Estudiante Law Journal

Volume 7 Number 1 February, 2025: Pp 252-266
Faculty of Law, Universitas Negeri Gorontalo, City of Gorontalo, Indonesia
https://ejurnal.ung.ac.id/index.php/eslaw/index

Fraud and Digital Crime: Challenges and Solutions in the Era of Blockchain Technology

Nurul Ananda Sahwa Mointi

Faculty of Law, Universitas Negeri Gorontalo, Indonesia.
Correspondence Email: Nurulananda50@gmail.com

Abstract: This study aims to identify the challenges in combating fraud crimes involving blockchain technology and explore effective solutions to address these issues. The research uses a descriptive qualitative approach with a case study. Data is collected through a literature review of relevant literature on blockchain, digital fraud, as well as regulations and policies implemented in various countries. The findings of this study reveal several key challenges in addressing fraud crimes involving blockchain. First, the anonymous nature of blockchain transactions makes it difficult to track and identify fraudsters. Second, the decentralized nature of blockchain reduces the role of central authorities in overseeing and controlling transactions. Third, the lack of clear regulations in several countries regarding the use of blockchain and cryptocurrency. Proposed solutions include the use of analytical technology, such as blockchain forensics, to track transaction traces, as well as strengthening regulations on cryptocurrency, including identity verification and reporting suspicious transactions. Additionally, education and digital literacy for the public are essential to raise awareness about digital fraud risks and provide a better understanding of how to protect oneself in the blockchain world.

Keywords : Digital Fraud; Blockchain; Cryptocurrency.

How to cite (Chicago Style) :

Nurul Ananda Sahwa Mointi. "Fraud and Digital Crime: Challenges and Solutions in the Era of Blockchain Technology". *Estudiante Law* Journal 7 (1) (February 2025): 252-266. https://doi.org/10.33756/eslaj.v7i1.30794.

1. Introduction

The rapid development of digital technology in recent decades has had a significant impact on various aspects of life, including crime. One form of crime that has become more prevalent in the digital age is fraud involving information technology. Cyber fraud, as it is commonly known, has become a serious threat in many countries, including Indonesia. This crime refers to manipulative actions aimed at obtaining illegal gains through electronic media or the internet. Along with advancements in technology, particularly in the fields of finance and electronic transactions, many individuals and groups are exploiting gaps in the digital world to commit more sophisticated frauds that are harder to detect. In this context, blockchain technology, originally designed to ensure security and transparency in digital transactions, also has the potential to be used in digital crimes, including fraud and various other forms of criminal activity.[1]

Blockchain is a decentralized technology that allows secure, transparent, and immutable data storage after a transaction is made. This technology first gained widespread recognition through the introduction of Bitcoin, a digital currency that operates on a blockchain network. In this system, transactions made by users are recorded in a digital ledger that is open and accessible to all parties, yet protected using advanced cryptography. Blockchain enables the transfer of information or digital assets between parties without the need for third parties, such as banks or other financial institutions. The main advantage of blockchain technology is its decentralized nature, meaning no single party can control or alter the data recorded in it, making it highly secure and transparent.

However, despite offering various benefits in terms of security and transparency, blockchain also presents its own challenges, particularly regarding digital crime. Fraud crimes that leverage blockchain are often very difficult to trace and stop, given the anonymous and decentralized nature of the technology. Fraud carried out through blockchain often takes the form of fake investment schemes or illegal cryptocurrency scams. Criminals exploit the public's lack of understanding or their unfamiliarity with how blockchain and cryptocurrencies work to deceive victims. In many cases, these criminals promise high returns in a short time, luring many people into fraudulent investment schemes that result in financial losses.[2]

Digital fraud crimes involving blockchain are often difficult to detect by law enforcement authorities because transactions that occur on the blockchain network are recorded without identifying the users who conducted them. In many cases, users' identities are only recorded in the form of a digital address, which is an alphanumeric string that cannot be directly linked to an individual without additional information.

---

[1] Arlinta Prasetian Dewi and Mohammad Ichsan Hakiki, "Transformasi Digital Dalam Industri Halal Di Indonesia (Studi Implementasi Teknologi Blockchain Dalam Proses Sertifikasi Halal)," *Indo-Fintech Intellectuals: Journal of Economics and Business* 3, no. 2 (2023): 360–70.

[2] Putri Kinanti et al., "Melintasi Era Digital Dengan Menganalisis Hukum Cryptocurrency Dan Blokchain Dalam Yurisprudensi Modern," *Innovative: Journal Of Social Science Research* 4, no. 1 (2024): 920–32.

This provides protection for the criminals, as they can engage in illegal transactions without leaving clear traces. Additionally, the decentralized nature of blockchain makes it hard to monitor by any specific institution or party. Every transaction conducted on a blockchain network is permanent and cannot be altered or reversed, making it difficult to cancel a transaction that has already been made in fraud cases.

