Prosecutorial Discretion in Tackling the Cryptocurrency Crime in Indonesia

Priyambudi
Head of Administration of the South Sulawesi High Prosecutors Office & The Law Doctoral Program, Diponegoro University, Semarang, Indonesia.
E-mail: budi_jpu@yahoo.co.id

Henry Dianto Pardamean Sinaga*
Staff of the Directorate General of Taxes & Student of the Law Doctoral Program, Diponegoro University, Semarang, Indonesia.
E-mail: sinagahenrydp@gmail.com

Received March 10, 2021; Accepted July 06, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18I2/WEB18308

Abstract

Data, reports, and information show that cryptocurrency has supported certain parties as a convenience, whereas the purpose of cryptocurrency is to minimize the weaknesses of conventional money systems in international relations in the current era of globalization. Countries that cannot represent or apply autonomous law in facing cryptocurrency challenges, because it is feared it is increasingly difficult to overcome global cryptocurrency crime. It is precisely in eradicating cryptocurrency crime, law enforcement authorities, priorities of prosecutors who have the highest supremacy in the field of prosecution and other discretion in law enforcement must be dynamic in law enforcement against facilitators from responses to social needs and aspirations, in accordance with legal considerations must acknowledge the wishes of the community and agree in achieving substantive justice. Considering that virtual currency has been banned in Indonesia but crypto-asset trading on the futures exchange has been in force, responsive discretionary prosecutions are needed in combating cryptocurrency crime in Indonesia. Liability that exceeds liability based on faults, namely strict liability, vicarious liability, and secondary liability to any parties that cause cryptocurrency crime can be applied to the mechanism of "follow the money" and "trace the information and communication technologies (ICTs) footprint". It is hoped that prosecution discretion by the prosecutor can reach to the monitoring of suspicious "nodes" and monitoring the registration of ICTs that are vulnerable to cryptocurrency crimes, such as laptops, cellphones, computers, and SIM cards, in providing a deterrent effect to the perpetrators of cryptocurrency crime.

Keywords

Cryptocurrency Crime, Responsive Law, Prosecutorial Discretion, Legal Liability.

Introduction

The rise and development of cryptocurrency (which until now there have been around 1300 cryptocurrency in the world, such as Bitcoin, Ethereum, Ripple, and Cardano) must be wary of countries with legal basis considering that their use is often used by certain parties as a means of carrying out the crime (Prasetyo, 2019) and considering many cases of data theft, malware, hacking, and cracking can be dangerous for the cryptocurrency ecosystem (Cheng, 2019). Various data, reports, and information have shown that cryptocurrency crime has led to an extraordinary crime. CipherTrace (2019) reports that the use of cryptocurrency by terrorists is not new, in fact, terrorists have developed new, more sophisticated ways to obscure the flow of funds. CipherTrace (2019) released total fraud and theft related to cryptocurrency up to the third quarter of 2019 reaching the US $ 4.4 billion, not counting the two major and still mysterious frauds that occurred before 2019, namely QuadrigaCX (amounting to the US $ 192 million) and PlusToken (in the amount of US $ 2.9 billion). In 2016, Dutch prosecutors arrested 10 people suspected of using digital currency Bitcoin to launder money from drug transactions in the "Dark Web" online market of up to 20 million euros (or about $ 22 million) (Sterling, 2016), and in 2018, unknown location hackers account managed to get cryptocurrency worth 58 billion yen (about US $ 533 million) from the Tokyo-based exchange, Coincheck Inc. (Kelly & Wilkes, 2018). In Indonesia, according to a press conference Indonesian Financial Transaction Reports and Analysis Center (Center for Reporting and Analysis of Financial Transactions, hereinafter referred to PPATK) on January 9, 2017, stated that one of the payment systems to fund terrorist activities that occur in Indonesia is through Bitcoin (Tisnadibrata, 2017). Then, a study conducted by Group-IB concluded that the United States is responsible for more than half of all global cryptocurrency crimes, followed by the Netherlands at 21.5%, Ukraine at 4.3%, the Russian Federation at 3.2%, France by 2.6%, and Germany by 1.3% (Thompson, 2016). This cryptocurrency crime always undergoes a transformation from time to time, such as some users who lose virtual currency units due to theft or hacking or suffer losses when a fraudulent exchange occurs, wallet providers lose electronic purses provided to individuals, and criminals who can wash the results crimes because they can store/transfer cryptocurrency virtual currencies anonymously, globally, quickly and irrevocably, or criminals/terrorists use virtual currency delivery systems and accounts for the purpose of financing their crimes (Raymaekers, 2015).

