



Corporate or Seller Accountability in Blockchain and Cryptocurrency Corporate Investments

RR. Ella Evrita H^{1*}, Eny Maryana², Efridani Lubis³
¹e.evrita@sae.edu, ²enny@yahoo.com, ³efridani@yahoo.com
Universitas Islam As-Syafi'iyah

*Corresponding Author: RR. Ella Evrita H
Email: e.evrita@sae.edu

ABSTRACT

The utilization of Information Technology, media, and communication has changed both the behaviour of society and human civilization globally, and the role of law is to regulate social life. At the same time, the digital world provides unlimited space and time for its users, one of the digital developments is related to cryptocurrencies. Cryptocurrency is a digital currency that secured by cryptographic security system. Crypto money can generally used to buy various kinds of digital goods. One of the uses of owning a cryptocurrency is for investment. Currently, the development of cryptocurrencies in Indonesia is swift. Generally, people from upper-middle class already know about the term. The same thing happened in international market. With the background of the rapid development of this cryptocurrency in community, in terms of growth, the obstacles and constraints found, the authors conducted this research, and it is technically challenging to identify the role of each party in current digital business in Indonesia and the existence of a knowledge gap between consumers and producers. This research is descriptive research with normative juridical method, meaning that in discussing existing problems, researchers will look at legislation's provisions.

Keywords: Blockchain Accountability, Cryptocurrency Investment, Corporate Liability

INTRODUCTION

The COVID-19 pandemic has forced us to reduce our activities outside the home. It has also driven us to enhance our internet capabilities, making everything increasingly digital. Likewise, currency has become an innovation in the financial sector. Human interaction in all fields has become effortless and highly dynamic with internet technology. Since unlimited internet access is no longer rare, people have taken advantage of this facility, providing comfort and convenience in accessing everything without limitations. However, this convenience also makes it easier for some individuals to commit cyber-crimes.

In the financial sector, a digital currency called Cryptocurrency has gained popularity, primarily due to the potential for high profits. This has led many people, including those with minimal effort, to flock to trade and invest in it. Cryptocurrency is a digital asset designed to function as a medium of exchange using strong cryptography to secure financial transactions, control the creation of additional units, and verify asset transfers. Its transaction system is peer-to-peer, meaning transactions occur directly between individuals online without intermediaries. This exchange process relies on cryptographic technology to secure transactions, regulate the amount created, and verify transactions. Each user remains anonymous, with no way to trace transactions, their participants, or their purposes.

Digital transactions involving cryptocurrencies are unique. They have introduced a new perspective in an increasingly modern era. The current paradigm is attractive, as it is perceived as freedom from conventional financial systems. Cryptocurrencies aim to revolutionize the monetary and financial system by eliminating trust in third parties and replacing them with tokens or cryptographic systems. This new system offers expected benefits for those who need it. However, it also provides opportunities for criminals to exploit vulnerabilities to their advantage.

Additionally, the decentralized nature of cryptocurrencies means that their circulation depends entirely on the market, with no central authority to regulate them. Consequently, the rapid spread and emergence of cryptocurrencies worldwide hold great potential to impact the global economy. Due to their highly volatile prices and circulation, there are concerns about their potential to destabilize the international economy if left unchecked.

The cryptocurrency trading process operates on a mechanism of personal accountability for crypto users. Individuals run their own servers and manage their trade transactions. Sales, purchases, and pricing are determined by mutual agreement between parties. This decentralized system makes each user's computer a server, meaning everyone is responsible for their wealth. Consequently, losses such as wallet theft are not the responsibility of the state.

The blockchain mechanism's decentralized nature ensures that no institution or country has complete control over cryptocurrency technology.

Another potential issue is the lack of an adequate security system in cryptocurrency transactions. Since transactions are irreversible, fraudsters can exploit this to their advantage—once a transaction is completed, it cannot be reversed or refunded. In such cases, banks or credit card companies cannot provide assistance.

There is also a risk of Bitcoin theft from digital wallets, making users vulnerable to hackers and viruses. They are at risk of falling victim to bad faith from fellow Bitcoin activists or fraudulent transactions due to the anonymity or pseudonymous of participants.¹

RESEARCH METHODOLOGY

Amid the rapid development of cryptocurrency in the community, both in terms of growth and obstacles, this research addresses the issue of corporate responsibility in digital business crimes. The assumptions used include unclear regulations governing these matters, as the ITE Law has not yet been formulated to address these issues, the technical challenges in identifying the roles of each party in digital business, and the knowledge gap between consumers and producers. The research problem formulations related to cryptocurrencies in Indonesia include legal certainty regarding transactions conducted by corporations in digital businesses through Crypto Assets, identifying the roles of various parties in digital business, and addressing knowledge gaps within society to reduce corporate crime in digital business.

RESULT AND DISCUSSION

Legal Certainty in Transactions Conducted by Corporations in Digital Business through Crypto Assets

Economic Growth and Digital Era Development

The digital era, from Era 1.0 to the latest, is called Society 5.0. This era marks a time of advancements in all aspects of human life, transitioning from analogue to fully digital through technology that makes it easier for people to access information via the Internet with adequate device support. These changes and developments will continue in response to society's demand for more practical, faster, and efficient solutions. However, these transformations inevitably bring both positive and negative impacts on people's lives.

¹ Timbo Mangaranap Sirait, "The Implementation of Procedural Law of Responsibility Enforcement of Corporate Crime in Integrated Criminal Justice System," *Jurnal Dinamika Hukum* 17, no. 3 (October 24, 2017): 342, <http://dinamikahukum.fh.unsoed.ac.id/index.php/JDH/article/view/769>.

In general, the digital era represents a period where technology simplifies activities and everyday life. Past technologies have been replaced with more practical and modern innovations, allowing for faster access to information and essential needs.

