

Legal Aspects and Issues of Blockchain Implementation as The Technology Base of Smart Contract

Qur'ani Dewi Kusumawardani

Faculty of Law, Gadjah Mada University, Yogyakarta, Indonesia

quranidewi@gmail.com

M. Hawin

Faculty of Law, Gadjah Mada University, Yogyakarta, Indonesia

winha62@gmail.com

Article Info

Received: 2024-11-11

Revised: 2024-12-16

Accepted: 2024-12-16

Keywords:

Legal aspects,
Blockchain, Technology;

Abstract

Blockchain, as a supporting technology for the industrial revolution 4.0, has excellent potential to change many areas of private legal transactions, including as the technological basis of smart contracts. The application of blockchain technology has its own legal aspects, risks, legal issues and challenges to provide regulatory policies to optimize the technology's potential and simultaneously mitigate risks. This research aims, firstly, to discover the legal aspects that should be considered in blockchain technology and, secondly, the legal issues of implementing blockchain technology, especially those related to finance, jurisdiction, and cyber-attacks. The research method to be used is normative legal research. The research results obtained are, first, the aspect of the existence of the law itself, which is related to binary code through hash algorithms. Second, the legal issues of implementing blockchain in the financial sector are scalability, data privacy, data interoperability, and governance; related to jurisdiction related to the ability of blockchain to cross jurisdictional boundaries because nodes on the blockchain can transmit anywhere, in this world; related to cyber-attacks, namely brute force attacks on specific nodes which result in the dissemination of inaccurate information. Legal assistance and existence in technology (in this case, blockchain) are needed so that everything continues according to the rules to prevent more significant problems from arising.

I. Introduction

Darwin's theory of evolution suggests that a process of change takes a long time, up to thousands of years (Darwin, 2004), but this is different from today, namely during the fourth industrial revolution, where change now only takes a short time. In the fourth industrial revolution, there was a shift in the human paradigm in viewing nature (Prasetyo, 2018), thanks to new technologies such as 3D printing, artificial intelligence, financial technology, internet-of-things, cloud computing-based storage, big data, and robotics technology, communication technology between machines, uncrewed vehicles, nanotechnology, quantum supercomputers, biotechnology, automatic cars, genetic engineering, blockchain technology, and cryptocurrencies (Florentin, 2022). The presence of these technologies is increasingly helping humans carry out their duties to achieve all forms of significant optimization (Dirjen Aptika Kominfo, 2018).

A blockchain is managed in a block list containing sequential transactions, where the hash connects each block so that it can store and transmit data in a decentralized manner (Parung, 2019). The information stored on the blockchain is a shared database, not only in one location. Records stored on the blockchain are public and easy to verify because millions of computers host them. Simply put, a blockchain is like a database that stores distributed records of values and transactions (Raharjo, 2022). Initially, blockchain was only used for encrypted digital currency transactions (such as Bitcoin) and to avoid double-spending. Still, it was developed further in various fields because of its enormous benefits, such as digital identity, voting or decentralized notaries. This technology is also flexible because it can be related to existing technologies such as network topology, cryptography, and consensus algorithms (Zhang, 2016).

Based on the technical configuration, functional and governance structure, blockchain is divided into four categories, namely first, public permissionless blockchain (blockchain without public permission), namely when all parties can send, validate transactions, can read and access the system (unless the blockchain is encrypted so that only read the contents). Second, public permissioned blockchain (blockchain with public permission) when only authorized entities can have access to the blockchain, third, private permissioned blockchain (blockchain with private permission requests) when only authorized private persons in a specific area can execute or validate transactions, and fourth, private permissionless blockchain (blockchain that does not require personal permission) when anyone can send and validate transactions on a private blockchain as long as the transaction is carried out in a special area. Apart from that, a hybrid blockchain can also be made, which

combines the various aspects above (European Commission, 2018).

Blockchain technology has great potential to change many areas of private law transactions. Blockchain also offers interesting opportunities as the technological basis for smart contracts. Smart contracts are also included in one of the hottest areas in blockchain technology research. Especially with the advantages of using smart contracts, such as reducing costs and time for transactions, offering transparency, and offering predictability, the trail is public, and contracts can be executed automatically (H. Jacquemin & Y. Pouillet, 2018). The application of a new technology certainly poses its challenges, and this causes the government to need to provide regulatory policies in order to optimize the potential of technology and simultaneously mitigate risks because one important thing is not only the presence of new technology but how to respond to new technological innovations that appear with regulations. Current law.

Fundamental questions will arise to accommodate this new technology, such as what legal aspects need to be considered with the presence of blockchain technology, whether the existing legal system can easily interact with blockchain technology as a technological basis for self-executing agreements, or what legal issues will arise and related to the adequacy of rules to create legal certainty. The hope is that decentralized technologies such as blockchain will become the next wave comparable to the transformation of internet development. Therefore, as new technology faces various challenges, researchers want to know about the legal aspects of blockchain and legal issues that can arise from blockchain technology in the financial, cyber risk and jurisdictional fields.