Some data, reports, and information that have been stated show that cryptocurrency crime is a cross-border crime. Of course, in eradicating transnational crimes, it does not only involve exchanging information considering that there is potentially a huge problem, as Nykodim & Taylor (2004) warned that the very strengths of global cybercrime than the very weaknesses of the state's efforts to control it, including difficulties handling cross-border crime where the crime is just pressing a button on a computer or android, then for a moment some of the crimes that cross many countries have immediately occurred (Nykodym & Taylor, 2004). The severity of this problem requires a very hard effort from law enforcement to eradicate the crime, especially prosecutors who must successfully prosecute, develop cases, and carry out executions of the perpetrators of these crimes.

Research on cryptocurrency crimes in Indonesia has not been carried out by many previous researchers. Therefore, the research conducted by this writer is something new and can add to the development of science. This is the background of the paper that tries to answer the two main problems that are summarized. First, how are cryptocurrency crime settings in Indonesia? Second, how is the discretion of the prosecutors who are responsive in combating cryptocurrency crime in Indonesia?.

Literature Review

There are several studies of cryptocurrency phenomena that enrich the literature in this study. One of the results of Drozd's study, Lazur and Serbin (2017) concluded that criminal liability in cryptocurrency is very possible to deal with fraud or attempts to legalize money laundering from proceeds of crime, where one of the ways can be done through making appropriate qualifications of criminal violations related to cryptocurrencies, such as criminal liability against cryptocurrency market participants who do not have a license or license. This was stated by Drozd, Lazur, & Serbin (2017) considering that in Ukraine, its civil norms cannot apply its actions or violations to take civil responsibility in relation to the complexity of the application of civil liability to aspects, such as the possibility of contractual and non-contractual obligations. contractual without regulation on specific violations, the need to prove their claims in court due to forms of protection of rights that do not exist, and the complexity of collecting the relevant evidence base to be brought to court because all transactions with cryptocurrency are carried out electronically and anonymously. Then, Engle (2016) concludes that cryptocurrency is a threat to domestic and international security even in the form of assets or investments because cryptocurrency will only become a financial mode that will increasingly bubble, explode, and destroy/harm certain parties when reality finally pursues speculation, as the facts show that people face imperfect information and do not always act in an economically rational way, there is information that is biased, and tends to trade based on irrelevant information. Furthermore, Mabunda (2018) concluded that one of the biggest challenges for regulators today is the inherent nature of cryptocurrency that can be a money-laundering vehicle given that virtual currency has become a double-edged sword, which has made it easier to transact safely through the internet but at the same time has been exploited to facilitate a myriad of cyber crimes and help criminals to safely wash the proceeds of the sale. Indeed, although it cannot easily bind-users who can be identified in cryptocurrency activities that will make it possible for law enforcement to track the placement, coating, and integration of washed funds, Mabunda (2018) recommends banks and other financial institutions to conduct due diligence on cryptocurrency customers as the first line of defense against money laundering, wherein creating accountability to banks and related financial institutions, they are held liable for prosecution if they do not comply with regulatory requirements. The examination that must be carried out at least includes verification which proves that the customer is legitimate to conduct transactions involving: "(1) transfers from foreign institutions; (2) any transactions that involve a currency in an amount that would be greater than an internationally established threshold; (3) any transactions that involve a non-cooperative state Financial Action Task Force that is from a Financial Action Task Force on Money Laundering (FATF); or (4) where there are suspicions about whether or not the customer's previous information and data is accurate".