Digitally, the term refers to a system based on numerical states consisting of 0s and 1s, also known as binary digits. Digital data or signals are represented by these numbers and are typically associated with physical quantities such as magnetic polarity or voltage. Digital technology enables the storage, generation, and processing of data in two states—positive and negative—where positive is represented by 1 and negative by 0. The data stored using digital technology is expressed in sequences of 0s and 1s, with each individual digit known as a bit. Computers process these bits in groups, commonly referred to as bytes.

Before digital technology, electronic transmissions relied solely on analogue systems, which conveyed data through electronic signals of varying frequencies or amplitudes added to carrier waves. Examples include radio broadcasts and conventional telephone transmissions. Modern digital technology is now widely used in communication media, such as fibre optic transmission and satellites. For instance, a modem converts digital information from a computer into analogue signals for telephone lines and vice versa, converting analogue telephone signals into digital data for computer processing.

The Understanding of Digital Age and Its Impact on Life

Etymologically, “digital” comes from the Greek word *digitus*, meaning the fingers or toes of humans, which total ten. In this context, the value of 10 consists of two radices: 1 and 0. Digitization, or digital technology, refers to the transition from analog mechanical and electronic technology to digital technology. This process has been implemented since the 1980s and continues to this day.

The digital era began to emerge due to a revolution initially triggered by the younger generation in the 1980s. The rise of digitalization marked the beginning of the digital information era and technological advancements, which are now far more modern. Digitalization represents the modernization of technology and is often linked to the development of the Internet, computers, and advanced tools designed to simplify human tasks. However, the digitalization of companies in the modern era does not happen instantly; it undergoes various stages of transformation.

Benefits of the Digital Age for Life

A digital revolution is a form of globalization, specifically an integration process implemented internationally through the exchange of worldviews, thoughts, products, and various cultural aspects. This process is driven by advancements in internet telecommunications infrastructure and transportation.

One of the benefits of the digital era is ease of communication. Almost everyone is surrounded by sophisticated digital devices such as smartphones. Children, teenagers, and parents alike use smartphones in their daily lives. With these devices, people can easily connect with others through internet technology, making communication more seamless in the digital era.

Another advantage is mobility and flexibility. Beyond communication, the digital era allows people to perform tasks without spatial or temporal limitations. For example, people can watch live events from around the world without being physically present. Many activities can now be done remotely, such as student admissions without needing to visit the campus or shopping without going to physical stores.

The dominance of the internet over traditional phone credit is also a notable aspect. Many, especially millennials, prioritize internet data over traditional phone credit. This is because internet data allows access to cyberspace and provides a more cost-effective communication medium than regular phone credit.

Additionally, the digital era has made shopping and accessing necessities more convenient. With the internet, e-commerce platforms and online stores enable people to shop and obtain what they need without leaving their homes. These platforms also connect buyers and sellers across distances, enhancing accessibility and convenience.

Positive and Negative Impacts of Digital Era

In the development of digital technology, there are many impacts, both positive and negative. The positive impacts of the digital era include faster and easier access to information, the growth of innovation in various fields driven by digital technology that enhances efficiency in people's work, and the rise of digital-based mass media, especially electronic media, as a valuable source of public knowledge and information. Additionally, the quality of human resources improves through the development and utilization of information and communication technology. The availability of various learning resources, such as online libraries, e-learning platforms, and online discussions, contributes to better education quality. The emergence of e-businesses, such as online stores, also makes it easier for consumers to access goods based on their needs.

However, the digital era also brings negative impacts that must be anticipated. One of these is the risk of Intellectual Property Rights (IPR) violations due to easy data access, leading to plagiarism and fraud. There is also a decline in deep thinking skills, as children become accustomed to quick, surface-level thinking and reduced concentration. Another issue is the misuse of knowledge for criminal activities, such as hacking banking systems, which leads to ethical and moral degradation. Furthermore, information technology is not always used effectively as a learning tool, as some individuals still rely on printed

e-books instead of digital formats or prefer visiting physical libraries over utilizing digital ones.

The Differences in Digital and Analogue Technology and the Advantages and Disadvantages of Digital Technology

Digital technology is a fast calculation system that processes information in the form of digital codes, numerical values, or numbers. Before processing, a specific sensor is required to convert accurate data into a series of digital codes. Once processed, the results are displayed on a screen. Digital technology is simply a tool—a program designed with unique settings, similar to analogue computers. Analogue computers, used in various machines, function as measuring instruments that automatically provide information and control. However, one of the weaknesses of analogue technology is its decreasing accuracy over time and the lengthy processing required for information.

One of the advantages of digital technology is that data storage is not affected by bad weather or external noise since it is transmitted through a digital signal. Additionally, various types of communication systems can emerge, making it more versatile. Digital technology is also economical due to lower maintenance costs, increased practicality, and greater stability. However, it also has its drawbacks. There is a risk of errors when converting analogue signals to digital signals, which can impact accuracy. Furthermore, critical digital data, such as work documents and account numbers, are vulnerable to hacking. Another concern is its potential addictive effect on users, which can reduce empathy and social awareness in real-world interactions.

The Development of Digital Age

The development of communication in the digital era began with the emergence of smartphones equipped with highly advanced features. One of the most important aspects is the function of the internet, which has become more optimized and is used for communication, connecting people, and enabling online communication through video calls that were previously impossible.

Digital technology also makes it easier for companies to reach their consumers. As a result, entrepreneurs who are not prepared for the digital era will be left behind. To anticipate competition and keep up with product sales developments, sellers must transition to digital technology.

Financial technology (fintech), such as digital wallets, has emerged alongside the advancement of digital technology and business progress. This development remains closely linked to application-based businesses. Fintech relies heavily on applications to provide services to its users.