2. Research Method

This research uses the type of normative juridical research (Soekanto, Soerjono dan Sri Mamudji, 1994). Methods of data collection were collected through library research (Nazir, 2005). The library material used is secondary data supported by primary, secondary and tertiary legal materials. Primary legal materials consist of basic norms or rules, basic provisions or regulations, and statutory regulations. Secondary legal materials, namely books, research journal articles, previous research reports, and mass media related to blockchain and smart contracts, as well as tertiary legal materials, including the Black Law Dictionary, Big Indonesian Dictionary, etc (Hadikusuma, 1995).

3. Results and Discussion

Legal Aspects that should be Considered from the Presence of Blockchain Technology as the Technological Basis of Smart Contract

Blockchain technology has now entered various fields. In Indonesia, one field that has used blockchain technology is games, for example, Play Game. Here, the blockchain system is utilized to validate all gamer activities so that there is no loophole for a gamer to commit fraud. In addition, the United States has also implemented the world's first blockchain-based capital market called Crypto Securities Exchange (CSX). The exchange has been registered with the United States Securities and Exchange Commission (SEC). This system can streamline communication lines between issuers, securities consultants, brokers and custodian institutions. The convenience shown by blockchain technology has caused this technology even to be called a solution to all problems in the world (Alois, J.D,2022).

Understanding the fundamental dimensions of blockchain technology infrastructure can help identify new roles and legal aspects to interact with blockchain technology. When studying new technology, some aspects need to be considered as preventive and risk mitigation efforts. One aspect that must be considered is related to views from a legal perspective or legal aspects and legal issues that may arise. The legal aspects and issues are necessary to consider because blockchain is still in its infancy, and there is a lack of experience with the technology, so potential blockchain risks will be difficult to predict comprehensively. In addition, the probability and impact of risks will also depend on the specific use case and the nature of the blockchain solution itself.

The legal aspects that must be considered related to blockchain technology are related to the presence of this technology where the blockchain is present through a block arrangement, namely a series of binary codes through a hash algorithm. Then a question arises from legal experts, can codes like this be categorized as law, or can law consist of a series of codes? Consideration of legal aspects related to laws and codes is necessary because this can lead to new legal issues. According to Satoshi Nakamoto, blockchain technology can lead society to a self-enforcing society. In addition, blockchain technology can replace traditional laws even though there are so many expert opinions stating that, most likely, the relationship between the two will not reach substitution but will complement each other (Finck, 2018).

Some experts consider blockchain technology to be able to create a new legal system (Andy, 2018). It is based on *lex informatica*, supported by the development of *lex cryptography* on the blockchain. Lawrence Lessig also explained how codes in

blockchain technology can operate as law. According to him, this can happen because, through the means of a code, regulation of individual behavior can emerge. In addition, armed with technological means arranged by codes, Lex Cryptographic can systematically enforce individual behavior in an artificial environment. Code designers can also be called rule setters in a technological environment (Wright, et.al, 2015).

According to Lawrence Lessig, there are four main ways of regulating and limiting individual behavior: law, social norms, market forces and architecture. In blockchain technology, the regulation of individual behavior is carried out through blockchain architectural governance. The procedure for regulation is carried out utilizing code as a virtual world architecture made by humans so that that code can operate as law, or it can be said that code is law, or law is enforced within the scope of codes (Wu, 2003).

Since the emergence of blockchain technology, the law has progressively made assumptions regarding the characteristics of the code, whereby blockchain technology establishes regulation through the codes. The immutable nature of the ledger and its nature of automating transactions makes lex cryptography a very efficient regulatory code. At the same time, lex cryptography can also be subject to legal regulations from the real world, so blockchain technology demonstrates that code is the law and the implementation of new laws through code. Added by de Filippi and Wright, blockchain technology can also accelerate power transfer from rules of law pre-arranged by government authorities to rules and protocols based on decentralized code (Yeung, 2018).

Legal aspects related to the existence of codes that can be categorized as legal or not deserve to be considered because, according to the European Insurance and Occupational Pensions Authority (EIOPA), blockchain technology is a technology that deserves further exploration because blockchain can be used in various applications in various industries, including digital identity, social networking, voting, cloud storage, centralized applications and more. In addition, blockchain can also help automate reporting, make digital transactions more efficient by reducing compliance-related costs, increase transaction transparency, reduce business risk, improve data consistency and quality across companies, and allow regulators to gain data in new fields through access. Real-time (Kavassalis, P, et.al, 2018).

Second, the broad scope of the law, which covers many aspects, especially related to the meaning of multi-aspect (multidimensional and multifaceted) law, is certainly an aspect that is also considered by blockchain technology because, in principle, the law must remain side by side in any field. Assistance and the existence of law in technology are intended to keep everything running according to the rules to prevent bigger problems

from arising. In addition, fulfilling compliance with the rules is also very necessary, considering that the development of blockchain-based applications will be increasingly massive in the future.

