Jurnal Dinamika Hukum
Vol. 23 Issue 2 , May 2023
E-ISSN 2407-6562 **P-ISSN** 1410-0797
National Accredited Journal, Decree No. 21/E/KPT/2018
DOI: 10.20884/1.jdh.2023.23.2.3478

CHARACTERISTICS OF CRYPTOASSET-RELATED CRIMES AND CONVERGENCE-BASED LAW ENFORCEMENT POLICIES

Peter Jeremiah Setiawan✉[1], **Jennifer**[2]
[1,2]Faculty of Law, University of Surabaya

Abstract
Crimes related to cryptoassets that develop in a complex manner give rise to distinctive characteristics and require a convergence-based countermeasure that is not only responsive but also anticipatory and futuristic. This article is examined from normative juridical research with a case and conceptual approach. It aims to study the characteristics of crimes related to cryptoassets and how to formulate convergence-based law enforcement policies in Indonesia. Law enforcement policies in tackling these crimes must have a convergence load with various technological innovations. The formation of convergence-based criminal policies cannot be separated from awareness and continuous efforts to develop the quality of human resources in digital literacy. This quality is in the mastery of technology itself and ethical behavior. This digital ethics-based legal culture should not only be aimed at the general public as a norm target (norm address) but also for law enforcement officers (rechtshandhaving).

Keywords: convergency; cryptoasset; law enforcement.

Introduction

Technological developments lead to various consequences on various aspects of human life. One form of manifestation of developing technological developments in the last ten years is cryptoassets, such as Bitcoin, Ethereum, Litecoin, Ripple, Namecoin, Swiftcoin, and many more, all based on blockchain technology. Blockchain is a database technology that distributes and records transactions provided to parties collected in a distributed database (Yulianton et al., 2018). Blockchain technology has undergone several developments to reach at least four current phases, which include (Bhattacharya et al., 2018). Blockchain 1.0 technology as the initial development of cryptocurrency currency with the type of bitcoin to Blockchain 4.0, which focuses on public ledger services and databases that distributed in real time that integrates smart contracts as a way to eliminate the need for paper-based agreements which make it easier especially in the industrial sector (Bodkhe et al., 2020). The dynamically developing application of blockchain technology has penetrated other sectors, not just

✉Corresponding Author: peterjsetiawan@staff.ubaya.ac.id

business and finance. Blockchain technology comes by simplifying the conventional transaction process through a distributed ledger withan updated and transparent copy of the blockchain. Even in government, blockchain technology can be used to increase the accountability of government organs by providing information and news to the public that can be accessed at all times. The field of intellectual property rights can also utilize blockchain technology for data and be a solution in handling disputes (B. Rawat et al., 2020).

Blockchain technology provides many impacts and conveniences across sectors but does not close the loopholes and spaces for crimes to occur. FATF studies based on the AML/CFT regime that use risk-based assessments produce important conclusions about the threats, vulnerabilities, and negative impacts of using crypto assets on the potential vulnerabilities of financial crimes, especially money laundering and terrorism financing. The rapid developments in the market, the application potential of blockchain technology, and the increasing risks arising from using crypto assets have made the mode of crime involved more complex. Crimes that occur due to the use of blockchain technology can be seen in several major cases that have occurred, such as the hacking and theft of Mt. Gox in 2014, which had to lose as much as 850,000 bitcoins or the equivalent of half a trillion US dollars (USD 450 million) as well as USD 28 million in cash in bank accounts. Cases of narcotics trafficking and Silk Road money laundering on marketplace websites as well as cases of fraud and money laundering by Alexander Vinnik. Several of these cases show that the typology of crime related to blockchain technology is a financial crime (Jung & Lee, 2017), which cannot be separated from cybercrime because it involves modes of information technology platforms and networks or other special virtual technologies.

Crimes related to cryptoassets based on blockchain technology give rise to special characteristics different from other types of financial crimes and cybercrimes. These characteristics will be described in the results of the discussion of this article. Understanding the characteristics of crimes related to cryptoassets is able to create a complete discourse on policy-making in the criminal justice system. The basis of the concept of convergence between the legal order and other aspects of life can be used as a reference in formulating anticipatory and futuristic law enforcement policies. This policy is based on the use of technology to tackle crime. However, such a policy cannot be separated from problems and obstacles at the implementation level, namely legal culture. This can hinder creating an efficient situation (Budhijanto, 2011a). Discussion regarding this matter is an important point in forming convergence-based law enforcement policies.