E-commerce has emerged as a provider of online product and goods sales through digital applications or websites. People no longer need to go to malls to

shop, as they can purchase products directly via smartphones. Additionally, e-commerce helps sellers increase their sales.

Must-have Things in the Digital Age

The Essential Things Needed in Today's Digital Era Are as Follows: Cognitive skills, which involve acquiring knowledge based on experience and information. In the digital field, this includes skills in internet technology and an understanding of current technology. Social skills related to how to control emotions. Specific skills related to work that range from personal development, sales and marketing, finance, business, and lifestyle to health. Communication skills, which are the primary skills that must be possessed, as they help improve speaking abilities and build a person's confidence, making it easier to communicate and negotiate with clients. Leadership skills, systematic thinking skills, and networking skills are also essential. Leadership skills are demonstrated through actions when facing problems and finding solutions to overcome them, reflecting the ability to lead, supported by critical thinking.

The Digital Age and Its Influence on Consumer Behavior

Consumers in the digital era will be easier to get information from a product. They want a quality product by comparing it via the Internet. Therefore, producers must be able to provide quality products to consumers. The digital era will also make consumers want an easy way of ordering and paying. Because, of course, they want an efficient manner and it doesn't require a lot of time to buy a product. Consumer behaviour will continue to follow the current style or fashion. This behaviour will make it easier for producers to find what consumers want and need. Society demands something more sophisticated. Although, of course, there are some repercussions behind it.

Corporate crimes are committed without violence (non-violent crimes) but are always accompanied by fraud (deceit) and misrepresentation of reality. Concealment of facts, manipulation, breach of trust (breach of faith), deception (fraud), and circumvention of regulations (illegal circumvention) distinguish it from civil and administrative cases. From this classification, the forms of corporations can be classified as follows: Public Corporations are established by the government to fulfil administrative tasks in public affairs. For example, district or city government. Private Corporations are established for private interests, which can be engaged in finance, industry, and trade. These private corporation shares can be sold to the public and added with the term "go public." Quasi-Public Corporations serve the public interest (public service). Examples include PT Kereta Api Indonesia, State Electricity Company, Pertamina, and Drinking Water Company.

Based on the conditions that occur in society, corporate crime is divided into several forms, namely corporate crime in the modern era involving administration,

environment, finance, labour, goods products, and dishonest trading practices. These crimes can also be described as follows: Administrative violations include non-compliance with the requirements of a government agency and court, such as disobeying orders from government officials. For example, illegally building environmental pollution control facilities and unauthorized gains, such as violations related to letters or valuable information through digital media—namely providing wrong information to the primary guardian or issuing false statements. Hunting violations can be divided into four types: labour discrimination (race, gender, and religion), worker safety, unfair hunting practices, and wages and work violations. Serious violations involve the factory fee and three government agencies: The Consumer Product Safety Commission, responsible for violations such as the ageing AVT poison prevention package, the flammable fabric law, and the consumer product safety law; The National Highway Traffic Administration, regulating the motor vehicle manufacturing community; Assigning defects to owner's agents, buyers, and dealers so that the manufacturing community (factory) has to repair defects, including faulty installation parts, system malfunctions, and poor design. Dishonest trading practices include abuse of competition (monopoly, incorrect information, price discrimination) and false and misleading advertising, which are essential in dishonest trading practices. These result from unlawful acts committed by the corporation.

Blockchain is a technology used as a digital storage system or data bank connected to cryptography. Its use is inseparable from Bitcoin and other cryptocurrencies. However, many other sectors can also use this technology. "Block" means group, and "chain" means chain. The naming reflects how blockchain technology works, utilizing computer resources to create connected blocks (chains). These interconnected blocks are later used to execute transactions. This technology is quite interesting because it is decentralized. Blockchain can run itself using computer algorithms without any particular system regulating it. Cryptocurrency is a digital currency system secured using cryptography. Thus, the currency cannot be counterfeited by irresponsible people. These crypto-assets use blockchain technology, which is a database that cannot be changed or altered. Cryptocurrencies and blockchain are different but related. Crypto is a digital currency, while blockchain is the technology and digital data storage connected to cryptocurrency transactions. Blockchain has a decentralized nature, meaning it does not have a single authority with complete control. Instead, control is distributed across multiple computers with special software. Bitcoin miners are people who prepare special computers to perform mathematical calculations to open new block gaps in the blockchain. They calculate a unique hash value based on a combination of previous cryptographic hashes. When a transaction occurs between an online store that provides a Bitcoin wallet and a

buyer, the transaction is sent to the miners. This process creates a new block and stores the Bitcoin in the transaction.²