As some of the studies mentioned above have suggested the cryptocurrency phenomenon, there is a common thread in handling cryptocrime crime management, namely accountability. This is also in line with the views of Sinaga (2019) and the ideas of Sinaga, Wirawan, and Pramugar (2020) which emphasize that to minimize the dominance of criminal liability based on mistakes which so far tend to only ensnare certain natural human violations that are not necessarily the actual beneficiaries of the occurrence a crime, then the reconstruction of criminal liability in Indonesia needs to be done based on existing accountability models, namely the piercing model of the corporate veil, strict liability, vicarious liability, and secondary liability, because a responsibility should meet the consideration of public benefit (as economic considerations), as well as legal certainty and justice (as a moral consideration) considering that there have been losses to the victim must also have consequences for each party that is interrelated, namely the victim, direct perpetrators, and beneficiaries of the occurrence of a violation related to regulatory and welfare offenses.

Of course, for the application of accountability to be effective in handling cryptocurrency crime, it must be carried out by an official government institution that already has a legitimate source of authority from the state. These law enforcement institutions, which in the criminal law system in Indonesia should operate in the form of an integrated criminal justice system network or known as the integrated criminal justice system (ICJS). The government institution which has the supremacy in determining a crime is prosecuted or not prosecuted in a court and is also an institution that has an independent and accountable position between the executive and the judiciary, is the Prosecutor's Office. In Indonesia, Article 2 paragraph (1) of Law Number 16 of 2004 concerning the Prosecutor's Office (Prosecutor's Law) and Article 1 number 6 letter b and Article 13 of the Criminal Procedure Code (KUHAP) governs the prosecutor's office as a government institution which implements state power in the field of prosecution and other authorities based on the law, for example as the executor of a judge's ruling (Priyambudi, Sinaga & Bolifaar, 2020). The prosecution and prosecutorial discretion authority possessed by the prosecutor in handling cryptocurrency crime must be able to go beyond mere legal procedures, which in the context of a democratic country means that it must be able to understand certain communities or societies which in their interactions always proceed and transform in facing the globalization era. The state must not be repressive or apply autonomous law in dealing with the challenges that exist in cryptocurrency, because it actually strengthens the occurrence of global cryptocurrency crime. That is, the state must remain responsive to every social phenomenon, as Frank (1932) and Fuller (1934) once tried to mediate the rise of the exploitation of critics that are far from the truth and try to remind that the existing rules at that time tend to often fail to reveal the principles that apply adequately due to these principles do not have the force of enforcement in society, so a law is proposed that can improve the legal system that is more efficient, fairer, and more responsive to social needs.

The responsiveness of the state in dealing with the challenges of cryptocurrency crime must refer to the capacity to adapt the law responsibly, selectively, and not recklessly, rather than referring to the word open or adaptive. That is, in the organizational order of prosecution, the institution must assume that the pressures or social constraints in dealing with cryptocurrency crime are part of the source of knowledge and opportunities to improve themselves, which can present themselves as facilitators of various responses to the needs and aspirations social (Nonet & Selznick, 2010). Furthermore, Nonet and Selznick (2010) assert that responsive law is a legal theory that seeks to overcome the occurrence of repressive law and autonomous law in society through the following propositions: (i) The purpose of the law is competence in the form of participation through increased access with the integration of advocacy legal and social; (ii) Good law must offer more than formal justice, that is, a law that must be competent and be able to recognize the public desires and be committed to achieving substantive justice; (iii) Legal institutions must be more dynamic for social structuring and social change so that in their reconstruction they will be combined with basic themes in the form of activism, openness, and cognitive competence.

Responsive law in cryptocurrency should not be considered as a thing that prevents certain people or communities from transforming, because the uncertainty of cryptocurrency regulation will make its development uncontrollable which will lead to various risks, such as the potential to threaten the safety and stability of a country's financial system, including Indonesia, as well as being vulnerable to the emergence of economic crimes, namely money laundering, financing of terrorism, fraud, and other financial crimes (Ducas & Wilner, 2017). The government, in this case based on the prosecutorial discretion, must strive to encourage the participation of each party to make commitments accompanied by accountability in dealing with problems that arise (Nonet & Selznick, 2003) from the misuse of crypto assets (considering that in Indonesia bitcoin is legitimate as a crypto asset, not as a legal tender).