Even though efforts are being made to develop technologies capable of tracking blockchain transactions, the process remains highly complex and requires advanced technical skills. Many authorities, both at the national and international levels, still struggle to identify and address crimes occurring in cyberspace, especially those involving blockchain and cryptocurrency. One particularly harmful form of crime is cryptocurrency investment fraud. Criminals use blockchain to promise large profits through investments in digital currencies or blockchain projects that are either unauthorized or non-existent. Many individuals fall victim due to their lack of understanding of how this technology works and their inability to differentiate between legitimate and fraudulent investments.[3]

These types of fraud not only affect individuals but also companies and financial institutions involved in digital transactions. Many companies are trying to innovate by using blockchain technology to improve operational efficiency and security, but they also face significant risks related to potential fraud and other digital crimes.[4] In recent years, several fraudulent investment schemes involving blockchain and cryptocurrency have caused massive financial losses. The public, lacking in-depth understanding of blockchain and cryptocurrency technologies, is often an easy target for criminals looking to exploit their ignorance.

Furthermore, this issue becomes more complex with the emergence of various types of cryptocurrency and blockchain projects that promise high returns in a short time. Many projects operating under the guise of legitimate blockchain endeavors are actually designed to deceive people. These schemes are often referred to as "Ponzi

[3] Uli Wildan Nuryanto and Pramudianto Pramudianto, "Revolusi Digital & Dinamika Perkembangan Cryptocurrency Ditinjau Dari Perspektif Literatur Review," in *National Conference on Applied Business, Education, & Technology (NCABET)*, vol. 1, 2021, 264–91, http://ncabet.conferences-binabangsa.org/index.php/home/article/view/22.

[4] Mohamad Rivaldi Moha et al., "The Comparative Law Study: E-Commerce Regulation in Indonesia and Singapore," *JURNAL LEGALITAS* 16, no. 2 (October 30, 2023): 248–59, https://doi.org/10.33756/jelta.v16i2.20463; Dian Ekawaty Ismail et al., "Cyber Harassment of Public Figures: Causes and Importance of Legal Education," *E3S Web of Conferences* 594 (2024): 03005, https://doi.org/10.1051/e3sconf/202459403005; Rifky Pulubolo, Mutia Cherawaty Thalib, and Ahmad Ahmad, "Legal Process for Banking Negligence in Violations of Customers' Privacy Rights and Personal Data," *Estudiante Law Journal* 1, no. 1 (January 25, 2024): 1–13, https://doi.org/10.33756/eslaj.v1i1.24195; Abdusalam Rauf, Fenty U. Puluhulawa, and Ahmad Ahmad, "Ideal Arrangements for Fines to Enhance Legal Awareness and Minimize Waste Effectively in Society," *Estudiante Law Journal* 6, no. 3 (October 10, 2024): 593–606, https://doi.org/10.33756/eslaj.v6i3.28916; Viorizza Suciani Putri, Ahmad Ahmad, and Mohamad Hidayat Muhtar, "Antara Otoritas dan Otonomi : Pertautan Hak Asasi Manusia dalam Praktik Eksekusi Putusan PTUN: Perlindungan HAM dalam Eksekusi Upaya Paksa Terhadap Putusan Peradilan Tata Usaha Negara," *Jurnal Konstitusi* 21, no. 3 (September 1, 2024): 392–412, https://doi.org/10.31078/jk2133.

schemes," where money from new investors is used to pay returns to earlier investors, without any real assets or products being produced. This problem is often exacerbated by aggressive advertising and promotion on social media, which deceives many people into investing in unclear schemes.[5]

This phenomenon highlights the importance of education and public awareness regarding blockchain technology and the risks associated with it. The public needs to be provided with a better understanding of how blockchain works, how to identify legitimate investments, and how to protect themselves from digital fraud. Without sufficient understanding, people will continue to be vulnerable to fraudsters who exploit digital technology to commit crimes.

Efforts to address digital fraud crimes in the era of blockchain technology require a comprehensive and multidimensional approach. On one hand, existing criminal laws must be adjusted to keep up with rapidly evolving technology in order to provide maximum protection for the public. Law enforcement must be able to identify and pursue criminals using blockchain technology, employing the right tools to trace transactions and prove the occurrence of fraud. Effective law enforcement in the context of blockchain also requires collaboration between various agencies at both the national and international levels.[6]

On the other hand, the public must also be provided with better knowledge about blockchain technology and the potential crimes that can occur within it. Education on the risks and ways to protect oneself from digital crimes should be a crucial part of broader prevention efforts.[7] Additionally, authorities need to establish clear regulations concerning the use of blockchain technology and cryptocurrency to ensure that the industry can develop safely and securely for all parties involved.

In this regard, the role of relevant authorities and financial institutions is essential to maintaining the integrity of the blockchain and cryptocurrency systems. They must

---

[5] Rahmat Eka Putra R. Palaloi and Rakhmadi Rahman, "Analisis Dan Pencegahan Serangan Sosial Enginering Pada Jaringan Komputer Studi Kasus Penipuan Investasi Crypto," *Jurnal Riset Sistem Informasi* 1, no. 3 (2024): 08–16.

[6] Mia Ika Rahmawati and Anang Subardjo, "Apakah Blockchain Mampu Mencegah Kecurangan Akuntansi?," *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan* 4, no. Spesial Issue 5 (2022): 2204–10.

