IJEELSC, Vol. 1 No. 01, January 2025
DOI: https://doi.org/10.61990/ijeelsc.v1i1 e-ISSN

LEGAL REVIEW OF THE CRIME OF HACKING CRYPTOCURRENCY BASED ON BLOCKCHAIN TECHNOLOGY

Abdul Kadir[1]*, Khozinatul Asrori[2]
[1.2]Muhammadiyah Tangerang University, Indonesia
*Corresponding Author:
abdulkadir.usman87@gmail.com

Abstract
Hacking cryptocurrencies (digital currencies that include Bitcoin, Ethereum, Litecoin, Ripple, Stellar, Dogecoin, Cardano, Eos, and Tron) is a serious challenge in the context of blockchain technology, threatening the security and trust of users and the system as a whole. This research aims to explore cryptocurrency hacking with a focus on blockchain technology. The first problem statement identifies the types of hacks that are common in cryptocurrency transactions, while the second problem statement explores the factors that influence the vulnerability of blockchain systems to hacking. The research method uses a normative research type, with a detailed literature study approach to hacking cases that have occurred before, as well as technical analysis of system weaknesses that allow hacking to occur. Data was collected from relevant primary and secondary sources to support the analysis. The outcome of this research is an in-depth understanding of how hacking mechanisms work in the context of blockchain, as well as the identification of risk factors that can be evaluated to strengthen blockchain security. The findings provide a foundation for practical advice for blockchain platform developers, cryptocurrency users, and regulators in an effort to improve the security of future blockchain infrastructure. It is hoped that the results of this study will not only improve the understanding of cryptocurrency hacking threats, but will also make a significant contribution to building a more secure and trustworthy blockchain ecosystem.

Keywords: Cryptocurrency, Hacking, Blockchain Technology

1. Introduction

In today's digital era, the development of information and communication technology has had a significant impact on various aspects of life, one of which is the emergence of cryptocurrency as a digital medium of exchange that uses blockchain technology to secure its transactions. Cryptocurrency has changed the traditional view of currencies and financial systems, offering higher speed, transparency, and efficiency in transactions (Kadir, 2023). However, along with its development and popularity, cryptocurrency has also become an attractive target for cyber criminals, particularly hacking. Cryptocurrency hacking crimes not only threaten the security of digital assets of individuals and institutions, but also raise serious questions about the reliability and security of blockchain technology, which has been considered secure.

The development of blockchain technology applied to cryptocurrencies does offer various advantages, such as decentralization, resistance to manipulation, and anonymity. But ironically, these characteristics also make cryptocurrencies an easy target for hackers. Hacking can occur through a variety of loopholes, be it on digital wallets exchanges, to the blockchain infrastructure itself. The hacking cases that have occurred have caused huge financial losses to users and undermined public confidence in the security and stability of this digital financial system.

The rapid development of cryptocurrencies in Indonesia has also been followed by an increase in hacking activities that have caused harm to many parties. Although the government and regulators such as Bank Indonesia and the Financial Services Authority have provided a number of regulations and guidelines regarding the use and trading of cryptocurrencies, the existing regulations are still considered insufficient to address the increasingly complex problem of hacking crimes. This is due to the grey nature of cryptocurrency law, as well as the challenges in applying the law to cybercrime that is transnational in nature (Hediati, 2022).

Considering the impact that hacking crimes can have on the cryptocurrency ecosystem, an in-depth legal study is needed to identify loopholes that can be exploited by hackers and build a legal framework that can protect cryptocurrency users and investors. This study should be able to propose solutions that are not only effective in counteracting hacking, but also support the growth of the cryptocurrency industry in Indonesia within a safe and secure framework. The questions of how the law can adapt to the development of blockchain technology and cryptocurrencies, as well as how to enhance cross-border co-operation in tackling cybercrime, are crucial to answer.