The Impact of Digital Era on Corporate Crime Development in Indonesia

Security in Line with Anti-Money Laundering and Anti-Terrorist Funding Programs. The technology used by blockchain is very transparent and makes transactions easier. Every new technological development certainly has its element of excellence. Likewise, in the field of blockchain. The advantages that its users can obtain are pretty diverse. Technology blockchain has secure and transparent transaction data because when we make transactions, there will be public access that we can see without other people having access to join. This transparency is not contained in the banking or financial system or pattern in general. In addition to being transparent, this technology also has a very secure data protection system because there is a verification system by every miner or miner when making a transaction, namely before it will be executed on many computers later, and the database structure is append-only or can only add and have no edit command access. This is what makes hackers unable to hack or social engineering to change their data. In general, the conventional currency transaction process will take quite a lot of time, and there is a human error factor involved in it. Technology blockchain, transactions become more efficient, fast, and of course safe. Technology blockchain is equipped with the advantages of encryption with cryptography, so transaction security is not a problem. By using cryptography, transaction history cannot be changed because it is encrypted to minimize fraud. In addition, an essential function of blockchain is its audit capability. Everyone can view and track transaction data, making it possible to know the audit trail of an asset. There is no longer any potential for embezzlement of corruption funds because transaction data are public, immutable, and only supplementary. Based on the various advantages of blockchain, it is highly coveted by economic actors and the government because this technology is very much in line with anti-money laundering and anti-terrorist funding programs. Blockchain is helpful as a tool in new anti-money laundering solutions for fraud and reduces risk across financial institutions. This is because the data stored in the framework cannot be changed. In a blockchain, incoming data cannot be edited or modified. Instead, they can only be added after entering the system. This is especially useful in monitoring anti-money laundering transactions as it prevents criminals from trying to cover up their transactions to prevent their crimes from being detected. Commerce will always exist on the blockchain, no matter what criminals do to try to change them. Technology blockchain and its distributed ledger should be incorporated into new fraud and risk compliance solutions for financial institutions worldwide. This creates opportunities for greater transparency between financial institutions and regulations in the long term. Using

² Klaus Schwab, *Revolusi Industri Keempat* (Jakarta: PT. Gramedia Pustaka Utama, 2019).

blockchain will make it easier for financial institutions to report suspicious activity with worldwide laws. This transparency will create new opportunities for financial institutions and rules to work together.³ By encouraging standardization using blockchain, they can simplify the creation of anti-money laundering solutions that work. Together, they can make a difference in curbing money laundering in the global economy.⁴

Convenience in Knowledge Gap to Reduce the Occurrence of Corporate Crime. The knowledge gap is a gap, meaning that there is no regulation to face the challenges of new technology. This is the challenge of implementing new technology in Indonesia, making the government need to issue regulations that can optimize the potential of technology and simultaneously mitigate the risks of using technology. Conditions like this can cause these technologies to develop and converge quickly without adequate supervision and protection for their operation, causing people to feel worried and uncomfortable using digital technology. To fill the knowledge gap that exists in Indonesia, the Directorate General of Informatics Applications, Ministry of Communication and Informatics, and the Center for Innovation Policy and Governance conducted studies to understand the development of big data, artificial intelligence, blockchain, and financial technology in Indonesia, describe the practices of these technologies in Indonesia, their implications, and the challenges they face, and describe what policy principles should be accommodated in technology governance over big data, artificial intelligence, blockchain, and financial technology. These four technologies were chosen because they are the main preconditions that lead to the emergence of various technological phenomena and new technological innovations.

Halal in The Legal Status of Cryptocurrency Based on Islamic Law. Cryptocurrency has become the first implementation of blockchain technology, and its potential is not limited to payment systems. Decentralized applications affect areas of life such as economics, science, education, art, and culture. The first cryptocurrency to be introduced was Bitcoin, and it started operating in 2009. Public interest is high, resulting in the price of Bitcoin soaring. Recorded in July 2010, the price of Bitcoin was USD 0.04951 and reached its highest on April 17, 2021, which was USD 63,223.88, or up 127,699,212.28 percent from the first record price. Despite the promising prospects with futuristic technology, Bitcoin and other cryptocurrencies harm various sectors. In Indonesia, there are pros and cons to using cryptocurrencies as a means of payment transactions. This is because cryptocurrencies have not met the criteria as applicable currencies in

³ Behzad Esmaeilian et al., "Blockchain for the Future of Sustainable Supply Chain Management in Industry 4.0," *Resources, Conservation and Recycling* 163 (December 2020): 105064, <https://linkinghub.elsevier.com/retrieve/pii/S0921344920303815>.

⁴ Yasanur Kayikci et al., "Critical Success Factors for Implementing Blockchain-based Circular Supply Chain," *Business Strategy and the Environment* (April 27, 2022), <https://onlinelibrary.wiley.com/doi/10.1002/bse.3110>.

Indonesia as regulated in Law No. 7/2011 concerning Currencies. From a sharia perspective, there is a debate about the existence of virtual currencies. The religious authorities of the Turkish Government and the Grand Mufti of Egypt have declared that virtual currency is haram or prohibited. The verse of the Quran that represents economic activities or activities in general, including cryptocurrencies, can be found in An-Nisa verse 29, which explains that every transaction activity must be avoided from vanity.⁵ About the use of cryptocurrency, currently, cryptocurrency users use it more as a means of speculation and trading. It aims to profit from investing and trading activities with speculation, which contains elements of *gharar*, *maysir*, and *usury*. In the Quran, Surah Al-Maidah verse 50 describes investment and trading activities with speculation. Cryptocurrencies currently still contain high price volatility and instability to very high fluctuations in value; this is synonymous with speculation on price differences. So that the intention to get results or profits from the price difference is included in the elements of *gharar* and *maysir* if used for investing and trading cryptocurrencies.⁶

Barriers to Blockchain Development in Indonesia. Blockchain technology has become well-known as one of the most significant innovations in the modern era. In its simplest form, a blockchain is a distributed ledger that facilitates data exchange on a peer-to-peer network. Blockchain technology is a very secure method of storing and maintaining records. Once a transaction is created and validated by all parties involved, it becomes immutable and cannot be modified or reordered. On the other hand, blockchain technology is still in its infancy, so it has several limitations, including scalability, security, privacy, and energy consumption. These barriers must be removed to ensure effective technology integration. Some barriers include uncertainty and immaturity of the technology, slow adoption rates, scalability issues, security risks, privacy concerns, high energy costs, and high investment costs.⁷

Regulations Are Still Scattered. The role of the law is to regulate social life. In developing countries, the progress of people's lives cannot be separated from the role of orderly implementation of the law. Regarding infrastructure and law governing policies in cyberspace, the government has prepared supporting facilities and infrastructure such as the Information and Electronic Transactions Law. The digital world provides unlimited space and time for its users. However, regulations supporting this development must meet several criteria, such as being

⁵ Isti Nuzulul Atiah Prima Dwi Priyatno, "Melirik Dinamika Cryptocurrency Dengan Pendekatan Ushul Fiqih," *JURNAL ILMIAH EKONOMI ISLAM (JIEI)* 7, no. 3 (2021).

