E-ISSN: 2962-2816 I P-ISSN: 2747-1985

DINASTI RESEARCH

JOURNAL OF LAW, POLITIC AND HUMANITIES (JLPH)

https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455

DOI: https://doi.org/10.38035/jlph.

The Role of Blockchain in Addressing Unlicensed Mining: Opportunities and Challenges for Law Enforcement

Baginda Khalid[1], Esmi Warassih Pujirahayu[2], Tedi Asmara[3].

[1]Jenderal Soedirman University, Banyumas, Indonesia, baginda.khalid@unsoed.ac.id.

[2]Diponegoro University, Semarang, Indonesia, esmiwp@yahoo.com.

[3]Swadaya Gunung Jati University, Cirebon, Indonesia, te_asmara@yahoo.com.

Corresponding Author: baginda.khalid@unsoed.ac.id[1]

Abstract: Digital transformation through blockchain technology offers new potential for combating illegal mining in Indonesia, but it also presents challenges for the legal profession. According to 2023 data from the Ministry of Energy and Mineral Resources (ESDM), there are 2,741 unauthorized mining (PETI) locations, with 1,215 designated as People's Mining Areas (WPR). This study aims to explore how blockchain can be integrated into the legal system to enhance surveillance and law enforcement against illegal mining. Utilizing a qualitative-normative approach and content analysis, the research investigates blockchain's role in recording transactions and verifying the legality of mining activities. The findings reveal that blockchain improves transparency in mining oversight but requires regulatory adjustments and enhancements in law enforcement's technical capabilities. The study concludes that cross-sector collaboration among government, private industry, and academia is crucial to developing a legal framework that supports blockchain implementation, while providing targeted guidance to communities involved in illicit mining.

Keyword: Blockchain, Illegal Mining, Legal Supervision

INTRODUCTION

In the current digital era, the advancement of digital technology has opened up numerous new opportunities across various sectors, including in the efforts to combat illegal activities such as unauthorized mining. The application of technology in the fight against illegal mining has already been implemented in countries like Brazil. As reported by Alejandro Solis, digital technology has demonstrated its effectiveness in addressing similar issues in the Amazon, where more than 2,000 sites of illegal mining and deforestation activities were successfully detected through the use of satellite imagery and spatial analysis (Solis, 2019).

In Indonesia, the utilization of similar technologies could prove pivotal. Drones, which have successfully validated satellite data in the Amazon, could be employed to monitor remote and inaccessible areas. Meanwhile, applications such as Alerta SERFOR in Peru, which facilitate the reporting of illegal activities impacting flora and fauna in the Amazon rainforest, could be adapted to enhance community participation in monitoring unauthorized mining activities (Solis, 2019). These practices demonstrate how the integration of technology can strengthen efforts to prevent and address illegal mining activities (PETI) in Indonesia.

In addition to the use of drones and applications like Alerta SERFOR, blockchain technology offers a solution that enhances transparency in the recording of mining transactions. With its immutable nature, blockchain facilitates strict compliance with mining regulations, thereby strengthening industry governance. It provides law enforcement with an effective tool to identify, verify, and take legal action against illegal mining operations more efficiently from upstream to downstream. Blockchain can increase the speed and accuracy of tracking the origins of minerals, enabling quicker intervention and enforcement against violations, reducing opportunities for corruption, and bolstering public trust in the management of natural resources (Mochamad Ravy Mauludy Baza & Agil, 2023).

Illegal mining has long been a significant issue in Indonesia, causing environmental degradation and undermining the national economy. According to the latest mapping by the Ministry of Energy and Mineral Resources (ESDM) in 2023, 2,741 illegal mining sites (Pertambangan Tanpa Izin, PETI) have been identified across the country, marking an increase from the 2,700 locations recorded in 2021. Of these, 1,215 sites have now been designated as People's Mining Areas (Wilayah Pertambangan Rakyat, WPR). This situation underscores the urgent need for a more structured and effective approach to address the problem. Many PETI operators are members of communities with limited access to formal employment, highlighting the necessity for tailored approaches and capacity-building initiatives to regularize and manage unauthorized mining activities conducted by local populations (Humas Minerba, 2023).

The government has indeed implemented various regulations, such as Law No. 4 of 2009 on Mineral and Coal Mining and Government Regulation No. 96 of 2021 on the Implementation of Mineral and Coal Mining Business Activities, to regulate mining activities and penalize violations. However, in reality, illegal mining practices (PETI) continue unabated, with significant ecological and economic repercussions. These practices cause environmental degradation, loss of state revenue, and diminished investor confidence (Sunarto, 2023).

Although PETI lacks a specific legal definition, Interpol describes such activities as the illegal extraction and trade of earth minerals. This process often involves the use of hazardous chemicals like cyanide and mercury, which contribute to water and soil contamination around mining areas. In addition to pollution, these activities lead to deforestation, loss of biodiversity, soil erosion, the formation of sinkholes, and increased carbon emissions, all of which have detrimental effects on the atmosphere. This environmental damage exacerbates the existing ecological conditions and reduces the quality of life, highlighting the urgent need for more effective and coordinated interventions to address the ongoing challenges posed by illegal mining (Interpol, 2022).

Illegal mining (PETI) can be classified as a form of environmental crime, or green crime. According to criminologist Michael J. Lynch, identifying green crime is significantly more complex than conventional crimes, such as street crime. This complexity arises because activities like PETI often occur clandestinely and are organized, involving multifaceted environmental aspects. Understanding the concept of green crime requires a deep and integrated approach to identification and mitigation, reflecting the intricate nature and broad impact of such activities on the environment (Lynch, 2020).