Third, the legal aspect that should be considered by blockchain technology is that in Indonesia, there is no regulation in the form of a law that specifically regulates the application of blockchain technology. However, industry players adopting blockchain technology must comply with Law 11 of 2008 in conjunction with Law 19 of 2016 concerning Information and Electronic Transactions (UU ITE). This compliance is due to implementation of a blockchain-based transaction system involving activities in electronic systems. In addition, the birth of the ITE Law has implications for two things: First, electronic transactions and documents are legitimate to guarantee legal certainty. Second, the classification of unlawful acts and violations to provide legal protection, where blockchain technology can also be interpreted as having these implications because blockchain acts as a distributed ledger through a computer network (Setia, 2014).

In Indonesia, a standard operational policy for implementing blockchain has been regulated, as contained in the Regulation of the Financial Services Authority of the Republic of Indonesia Number 37/POJK.04/2018 concerning Crowdfunding Services through Information Technology-Based Share Offerings (Equity Crowdfunding). In Article 47, OJK Regulation 37/POJK.04/2018, the definition of blockchain is defined as an information technology-based financial transaction bookkeeping service that records and stores transaction evidence data or ledgers distributed through computer networks, both private and public. However, this regulation only regulates the limited use of blockchain in technology-based stock offering activities to improve the quality of Crowdfunding Services. This rule also does not serve as the main statutory regulation, and the definition does not have binding legal force because it is only listed in the elucidation section of OJK regulations. Its location, which is only in the explanation section, creates difficulties in forming, implementing, and harmonizing statutory regulations (Satria Muhammad Nur Lase, et.al, 2021).

Fourth, the legal aspects must be considered when blockchain technology is still in the development stage; namely, the use of blockchain technology must meet eligibility standards with the principles of being safe, reliable and trustworthy. Blockchain technology must also obtain release permit standards and clear operational rules. After blockchain technology is deemed qualified, predictable through more mature analysis and capable of bridging innovations related to this technology, blockchain can then be regulated with stronger regulations, namely through laws or government regulations (Zhao, 2019).

Fifth, blockchain technology is the technological basis for the presence of smart contracts. A *smart contract* is a computer program code that converts the contents of a contract into a series of binary codes via a hash algorithm. When the conditions set by the program are met, the system will trigger automatic execution (Kshetri, 2018). The legal aspects of blockchain technology as the basis of smart contracts are related to statements by various bodies of literature indicating that the challenge of correctly coding smart contracts can often be more difficult than programming traditional software. The automated nature of execution and the computer-coded form of smart contracts means that even small mistakes can have significant consequences (Delmolino, 2015). So that it has legal consequences, namely when some parties argue that it will be difficult to regulate or organize matters related to force majeure in smart contracts because, seen from the nature of smart contracts, which will immediately execute automatically when the achievements agreed upon in the contract have been fulfilled or not fulfilled (Philippe, 2022).

Sixth, the legal aspect that must be considered in blockchain technology as the basis of a smart contract is what if there is a coding error in the smart contract? Or Who will be responsible when the smart contract code is damaged? This question must be questioned because there has been hacking recently due to software system defects or smart contract programming bugs (Coie, 2017). Seventh, the legal aspect that should be considered is when the parties want to use the services of a lawyer to review or compile a smart contract; the lawyer must understand what he has read or written. Even though smart contracts are not written in a language that most lawyers can understand (in the form of codes), of course, this is a challenge for lawyers to protect their clients (Hasting, 2020).

Legal Issues from the Implementation of Blockchain Technology as a Smart Contract Technology Forming

Blockchain and distributed ledgers are also the strongest challenges to state monopoly over the creation and storage of public records and verification processes through institutions (Markey-Towler, 2018). This challenge arises because later trust in blockchain has the potential to replace trust in the government seen from the system, which does not require centralized authorization (Werbach, 2018). Blockchain is a relatively new technology, so there are several legal issues when this technology is implemented, such as regarding the performance and scalability of this technology, huge energy consumption, data privacy law issues, legal and regulatory issues when this technology infrastructure integrates with old infrastructure, issues laws relating to the regulation of token and coin classification (Reyes, 2016), legal issues of blockchain technology related to the validity of smart contracts (because this technology is the

basis of the presence of smart contracts) as well as interoperability between different platforms, which will be narrowed down in three areas, namely finance, jurisdiction and cyberattacks. The following are legal issues regarding the implementation of blockchain technology in the financial sector, jurisdictions and when there is a cybercrime attack:

1) The legal Issue of Implementing Blockchain Technology is related to the Financial Sector.

Research from the Harvard Business Review in 2017 stated that blockchain has the potential to create a new foundation in economic and social systems, so financial and banking service companies around the world are trying to develop blockchain-based systems to replace existing databases. Seeing the great potential of this blockchain technology, it is likely to develop more rapidly, especially in Indonesia (Darmawan, 2018). The use of blockchain technology in the financial sector in Indonesia is related to digital currency as the subject of commodity futures contracts. Blockchain is regulated in Bapepebti Regulation Number 5 of 2019 concerning Technical Provisions for Organizing a Physical Crypto Asset Market on the Futures Exchange (Ketentuan Teknis Penyelenggaraan Pasar Fisik Aset Kripto di Bursa Berjangka). The Technical Provisions for Organizing a Physical Crypto Asset Market on the Futures Exchange Regulation is an elaboration of the Regulation of the Minister of Trade of the Republic of Indonesia number 99 of 2018 concerning the General Policy for Organizing Crypto Asset Trading. Crypto assets traded through commodity futures exchanges in Indonesia must comply with various provisions in Article 3 of Technical Provisions for Organizing a Physical Crypto Asset Market on the Futures Exchange Regulation number 5 of 2019, which, among other things, requires crypto assets to be based on blockchain technology.