Method

In answering the existing problems, this study will use the doctrinal method or termed by Salter & Mason (2007) as black-letter approaches to doctrinal law, because the central point of this study interprets the relevant legal material or material to reveal a series of existing regulations based on a number of general legal principles defining. Furthermore, Salter & Mason (2007) assert that certain assumptions of the black-letter approach are that "rules give effect to, and specify, certain underlying and more general legal principles, such that the law can be interpreted as a more or less rational and coherent system rules". Since legal concepts and principles are the main basis of this research, this study uses secondary data relevant to the proposition, which focuses on legal data collected from legal cases, laws, legal journals and articles, research results, policy documents, and relevant legal textbooks (Gawas, 2017).

Result and Discussion

Overview Cryptocurrency

The weakness of the traditional currency payment system, which is high transaction costs with a long settlement period, has led people to alternative currencies that allow peer-to-peer (P2P) processing time: shorter, no intermediaries, and settlement risks that are lower. Then, increasingly triggered by the global financial crisis in 2008, coupled with a lack of confidence in the financial system when it increasingly triggers a great interest in cryptocurrency (Chuen, Guo & Wang). Some scholars support cryptocurrency due to the many key benefits of cryptocurrency, including borderless currency in the form of digital assets that can be used as a substitute for a currency that can be printed for monetary transactions, low transfer costs, simplicity and flexibility for users with simultaneous security systems in connection with public registration of transactions that can use a pseudonym account while maintaining system transparency and confidentiality, its management is based on cryptography that must use encryption and decryption techniques, the impossibility of confiscating funds, capital movements independent of the banking operating system, fewer bureaucratic obstacles because without regulatory authority or official issuer, using a decentralized method of verifying, recording and monitoring all transactions, issuance is limited through a regulation algorithm, and the fluctuation of values is based on the consensus of the parties in it (Matharu, 2019; Drozd, Lazur & Serbin, 2017).

The cryptocurrency concept built on blockchain technology, which allows verification of payments and other transactions without a centralized custodian (Makarov & Schoar, 2020), was closely related to the birth of Bitcoin which was put forward by someone whose pseudonym was Satoshi Nakamoto (2008).

Bitcoin that is purely P2P uses proof-of-work to record the history of public transactions quickly, allowing online payments to be sent directly from one party to another without going through financial institutions and without being attacked by hackers who want to cheat. Network security cannot be separated from the network of timestamps that transact it by hashing them into an ongoing chain of hash-based proof-of-work, which forms an irreversible record. Digital signatures are available as part of the solution to provide strong ownership control, but the main benefit is lost if a trusted third party is still required to prevent double-spending. Transaction authentication is carried out by third parties with the power of their CPU with a consensus mechanism that can declare their acceptance of a valid block by trying to expand it and reject an invalid block by refusing to work on it (Nakamoto, 2008). Bitcoin also cannot be separated from the use of blockchain technology (public digital ledger) by using a decentralized system, which allows transactions to run efficiently, and every bitcoin movement can be ensured clearly and can be seen in general (Ducas & Wilner, 2017).

Various treatments have been applied by countries in the world related to the implementation of virtual currencies. Some officially enforce in their country, some do certain restrictions, and there are those that strictly prohibited. Some countries that apply virtual currencies, such as Australia, Germany, the Netherlands, New Zealand, Singapore, Spain, and Canada, apply cryptocurrency as a money service business that is required to obtain a license and be taxed. Some countries that apply restrictions on digital money, such as Indonesia, Japan, China, and Russia only recognize it as a financial asset, not as a legal instrument of payment. Then, some countries which directly prohibit the implementation of cryptocurrencies, such as Bolivia, Ecuador, Thailand, Bangladesh, and Vietnam, because of their use as 'punitive offenses' that have the potential to be used illegally, money laundering, and use of the underground economy (Drozd, Lazur and Serbin, 2017; Raymaekers, 2015). Furthermore, the results of the Misnik study in 2017 (Drozd, Lazur & Serbin, 2017) conclude that the recognition of digital currencies is highly dependent on the level of development of the country, where countries with weak economies are not ready to enforce cryptocurrency payment systems, but countries who have advanced trying to regulate electronic payments by controlling and inviting them.

