Media Iuris Vol. 7 No. 3, October 2024 p-ISSN: 2721-8384
DOI: 10.20473/mi.v7i3.56116 e-ISSN: 2621-5225
Article history: Submitted 19 March 2024; Accepted 30 September 2024; Available online 18 October 2024.
How to cite: Gorizky and Supardi, 'Blockchain as Electronic Evidence Against Crypto Crimes in Indonesia' (2024) 7 Media Iuris.

Blockchain as Electronic Evidence Against Crypto Crimes in Indonesia

Gorizky[1] and Supardi[2]
[1] Faculty of Law, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia.
E-mail: gorizkygorizky306@upnvj.ac.id
[2] Faculty of Law, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia.
E-mail: supardi@upnvj.ac.id

Keywords:
Blockchain; Electronic Evidence; Crypto Crimes.

Abstract
In the context of digital security, the utilization of blockchain technology as a means of evidence against crypto crimes has become an exceedingly crucial topic. This research elucidates whether the admissible evidence tool stipulated in Article 184 paragraph (1) of the criminal procedural law encompasses proof relating to crypto crimes and how the decentralized structure and transparent nature of blockchain can aid in furnishing accurate and credible evidence pertaining to crypto crimes. This study offers profound insights into the potential of blockchain concerning evidence provision and prevention of crypto crimes. The author employs normative research, a process aimed at uncovering legal rules, principles, and doctrines to address legal issues encountered. Based on the discussion, it can be concluded that blockchain can serve as an electronic evidence tool in crypto crimes. Aligned with the decentralized and transparent nature of blockchain, it can provide precise and permanent data.

Introduction

The development of technology in human life begins with simple processes in daily life and progresses to the fulfillment of satisfaction as individuals and social beings. From time to time, technological advancement continues to evolve, starting from the era of agricultural technology, industrial technology, information technology, to communication and information technology. This development brings various impacts on societal, national, and international levels, where every individual is interested in utilizing and benefiting from these advancements.[1]

In the 18th and 19th centuries, the industrial revolution brought significant changes to the way humans produce goods and services. Human lifestyle patterns changed drastically with the advent of steam engines, railway transportation, and advancements in the textile industry. During this period, technological development began, such as the

[1] Danuri, 'Perkembangan Informasi Dan Teknologi' (INFOKAM, Nomor II Th. XV/SEPTEMBER/2019).

telegraph and telephone. In the 20th century, transportation continued to advance, marked by the development of airplanes, automobiles, and more. Beyond transportation, the discovery of DNA (deoxyribonucleic acid) played a crucial role in technological progress.

Information and communication technology has rapidly advanced, and the internet has become essential in daily life. Not only the internet, but computers also play a vital role in solving human problems. The transformation of humanity into the digital era is being accelerated by technological advancements, such as the Internet of Things (IoT), Artificial Intelligence (AI), blockchain, and other technologies. These technological advancements change the way humans work, communicate, and live their daily lives.

This research focuses on one of the current technological advancements, specifically blockchain. Along with the development of blockchain technology, crimes in the world of crypto or digital currencies are increasing. As the underlying technology of cryptocurrencies like Bitcoin, Ethereum, and others, blockchain provides good security and transparency. However, crypto crimes such as money laundering, embezzlement, fraud, and other illegal activities are also becoming more sophisticated. Proof through blockchain emerges as a solution to address these issues.

Generally, blockchain is a collection of interconnected blocks containing various records of transactional data and can be utilized to track the existence of an asset within the network.[2] Blockchain operates on a system of digital transaction storage. It permanently records every transaction made, storing the data in a public database known as a ledger. This ledger is distributed; transactions are stored in blocks and distributed across a peer-to-peer network where each node stores a copy of the ledger. As a data center, blockchain is designed to store electronic information in digital format securely and in a decentralized manner.[3] Blockchain is a decentralized ledger that stores all transactions systematically and chronologically.

Blockchain, as the underlying technology behind cryptocurrencies such as Bitcoin and Ethereum, has opened doors to various applications beyond the financial realm,

[2] Hendrik, 'Pengertian Blockchain: Sejarah, Asas Dan Cara Kerjanya' (Gramedia Blog, 2022) https://www.gramedia.com/literasi/pengertian-blockchain/, accessed on 1 March 2024.