In the fight against illegal mining (PETI), legal professionals such as judges, prosecutors, police officers, Mining Inspectors from the Ministry of Energy and Mineral

Resources (ESDM), and Civil Service Investigators (PPNS) play a crucial role. As the backbone of law enforcement, they are not only responsible for enforcing regulations but also for shaping an effective framework for the prevention and prosecution of violations within the mining sector. The suboptimal performance of oversight in certain regions of Indonesia underscores the urgent need to strengthen the role of legal professionals in the mining oversight system (Herman & others, 2022).

In efforts to enhance oversight and law enforcement within the mining sector, it is crucial to strengthen vertical coordination between central, provincial, and district governments. The key to effective mining governance lies in the synergy between various levels of government and improved communication with stakeholder groups, including the private sector and local communities. A common challenge is the asymmetry of information among the public, which can hinder monitoring and law enforcement efforts. The implementation of robust governance practices will reinforce the oversight system, increase the effectiveness of law enforcement, and significantly reduce the harmful practices of illegal mining (PETI) (Herman & others, 2022).

A previous study relevant to the current research theme was conducted by Gurpreet Tung. In his research, Tung revealed how technology not only plays a role in strengthening law enforcement and monitoring of illegal activities but also in facilitating transnational crimes, including money laundering. He highlights how the internet and digital technology enhance anonymity and expand the interconnectedness of global criminal networks. This phenomenon enables these networks to develop and expand their illegal operations more efficiently. The duality of technology illustrates that, while it can support law enforcement efforts, it can also be exploited by criminals to evade detection and enhance their activities (Tung, 2021). The challenges posed by increased connectivity are parallel to the difficulties in combating illegal mining, demonstrating how digitalization expands opportunities but also increases the complexity of law enforcement and monitoring efforts.

A subsequent study by Alexander Ivanov and colleagues provided valuable insights into how digitalization can impact law enforcement processes, offering both opportunities and challenges. In the context of illegal mining, digital technology presents significant potential to enhance the effectiveness of law enforcement by facilitating the detection and monitoring of illicit activities. However, it also encounters obstacles, including issues of privacy and data security, resistance from stakeholders accustomed to traditional systems, and the need for adequate resources to integrate advanced technology into law enforcement operations (Ivanov & others, 2020). This underscores the importance of more innovative and integrated strategies in addressing increasingly sophisticated organized crime in the digital age.

In this context, blockchain technology has emerged as a potential solution to support transparency and enhance the effectiveness of law enforcement in combating illegal mining in Indonesia. The integration of blockchain into mining oversight presents a range of challenges and opportunities. This study will explore how blockchain technology can be effectively integrated into Indonesia’s legal system to improve oversight and law enforcement against illegal mining activities, and what regulatory adjustments are necessary to support this integration. Additionally, it will examine the specific challenges faced by law enforcement in utilizing blockchain technology to strengthen transparency and accountability in mining oversight, and how their technical capacity can be enhanced.

This research proposes a legal framework to support the implementation of blockchain technology in the mining sector, with a particular focus on the necessary regulatory adjustments and the enhancement of law enforcement's technical capacity. The novelty of this study lies in its practical application of blockchain within the legal context of mining in

Indonesia a topic that has been relatively underexplored, especially in terms of regulatory development and the institutional capacity building required to support this technology.

METHOD

This study is normative research that employs content analysis to examine legislation, cases, and concepts. Content analysis is a systematic technique for evaluating codified forms of communication, including text, images, and other symbols, whether in digital or non-digital form (Krippendorff, 2004). This approach is particularly relevant for exploring how blockchain technology can be applied in addressing illegal mining, where data and transactions recorded on the blockchain can be analyzed to identify patterns of legitimate and illegitimate use.

The data utilized in this study consists of secondary sources, primarily legal materials such as statutes related to blockchain technology and mining oversight, as well as various scholarly works and books discussing the implementation of digital technologies in law, including news reports from official media outlets. The analysis is conducted qualitatively by elaborating on the concept of digital-based oversight of illegal mining, drawing on the perspectives of legal and technology experts

Richard Susskind's views on the future of the legal profession in the digital era will serve as a foundational framework for further analysis of the issue (Susskind & Susskind, 2015). This perspective will be integrated to understand how blockchain technology can be incorporated into the legal system to enhance the effectiveness of oversight and law enforcement against illegal mining activities. The study also adopts insights from other scholars, such as Manuel Castells' theory of the network society, to comprehend the dynamics of digitalization within the context of law and oversight (Castells, 2010).

RESULTS AND DISCUSSION

Integration of Blockchain Technology as a Mechanism for Combating Illegal Mining (PETI) within Indonesia's Legal Framework

The rapid advancement of technologies such as Artificial Intelligence, Drones, Virtual Reality, Robotics, and the Internet of Things, which have ushered us into the digital era of Industry 4.0, transforming various sectors, including legal processes. This transition presents new challenges for law enforcement, particularly in handling digital evidence such as photos, videos, and documents. Digital evidence is inherently fragile and easily altered, necessitating special handling to ensure its admissibility in court (Ramadhan, 2023).

This section must answer the problems or research hypotheses that have been formulated previously.