Blockchain regulations in Indonesia need to be underlined because Bank Indonesia (BI) and the Financial Services Authority (OJK) have never banned blockchain technology in the financial services industry. BI only prohibits the use of digital currency as a legal means of payment in the territory of the unitary state of the Republic of Indonesia as stipulated in Article 21 of Law 7/2011 concerning currency. BI's legal basis for prohibiting virtual currency is also regulated in PBI Number 18/40/PBI/2016 concerning the Implementation of Payment Transaction Processing and PBI Number 19/12/PBI/2017 concerning the Implementation of Financial Technology. Therefore, banning digital currency does not mean banning blockchain technology because blockchain is not the same as cryptocurrency.

Blockchain technology for recording transactions has been legalized through Bank Indonesia Regulation Number 19/12/PBI/2017 of 2017 concerning implementing Financial Technology. Specifically, the elucidation of Article 3 paragraph (1) letter of the

PBI concerning the Implementation of Financial Technology states that blockchain as a form of implementing financial technology in the payment system functions to carry out authorization, clearing, final settlement and payment settlement.

Based on the specifications of the level of security, blockchain can properly store information related to the activities of various online financial transactions. The sharing security system owned by the blockchain can keep existing financial data safe, so financial institutions such as the Financial Services Authority and Bank Indonesia can use it as a recorder and a repository for financial transaction activities carried out online. Financial institutions and the wider community will feel the existence of blockchain in the financial sector (Nugroho, dkk, 2021). For example, in the United States, blockchain is used by a company that produces computer software called International Business Machine Corporation (IBM), which operates in the industrial and business sectors. In addition, this company also creates an exchange rate trading platform called hyper ledger fabric. This project is supported by seven world banks, including Unicredit, KBC and HSBC. However, there are concerns from the Financial Stability Oversight Counsel (FSOC) that some blockchain-based systems could be more vulnerable to fraud than systems currently understood. However, this concern is still based on small-scale testing (International Business Machines Corporation, 2022)

Legal issues in finance regarding implementing blockchain technology are related to blockchain-based systems that can span many different regulatory jurisdictions and national boundaries. Of course, large financial institutions should be careful when moving to a system where the regulations still need to be clarified/uncertain. The financial and business risks will be too high if the government does not have clear regulations on how blockchain-based assets are treated. Concerns regarding regulation, mutual integration costs and lack of large-scale application of blockchain-based systems may be the reasons for the slow uptake of the technology by financial institutions and governments (Davidson, 2016).

Crypto-token issuance is the world's most popular application of blockchain technology, issued in initial coin offerings (ICO) for financing. The excitement around ICOs slowly died down in 2018 due to increased regulatory scrutiny and falling token valuations. Despite this, blockchain-based asset tokenization in financial markets continues to grow, as blockchain applications are the most prominent in financial markets. Although the use of tokenization is currently limited, the potential of the instrument grows significantly as blockchain has benefits in terms of cost efficiency, increased transparency, liquidity, and more inclusive participation of retail investors (Raustiala, Kal & Christopher Jon Sprigman, 2018). Legal issues that may arise from implementing blockchain-based financial asset tokenization on a large scale are scalability, data

privacy, data interoperability, operational risk from technology, and governance issues. The potential expansion in tokenized assets has broad implications that affect financial markets, such as trading, liquidity, prices, and clearing. However, the regulatory and legal ambiguity surrounding asset tokenization can create uncertainty and risk for users of tokenized assets (Sinclair Davidson et al, 2016)

2) Legal Issues regarding Jurisdictional Implementation of Blockchain Technology

Blockchain technology can cross jurisdictional boundaries because nodes on the blockchain can transmit anywhere in the world (Salmon, 2017). Implementing blockchain can raise several legal issues related to complex jurisdictions and require careful consideration, such as contractual relationships. The different principles of contract in different jurisdictions require identification concerning the governing law in each country. Furthermore, blockchain regulations must be international and widely accepted because blockchain contracts are cross-jurisdictional and international, with the participation of parties from different countries (Kaal, Wulf A & Craig Calcaterra, 2018).

Parties conducting electronic transactions through blockchain technology must use an agreed electronic system. However, in electronic transactions, what is meant by the word 'agreed upon' also includes agreed-upon procedures contained in the electronic system. To reach an agreement in an electronic system, paying attention to several things that must be included in an electronic contract is necessary. The Electronic Contract must at least contain the following: (a) identity data of the parties; (b) objects and specifications; (c) electronic transaction requirements; (d) prices and costs; (e) procedures in the event of cancellation by the parties; (f) provisions that provide rights to the aggrieved party to be able to return the goods and request a product replacement if there are hidden defects; and (g) choice of law for electronic transaction settlement.