[3] Muhammad Akbar, 'Blockchain: Pengertian, Manfaat, Dan Cara Kerjanya' (BINUS ONLINE, 2020) 20.

including legal and security aspects. Crypto crimes, involving fraud, money laundering, and other criminal activities involving digital currencies, have become increasingly complex with the growth of the crypto ecosystem. In addressing these challenges, blockchain emerges as a potential electronic evidence tool to combat crypto crimes.[4]

As a decentralized ledger that transparently and securely records transactions, blockchain holds the potential to provide reliable electronic evidence tools. Through this decentralized approach, every transaction within the blockchain network can be verified and accessed by stakeholders, providing the necessary transparency to identify and combat crypto crimes.[5]

By analyzing blockchain's ability to verify transactions, trace the origins of digital assets, and enhance transparency, we can understand how this technology can serve as a crucial ally in the effort to combat crypto crimes. However, it is important to note that, while blockchain can be an effective electronic evidence tool, the challenges and ethical considerations associated with its use also need to be considered.

In this article, we will further explore how blockchain not only provides security for the crypto ecosystem but also lays a solid foundation for electronic evidence tools in combating the increasingly sophisticated crypto crimes.

Research Method

The research method utilized is normative legal research, which involves examining bibliographical materials or secondary data.[6] Normative legal research is a process aimed at discovering legal rules, principles, and legal doctrines to address legal issues encountered.[7] The process of normative legal research involves critically analyzing legal documents and existing legal literature. The initial step involves identifying the legal issues that need clarification or resolution. Subsequently, the researcher will search for

[4] Arwono DG, Iskandar H, and Wardana DJ, 'Tinjauan Yuridis Regulasi Cryptocurrency Terhadap Tindak Pidana Kejahatan Di Indonesia' (2023) 5(1) Amnesti Jurnal Hukum 110–125 https://jurnal.umpwr.ac.id/index.php/amnesti/article/view/2759.

[5] Ibid.

[6] Soekanto, Soerjono, and Sri Mamuji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Raja Grafindo Persada 2013) 87.

[7] Marzuki, Peter Mahmud, *Penelitian Hukum* (Kencana Pranada Media Group 2007) 50.

relevant bibliographical materials to support the research as secondary legal resources in the form related publication.[8] This research will rely on Law No 8 of 1981 concerning Criminal Procedure Law and Law No 19 of 2016 concerning Information and Electronic Transaction as main primary laws and regulations.

Inception of Blockchain

Cryptocurrencies, including Bitcoin, operate on a distributed ledger system known as blockchain, which records transactions across multiple nodes globally.[9] Unlike traditional ledgers maintained by centralized entities like banks, blockchain eliminates the need for a single trusted authority by distributing the ledger among multiple nodes. This decentralization enhances security, with the integrity of the ledger protected against unauthorized alterations.[10] Notably, Bitcoin, with its approximately 15,000 full nodes, exemplifies a permissionless and trustless network, enabling users to transact without intermediaries.[11]

Bitcoin's genesis in 2009 emerged as a response to the 2008 financial crisis, with its blockchain now comprising over 777,949 blocks. While Bitcoin facilitates international transfers, its 10-minute block creation time renders it impractical for most retail transactions. To address this limitation, the Lightning Network was introduced, enabling near-instant Bitcoin transactions at minimal costs.[12] Notably, El Salvador, an early adopter of Bitcoin as legal tender, leveraged the Lightning Network for government-to-citizen transactions.[13]

Bitcoin's distributed consensus mechanism, known as mining, employs cryptographic hashing to confirm transactions and secure the blockchain.[14] However,

[8] Faizal Kurniawan *et al*, 'Evidence of Contract Dispute Settlement in Electronic Trials in Indonesia in the Construction of the Ius Constitutum dan Ius Constituendum' (2021) E-Book of Extended Abstract UiTM International Conference on Law & Society.

[9] Reza Soltani, Marzia Zaman, Rohit Joshi, and Srinivas Sampalli, 'Distributed Ledger Technologies and Their Applications: A Review' (2022) 12 Applied Sciences 7898.

[10] Filipe Pinto, Catarina Ferreira da Silva, and Sergio Moro, 'People-centered distributed ledger technology-IoT architectures: A systematic literature review' (2022) 70 Telematics and Informatics 101812.

[11] Andrew M. Bailey and Craig Warmke, 'Bitcoin is King' in Cryptocurrency: Concepts, Technology, and Issues, ed. by J. Liebowitz (London and New York: Taylor & Francis, 2023) 175–197.

[12] Anantha Divakaruni and Peter Zimmerman, 'The Lightning Network: Turning Bitcoin into Money' (2023) 52 Finance Research Letters 103480.

[13] Luke Taylor, The World's First Bitcoin Republic (Amsterdam: Elsevier, 2022).

[14] David Allenotor and D. A. Oyemade, 'An Optimized Parallel Hybrid Architecture for Cryptocurrency Mining' (2021), available online: https://www.isteams.net/_files/ugd/185b0a_6f88b82981424f87850d11fea3f52e1b.pdf, accessed on 27 February 2023.

mining's proof-of-work model has drawn criticism for its high energy consumption, prompting exploration of alternative consensus mechanisms like proof of stake.[15] In proof of stake, validators are selected based on their stake in the cryptocurrency, aiming to incentivize network security and efficiency.