In anticipation of these challenges in managing digital evidence in Indonesia, the Information and Electronic Transactions Law (Law No. 11/2008) and its amendment (Law No. 19/2016) provide a crucial legal framework. These laws specifically outline the criteria that must be met for digital evidence to be recognized and adjudicated within the judicial system. For instance, Article 5 of the ITE Law clarifies that electronic information and digital documents including emails, digital images, and recordings constitute valid evidence if they meet the formal and substantive requirements stipulated by law. This ensures that digital evidence can be integrated into the existing legal framework, such as the Indonesian Criminal Procedure Code (KUHAP), where printouts of electronic documents are treated as equivalent to traditional paper documents.

Furthermore, Article 31, paragraph 3 of Law No. 19/2016 stipulates that the collection of digital evidence must be conducted by authorized legal authorities and only through lawful procedures. This ensures the integrity of the legal process and the accountability of the evidence obtained. The strength of this regulation is reinforced by the material requirements outlined in Articles 15 and 16 of the Electronic Information and Transactions Law (UU ITE), where the authenticity, integrity, and availability of information must be guaranteed, often necessitating digital forensic techniques for verification. Thus, as the era of Industry 4.0 demands adaptation toward the digitalization of legal processes, the UU ITE and its amendments play a crucial role as the legal foundation facilitating this transition. The requirements imposed not only ensure the legitimacy of evidence in court but also protect individual rights throughout the digital judicial process.

In today's modern world, the principles underlying blockchain technology are not only pivotal in the financial sector but are also finding significant applications in legal regulation, particularly in managing digital evidence in Indonesia. Originally designed as a mechanism to facilitate cryptocurrency transactions, blockchain technology now extends far beyond the creation of digital currency. The historical roots of blockchain can be traced back to what is believed to be an ancient form of distributed ledger during the Roman Empire, known as "Praescriptione." This ancient ledger system managed transactions across the vast expanse of the Roman Empire. The fundamental idea of blockchain is to streamline and secure transactions through a decentralized recording method. This capability to efficiently document transactions has paved the way for the further development of what we now recognize as distributed ledger technology (Sugiharto & Musa, 2020).

Distributed ledger technology (DLT) and blockchain, while closely related, serve distinct functions and applications within the digital economy. DLT encompasses various decentralized databases distributed across multiple nodes, where changes can be made independently on all nodes without requiring a specific sequence of data. Blockchain, as a subcategory of DLT, organizes data into sequentially linked blocks, ensuring security and tamper-proof evidence through consensus mechanisms like proof-of-work (PoW). Unlike general DLT systems that may not require native currencies, blockchain often necessitates tokens or cryptocurrencies to facilitate transactions and reward network participants. While blockchain is commonly associated with financial applications, particularly cryptocurrencies, DLT offers a wide range of potential uses in sectors such as supply chain management and healthcare, demonstrating its versatility and capability to ensure data integrity and security across various fields (Sugiharto & Musa, 2020).

An essential element of both DLT and blockchain is cryptography. Cryptography plays a crucial role in these technologies by providing a strong security foundation through the encryption and decryption of data. This process ensures that transactions within DLT and blockchain networks are protected from unauthorized access. Encryption adds a layer of confidentiality, converting accessible information into a code readable only by those with the correct key. Asymmetric systems, in particular, enhance security by separating encryption and decryption keys, minimizing the risk of key compromise. Cryptography not only secures data but also verifies its authenticity and integrity, ensuring that every element within a blockchain or DLT record is authentic and unaltered, while also providing an effective solution for non-repudiation (Judhieputra & Anisa, 2024).

Cryptography is employed to encrypt data within a block by converting it into a hash, a random code composed of numbers and letters, allowing blocks to be linked within the network. If someone attempts to alter the data, other blocks will detect and validate the change through consensus, ensuring that the valid data is the majority consensus. This mechanism underpins the security of blockchain technology against data manipulation attempts by hackers, as any modification in one block will be detected by the surrounding blocks (Ramadhan, 2023).

While closely associated with cryptocurrency technology, the application of blockchain extends far beyond digital financial transactions. Services like Google, Facebook, and Twitter, which are dominated by centralized control, present blockchain with an opportunity to serve as an alternative that reduces the risks of central control and manipulation for users. This can be achieved through data decentralization, offering a more transparent and secure method of managing information. This is crucial for enhancing user privacy and mitigating the increasingly prevalent risks on the internet (Cekerevac & Cekerevac, 2022).

Moreover, blockchain enables secure and transparent transactions between individuals without the need for centralized verification, making it ideal for applications such as the Internet of Things (IoT) and cloud-based services. The application of blockchain can extend to various sectors, such as supply chain management, where it enhances transparency and efficiency within the supply chain. This allows for the tracking of a product's journey from production to delivery, a particularly valuable strategy in industries like food, where ensuring product authenticity and safety is paramount (Pardede, 2023).

The Indonesian government has also begun to express interest in the application of this technology. Since early 2022, seven ministries have explored collaborations with the Indonesian Blockchain Association (ABI) for blockchain implementation, including the National Public Procurement Agency (LKPP), which has started using it to enhance the traceability of procurement products through the e-Catalog. Blockchain technology records every transaction or piece of information within business processes in a decentralized manner, as opposed to conventional centralized record-keeping. This decentralization allows interconnection between computer networks (nodes) within a single blockchain framework, resulting in more evenly distributed and secure data storage. Asih has noted that the decentralized nature of blockchain can be leveraged to streamline public services, such as simplifying the tax reporting process, which involves multiple institutions. The implementation of this technology by state-owned banks has also facilitated their business processes, highlighting blockchain's significant potential to improve efficiency and transparency across various sectors in Indonesia (Pardede, 2023).