The study should also consider the technical aspects of blockchain technology and cryptocurrencies, given that hacking crimes often exploit weaknesses in these technical aspects. Therefore, this legal study requires not only a normative juridical approach, but also an interdisciplinary approach involving expertise in the field of information technology. Thus, the results of the study are expected to provide comprehensive advice, covering legal, technical, and policy aspects, to strengthen the cryptocurrency ecosystem in Indonesia from the threat of hacking crimes.

Past research on cryptocurrency hacking crimes based on blockchain technology has highlighted various aspects related to system vulnerabilities, applicable regulations, and applicable prevention and countermeasures. Past research has revealed that although blockchain is considered a secure and transparent technology, there are still security gaps that hackers can exploit, such as problems with smart contracts, security gaps in digital wallets, and weaknesses in exchange points (Atmojo, 2023). The research emphasizes the importance of ongoing security audits and the development of stronger security protocols to protect digital assets. Another study showed that many cryptocurrency users do not fully understand the security risks associated with using and storing their digital assets (Sajidin, 2021). This often opens up opportunities for hackers to conduct phishing attacks or malware to steal private keys that grant access to users' digital wallets. The research suggests increased awareness and education for cryptocurrency users on basic security practices, such as the use of two-factor authentication and storing private keys in more secure hardware wallets.

The title was chosen due to its high relevance to recent developments in the world of cybersecurity and blockchain technology. Cryptocurrency hacking crimes are an increasingly urgent issue to address given the rapid growth of the cryptocurrency industry and a series of hacking incidents that have resulted in huge financial losses to users. By taking up this title, the research has the potential to make a significant contribution in identifying security gaps, evaluating the effectiveness of regulations, and designing prevention strategies that can reduce the risk of hacking in the cryptocurrency ecosystem. In addition, the research will also provide valuable insights for regulators, industry stakeholders, and the general public on how best to protect their digital assets and improve security in cryptocurrency transactions.

Based on the background of the problem above, the research problem formulation is: How is the Legal Regulation of Cryptocurrency Hacking Crimes with a focus on digital currency systems that include (Bitcoin, Ethereum, Litecoin, Ripple, Stellar, Dogecoin, Cardano, Eos, and Tron)? Based on Blockchain Technology in Indonesia and How is the Government's Efforts to Make Regulations and Policies on Cryptocurrencies with a focus on digital currency systems that include (Bitcoin, Ethereum, Litecoin, Ripple, Stellar, Dogecoin, Cardano, Eos, and Tron)? Based on Blockchain Technology in Indonesia.

2. Theoretical Background

In a regulatory context, several studies have examined how different countries have responded to the legal challenges posed by cryptocurrencies and related cybercrime. These comparative studies have found that there are significant differences in regulatory approaches between countries, from very strict to more liberal. Past research suggests that an effective legal framework for regulating cryptocurrencies should be able to protect consumers and investors, while also supporting innovation and industry growth (Alfaris, 2019). The research further emphasizes the need for international cooperation in tackling hacking crimes that are often cross-border in nature. A previous study also explored the potential applications of blockchain technology itself in enhancing information security and digital transactions (Indraprakoso, 2023). Leveraging the decentralization and transparency characteristics of blockchain, several innovative proposals have been put forward to develop systems that are more resistant to hacking and fraud. For example, the use of automated smart contracts can reduce the risk of human intervention and data manipulation.

The case law focused on in this research is a massive hacking incident that occurred in mid-2023, targeting one of Indonesia's leading cryptocurrency exchange platforms. In the attack, hackers managed to steal digital assets worth hundreds of billions of rupiah, an incident that caused panic among investors and users and opened the eyes of many parties to the vulnerability of the digital asset security system in this country. The incident not only caused huge financial losses to platform users but also dragged public attention and regulators into a debate about the effectiveness of existing regulations and security standards in protecting digital assets and blockchain transactions.

In responding to this case, various applicable laws form the basis for handling and investigation. Law No. 11/2008 on Electronic Information and Transactions (ITE Law) and its amendment, Law No. 19/2016, provide the legal framework to prosecute perpetrators of cybercrime, including hacking. The ITE Law, as the main legal instrument, sets out provisions regarding criminal offences in the digital space and enables law enforcement to take action against individuals or groups responsible for these illegal activities.