[7] Ahmad Ahmad, "Measuring The Application of Corporate Social Responsibility of PT. Gorontalo MineralS," *Estudiante Law Journal* 4, no. 2 (February 15, 2022): 132–45, https://doi.org/10.33756/eslaj.v4i2.16489; Ahmad Ahmad, Fence M. Wantu, and Dian Ekawaty Ismail, "Convergence of Constitutional Interpretation to the Test of Laws Through a Constitutional Dialogue Approach: Konvergensi Penafsiran Konstitusional Terhadap Pengujian Undang-Undang Melalui Pendekatan Constitutional Dialogue," *Jurnal Konstitusi* 20, no. 3 (September 1, 2023): 514–35, https://doi.org/10.31078/jk2038; Bintang Muhamad Hendri and Ahmad Ahmad, "Studying the Steps of the General Election Commission in Responding to the Recommendations of the Election Supervisory Body," *Estudiante Law Journal* 5, no. 2 (June 18, 2023): 393–406, https://doi.org/10.33756/eslaj.v5i2.18726; Maya Lasena et al., "Cockfighting Gambling Criminal Acts Commitment," *Estudiante Law Journal* 4, no. 2 (June 1, 2022): 77–90, https://doi.org/10.33756/eslaj.v4i2.16039; Novia Rahmawati A. Paruki and Ahmad Ahmad, "Efektivitas Penegakan Hukum Tambang Ilegal," *Batulis Civil Law Review* 3, no. 2 (August 26, 2022): 177–86, https://doi.org/10.47268/ballrev.v3i2.966.

ensure that the sector operates with high levels of transparency and accountability, minimizing opportunities for criminals to exploit this technology. Moreover, clear and firm regulations regarding the use of blockchain and cryptocurrency must be implemented immediately, so that criminals cannot easily exploit legal loopholes.[8]

However, despite the relevance of this issue, there is still a significant research gap in terms of a comprehensive study of blockchain-based digital crime. Previous research tends to focus on technical or regulatory aspects in isolation, without touching on the integration between technology, regulation, and public education. This research aims to fill that gap by developing a holistic approach to addressing blockchain-based digital crime.

2. Method

The method used in this study is a qualitative approach with a case study.[9] This research collects data through the analysis of legal documents, case reports, and interviews with legal practitioners and blockchain technology experts. The data obtained will be analyzed using content analysis techniques to identify patterns of fraud occurring in digital transactions involving blockchain. In addition, a literature review is also conducted to compare regulations in several countries regarding the counteraction of digital crimes. The results of this study are expected to provide insights into the challenges and solutions in addressing fraud crimes involving blockchain technology.

3. Challenges in Countering Fraud Crimes Involving Blockchain Technology

The development of digital technology in recent decades has had a significant impact on various aspects of human life, including the economic, social, and legal sectors. One of the most striking technological innovations in recent years is blockchain technology. Initially known through cryptocurrencies such as Bitcoin, this technology promises numerous benefits, ranging from transparency and decentralization to efficiency in conducting digital transactions. However, behind the great potential it offers, blockchain also presents significant challenges, particularly in terms of law enforcement, especially regarding fraud-related crimes.[10]

Blockchain is a decentralized data storage system that ensures each transaction is permanently recorded and cannot be altered once completed. By utilizing cryptography, this technology guarantees security and transparency in digital transactions. Despite the many positive aspects offered by blockchain, there is a dark

[8] Muhammad Citra Ramadhan and Arie Kartika, "Penegakan Hukum Pidana Terhadap Pelaku Tindak Pidana Penipuan Investasi Ilegal Dengan Cryptocurrency Pada Pasar Komoditi" (PhD Thesis, Universitas Medan Area, 2023), https://repositori.uma.ac.id/jspui/handle/123456789/21291.
[9] Ishaq, *Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, serta Disertasi* (ALFABETA, 2017).
[10] Blassyus Bevry Sinaga and Raia Putri Noer Azzura, "Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan Di Era Society 5.0," *Padjadjaran Law Review* 12, no. 1 (June 28, 2024): 71–82, https://doi.org/10.56895/plr.v12i1.1651.

side emerging as this technology develops. One of these is the increasing prevalence of fraud crimes that exploit blockchain. Fraud in the blockchain world is often difficult to detect and extremely complex, posing a significant challenge for law enforcement agencies to effectively address these issues.

One of the biggest challenges in combating crimes involving blockchain is the anonymity inherent in this technology. Transactions carried out within the blockchain network do not disclose the true identities of users, but only alphanumeric addresses that can be used to identify the parties involved in a transaction. While these transactions can be viewed by anyone on the network, the user's identity remains concealed. This makes it extremely difficult to track and identify perpetrators of crimes, such as cryptocurrency investment fraud. Fraudsters can exploit this anonymity to hide their identities and commit fraud without the risk of being exposed. In many cases, fraudsters use blockchain addresses not linked to real-world identities, making it difficult for authorities to find them.[11]

The anonymity issue is further exacerbated by the fact that blockchain technology operates within a decentralized system. Unlike traditional financial systems, which have intermediaries or supervisory institutions such as banks responsible for the transactions that occur, blockchain does not rely on any third party. This means there is no single authority that can control the entire system or be accountable for the transactions that occur within it. Every individual in the blockchain network has full control over their own transactions, without any third party overseeing or validating these transactions. This creates difficulties for law enforcement in identifying who is responsible for crimes occurring within the blockchain network.