In Indonesia, the regulatory framework for blockchain technology is still in its early stages. Currently, there are only two major regulations related to the use of blockchain: Bank Indonesia Regulation No. 19/12/PBI 2017 on the Implementation of Financial Technology and the Financial Services Authority Regulation No. 37/POJK.04/2018 on Equity Crowdfunding via Information Technology-Based Offerings. These regulations do not explicitly govern blockchain but acknowledge its use in specific contexts, such as payment systems and crowdfunding services. This indicates a recognition of blockchain's potential, but there is no comprehensive policy fully supporting the widespread implementation of this technology (Lase & others, 2021).

Given the limitations of the existing regulations, it is crucial for Indonesia to develop a more integrated and comprehensive legal framework for blockchain. One approach could be the establishment of a 'regulatory sandbox,' which would allow for the testing of various blockchain applications in a controlled environment. This would enable the National Cyber and Encryption Agency (BSSN) and other relevant institutions to assess the effectiveness of this technology before it is implemented more broadly. Additionally, efforts should be made to create regulations that set standards for security and reliability, ensuring that blockchain innovations operate in an ethical and fair manner, with due consideration for legal certainty and protection for all users (Lase & others, 2021).

The application of blockchain technology has been implemented to address the issue of illegal mining, particularly in the context of managing conflicts related to diamond mining, or "blood diamonds," in the Democratic Republic of Congo and Zimbabwe. This technology was employed by the International Business Machines Corporation (IBM) in collaboration with Everledger and De Beers, two leading diamond companies, through the Tracr platform. This platform ensures that every diamond on the market is marked and tracked from the point of extraction to the marketplace. Transactions and the movement of diamonds are recorded in an immutable ledger, allowing for verification of their origin and the ethics of their sourcing. The application of this technology supports a clean mining industry by adhering to the Kimberley Process Certification Scheme, which aims to eliminate the trade in conflict diamonds, while also enhancing security and efficiency within the supply chain. With blockchain, the diamond industry ensures that diamonds in the global market have been mined and distributed ethically, without harming communities. In Zimbabwe, the estimated revenue loss from illegal diamonds reached up to USD 15 billion due to corruption and conflict during the Marange diamond rush losses that could have otherwise increased the country's revenue (Onifade & others, 2024).

Although blockchain regulations in Indonesia remain relatively limited, mining oversight is primarily governed by the Minister of Energy and Mineral Resources Regulation No. 26 of 2018 on the Implementation of Good Mining Practices and Supervision of Mineral and Coal Mining. Article 1(16) defines the role of a Mining Inspector as a civil servant responsible for ensuring good mining practices and adherence to technical standards in processing and refining. However, this oversight does not extend to illegal mining (PETI), as outlined in Article 45(6), which focuses on evaluating reports submitted by permit holders, such as IUPs and IUPKs. Criminal sanctions for PETI are detailed in Law No. 3 of 2020, amending Law No. 4 of 2009. Article 158 prescribes up to five years' imprisonment and a fine of IDR 100 billion for unauthorized mining. Articles 160(2) and 161 impose similar penalties for unauthorized production operations and the illegal handling of minerals and coal without the necessary permits.

While the significant potential of blockchain in addressing legal challenges and enhancing regulatory enforcement has been outlined, various implementation challenges must still be overcome to fully realize the benefits of this technology. These obstacles include issues related to development and implementation, performance, efficiency, sustainability, scalability, adoption, as well as legal and standardization concerns (Nur & others, 2020). Understanding and addressing these challenges is crucial to ensuring that blockchain technology can be effectively integrated into Indonesia's legal and administrative systems, providing a robust and efficient solution for combating illegal mining (PETI) and other legal issues. The following is a list of the challenges associated with the implementation of blockchain technology:

1. Development and Implementation

Blockchain technology is still in its early stages of development, facing significant challenges in implementation, particularly within the complex global supply chain systems that must comply with various cross-border legal regulations. This necessitates accurate standardization and mapping within blockchain to align with existing supply chain standards. Additionally, blockchain must be prepared for future applications such as the Internet of Things (IoT), Artificial Intelligence (AI), and big data analytics, which complicates the development process due to blockchain's inherently low adaptability and extensibility. The difficulty in integrating third-party logistics providers into a blockchain platform exemplifies the complexity within a broader ecosystem (Nur & others, 2020).

Implementing smart contracts and separating blockchain into two parts one for data storage and another for contract execution could offer solutions; however, these still require substantial computational resources, especially for blockchains using proof-of-work validation methods. Identifying the appropriate validation method is critical for addressing performance, scalability, security, and privacy challenges (W.-M. Lee, 2019).

2. Performance and Efficiency

Blockchain systems require significant resources, demanding substantial computational power and bandwidth. This high resource demand results in lower performance compared to centralized systems, which can process transactions more quickly and efficiently. For example, the Bitcoin blockchain can process only about 3-7 transactions per second, far lower than payment systems like Visa, which can handle over 24,000 transactions per second. Ethereum, even with upgrades, can only manage around 15-30 transactions per second. Additionally, mining for Bitcoin and Ethereum requires specialized hardware that consumes significant energy, with total electricity consumption comparable to that of small countries (Hill, 2017). The inherent design of blockchain, which prioritizes security and decentralization, often sacrifices speed and throughput, illustrating the trade-offs between security and efficiency within this technology (Nur & others, 2020).