In addition, Bank Indonesia's regulation on the Use of Information Technology by Payment System Service Providers, while not specifically mentioning cryptocurrency as a legal currency, provides guidance on the security standards that payment system service providers should meet. This is relevant to cryptocurrency exchange platforms in the context of digital asset storage and transactions. On the other hand, the Financial Services Authority (OJK) through its regulation on Digital Financial Services is trying to provide an additional layer of protection for consumers and maintain financial system stability from potential operational risks that may arise from digital exchange activities.

This hacking incident opened up a wide discussion regarding the need for stricter oversight and better-defined regulations for cryptocurrency exchange platforms. Highlighting existing security gaps, this case shows how critical the role of ongoing security audits and the implementation of stronger security protocols are to prevent similar incidents from occurring in the future. In addition, this case also emphasizes the importance of user awareness and education on the security risks associated with storing and transacting digital assets. Law enforcement actions against this kind of cybercrime also highlight the need for close coordination between various government agencies such as the Police, Bank Indonesia, and OJK, as well as international collaboration in pursuing and bringing perpetrators to justice. Cybercrimes, particularly those relating to digital assets and blockchain technology, often involve perpetrators from multiple jurisdictions, complicating the investigation and prosecution process.

The hacking of this cryptocurrency exchange platform is an important case study that reflects the challenges faced by Indonesia in regulating and protecting its growing digital financial ecosystem. This underscores the importance of revising and developing regulations that are adaptive and responsive to technological developments, as well as building awareness and capacity for all stakeholders in dealing with evolving cybersecurity risks. In this context, the importance of a legal study on cryptocurrency hacking crimes based on blockchain technology is very relevant and urgent. This study is expected to provide a deeper understanding of the complexity of the issues at hand as well as identify strategic steps that can be taken by the government, regulators, industry, and society to face cybersecurity challenges in the cryptocurrency world. As such, this review will not only contribute to the development of legal literature in Indonesia, but also to the development of legal practices and policies that can support the healthy growth of the cryptocurrency industry in the future.

3. Methods

The type of research used in this writing is normative legal research (library research), namely legal research carried out by examining library materials or secondary data as a basis for research by conducting searches of regulations and literature relating to the problem at hand. Researched (Soekanto & Mamudji, 2015).

4. Results and Discussion

4.1 Legal Arrangements Regarding Cryptocurrency Hacking Crimes Based on Blockchain Technology in Indonesia

Legal arrangements regarding cryptocurrency hacking crimes based on blockchain technology in Indonesia can be seen from several perspectives, ranging from the existing legal framework to the theory of law enforcement and relevant laws and regulations. The development of blockchain technology and cryptocurrency has brought various conveniences in financial transactions, but on the other hand, it also poses new challenges in law enforcement, especially related to hacking crimes (Arwani, 2024).

In Indonesia, regulations governing cryptocurrencies are still relatively new and evolving. Law No. 11/2008 on Electronic Information and Transactions (ITE Law) is one of the legal bases that can be used to address hacking cases that occur in the digital space, including in the cryptocurrency ecosystem. Amendments to the ITE Law in 2016 further strengthened this legal framework by adding stricter sanctions and provisions against offences in cyberspace.

In addition to the ITE Law, Law No. 19/2016 on the Amendment to Law No. 11/2008 on Electronic Information and Transactions also clarifies sanctions for cybercrimes, including hacking. However, these two laws do not specifically mention cryptocurrency or blockchain technology, so their interpretation and application to hacking cases in this area requires a more detailed and specific approach.

In terms of more specific regulations, the Commodity Futures Trading Supervisory Agency (Bappebti) as a regulator under the Ministry of Trade has issued regulations governing crypto assets as tradable commodities. However, these regulations focus more on the trading and consumer protection aspects, and do not explicitly regulate hacking or fraud crimes that occur in cryptocurrency transactions.

