# The Role of Blockchain in Strengthening Indonesia's Economic Stability

Pujiyono Pujiyono(✉), Moch Najib Imanullah, Hernawan Hadi, and Sendari Waskita

Department of Law Science, Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia
pujifhuns@staff.uns.ac.id

**Abstract.** The development of technology introduces people to the topic of the Internet of Things (IoT), artificial intelligence (AI), big data, and the blockchain. The blockchain became popular in 2009 and growing rapidly because the use of the Blockchain tends to be profitable in the business and government systems. This study aims to identify and analyze regulations regarding blockchain in Indonesia. This study compares blockchain regulation in Indonesia with countries in the Americas, Europe, and Asia. Based on regulatory comparisons with several countries, blockchain regulation in Indonesia is still weak. The blockchain, which stores several smart contracts, needs to be further regulated in the legislation. The use of blockchain that knows no boundaries of time and territory is the government's task in making several regulations, including regulations regarding taxation, protection of personal data, and prevention of money laundering and terrorist financing. One way that can be done is to fulfill the recommendations from the FATF which has previously regulated how blockchain works. In addition to the government, the active role of the community, especially crypto asset trading actors is needed to build a healthy ecosystem and bring prosperity to society and the country.

**Keywords:** blockchain · regulation · anti-money laundering

## 1 Introduction

The massive development of technology continues to penetrate the global boundaries of time and space. The ease of accessing information through the internet is currently inevitable and significantly affects the pattern of human life, such as how to dress, think, communicate, and others. This pattern forms a dependence of humans on technology which aims to simplify and speed up human work. Technological developments brought about the fourth industrial revolution, where smartphones play an important role in enhancing the internet in society. Therefore, the term "Internet of Things" (IoT), artificial intelligence (AI), big data, and blockchain have become mainstream.

The term blockchain became popular in 2009 when "Bitcoin" was successfully mined and started to enter the market. However, the concept of blockchain existed before Satoshi Nakamoto wrote the article entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" [1] in 2008. This concept began in 1991 when Stuart Haber and W. Scott Stornetta wrote an article entitled "How To Time-Stamp a Digital Document" in which Harber

G. D. Suprobowati et al. (Eds.): ICDNR 2022, ASSEHR 713, pp. 198–207, 2023.
https://doi.org/10.2991/978-2-494069-75-6_25

and Stornetta offered a solution using cryptography with hash functions [2]. Further research was carried out in 1998 where Nick Szabo described a complete concept of a blockchain-based currency called a bit gold. This discovery constituted the initial idea of implementing a decentralized digital currency mechanism [3], which changes control from one entity to various smaller entities.

Blockchain technology works in a decentralized manner and plays an important role in the development of the fourth industrial revolution. This is because it does not only refer to technology but how every human being can be more connected to each other quickly, to enable social and business relations in a peer-to-peer fashion [4]. Furthermore, this technology enables stakeholders to run a business efficiently, flexibly, and safely. Peer-to-peer automation with cryptosystems provides a variety of information to solve various problems in several industries, not only "cryptocurrencies", but in maritime, logistics, chemical, and others, which are enhanced by blockchain technology. An example of its implementation is the concept of intellectual property management which provides several advantages. First, the data entered into the "block" will be genuine metadata and difficult to change. Second, the tracking system and processes are accessible to the original owner. Third, royalty payments are faster and more accountable [5].

Based on the advantages and sophistication offered by Blockchain Technology, it is important to note that its use also carries many threats of crime. Along with the increase in the use of its services by governments, large companies, and private individuals, various parties are aware of the weaknesses of blockchain technology. This is evidenced by the publication of reports about cyber attacks on Ethereum. A loss of 3,068,654 million Ether occurred, equivalent to about US$30 million. This financial loss was due to the vulnerability of smart contracts, wherein the following period, hackers again found loopholes in the lack of smart contracts on the Ethereum blockchain and stole Ether equivalent to more than US$60 million in 2016 from DAO [6]. Another example cites when a hacker attacked Mt Gox in 2014 (the largest platform for trading Bitcoin) and stole the Bitcoin equivalent of US$460 million and another $27.4 million was lost from the bank account. This led to the bankruptcy of Mount Gox (Robert McMillan, 2014 https://www.wired.com/2014/03/bitcoin-exchange/). Furthermore, another research on the threat of blockchain technology was written by Ayman Alkhalifah, which documented 65 cybersecurity incidents from 2011 to 2019 with a total loss of US $ 3 billion. The common causes of these problems include hacks, scams, and smart contract errors [7].