3. Sustainability and Scalability

Blockchain faces significant challenges in sustainability and scalability due to its append-only nature, which causes the data to continuously grow and potentially become too large to manage, as each node must store a complete copy. By December 2016, the Bitcoin blockchain already required 100GB, negatively impacting performance. This issue is contingent upon the data stored, transaction frequency, and number of participants. Solutions such as Bitcoin-NG, which separates the ledger into microblocks and key blocks, have been proposed to address this challenge. However, changes to the blockchain system can render older versions invalid, a phenomenon known as a hard fork. The difficulty of adapting blockchain for third parties, such as logistics providers, and the use of smart contracts further adds to the complexity (Bashir & Prusty, 2019). Despite advancements, blockchain technology remains insufficiently mature, particularly for supply chain applications, necessitating further research and large-scale testing to address these challenges.

4. Adoption

The adoption of blockchain technology is often hindered by its complexity and the substantial changes required for its implementation. Much of blockchain technology is still in the experimental stage and has not been widely tested, necessitating new IT infrastructure and often requiring updates or replacements for outdated systems. Additional challenges include convincing various stakeholders to share data through blockchain and the lack of understanding among supply chain participants regarding the benefits and operation of blockchain (Tyagi & others, 2020). Developing blockchain systems requires significant investment and can fundamentally alter existing organizational processes, making change management difficult. Furthermore, blockchain tends to be slower than centralized systems, so organizations must weigh the benefits against the slower speed.

5. Legal and Standardization Issues

Legal and standardization challenges remain major obstacles to the adoption of blockchain technology, given its large-scale operations in a regulatory landscape that is still ambiguous. Regulatory uncertainty and the lack of specific standards invite legal unpredictability and compliance issues, as observed in policies from countries like South Korea, which have attempted to regulate or ban blockchain-supported cryptocurrencies. The absence of specific rules governing blockchain hinders its broader adoption, particularly in supply chains, and the lack of standards leads to low interoperability between different blockchain systems. Hacker and Lianos argue that the debate over whether blockchain should conform to existing regulations or create a new legal ecosystem reflects the struggle to balance innovation with regulatory needs (Hacker & others, 2019). This perspective is further expanded by Dimitropoulos and Eich, who emphasize the importance of understanding blockchain not only as a technological tool but also as a social and political phenomenon that requires a dynamic and responsive legal approach to accommodate both private and public uses of blockchain (Hacker & others, 2019).

As the digital era rapidly advances, with technologies like blockchain continually reshaping the foundations of social and economic interactions, Manuel Castells' Theory of the Network Society becomes increasingly relevant for analyzing the transformations occurring within legal systems and regulatory oversight. Castells describes the network society as one where the primary social structures and activities are built around digitally connected electronic networks. The existence and operation of these networks facilitate the global flow of various forms of capital and information, altering our understanding of rights, obligations, and the distribution of power in society. In Castells' Network Society Theory, control and authority become more diffuse and less centralized, no longer solely held by traditional institutions such as governments or large corporations, but increasingly distributed among various digital platform owners, social media, and other technologies that facilitate electronic communication and transactions, including the users of these platforms (Castells, 2010).

In connection with Castells' Network Society Theory, the use of blockchain can have significant implications in supporting the social structures and economic activities built on digital networks. This shift is particularly influenced by the increasingly dispersed control among various media and digital platform owners, as well as among users, who collectively create Decentralized People Operations (DePo). Blockchain, with its decentralized characteristics, underpins this idea by enabling a more egalitarian distribution of power and transparency in transactions. Blockchain facilitates the creation of an ecosystem where data and transactions are not controlled by a single central entity but by a network comprising multiple stakeholders (Sharif & Ghodoosi, 2022).

As it relates to the context of oversight and law, blockchain technology first introduced as the foundational technology for Bitcoin by Satoshi Nakamoto in 2008, offers an innovative method for monitoring and auditing transactions and economic activities in real-time. The advent of smart contracts, popularized by the Ethereum platform created by Vitalik Buterin, enables the execution of agreements with immutable transaction records, thereby enhancing fairness and accountability. Smart contracts within blockchain facilitate more effective agreement execution without the need for bureaucratic and complex intermediaries, reducing the potential for corruption and inefficiency (Khan & others, 2021). Consequently, the use of blockchain supports the transition from traditional hierarchical structures to broader distributed networks, reflecting Manuel Castells concept of the network society, where power distribution is more equitable and transparent.

The Indonesian government has begun adjusting its regulatory and legal approaches to accommodate the various changes brought about by the emergence of the network society. This includes developing laws and policies that more effectively address issues related to the digital economy, data privacy, and cybersecurity. The implementation of Law No. 27 of 2022 on Personal Data Protection, issued by the government, aims to regulate the management of personal data by digital platforms and provides a clearer legal framework for protecting individual rights.

The formation of the Personal Data Protection Law (UU PDP) in Indonesia was driven by the urgent need for a comprehensive legal framework to regulate the use and protection of citizens' personal data. A key constitutional foundation that catalyzed the creation of this law is Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states: "Every person has the right to the protection of themselves, their family, honor, dignity, and property under their control, as well as the right to security and protection from fear of threats to do or not do something that is a human right." This constitutional provision explicitly establishes the right to privacy and the protection of personal data as fundamental human rights that the state must safeguard. The enactment of UU PDP is a response to global dynamics and the increasing demands for economic integration and cybersecurity, necessitating robust data protection standards to support secure digital transactions and information exchange.

Enhancing Future Law Enforcement Competencies in the Oversight and Mitigation of Illegal Mining through Blockchain Technology

In their work "The Future of the Professions," Richard Susskind and Daniel Susskind predict fundamental changes in various professions in the coming years, driven by rapid technological advancements. Richard and Daniel outline two potential future scenarios for the role of professionals, including legal practitioners. In the first scenario, technology enhances and facilitates existing professional practices without fundamentally altering them; technology acts as a complement to professionals in performing their traditional roles. The second scenario is more transformative, suggesting that technological advancements and systems may not only assist but even replace many tasks performed by legal professionals. In this scenario, technology could operate autonomously or be managed by operators, posing an existential challenge to the traditional roles within the legal profession (Susskind & Susskind, 2015).