⁶ Shamil Shovkhalov and Hussein Idrisov, "Economic and Legal Analysis of Cryptocurrency: Scientific Views from Russia and the Muslim World," *Laws* 10, no. 2 (May 10, 2021): 32, <https://www.mdpi.com/2075-471X/10/2/32>.

⁷ Centre for Innovation Policy and Governance (CIPG), *Big Data, Kecerdasan Buatan, Blockchain, Dan Teknologi Finansial Di Indonesia Usulan Desain, Prinsip, Dan Rekomendasi Kebijakan*, 2018.

technology-neutral, transparent, non-discriminatory, supporting innovation, ensuring legal certainty, and balancing harmonization and innovation. Blockchain itself has rules in the form of changing the world by improving peer-to-peer interaction, providing full control of assets, encouraging scientific advancement, offering stability against inflation, and boosting fundraising.⁸

The Concept of Corporate/Seller Liability in Blockchain and Cryptocurrency Investments

Several Systems of Corporate Criminal Liability in International Conventions

The fields of business development and human rights encompass various ways to bridge the impunity gap by increasing corporate accountability for human rights violations. One key aspect of corporate accountability is the controversial development of corporate criminal liability at the international level. However, none of the contemporary international criminal courts have explicit jurisdiction over legal entities such as corporations. Over the years, these courts have developed a solid body of jurisprudence addressing violations of the administration of justice and have taken such matters very seriously. Most importantly, what is at stake in this process is not just a vague or complex notion of respecting the Tribunal or judge.

There is no doubt that corporations, including digital-based ones, enjoy rights under international law, particularly under international human rights treaties. Two examples illustrate this point. Corporations have rights under the European Convention for the Protection of Human Rights and Fundamental Freedoms and have filed claims before the European Court of Human Rights ("ECHR") alleging violations of these rights. Additionally, companies can bring international claims against the United States, Mexico, and Canada under the North American Free Trade Agreement.

Corporations are also subject to obligations under international law, both directly and indirectly. International law requires states to regulate their citizens, including corporations, thereby indirectly imposing corporate obligations rooted in international law. To fulfill this obligation, and sometimes on their initiative, states hold corporations accountable for acts committed outside their territory.

Corporations must be held criminally responsible for three reasons: collective actions are likely to cause greater harm than individual actions; the actions of individual employees may not be sufficient to hold any one of them liable under international law, even when a clear wrong has been committed; and effective prevention of collective wrongdoing requires systemic punishment.

⁸ Raji Ajwani-Ramchandani et al., "Towards a Circular Economy for Packaging Waste by Using New Technologies: The Case of Large Multinationals in Emerging Economies," *Journal of Cleaner Production* 281 (January 2021): 125139, <https://linkinghub.elsevier.com/retrieve/pii/S0959652620351830>.

Integrated System Model in Eradication of Corporate Crime

Digital investment-based corporate fraud is a new crime that has evolved across various business activities, with increasingly diverse types, particularly in the economic sector. These include non-compliance with court decisions, failure to pay court fines, investment fraud schemes, Ponzi scheme fraud, mass marketing fraud, health care fraud, fictitious after-sales services, bribery, separation of tests and services to inflate costs, durable medical equipment fraud, diversion of pharmaceutical drugs, fraudulent outpatient surgeries, internet pharmacy sales, and financial institution fraud. The latter includes fictitious bank accounts, securities/commodity fraud, financial fair violations, illegal banking transactions, corporate fraud, and many more.

Criminal policy is a crucial tool in addressing corporate crime. Therefore, criminal sanctions for corporate offenses must be assessed for their urgency and effectiveness. In particular, criminal procedures must be systematic and integral to ensure a simple, straightforward, and cost-effective corporate justice system. Additionally, they should prevent disparities in sanctions and inconsistencies in applying different models of criminal responsibility when judges make decisions.

The rapid development of corporate crime necessitates the establishment of an integral criminal procedure law within Indonesia's criminal justice system to ensure a fair and impartial judiciary. Despite various legislative provisions governing corporate crime, fragmented criminal procedure laws remain a major obstacle to effective law enforcement.

A "systematic" approach means creating a structured legal framework within a specific or general area of law. Instead of a disorganized collection of regulations resembling an impenetrable forest, the legal system should function like an orderly garden, maximizing its utility for society. This systematic legal procedure should guide the handling of corporate criminal cases comprehensively, covering investigation, prosecution, and sentencing by judges in court.

Legal Regulation (Sanctions) Model and Actions to Prevent the Corporate Crime

The criteria by Clinard and Yeager are as follows: the degree of loss to the public, which refers to the extent of harm caused to society; the duration of the violation, indicating how long the corporation has committed the offense; the frequency of violations by the corporation, which measures how often such offenses occur; evidence of intent to violate, proving that the corporation acted deliberately; evidence of extortion, as in bribery cases, showing involvement in corrupt practices; the degree of notoriety engendered by the media, reflecting the level of public awareness due to media coverage; precedent in law, referring to relevant legal cases; the history of serious violations by the corporation, which considers past offenses; deterrence potential, assessing the likelihood of preventing future violations; and the degree of cooperation evinced by the

corporation, indicating how willing the corporation is to comply with legal processes. Therefore, Packer further emphasized that the conditions for the optimal use of criminal sanctions must include the following: the prohibited acts, in the view of most members of the community, must be clearly dangerous to society and cannot be justified by any important societal interest; the application of criminal sanctions for such acts must align with the purposes of punishment; eliminating such acts must not obstruct or hinder desirable societal behavior; these acts must be addressed impartially and without discrimination; criminal law enforcement should not appear excessively burdensome, either qualitatively or quantitatively; and there must be no reasonable alternatives to criminal sanctions for addressing the behavior in question.