Based on the cases of blockchain technology above, apart from technical reasons, many occurred due to the weakness of the smart contracts used. This is nothing new, but when combined with blockchain technology, abuse and crime have significantly greater opportunities. In a blockchain, there is a portion used to complete a decision quickly and automatically known as a smart contract. It does not always relate to "legal contracts" but can also relate to other general aspects. It is defined as a computer code that is intentionally created to respond to certain types of important events which take place without the active involvement of several parties. The initial command is made using certain codes that the computer will respond to as a rule that must be applied when the system works [8]. Although smart contracts have the potential to revolutionize modern methods of work, the absence of an intermediary in transactions in form of a responsible authority, becomes a significant problem when a crime occurs. Furthermore, blockchain also encountered constraints regarding the pre-conditions for contract formation in different jurisdictions. Contractual matters involving complex jurisdictions require careful consideration, as the principles of contract law will differ in each jurisdiction. For example, when fraud, hacking, or wrong transactions occur, location in the blockchain becomes a problem and it is related to the identification of the appropriate regulation. Blockchain users, on the one hand, have the advantage of fast peer-to-peer transactions, and also require legal certainty to be implemented as the rights and obligations of the parties in the agreement.

Another problem in blockchain smart contracts is the protection of personal data. The blockchain work system applies all data that is entered, rendering it difficult to recheck, change, or delete. This is because this technology adopts a hash function where every transaction that runs on it will be hashed together before entering a "block". Furthermore, the hash pointer connects one block to another to store the previous hash data. Each chain locked by a hash function is difficult to change and delete because the function in each block is different. Therefore, this concept of data that is difficult to change is contextualized with a person's data, and conflicts with the legal principle of personal data protection which accommodates the right to delete personal data in a certain network or device [9]. In addition to the description of the problems of blockchain technology and smart contracts above, there are still many others that constitute a concern for stakeholders worldwide.

The legal role related to blockchain technology and regulation poses a significant discussion in this research. This is because it aims to answer the challenges of the existing problems. In Indonesia, regulations related to blockchain which are often used in cryptocurrency transactions are still inadequate and need to be refined to create a healthy business climate and enhance people's welfare.

## 2 Research Method

This normative legal research, known as a study of documents, uses a qualitative method in analyzing data and uses secondary data as the source such as regulations, court decisions, books, legal theories, and doctrines [10]. It is also known as doctrinal legal research, which involves efforts to understand the best balance of rights and obligations under the framework defined by law. Their inspiration is drawn from moral, legal, and political philosophy [11]. This is carried out with a comparative approach, namely by comparing the laws of one country with that of others. This research compares the laws related to blockchain and cryptocurrencies with that of the United States, Switzerland, France, Germany, and Japan to make coherence a part of domestic law (Indonesian Law). Furthermore, this research aims to apply comparative law as a learning tool to better understand legal practice and its consequences in various countries [12]. The law to be adopted will pass through the harmonization stage and is adapted to the social conditions of the Indonesian people.

## 3 Blockchain Technology and Cryptocurrency Regulation

Blockchain technology and cryptocurrency are two closely related discussions. Blockchain technology helps to process cryptocurrency transactions in every country. Some countries strictly prohibit its use, while others support every development of cryptocurrency. Furthermore, rapidly developing technology forces other countries to learn immediately. Countries that either prohibit or support it, must understand how blockchain technology works because gradually it will evolve to modify every activity. Furthermore, the government needs to enact regulations to prevent the adverse effects of its use.

It is undeniable, that making laws related to technology is not easy. Law is static, while technology is highly dynamic. Therefore, in line with Herian Robert [13], the focus of enacting regulations related to blockchain technology is not only on discussing prohibitions and sanctions but on the form and use of blockchain in the future. Therefore, a very in-depth critical analysis by publicly accountable bodies, individuals, governments, and domestic regulators will be required. The next few years will involve the international community of government authorities being able to focus on blockchain and how it interacts with society. It will be necessary to answer important questions in the future on the relationship between technology and individuals that use it intentionally or unknowingly submit to it.

Regulations restricting and prohibiting the use of blockchain, especially related to cryptocurrencies, are currently applied by several countries, such as Mexico, Bolivia, and Columbia [14]. However, most countries worldwide are already in the process of developing a blockchain regulatory framework. It is noted that several countries in the United States, European Union, and Asia have developed regulations for the use of blockchain technology.