By 2024, cybersecurity in Indonesia remains in need of improved management. In the first quarter alone, there was a significant increase in digital security incidents compared to the previous year, rising by 43%, nearly doubling to 61 cases. In January 2024, there were 13 incidents, followed by 20 cases in February, and 27 cases in March. Political motives, particularly related to the 2024 elections and criticism of the government, are suspected to be key drivers behind the surge in cyberattacks this year (CNN, 2024).

The recent wave of cyberattacks has targeted various components, from public figures to government-managed websites. Notably, in June 2024, a ransomware attack on the National Data Center resulted in significant data breaches with the potential to escalate into a national disaster. This situation underscores the need for stricter oversight and a swift response. The attack involved a ransom demand of IDR 131 billion, and the hackers ultimately returned the national data out of pity for the Ministry of Communication and Information Technology of the Republic of Indonesia. This incident highlights the ongoing vulnerabilities in the nation's cybersecurity infrastructure. The days-long data recovery process further indicates an urgent need to enhance both infrastructure and human resource capacity to manage and protect the country's sensitive data from similar future threats (Nababan, 2024).

In the context of oversight and mitigation of illegal mining, the use of blockchain technology will undoubtedly present unique challenges for law enforcement in Indonesia. A primary obstacle in adopting this technology relates to the lack of technical understanding and expertise among law enforcement officers, given the rapid pace of technological advancement. The large-scale cyberattacks serve as a stark reminder of the necessity for improving proficiency in utilizing more advanced technologies. Similar challenges are faced by law enforcement agencies in other countries, where the need for effective training for frontline officers, such as the police, is crucial to bridging the skills gap in handling cybersecurity incidents (Curtis & Oxburgh, 2022).

The challenge of using blockchain technology for oversight and mitigation of illegal mining represents a critical area that demands legal human resource preparedness. The integration of technology requires a deep understanding of emerging technologies and adaptive policies. Systematic efforts are needed to train law enforcement in digital technology and cybersecurity to enhance their effectiveness in addressing the complex and multifaceted issues posed by illegal mining. This includes developing responsive curricula in legal education and ongoing training that emphasizes the practical application of blockchain technology in law enforcement (Azharuddin & others, 2020).

Integrating blockchain into the mitigation of illegal mining (PETI) will undoubtedly present significant challenges, particularly concerning the technical capabilities of law enforcement in Indonesia. The rapid development of blockchain technology demands expertise that extends beyond legal aspects to include a deep understanding of technical mechanisms and cybersecurity. This difficulty is exacerbated by the potential risks posed by the inherent decentralization of blockchain technology, which complicates the process of monitoring and tracking illegal transactions without an adequate regulatory framework. There is an urgent need for comprehensive and ongoing training for law enforcement officers, covering not only the fundamentals of blockchain but also strategies to combat cybercrime that may arise from the implementation of this technology (J. Lee, 2022).

Integrating blockchain into the mitigation of illegal mining (PETI) will undoubtedly present significant challenges, particularly concerning the technical capabilities of law enforcement in Indonesia. The rapid development of blockchain technology demands expertise that extends beyond legal aspects to include a deep understanding of technical mechanisms and cybersecurity. This difficulty is exacerbated by the potential risks posed by the inherent decentralization of blockchain technology, which complicates the process of monitoring and tracking illegal transactions without an adequate regulatory framework. There is an urgent need for comprehensive and ongoing training for law enforcement officers, covering not only the fundamentals of blockchain but also strategies to combat cybercrime that may arise from the implementation of this technology (J. Lee, 2022).

One strategy that could be employed is the application of the Socratic Method and Critical Legal Thinking in the curriculum development for prospective law enforcement officers. These methods focus on critical thinking and deep dialectical analysis, providing an effective foundation for legal training and professional development programs. Through structured dialogue and the formulation of questions, this approach enables law enforcement officers to grasp complex legal concepts and to articulate and defend their positions in real and often intricate legal situations. This ensures they are equipped with the necessary tools, including sound logic and well-reasoned legal arguments, to address the challenges posed by technological advancements (Gane & Huang, 2017).

In addressing the challenges of continuous legal education, it is crucial to consider the impact and integration of technology into the curriculum. The incorporation of critical thinking and the ability to adapt to technological changes and social norms are essential components of legal education. Asikin Zainal highlights the importance of updating teaching methods and materials to better reflect the realities of legal practice and the challenges of modern society (Asikin, 2020). This approach aims to train future law enforcement officers not only in theoretical aspects but also in effective and ethical practical applications. According to Zainal, revising the legal curriculum should reflect the need for a broader understanding of international law and technology, particularly in the ever-evolving digital era. This not only enhances the relevance of legal education materials to current conditions but also prepares law students to adapt to and address complex transnational legal issues. This initiative aligns with the objectives of Permenristekdikti No. 44 of 2015 (now replaced by Minister of Education and Culture Regulation No. 3 of 2020 on National Standards of Higher Education), which underscores the necessity for curriculum updates that meet both national and international higher education standards (Asikin, 2020).