A theory of law enforcement that could be applied in the context of blockchain-based cryptocurrency hacking crimes includes restorative justice, which emphasizes the restoration of losses suffered by victims and the reintegration of offenders into society. This approach is relevant given that many victims of cryptocurrency hacking crimes suffer significant financial losses, and case resolution often prioritizes asset recovery over simply sanctioning the perpetrator.

In addition, general prevention and special prevention are also important to be applied in law enforcement related to cryptocurrency hacking crimes. General prevention is carried out through the application of sanctions aimed at providing a deterrent effect to the wider community so as not to commit similar crimes (Alias, 2022). Meanwhile, special prevention aims to prevent offenders from re-offending through rehabilitation or educational sanctions.

The implementation of law enforcement against cryptocurrency hacking crimes in Indonesia requires collaboration between various parties, including regulators, law enforcement agencies, the cryptocurrency industry, and the public. Increased digital literacy and understanding of the risks associated with cryptocurrencies are also key in preventing hacking crimes. In addition, the development of cybersecurity technologies capable of addressing the challenges posed by the development of blockchain technology and cryptocurrencies is also indispensable.

Cryptocurrencies have become a global phenomenon, offering great opportunities for financial and economic innovation, but also bringing a range of threats that are becoming increasingly evident in various countries, including the United States. As a country with a well-established cryptocurrency ecosystem, the United States has faced various challenges and risks arising from the popularity of these digital currencies. The emerging threats in the United States can be a reflection for Indonesia, whose cryptocurrency ecosystem is still in the development stage but is gaining traction. Understanding the threats faced by the United States can help Indonesia formulate appropriate policies and strategies to prevent and address similar risks in the future.

One of the biggest threats faced by the United States regarding cryptocurrencies is digital hacking and fraud. There have been many cases where digital platforms and wallets have been hacked, causing huge losses to investors. For example, the hack of Mt. Gox, a cryptocurrency exchange based in Japan but catering to many users from the United States, led to the loss of approximately 850,000 Bitcoins which at that time was worth approximately 450 million USD (Crimmins, 2015). This was one of the biggest hacks in cryptocurrency history, and its impact was felt worldwide. In addition, the Ronin Network hack in 2022, which resulted in a loss of 620 million USD, shows that the threat of hacking is not going away (Zheng). If Indonesia does not prepare an

adequate legal framework and security infrastructure, then a similar case could happen here, given the growing number of Indonesians involved in cryptocurrency investment.

The other threat faced by the United States is the use of cryptocurrencies in illegal activities, including money laundering, drug trafficking, and terrorism financing. The anonymity offered by some types of cryptocurrencies is attractive to criminals to hide their illegal activities from the scrutiny of legal authorities. For example, in 2021, the United States Department of Justice seized more than USD 70 million in Bitcoin related to a global money laundering operation conducted by an organized crime group (Dimovski, 2023). This threat cannot be underestimated, because as the use of cryptocurrencies in Indonesia increases, there is a possibility that cryptocurrencies will be used in illegal activities that are difficult to trace by local authorities. The Indonesian government needs to learn from the United States' experience in developing effective regulations to prevent the misuse of cryptocurrencies in illegal activities.

In addition, the extreme volatility of the cryptocurrency market in the United States also shows that cryptocurrency is a very risky investment. Sharp price fluctuations can cause huge losses for investors in a very short period of time. For example, in early 2021, the price of Bitcoin surged from around 30,000 USD to more than 60,000 USD, but then dropped dramatically to less than 30,000 USD within a few months (Iyer, 2023). Many investors are tempted by the potential for huge profits without realizing the risks of this volatility. In Indonesia, a similar trend is likely given the growing popularity of investing in cryptocurrencies. Without adequate education on the risks involved, many Indonesian investors, especially the less experienced ones, may suffer huge losses.