To transact on the blockchain, users possess public and private keys, akin to email addresses and passwords, respectively. While public keys enable receipt of cryptocurrency, private keys authorize transactions, emphasizing the importance of safeguarding them. Digital wallets streamline this process by storing private keys and enabling seamless transactions, though users must remain vigilant against loss or theft.

Beyond Bitcoin, digital assets encompass various classes, including stable coins, governance tokens, and smart contract-capable assets, each serving distinct purposes within decentralized ecosystems.[16]

Despite the technological advancements and potential benefits of cryptocurrencies, concerns persist regarding energy consumption, money laundering, fraud, tax evasion, and illicit activities.[17] Consequently, regulatory responses vary globally, with some jurisdictions embracing digital assets as catalysts for innovation while others impose stringent regulations or outright bans. Notably, countries like El Salvador and the Central African Republic have embraced Bitcoin as legal tender, signaling a paradigm shift in the financial ecosystem.[18]

Example of Crimes Involving Cryptocurrency

The landscape of cryptocurrency legislation often remains ambiguous, necessitating further clarification.[19] Similar to any tool, cryptocurrency harbors potential for

[15] Moritz Wendl, My Hanh Doan, and Remmer Sassen, 'The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review' (2023) 326 Journal of Environmental Management 116530.

[16] Lennart Ante, Ingo Fiedler, Jan Marius Willruth, and Fred Steinmetz, 'A Systematic Literature Review of Empirical Research on Stablecoins' (2023) 2 FinTech 34–47, available online: https://www.mdpi.com/2674-1032/2/1/3 (accessed on 27 February 2023).

[17] Jon Truby, 'Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies' (2018) 44 Energy Research & Social Science 399–410.

[18] Fernando E. Alvarez, David Argente, and Diana Van Patten, Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador (Cambridge: National Bureau of Economic Research, 2022).

[19] Sergio Luis Náñez Alonso, 'Activities and Operations with Cryptocurrencies and Their Taxation Implications: The Spanish Case' (2019) 8 Laws 16 https://www.mdpi.com/2075-471X/8/3/16 accessed on 27 February 2023.

both constructive and illicit purposes. Predominantly, criminal activities involving cryptocurrency revolve around fraud or theft, commonly manifesting as breaches of crypto wallets. During Bitcoin's inception, it acquired a reputation for its association with unlawful activities, particularly its use on like the Silk Road, a dark web marketplace facilitating illegal trade.[20] This was largely attributed to Bitcoin's perceived anonymity and limited adoption. Presently, while cryptocurrency can indeed be utilized for illicit transactions or money laundering, contemporary criminal activities predominantly involve fraud or cyber intrusions, often exploiting victims' unfamiliarity with the industry to abscond with cryptocurrency.[21] This section will present four instances of cryptocurrency-related crimes or alleged illicit activities, encompassing jurisdictional complexities.

First, deceptive Initial Coin Offering or ICO. When corporations seek funding, they traditionally issue stocks. In the realm of cryptocurrency, projects raise capital through initial coin offerings (ICOs).[22] While not all projects resort to ICOs, they are prevalent among endeavors necessitating substantial developmental efforts over time. This centralized reliance on the development team and the initial concentration of coins pose characteristics akin to securities, falling under the purview of regulatory bodies like the US Securities and Exchange Commission. While not all cryptocurrencies opt for ICOs (e.g., Bitcoin), which commenced in a considerably decentralized fashion.

Investors participating in ICOs often pay a premium based on the expectation of continued project development. However, numerous fraudulent entities exploit this trust through tactics like "rug pulls", where promises outlined in white papers are abandoned post-funding.[23] Such scams proliferated during the 2017 cryptocurrency market boom, detrimentally impacting investors and impeding legitimate capital raising efforts.[24]

[20] Amy Phelps and Allan Watt, 'I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia' (2014) 11 Digital Investigation 261–272.

[21] Mark A. Nickerson, 'Fraud in a world of advanced technologies: The possibilities are (unfortunately) endless' (2019) 89 The CPA Journal 28–34.

[22] Zhijie Tao, Bo Peng, and Lina Ma, 'Optimal initial coin offering under speculative token trading' (2023) 306 European Journal of Operational Research 632–644.

[23] David S. Kerr, Karen A. Loveland, Katherine Taken Smith, and Lawrence Murphy Smith, 'Cryptocurrency Risks, Fraud Cases, and Financial Performance' (2023) 11 Risks 51.

