

Criminal Law in the Digital Age: Challenges of Law Enforcement Against Cyber and Crypto Crime in Indonesia

Rio Armanda Agustian¹⁾, Wirazilmustaan²⁾, Ageng Triganda Sayuti³⁾ & Herlina Manik⁴⁾

¹⁾Faculty of Law, Universitas Bangka Belitung, Indonesia, E-mail: rioarmanda.agustian@yahoo.com

²⁾Faculty of Law, Universitas Bangka Belitung, Indonesia, E-mail: wirazilmustaan@ubb.ac.id

³⁾Faculty of Law, Universitas Jambi, Indonesia, E-mail: ageng.fh@unja.ac.id

⁴⁾Faculty of Law, Universitas Jambi, Indonesia, E-mail: herlina_manik@unja.ac.id

Abstract. *The rapid development of information and communication technology in the digital era has a major impact on people's social and economic lives. Many human activities are now shifting to virtual spaces, including online transactions and the use of cryptocurrencies. However, behind this progress, there are major challenges in criminal law enforcement against cybercrime and crypto-related crimes. These crimes have different characteristics than conventional crimes, so existing regulations are not effective enough in addressing this problem. This study uses a juridical-normative and empirical approach to examine the gap between the prevailing criminal law regulations and the development of digital crime. Data was obtained through interviews with law enforcement officials and legal practitioners as well as analysis of existing laws and regulations. The results of the study show that there is a legal vacuum related to cybercrime and crypto, as well as the limitations of law enforcement officials in terms of technological knowledge and digital forensic facilities. In addition, complex international jurisdictional issues have exacerbated law enforcement against transnational crimes. In conclusion, criminal law reform is needed that includes regulatory reforms, capacity building of law enforcement officials, and strengthening international cooperation. With these steps, Indonesia's criminal law system is expected to be more responsive and adaptive to the challenges of digital crime in this modern era.*

Keywords: *Criminal Law; Cybercrime; Crypto; Digital Technology; Law Enforcement.*

1. Introduction

The development of information and communication technology in the digital era has created fundamental changes in the structure of modern society. Many human activities have shifted to the virtual space, marked by the emergence of digital platforms, online transaction systems, and the use of digital assets such as cryptocurrencies. Despite the significant benefits offered by this digital transformation, various new, complex and difficult-to-control forms of crime have emerged, known as cybercrime and cryptocurrency-related crime. These crimes have very different characteristics from conventional crimes, both in terms of their *modus operandi*, perpetrators, and even the scope of their jurisdiction, thus posing significant challenges to the national criminal justice system. (Raihana et al., 2023).

In the Indonesian context, the existing criminal justice system appears unprepared to address the highly dynamic development of digital crime. Although several regulations exist, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and general provisions in the Criminal Code, these regulations are insufficient to accommodate increasingly sophisticated forms of digital crime, particularly those involving blockchain technology and crypto assets. This creates a gap between the prevailing legal principles and the evolving social reality of a digital society. For example, although crypto transactions are frequently used for illegal activities such as money laundering or online fraud, there are no regulations that explicitly and systematically address the criminal aspects of crypto misuse within the Indonesian legal system. (Fadlan Ali et al., 2023).

This gap impacts the weak effectiveness of law enforcement. Law enforcement officials often face obstacles in proving crimes in the digital space, due to limited electronic evidence, a lack of technical competence in human resources, and cross-border jurisdictional barriers that are difficult for national legal systems to address. As a result, many cyber and cryptocrime cases are not optimally handled, harming the public and eroding public trust in the legal system. (Handayani et al., 2025). Based on this reality, this study aims to: (1) identify and analyze the gap between applicable criminal law norms and cyber and crypto crime practices in Indonesia; (2) evaluate the effectiveness of criminal law enforcement against these digital crimes; and (3) formulate strategies and solutions that can strengthen the role of criminal law in facing digital challenges.