Cryptocurrency Settings in Indonesia

Press release of Central Bank of Indonesia (2018) (Bank Indonesia, hereinafter referred to BI) Number 20/4/DKom on January 13, 2018, confirms that in accordance with Law No. 7 of 2011 concerning Currency (hereinafter referred to Currency Law) which states that currency is money issued by the Unitary State of the Republic of Indonesia and any transactions that have payment purposes, or other obligations that must be fulfilled with money, or other financial transactions carried out in the territory of the Unitary Republic of Indonesia are required to use Rupiah so that virtual currency (including bitcoin) is not recognized as a legal payment instrument and is prohibited from being used as a payment instrument in Indonesia. The legal reasoning stated by BI is based on virtual currency ownership which is very risky, full of speculation, there is no responsible authority, there are no official administrators, there are no underlying assets that underlie the price of virtual currency, the value of trade is very volatile so it is vulnerable to the risk of inflation (bubble), and is prone to be used as a means of money laundering and financing of terrorism so that it can affect the stability of the financial system and harm society.

BI's prohibition on cryptocurrency as a virtual currency, but the development of cryptocurrency that has developed widely in society has been addressed in Article 1 of the Regulation of the Minister of Trade of the Republic of Indonesia No. 99 of 2018 on September 20, 2018, concerning the General Policy for the Implementation of Crypto

Asset which makes cryptocurrency a crypto asset that is traded as a commodity on the Futures Exchange. Furthermore, the Republic of Indonesia Commodity Futures Trading Regulatory Agency (hereinafter referred to Bappebti) regulates the technical provisions for the operation of the crypto asset physical market on the Futures Exchange in accordance with the Regulatory Commodity Futures Trading Regulatory Agency Number 5 the Year 2019 on February 8, 2019. Cryptocurrency used as a crypto asset commodity is defined as an intangible commodity in the form of digital assets, using cryptography, peer-to-peer networks, and distributed ledgers, to manage the creation of new units, verify transactions, and secure transactions without interference from other parties. In Article 3 paragraph 2, the regulation requires that crypto assets that meet the trade are based on distributed ledger technology, in the form of utilized crypto or crypto backed assets whose market stamp ranks into 500 coin market cap for crypto utilities, entered into the largest crypto asset exchange transactions in the world, has economic benefits (such as taxation, growing the informatics industry and digital talent, and risk assessments have been carried out, including the risks of money laundering and financing of terrorism as well as the proliferation of weapons of mass destruction. In addition, the Physical Traders of crypto assets in the futures exchange must meet several the following important thing:

1. Provide and/or open access to the entire system used for CoFTRA (the Commodity Futures Trading Regulatory Agency),
2. Submit periodic and occasional reports on the implementation of crypto-asset trading,
3. Every implementation of coordination and cooperation with Bappebti, authorities or other ministries/institutions,
4. Audited or audited online trading systems and/or facilities by independent institutions that have certification and are competent in the field of information systems,
5. Submit risk notification documents and enter into a crypto asset Customer agreement,
6. Carry out provisions on the implementation of anti-money laundering programs and prevention of financing of terrorism and the proliferation of weapons of mass destruction,
7. Receive or send funds by transfer between the bank account and the crypto asset customer (not in cash) whose identity must be in accordance with the Rupiah currency, and
8. Report any suspicious crypto asset transactions to the Head of CoFTRA and report any suspicious financial transactions to the Head of Indonesian Financial

Transaction Reports and Analysis Center (*Pusat Pelaporan dan Analisis Transaksi Keuangan*/PPATK).

Then in Article 20 of the Commodity Futures Trading Regulatory Agency Regulation Number 5 of 2019, it is stated that violations committed by the parties will be subject to sanctions in accordance with the provisions of the applicable laws and regulations in Indonesia.

The Regulation of the Commodity Futures Trading Regulatory Agency Number 5 the Year 2019 has explicitly tried to close the gap for those who try to misuse crypto assets for criminal purposes. But the lack of law enforcement rules in these regulations, especially regarding the accountability of the parties really requires prosecutorial discretion in an effort to eradicate cryptocurrency crime in Indonesia. It is feared that transactions through the futures market are only a means for criminals to disguise money from and or abroad for certain purposes through crypto-asset customers who are only intermediaries, bearing in mind the prohibition of virtual currency transactions in Indonesia and the strict control of cash at airports, ports or national borders. and the strict regulation of banking transactions when transferring to and from abroad in Indonesia. In addition, the regulation of criminal liability in the event of a violation of crypto assets still touches on liability based on mistakes, which will not be relevant to the perpetrators who receive actual benefits or have been known as beneficial owners, whose names will never be seen on paper.