Legal studies regarding crimes related to cryptoassets and law enforcement on these issues are still new things in Indonesia. Research and publications related to this topic are broadly examined from the legal and regulatory perspective regarding cryptoassets in investment and security. Some examples include "Smart Contract Implementation in Blockchain Technology in Relation to Notaries as Public Officials," written by Sabrina Oktaviani and Yoni Agus, as well as Eureka I.K's writings with several other authors in the journal "Legitimacy of Blockchain-Smart Contracts in Electronic Transactions: Indonesia, America, and Singapore." Other authors, such as Hans C.K. and several other authors, are more focused on the importance of regulatory regulation regarding crytoassets in the article "The Urgency of Regulation of the Physical Market Crypto Asset (Crypto Asset) Law." Research in international journals is even earlier and more written about the problem of the characteristics of crypto asset-related crimes and convergence-based law enforcement. Danda B.R, Vijay C., and Ronald D. wrote in a journal entitled "Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems," that several countries have started converging through blockchain technology and security systems. Another journal entitled "Legal and human rights issues of AI: Gaps, challenges, and vulnerabilities," written by Rowena Rodrigues discuss human rights and legal arrangements in the use of Artificial Intelligence, a technological development also used in cryptoasset systems. Based on the research reviews mentioned above, the study in this paper will discuss something more recent and important because not much discussion has been carried out, especially in convergence-based law enforcement related to cryptoassets in Indonesia. The findings in this paper are expected to be a starting point for further research on this matter. Starting from the explanation above, the research article discusses the characteristics of crypto-asset-related crimes and how convergence-based law enforcement policies are formulated in Indonesia.

Research Problems

First, this research need to explore on, what are the characteristics of crypto-asset-related crimes?. Second, the problems that need to be answered is on what are the convergence-based law enforcement policies relating to cryptoassets in Indonesia?

Research Methods

This article was compiled from the results of normative juridical research using a case approach, a conceptual approach, and a statutory approach. The

research begins by carrying out an inventory and classifyingying legal materials relevant to the formulation of the problem. The main legal material used is literature explaining the system and how blockchain works as a basis for cryptoasset technology, followed by literature relating to cryptoasset-related crime cases, as well as an understanding of the typology of crime within the framework of criminal law science, the concept of criminal policy and legal convergence. In the analysis section, the first thing to do is review several criminal cases related to cryptoassets to formulate the characteristics of these cases. The next analysis examines a law enforcement policy prescription for crimes related to cryptoassets as a criminal policy, along with challenges related to legal culture in terms of existing regulations.

Discussion

1. Characteristics of Cryptoasset-Related Crimes

Crimes related to cryptoassets do not only occur in Indonesia but also various countries in the world to the extent that they are transnational (cross-country) and cyberspace (occurring in computer networks and devices). According to the study of some cases, crimes related to cryptoassets can be formulated in several characteristics. First, in terms of the mode and typology of crime. Cryptoasset-related crimes were committed in various modes, as explained in the following table:

No	Cases	Type of Crime
1	*Silk Road* Website Marketplace Case (2011)	Transactions of illegal goods, money laundering.
2	Sheep Website Marketplace Case (2013)	Transactions of illegal goods, theft, and money laundering.
3	Trendon Shavers Case (2011)	Fraud
4	Mt. Case Gox (2014)	Embezzlement, hacking for theft.
5	Ransomware virus case (2017-2018)	Hacking, extortion
6	Cases on Several Cryptoasset Exchanges (2015-2016)	Hacking for theft
7	BTC-e Case (2017)	Fraud, money laundering

8	The Alam Sutera Mall Bombing Case (2015)	Extortion
9	Indonesian Ransomware Case (2019)	Hacking, extortion
10	Case of Surabaya Black Hat (2017)	Hacking, extortion

Based on the modes used in cryptoasset-related crimes, six major groups of crime modes can be identified, namely (1) transactions or trade in illegal goods and services, (2) fraud and embezzlement, (3) extortion, (4) theft (5) money laundering. (6) hacking. In the illegal goods transaction mode of the *Silk Road* and *Sheep* cases, cryptoassets are used as payment instruments in a virtual market that trades various illegal goods and services, especially narcotics and illegal drugs, arms trade, stolen identity information, and others from various countries. This virtual market is on a website intentionally hidden under the dark web category. The dark web is at the deepest level of the internet layer, preceded by the surface and deep web (Finklea, 2017). This website is not indexed by web search engines (Google, Bing, yahoo), cannot be accessed using a standard browser, and is created and used by people who choose anonymity (without a real identity). Dark webs such as *Silk Road* and *Sheep* can only be accessed using a browser or special software such as TOR (The Onion Routing) and certain passwords or authorization (Beshiri & Susuri, 2019). The dark web is identified as the center of crime because its anonymity is considered a 'gate' for perpetrators to start their crimes (Naseem et al., 2016). The way perpetrators use the dark web as a means of virtual markets can certainly be understood in line with their use of cryptoassets. Cryptoassets based on blockchain technology that is created can also accommodate similar features. Regarding the modes of fraud, embezzlement, extortion, and money laundering, the selection of cryptoassets in crime is not solely as a target or result of crime but also as an instrument or means to commit a crime.

In the Trendon Shavers case, cryptoassets were used as investment instruments for Ponzi scheme fraud. In the Alam Sutera Mall bombing terrorism case and the Surabaya Black Hat case, cryptoassets were used as extortion transaction instrument. In contrast, in the BTC-e case, Alexander Vinnik as the perpetrator, used the cryptoasset exchange platform as the main instrument of money laundering, namely the instrument for collecting and transferring various forms of crime proceeds. In crimes with these modes, cryptoassets are chosen as instruments or means to facilitate a crime that is primarily aimed at illegally obtaining or enjoying financial benefits, previously mentioned, the use of

cryptoassets as instruments to facilitate enable crime is inseparable from the characteristics of cryptoassets.