The security and regulation of the blockchain technology underlying cryptocurrencies is also a major concern in the United States. While this technology offers transparency and decentralization, weaknesses in security protocols can be exploited by hackers. The United States has begun taking steps to address this issue by developing stricter regulations and working with technology providers to improve system security. However, Indonesia may face greater challenges in this regard, given its still-developing digital infrastructure and cybersecurity awareness. It is important for the Indonesian government to prepare strict policies and support research and development of blockchain security technologies.

Then, there is also the risk of uncertain regulation in the United States, where the government is still figuring out how to regulate cryptocurrencies without stifling innovation. This uncertainty causes confusion and instability in the market, which can affect investor confidence. In Indonesia, this regulatory challenge could be even more complex given the dynamic nature of blockchain technology and cryptocurrencies. Regulations that are too strict may stifle innovation and technology adoption, while regulations that are too lax may pose greater security and fraud risks. Indonesia should learn from regulatory efforts in the United States to find the right balance between encouraging innovation and protecting consumers and market stability.

Overall, the cryptocurrency threat in the United States provides a glimpse of what Indonesia may face in the future if cryptocurrency adoption continues to grow without adequate regulation and oversight. It is important for Indonesia to learn from the experiences of countries that have already widely adopted cryptocurrency. Developing clear regulations, increasing public digital literacy, and international cooperation in dealing with cybercrime are steps needed to ensure that Indonesia is ready to face the challenges that arise from these technological advances. With the right steps, Indonesia

can take advantage of the opportunities offered by cryptocurrencies while minimizing the associated risks.

Legal regulations regarding cryptocurrency hacking crimes based on blockchain technology in Indonesia still require further development, both in terms of more specific regulations and the implementation of effective law enforcement theories. Collaboration between agencies and increasing the capacity of law enforcement officials, as well as awareness and education to the wider community, are important factors in building a safe and trustworthy cryptocurrency ecosystem in Indonesia.

4.2 Legal Regulations Regarding Government Efforts in Making Regulations and Policies

Legal regulations regarding cryptocurrency based on blockchain technology in Indonesia are a comprehensive effort involving various stakeholders, including government, regulators and industry. In recent years, the Indonesian government has shown its seriousness in regulating the cryptocurrency ecosystem with the aim of protecting consumers, encouraging innovation, and anticipating financial risks and cybercrime. Legal and policy regulations in this field continue to develop along with the dynamics of technology and global markets.

One of the significant first steps is the recognition of cryptocurrency as a commodity by the Commodity Futures Trading Supervisory Agency (Bappebti), which allows crypto assets to be traded on futures exchanges in Indonesia. This decision is contained in CoFTRA Regulation Number 5 of 2019 concerning the Implementation of Crypto Asset Trading. This regulation opens the door for the growth of the crypto asset trading ecosystem in Indonesia by providing a clear legal framework.

Furthermore, the government through the Ministry of Trade and CoFTRA continues to improve regulations by introducing further technical provisions and requirements regarding the operations of crypto asset exchanges, crypto wallet operators, as well as other aspects related to crypto asset trading. The goal is not only to protect consumers but also to create a healthy and competitive market.

From a law enforcement perspective, the government relies on Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments as one of the legal bases for handling cases related to cyber crime, including fraud or hacking in the cryptocurrency ecosystem. However, given the uniqueness and complexity of blockchain and cryptocurrency technology, there is a need for the development of a more specific and detailed legal framework.

In terms of law enforcement theory, Indonesia adopts an approach that combines prevention, retribution and rehabilitation. The implementation of prevention is intended to reduce the risk of crime through public education and the creation of regulations accompanied by strict supervision. Meanwhile, retribution is reflected in the implementation of strict sanctions for violations of the law, and rehabilitation is realized through efforts to reintegrate criminals into society in a constructive way.

The implementation of cryptocurrency policies and regulations in Indonesia still faces challenges, especially related to the digital literacy gap among the public, the need for stronger cyber security infrastructure, and the need for a balance between innovation and consumer protection. The government and regulators must continue to adapt to technological developments and global market trends to ensure that Indonesia is not left behind in the adoption of blockchain technology and the use of cryptocurrencies, while

ensuring that its operational environment is safe, transparent and fair for all parties (Fattah, 2022).