### 3.1 United States of America

The United States of America, which is the country in which this technology was developed, found it difficult to make legal arrangements. Understanding the blockchain that is constantly evolving, from simple cryptocurrency transactions to the latest ones such as tokenization [15] and Initial Coin Offering (ICO) (a replacement for Initial Public Offering (IPO)) requires a complex understanding. It does not stop at blockchain knowledge itself, as other problems such as distributed blockchain networks require a difficult approach, because they have to adapt to the jurisdiction of each of these technologies. The impact of this network distribution is the difficulty of executing crimes by the regulator when a violation occurs. When blockchain regulations are applied differently to jurisdictions, potential problems of overlapping jurisdiction and overlapping of responsible authorities will arise. There are many different views regarding blockchain and cryptocurrency between agencies. While The Securities and Exchange Commission (SEC) is the most powerful regulator, Treasury's FinCEN, the Federal Reserve Board, and the Commodity Futures Trading Commission (CFTC) differ in terms of definition.

For example, the SEC views crypto as a security, the CFTC calls bitcoin a commodity, and the treasury calls it currency. Each believes that the application of blockchain technology falls under their jurisdiction, depending on the circumstances under which it is used. These many differences have made The President's Working Group and the Financial Stability Oversight Council decide to coordinate several of these institutions. In the end, America has succeeded in uniting the differences between these agencies and developing an appropriate regulatory framework. One of the regulations is that the Internal Revenue Service (IRS) requires investors to disclose annual cryptocurrency activity on their tax returns. This is to detect the transaction history of each investor and make it easier to monitor violations. Currently, the United States is home to a large number of crypto investors, exchanges, trading platforms, crypto mining companies, and investment funds.

### 3.2 Europe

One of the innovations of cryptocurrencies is modifying an IPO into ICO. In France, after the emergence of bitcoin as a cryptocurrency and a blockchain platform that uses smart contracts, the implementation of ICOs has developed. ICOs replace IPOs because the process is easy and fast. At the IPO, it is required to meet complicated conditions and wait for approval from regulators such as the SEC in America, and companies must provide funds to hire lawyers, accountants, notaries, and others. However, an ICO does not require such conditions. In connection with the emergence of ICOs which when explored further turned out to be prone to causing crime, the French government made a regulation in form of the Action Plan for Business Growth and Transformation Act (PACTE Act). This Act sets the course of work for ICOs and Digital Assets Service Providers (DASPs). The PACTE Act was implemented only in December 2019 which stipulated that ICO initiators must first apply for a visa from the French financial market authority, Autorite des Marches Financiers (AMF) to be whitelisted for trusted publishers [16]. The verification of the individual/company in the whitelist of trusted issuers in France indicates that the token offering is safe and has passed the checking process from the AMF.

Similar regulations to France are also applied in Germany, where companies that will open an ICO must obtain approval from the Federal Financial Supervisor Authority. In Switzerland, the Swiss Federal Council provides legal certainty to the public by enacting the DLT Act to avoid regulatory mismatches, one of which is by regulating the "Uncertified Register Securities" [17]. This arrangement provides a mechanism for tokenizing rights and a way to transfer these rights.

### 3.3 Asia

On March 5, 2019, The Financial Services Agency (FSA) of Japan has submitted legal revisions for the regulation of virtual currencies, such as the Payment Services Act (PSA), The Financial Instruments and Exchange Act (FIEA), and The Act on Sales. These are mutually adjusted in regulating cryptocurrencies, where Japan requires every exchange to register, record all transaction activities, and follow several rules regarding customer protection. Even more stringent, the FIEA revision states that the method of managing cryptocurrency transactions carried out by business actors must have a company/bank trust to ensure the virtual currency of investors is safe [18].

### 3.4 Indonesia

In Indonesia, the emergence of blockchain technology is admittedly late compared to other ASEAN countries. Currently, the implementation of technology projects is still rare. Blockchain technology became popular alongside the development of the term cryptocurrency which is starting to attract the younger generation. One of the cryptocurrencies that were first popular in the community was bitcoin. It is an example of a concept carrier where it not only has the potential to become a digital currency but users can also turn it into a commodity [19].