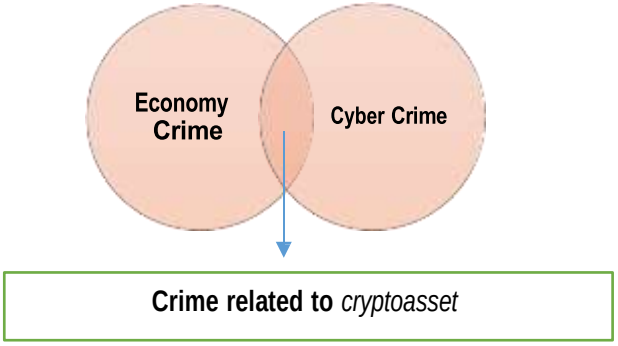
The type of transaction of illegal goods or services, fraud, extortion, and money laundering, from the perspective of crime typology, is certainly a financial crime, or some opinions also call it an economic crime, namely acts against the law that aims to gain profit. certain financial or professional consequences for the perpetrator, while for the victim, it results in financial costs or losses (Saddiq & Abu Bakar, 2019). Whatever the modus operandi of the perpetrators, these cryptoasset-related crimes inevitably lead to a malicious will (guilty mind) to gain illegal financial gain, whether using cryptoassets as a means of transaction such as in the case of *Sheep* or *Silk Road* Web Marketplace or using cryptoassets as objects of hacking. (theft) as in the case of the Mt. Gox or cryptoasset exchanges Bitstamp, Bitfinex, Shapeshift. These financial crimes involve cryptoassets which, when converted into fiat currency, have a large amount of value, for example, the loss in the Trendon Shavers case, which reached USD 1.2 million, or the value of cryptoasset transactions on the *Silk Road* Web Marketplace, which reached USD 1.2 billion. The high value of this loss or transaction positively correlates with the particularity of blockchain as a cryptoasset transaction technology.

Blockchain technology results in faster and easier acceleration of financial transactions compared to conventional transactions involving banks or financial institutions (Chan et al., 2017). The next mode that is important to explain is related to hacking. This mode is primarily aimed at illegally entering certain electronic systems to commit the following mode of crime. In cryptoasset-related crimes, this hacking mode is followed by extortion, theft, and theft modes. In extortion mode, the perpetrator hacks by giving certain viruses to destroy certain electronic systems, forcing the victim to pay a sum of money in the form of cryptoassets. In the theft mode, the perpetrator hacks by illegally entering the cryptoasset electronic system belonging to a certain entity and taking the cryptoasset in it. The hacking mode is closely related to cybercrime, as illegal acts that use information and communication technology (data, systems, electronic networks, websites, and others), both as targets of acts and as instruments of these illegal acts(*UNODC Teaching Module Series on Cybercrime*, n.d.).

Cryptoassets as a financial transaction system (Prisco, 2018) use the basis of blockchain technology, namely information technology based on its distinctive features, including information storage on decentralized/distributed computer networks (distributed ledger technology), direct networks between entities, use of cryptographic protocols and algorithm consensus (Xu et al., 2019).

Crimes based on such technology are certainly within the scope of cybercrime. Regarding the division of types of cybercrime, Europol (2018) divides it into two classifications based on the role of information and communication technology, namely cyber-dependent crime and cyber-enabled crime. Cyber-dependent crime can only be committed using a computer, computer network, or other forms of information technology, which negatively impacts three aspects, namely confidentiality, integrity, and availability. Data and computer systems are the CIA Triad (Andress & Winterfeld, 2014) (Qadir & Quadri, 2016). Meanwhile, related to cyber-enabled crime is a conventional crime facilitated by information and communication technology. In this crime, information and communication technology does not act as a target butas part of the modus operandi that makes the crime have a wider reach. These crimes are identified as existing crimes or traditional crimes, which involve technology as an instrument that facilitates the perpetrators of committing crimes. These crimes include computer-related offenses and content-related offenses (*UNODC Teaching Module Series on Cybercrime*, n.d.) (Clough, 2010).

Referring to this classification, the crime related to cryptoassets moves either in the form of cyber-dependent or cyber-enabled crime. Hacking of electronic systems, including cryotoasset systems, as in the Mt Gox case or the cases of several cryptoasset exchanges, in this case, is included in the category of cyber-dependent crime because the perpetrator's actions harm confidentiality, integrity, and data availability of an electronic system. However, in terms of the main objectives (ulterior motives) of these crimes, in fact, all modes of crime related to cryotoassets are on the spectrum of cyber-enabled crime. All of the modes carried out aim to gain financial gain illegally. These crimes, such as illegal goods transactions, fraud, and extortion, are conventional crimes (existing crimes). However, with cryptoassets as instruments or means, crimes become easier to commit, and the range of these crimes becomes wider, both in terms of *locus delicti* and victims. The description of characteristics related to the mode and typology of crime shows that crimes related to cryptoassets are at a convergence between financial crimes and cyber-office. Crimes related to cryptoassets are financial crimes whose modes are aimed at obtaining financial benefits unlawfully. In contrast, crimes related to cryptoassets are called cybercrimes because of the use of blockchain-based technology as information technology. The two typologies form a convergence scheme for cryptoasset-related crimes as follows:



In addition, the description of the characteristics shows that the modes related to these crimes do not only standalone but are often carried out simultaneously, in tandem, or continue with one another. For example, in the case of MT Gox, the mode of hacking carried out on the cryptoasset exchange platform is aimed at stealing or stealing a number of cryptoassets. In this case,, the perpetrators' modus operandi, was not only illegal access to Mt. Gox but also illegal data collection of various cryptoassets belonging to many people stored at Mt. Gox. Not only that, Mark Karpeles as the owner of Mt Gox, also embezzled many people's cryptoassets on his platform. Another example is in the BTC-e case, the perpetrator in the case provided BTC-e as a crytoasset exchange platform that could be used by criminals as a means of laundering money from the proceeds of various crimes, ranging from the proceeds of hacking, proceeds from illegal goods transactions, proceeds of fraud to other proceeds of money laundering. Money laundering in various cases of crime related to cryptoassets shows a mode of crime that cannot stand alone. This is because money laundering is a follow-up or continuation of the main crime.

The second characteristic is related to the subject of the crime. As previously explained, the modes of crime related to cryptoassets are more related to financial crimes. Such crimes are also often identified as white-collar crimes (Jung & Lee, 2017) or non-violent crimes where the perpetrators have qualified knowledge up to a certain professional background (Marriott, 2020). Perpetrators with such knowledge certainly do not come from disadvantaged social or economic backgrounds (Marriott, 2020). Criminals related to cryptoassets have at least certain knowledge and skills in utilizing cryptoasset transaction technology. Based on the cryptoasset transaction scheme, criminals related to cryptoassets are described as not only parties who solely carry out cryptoasset transactions but also third parties who provide services related to cryptoasset transactions, such as cryptoasset exchange service providers, virtual wallet providers, providers of cryptocurrency payment processing services to cryptoasset ATM providers.

A complete description of criminals related to cryptoassets can be shown in the following table:

No	Cases	Perpetrator Description
1	*Silk Road* Website Marketplace Case (2011)	Illegal marketplace owners and users who carry out crypto-asset transactions.
2	*Sheep* Website Marketplace Case (2013)	Illegal marketplace owners and users who carry out cryptoasset transactions.
3	Trendon Shavers Case (2011)	Illegal investment business perpetrators are conducting cryptoasset transactions.
4	Mt. Case Gox (2014)	Parties that provide services or carry out business related to cryptoassets and individual or group hackers who carry out cryptoasset transactions.
5	Ransomware virus case (2017-2018)	Individual or group hackers are conducting cryptoasset transactions.
6	Cases on Several Cryptoasset Exchanges (2015-2016)	Individual or group hackers who carry out cryptoasset transactions.
7	BTC-e Case (2017)	Parties that provide services or carry out business related to cryptoassets
8	The Alam Sutera Mall Bombing Case (2015)	Individual or group hackers who carry out cryptoasset transactions.
9	Indonesian Ransomware Case (2019)	Individual or group hackers who carry out cryptoasset transactions.
10	Case of Surabaya Black Hat (2017)	Individual or group hackers who carry out cryptoasset transactions.

Related to the perpetrators' motives in committing crimes, the previous explanation of the mode of financial crime has affirmed the existence of ulterior motives to gain illegal financial gain. The main motive or purpose is basically

supported by various perpetrators positively correlated with cryptoasset transactions' characteristics. The standard anti-money laundering perspective has emphasized various characteristics of cryptoasset transactions as vulnerabilities that constitute the risk of committing a crime. The characteristics of cryptoasset transactions that show these vulnerabilities include(*Financial Action Task Force, Guidance for a Risk-Based Approach to Virtual Currencies*, n.d.): (1) Cryptoasset system allows entities to carry out transactions in a pseudo-anonymous state (pseudonymity or pseudonymous). This situation means that funding transactions, transfers, or any financial transactions are carried out without using the identity of the actual source; (2) The cryptoasset system can be operated without having certain supervisors or devices to monitor, identify and record financial transactions with unusual or suspicious (potentially criminal) patterns; (3) The cryptoasset system has a broad reach, cross borders, and various jurisdictions because this system can be accessed anywhere as long as there is internet access; (4) The cryptoasset system continues to grow rapidly, starting in terms of technological development (blockchain phase 1.0 to 4.0 and will probably continue to grow), the development of business models and services that use cryptoassets, the quantity of cryptoasset types, to the number of their users. Do not rule out the possibility that these cryptoasset developments strengthen various vulnerabilities. These characteristics influence criminals to choose cryptoassets as financial crime instruments. These characteristics do not only make it easier or help the perpetrators to commit crimes and enjoy the proceeds of their crimes but also make it complicated for law enforcement to track, examine and punish the perpetrators.

The third characteristic is related to where the crime related to cryptoassets or *locus delicti* was committed). Crimes related to cryptoassets have been identified as cyber crimes. Cybercrime is postulated to be in cyberspace, namely a special place in computer systems and networks that goes beyond the rules and boundaries of geographic locations (Clough, 2010). In crimes that occur in cyberspace, perpetrators and victims, including devices (tools), do not have to be in the same physical geographic location. Perpetrators and devices used, as well as victims of crime, can be anywhere as long as they are connected to a computer network (internet).