While the decentralized nature of blockchain provides security and freedom for users, it also creates significant issues in terms of oversight and law enforcement. In the blockchain world, transactions can be conducted between two parties without any intervention from financial institutions or regulators. When fraud occurs within the blockchain context, law enforcement has no third party to hold accountable. For instance, if someone is deceived in a transaction involving digital currencies or investment in a blockchain project that turns out to be fraudulent, there is no institution or party that can be called upon to provide compensation or take responsibility for the loss.[12]

Moreover, blockchain technology is not bound by territorial or national legal boundaries. The blockchain network is global, meaning transactions can be conducted between users in different countries. This makes law enforcement increasingly complicated, as the laws of one country cannot be directly applied to users in another

---

[11] Tito Wira Eka Suryawijaya, "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia," *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 55–68.

[12] Erlangga Putra Widanta and Muhammad Risto Abrar, "Pemanfaatan Teknologi Blockchain Cryptocurrency Di Era Web 3.0," accessed February 27, 2025, https://www.academia.edu/download/88425382/Pemanfaatan_Teknologi_Blockchain_Cryptocurrency_di_Era_Web_3.0.docx.pdf.

country. Furthermore, some countries have not yet established clear regulations regarding the use of cryptocurrency or blockchain, further complicating efforts to combat fraud. At the same time, countries that have regulated cryptocurrency and blockchain often lack adequate mechanisms to handle fraud cases involving this technology, allowing criminals to evade responsibility by exploiting legal loopholes between countries.

In addition to decentralization and anonymity, fraud within the blockchain world is often highly complex and difficult to detect. Many criminals use sophisticated techniques to cover their tracks, such as creating fake blockchain projects that appear legitimate on the surface. Ponzi schemes and fake investments are often the main modus operandi in blockchain fraud. In these schemes, perpetrators promise significant profits in a short time and convince victims to invest in projects that lack underlying value or assets. One common example is perpetrators offering fake tokens or digital currencies that seemingly promise large returns, while in reality, they are simply gathering money from new investors to pay old investors. Once the funds have accumulated sufficiently, the perpetrators will withdraw and leave the victims deceived.[13]

When such fraud occurs, perpetrators are typically difficult to trace, as the transactions that take place within the blockchain are hard to reverse or recover. Blockchain guarantees that every transaction recorded in it is permanent and cannot be altered. Once money or digital assets change hands, there is no way to return them to the defrauded party. This causes blockchain fraud victims to feel increasingly trapped, as they cannot take legal action to recover their lost assets. Additionally, the tools used to track blockchain transactions are not yet sufficiently developed to handle fraud that occurs on a massive and global scale. Some existing blockchain transaction tracking tools still have limitations in terms of accuracy and speed, meaning they are not always able to detect fraud in a timely manner.

The next challenge is the lack of education and understanding among the public about how blockchain works and the risks associated with it. Although blockchain has become a popular topic in recent years, many people still do not fully understand how it operates. This lack of knowledge makes society more vulnerable to fraud involving this technology. Many people fall for investment schemes promising quick returns without realizing they are being exploited by fraudsters. The lack of education about how blockchain and cryptocurrency work makes it difficult for the public to distinguish between legitimate and fraudulent investments. Without adequate understanding, people will continue to be easy targets for fraudsters who exploit digital technology to deceive them.[14]

Finally, in order to address the challenges of fraud involving blockchain, a more comprehensive approach is required. On one hand, regulators and law enforcement

[13] Zayyan Hadhari Bik, "Manajemen Resiko, Tantangan Dan Ketidakpastian Regulasi Investasi Cryptocurrency Dalam Pandangan Ekonomi Syariah," *Jurnal Kewarganegaraan* 6, no. 3 (2022): 6466–78.
[14] Resa Endrawan, "Penggunaan Blockchain Smart Contract Dalam Sisi Keamanan Dan Cryptocurrency," *Researchgate. Net, April*, 2023, 0–10.

agencies must work together to develop clearer and more detailed regulations regarding the use of blockchain technology and cryptocurrency. These regulations must include ways to handle fraud occurring within the blockchain network and provide guidelines for the public and businesses on how to protect themselves from digital crime risks. On the other hand, the public must also be given a better understanding of the risks that can occur within the blockchain world. Education about blockchain and how to protect oneself from digital fraud should be a priority, so that society is better prepared to face these challenges.

International collaboration is also crucial, given the global nature of blockchain technology. Countries around the world need to work together to create uniform and effective policies to combat fraud involving blockchain. In this regard, technology and innovation can also play a key role in assisting law enforcement in tracking and identifying fraud perpetrators. By using more advanced tools to analyze and track blockchain transactions, authorities can improve their ability to uncover crimes occurring within the blockchain network. All these efforts, if done well, can help create a safer and more transparent blockchain ecosystem for all parties involved.

