fungsi Ppatk Dalam Pencegahan Dan Pemberantasan Tindak Pidana Pencucian Uang. *Jihad Jurnal Ilmu Hukum Dan Administrasi*. https://doi.org/10.58258/jihad.v2i1.1107

Al-Tawil, T. N. (2022). Anti-Money Laundering Regulation of Cryptocurrency: UAE and Global Approaches. *Journal of Money Laundering Control*. https://doi.org/10.1108/jmlc-07-2022-0109

Albrecht, C., Duffin, K. M., Hawkins, S. R., & Morales-Rocha, V. (2019). The Use of Cryptocurrencies in the Money Laundering Process. *Journal of Money Laundering Control*. https://doi.org/10.1108/jmlc-12-2017-0074

Daud, B. S., & Putra Jaya, N. S. (2022). Kebijakan Hukum Pidana Dalam Tindak Pidana Pencucian Uang Di Pasar Modal. *Journal of Judicial Review*. https://doi.org/10.37253/jjr.v24i1.5953

Dhali, M., Hassan, S., Mehar, S. M., Shahzad, K., & Zaman, F. (2023). Cryptocurrency in the Darknet: Sustainability of the Current National Legislation. *International Journal of Law and Management*. https://doi.org/10.1108/ijlma-09-2022-0206

Drawve, G., Thomas, S. A., & Hart, T. C. (2017). Routine Activity Theory and the Likelihood of Arrest: A Replication and Extension With Conjunctive Methods. *Journal of Contemporary Criminal Justice*. https://doi.org/10.1177/1043986216689747

Dwi Lestari, A. A. (2023). Peran Teknologi Dalam Perubahan Bisnis Di Era Globalisasi. *Syntax Literate Jurnal Ilmiah Indonesia*. https://doi.org/10.36418/syntax-literate.v7i11.13517

Grabowski, M. (2024). Account Information and Payment Initiation Services and the Related AML Obligations in the Law of the European Union. *Fintech*. https://doi.org/10.3390/fintech3010011

Huey, Y. C. (2024). Text Analytics on Regulation of Cryptocurrency. *Kne Social Sciences*. https://doi.org/10.18502/kss.v9i14.16140

Jackon, G. (2024). Cryptocurrency Adoption in Traditional Financial Markets in the United States. *American Journal of Finance*. https://doi.org/10.47672/ajf.1810

Japinye, A. O. (2024). Integrating Machine Learning in Anti-Money Laundering Through Crypto: A Comprehensive Performance Review. *European Journal of Accounting Auditing and Finance Research*. https://doi.org/10.37745/ejaafr.2013/vol12n45480

Kethineni, S., & Cao, Y. (2019). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*. https://doi.org/10.1177/1057567719827051

Kurniawan, W. R., Hadiyanto, A., & Ciptono, C. (2024). Tindak Pidana Perdagangan Orang Dalam Perspektif Tindak Pidana Pencucian Uang Di Indonesia. *Jurnal Usm Law Review*. https://doi.org/10.26623/julr.v7i2.8900

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual Money Laundering: Policy Implications of the Proliferation in the Illicit Use of Cryptocurrency. *Journal of Financial Crime*. https://doi.org/10.1108/jfc-07-2022-0161

Liaqut, S., & Siddiqui, A. (2021). Crypto Currency Cognizance: A New Entrant in Financial Heaven. *Kiet Journal of Computing and Information Sciences*. https://doi.org/10.51153/kjcis.v4i2.71

Mehlkop, G., & Graeff, P. (2010). Modelling a Rational Choice Theory of Criminal Action: Subjective Expected Utilities, Norms, and Interactions. *Rationality and Society*. https://doi.org/10.1177/1043463110364730

Mehta, K., & Chawla, S. (2024). Illuminating the Dark Corners: A Qualitative Examination of Cryptocurrency's Risk. *Digital Policy Regulation and Governance*. https://doi.org/10.1108/dprg-10-2023-0147

Narasimhan, P., & Kala, N. (2025). Emerging Trends in Digital Forensics : Investigating Cybercrime. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*. https://doi.org/10.32628/cseit251451

Paramitha, A. F., Arimbi, Y. D., Riyanto, S., Apriani, N. F., & Akbar Siagian, A. H. (2024). Classification of Suspicious Financial Transactions Using Light Gradient Boosting Machine Method (LGBM) Based on Social Network Analysis (SNA) Indicators. *Sistemasi*. https://doi.org/10.32520/stmsi.v13i2.3273

Radiyah, A. N., & Fithry, A. (2024). Kejahatan Keuangan Pada Tindak Pidana Money Laundering Dalam Menghilangkan Jejak Kejahatan. *Snapp*. https://doi.org/10.24929/snapp.v2i1.3179

Radovanović, B. (2019). Rational Choice Theory and Charitable Giving. *Sociološki Pregled*. https://doi.org/10.5937/socpreg53-19679

Regina, O. (2025). Illicit Cryotocurrency Investigation Digital Forensic Framework: Integrating Off-Chain and on-Chain Analysis for Two Types of Crime. *Ijecbe*. https://doi.org/10.62146/ijecbe.v3i2.135

Rosseno Aji Nugroho. (2024). *PPATK Ungkap Pencucian Uang Lewat Kripto Sebesar Rp 800 Miliar!* CNBC INDONESIA. https://www.cnbcindonesia.com/news/20240419105454-4-531615/ppatk-ungkap-pencucian-uang-lewat-kripto-sebesar-rp-800-miliar

Ruiz, E. P., & Angelis, J. (2021). Combating Money Laundering With Machine Learning – Applicability of Supervised-Learning Algorithms at Cryptocurrency Exchanges. *Journal of Money Laundering Control*. https://doi.org/10.1108/jmlc-09-2021-0106

Sastrawati, N. (2020). Partisipasi Politik Dalam Konsepsi Teori Pilihan Rasional James S Coleman. *Al-*

Risalah Jurnal Ilmu Syariah Dan Hukum. https://doi.org/10.24252/al-risalah.v19i2.12730

Suparman, O. (2019). Kejahatan Pencucian Uang Dan Dampaknya Bagi Sektor Ekonomi Dan Bisnis. *Jurnal De Jure Muhammadiyah Cirebon*. https://doi.org/10.32534/jdmc.v3i2.1051

Teichmann, F., & Falker, M.-C. (2020). Money Laundering via Cryptocurrencies – Potential Solutions From Liechtenstein. *Journal of Money Laundering Control*. https://doi.org/10.1108/jmlc-04-2020-0041

Usman, M., Suji'ah, U., & Nashirudin, M. (2022). Cryptocurrency in Islamic Law. *Jurnal Multidisipliner Bharasa*. https://doi.org/10.56691/jurnalmultidisiplinerbharasa.v1i1.6

Usman, & Surono, A. (2024). Dinamika Dan Tantangan Penegakan Hukum Perampasan Aset Korporasi Dalam Tindak Pidana Pencucian Uang. *Pamulang Law Review*. https://doi.org/10.32493/palrev.v7i2.44756

Uzougbo, N. S. (2024). International Enforcement of Cryptocurrency Laws: Jurisdictional Challenges and Collaborative Solutions. *Magna Scientia Advanced Research and Reviews*. https://doi.org/10.30574/msarr.2024.11.1.0075