Furthermore, perpetrators can manipulate internet protocol addresses so that perpetrators and devices are identified as if they were in a different place from the real place. In addition, determining locus delicti in crimes related to cryptoassets can be associated with various theories that produce different

determining *locus delicti* crimes related to cryptoassets. These can be associated with various theories that produce different *locus delicti* answers. Several theories can be used to determine the *locus delicti* of crime in cyberspace, including the uploader and downloader theory and the server law theory, from the theory of international space as expressed by Darrel Menthe.

In addition, some theories conventionally can be applied, including the theory of material action, the theory of tools, and the theory of consequences. Each country has sovereignty in determining which theory is applied to its jurisdiction. Determination of different *locus delicti* will have implications for different jurisdictions, namely, which country's regulations apply to the crime, including the country that has the authority to enforce the law against the crime.

For example, in the case of the *Sheep* marketplace website, Czech criminals created websites and made illegal transactions in the Czech Republic. At the same time, other perpetrators also carried out illegal transactions in various countries, including the United States. Perpetrators from the United States even stolen cryptoassets (exit scam) on the website. Thus, the *locus* of these crimes is in the Czech Republic, the United States, and many other countries. The state that determines its territory as the *locus delicti* of the crime will claim the authority to enforce its rules and justice system. Therefore, crimes related to cryptoassets that occur in cyberspace, mostly have *locus delicti* and jurisdictions that vary or are not only located in one country.

2. **Law Enforcement Based on Convergency**

Indonesia's criminal policies, especially related to law enforcement, still rely on conventional methods, which are inefficient, merely responsive, and ultimately not convergent with existing technological updates. For example, in the regulation of electronic evidence in various laws in Indonesia, the Indonesian ITE Law already stipulates that electronic information or data or their printed output is valid legal evidence. This arrangement is then not understood convergently at the practice level, creating ambiguity. Several examinations of cases place electronic information or data as evidence, while several examinations of criminal cases place electronic information or data as evidence. In addition, the presentation of electronic information or data as evidence in court is not accompanied by a chain of custody architecture as a form of verification of its authenticity, integrity, and availability according to the mandate of the ITE Law itself.

The formulation of criminal policy requires a convergence basis that focuses on maintaining the rule of law against any events that may occur in the future. This policy interacts with various resources synergistically to produce a new state of efficiency (Kim et al., 2014). Such a criminal policy should not only operate on a responsive spectrum or only respond to developments in crime modes. Reasonable efforts built by legislators and law enforcers in tackling crime should have an anticipatory and futuristic understanding (Barda Nawawi, 2008, quoted from Marc Ancel, 1965) and be truly efficient and optimal in preventing or resolving problems that occur (Budhijanto, 2011b). In this case, existing criminal policies should also be able to utilize blockchain technology in later generations as a form of payload. The legal order in criminal policy must be able to collaborate functionally and optimally with systems or principles for the use of technology. Some examples of criminal policies that have convergence content with technological innovation, including with blockchain technology itself in preventing and eradicating crimes related to cryptoasset technology, include:

1. Data Storage of the Criminal Justice System Using the Blockchain System. Efforts to modernize and digitize the justice system in various forms require all information and documents in the justice system to be stored and/or converted into digital format. In the criminal justice system in Indonesia, modernization and digitization of the justice system have also been carried out, starting from an electronic-based case tracing system and e-court system, to online trial cases (Perma No. 4 of 2020). Digital information and documents as sensitive information, which are produced from various processes of the justice system, indeed cannot be separated from various risks of crime, both in the form of illegal access and interception, interference, and theft (illegal data processing) to falsification (data forgery). Some sensitive information in the criminal justice system includes a person's criminal record, documentary evidence, results of investigations by law enforcement officials, and decisions. Blockchain, in this case, can be used as a basis of choice in building a management system for storing and communicating data on the criminal justice system in Indonesia. Compared to conventional centralized data storage systems, the use of blockchain can improve system security and reduce any access that aims to damage the integrity and validity of data. Data related to the criminal justice system will be stored not in one database (centralized server), but on every computer of all network members.

Furthermore, the data is locked with cryptographic protocols, hash functions, asymmetric encryption, use of keys, and so on. In this case, there is no single point for the entire database to attack, so it's difficult to compromise or steal all the data simultaneously. The blockchain system ensures that no one party can control the peer-to-peer network. In the blockchain system, problems with hardware and software damage problems will not affect the data's integrity. Data communication between law enforcement officials using this system also becomes easier and more efficient because each agency no longer requires a separate database. It even reduces corrupt behavior that affects the decisions of law enforcement officials due to possible changes or destruction of data (Tasnim et al., 2018).