The novelty of this research lies in its holistic and critical approach to the integration of conventional criminal law with the challenges of contemporary digital crime, particularly those related to crypto. Unlike previous studies that generally separate the issues of cybercrime and cryptocurrency, this research presents a synthesis of both within the framework of national criminal law enforcement and proposes a legal and institutional formulation that is adaptive to the digital era. The methodology used in this research is a legal-normative approach with conceptual and legislative analysis, supported by an empirical approach through in-depth interviews with law enforcement officials, legal practitioners, and information technology experts. The data obtained are analyzed descriptively and qualitatively to reveal weaknesses and potential reforms in criminal law in the digital context. (Udayana & Kelod, 2025).

Thus, this article is expected to provide scientific and practical contributions to strengthening the position of Indonesian criminal law to be more responsive, adaptive, and progressive in facing the digital era full of challenges and legal uncertainty. With the rapid development of information and communication technology, and the increasing use of cryptocurrency and digital platforms in everyday life, the Indonesian criminal law system must be able to transform to address the various forms of crime that continue to develop in cyberspace. (Ginting, 2025). Existing criminal law needs to be updated to better align with current digital dynamics, including addressing cybercrime, illegal crypto-based transactions, and personal data theft that can harm individuals and the state. (Rotty et al., 2022). Therefore, criminal law reform, which includes the development of more comprehensive regulations, increased human resource capacity, and the development of law enforcement tools that are in line with technological advances, is crucial.

2. Research Methods

This study uses a normative legal research method combined with an empirical approach. The normative approach is used to examine applicable positive legal norms, particularly those related to criminal law, cybercrime, and regulations regarding crypto assets in Indonesia. The legal sources include primary legal materials such as laws and regulations (e.g., the Criminal Code, the Electronic Information and Transactions Law, and crypto-related regulations from Bappebti and the Financial Services Authority), secondary legal materials such as literature, journals, and scientific articles, and tertiary legal materials such as legal dictionaries and legal encyclopedias. The empirical approach is used as a complement to understanding the application of criminal law in practice, particularly how law enforcement officials (the police, prosecutors, and courts) handle cybercrime and cryptocrime cases. Empirical data was obtained through semi-structured interviews with competent sources, such as cybercrime investigators, criminal law practitioners, and academics in the field of technology law. Data collection techniques included documentation of relevant regulations and court decisions, as well as direct interviews and case studies of several cybercrime and cryptocrime cases in Indonesia. The data analysis technique was conducted descriptively and qualitatively, namely by describing, reviewing, and analyzing data based on legal logic to identify gaps between legal norms and the reality of legal practice in the field. The results of this method are expected to provide a comprehensive understanding of the challenges of criminal law enforcement in dealing with digital crimes, as well as formulate solutions that can serve as recommendations for updating national criminal law to be more responsive to technological developments. (Efendi, 2018).

3. Results and Discussion

This research reveals several key findings related to the challenges of criminal law enforcement against cyber and crypto crimes in Indonesia, encompassing various normative and practical aspects. First, a significant regulatory gap was found between existing laws and the reality on the ground. Although Indonesia has the Electronic Information and Transactions Law (ITE Law) that regulates several legal aspects related to the digital world, as well as regulations related to crypto, these regulations are still limited and do not cover all forms of digital crime that continue to evolve, particularly those involving blockchain technology and crypto asset transactions. This often leads to law enforcement officials experiencing confusion in interpreting existing laws when

handling related cases. Second, the limited capabilities of law enforcement officials are a major obstacle to criminal law enforcement in the digital era. Many law enforcement officials lack an adequate understanding of digital technology, including blockchain and crypto, which makes the investigation and evidence-gathering process even more difficult. Furthermore, the lack of digital forensic facilities in many regions also limits the ability of law enforcement officials to conduct in-depth and accurate investigations. Most units with this capacity are located only in large cities, hampering the handling of cases in remote areas. Furthermore, international jurisdictional issues also add complexity to law enforcement against digital crimes, particularly those involving perpetrators or infrastructure located abroad. Cybercrimes and crypto transactions often involve perpetrators located in other countries or using foreign servers, making Indonesian law difficult to enforce. Limited international cooperation regarding data exchange or extradition of perpetrators also hinders resolving these cases. All these findings indicate that criminal law enforcement in Indonesia is still significantly lagging behind in the face of rapid technological developments and the cross-border nature of digital crime.(Arafat et al., 2024).