[24] Christoph Wronka, 'Financial crime in the decentralized finance ecosystem: New challenges for compliance' (2023) 30 Journal of Financial Crime 97–113.

In the instance of OneCoin, founders promoted packages facilitating OneCoin token mining—an imaginary cryptocurrency that was never actualized.[25] This resulted in investors being defrauded of billions, leading to convictions and indictments for conspiracy and fraud charges. Despite challenges in asserting jurisdiction over global activities, founders' widespread promotional efforts suggest submission to multiple jurisdictions.

Secondly, the FTX misappropriation. The FTX debacle underscores issues within centralized exchanges rather than inherent problems with cryptocurrency. FTX's collapse led to substantial losses for users, emphasizing the importance of transferring assets to private wallets. Unlike banks, which operate as custodians, crypto exchanges function more as creditors, lacking government insurance. The FTX case involved loans of customer funds to an affiliated investment firm, leading to insolvency when asset values plummeted.

FTX's active targeting of US customers and engagement in US-based activities establish grounds for jurisdiction, although implications for account holders in other jurisdictions remain unclear.

The hack of Mt Gox in 2014 sent shockwaves through the cryptocurrency community, exposing the vulnerabilities of centralized exchanges and shaking investor confidence in the nascent asset class.[26] Originally established as a platform for trading card games, Mt Gox grew to become the largest Bitcoin exchange in the world, handling the majority of global Bitcoin transactions. However, the hack resulted in the theft of hundreds of thousands of Bitcoins, leading to the exchange's eventual bankruptcy filing and ongoing legal proceedings. The fallout from the Mt Gox breach highlighted the need for robust security measures and risk management protocols within cryptocurrency exchanges.

Beyond the immediate financial losses, the Mt Gox hack raised profound questions about jurisdictional authority and regulatory oversight in the cryptocurrency space. The decentralized nature of cryptocurrencies complicates the attribution of responsibility

[25] Muneer M. Alshater, Mayank Joshipura, Rim El Khoury, and Nohade Nasrallah, 'Initial Coin Offerings: A Hybrid Empirical Review' (2023) Small Business Economics, 1–18.

[26] Marco Linton, Ernie Gin Swee Teo, Elisabeth Bommes, C. Y. Chen, and Wolfgang Karl Härdle, Dynamic Topic Modelling for Cryptocurrency Community Forums (Berlin/Heidelberg: Springer, 2017).

and enforcement of legal remedies, particularly in cases involving transnational criminal activity. Moreover, the global distribution of victims and perpetrators further exacerbates these challenges, underscoring the need for international cooperation and coordination among law enforcement agencies and regulatory bodies.

Lastly, Tornado Cash money laundering allegations. Tornado Cash, a privacy-focused Ethereum mixer, exemplifies the tension between privacy rights and regulatory compliance in the cryptocurrency space.[27] While designed to enhance the anonymity of cryptocurrency transactions, Tornado Cash has faced scrutiny for its potential facilitation of illicit activities, including money laundering and terrorist financing. The allegations against Tornado Cash raise complex legal and ethical questions about the responsibilities of developers and the regulation of decentralized technologies.

The case of Tornado Cash highlights the evolving nature of financial crime in the digital age and the challenges it poses to traditional law enforcement and regulatory frameworks. As cryptocurrencies continue to gain mainstream acceptance, regulators face mounting pressure to strike a balance between fostering innovation and safeguarding against illicit activities. However, the decentralized and pseudonymous nature of cryptocurrencies complicates traditional law enforcement efforts, requiring novel approaches and international cooperation to effectively combat financial crime especially crypto crimes in the digital era.

Blockhain as Criminal Evidence under Indonesian Law

Evidence is anything that, according to the law, can be used to prove the truth or falsehood of something (an accusation).[28] Evidence also pertains to tools that are related to a crime, where such tools can be used as evidence to establish a judge's belief in the correctness of the criminal act committed by the accused. The importance of evidence is evident in the context of criminal courts, where evidence becomes a crucial element

[27] Shamil Shovkhalov and Hussein Idrisov, 'Economic and Legal Analysis of Cryptocurrency: Scientific Views from Russia and the Muslim World' (2021) 10 Laws 32 https://www.mdpi.com/2075-471X/10/2/32 accessed on 27 February 2023.

[28] Puspa, Yan Pramadya, *Kamus Hukum Edisi Lengkap: Bahasa Belanda, Indonesia, Inggris* (Aneka 1977) 27.

in determining the presence or absence of a criminal act allegedly committed by a defendant. Evidence can encompass various forms, ranging from written documents, witness testimonies, physical evidence, recording notes, to forensic experts.