2. Disclosure and Examination of Crimes Using the Blockchain System. The blockchain system used in cryptoasset transactions allows an entity to conduct transactions under pseudo-anonymous conditions. This condition is emphasized repeatedly as a risk perpetrator for committing crimes because it makes it difficult to trace the perpetrator's identity and the actual transaction's purpose (*Financial Action Task Force, Guidance for a Risk-Based Approach to Virtual Currencies*, n.d.). Even so, technological innovation, even with the help of the blockchain system itself, also gave birth to progressive ways of tracking crimes according to the follow-the-money principle, making it possible to follow the suspect. Some of these methods include (1) Bitcoin Analysis. Investigations into illegal Bitcoin use can be forensically reconstructed. This system identifies ownership once any suspicious activity occurs. This requires collecting targeted Bitcoin addresses or transaction IDs to study and train the model for prediction, investigation, and future analysis. This method can identify the mapping between Bitcoin addresses and similar users. There is also the potential to discover relationships between Bitcoin addresses, IP addresses, and spending patterns through this analysis (Reid & Harrigan, 2013) (2) Graph Analysis. This analysis is formed by transactions and addresses in the Bitcoin network to divide the entire Bitcoin graph into smaller graphs. (Reid & Harrigan, 2013). Breaking the Bitcoin system down into charts allows mapping behavior such as user transaction habits and Bitcoin transactions over time, including suspicious behavior or other prohibited transaction scenarios on the Bitcoin network. In 2014, Spagnuolo provided forensic analysis of illegal Bitcoin transactions and

went on to develop automated chart analysis and software called Bitiodine. This software is used to parse the Bitcoin blockchain for transactions and addresses and then augment it with different data fetched from the web to the cluster, visualizing graphs of Bitcoin transactions. Actual use of the Bitiodine application in the cryptolocker ransomware investigation case to detect the malware author's cryptoLocker cluster, and calculate some statistics of ransoms paid by victims. (Spagnuolo et al., 2014) (3) Analysis through Machines. This method relates to how the machine performs its tasks (Richert & Coelho, 2015). Artificial Intelligence has developed rapidly and can help analyses that need to be time-consuming for large amounts of data. The ability to apply high-performance computing to large amounts of data in the Bitcoin ecosystem provides efficiency in analysis. Currently, several companies have actively developed blockchain solutions to combat money laundering. Some of them are successfully used in analytics and risk monitoring for cryptoasset transactions. Blockchain analytics startup Coinfirm has developed a platform that enables tracking suspicious transactions and countering the financing of terrorism using more than 270 risk indicators.

3. Proof Verification Using Blockchain. After the crime has been uncovered, the examination process relies on proving that the perpetrator and his crime can be proven to have violated certain criminal law provisions. The process of verifying proof of crimes related to cryptoassets that can be carried out is one of them with a blockchain-based chain of custody (B-CoC) architecture. This choice has been driven by the authentication requirements of the CoC process, which does not allow unauthorized and untrusted parties to manage digital evidence and reside in a network. future work, experts in this field are investigating how it is possible to manage a dynamic set of validators. Also, studying possible alternatives to increase the validator's privacy level does not change dependencies and other security attributes (Bonomi et al., 2018)
4. Confiscation and confiscation of money/cryptoassets related to crime. In every cryptocurrency/asset transaction, the cryptoasset wallet acts as a medium for storing and sending money/crypto assets. Law enforcement officials must own and manage cryptoasset wallets. According to its characteristics, cryptocurrency/assets have high transfer flexibility. Even if the criminal has been arrested and his

> electronic equipment has been confiscated, other related perpetrators can use the private key to move cryptoassets in certain wallets anywhere and anytime (timeless and borderless characteristics). Therefore, crypto money/assets identified as proceeds or media of crime must be confiscated as evidence as soon as possible by transferring them to a wallet created and managed by law enforcement officials. Besides that, if based on a criminal court decision

Forming a law enforcement policy as a convergence-based criminal policy is, of course, carried out not without prerequisites to forming a law enforcement policy as a convergence-based criminal policy is carried out not without prerequisites to resolve various challenges. The challenge or obstacle that always exists in convergence is what Pierre Legrand calls legal culture. The operation of law in a society cannot be separated from the legal culture, which is part of a legal system (Roper & Friedman, 1976). Legal culture is a response that accepts or rejects a legal event. This shows the attitude of human behavior toward legal issues and legal events carried into society (Rahardjo, 2014). Two problems with measuring the convergence of legal systems focus on the following propositions. First, the binding force of the rule of law is a more complicated notion than appears to be the rule that embodies the entire culture of a society. The rule of law is only an outward manifestation of the implicit structure of behavior and references (examples) that exist and develop in that society.

The rules that are made show a certain legal culture. This applies to all rules, even the most innocuous ones, such as "meta-rules", i.e., rules developed by a legal system to help manage the body of rules that develop within that system (Legrand, 1996). Second, rules are not the whole law. The conception of law as a separate subsystem of rules in society, which operates independently of society, must be abandoned. The law cannot be separated analytically from "non-law." The reality of society because the two worlds are interrelated. Law is part of the social subsystem (Legrand, 1996).