However, in a decentralized environment such as blockchain technology, it can take more work to identify the application of the right set of rules. The difficulty in identifying which rules apply occurs because every transaction is potentially under the jurisdiction of a location on every node in the network. This has the legal effect that blockchain technology must comply with many legal and regulatory regimes. If a transaction leads to fraud, determining the location (*locus delicti*) in the blockchain can become a separate legal issue. Therefore, it is necessary to include legal and jurisdictional clauses that regulate exclusively and determine the rights and obligations of the parties and which court will handle disputes within the scope of blockchain technology when a dispute occurs between the parties to create legal certainty. Apart from that, the legal issue is how the courts can find a method to define and determine the exact place of transactions made in the blockchain network (Fulmer N, 2019).

The provisions that apply in the ITE Law have jurisdiction not only for legal actions that apply in the Republic of Indonesia and are carried out by citizens of the Republic of Indonesia but also apply to legal actions that are carried out outside the jurisdiction (jurisdiction) of Indonesia either by Indonesian citizens or foreign citizens or Indonesian legal entities or foreign legal entities that have legal consequences in Indonesia. This is important considering the use of information technology for electronic information, and blockchain-based transactions can be cross-territorial or universal.

Article 18, paragraph (3) of the ITE Law is felt to accommodate transactions carried out in a decentralized environment, where parties can conduct transactions from anywhere and anywhere. Article 18, paragraph 3 of the ITE Law states, "If the parties do not make a choice of law in international electronic transactions, then the applicable law is based on the principle of International Private Law." Several theories accommodate which law applies in a contract, namely: first, the theory of *Lex Loci Contractus* is based on the law where the agreement or contract is made and signed by the parties. Second, *Lex Loci Solutionis* Theory, the law that applies to a contract is the place where the contract is implemented. Third, Theory of the Proper Law of the Contract, which is based on the legal system desired by the parties, or if the will is not expressly stated or cannot be known from the surrounding circumstances, then the proper law of the contract is the closest legal system and deal with the transactions that occur. Fourth, The Most Characteristic Connection Theory, namely the obligation to carry out an achievement that is most characteristic, is a benchmark for determining the law that will govern the agreement (Khairandy, et.al, 1999).

Settlement of online transaction disputes can be done through court forums or Arbitration. Alternatively, the parties may determine alternative dispute resolution institutions through consultation, mediation, negotiation, conciliation, or expert judgment. If the parties do not choose a forum for dispute resolution, then the dispute resolution is based on the principle of Private International Law. The principle of international private law used will be based on the principle of the defendant's residence (the basis of presence) and effectiveness which emphasizes where the defendant's property is located (the principle of effectiveness). However, issues related to jurisdiction gave rise to differences of opinion between the two camps. The first camp considers that cyberspace is sufficiently regulated by laws and concepts that have existed and been used in the real world (cyber paternalist). The second camp believes cyberspace is unique, so separate laws and concepts are needed. This view tries to separate cyberspace from the real world (cyber-libertarian) (Murray, 2007).

David R. Johnson then tries to offer four models that are worth considering as a solution, including a) Execution of control by existing judicial bodies; b) Entering into international agreements on cyberspace regulation; c) Establishing an international organization that specifically regulates cyberspace; d) Self-regulation by internet users (self-governance). The Council of Europe also regulates jurisdictional issues in Article 22 of the Convention on Cybercrime. This article adheres to the territorial principle, which means that every country party to this convention has the right to try the crimes listed in its territory (Johnson, David R. and David G. Post, 1996).

3) Blockchain Legal Issues related to Cyber-Crime

Rapid developments in blockchain technology can invite cyber risks and cybercrimes. These crimes are categorized as a development of computer crime. For example, legal issues related to cryptocurrencies based on blockchain technology, such as bitcoin, can be used as a virtual transaction tool for transactions in cyberspace. Cyberspace is a strategic place cybercriminal use to commit crimes such as money laundering and illegal drug and weapon transactions. Bitcoin can be a tool, means, and media for cybercriminals to carry out illegal activities. Additionally, there have been several security breaches related to blockchain applications, including Bitcoin, but these breaches were due to human error, not systemic deficiencies of the blockchain. For example, Ethereum-based decentralized autonomous organizations are called DAOs (Distributed Autonomous Organizations). The DAO system had been operating according to the smart contract computer code. However, the code contained a bug that allowed one of The DAO participants to transfer 3.6 million ether (ETH), worth \$50,000,000 (fifty million dollars). DAO programmer Christoph Jentzsch is considered an Ethereum veteran, pointing out that even seasoned programmers with a deep understanding of Ethereum can make mistakes when programming smart contracts (Siegel, 2016).

In some cases, attacks on The DAO (Distributed Autonomous Organization) occur because humans poorly code smart contracts. In the case of Mt. Gox and Bitfinex, Bitcoin users entrust cryptographically based private security keys to third-party providers where those third parties fail to secure them. In addition, regardless of the high level of security on the blockchain system, there are cybersecurity risks that will still arise; for example, on a public blockchain, data input comes from several nodes, so there is a possibility of the risk of interference from each node. This type of attack is not aimed at the blockchain but can only target external blockchain systems such as cryptocurrency wallets (Siegel, 2016).