Piercing the Cryptocurrency Crime Liability Veil

In the case of violations that result in harm to victims, the legal regime (responsive) must show its role in seeking to mitigate or recover damages to victims through assigning responsibility not only to direct perpetrators but also touching those who receive benefits. for the violation (Sinaga, 2017). Furthermore, for cryptocurrency crime liability to touch substantive justice, responsibility must refer to cumulative acts in the form of violations (which are not only committed by direct perpetrators but also to anyone who is legally related to the perpetrators of these violations) to existing agreements (agreements can refer to the applicable law in Indonesia) which has caused losses to the victim so it must be resolved in the realm of criminal law (Sinaga & Sinaga, 2018).

The broad meaning of the accountability shows that in dealing with cryptocurrency crime issues, it should not only apply liability based on fault (that always requires proof of three interrelated components: actus reus, mens rea, and without a recognized legal defense

(Ferguson, 2015), but able to reach responsibility that is able to fulfill justice (at least in the form of equality or fairness), because it is related to the occurrence of loss to the victim and at the same time to provide objective legal consequences to each party involved in cryptocurrency crime, and which is able to provide public benefit, as a solution to the complexity of the problems that occur in the field of social welfare or the rise of certain behaviors that require a due care standard in a particular community or community (Sinaga, 2019) Some accountability models that are not based on liability based on fault strict liability, vicarious liability, and secondary liability.

Strict Liability of the Cryptocurrency Crime

There are several literature reviews that discuss absolute accountability. Arief (2010) explains that absolute criminal liability is imposed because it has violated certain obligations or conditions or situations that have been determined by law. Atmasasmita (2009) asserted that absolute accountability regarding crimes that “mens rea” is casuistically needed not to be proven because it is a coercion of the rights of others, welfare offenses, or regulatory offenses so it is feared that having to prove mens rea will be able to hamper the purpose of the legislation these laws. Jones (2013) revealed that absolute liability is imposed on a person even if he did not make a mistake due to acts against the law. Some of these opinions show that absolute liability is imposed for an unlawful act on a certain obligation or condition or situation that has been determined by the law imposed on a person even if he did not make a mistake and does not need to be proven in his rea and has caused harm to the victim. This accountability is able to anticipate violations of economic substance doctrine, provide a deterrent effect, and anticipate the intentions of certain parties to create complex transaction structures (Thomas, 2011). However, this regulation regarding liability is still limited in the Draft Penal Code, as Article 39 paragraph (1) states that for certain criminal acts, the law can determine that a person can be convicted solely because it has fulfilled the elements of criminal acts without paying attention to any mistakes (DPR, 2017).

The application of strict liability in cryptocurrency crime is very adequate to be applied to the parties in the transaction as if it were made very complex and not in accordance with the economic substance doctrine, because of certain crimes that must be covered up. Of course, the implementation of strict liability is in line with blockchain technology in recording every cryptocurrency transaction transparently, minimally to be cheated, efficient, and fast.

Vicarious Liability of the Cryptocurrency Crime

There is some literature that explains about vicarious liability. Jones (2013) describes vicarious liability as an act of taking responsibility for violations committed by another person, which arises because of a special relationship between the parties. Chen (2017) argues that vicarious liability is the responsibility of those who obtain direct financial benefits for a direct violation committed by another party because it relates to supervision and control imposed on the responsible party. So with this accountability, the responsible party will increasingly increase prudence in selecting, supervising, supervising, and monitoring the parties working for it. Furthermore, Greene (2017) suggests several arguments that justify vicarious liability against certain parties for criminal acts committed by other parties, namely: a) The ability of the party being held responsible for paying insurance in anticipation of risk and its ability to improve standards or systems; b) Is the beneficiary of the work of the party who commits the crime and at the same time the party being held responsible is able to apply the rules, such as the obligation of compensation to the party responsible if there is a loss committed by the party who committed the crime in the scope of work. To prove that the party committing the crime has a position within the scope of the business or is an independent contractor against the party being held responsible, Greene recommends conducting 3 (three) tests, namely the control test (to ascertain the extent to which the party's control is held responsible for the party conducting the crime), organizational test (to believe that the party committing the crime is integrated with the organization of the party held responsible, or is part of the organization's completeness), and the economic reality test or multiple tests (is the development of certain cases by considering various factors applicable).