Based on this proposition, the formation of convergence-based criminal policies cannot be separated from awareness and continuous efforts to train and develop the quality of human resources in mastering technology or digital literacy. This quality is translated into obedience to written rules and ethical behavior. In this digital literacy process, the ethics that are instilled are not only contemporary but also ethics based on the cultural values of a country itself (Kusumastuti et al., 2021). Consistent inculcation of ethics can provide a foundation for the formation of convergence-based criminal policies, which is

solely oriented towards the common good and human values(Kusumastuti et al., 2021). This digital ethics-based legal culture should not only be aimed at society in general as a target norm but also at law enforcement officers (rechtshandhaving). In addition, law enforcement policies as convergence-based criminal policies cannot independently exclude other scientific contributions. Multidisciplinary studies, especially based on information technology, are needed to formulate appropriate and adaptive policies. This understanding aligns with the thoughts of G. Peter Hoefnagels (1973) that the formulation of criminal policy is a series of processes that begin with the support of various theories from scientific disciplines and allied sciences before giving birth to general criminology.

Mochtar Kusumaatmadja thinks that problems in a developing society that must be regulated by law can be broadly divided into two groups, namely: (a) problems that directly concern a person's personal life and are closely related to the cultural and spiritual life of society; and (b) issues related to society and progress are generally "neutral" from a cultural point of view (Kusumaatmadja, 1976). Legislation products that are effective in their application require attention to the institutions and procedures needed in their implementation. Because the notion of good law should not only view the law as a set of rules and principles that govern human life in society but also include the institutions and processes needed to realize the law in real life (Kusumaatmadja, 2006). Most Indonesian people do not trust institutions and law enforcement because of legal issues that have not been effectively handled (Rahardjo, 2010). Distrust in the legal system and legal apparatus in Indonesia is very concerning. This tendency does not only occur in judicial institutions but also in all social strata (Manullang, 2007). In forming legal regulations by political institutions, the role of political forces sitting in political institutions is very decisive. In Indonesia, there is still political domination of the formulation of legal products so that there is no balance between law and political requirements with political interests in their formulation so that the resulting quality does not touch or even answer problems that arise in society because the purpose of making legal products is for the interests of those concerned (Salam, 2015). The condition of Indonesia's legal culture in the form of a deficit of trust in the legal system is a challenge in implementing new systems, such as the blockchain system in the Indonesian justice system. The many cases regarding cryptocassets are cause for concern, not dispelling the negative perspectives on the blockchain system and everything related. Even though the blockchain system can offer many new things and efficiencies in the Indonesian justice system, the government and other parties

who support updating the system still need a long time, understanding, and research to be able to implement this system in the Indonesian justice system and gain public trust in the blockchain system.

Conclusion

Based on the analysis that has been done, crimes related to cryptoassets can be formulated in several characteristics. First, the description of the modes of crime related to cryptoassets shows that this crime is a convergence between financial crime and cybercrime. Crimes related to cryptoassets are referred to as financial crimes whose modes are aimed at obtaining financial benefits unlawfully, while crimes related to cryptoassets are called cybercrimes because of the use of blockchain-based technology as information technology. Second, criminals related to cryptoassets are not only described as parties who solely carry out cryptoasset transactions but also third parties who provide services related to cryptoasset transactions, such as cryptoasset exchange service providers (exchangers), virtual wallet providers, and virtual wallet providers. cryptocurrency payment processing services to cryptoasset ATM providers. Third, crimes related to cryptoassets occur in cyberspace, most of which have locus delicti and jurisdictions that are diverse or not only in one country.

Criminal policies tackling cryptoasset-related crimes must converge with various technological innovations, including blockchain technology. The legal order in criminal policy must be able to collaborate functionally and optimally with systems or principles for the use of technology. Some examples of law enforcement policies that have convergence content with technological innovation, including with blockchain technology itself in preventing and eradicating crimes related to cryptoasset technology, include: (1) Criminal Justice System Data Storage Using the Blockchain System (2) Disclosure and Examination Crimes Using the Blockchain System, including using bitcoin analysis, graphical analysis and engine analysis. (3) Verify proof of cryptoassets using the Chain of Custody architecture (4) Confiscation and confiscation of money/crypto assets related to crime.

Suggestion

The formation of convergence-based criminal policies cannot be separated from awareness and continuous efforts to train and develop the quality of human resources in mastering technology or digital literacy. This quality is translated into obedience to written rules and ethical behavior. In this digital literacy

process, the ethics that are instilled are not only contemporary in nature, but also ethics based on the cultural values of a country itself. Consistent inculcation of ethics can provide a foundation for the formation of convergence-based criminal policies, which is solely oriented towards the common good and the value of humanism. This digital ethics-based legal culture should not only be aimed at society in general as a target norm (norm address), but also law enforcement officers *(rechtshandhaving)*. In addition, forming law enforcement policies as convergence-based criminal policies cannot independently exclude other scientific contributions. Multidisciplinary studies, especially based on information technology, are needed to formulate appropriate and adaptive policies.

References

Andress, J., & Winterfeld, S. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition. In *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition*.

B. Rawat, D., Chaudhary, V., & Doku, R. (2020). Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems. *Journal of Cybersecurity and Privacy*. https://doi.org/10.3390/jcp1010002

Beshiri, A. S., & Susuri, A. (2019). Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. *Journal of Computer and Communications*. https://doi.org/10.4236/jcc.2019.73004

Bhattacharya, P., Singh, A., Srivastava, A., & Mathur, A. (2018). A Systematic Review on Evolution of Blockchain Generations ITEE Journal A Systematic Review on Evolution of Blockchain Generations. In *International Journal of Information Technology and Electrical Engineering ITEE*.