The next legal issue regarding cyberattacks is when someone targets data input points that lead to the spread of inaccurate information. Blockchain users will unknowingly rely on this misleading information, or through compromising blockchain data with brute force attacks on certain nodes due to some blockchain networks, a concentrated number of nodes will do almost all the processing. However, such an attack would require enormous computing power. In some systems, even the attack only needs to control more than half the computing power of all nodes. This kind of attack is more likely to succeed when the attacker specifically attacks the nodes with the highest computing power where most transactions are concentrated (Goodin,2018).

In Indonesia, Law No. 11 of 2008 concerning Information and Electronic Transactions. Regulates everything regarding electronic data and its utilization for the public interest, including regulations related to risks or cyber-attacks. This law is explained in detail regarding all actions classified as cybercrimes, as regulated in Articles 27 to 37 of the ITE Law. Therefore, in reviewing the rules and ways of solving problems around cyber risks or cyber-attacks (in blockchain technology) in Indonesia, you can refer to the ITE Law.

4. Conclusion

Blockchain technology is predicted by experts to replace traditional law and lead society to a self-enforcing society. This happened because blockchain technology created a new legal system based on the idea of *lex informatica*, supported by the development of *lex cryptographia*. The immutable nature of a decentralized ledger and its ability to automate transactions make *lex cryptographia* a very efficient regulatory code. The most important thing to note is that blockchain is a regulatory technology because it can guide individual behavior and regulate and create rules for individuals operating in the network through cyber architectural procedures.

Blockchain technology has many advantages; besides being effective in keeping track of information and transactions, blockchain also offers security, transparency, efficiency, improved traceability and cost savings. However, when adopting blockchain technology, the legal aspects and issues accompanying it must be considered. Legal issues regarding blockchain technology can arise because this technology is relatively new and is still under development. General concerns that arise and can become legal issues, such as uncertainty caused by the lack of clarity in regulations that specifically regulate this technology in detail in the financial sector, technological complexity, jurisdictional issues, enormous energy consumption, legal issues of integration with old infrastructure, performance and scalability issues, legal issues related to the classification of tokens and coins, issues of interoperability and standardization

between different blockchains, legal issues related to jurisdictions. In addition, blockchain's decentralized nature can create risks different from traditional centralized technologies (OECD, 2019).

Therefore, in the future, when the government wants to make arrangements related to blockchain technology, it can do it through two legal and political approaches. First, the formulation of blockchain regulations is based on a cyber law approach that focuses on regulating the hardware and software infrastructure layers. Second, blockchain regulations are formulated based on a governance approach and regulatory implementation that focuses on regulating content layer infrastructure through computational law theory (Daniel W. Linna Jr, 2019) and lex cryptographic (Jones, 2020). In addition to the two approaches mentioned above, it needs to be supported by the regulatory sandbox concept to be applied to blockchain technology. This is crucial because first, from a philosophical point of view, the sandbox can be interpreted as safety sand; second, contextually, it is interpreted as a form of guidance based on testing, namely the test-and-learn approach, trials and mentoring. In this concept, regulators and innovators will jointly develop a framework to test new ideas, including their safety nets. Establishing a memorandum of understanding between regulators and innovators in the regulatory sandbox is to minimize blockchain service failures and establish standard operating guidelines and work success standards (EIOPA, 2019).

References

Books

- Darwin, Charles, (2004), *On the Origin of Species*, New Jersey, Castle book.
- Direktorat Jenderal Aplikasi Informatika, (2018), *Big data, Kecerdasan buatan, Blockchain dan Teknologi Finansial di Indonesia, Usulan Desain, Prinsip dan Rekomendasi Kebijakan*, Kementerian Komunikasi dan Informatika, Jakarta.
- Hadikusuma, H, (1995), *Metode Pembuatan Kertas Kerja atau Skripsi Ilmu Hukum*, Bandung, Mandar Maju.
- Johnson, David R. and David G. Post, (1996), *And How Should the Internet Be Governed? The American Lawyer*.
- Kaal, Wulf A & Craig Calcaterra, (2018), *Crypto Transaction Dispute Resolution*, 73 Business Law 1, pp. 37-38.
- Khairandy, Ridwan, Nandang Sutrisno, dan Jawahir Thontowi, (1999), *Pengantar Hukum Perdata Internasional Indonesia*, Yogyakarta, Gama Media, 114.
- Kshetri N and Voas J, *Blockchain-Enabled E-Voting*, (2018), IEEE Software 35, 95-99.
- Murray, Andrew D, (2007), *The Regulation in Cyberspace: Control in the Online Environment*, Routelage and Cavendish.
- Nazir, M, (2005), *Metode Penelitian*. Jakarta, Ghalia Indonesia.
- Prasetyo, Banu, (2018), *Alam dan Manusia*, Waskita, pp.37-46.
- Raharjo, Budi, (2022), *Uang Masa Depan*, Semarang, Yayasan Prima Agus Teknik, pp.1.
- Soekanto, Soerjono dan Sri Mamudji, (1994), *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*, Jakarta, Raja Grafindo Persada, pp.13.