Digital Legal Basis

From the various scopes of cybercrimes that have infiltrated different aspects of people's lives, several categories require attention. Criminal acts via social media include mocking, humiliating, slandering, defamation, misleading, lying, inciting, insulting, promoting violence, pornography, gambling, drug abuse, neglecting religious values, violating human dignity, and jeopardizing international relations. Variations of decency crimes include pedophilia, sexual exploitation of children, live sex shows, obscene and indecent transmissions, and obscene or indecent telephone calls. Cybercrimes in telematics include illegal access (hacking), cracking, illegal interception, data interference, system interference, misuse of equipment, computer-related forgery, and internet fraud. Violations of intellectual property rights include copyright infringement, cybersquatting, cyber parasites, typosquatting, and domain hijacking. Criminal acts related to privacy and personal data include identity theft, illegal access, and the dissemination of private and sensitive personal data. Cyber terrorism involves politically motivated attacks on official government websites, information systems, and data, leading to violence against civilians and carried out by sub-national or secret groups. Cybercrimes in trade and finance include spamming, internet scams, carding, page jacking, phishing, security fraud, cyber laundering, and illegal trafficking of alcohol and drugs. Cybercrimes in taxation involve tax evasion or tax embezzlement through internet transactions.

According to legal expert Barda Nawawi Arief, cyber offenses align with the Council of Europe's Convention on Cybercrime (No. 25/2000). These crimes include computer-related offenses such as illegal access to computer systems, illegal interception of transmissions and broadcasts, illegal data interference, illegal system interference, and misuse of devices. Additional offenses include computer-related forgery and fraud, content-related offenses such as child pornography, and copyright-related offenses such as copyright infringement. Cybercrimes also extend to corporate activities as businesses adapt to the Industrial Revolution 4.0.

With the rapid development of information technology, media, and communication, societal behavior and global civilization have transformed significantly. This advancement has made world relations borderless, causing rapid social, economic, and cultural changes. While information technology contributes to human welfare and progress, it also serves as an effective tool for legal violations. A new legal regime, known as cyber law or telematics law, has emerged. Cyber law is an internationally recognized legal term related to information and communication technology. Telematics law represents the convergence of telecommunications law, media law, and informatics law. Other related terms include the law of information technology, cyberspace law, and virtual world law. These legal frameworks address activities conducted through computer and communication networks, both locally and globally, utilizing computer-based information technology. This electronic system can be perceived virtually.

Corporate Legal Liability in Information Crime and Electronic Transactions (ITE)

Corporate crimes are associated with criminal acts regulated in Law No. 19/2016 concerning Electronic Information and Transactions (ITE). This law states that corporations can be individuals or legal entities, as outlined in Article 1, points 21 and 22. According to these provisions, a person is defined as an individual, whether an Indonesian citizen, a foreign national, or a legal entity, while a business entity refers to individual or partnership companies, both legal and non-legal entities.

Almost all crimes related to Information and Electronic Transactions are heavily influenced by human actions and can also be committed by corporations. Although corporations, like humans, are subject to criminal law, they are artificial legal entities. Consequently, certain offenses may be committed by individuals but are not inherently applicable or possible for corporations.

As legal entities, corporations have their own legal identity, which is distinct from that of their shareholders, directors, or other corporate organs. Under civil law, corporations or legal entities, as subjects of civil law, have the ability to engage in buying and selling activities, enter into agreements or contracts with other parties, and sue or be sued in court regarding civil matters.

Shareholders benefit from the concept of limited liability, and corporate activities remain continuous, meaning the corporation's existence is unaffected by changes in membership, including the addition of new members or the departure or death of existing ones. However, the concept of corporate criminal liability remains a topic of debate. Many argue against the notion that an artificial legal entity can commit a crime or possess criminal intent leading to liability. Furthermore, a corporation, lacking physical presence, cannot literally appear in court or sit as a defendant during judicial proceedings.

Legal Certainty of Corporate Transactions in the Cryptocurrency Asset Business

One of the most important factors in transactions and activities conducted through information technology is the protection of personal and confidential data. Personal data includes highly private information such as medical records, family data, and other sensitive details like a biological mother's maiden name, transaction data, and credit card payments. Such information can potentially be exploited for criminal activities and illegal financial gain. For example, the remaining balance of a credit card can be identified if an unauthorized party gains access by providing certain personal details to the credit card provider's customer service. Digital technology significantly accelerates the delivery of necessary information for companies to operate efficiently.

With digitalization techniques, companies can more easily access the data they need, including employee records, performance data, and other critical information. Digitalization systems can be tailored to meet specific business needs. However, broader challenges arise in civil matters as e-commerce transactions become an integral part of both national and international commerce.

The emergence of crypto assets or cryptocurrencies began with blockchain technology. Blockchain serves as the foundation for cryptocurrencies such as Bitcoin, Ethereum, and other digital assets. However, its benefits extend beyond cryptocurrencies to various fields involving technology and digitization. The primary purpose of blockchain is to allow digital information to be recorded and distributed irreversibly, ensuring that ledgers cannot be altered, deleted, or destroyed. This characteristic makes blockchain known as distributed ledger technology (DLT). Some sectors utilizing blockchain focus on data decentralization, leading to the issuance of tokens or digital currencies (cryptocurrencies) as platform commodities.