3.1. Regulatory Gap (Legal Gap)

There is a significant difference between the prevailing criminal law norms (*das sollen*) and the legal practices occurring in the field (*das sein*), reflecting a significant regulatory gap. Although Indonesia has Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which provides the legal basis for several aspects of cybercrime, as well as several crypto-related regulations issued by financial authorities such as Bappebti and OJK, these regulations are still general in nature and do not provide sufficiently in-depth provisions for cybercrime involving cutting-edge technologies, such as blockchain and cryptocurrencies. The ITE Law focuses more on the dissemination of negative content, defamation, and electronic transactions, but does not explicitly and explicitly cover more sophisticated forms of cybercrime, such as blockchain-based fraud, cyberattacks that damage critical infrastructure, or money laundering through crypto assets. Furthermore, although crypto transactions have become increasingly common in various sectors, Indonesian law has not yet established a clear legal status for crypto as a transaction tool or investment asset. Crypto is only recognized as a commodity by Bappebti, but not as legal tender in Indonesia, creating confusion among law enforcement officials when handling related cases. This ambiguity often makes it difficult to classify crypto transactions related to illegal activities, such as fraud, money laundering, and terrorism financing.(Arifin, 2021).

As a result of this regulatory gap, law enforcement officials often experience confusion in interpreting the applicable legal framework, particularly in handling cases involving emerging technologies such as blockchain and crypto assets. When cyber or crypto crimes occur, law enforcement must confront the reality that existing regulations do not provide clear and comprehensive guidelines on how to prosecute perpetrators or impose appropriate penalties. This adds complexity to handling digital crimes and leads to suboptimal law enforcement. This gap also undermines public trust in the legal system, which is considered incapable of meeting the challenges of rapidly evolving digital technology. Therefore, regulatory reforms are crucial to be more responsive and adaptive to the dynamics of digital crime in Indonesia.

3.2. Lack of Capacity of Law Enforcement Officers

One of the main challenges in enforcing criminal law against cyber and crypto crimes in Indonesia is the limited ability of law enforcement officers to understand and handle the ever-evolving digital technology. Many law enforcement officers, especially in regional areas, lack a thorough understanding of digital technologies, such as how blockchain, digital wallets (e-wallets), and other forms of cryptocurrency operate. This limited knowledge hinders officers from carrying out effective investigations and establishing evidence, given the complexity and depth of the technology involved in these digital crimes. For example, blockchain, the technology underlying crypto transactions, has very different characteristics from traditional financial systems. This technology enables anonymous and decentralized transactions, making them extremely difficult to trace or alter. Law enforcement officers who do not understand the mechanisms of smart contracts or the cryptography used in blockchain will have difficulty identifying relevant evidence in a case. This not only slows down the investigation process but also opens up opportunities for criminals to exploit legal and technological loopholes to evade detection.(Iqbal et al., 2024).

Furthermore, digital wallets used to store and transfer crypto also complicate investigations. E-wallets serve as storage for digital assets, but their owners' identities are often not easily traceable due to their anonymous or pseudonymous nature. Without a sufficient understanding of digital forensics and transaction tracking methods, law enforcement officials are often unable to optimally utilize available electronic evidence. This situation is further exacerbated by the lack of technical training for law enforcement officials in the areas of cybercrime and crypto, leaving them ill-prepared to deal with increasingly sophisticated digital crime cases. These limitations also impact the overall effectiveness of law enforcement, as the process of establishing evidence in cybercrime and crypto often requires electronic evidence that is not only adequate but also must be processed using appropriate techniques. Without the proper skills and tools, many cases cannot be fully pursued, resulting in a low success rate in bringing perpetrators to justice. Therefore, investing in training and capacity building for law enforcement officials in the areas of digital forensics and crypto is crucial to improving law enforcement capabilities in this digital era.(Yamin et al., 2022).