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A Comprehensive Review. *IEEE Access*, *8*, 79764–79800. https://doi.org/10.1109/ACCESS.2020.2988579

Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-CoC: A blockchain-based chain of custody for evidences management in digital forensics. *In the Proceeding of International Conference on Blockchain Economics, Security and Protocols*.

Budhijanto, D. (2011a). Pembentukan Hukum yang Antisipatif Terhadap Perkembangan Zaman dalam Dimensi Konvergensi Teknologi Informasi dan Komunikasi. *Jurnal Ilmu Hukum*.

Budhijanto, D. (2011b). Pembentukan Hukum yang Antisipatif Terhadap Perkembangan Zaman Dalam Dimensi Konvergensi Teknologi Informasi dan Komunikasi. *Jurnal Ilmu Hukum*, *14*(2), 225.

Chan, S., Chu, J., Nadarajah, S., & Osterrieder, J. (2017). A Statistical Analysis of Cryptocurrencies. *Journal of Risk and Financial Management*. https://doi.org/10.3390/jrfm10020012

Clough, J. (2010). Principles of Cybercrime by Jonathan Clough. *Cambridge Core*.

Financial Action Task Force, Guidance for a Risk-Based Approach to Virtual Currencies. (n.d.). https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-rba-virtual-currencies.html

Finklea, K. (2017). *Dark Web*. Congressional Research Service.

Jung, J., & Lee, J. (2017). Contemporary Financial Crime. *Journal of Public Administration and Governance*. https://doi.org/10.5296/jpag.v7i2.11219

Kim, E., Kim, J., & Koh, J. (2014). Convergence in Information and Communication Technology (ICT) Using Patent Analysis. *Journal of Information Systems and Technology Management*. https://doi.org/10.4301/s1807-17752014000100004

Kusumaatmadja, M. (1976). *Hukum dan Masyarakat dan Pembinaan Hukum Nasional*. Penerbit Binacipta.

Kusumaatmadja, M. (2006). *Konsep-Konsep Hukum dalam Pembangunan*. Penerbit PT Alumni.

Kusumastuti, F., Kurnia, N., Astuti, S. I., Birowo, M. A., Hartanti, L. E. P., Amanda, N. M. R., & Kurnia, N. (2021). Modul Etis Bermedia Digital. In *Modul Etis Bermedia Digital*.

Legrand, P. (1996). European legal systems are not converging. *International and Comparative Law Quarterly*. https://doi.org/10.1017/S0020589300058656

Manullang, E. F. M. (2007). *Menggapai Hukum Berkeadilan Tinjauan Hukum Kodrat dan Antinomi Nilai*. PT Kompas Media Nusantara.

Marriott, L. (2020). White-Collar Crime: The Privileging of Serious Financial Fraud in New Zealand. *Social & Legal Studies*, *29*(4), 486–506. https://doi.org/10.1177/0964663919883367

Naseem, I., Kashyap, A. K., & Mandloi, D. (2016). Exploring Anonymous Depths of Invisible Web and the Digi-Underworld. *International Journal of Computer Applications*.

Prisco, G. (2018). *What the fork happened to Bitcoin price?* https://medium.com/chainrift-research/what-the-fork-happened-to-bitcoin-price-428cfaaodeeb.

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*. https://doi.org/10.4236/jis.2016.73014

Rahardjo, S. (2010). *Pemanfaatan Ilmu-Ilmu Sosial Bagi Pengembangan Ilmu Hukum*. Genta Publishing.

Rahardjo, S. (2014). *Ilmu Hukum*. PT Citra Aditya.

Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and Privacy in Social Networks*. https://doi.org/10.1007/978-1-4614-4139-7_10

Richert, W., & Coelho, L. P. (2015). Building Machine Learning Systems with Python, Second Edition. In *Book*. https://doi.org/10.1007/s13398-014-0173-7.2

Roper, D. M., & Friedman, L. M. (1976). The Legal System: A Social Science Perspective. *Political Science Quarterly*. https://doi.org/10.2307/2148447

Saddiq, S. A., & Abu Bakar, A. S. (2019). Impact of economic and financial crimes on economic growth in emerging and developing countries. *Journal of Financial Crime*, *26*(3), 910–920. https://doi.org/10.1108/JFC-10-2018-0112

Salam, A. (2015). Pengaruh Politik dalam Pembentukan Hukum di Indonesia. *Mazahib Jurnal Pemikiran Hukum Islam*, *14*(2), 119–131. https://doi.org/https://doi.org/10.21093/mj.v14i2.341

Spagnuolo, M., Maggi, F., & Zanero, S. (2014). Bitiodine: Extracting intelligence from the bitcoin network. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-662-45472-5_29

Tasnim, M. A., Omar, A. Al, Rahman, M. S., & Bhuiyan, M. Z. A. (2018). CRAB: Blockchain based criminal record management system. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-030-05345-1_25

UNODC Teaching Module Series on Cybercrime. (n.d.). https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-1/index.html

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. In *Financial Innovation*. https://doi.org/10.1186/s40854-019-0147-z

Yulianton, H., Santi, R. C. N., Hadiono, K., & Mulyani, S. (2018). Implementasi Sederhana Blockchain. *Sintak*.