According to Wikipedia, a crypto asset is a digital asset designed to function as a medium of exchange using strong cryptography to secure transactions, control the creation of additional units, and verify asset transfers. These digital assets exist solely in cyberspace without a physical form. They can function as a medium of exchange, facilitating transactions for goods, services, or currency exchanges. The peer-to-peer nature of cryptocurrency transactions ensures they are conducted directly online without intermediaries. Cryptographic technology secures transactions, controls the amount of currency created, and verifies transactions. Neither buyers nor sellers can determine the identity of transaction participants. One advantage of digital currency is its global acceptance, allowing seamless international transactions without exchange rate fluctuations. Since no third parties are involved, transactions remain highly secure, and users maintain full responsibility for their funds. Additionally, the decentralized system reduces risks associated with data loss or corruption, as data is stored on local servers belonging to miners who generate blockchain blocks.

The fundamental value of cryptocurrencies increases as more businesses accept them as a payment method. This value growth is driven by supply and demand, where the limited supply of digital money contrasts with increasing demand. This dynamic results in continuous appreciation, attracting individuals seeking high-profit potential.

Despite its growth, many financial institutions remain divided on the legal status of cryptocurrencies. Their development necessitates modern financial and banking regulations, particularly those that emphasize risk-based approaches to minimize potential externalities. In the cryptocurrency ecosystem, most risks arise when digital assets interact with the real economy. Criminal activities often exploit these interactions, underscoring the need for regulations that mitigate risks by focusing on intermediaries facilitating exchanges between cryptocurrency and legal tender. Such regulations operate indirectly, targeting third-party partners rather than business entities when converting bitcoin into national currency.

Roles Played by Parties in Digital Business

Central Bank (Bank Indonesia)

Previously, Bank Indonesia strictly prohibited financial institutions from using cryptocurrencies. Not only is their use banned, but financial institutions are also prohibited from facilitating transactions involving Bitcoin and other cryptocurrencies. Bank Indonesia enforces this restriction, particularly for institutions working with BI, as cryptocurrencies are not recognized as legal payment instruments or financial services under the Constitution (UUD), the Currency Act (UU), and the BI Law. Cryptocurrencies are considered assets, not fiat currencies.

For cryptocurrencies to be legally recognized, governments and central banks must acknowledge them as legal tender. However, the government and central bank reject this recognition for several reasons, including the central bank's responsibility to control the money supply, which influences inflation and economic growth. If cryptocurrencies emerge as a widely used trading tool, they could undermine the central bank's role and disrupt monetary policy. Consequently, central banks do not accept cryptocurrencies and prohibit them as legal tender.

The GovernmentThe government emphasizes the risks associated with cryptocurrency circulation, particularly its potential use for criminal activities such as drug trafficking, prostitution, terrorism, and money laundering. Since cryptocurrency transactions are encrypted, they cannot be easily tracked by third parties, including governments. This lack of transparency makes governments reluctant to allow the widespread circulation of cryptocurrencies.⁹

⁹ Supramana, *Hukum Uang Di Indonesia* (Bekasi: Gramata Publishing, 2014).

Financial Services Authority (OJK)

OJK is an independent financial institution responsible for regulating, supervising, inspecting, and investigating the financial services industry, including capital markets, banks, and non-bank financial service providers such as insurance companies and fintech firms. OJK's primary focus is to maintain financial stability and enhance Indonesia's economic competitiveness.

OJK reportedly prohibits cryptocurrencies because they do not meet the criteria to function as a currency. As an investment vehicle, cryptocurrencies must be legally enforceable, possess clear fundamental value, and serve a defined function. Currently, cryptocurrencies do not fulfill these criteria, making them more speculative than a legitimate investment. Additionally, cryptocurrencies are highly volatile, with price fluctuations driven by supply and demand imbalances. When these imbalances correct, investors risk significant financial losses.

Commodity Futures Trading Supervisory Agency (CoFTRA)

BAPPEBTI, under the Ministry of Trade, is responsible for overseeing and regulating futures trading, including cryptocurrencies. The agency operates under Law No. 32 of 1997 on commodity futures trading. CoFTRA monitors and regulates futures trading activities related to cryptocurrencies, treating them as tradeable commodities rather than currencies. It oversees various commodities, including non-financial primary products (such as mining, energy, and agricultural products) and non-financial non-primary products (such as bonds, foreign exchange, interest rates, and crypto-assets). While both CoFTRA and OJK regulate different aspects of the financial sector, CoFTRA specifically focuses on commodity-based trading.

Indonesian Ulema Council (MUI)

The Indonesian Ulema Council (MUI) is an organization composed of Muslim scholars, intellectuals, and community leaders. While it operates independently, it collaborates with various domestic and international entities, provided that these partnerships align with its mission and values. MUI aims to contribute to national progress while upholding Islamic principles.

MUI has issued a fatwa on the legal status of cryptocurrencies based on Islamic law. According to this ruling, cryptocurrency as a legal currency is haram due to elements of gharar (uncertainty), dharar (harm), and qimar (gambling). It also contradicts Law Number 7 of 2019 and BI Regulation Number 17 of 2015.

Gharar refers to uncertainty or deceptive practices that could lead to harm. Dharar denotes transactions that cause damage or financial loss, potentially resulting in an unfair transfer of ownership rights. Qimar relates to contracts involving uncertainty, often linked to gambling. Furthermore, cryptocurrency does not meet the requirements of *syar'i sil'ah*, which stipulates that an asset must have a physical form, intrinsic value, a known quantity, clear ownership rights,

and the ability to be transferred to a buyer. However, MUI permits cryptocurrency trading as a commodity or asset under specific legal conditions, provided it qualifies as *sil'ah*, has an underlying asset, and offers clear benefits.