3.3. Limitations of Digital Forensic Tools

One significant obstacle to law enforcement against cyber and crypto crimes in Indonesia is the limited availability of adequate digital forensic facilities, particularly in areas outside major cities. Supporting facilities, such as digital forensic laboratories, which analyze electronic evidence, including hardware and software involved in criminal acts, remain very limited. Many regions in Indonesia, especially outside major cities, lack adequate digital forensic infrastructure to handle increasingly complex cybercrimes. This makes it difficult for law enforcement officials in these regions to access or use the tools and technology necessary for accurate investigations and evidence collection. Most cybercrime and crypto-related crime cases can only be handled by specialized units in major cities, which have more comprehensive digital forensic facilities. In large cities, for example, some police departments or state institutions have laboratories equipped with sophisticated hardware and software for digital data analysis. However, in areas with limited resources, law enforcement officials often struggle to obtain electronic evidence

that can be used in court. This impacts the effectiveness of law enforcement, as without adequate facilities, many cases risk not being legally proven.(Gustina et al., 2025).

The limited availability of digital forensic facilities also contributes to delays in responding to crimes, particularly those involving decentralized and anonymous crypto transactions. Cybercrimes involving the use of blockchain and digital wallets require highly specific forensic methods to accurately identify transactions and trace evidence. Without sophisticated forensic laboratories or tools, authorities cannot conduct thorough investigations. For example, criminals using crypto often utilize a layer of anonymity to conceal their identities. Without adequate forensic facilities, investigations into these crimes are hampered, and evidence is at risk of being lost or destroyed. Therefore, it is crucial for governments and law enforcement agencies to invest in the development of digital forensic infrastructure, including training for local authorities. This will strengthen investigative and evidentiary capacity at the national level and provide local law enforcement with a better opportunity to handle cyber and crypto crimes more effectively. The provision of these facilities must also be accompanied by efforts to expand access to the latest forensic technology that can handle various forms of digital evidence that are more complex and involve advanced technology.(Prayoga & Tuasikal, 2024).

3.4. Complicated International Jurisdiction

One of the biggest challenges in law enforcement against cybercrime and crypto transactions is the complexity of international jurisdiction, given the nature of digital crimes, which often involve perpetrators or infrastructure located abroad. Many cybercriminals leverage global networks, using servers or platforms based in other countries to conceal their tracks. In the case of crypto transactions, which often involve digital wallets and exchange platforms operating internationally, perpetrators can easily conduct transactions undetected by local legal systems. This creates a significant gap in law enforcement, as the countries involved have no direct control or authority over actions taken outside their jurisdiction. Jurisdictional limitations become even more complex when criminals use decentralized technologies like blockchain, which are not tied to a specific server or geographic location. With this technology, transactions can occur without a clear physical link, making it difficult to directly trace the source or location of the perpetrator. For example, in cases of money laundering using cryptocurrency, perpetrators can divert funds through multiple transactions between wallets spread across multiple countries, making it difficult to identify the overall transaction flow.(Sinaga & Raia Putri Noer Azzura, 2024).

These obstacles are further exacerbated by the lack of international cooperation on digital data exchange, cross-border prosecution, and extradition of criminals. Many countries have differing regulations and policies regarding data management and digital privacy, making it difficult to establish mutually acceptable legal standards. Without clear international cooperation agreements, countries struggle to exchange the information necessary to track and apprehend perpetrators outside their jurisdictions. Some countries even have very strict regulations regarding personal data, which can prevent other countries from accessing information crucial to digital crime investigations.(Lumaing et al., 2024).

Furthermore, an international court for cyber and cryptocrime has not yet been fully established, despite efforts by international organizations such as Interpol and EUROPOL to address this challenge. However, resource constraints and jurisdictional limitations between countries continue to hamper the effectiveness of this cooperation, making law enforcement against cross-border digital crimes a significant challenge. To address this issue, a stronger international legal framework is needed, including more effective bilateral and multilateral agreements to address cybercrime. Countries should also harmonize privacy and data regulations to facilitate smoother information exchange and enhance the capacity for international cooperation in addressing cybercrime and cryptocrime globally. Strengthening this cooperation will enable more efficient and expeditious law enforcement in addressing the ever-evolving and increasingly difficult-to-trace digital crime.(Mustam, 2023).