As a digital currency, the law in Indonesia still prohibits its application. The financial authority, Bank Indonesia, 2018, prohibited the use of virtual currency as a means of payment. This is because the risk it carries is high, namely the absence of a responsible authority, no underlying assets, and highly volatile trading values. The use of virtual currency as currency is also contrary to Law Number 7 of 2011 concerning Currency, as well as Bank Indonesia Regulation Number 17/3/PBI/2015 concerning the Obligation to Use Rupiah in the Territory of the Unitary State of the Republic of Indonesia. This law states that the currency used in Indonesia is money issued by the Unitary State of the Republic of Indonesia and every financial transaction must use Rupiah. Although virtual currency is prohibited as a legal tender, it is permitted to be used in the investment sector. Furthermore, as a country that is not anti-technology development, Indonesia must open and provide regulations for the development and use of virtual currency in the investment sector. Through the Minister of Trade Regulation Number 99 of 2018 concerning General Policy for the Implementation of Crypto Asset Futures Trading (Permendag 99/2018), it is determined that Crypto Assets are legal commodities, which can be used as Futures Contract Subjects traded on the Futures Exchange.

The Ministry of Trade, in terms of developing the cryptocurrency sector in Indonesia, authorizes the Commodity Futures Trading Regulatory Agency (CoFTRA) to supervise, manage, and foster. Currently, there are 4 important regulations issued by CoFTRA, including:

1. Commodity Futures Trading Supervisory Agency Regulation Number 5 of 2019 Regarding Technical Provisions for the Implementation of the Physical Crypto Asset Market on the Futures Exchange.
2. Commodity Futures Trading Supervisory Agency Regulation Number 9 of 2019 concerning Amendments to Commodity Futures Trading Supervisory Agency Regulation Number 5 of 2019 concerning Technical Provisions for the Implementation of Crypto Assets Physical Markets on Futures Exchanges.
3. Commodity Futures Trading Supervisory Agency Regulation Number 2 of 2020 concerning the Second Amendment to Commodity Futures Trading Supervisory Agency Regulation Number 5 of 2019 concerning Technical Provisions for the Implementation of Crypto Assets Physical Markets on Futures Exchanges.
4. Commodity Futures Trading Supervisory Agency Regulation Number 3 of 2020 concerning the Third Amendment to the Regulation of the Commodity Futures Trading Supervisory Agency Number 5 of 2019 concerning Technical Provisions for the Implementation of the Crypto Asset Physical Market on the Futures Exchange.

Observing the four regulations above, cryptocurrencies, legally known as "crypto-assets" are defined as intangible commodities in form of digital assets using cryptography, peer-to-peer networks, and distributed ledgers, to regulate the creation of new units, verify, and secure transactions without interference from other parties. Unfortunately, the four rules above only define crypto assets as intangible commodities. Blockchain technology has not yet been defined or regulated. Although the technology built on cryptocurrencies does not solely use blockchain technology, blockchain is closely related to crypto asset trading activities. The blockchain itself is composed of several smart contracts of which law enforcement is currently weak. Therefore, hackers gain access to the system, make the desired huge profits, and escape. In carrying out crypto transactions on the blockchain, it is necessary to include legal and jurisdictional clauses that regulate exclusively, the crypto assets of customers. These clauses enhance legal certainty and understanding of all the rights and obligations of the parties in the agreement. Due to crypto asset trading being cross-jurisdictional, some legal terms or conditions are designed to have extra-territorial binding by executing using arbitration. Moreover, arbitration is seen as a forum that is quite flexible and universal for interpreting and resolving issues related to smart contracts. It is possible to enact regulations related to blockchain technology to involve several parties, such as the Ministry of Communication and Information (Kominfo) or the National Cyber and Crypto Agency (BSSN).

Alongside the developments related to the use of blockchain technology, the imposition of taxes on crypto-assets requires regulations. However, the Directorate General of Taxes (DGT) has not issued a tax policy for crypto assets. CoFTRA as the builder, regulator, and supervisor of crypto assets annually produce cryptocurrency reports and analyzes their impact on the Indonesian economy. If digital currency activities enhance economic progress, a tax assessment can be drawn up along with its technical guidance documents by the Directorate General of Taxes. The imposition of taxes on crypto-assets is in line with the current preparations by the Organization of Economic Co-operation and Development (OECD). The OECD aims to modernize tax transparency instruments to develop a global tax framework [20]. Furthermore, the Directorate General of Taxes can automatically impose crypto global taxes on crypto-asset trading activities.