4. Solutions in Overcoming Fraud Crimes in the Blockchain Era

Blockchain is a technology that ensures transparency, security, and decentralization in various digital transactions. While this technology offers numerous benefits, it also presents significant challenges, particularly concerning crimes involving fraud. Fraud occurring through blockchain is often difficult to detect and even more complex due to the anonymous nature of transactions within the blockchain network. This type of fraud has become a serious challenge for law enforcement agencies in various countries. For instance, according to the Chainlysis Crypto Crime Report 2022, crimes involving cryptocurrency totaled more than $14 billion in that year, with fraud and fake investment schemes being the largest category. Therefore, addressing fraud crimes in the blockchain era requires an integrated and comprehensive approach involving analytical technology, clearer regulations, and public education on risks and how to protect themselves from digital fraud.[15]

One of the main solutions to tackle fraud involving blockchain is to utilize analytical technology to track and identify suspicious transaction traces. Blockchain is known for its transparency, where every transaction is recorded in a digital ledger accessible to the public. However, despite every transaction being recorded, user identities in the blockchain remain anonymous, which poses a significant issue in tracking and enforcing laws against digital crimes. This is where analytical technology plays a crucial role. The use of specialized software designed to track and map transactions in the blockchain network can assist law enforcement agencies in identifying suspicious transaction patterns, linking these transactions to specific individuals or entities, and finding perpetrators.

[15] Husnul Fatarib and Meirison Alizar Sali, "Cryptocurrency and Digital Money in Islamic Law: Is It Legal?," *Jurisdictie: Jurnal Hukum Dan Syariah* 11, no. 2 (2020): 237–61.

Several leading technology companies have now developed tools for blockchain forensics, such as Chainalysis, Elliptic, and CipherTrace. These tools allow law enforcement agencies to visualize the flow of funds in the blockchain network and trace transaction paths, even when different or anonymous digital addresses are used. For example, in 2021, Chainalysis helped U.S. authorities uncover a fraud scheme involving over $3 million collected through a fake cryptocurrency investment scam. By using this technology, authorities can determine whether a transaction is linked to crimes, such as investment fraud or money laundering. Through this analytical technology, law enforcement can map blockchain transactions, identify fraudsters, and gather enough evidence to take the necessary legal actions.[16]

However, despite the usefulness of analytical technology, it still has limitations, particularly in its ability to track transactions conducted in highly decentralized and careful ways. In some cases, criminals can use multiple wallets or blockchain addresses to conceal their tracks, making it harder to find the perpetrators. This poses a major challenge for law enforcement, and a similar challenge is faced in detecting Ponzi schemes, which are increasingly difficult to identify. For example, in the BitPetite case in 2020, the perpetrators used a series of separate blockchain addresses to avoid tracking and deceive investors. Therefore, in addition to analytical technology, another crucial solution in addressing fraud in blockchain is the introduction of clearer and more stringent regulations regarding the use of blockchain and cryptocurrency.

The implementation of clear and detailed regulations concerning blockchain and cryptocurrency is essential to reduce the potential for abuse of this technology. Currently, many countries do not have comprehensive regulations governing blockchain usage. This lack of regulatory clarity allows criminals to exploit legal loopholes and commit fraud without fear of punishment. Therefore, clear regulations are needed to ensure that blockchain technology and cryptocurrency are used legally and are not misused for personal gain that harms others. One example of regulation that can be implemented is requiring cryptocurrency platforms to carry out identity verification (Know Your Customer/KYC) for their users. Through KYC verification, authorities can ensure that the transactions carried out by individuals or entities involved in the blockchain can be identified, thus minimizing the chances of fraud.[17]

Governments in various countries, such as the United States and several European nations, have already begun regulating cryptocurrency usage with regulations like Anti-Money Laundering (AML) and counter-terrorism financing measures. These regulations require financial institutions and cryptocurrency platforms to report suspicious transactions and verify user identities, which is crucial in preventing fraud. In Indonesia, although there are some policies related to cryptocurrency, regulations

[16] Intan Monica Gulo et al., "Pengaruh Mata Uang Digital Pada Akuntansi Keuangan," *Jurnal Riset Ilmiah Manajemen Dan Akuntansi* 1, no. 1 (2024): 38–45.

[17] Muhammad Naufal Hasani et al., "Analisis Cryptocurrency Sebagai Alat Alternatif Dalam Berinvestasi Di Indonesia Pada Mata Uang Digital Bitcoin," *Jurnal Ilmiah Ekonomi Bisnis* 8, no. 2 (2022): 329–44.

regarding blockchain are still limited and lack strong legal certainty. Therefore, the government needs to develop more comprehensive regulations regarding blockchain and cryptocurrency use in Indonesia. These regulations should focus on overseeing blockchain and cryptocurrency platforms offering investment and trading services and require them to adhere to strict security procedures.[18]

Additionally, regulations related to blockchain should also provide guidelines on how suspicious transactions should be handled by authorities. Such regulations would give law enforcement clearer authority in addressing fraud and crimes involving blockchain. For instance, the regulation could include requirements for platforms to audit registered blockchain or cryptocurrency projects to make it easier to detect projects with potential fraud or Ponzi schemes.