The use of evidence in court is not merely mechanical but also follows principles regulated by criminal procedural law. The process of collecting, presenting, and evaluating evidence must comply with applicable legal provisions to ensure fairness and the validity of court judgments.

According to Law No. 1 of 1981 concerning criminal procedural law, Article 184 paragraph (1) stipulates that valid evidence includes testimony of witnesses, expert testimony, documents, indications, and defendant's testimony. In the criminal procedural law system adhering to the negative legal system, only evidence that is valid according to the law can be used for proof.[29] Furthermore, evidence expands beyond those mentioned in Article 184 paragraph (1). The expansion referred to here must be related to the types of evidence regulated in Article 5 paragraph (1) of the ITE Law (Law No. 19 of 2016).

In accordance with Article 5 paragraph (2), evidence expansion entails adding evidence tools already regulated in criminal procedural law in Indonesia, in accordance with criminal procedural law. Electronic information and/or electronic documents as electronic evidence add to the types of evidence regulated in the criminal code. Expansion can also be interpreted as broadening the scope of evidence already regulated in criminal procedural law.[30]

In the context of the development of information and electronic technology, the recognition of electronic information and documents as valid evidence presents challenges and the need to establish clear standards. Legal processes and justice systems must be able to accommodate this dynamism without sacrificing validity and fairness. Therefore, the Information and Electronic Transactions (ITE) Law in Indonesia provides guidelines and conditions to ensure that electronic information and documents can be considered valid evidence in the eyes of the law.

[29] Prodjohamidjojo, Martiman, *Sistem Pembuktian Dan Alat-Alat Bukti* (Ghalia Indonesia 1983) 34.
[30] Sitompul, Josua, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana* (Tata Nusa 2012) 35.

One formal requirement stipulated in Article 5 paragraph (4) of the ITE Law is that electronic information or documents cannot be considered as documents or letters that must be in written form according to regulations. This reflects the legislature's awareness of the electronic nature, which may not always follow traditional written formats. The acceptance of information and documents in electronic form is a significant step in recognizing digital reality and facilitating electronic transactions and interactions.

In addition to formal requirements, there are also material requirements that must be met for electronic information and documents to be considered valid evidence. These material aspects involve considerations of integrity, authentication, and authenticity of electronic information. Data security and protection against manipulation or forgery are the main focuses to ensure that electronically submitted information can be relied upon and holds high evidentiary value in court.

Meanwhile, material requirements are regulated in Article 6, Article 15, and Article 16 of the ITE Law, which essentially state that electronic information and documents must be guaranteed for their authenticity, integrity, and availability. The existence of electronic evidence materially has been recognized, but in terms of procedural law (formal), it is not yet fully accommodated. Based on the provisions of Article 5 paragraph 3 of the ITE Law, electronic information and/or electronic documents are deemed valid if they use an electronic system in accordance with the provisions of the ITE Law.

This is in line with Article 6 of the ITE Law, which determines that electronic documents are considered valid if the information contained therein can be accessed, displayed, guaranteed for integrity, and can be accounted for, thus explaining a situation. Additionally, the status of electronic documents can be equated with documents made on paper. With the enactment of the ITE Law, a legal basis for electronic transactions and information within the jurisdiction of Indonesia is established.[31]

Blockchain, as an innovation revolutionizing the world of technology, holds tremendous potential in addressing the increasing complexity of crypto crimes. The primary uniqueness and advantage of this technology lie in its decentralized nature

[31] Nafri, Moh., 'Dokumen Elektronik Sebagai Alat Bukti Dalam Hukum Acara Perdata Di Indonesia' (2019) 3 (1) Maleo Law Jurnal 126.

and the concept of immutability, which reshapes the paradigm of information and transaction management.

The significance of blockchain in combating crypto crimes lies in its ability to create indisputable digital evidence. With its decentralized nature, every transaction or piece of information recorded in the blockchain is not centralized under one authority but distributed across the network. This eliminates the risk of data manipulation or forgery, as altering a single block of information requires the majority approval of the involved network.

Immutability, a key characteristic of blockchain, refers to the inability to alter recorded historical data. Once a transaction or piece of information is entered into the blockchain, it becomes an integral part of the blockchain and cannot be changed without altering the entire history of preceding blocks. This creates a high level of security, as tampering or falsifying recorded data becomes an exceedingly difficult and impractical task.

The solid foundation of decentralization and immutability forms a transparent and reliable system. Every party involved in transactions or activities on the blockchain can easily verify transaction records directly, without the need to trust intermediaries. This not only enhances transparency but also reduces the risks of fraud and manipulation often associated with centralized systems.