Another problem faced by the government regarding the blockchain and cryptocurrency industry is that of Personal Data Protection (PDP) as well as Money Laundering and Terrorism Financing. The intermediary agency for selling crypto assets commonly called "Exchange" contains the personal data of users. PDP regulations must be passed immediately to protect and monitor the personal data of cryptocurrency customers on exchanges. The role of the government is highly significant for the security of the community. Personal data security of crypto-asset customers will increase the public's sense of trust in the cryptocurrency sector. Similar to the potential for misuse of personal data, cryptocurrencies are also a medium for carrying out money laundering and terrorism financing.

Based on the regulations issued by CoFTRA, cryptocurrency activities, both traders and customers of crypto assets have been charged with Anti Money Laundering (AML) and Combating The Financing of Terrorism (CFT) SOPs. However, because the working system of this crypto exchange itself takes place digitally, the AML and CFT policies must also at least work digitally. This is due to the nature of digital currency as a cross-border transaction that eases perpetrators to transact anywhere and anytime in a peer-to-peer manner. Furthermore, blockchain technology can be utilized as a tool in implementing AML and CFT policies. The technology, which is based on Distributed Ledger Technology (DLT), records all activities that occur and stores them permanently in blocks. Every transaction between users is traceable and difficult to trace. This tracking system can also be used in the Know Your Customer (KYC) principle which is highly required in crypto asset trading activities. Meanwhile, the implementation of blockchain in KYC and AML policies was in June 2018, when Synechron and R3 (which represents more than 300 partner members across multiple industries and jurisdictions) tested a KYC compliance system built on DLT. This proof-of-concept completed 300 KYC transactions involving 39 participants across 19 countries (Abbas Ali, 2018) https://www.r3.com/blog/knowing-your-customer-blockchains-ultimate-killer-app/. In this case, the financial institution managed to request access to KYC test data from the customer at the same time. This can also be done by CoFTRA in screening crypto exchanges or traders which issue the legality of licensing crypto asset trading. Furthermore, blockchain technology can be used as a means of monitoring and law enforcement against cryptocurrency activities in Indonesia. Using blockchain, certain government stakeholders do not need to manually review important documents related to KYC/AML. The use of DLT for KYC/AML policies also minimizes the potential for crimes committed by humans. If KYC/AML is carried out manually, where there is an agency or authority that holds/manages important information, it will be vulnerable to being disseminated and slow in the data verification process.

In utilizing blockchain technology, Indonesia applies the KYC/AML policy which involves the guidelines and recommendations of the Financial Action Task Force (FATF). In June 2019, the FATF adopted changes to Recommendation 15 to further clarify the requirements to be applied to Virtual Assets (VA) and Virtual Asset Services Providers (VASP). This is specifically related to applying a risk-based approach to VA activities, monitoring of VASPs for AML/CFT purposes, licensing or registration, precautions, customer due diligence, recording and reporting of suspicious transactions, sanctions, and other enforcement actions, as well as international cooperation [21]. The implementation of KYC and AML/CFT policies by FATF standards is a challenge for Indonesia's PPATK (Financial Transaction Reports and Analysis Center) as an independent institution tasked with preventing and eradicating money laundering.

## 4 Conclusion

Technological developments have brought humans into the fourth industrial revolution, which enhances human-to-human activities. One of the technology utilizations that enhances these connections is blockchain technology. This was developed to facilitate all human activities, such as in the field of cryptocurrencies. However, in line with the development in a positive direction, it is undeniable that the negative potential also develops. The prevention of, and legal action related to the use of cryptocurrencies have become a common concern globally. The lack of clarity regarding regulations on blockchain and cryptocurrencies constitutes an opportunity for criminal acts of fraud and money laundering.

In Indonesia, regulations on cryptocurrency as a commodity have not yet been extended to the blockchain. This technology is known to store several smart contracts, and its current position is weak and requires laws and regulations. The government's role in enacting regulations regarding the imposition of taxes, protection of personal data, prevention of money laundering, and terrorist financing also constitutes a challenge in the implementation process. The active role of the community, especially crypto asset trading actors, is no exception to carrying out as well as possible the existing legal provisions to build a healthy ecosystem and bring prosperity to society and the country.