Although analytical technology and regulations are crucial, another important solution in combating digital fraud crimes is public education on the risks involved and how to protect oneself from fraud. Most frauds involving blockchain occur because the public does not fully understand how this technology works and how to protect themselves from the risks of fraud. Many cryptocurrency fraud victims are attracted to investments promising quick profits without truly understanding the fundamentals of blockchain technology. Therefore, improving digital literacy and education about blockchain is crucial to reducing the potential for fraud.[19]

Education about blockchain and cryptocurrency should start at an early age. Governments, educational institutions, and non-governmental organizations can collaborate to organize educational programs and outreach about blockchain, in the form of seminars, workshops, or online courses. This education should not only cover how blockchain works but also how to identify signs of digital fraud and how to protect personal data and digital assets. By providing a better understanding of the risks associated with blockchain technology, the public will become more cautious about potential fraud and more careful when investing.

One way to improve digital literacy is by holding public awareness campaigns. These campaigns can include explanations about common types of fraud in the cryptocurrency world, such as investment fraud, Ponzi schemes, and phishing scams. Additionally, these campaigns can also provide information on how to recognize legitimate and illegitimate blockchain projects, as well as how to report fraud cases to authorities. As more people are educated, it is expected that the number of fraud victims will decrease significantly.[20]

---

[18] Kevin Septianzah and Gilang Ryan Fernandes, "Blockchain Techonology for Payless Transactions and Investment Activities in the Digital Era With a SWOT Approach," in *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)*, vol. 5, 2021, 012–017, https://proceeding.unpkediri.ac.id/index.php/inotek/article/view/895.

[19] Yuli Destriani Sirait, "Blockchain Dalam Dunia Keuangan: Teknologi Desentralisasi Untuk Transaksi Aman," *Circle Archive* 1, no. 6 (2024), http://circle-archive.com/index.php/carc/article/view/294.

[20] SUWITO SUWITO, "Penegakan Hukum Terhadap Pelaku Tindak Pidana Pencucian Dari Hasil Penipuan Investasi Dengan Modus Cryptocurrency (Bitcoin)" (PhD Thesis, Universitas Islam Sultan

Furthermore, education should also be provided to blockchain developers and industry participants. Blockchain developers and cryptocurrency platform providers need to be better informed about ethics and social responsibility in managing their projects. They must be reminded that, in addition to seeking profits, they also bear the responsibility to ensure that the technology they develop is not misused by irresponsible parties. Clear regulations and stronger ethical guidelines in this industry will create a safer and more transparent ecosystem for users.[21]

Overall, combating fraud involving blockchain requires a multidimensional approach. Effective solutions must involve analytical technology to detect suspicious transactions, the implementation of clear regulations to govern blockchain usage, and enhanced digital literacy to protect the public from fraud. By combining these three solutions, we can create a safer and more trustworthy blockchain ecosystem that will reduce the potential for fraud and provide better protection for digital technology users. Collaboration between governments, the blockchain industry, and the public is crucial to create a secure, transparent, and reliable system in combating digital fraud in the blockchain era.[22] With greater and coordinated efforts, it is hoped that blockchain technology can continue to develop positively without posing harmful threats to users and society as a whole.

5. Conclusion

The conclusion of the discussion on the challenges and solutions to address fraud crimes involving blockchain technology highlights that tackling this issue requires a comprehensive approach. The anonymous and decentralized nature of blockchain presents a primary challenge for law enforcement, as it complicates the identification of perpetrators. Analytical technologies, such as blockchain forensics, can offer a solution for tracking transactions and uncovering the perpetrators' traces. Additionally, clearer and more stringent regulations on the use of blockchain and cryptocurrency need to be implemented to close legal loopholes that fraudsters can exploit. Equally important is the need to strengthen public education on the risks of digital fraud to raise awareness and digital literacy, so that people can be more cautious and protect themselves from scams. By combining technology, strong regulations, and proper education, we can create a safer and more transparent blockchain ecosystem and reduce the potential for digital crimes that harm many parties.

Agung Semarang, 2024), http://repository.unissula.ac.id/37016/1/Magister%20Ilmu%20Hukum_20302200324_fullpdf.pdf.

[21] Donny Trihanondo and Soni Sadono, "Token Non-Fungible (NFT) Sebagai Instrumen Investasi Seni Berbasis Blockchain," *Ideas: Jurnal Pendidikan, Sosial, Dan Budaya* 9, no. 2 (2023): 333–42.

[22] Angelina Agung Putri Zaman and Anita Zulfiani, "Pertanggungjawaban Pidana Penggunaan Mata Uang Digital (Cryptocurrency) Sebagai Sarana Tindak Pidana Pencucian Uang," accessed February 27, 2025, https://www.researchgate.net/profile/Angel-Zaman-2/publication/381639433_Pertanggungjawaban_Pidana_Penggunaan_Mata_Uang_Digital_Cryptocurrency_Sebagai_Sarana_Tindak_Pidana_Pencucian_Uang/Links/6677db2a1846ca33b84599d0/Pertanggungjawaban-Pidana-Penggunaan-Mata-Uang-Digital-Cryptocurrency-Sebagai-Sarana-Tindak-Pidana-Pencucian-Uang.Pdf.