The adequacy of the use of vicarious liability has not been supported by positive direct regulation (KUHP), because until now the regulation on liability is still limited in the Draft Penal Code, as in Article 39 paragraph (2) the Draft Penal Code formulates that in the case determined by Law Act, everyone can be held accountable for criminal acts committed by others (DPR, 2017).

The existence of vicarious liability is very urgent and urgent to be applied in cryptocurrency crime, given the proper and adequate criteria to pursue acts against the law committed by actual beneficiaries, so as to provide fairness and equality to parties deemed to make mistakes but can prove not to receive any additional benefits from the occurrence a cryptocurrency crime.

Secondary Liability of the Cryptocurrency Crime

Dinwoodie (2017) explains that the core secondary liability or accessory liability or indirect liability of the defendant's liability for losses caused by the wrongdoing of the primary party, or liability that is a derivative of primary liability. Secondary liability can occur because of participant-based or relationship-based. Participant-based liability occurs through the involvement of secondary actors, which causes or which contributes to or facilitates the occurrence of harmful actions committed by primary wrongdoers, while relationship-based liability occurs because of the benefits received by secondary actors for violations that harm certain parties and their presence very close relationship with the primary wrongdoer. Dinwoodie gave an example of secondary liability in internet service providers that can be held responsible when criminal acts occur in cyberspace, where primary wrongdoers are often anonymous, do not have sufficient financial capacity, or are outside the jurisdiction (Dinwoodie, 2017).

Secondary liability is feasible in cryptocurrency crime because the criteria are met to punish secondary parties or intermediaries who turn out to have the right and ability to supervise the activities of other parties so as not to violate laws or harm other parties. Even the ideal of secondary criminal liability lies in its nature which must notify specific things to a party regarding the impact of a violation of a purpose, and failure to prevent the use of the violation, or intentionally ignoring the existence of the violating act (Sinaga & Sinaga, 2020).

Prosecutorial Discretion in Cryptocurrency Crime

The majority of prosecutors in the world have at least authority as prosecutors, executors of court decisions, and other authorities. This also applies in Indonesia, where Article 2 of Law Number 16 of 2004 concerning the Prosecutor's Office (hereinafter referred to Prosecutor Law), which asserts that the prosecutor's office is the executor of state power in the field of prosecution as well as other authorities based on an independent law. Strengthening the power of prosecutors is also regulated in Article 1 number 6 (a) and 6 (b) and Article 13 of the Criminal Procedure Code, and Article 1 number 1 and number 2 of the Prosecutor's Law which authorizes prosecutors to act as public prosecutors as well as implement court decisions that have obtained permanent legal force. Furthermore, in the case of the prosecution, the explanation of Article 30 paragraph 1 letter (a) of the Prosecutor's Law has stated that in conducting the prosecution, prosecutors can conduct pre-prosecution, where the prosecution is an act of the prosecutor to monitor the progress of the investigation after receiving notification of the commencement of the investigation from the investigator, providing instructions to be completed by the investigator to be able to determine whether the file can be delegated or not to the prosecution stage.

The amount of authority and prosecutorial discretion possessed by prosecutors, such as bringing a case to court, the length of imprisonment indicted, and/or the number of criminal fines charged in a case, have often been the subject of much debate in much of the literature because it is feared to be a bargaining loophole. But there is also some debate regarding the absence or lack of discretion in prosecutions because they are under a full and mandatory prosecution system which turns out to have implications for the fair administration of criminal law (Levine & Feeley, 2015).