In the future, regulatory development in the cryptocurrency sector in Indonesia will continue to require constructive dialogue between the government, industry and the user community. This collaboration is important to ensure that Indonesia can take full advantage of the potential of blockchain and cryptocurrency technology, while still controlling risks and protecting user rights. Increasing financial and digital literacy among the public is also the key to supporting this ecosystem so that it develops healthily and sustainably.

3. Conclusion

Legal regulations in Indonesia regarding the crime of hacking cryptocurrency systems based on blockchain technology are still in the development stage. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments through Law Number 19 of 2016, provides the basic legal framework for law enforcement against cybercrimes, including cryptocurrency hacking. In addition, the Commodity Futures Trading Supervisory Agency (Bappebti) Regulations also regulate trading of crypto assets as commodities, providing legitimacy and legal protection in crypto asset transactions. Despite this, challenges in implementing the law still exist, especially in terms of society's digital literacy and law enforcement's ability to handle complex blockchain technology. There is a need to increase the capacity and knowledge of law enforcement officials and the public to be more effective in preventing and dealing with cryptocurrency hacking crimes.

The Indonesian government has made various efforts to regulate and supervise the cryptocurrency ecosystem based on blockchain technology through cross-sector collaboration and the preparation of comprehensive regulations. Bappebti has issued several regulations governing crypto asset trading, providing a clear framework for industry players and protection for investors. In addition, the government has passed the Financial Sector Strengthening and Development Law, which transfers the authority to regulate and supervise financial technology innovation sector activities, including cryptocurrency, to the Financial Services Authority (OJK). This effort reflects the government's commitment to creating a safe and supportive environment for the development of blockchain and cryptocurrency technology. Even though there has been a decline in the value of crypto asset transactions, the increase in the number of investors shows that Indonesian people are increasingly interested and believe in the potential of the digital economy offered by blockchain technology. The government continues to strive to strengthen regulations, increase digital literacy, and build cooperation with various parties to optimize the benefits and minimize the risks of using cryptocurrency.

References

Alexander Sugiharto, S. H., Muhammad Yusuf Musa, M. B. A., Falahuddin, M. J., & ST, M. (2022). NFT & Metaverse: Blockchain, Dunia Virtual & Regulasi (Vol. 1). Indonesian Legal Study for Crypto Asset and Blockchain.

Alfaris, Maulana Reyza, Muhammad Waliyam Mursida, and Moch Irfan Dwi Syahroni. "Model regulasi financial technology syariah dalam kerangka hukum Indonesia: Studi perbandingan Malaysia dan Inggris." Legislatif (2019): 73-96.

Alias, Alima Tsusyaddya, and Suryaningsi Suryaningsi. "Hukuman Mati Pelaku Tindak Korupsi dalam Perspektif Hukum dan Hak Asasi Manusia." Nomos: Jurnal Penelitian Ilmu Hukum 2, no. 4 (2022): 138-147.

Ali, Zaenudin. (2010). Metode Penelitian Hukum. Jakarta: Sinar Grafika, 18.

Amsi, M. (2020). Berkah dengan investasi syariah: Saham syariah kelas pemula. Elex Media Komputindo.

Ardhianti, M., Prawoto, E. C., Pujiastuti, R., & Risaldi, A. (2023). Semiotika Kritis Pendekatan dalam Teks Kejahatan Siber. CV Pena Persada.

Arini Novandalina, S. E., & Wijayanto, H. G. (2024). MEMBANGUN KEUANGAN BERBASIS FINTECH: Bagi Usaha Mikro, Kecil, dan Menengah. Feniks Muda Sejahtera.

Arwani, Agus, and Unggul Priyadi. "Eksplorasi Peran Teknologi Blockchain dalam Meningkatkan Transparansi dan Akuntabilitas dalam Keuangan Islam: Tinjauan Sistematis." Jurnal Ekonomi Bisnis dan Manajemen 2, no. 2 (2024): 23-37.