References

Ahmad, Ahmad. "Measuring The Application of Corporate Social Responsibility of PT. Gorontalo MineralS." *Estudiante Law Journal* 4, no. 2 (February 15, 2022): 132–45. https://doi.org/10.33756/eslaj.v4i2.16489.

Ahmad, Ahmad, Fence M. Wantu, and Dian Ekawaty Ismail. "Convergence of Constitutional Interpretation to the Test of Laws Through a Constitutional Dialogue Approach: Konvergensi Penafsiran Konstitusional Terhadap Pengujian Undang-Undang Melalui Pendekatan Constitutional Dialogue." *Jurnal Konstitusi* 20, no. 3 (September 1, 2023): 514–35. https://doi.org/10.31078/jk2038.

Bik, Zayyan Hadhari. "Manajemen Resiko, Tantangan Dan Ketidakpastian Regulasi Investasi Cryptocurrency Dalam Pandangan Ekonomi Syariah." *Jurnal Kewarganegaraan* 6, no. 3 (2022): 6466–78.

Dewi, Arlinta Prasetian, and Mohammad Ichsan Hakiki. "Transformasi Digital Dalam Industri Halal Di Indonesia (Studi Implementasi Teknologi Blockchain Dalam Proses Sertifikasi Halal)." *Indo-Fintech Intellectuals: Journal of Economics and Business* 3, no. 2 (2023): 360–70.

Endrawan, Resa. "Penggunaan Blockchain Smart Contract Dalam Sisi Keamanan Dan Cryptocurrency." *Researchgate. Net, April*, 2023, 0–10.

Fatarib, Husnul, and Meirison Alizar Sali. "Cryptocurrency and Digital Money in Islamic Law: Is It Legal?" *Jurisdictie: Jurnal Hukum Dan Syariah* 11, no. 2 (2020): 237–61.

Gulo, Intan Monica, Albertus Ray Calvin Lase, Noviza Asni Waruwu, and Sanday Putra Kurnia Sang Putra Mei. "Pengaruh Mata Uang Digital Pada Akuntansi Keuangan." *Jurnal Riset Ilmiah Manajemen Dan Akuntansi* 1, no. 1 (2024): 38–45.

Hasani, Muhammad Naufal, Muhammad Ramadhan, Kristin Mariyani, Reksa Setiawan, and Irma Sucidha. "Analisis Cryptocurrency Sebagai Alat Alternatif Dalam Berinvestasi Di Indonesia Pada Mata Uang Digital Bitcoin." *Jurnal Ilmiah Ekonomi Bisnis* 8, no. 2 (2022): 329–44.

Hendri, Bintang Muhamad, and Ahmad Ahmad. "Studying the Steps of the General Election Commission in Responding to the Recommendations of the Election Supervisory Body." *Estudiante Law Journal* 5, no. 2 (June 18, 2023): 393–406. https://doi.org/10.33756/eslaj.v5i2.18726.

Ishaq. *Metode Penelitian Hukum dan Penulisan Skripsi, Tesis, serta Disertasi*. ALFABETA, 2017.

Ismail, Dian Ekawaty, Jufriyanto Puluhulawa, Novendri M. Nggilu, Ahmad Ahmad, and Ottow W. T. G. P. Siagian. "Cyber Harassment of Public Figures: Causes and Importance of Legal Education." *E3S Web of Conferences* 594 (2024): 03005. https://doi.org/10.1051/e3sconf/202459403005.

Kinanti, Putri, Rival Mahesa, Fathan Hariz, Prastiti Suryaning Ramadhani, Yasmin Sobikhoh Nawaidah, and Diani Sadia Wati. "Melintasi Era Digital Dengan Menganalisis Hukum Cryptocurrency Dan Blokchain Dalam Yurisprudensi Modern." *Innovative: Journal Of Social Science Research* 4, no. 1 (2024): 920–32.

Lasena, Maya, Fenty U. Puluhulawa, Fence M. Wantu, and Ahmad Ahmad. "Cockfighting Gambling Criminal Acts Commitment." *Estudiante Law Journal* 4, no. 2 (June 1, 2022): 77–90. https://doi.org/10.33756/eslaj.v4i2.16039.

Moha, Mohamad Rivaldi, Ahmad Ahmad, Amanda Adelina Harun, and Nurul Fazri Elfikri. "The Comparative Law Study: E-Commerce Regulation in Indonesia and Singapore." *JURNAL LEGALITAS* 16, no. 2 (October 30, 2023): 248–59. https://doi.org/10.33756/jelta.v16i2.20463.

Nuryanto, Uli Wildan, and Pramudianto Pramudianto. "Revolusi Digital & Dinamika Perkembangan Cryptocurrency Ditinjau Dari Perspektif Literatur Review." In *National Conference on Applied Business, Education, & Technology (NCABET)*, 1:264–91, 2021. http://ncabet.conferences-binabangsa.org/index.php/home/article/view/22.

Palaloi, Rahmat Eka Putra R., and Rakhmadi Rahman. "Analisis Dan Pencegahan Serangan Sosial Enginering Pada Jaringan Komputer Studi Kasus Penipuan Investasi Crypto." *Jurnal Riset Sistem Informasi* 1, no. 3 (2024): 08–16.