3.5. The Unclear Legal Status of Crypto Assets

One of the major issues facing the Indonesian criminal justice system in addressing crypto crimes is the unclear legal status of crypto assets. In Indonesia, crypto assets, such as Bitcoin and Ethereum, are only recognized as tradable commodities, not as legal tender. This is in accordance with regulations issued by Bappebti and the Financial Services Authority (OJK), which stipulate that crypto is a tradable good, similar to other commodities such as gold or stocks. However, its status as a commodity rather than legal tender creates confusion when crypto is used as a means of illegal transactions, such as fraud, money laundering, or terrorism financing. In practice, crypto is often used in various illegal transactions due to its anonymous and decentralized nature, allowing perpetrators to transact undetected by authorities. Crypto, which should be regulated in the context of trading goods and investments, is often used as a means of transaction for illegal activities involving the exchange of value or money in a system that cannot be easily traced. This ambiguity makes it difficult for law enforcement officials to determine the legal status of crypto as an object of crime, as there are no regulations that explicitly classify crypto as a means of illegal transactions.(Amrullah, 2024).

On the one hand, the use of crypto involving criminal transactions, such as online fraud or money laundering, demands stricter legal enforcement. However, on the other hand, the lack of clarity regarding the status of crypto hinders the effective implementation of criminal law, as there is no clarity on whether transactions using crypto should be considered criminal acts. Moreover, if crypto transactions occur outside of Indonesia, legal jurisdiction becomes unclear, as other countries may have different regulations regarding the legal status of crypto. This unclear legal status also undermines consumer protection. Consumers engaging in crypto transactions for investment or trading do not have the same guarantees as consumers transacting with legitimate money or assets. In the event of fraud or financial loss, consumers often struggle to seek compensation or initiate legal proceedings due to the ambiguous legal status of the assets used in the transactions.(Djibu, 2025).

Therefore, it is crucial to immediately update regulations regarding the legal status of crypto in Indonesia. One step that can be taken is to develop clearer and more comprehensive regulations regarding crypto, whether it is legal tender or remains a tradable commodity. This update will provide legal certainty, strengthen law enforcement against crypto misuse, and provide better protection for consumers and the wider community involved in the crypto ecosystem. Furthermore, clear regulations will

strengthen Indonesia's efforts to collaborate with other countries in addressing cross-border crypto crime.

Discussion

The findings above indicate that Indonesia's criminal justice system is still lagging behind in responding to the dynamics of digital crime. The gap between *das sollen* (the legal norms that should apply) and *das sein* (the reality of legal practice on the ground) creates a legal vacuum that further exacerbates the situation of law enforcement in Indonesia. Although regulations related to digital and crypto crimes already exist, particularly with the issuance of the Electronic Information and Transactions Law (UU ITE), the numerous overlapping regulations, the lack of comprehensive technical provisions, and the inability of existing laws to accommodate the rapid development of digital technology, result in many digital crimes being left unaddressed.(Tanggung et al., 2024).

This gap exacerbates legal protection for the public, as many digital crimes, such as online fraud, money laundering, and cyberattacks, continue to evolve rapidly and involve international platforms, anonymous networks, and cryptocurrencies that remain undetected by existing laws. The public often falls victim without adequate protection from a legal system unprepared for digital complexity. These crimes not only harm individuals but also have the potential to disrupt economic stability and national security. Furthermore, the limited reach of the state in combating digital crime is a growing concern. Cybercrime and crypto transactions are often transnational and involve perpetrators located outside Indonesia's jurisdiction, as mentioned in the issue of international jurisdiction. Due to the lack of clear international agreements, Indonesia is often unable to cooperate effectively with other countries to pursue and apprehend perpetrators involved in these crimes. The lack of international cooperation on data exchange or extradition of perpetrators makes law enforcement against digital crime even more difficult and limited.(Sariani, 2024).