Atmojo, Robertus Nugroho Perwiro, and Fokky Fuad. "Upaya Perlindungan Hukum Bagi Para Konsumen Pemegang Aset Kripto di Indonesia." Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat 9, no. 2 (2023): 254-276.

Crimmins, D., Falk, C., Fowler, S., Gravel, C., Kouremetis, M., Poremski, E., ... & Liles, S. (2015, March). US Bank of Cyber. In Proceedings of the 16th Annual Information Security Symposium (pp. 1-1).

Dhanu Prayogo, S. H., Shivendra Adistya, S. H., Eliadi Hulu, S. H., & Nikita Johanie, S. H. (2022). Mengenal Hukum Aset Kripto. Deepublish.

Dimovski, D. (2023). CRYPTOCURRENCIES AND CRIME. Teme-Časopis za Društvene Nauke, 47(4), 975-990.

Disemadi, Hari Sutra, and Delvin Delvin. "Kajian Praktik Money Laundering dan Tax Avoidance dalam Transaksi Cryptocurrency di Indonesia." NUSANTARA: Jurnal Ilmu Pengetahuan Sosial 8, no. 3 (2021): 326-340.

Faizal, Muhazzab Alief, Zelyn Faizatul, Binti Nur Asiyah, and Rokhmat Subagyo. "Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman Dan Tantangan Terkini." Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam 5, no. 2 (2023): 87-100.

Fattah, H., Riodini, I., Hasibuan, S. W., Rahmanto, D. N. A., Layli, M., Holle, M. H., ... & Marzuki, S. N. (2022). Fintech dalam Keuangan Islam: Teori dan Praktik. Publica Indonesia Utama.

Hamin, Dewi Indrayani. "Crypto Currensi Dan Pandangan Legalitas Menurut Islam: Sebuah Literature Review." JAMBURA: Jurnal Ilmiah Manajemen dan Bisnis 3, no. 2 (2020): 127-139.

Haripin, M. (2022). Intelijen dan keamanan nasional di Indonesia pasca-Orde Baru. Yayasan Pustaka Obor Indonesia.

Hediati, Febri Noor. "Perkembangan Mata Uang Kripto Dan Perlindungan Hukum Terhadap Investasi Mata Uang Kripto di Indonesia'." (2022): 48-60.

Ifadhila, I., Rukmana, A. Y., Erwin, E., Ratnaningrum, L. P. R. A., Aprilia, M., Setiawan, R., ... & Setiawan, H. (2024). Pemasaran Digital di Era Society 5.0: Transformasi Bisnis di Dunia Digital. PT. Sonpedia Publishing Indonesia.

Indraprakoso, Dondy. "Eksplorasi Potensi Penggunaan Blockchain Dalam Optimalisasi Manajemen Pelabuhan di Indonesia: Tinjauan Literatur." Sanskara Manajemen Dan Bisnis 1, no. 03 (2023): 140-160.

Indrawanto, S. (2024). Merajut Keberlanjutan Usaha: Panduan Hukum Dagang dan Bisnis. PT Indonesia Delapan Kreasi Nusa.

Indrayani, N., Hariyono, H., Marpaung, S. H., Ikhsan, F. K., Aladdin, Y. A., Lestyarini, B., & Rusliyadi, M. (2024). Buku Ajar Literasi Digital. PT. Sonpedia Publishing Indonesia.

Iyer, R., & Popescu, A. (2023). New Evidence on Spillovers Between Crypto Assets and Financial Markets. International Monetary Fund.

Jaya, A. S., & Widyastuti, T. V. (2022). Legalitas Cryptocurrency di Indonesia. Penerbit NEM.

Kadir, Syahruddin. "Keuangan Terdesentralisasi (DeFi) Dan Teknologi Keuangan (FinTech) Syariah Dalam Sistem Keuangan Abad 21." Journal of Accounting and Finance (JACFIN) 5, no. 2 (2023): 1-14.