## References

1. J. H. Larrier, "A Brief History of Blockchain," pp. 85–100, 2021, doi: https://doi.org/10.4018/978-1-7998-5589-7.ch005.
2. D. Bayer and W. S. Stornetta, "Sequences II," *Seq. II*, no. September 1999, 1993, doi: https://doi.org/10.1007/978-1-4613-9323-8.
3. H. Guo and X. Yu, "A Survey on Blockchain Technology and its security," *Blockchain Res. Appl.*, vol. 3, no. 2, p. 100067, 2022, doi: https://doi.org/10.1016/j.bcra.2022.100067.
4. K. Schwab, "the Fourth Industrial Revolution (Industry 4.0) a Social Innovation Perspective," *Tạp chí Nghiên cứu dân tộc*, vol. 7, no. 23, pp. 12–21, 2018, doi: https://doi.org/10.25073/0866-773x/97.
5. V. Koolwal, S. Kumar, and K. K. Mohbey, "The Role of Blockchain Technology to Make Business Easier and Effective," no. November, pp. 16–44, 2019, doi: https://doi.org/10.4018/978-1-7998-0186-3.ch002.
6. L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," *Proc. ACM Conf. Comput. Commun. Secure.*, vol. 24–28-Octo, pp. 254–269, 2016, doi: https://doi.org/10.1145/2976749.2978309.
7. A. Alkhalifah, A. Ng, A. S. M. Kayes, J. Chowdhury, M. Alazab, and P. A. Watters, "A Taxonomy of Blockchain Threats and Vulnerabilities," *Blockchain Cybersecurity Priv.*, no. December, pp. 3–28, 2020, doi: https://doi.org/10.1201/9780429324932-2.
8. R. Santos, K. Bennett, and E. Lee, "Blockchain: Understanding its Uses and Implications, The Linux Foundation." 2021, [Online]. Available: https://www.edx.org/course/b%0Alockchain-understanding-its-uses-and-implications.
9. E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain Mutability: Challenges and Proposed Solutions," *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 4, pp. 1972–1986, 2021, doi: https://doi.org/10.1109/TETC.2019.2949510.
10. C. F. . S. Hartono, *Penelitian Hukum di Indonesia Pada Akhir Abad ke-20*, 1st ed. Bandung: Alumni, 1994.
11. T. R. Tyler, "Methodology in Legal Research," *Utr. Law Rev.*, vol. 13, no. 3, p. 12, 2017, doi: https://doi.org/10.18352/ulr.410.
12. M. I. Ali, "Comparative Legal Research-Building a Legal Attitude for a Transnational World," *J. Legal Stud.*, vol. 26, no. 40, pp. 66–80, 2020, doi: https://doi.org/10.2478/jles-2020-0012.
13. R. Herian, *Regulating blockchain: Critical perspectives in law and technology*, no. December. 2018.
14. T. Ehret and S. Hammond, "Cryptocurrency regulations by country," *Regul. Intell.*, pp. 20–29, 2021.
15. A. Kharitonova, "Capabilities of Blockchain Technology in Tokenization of Economy," *Proc. 1st Int. Sci. Conf. "Legal Regul. Digit. Econ. Digit. Relations Probl. Prospect. Dev. (LARDER 2020)*, vol. 171, no. Larder 2020, pp. 28–32, 2021, doi: https://doi.org/10.2991/aebmr.k.210318.006.

16. I. Newsletter, "International Newsletter, July 2019 Launch of the PACTE Act – Action Plan for Business Growth and Transformation. Recently, DELSOL Avocats completed the following cross-border transactions : Advised ALTIFORT on three," no. July, pp. 10–12, 2019.
17. T. G. Albert, "Framework Act Adopted and Partially in Force," vol. 117, no. 5, pp. 215–219, 2021.
18. K. Kawai, A. Miyake, S. Aoki, T. Tanaka, T. Nagase, and K. Hayashi, "Revisions to Payment Services Act Provisions, etc. on Crypto Assets," no. May, pp. 1–27, 2019.
19. F. N. A. Wijaya, "BITCOIN SEBAGAI DIGITAL ASET PADA TRANSAKSI ELEKTRONIK DI INDONESIA (Studi Pada PT. Indodax Nasional Indonesia)," *J. Huk. Bisnis Bonum Commune*, vol. 2, no. 2, p. 126, 2019, doi: https://doi.org/10.30996/jhbbc.v2i2.2388.
20. OECD, "Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard," no. April 2022.
21. U. Guidance and F. O. R. A. R. Approach, "VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS," no. October 2021.