The future legal curriculum must encompass comprehensive training on the use of technology within the legal context, including aspects of cybersecurity, data privacy, and the development of regulations concerning technology. Training programs should target not only theoretical knowledge but also practical skills in applying technology to legal practice. It is equally important to integrate real-world case studies and simulations, enabling law students to experience firsthand how technology can be utilized in law enforcement and dispute resolution (Smith, 2022).

In line with this approach, legal education institutions should collaborate with technology experts to ensure that educational materials are continuously updated with the latest developments in both technology and law. Curriculum development should ultimately focus on the impact of technology on legal regulations and its implications for society. This way, legal education not only prepares students to become competent legal professionals but also innovators and critical thinkers capable of navigating and influencing societal changes driven by new technologies (Smith, 2022).

The integration of technology into legal education, as discussed by Richard Susskind and Daniel Susskind, presents an opportunity for the legal profession to adapt and anticipate forthcoming transformations. Their theory on the role of technology in enhancing and modernizing legal practice underscores the importance of preparing legal professionals for the accelerating pace of technological change. Developing a curriculum that integrates technological proficiency is a strategic key to equipping law students to effectively utilize digital tools for legal analysis and problem-solving (Brownsword, 2022). This initiative emphasizes the need for holistic and adaptive education, focusing not only on theory but also on practical and innovative applications in legal practice, thereby preparing future legal professionals for a dynamic and challenging digital era.

This preparation is also crucial to avoid the second scenario proposed by Susskind, where legal professionals could be entirely replaced by technologies such as Artificial Intelligence and automated systems. A comprehensive, technology-oriented legal education is essential to ensure that legal professionals do not become passive users of technology but informed and critical decision-makers. By developing expertise in technology, legal professionals will be able to leverage tools like blockchain, A.I., and other automated systems as supportive tools, rather than replacements, thereby maintaining the essential human role in legal judgment, ethics, and empathy, which cannot be fully replicated by machines (George, 2003).

CONCLUSION

Blockchain technology offers significant strategic potential for enhancing oversight and law enforcement against illegal mining activities (PETI) in Indonesia. However, effective integration of this technology requires regulatory adjustments that support transparency, data security, and the legal validity of digital transactions. This necessitates the expansion of existing legal frameworks, such as the Electronic Information and Transactions Law (UU ITE) and mining regulations, to include specific operational standards for blockchain. The development of a 'regulatory sandbox' is also needed to allow for the controlled testing of blockchain applications, ensuring that the technology can be tailored to local needs before broader implementation. Strengthening collaboration between regulatory bodies, the tech industry, and law enforcement agencies will ensure that this technology is not only innovative but also aligned with prevailing legal policies.

On the other hand, the use of blockchain by law enforcement to enhance transparency and accountability in mining oversight faces specific challenges. These challenges include a lack of technical expertise, currently inadequate infrastructure, and the need for cultural change in the adoption of new technology. To address these issues, law enforcement agencies require comprehensive training to master both the technical and legal aspects of blockchain, improvements in information technology infrastructure, and organizational cultural shifts towards more transparent and automated practices.

The conclusion of this research is that integrating blockchain into Indonesia's legal system can increase efficiency, reduce bureaucratic complexity, and strengthen justice, helping Indonesia move towards a responsible and transparent digital era. However, to bolster the technical capacity of law enforcement, the recommendations include investing in cutting-edge technology, providing continuous training, and fostering collaboration with academic institutions and the tech industry. This will prepare law enforcement not only to meet current challenges but also to adapt to future technological developments.

REFERENCE

Asikin, Z. (2020). Menggugat Pendidikan Hukum di Indonesia. In W. D. Putro & others (Eds.), *Menemukan Kebenaran Hukum dalam Era Post-Truth*.

Azharuddin, A., & others. (2020). Kesiapan Sumber Daya Manusia Dalam Bidang Hukum Terhadap Revolusi Industri 4.0. *Hermeneutika: Jurnal Hermeneutika*, *6*(2). https://doi.org/10.30870/hermeneutika.v6i2.9063

Bashir, I., & Prusty, N. (2019). *Advanced Blockchain Development: Build Highly Secure, Decentralized Applications and Conduct Secure Transactions*. Packt Publishing.

Brownsword, R. (2022). *Rethinking Law, Regulation, and Technology*. Edward Elgar Publishing Limited.

Castells, M. (2010). *The Rise of the Network Society, 2nd ed., vol. 1 of The Information Age: Economy, Society, and Culture*. Wiley-Blackwell.

Cekerevac, Z., & Cekerevac, P. (2022). Blockchain and the Application of Blockchain Technology. *MEST Journal*, *10*(2). https://doi.org/10.12709/mest.10.10.02.02

CNN. (2024). *SAFEnet: Serangan Siber Naik Dua Kali Lipat di Awal 2024*. https://www.cnnindonesia.com/teknologi/20240509092409-192-1095674/safenet-serangan-siber-naik-dua-kali-lipat-di-awal-2024

Curtis, J., & Oxburgh, G. E. (2022). Understanding cybercrime in `real world' policing and law enforcement. *The Police Journal*, *96 (diakse*. https://doi.org/10.1177/0032258X221107584

Gane, C., & Huang, R. H. (2017). *Legal Education in the Global Context: Opportunities and Challenges*. Taylor & Francis.

George, R. T. De. (2003). *The Ethics of Information Technology and Business*. Blackwell Publishing Ltd.

Hacker, P., & others. (2019). *Regulating Blockchain: Techno-Social and Legal Challenges*. Oxford University Press.