Overall, the gap between *das sollen* and *das sein* in Indonesian criminal law creates a vacuum that digital criminals exploit. This demonstrates the importance of in-depth and adaptive legal reforms to make Indonesian criminal law more responsive to technological changes and the ever-evolving dynamics of digital crime. Without adequate legal reform, Indonesia will struggle to provide maximum protection for the public and combat increasingly complex, organized, and global digital crime.(Zainudin Hasan et al., 2024).

In terms of regulation, the ITE Law still focuses on insults, defamation, and the dissemination of negative content, but has not yet addressed the criminal aspects of the illegal use of blockchain and crypto technology. Similarly, the Criminal Code, as an outdated legal product, has not been designed to respond to developments in digital technology. This demonstrates the need for comprehensive criminal law reform to be more responsive to cutting-edge technology. Limited human resources are also a crucial issue. Law enforcement officers are required to understand advanced technology to handle cross-border and sophisticated crimes. Without mastery of the working mechanisms of crypto technology, law enforcement will be suboptimal.(Pantow et al., 2024).

The issue of international jurisdiction adds complexity, as digital crimes are often committed by perpetrators domiciled abroad. This necessitates international cooperation

agreements, both bilateral and multilateral, particularly regarding digital data exchange, extradition, and cross-border law enforcement cooperation. Furthermore, the unclear legal status of crypto assets creates confusion among law enforcement and the public. Although crypto assets such as Bitcoin, Ethereum, and others are increasingly popular as a means of transaction, especially among investors and digital users, their legal status remains ambiguous in the Indonesian legal system. For example, while crypto is recognized as a commodity by financial authorities such as Bappebti and the Financial Services Authority (OJK), Bank Indonesia (BI) does not recognize it as legal tender. This creates difficulties in determining the legal status of crypto, particularly when it is used in illegal transactions. This ambiguity not only confuses the public in understanding how crypto should be treated but also confuses law enforcement officials in determining whether transactions involving crypto can be categorized as criminal acts.(Matondang & Andryan, 2025).

Unsynchronized regulations between financial authorities (Bappebti, OJK, Bank Indonesia) and criminal law add to this complexity. Each of these institutions has different views and regulations regarding the status and regulation of crypto. Meanwhile, existing criminal laws, particularly those related to money laundering, fraud, or terrorism financing, do not explicitly accommodate crypto-based transactions, which are often conducted anonymously and across borders. This creates legal loopholes that criminals can exploit to avoid detection or even prosecution. These loopholes also undermine the security of the national financial system, as crypto can be used for illegal activities that harm society and the state, such as illicit trade, financial fraud, or terrorist financing.(Arafat et al., 2024).

Therefore, in-depth criminal law reform is needed, not only addressing gaps in existing regulations but also strengthening legal protection in the digital age. This reform should encompass several strategic steps, including:

1. Drafting specific regulations regarding digital crime and crypto assets: Clearer and more specific regulations regarding the use of crypto in the context of criminal law must be drafted immediately. These regulations should address how crypto-based transactions are treated under criminal law, including provisions on crypto surveillance, digital fraud, and crypto-based money laundering. These regulations should also provide clear guidelines for law enforcement officials in handling digital crimes involving crypto.
2. Intensive training for law enforcement officers in information technology: Law enforcement officers, including the police, prosecutors, and courts, must be provided with intensive training to understand blockchain technology, digital wallets, and the mechanisms of crypto-related crimes. This knowledge is crucial for improving officers' technical competence in handling increasingly complex digital crime cases.
3. Developing adequate digital forensic facilities: To improve capabilities in investigating digital crimes, developing adequate digital forensic facilities is crucial. Forensic laboratories capable of analyzing crypto data and digital evidence using the latest equipment and technology should be established in various regions, not just large cities. This will enable more effective investigations into cybercrimes involving crypto assets.