How to Deal with the Knowledge Gap to Reduce the Occurrence of Corporate Crime in Digital Business

In Indonesia, cryptocurrency is only recognized as a commodity asset or investment tool, regulated by BAPPEBTI (Commodity Futures Trading Supervisory Agency). It is not considered a means of payment or medium of exchange due to Law No. 7 of 2011, which prohibits the use of currencies other than Rupiah. Consequently, a mutual agreement and legal framework are necessary to regulate cryptocurrency adoption. This legal framework will establish regulations governing cryptocurrency movements in Indonesia. However, regulatory development in Indonesia is often influenced by the country's political economy. Even if a policy benefits the public, it cannot be implemented without political support.¹⁰

Despite legal obstacles to cryptocurrency adoption, the government must act swiftly in addressing this issue. The development of cryptocurrencies in Indonesia is significant, yet existing regulations remain unclear and unsynchronized between different agencies. Nevertheless, challenges and obstacles do not eliminate the possibility of cryptocurrency growth in Indonesia. Therefore, it is essential to encourage new players to learn about cryptocurrencies, becoming experts who can contribute to their development domestically and internationally. The potential for growth in this sector remains vast.

Education on cryptocurrency development is crucial. Educational institutions and crypto-related organizations should facilitate learning opportunities, with support from both the government and the community. Investors and traders must take the initiative to continually educate themselves and seek information on cryptocurrencies to enhance their understanding. Universities, in particular, should allocate dedicated spaces for developing digital asset trading literacy, including cryptocurrency.

It is important to ensure that everyone has the opportunity to learn about this emerging field. The government and institutions such as CoFTRA must actively participate in educating the public to prevent misinformation and promote cryptocurrency literacy. Proper education will help people understand how crypto and blockchain applications work, their benefits, and their risks. This will encourage a rational approach to cryptocurrency transactions rather than one driven by emotions or social trends. Currently, many individuals engage in crypto transactions based on prestige or peer influence without fully understanding the asset. Economic, technical, and psychological knowledge is essential for responsible participation in cryptocurrency trading.

¹⁰ Sumantoro, *Hukum Ekonomi* (Jakarta: Penerbit Universitas Indonesia, 1986).

A key concern is Indonesia's relatively low financial literacy, which often leads to digital crimes such as Ponzi schemes and other fraudulent activities related to cryptocurrency transactions. Addressing this issue through education and regulatory clarity will be crucial in ensuring a safer and more informed crypto ecosystem in Indonesia.

CONCLUSION

Cryptocurrencies are generally not legal as a means of payment in Indonesia; however, they can still be used, stored, and traded as assets by the public. Blockchain technology has indirectly facilitated digital transactions with various advantages, such as data security and transparency. In practice, blockchain technology enables diverse and rapid applications. Therefore, the government must establish regulations that can keep pace with technological advancements. When formulating regulations, the government should ensure they remain flexible (agile regulation) to avoid becoming outdated due to rapid developments. In Indonesia, crypto assets should be viewed as commodities rather than currencies, as the law recognizes Rupiah as the only legal tender.

REFERENCES

- (CIPG), Centre for Innovation Policy and Governance. *Big Data, Kecerdasan Buatan, Blockchain, Dan Teknologi Finansial Di Indonesia Usulan Desain, Prinsip, Dan Rekomendasi Kebijakan*, 2018.
- Ajwani-Ramchandani, Raji, Sandra Figueira, Rui Torres de Oliveira, Shishir Jha, Amit Ramchandani, and Louisa Schuricht. "Towards a Circular Economy for Packaging Waste by Using New Technologies: The Case of Large Multinationals in Emerging Economies." *Journal of Cleaner Production* 281 (January 2021): 125139. <https://linkinghub.elsevier.com/retrieve/pii/S0959652620351830>.
- Esmailian, Behzad, Joe Sarkis, Kemper Lewis, and Sara Behdad. "Blockchain for the Future of Sustainable Supply Chain Management in Industry 4.0." *Resources, Conservation and Recycling* 163 (December 2020): 105064. <https://linkinghub.elsevier.com/retrieve/pii/S0921344920303815>.
- Kayikci, Yasanur, Nazlican Gozacan-Chase, Abderahman Rejeb, and Kaliyan Mathiyazhagan. "Critical Success Factors for Implementing Blockchain-based Circular Supply Chain." *Business Strategy and the Environment* (April 27, 2022). <https://onlinelibrary.wiley.com/doi/10.1002/bse.3110>.
- Prima Dwi Priyatno, Isti Nuzulul Atiah. "Melirik Dinamika Cryptocurrency Dengan Pendekatan Ushul Fiqih." *JURNAL ILMIAH EKONOMI ISLAM (JIEI)* 7, no. 3 (2021).
- Schwab, Klaus. *Revolusi Industri Keempat*. Jakarta: PT. Gramedia Pustaka

Utama, 2019.

Shovkhalov, Shamil, and Hussein Idrisov. "Economic and Legal Analysis of Cryptocurrency: Scientific Views from Russia and the Muslim World." *Laws* 10, no. 2 (May 10, 2021): 32. <https://www.mdpi.com/2075-471X/10/2/32>.

Sirait, Timbo Mangaranap. "The Implementation of Procedural Law of Responsibility Enforcement of Corporate Crime in Integrated Criminal Justice System." *Jurnal Dinamika Hukum* 17, no. 3 (October 24, 2017): 342. <http://dinamikahukum.fh.unsoed.ac.id/index.php/JDH/article/view/769>.

Sumantoro. *Hukum Ekonomi*. Jakarta: Penerbit Universitas Indonesia, 1986.

Supramana. *Hukum Uang Di Indonesia*. Bekasi: Gramata Publishing, 2014.