Herman, A., & others. (2022). Penegakan Hukum Terhadap Tindak Pidana Penambangan Mineral di Kawasan Hutan Tanpa Izin. *Halu Oleo Legal Research*, *4*(2), 270–272. https://doi.org/10.33772/holresch.v4i2.47

Hill, B. (2017). *Ethereum And Bitcoin Energy Consumption Surpasses Entire Countries' Power Budgets*. https://hothardware.com/news/ethereum-and-bitcoin-energy-consumption-surpass-entire-countries-power-budgets

HumasMinerba. (2023). *Serius Tangani Tambang Ilegal, Ditjen Minerba ESDM Akan Bentuk Satgas!* Kementerian Energi Dan Sumber Daya Mineral. https://minerba.esdm.go.id/berita/minerba/detail/20231208-serius-tangani-tambang-ilegal-ditjen-minerba-esdm-akan-bentuk-satgas

Interpol. (2022). *ILLEGAL MINING AND ASSOCIATED CRIMES : A Law Enforcement Perspective On One Of the Most Lucrative Crimes* (Issue April).

Ivanov, A., & others. (2020). Law Enforcement in the Context of Digitalization: Problems and Prospects for Improving Efficiency. In (Makalah dipresentasikan pada 1st International Scientific Conference (Ed.), *Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development*. LARDER 2020).

Judhieputra, R. R., & Anisa, I. N. (2024). *Kriptografi: Penerapan dalam Keamanan Transaksi Komersial*. Indonesia Emas Group.

Khan, S. N., & others. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications (Diakses, 22 i 2024*. https://doi.org/10.1007/s12083-021-01127-0

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Sage Publications.

Lase, N., & others. (2021). Kerangka Hukum Teknologi Blockchain Berdasarkan Hukum Siber di Indonesia. *Pajajaran Law Review*, *9*(1), 2357–2685.

Lee, J. (2022). *Crypto-Finance, Law and Regulation: Governing an Emerging Ecosystem*. Taylor & Francis.

Lee, W.-M. (2019). *Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript*. Apress.

Lynch, M. J. (2020). Green Criminology and Environmental Crime: Criminology That Matters in the Age of Global Ecological Collapse. *Journal of White Collar and Corporate Crime*, *1*(1), 50–61. https://doi.org/10.1177/2631309x19876930

Mochamad Ravy Mauludy Baza, & Agil, M. (2023). Peran Penting Teknologi Digital Blockchain dalam Upaya Mengurangi Kasus Korupsi Penggelapan Surat Berharga. *Jurnal Hukum Dan Sosial Politik*, *1*(3). https://doi.org/10.59581/jhsp-widyakarya.v1i1

Nababan, W. M. C. (2024). *Bencana' Nasional Serangan ke Pusat Data Nasional Bisa Buka 'Perang' Siber dan Ancaman Negara*. Kompas.

Nur, M. R., & others. (2020). CHALLENGES IN USING BLOCKCHAIN FOR SUPPLY CHAIN MANAGEMENT INFORMATION SYSTEMS. *J@ti Undip: Jurnal Teknik Industri*, *15*(2). https://doi.org/10.14710/jati.15.2.82-92

Onifade, M., & others. (2024). Recent Advances in Blockchain Technology: Prospects, Applications and Constraints in the Minerals Industry. *International Journal of Mining, Reclamation and Environment*, *10*(1080). https://doi.org/10.1080/17480930.2024.2319453

Pardede, R. K. B. (2023). *Adopsi Teknologi Rantai Blok di Indonesia Terus Tumbuh*. Kompas. https://kompas.id/baca/ekonomi/2023/03/25/adopsi-teknologi-blockchain-di-indonesia-perlu-didorong

Ramadhan, K. (2023). *Chain of Custody berbasis Blockchain dalam Penanganan Bukti Digital*. Hukumonline.Com. https://www.hukumonline.com/berita/a/chain-of-custody-berbasis-blockchain-dalam-penanganan-bukti-digital-lt64ce49bc3bf67/

Sharif, M. M., & Ghodoosi, F. (2022). The Ethics of Blockchain in Organizations. *Journal of Business Ethics : (Diakses*, *22* i *2024*. https://doi.org/10.1007/s10551-022-05058-5

Smith, M. (2022). Technology Law in Legal Education: Recognising the Importance of the Field. *Legal Education Review*, *32*(1), 19–32. https://doi.org/10.35300/001c.35492

Solis, A. (2019, January). *How Digital Tools Help Combat Illegal Mining and Logging in the Amazon*. DAI Digital @ DAI. https://dai-global.digital.com/digital-tools-against-illegal-mining-and-logging-in-the-amazon.html

Sugiharto, A., & Musa, M. Y. (2020). Blockchain & Cryptocurrency. In *Perspektif Hukum di Indonesia dan Dunia (: Perkumpulan Kajian Hukum Terdesentralisasi INDONESIAN LEGAL STUDY FOR CRYPTO ASSET AND BLOCKCHAIN.*

Sunarto, K. (2023). *Dilema Pertambangan Tanpa Izin Sebagai Pertambangan Rakyat*. Hukumonline.Com. https://www.hukumonline.com/berita/a/dilema-pertambangan-tanpa-izin-sebagai-pertambangan-rakyat-lt652657a0b50f1/page=1

Susskind, R., & Susskind, D. (2015). *The Future of the Professions: How Technology Will Transform the Work of Human Experts*. Oxford University Press.

Tung, G. (2021). Technology as a Tool for Transnational Organized Crime: Networking and Money Laundering. *The Journal of Intelligence, Conflict, and Warfare*, *4*(1). https://doi.org/10.21810/jicw.v4i1.2820

Tyagi, A. K., & others. (2020). *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*. IGI Global.