The use of blockchain in combating crypto crimes can encompass tracking digital currencies, verifying identities, and ensuring the integrity of smart contracts. Thus, this technology not only provides solutions to crypto security challenges but also transforms the landscape of business and finance in a more efficient, secure, and transparent manner.[32]

However, when we bring the legal perspective into this context, the role of blockchain becomes even more prominent. Data generated by this technology can be considered as very strong electronic evidence and can be verified in a courtroom setting. The use of

[32] Arbina, Maria, and Putuhena, M. Ilham F., 'Tata Kelola Pembentukan Regulasi Terkait Perdagangan Mata Uang Kripto (Cryptocurrency) Sebagai Aset Kripto (Crypto Asset)' (2022) 1(1) Mahadi: Indonesia Journal of Law 33–57 https://doi.org/10.32734/mah.v1i1.8314.

blockchain by law enforcement agencies provides an advantage in strengthening their legal position when prosecuting crypto crime perpetrators. However, challenges related to privacy aspects and compliance with regulations need to be carefully addressed to avoid potential misuse of information and ethical conflicts.

The uncommon terms and mechanism within blockchain environment create a significant gap among legal practitioners, especially when such terms go to court. Not to mention the legal perspective regarding what-to-how these new item rendered as evidence before the court. On the other hand, existing legal theory concerning proof, such as law of evidence based on law positively (*postifief wettelijke bewijstheori*), law of evidence based on the judge's belief alone *(conviction intime, conviction raisonee*), and law of evidence based on law negatively (*negatief wettelijke bewijstheori*) play a crucial part.[33] Besides, pertaining to how the evidence is collected, arises the urge to confront how these new forms of evidence meet the standards provided by the law.

The importance of integrating blockchain into the legal framework becomes increasingly evident through its potential to create and support smart contracts. The concept of smart contracts has a significant impact on enhancing the efficiency of law enforcement against crypto crimes because they could automatically execute agreements or legal sanctions based on certain conditions being met.[34]

Smart contracts operate using programming code that can be automatically executed when predetermined conditions are fulfilled. This opens new opportunities in addressing the complexity and speed in responding to legal violations involving crypto aspects. For example, in the context of payments or digital asset transfers, smart contracts can ensure the automated execution of agreements without requiring the intervention of third parties.

However, alongside its positive potential, smart contracts also raise concerns regarding their legal validity. The implementation of smart contracts needs to consider legal clarity and certainty, ensuring that the contracts comply with applicable legal

[33] Eddy Hiariej, 'Teori Hukum dan Pembuktian' (Erlangga 2012) 17.

[34] Sukmariningsih, Retno Mawarini, Nurudin, Agus, and Nursanty, Eko, 'Pengenaan Hukum Pajak Pada Cryptocurrency Dan NFT Di Indonesia' (2022) 6(2) Owner 44-54 https://doi.org/10.33395/owner.v6i2.781.

provisions. This includes aspects such as the identification of involved parties, legal obligations, and accountability.

Questions regarding the legal validity of smart contracts become important to address in order to provide a strong legal basis for their use. Policymakers and relevant parties in the legal field need to collaborate to formulate relevant regulations that align with the development of blockchain technology. Further investigation into the legal and regulatory aspects of smart contracts is essential to address challenges and bridge the gap between technological innovation and existing legal frameworks.

In accordance to type of evidences, blockchain and smart contracts are candidate to a new concept of evidence within criminal procedure law. Pursuant to the latest legal discourses, such candidate may be deemed as to extend the scope of circumstantial evidence as well as being a new type of evidence alongside that provided by Article 184 Criminal Procedure Act.

By addressing legal uncertainties, the integration of blockchain and smart contracts can play a crucial role in enhancing the efficiency of law enforcement against crypto crimes while upholding the principles of justice and sustainability of the legal system.[35]

Considering the vast potential of blockchain as an electronic evidence tool in responding to crypto crimes, the importance of close cooperation among relevant parties becomes increasingly evident. Blockchain not only offers security and transparency but also transforms how we perceive and manage electronic evidence. To maximize its benefits, joint efforts from various stakeholders are needed to formulate a clear, fair, and responsive legal framework to address the complex challenges faced by the law in the current digital era.[36] First and foremost, cooperation among the government, legal institutions, and the technology industry is paramount. The government needs to play a role in designing and implementing regulations that support the use of

[35] Nitha, Dewa Ayu Fera, and Westra, I Ketut, 'Investasi Cryptocurrency Berdasarkan Peraturan Bappebti No. 5 Tahun 2019' (2020) 9(4) Jurnal Magister Hukum Udayana (Udayana Master Law Journal) 712 https://doi.org/10.24843/jmhu.2020.v09.i04.p04.