4. Harmonizing national laws with international laws to reach global jurisdiction: Given the often transnational nature of digital crime, international cooperation on data exchange and prosecution of perpetrators is crucial. Harmonizing laws between Indonesia and other countries regarding digital and crypto crimes will strengthen international coordination in addressing cyber and crypto crimes involving perpetrators from various countries. This effort should include the creation of international agreements governing procedures for the arrest of perpetrators, the exchange of digital evidence, and the extradition of perpetrators.

These steps will help create a more adaptive and progressive legal system and enhance Indonesia's ability to address the evolving legal challenges of the digital age and crypto-based crimes. With these updates, Indonesian criminal law can play a strategic role in addressing the challenges of digital crime and providing more effective legal protection for citizens in the digital age.

4. Conclusion

This study concludes that criminal law enforcement in the digital era, particularly against cybercrime and the use of crypto assets for illegal purposes, faces serious challenges both normatively and practically. There is a clear legal gap between applicable legal norms and the reality of practice on the ground, where existing laws are not fully able to address the complexity of rapidly evolving and transboundary digital crime. Normatively, Indonesia still relies on regulations that are not fully adaptive to the latest technology. The ITE Law, the Criminal Code, and regulations related to crypto do not comprehensively regulate the enforcement mechanisms for crypto-asset-based digital crimes, whether in the form of fraud, money laundering, or the financing of other illegal activities. Meanwhile, in terms of implementation, law enforcement officials still face limitations in terms of technological knowledge, digital forensic tools, and international cooperation. The unclear legal status of crypto as a means of transaction also increases legal loopholes that can be exploited by criminals. Therefore, comprehensive criminal law reform is needed, including regulatory updates that are responsive to technological developments, increased capacity of law enforcement officials, and strengthened international cooperation. This reform is crucial so that Indonesian criminal law is not merely repressive, but also adaptive and preventative in facing legal challenges in the digital era.

5. References

Journals:

- Amrullah, M. A. (2024). Inovasi Digital dalam Bentuk Aset Kripto Sebagai Sarana untuk Melakukan Tindak Pidana Pencucian Uang. *MLJ Merdeka Law Journal*, 5(November), 113–125.
- Arafat, M., Tito, A., Wirasto, E., Atma, U., & Yogyakarta, J. (2024). Kebijakan Kriminal dalam Penanganan Siber di Era Digital : Studi Kasus di Indonesia. *Equality: Journal of Law and Justice*, 1(2), 221–241. <https://doi.org/10.5281/Zenodo.4766614>
- Arifin, D. (2021). Pengaruh Teknologi terhadap Perkembangan Hukum di Indonesia. *Arus Jurnal Sosial dan Humaniora (AJSH)*, 5(1), 630–635.