Paruki, Novia Rahmawati A., and Ahmad Ahmad. "Efektivitas Penegakan Hukum Tambang Ilegal." *Batulis Civil Law Review* 3, no. 2 (August 26, 2022): 177–86. https://doi.org/10.47268/ballrev.v3i2.966.

Pulubolo, Rifky, Mutia Cherawaty Thalib, and Ahmad Ahmad. "Legal Process for Banking Negligence in Violations of Customers' Privacy Rights and Personal Data." *Estudiante Law Journal* 1, no. 1 (January 25, 2024): 1–13. https://doi.org/10.33756/eslaj.v1i1.24195.

Putri, Viorizza Suciani, Ahmad Ahmad, and Mohamad Hidayat Muhtar. "Antara Otoritas dan Otonomi : Pertautan Hak Asasi Manusia dalam Praktik Eksekusi Putusan PTUN: Perlindungan HAM dalam Eksekusi Upaya Paksa Terhadap Putusan Peradilan Tata Usaha Negara." *Jurnal Konstitusi* 21, no. 3 (September 1, 2024): 392–412. https://doi.org/10.31078/jk2133.

Rahmawati, Mia Ika, and Anang Subardjo. "Apakah Blockchain Mampu Mencegah Kecurangan Akuntansi?" *Fair Value: Jurnal Ilmiah Akuntansi Dan Keuangan* 4, no. Spesial Issue 5 (2022): 2204–10.

Ramadhan, Muhammad Citra, and Arie Kartika. "Penegakan Hukum Pidana Terhadap Pelaku Tindak Pidana Penipuan Investasi Ilegal Dengan Cryptocurrency Pada Pasar Komoditi." PhD Thesis, Universitas Medan Area, 2023. https://repositori.uma.ac.id/jspui/handle/123456789/21291.

Rauf, Abdusalam, Fenty U. Puluhulawa, and Ahmad Ahmad. "Ideal Arrangements for Fines to Enhance Legal Awareness and Minimize Waste Effectively in Society." *Estudiante Law Journal* 6, no. 3 (October 10, 2024): 593–606. https://doi.org/10.33756/eslaj.v6i3.28916.

Septianzah, Kevin, and Gilang Ryan Fernandes. "Blockchain Techonology for Payless Transactions and Investment Activities in the Digital Era With a SWOT Approach." In *Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi)*, 5:012–017, 2021. https://proceeding.unpkediri.ac.id/index.php/inotek/article/view/895.

Sinaga, Blassyus Bevry, and Raia Putri Noer Azzura. "Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan Di Era Society 5.0." *Padjadjaran Law Review* 12, no. 1 (June 28, 2024): 71–82. https://doi.org/10.56895/plr.v12i1.1651.

Sirait, Yuli Destriani. "Blockchain Dalam Dunia Keuangan: Teknologi Desentralisasi Untuk Transaksi Aman." *Circle Archive* 1, no. 6 (2024). http://circle-archive.com/index.php/carc/article/view/294.

Suryawijaya, Tito Wira Eka. "Memperkuat Keamanan Data Melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses Dalam Transformasi Digital Di Indonesia." *Jurnal Studi Kebijakan Publik* 2, no. 1 (2023): 55–68.

SUWITO, SUWITO. "Penegakan Hukum Terhadap Pelaku Tindak Pidana Pencucian Dari Hasil Penipuan Investasi Dengan Modus Cryptocurrency (Bitcoin)." PhD Thesis, Universitas Islam Sultan Agung Semarang, 2024. http://repository.unissula.ac.id/37016/1/Magister%20Ilmu%20Hukum_20302200324_fullpdf.pdf.

Trihanondo, Donny, and Soni Sadono. "Token Non-Fungible (NFT) Sebagai Instrumen Investasi Seni Berbasis Blockchain." *Ideas: Jurnal Pendidikan, Sosial, Dan Budaya* 9, no. 2 (2023): 333–42.

Widanta, Erlangga Putra, and Muhammad Risto Abrar. "Pemanfaatan Teknologi Blockchain Cryptocurrency Di Era Web 3.0." Accessed February 27, 2025. https://www.academia.edu/download/88425382/Pemanfaatan_Teknologi_Blockchain_Cryptocurrency_di_Era_Web_3.0.docx.pdf.

Zaman, Angelina Agung Putri, and Anita Zulfiani. "Pertanggungjawaban Pidana Penggunaan Mata Uang Digital (Cryptocurrency) Sebagai Sarana Tindak

Pidana Pencucian Uang." Accessed February 27, 2025. https://www.researchgate.net/profile/Angel-Zaman-2/publication/381639433_PERTANGGUNGJAWABAN_PIDANA_PENGGUNAAN_MATA_UANG_DIGITAL_CRYPTOCURRENCY_SEBAGAI_SARANA_TINDAK_PIDANA_PENCUCIAN_UANG/links/6677db2a1846ca33b84599d0/PERTANGGUNGJAWABAN-PIDANA-PENGGUNAAN-MATA-UANG-DIGITAL-CRYPTOCURRENCY-SEBAGAI-SARANA-TINDAK-PIDANA-PENCUCIAN-UANG.pdf.