[36] Hamin, Dwi Indriyani, 'Crypto Currensi Dan Pandangan Legalitas Menurut Islam: Sebuah Literature Review' (2020) 3 (2) Jurnal Ilmu Manajemen dan Bisnis.

blockchain as a valid evidence tool. Meanwhile, legal institutions must actively engage in understanding this technology and drafting legal guidelines that can accommodate the dynamics of blockchain.[37]

Additionally, collaboration with the private sector, including technology companies and blockchain platforms, is crucial. This helps ensure that the regulations created not only align with legal requirements but also consider the latest developments and innovations in the world of blockchain technology. By involving all relevant parties, a legal framework can be designed to create an environment conducive to the use of blockchain as a reliable and trustworthy evidence tool.[38] Practically, blockchain is widely applied in the financial sector. It enhances transaction security and reduces costs associated with verification and validation processes. As stated in Constitutional Court Decision No 20/PUU-XIV/2016, the evidentiary power of electronic evidence can be used as indicative evidence because of its form and function. The need for a concrete regulation that stipulates the legality of blockchain in Indonesia is urgent, as it will ensure its acquisition meets evidentiary value in court.

Crafting a careful legal framework also requires a deep understanding of ethical and privacy aspects. Indeed, as Constitutional Court Decision No 20/PUU-XIV/2016, the Court deemed electronic evidence may be referred as circumstantial evidence solely due to its form and function. In pursuit of justice, a balance must be maintained between using blockchain for law enforcement purposes and protecting individuals' rights against data misuse.

With this holistic and collaborative approach, we can harness the full potential of blockchain as an effective ally in upholding justice in the ever-evolving realm of crypto crime. Only through strong synergy among the government, legal institutions, technology industry, and the public can we tackle these challenges in a coordinated and sustainable manner.

[37] Ibid.
[38] Ibid.

Conclusion

In addition to its pivotal role in combatting crypto crimes, the integration of blockchain technology within legal frameworks offers profound implications for evidentiary practices. Beyond its inherent benefits of decentralization and immutability, blockchain serves as a powerful instrument for establishing verifiable electronic evidence, thereby bolstering the integrity of legal proceedings. Nevertheless, the implementation of blockchain within legal systems necessitates a nuanced approach, as concerns regarding privacy protection and adherence to regulatory standards emerge as pertinent considerations that demand careful navigation.

Furthermore, the utilization of blockchain as an electronic evidence tool underscores the imperative for ongoing dialogue and collaboration among stakeholders within the legal, technological, and regulatory spheres. By fostering a multidisciplinary approach, tailored solutions can be devised to address the evolving landscape of crypto crimes and digital evidence, thereby fortifying the efficacy of legal systems in an increasingly digitized world. In essence, while blockchain offers unprecedented opportunities for enhancing transparency and security, its integration into legal contexts mandates a harmonized effort to reconcile its benefits with the imperative of safeguarding privacy and ensuring regulatory compliance. This also implies that an implementing regulations regarding blockchain technology shall be prioritized among another regulation in consideration of its unprecedented opportunities and challenges.

Acknowledgments

-

Disclosure Statement

No potential conflict of interest was reported by the author.

Funding

No funding was received for this research.

References

Akbar M, 'Blockchain: Pengertian, Manfaat, Dan Cara Kerjanya' (BINUS ONLINE, 2020) 20.

Allenotor D and Oyemade D.A., 'An Optimized Parallel Hybrid Architecture for Cryptocurrency Mining' (2021), available online: https://www.isteams.net/_files/ugd/185b0a_6f88b82981424f87850d11fea3f52e1b.pdf, accessed on 27 February 2023.

Alonso SLN, 'Activities and Operations with Cryptocurrencies and Their Taxation Implications: The Spanish Case' (2019) 8 Laws 16 https://www.mdpi.com/2075-471X/8/3/16 accessed on 27 February 2023.

Alshater MM, Joshipura M, Khoury RE, and Nohade Nasrallah, 'Initial Coin Offerings: A Hybrid Empirical Review' (2023) Small Business Economics, 1–18.

Alvarez FE, Argente D, and Patten DV, Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador (Cambridge: National Bureau of Economic Research, 2022).

Ante L, Fiedler I, Willruth JM, and Steinmetz F, 'A Systematic Literature Review of Empirical Research on Stablecoins' (2023) 2 FinTech 34–47, available online: https://www.mdpi.com/2674-1032/2/1/3 (accessed on 27 February 2023).

Arbina M and Putuhena MIF, 'Tata Kelola Pembentukan Regulasi Terkait Perdagangan Mata Uang Kripto (Cryptocurrency) Sebagai Aset Kripto (Crypto Asset)' (2022) 1(1) Mahadi: Indonesia Journal of Law 33–57 https://doi.org/10.32734/mah.v1i1.8314.