Khunainah, I., Idayanti, S., & Rahayu, K. (2024). Pembuktian Kepemilikan Aset Investasi dengan Trading Kripto di Indonesia. Penerbit NEM.

Laksana, Tri Ginanjar, and Sri Mulyani. "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan." Jurnal Ilmiah Multidisiplin 3, no. 01 (2024): 109-122.

Maharani, Rista, and Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." JURNAL USM LAW REVIEW 7, no. 1 (2024): 333-347.

Mariana, C. D., St, M. M., & Sutanto, I. H. (2022). Crypto Currency: Terobosan atau Ancaman atas Tatanan Finansial Umum?. Prenada Media.

Marzuki, Peter Mahmud. (2019). Penelitian Hukum. Jakarta: Prenada Media Group, 35.

Maulani, G., Kom, S., Kom, M., Ika Fitria, S. A. P., Ansyah, R. H. A., Deni, H. A., ... & Deni Malik, S. A. B. (2024). Manajemen Pelayanan Publik. Cendikia Mulia Mandiri.

Mukhra, U. H., Makruf, J. J., Kesuma, T. M., Nizam, A., & Siregar, M. R. (2024). Mobile Banking dalam Persepsi Privasi Nasabah. Syiah Kuala University Press.

Nasution, D. S., Aminy, M. M., & Ramadani, L. A. (2019). Ekonomi Digital. Sanabil.

Nugraha, Ade Chandra. "Penerapan Teknologi Blockchain dalam Lingkungan Pendidikan: Studi Kasus Jurusan Teknik Komputer dan Informatika POLBAN." Produktif: Jurnal Ilmiah Pendidikan Teknologi Informasi 4, no. 1 (2020): 302-307.

Nurisman, Eko. "Risalah Tantangan Penegakan Hukum Tindak Pidana Kekerasan Seksual Pasca Lahirnya Undang-Undang Nomor 12 Tahun 2022." Jurnal Pembangunan Hukum Indonesia 4, no. 2 (2022): 170-196.

Palawe, J. (2024). CRYPTO VS SAHAM, Mana yang lebih baik?. Jaka Frianto Putra Palawe.

Purnomo, I. R. S. D., Iswi Hariyani, S. H., & Cita Yustisia Serfiyani, S. H. (2013). Pasar Komoditi: Perdagangan Berjangka dan Lelang Komoditi. Galangpress Publisher.

Sajidin, Syahrul. "Legalitas penggunaan cryptocurrency sebagai alat pembayaran di Indonesia." Arena Hukum 14, no. 2 (2021): 245-267.

Savitri, A. (2019). Revolusi industri 4.0: mengubah tantangan menjadi peluang di era disrupsi 4.0. Penerbit Genesis.

Setyani, M. (2023). Pasar Valuta Asing: Cerdas Berinvestasi di Pasar Berjangka. PT Elex Media Komputindo.

Soekanto, Soerjono dan Sri Mamudji. (2015). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: Raja Grafindo Persada, 2-6 and 13-14.

Soetrisno, B. A. J., Gunawan, K. E., Subijanto, T. M. E., Oktavia, S., Widagda, T. A. K., Estevania, T. A., ... & Irawan, A. V. (2024). Berubah Bersama Akuntansi Digital. SIEGA Publisher.

Stiawan, D. (2005). Sistem Keamanan Komputer. Elex Media Komputindo.

Tambun, Maria Arbina, and M. Ilham Putuhena. "Tata Kelola Pembentukan Regulasi Terkait Perdagangan Mata Uang Kripto (Cryptocurrency) Sebagai Aset Kripto (Crypto Asset)." Mahadi: Indonesia Journal of Law 1, no. 1 (2022): 33-57.

Yudha, A. T. R. C. (2021). Fintech syariah dalam sistem industri halal: Teori dan praktik. Syiah Kuala University Press.

Zheng, J., Lee, D. K. C., & Qian, D. (2023). An In-depth Guide to Cross-chain Protocols under a Multi-chain World. World Scientific Annual Review of Fintech, 1, 2350003.