Journal Article

- Disantara, F. P., Prasetio, D. E., Disantara, G. I. P., & Nutakor, B. S. M. (2024). The Problematics of the Legal Standing of Deoxyribonucleic Acid (DNA) Test Results Concerning Civil Relationships of Illegitimate Children: A Legal Pluralism Perspective. *Jurnal Ilmiah Mizani: Wacana Hukum, Ekonomi Dan Keagamaan*, 11(2), 435-448. <https://doi.org/http://dx.doi.org/10.29300/mzn.v11i2.5156>
- Finck, Michèle, (2018), Blockchains: Regulating the Unknown, 19 *German Law Journal*, pp. 85.
- Fulmer N, (2019), Exploring the Legal Issues of Blockchain Applications. *Akron Law Review*, vol. 52, pp. 185-186.
- Hasting, Ryan, (2020), Smart Contracts: Implications on Liability and Competence, 28 *University Miami Business Law Review* 358, <https://repository.law.miami.edu/umbl/vol28/iss2/6>.
- Jayantara, M., Kurniawan, I. G. A., & Samsithawrati, P. A. (2023). THE UNJUST ENRICHMENT; IN INTELLECTUAL PROPERTY RIGHTS: A PROPHETIC LEGAL PARADIGM. *Jurnal Pembaharuan Hukum*, 10(2), 215. <https://doi.org/10.26532/jph.v10i2.30673>
- Kavassalis, P, Stieber, H., Breymann, W., Saxton, K. and Gross, F, (2018), An innovative Regulatory Technology Approach to Financial Risk Monitoring and Supervisory Reporting, *Journal of Risk Finance*, Vol. 19 No. 1, pp. 39-55.
- Kurniawan, I. G. A. (2022a). Putusan Mahkamah Konstitusi Terhadap Undang-Undang Cipta Kerja Dalam Perspektif Filsafat Utilitarianisme. *JURNAL USM LAW REVIEW*, 5(1), 282-298. <https://doi.org/http://dx.doi.org/10.26623/julr.v5i1.4941>

- Kurniawan, I. G. A., Lulo, L. de D. M., & Disantara, F. P. (2023). IUS Constituendum of Expert Advisor in Commodity Futures Trading: A Legal Certainty. *Jurnal IUS Kajian Hukum Dan Keadilan*, 11(1), 31–45. <https://doi.org/https://doi.org/10.29303/ius.v11i1.1170>
- Nugroho, Inaz Indra, Reza Pratiwi, Salsabila Rahma Az Zahro, Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia, *IPMHI Law Journal*, Vol. 1 No. 2, (Edisi Juli-Desember 2021), P-Issn: 2797-8508, E-Issn: 2807-8330.
- Reyes, Carla L, (2016), Moving Beyond Bitcoin to An Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal, *61 Vill. Law Review* 191.
- Satria Muhammad Nur Lase, Aisyah Adinda, Rizkia Diffa Yuliantika, (2021), Kerangka Hukum Teknologi Blockchain Berdasarkan Hukum Siber di Indonesia, *Padjadjaran Law Review*, Volume 9, Nomor 1.
- Setia Putra, (2014), Perlindungan Hukum terhadap Konsumen dalam Transaksi Jual-Beli Melalui E-Commerce, *Jurnal Ilmu Hukum*, Vol.4, No.2 (Februari-Juli), 291.
- Weijie Zhao, (2019), “Blockchain technology: development and prospects,” *National Science Review*, Oxford University, Volume 6, Issue 2, 372.
- Widiatmika, R., Gorda, A. A. A. N. S. R., Kurniawan, I. G. A., & Huzaif, S. M. (2023). The Problems Related to Potential Trademark Rights Infringement: Construction in Inclusive Legal Perspective on Unregistered Marks. *Jurnal Dinamika Hukum*, 23(3), 499–513. <https://doi.org/http://dx.doi.org/10.20884/1.jdh.2023.23.3.3724>
- Wu, Tim, (2003), When Code Isn’t Law, *89 Va. Law Review*, 679.
- Yeung, Karen, (2018), Regulation by Blockchain: The Emerging Battle for Supremacy between The Code of Law and Code as Law, *82 Mod. Law Review* 207.

Working Paper

- Daniel W. Linna Jr., (2019), “The Future of Law and Computational Technologies: Two Sides of the Same Coin”, *MIT Computational Law Report*.