- Djibu, M. A. (2025). Transformasi Digital dan Keamanan Siber : Upaya Penanggulangan Kejahatan di Era Teknologi di Indonesia. *Judge : Jurnal Hukum*, 06(01), 341–347.
- Fadlan Ali, M., YImran, S., & Apripari, A. (2023). Penegakan Hukum Pidana Terhadap Praktek Rugpull Ditinjau Dari Hukum Positif Indonesia. *Jurnal Ilmu Hukum dan Sosial*, 1(4), 317–328. <https://doi.org/10.51903/hakim.v1i4.1478>
- Ginting, H. (2025). Pembaruan Hukum dalam Menangani Kasus-Kasus Cybercrime di Era Digital. *Innovative: Journal Of Social Science Research*, 5(3), 1–9.
- Gustina, S., Kurniawan, A., & Pandawa, Y. (2025). Tindak Pidana Judi Online : Penegakan Hukum Oleh Kepolisian , Serta Upaya Dan Strategi Penanganannya. *Jurnal Intelek Insan Cendikia*, 2(5), 7763–7776.
- Handayani, A., Hidayat, S., & Saputra, D. N. (2025). Penegakan Hukum Terhadap Praktik Judi Online di Era Digital : Studi Kasus Cyber crime di Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(2), 207–215.
- Iqbal, M., Ardie, H. J., & Hasan, Z. (2024). Analisis Hukum Dalam Melacak Jejak Digital Dan Memahami Tindak Pidana Pencucian Uang Dalam Era Teknologi. *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syari'ah*, 5, 286–298. <https://doi.org/10.24252/iqtishaduna.vi.43802>
- Lumaing, E. Y., Purba, C., Moga, J. V., Metusalach, W., Legi, R., & Dakh, R. (2024). Tinjauan Yuridis Tindak Pidana Pencucian Uang Pada Transaksi Digital Cryptocurrency. *Social Science*, 12(2), 155–161. <https://doi.org/10.53682/jss.v12i2.10838>
- Matondang, A. M., & Andryan. (2025). Kebijakan Hukum Pidana Terhadap Kejahatan Cyber Studi Perbandingan Antara Indonesia Dan Thailand Dalam Perspektif Hukum Internasional. *Rewang Rencang : Jurnal Hukum Lex Generalis*, 6(1), 1–14.
- Mustam, A. M. A. (2023). Memerangi Kejahatan Siber Di Indonesia: Analisis Regulasi Hukum Pidana Yang Berlaku Dan Tantangannya. *Jurnal Ilmiah Gema*, 35(1), 10–14. <https://journal.uniba.ac.id/index.php/GM/index/>
- Pantow, A. W., Mahat, C. S., Sitorus, G. V. C., Simarmata, G. M., & Gunawan, J. G. C. (2024). Pembuktian Terhadap Tindak Pidana Kejahatan Penjualan Obat Kesehatan Impor. *Jurnal Multidisiplin Ilmu Akademik*, 1(5), 177–190.
- Prayoga, H., & Tuasikal, H. (2024). The Dissemination of Deepfake Content as a Criminal Act: A Critical Analysis of Law Enforcement and Public Protection in Indonesia. *Abdurrauf Law and Sharia*, 1(2), 22–38.
- Raihana, R., Sari, T. E. K., & Fanny, F. (2023). Tindak Pidana Pencucian Uang Perspektif Hukum Pidana Dan Perkembangan Teknologi. *SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum*, 2(3), 347–355. <https://doi.org/10.55681/seikat.v2i3.639>
- Rotty, N. W., Cahyani, A., Nabila, D. K., & Komala, C. (2022). Pemanfaatan Cryptocurrency Dalam Tindak Pidana Pencucian Uang. *Jurnal Hukum Statuta*, 1(2), 137–152.

- Sariani, A. L. (2024). Efektivitas Penegakan Hukum Terhadap Kejahatan Siber di Indonesia. *Al-Dalil Jurnal Ilmu Sosial, Politik, dan Hukum*, 2(2).
- Sinaga, B. B., & Raia Putri Noer Azzura. (2024). Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan di Era Society 5.0. *Padjadjaran Law Review*, 12(1), 71–81. <https://doi.org/10.56895/plr.v12i1.1651>
- Tanggung, A., Pelaku, J., & Atas, U. (2024). Modernisasi Sistem Hukum Pidana Dalam Menanggapi Perkembangan Kejahatan Siber Global. *Jurnal Hukum Terapan dan Inovasi Hukum*, 6(2), 20–46.
- Udayana, U., & Kelod, D. P. (2025). Penegakan Hukum Terhadap Pelaku Kejahatan Judi Online Di Indonesia. *Jurnal Media Akademik (JMA)*, 3(3).
- Yamin, A. F., Rachmawati, A., Pratama, R. A., & Wijaya, J. K. (2022). Perlindungan Data Pribadi Dalam Era Digital: Tantangan dan Solusi. *Meraja Journal*, 5(3), 115–137.
- Zainudin Hasan, Wiryadi Wiryadi, Arkaan Fadhulrrahman, Muhammad Dimas, & Ronald Dzaky Al Jabbar. (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. <https://doi.org/10.55606/birokrasi.v2i2.1163>

Books:

- Efendi, J. (2018). *Metode Penelitian Hukum: Normatif dan Empiris*. Prenadamedia Group.