Arwono DG, Iskandar H, and Wardana DJ, 'Tinjauan Yuridis Regulasi Cryptocurrency Terhadap Tindak Pidana Kejahatan Di Indonesia' (2023) 5 (1) Amnesti Jurnal Hukum 110–125 https://jurnal.umpwr.ac.id/index.php/amnesti/article/view/2759.

Bailey AM and Warmke C, 'Bitcoin is King' in Cryptocurrency: Concepts, Technology, and Issues, ed. by J. Liebowitz (Taylor & Francis 2023), pp. 175–197.

Danuri, 'Perkembangan Informasi Dan Teknologi' (INFOKAM, Nomor II Th. XV/SEPTEMBER/2019).

Divakaruni A and Zimmerman P, 'The Lightning Network: Turning Bitcoin into Money' (2023) 52 Finance Research Letters 103480.

Hamin DI, 'Crypto Currensi Dan Pandangan Legalitas Menurut Islam: Sebuah Literature

Review' (2020) 3(2) Jurnal Ilmu Manajemen dan Bisnis.

Hendrik, 'Pengertian Blockchain: Sejarah, Asas Dan Cara Kerjanya' (Gramedia Blog, 2022) https://www.gramedia.com/literasi/pengertian-blockchain/, accessed on 1 March 2024.

Hiariej E, 'Teori Hukum dan Pembuktian' (Jakarta: Erlangga, 2012), pp. 17.

Kerr DS, Loveland KA, Smith KT, and Smith LM, 'Cryptocurrency Risks, Fraud Cases, and Financial Performance' (2023) 11 Risks 51.

Linton M, Teo EGS, Bommes E, Chen CY, and Härdle WK, Dynamic Topic Modelling for Cryptocurrency Community Forums (Berlin/Heidelberg: Springer, 2017).

Marzuki PM, *Penelitian Hukum* (Kencana Pranada Media Group 2007) 50.

Nafri M, 'Dokumen Elektronik Sebagai Alat Bukti Dalam Hukum Acara Perdata Di Indonesia' (2019) 3 (1) Maleo Law Jurnal 126.

Nickerson MA, 'Fraud in a world of advanced technologies: The possibilities are (unfortunately) endless' (2019) 89 The CPA Journal 28–34.

Nitha DAF, and Westra IK, 'Investasi Cryptocurrency Berdasarkan Peraturan Bappebti No. 5 Tahun 2019' (2020) 9(4) Jurnal Magister Hukum Udayana (Udayana Master Law Journal) 712 https://doi.org/10.24843/jmhu.2020.v09.i04.p04.

Phelps A and Watt A, 'I shop online–recreationally! Internet anonymity and Silk Road enabling drug use in Australia' (2014) 11 Digital Investigation 261–272.

Pinto F, Silva CF da, and Moro S, 'People-centered distributed ledger technology-IoT architectures: A systematic literature review' (2022) 70 Telematics and Informatics 101812.

Prodjohamidjojo M, *Sistem Pembuktian Dan Alat-Alat Bukti* (Ghalia Indonesia 1983) 34.

Puspa YP, *Kamus Hukum Edisi Lengkap: Bahasa Belanda, Indonesia, Inggris* (Aneka 1977) 27.

Shovkhalov S and Idrisov H, 'Economic and Legal Analysis of Cryptocurrency: Scientific Views from Russia and the Muslim World' (2021) 10 Laws 32 https://www.mdpi.com/2075-471X/10/2/32 accessed on 27 February 2023.

Sitompul J, *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana* (Tata Nusa 2012) 35.

Soerjono S, and Mamuji S, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Raja

Grafindo Persada 2013) 87.

Soltani R, Zaman M, Joshi R, and Sampalli S, 'Distributed Ledger Technologies and Their Applications: A Review' (2022) 12 Applied Sciences 7898.

Sukmariningsih RM, Nurudin A., and Nursanty E, 'Pengenaan Hukum Pajak Pada Cryptocurrency Dan NFT Di Indonesia' (2022) 6(2) Owner 44-54 https://doi.org/10.33395/owner.v6i2.781.

Tao Z, Peng B, and Ma L, 'Optimal initial coin offering under speculative token trading' (2023) 306 European Journal of Operational Research 632–644.

Taylor L, *The World's First Bitcoin Republic* (Elsevier, 2022).

Truby J, 'Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies' (2018) 44 Energy Research & Social Science 399–410.

Wendl M, Doan MH, and Sassen R, 'The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review' (2023) 326 Journal of Environmental Management 116530.

Wronka C, 'Financial crime in the decentralized finance ecosystem: New challenges for compliance' (2023) 30 Journal of Financial Crime 97–113.