Website

- Alois, J.D, *Crypto Securities Exchange Wants to be First Blockchain Based National Securities Exchange*, www.crowdfundinsider.com, Accessed 18 Februari 2022.
- Coie, Perkins, 2017, Legal Aspects of Smart Contracts Application, <https://www.perkinscoie.com/en/news-insights/more-legal-aspects-of-smart-contract-applications.html>, Accessed 29 Maret 2022.
- Daniel Darmawan, *Sebuah Startup, Coba Kembangkan Blockchain Bantu Petani Garap Sawah di Indonesia*, www.vice.com, Accessed 14 April 2022.
- David Siegel, *Understanding the DAO Attack*, Coindesk (June 25, 2016), <http://www.coindesk.com/understanding-dao-hack-journalists/>, Accessed 28 November 2021.
- Davidson, Sinclair, Et Al, *Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology*, (2016), <https://Ssrn.Com/Abstract=2811995>, Accessed 25 Oktober 2021.
- Delmolino, Kevin, Mitchell Amett, Ahmed Kosba, Andrew Miller & Elaine Shi, *Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab*, (2015), <https://eprint.iacr.org/2015/460.pdf>, Accessed 24 April 2022.

- EIOPA, 2019, *EIOPA Report on Best Practises on Licencing Requirements, Peer-to-Peer Insurance and the Principle of Proportionality in an InsurTech Context*, https://www.eiopa.europa.eu/content/report-best-practises-licencing-requirements-peer-peer-insurance-and-principle_en, Accessed 15 April 2022
- European Commission, *Study on Blockchains: Legal, Governance and Interoperability Aspects* (SMART 2018/0038), <https://digital-strategy.ec.europa.eu/en/library/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038>, Accessed 8 Maret 2022.
- European Union, 2019, *Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies*, Publications Office of the European Union, Luxembourg, <https://publications.jrc.ec.europa.eu/repository/handle/JRC117255>, Accessed 17 Januari 2022.
- Florentin, Vindry, Presiden Jokowi Luncurkan Roadmap Revolusi Industri 4.0, <https://bisnis.tempo.co/read/1076107/presiden-jokowi-luncurkanroadmap-revolusi-industri-4-0>, Accessed 4 April 2022.
- Goodin, Dan, *a Tamper-Proof Currency Wallet just got Backdoored by a 15-year-old*, (2018), arstechnica.com, <https://arstechnica.com/information-technology/2018/03/a-tamper-proof-currency-wallet-just-got-trivially-backdoored-by-a-15-year-old/>, Accessed 28 Desember 2021.
- H. Jacquemin & Y. Pouillet, *Blockchain: Une Revolution Pour Le Droit*, J.T., (2018), Pp.801 À 819, Accessed 14 April 2022.
- International Business Machines Corporation (IBM), *Welcome to IBM Blockchain*, <https://www.ibm.com/blockchain>, Accessed 18 Februari 2021.
- Jones Day, 2020, *China Accelerates Blockchain Adoption in the New Decade*, Lexology, <https://www.lexology.com/library/detail.aspx?g=b8948d42-9225-4674-be7f-9d012c27815a>, Accessed 19 Maret 2022.
- J, Parung, *The Use of Blockchain to Support Sustainable Supply Chain Strategy*, (2019), IOP Conference Series: Materials Science and Engineering, 703(1). <https://doi.org/10.1088/1757-899X/703/1/012001>, Accessed 5 April 2022.
- Markey-Towler, Brendan, *Anarchy, Blockchain and Utopia: A Theory of Political socioeconomic Systems Organised using Blockchain*, (2018), International Journal Brit. Blockchain Assn 13, <https://Srn.Com/Abstract=3095343>, Accessed 20 April 2022.
- OECD, *The Policy Environment for Blockchain Innovation and Adoption: 2019 OECD Global Blockchain Policy Forum Summary Report*, OECD Blockchain Policy Series, (2019), www.oecd.org/finance/2019-OECD-Global-Blockchain-Policy-Forum-Summary-Report.pdf, Accessed 19 Maret 2022.
- Philippe, Denis, *Blockchain and Smart Contract: Lex Cryptographia?* <https://Philippelaw.Eu/Wp-Content/Uploads/2018/12/Blockchain-And-Smart-Contract.Pdf>, Legal Review Daor, Accessed 17 April 2022.
- Raustiala, Kal & Christopher Jon Sprigman, *The Second Digital Disruption: Streaming & the Dawn of Data-Driven Creativity*, (Aug. 8, 2018), SSRN 6-16, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3226566, Accessed 9 Oktober 2021.
- Salmon J., Myers G., 2017, *Blockchain and Associated Legal Issues for Emerging Markets*, EM Compass, <https://www.ifc.org/wps/wcm/connect/da7da0dd-2068-4728-b846-7cffe1fd24a/EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets>.

- pdf?MOD=AJPERES&CVID=mxocw9F, Accessed 25 Oktober 2021.
- Sinclair Davidson Et Al., *Economics of Blockchain* (Unpublished Manuscript), (Mar. 9, 2016), <https://Ssrn.Com/Abstract=2744751>, Accessed 19 November 2021.
- Wright, Aaron and Primavera De Filippi, *Decentralized Blockchain Technology and The Rise of Lex Cryptographia* (Mar. 10, 2015) (Unpublished Manuscript), <https://Ssrn.Com/Abstract=2580664>, Accessed 21 April 2022.
- Zhang, E, 2016, Antshares Whitepaper 1.0, [https://github.com/AntShares/AntShares/wiki/Whitepaper -1.0](https://github.com/AntShares/AntShares/wiki/Whitepaper-1.0), Accessed 21 Januari 2022.