Even though there is a long debate about prosecutorial discretion, cases related to cryptocurrency crime must still use prosecutorial discretion from prosecutors. Prosecutorial discretion is an effort to present a law that truly supports substantive justice and public benefit, which is actually carried out through pre-prosecution (which is a stage owned by the public prosecutor to conduct a study of the results of the investigation accompanied by instructions from the public prosecutor) so that the investigator able to explore justice and truth, especially in terms of criminal liability in the event of cryptocurrency crimes, so that the resulting case file provides an output as well as a good outcome (Priyambudi et al., 2020). Challenges to prosecutorial discretion increasingly appear to transcend national boundaries, where prosecutors must deal with a global criminal justice system that demands the quality of evidence so that prosecution can succeed. A more tangible example is the crime of global terrorism that can not be separated from cryptocurrency crime, prosecutors must be able to instill and convince their prosecutorial discretion through support and certain approaches that can give preference to one set of objectives of the other party, which shows that the prosecution task must successfully refer to no more casualties in the form of innocent people in the future, prevention of mistakes that can release or release terrorists that will actually add casualties in the future, facilitate long-term peace due to the eradication of terrorists, and provide justice to the victims and his family (Levine & Feeley, 2015).

Cryptocurrency crime can endanger the country, such as Indonesia and several other countries experiencing terrorism cases allegedly funding through cryptocurrency, strengthening prosecutorial discretion can be done through the application of accountability beyond accountability based on mistakes. Indeed, the legal system in Indonesia which is identical to continental law seems to be an obstacle for prosecutors to apply strict liability, vicarious liability, and secondary liability that has not been explicitly regulated in the Criminal Code where the Criminal Code itself strongly adheres to the principle of legality, which emphasizes that no one can be convicted if not stipulated in advance in the Act. However, looking at the objectives to be achieved by the Prosecutor as the executor of state power in the field of prosecution as well as other authorities independently and considering the freedom of the Judge in deciding a case or case, as in Article 5 paragraph (1) of RI Law No. 48 of 2009 concerning Judicial Power has required Judges to explore, follow, and understand the legal values and sense of justice that lives in the community, then prosecutorial discretion in applying strict liability, vicarious liability, and secondary liability in cryptocurrency crime will be a legal discovery for judges in deciding every case that must be based on legal values and a sense of justice that lives in society. The distinctive characteristics of cryptocurrency decentralization and anonymity that are one of the main attractions for criminals must still be addressed through a "follow the money" strategy. This strategy is in line with Brown's (2016) explanation that suggests a cryptocurrency crime mode that cannot be separated from the official currency, ie when trying to exchange official currency to cryptocurrency and vice versa when trying to exchange cryptocurrency to official currency and using an email address suitable for receive transaction details. All cryptocurrency transactions, such as Bitcoin, will at least go through placing, layering, and integration stages, where layering will involve the import of illicit money into the financial system (often employing several "smurfs") to then spread to different financial institutions through depositing in low amounts to different accounts (note, the amount is kept below the reporting threshold according to applicable law so as not to attract the attention of the authorities), then layering will go through several transactions or layers to obscure the source, and then move towards the stages of integration into the "legitimate" circulation (Brown, 2016). Indeed, an analysis of cryptocurrency transactions distributed to all account holders in the ledger is expected to be a guide in tracing transaction flows to find the pseudonyms involved and to follow the transaction history of the perpetrators, but the biggest challenge is connecting pseudonyms with real people. These challenges can be overcome through the application of accountability not based on mistakes, as criminal violations committed by primary wrongdoers cannot be carried out if they do not involve means of information and communication technologies (ICTs), such as e-mail, disposable and anonymous mobile phone numbers, and the internet that helps perpetrators of crypto crimes (Meteab, 2020). As Brown (2016) has emphasized that cryptocurrency cannot be separated from the use of an email address that is suitable for receiving transaction details. It is clear that to do this it is necessary to use an alias to create a disposable e-mail account, so the step that is often used by criminals is to buy cheap mobile phones that cannot be traced, wherein the cellphone number can then be used to validate the new e-mail account (Brown, 2016), so that strict liability, vicarious liability, and secondary liability must be applicable to sellers of ICTs and to buyers and traders of crypto physical assets on the futures exchange.

If strict liability, vicarious liability, and secondary liability can be applied to cryptocurrency crime through prosecutorial discretion, then the anonymity constraints in buying and selling crypto must be overcome by prosecutors through its prosecutorial discretion. As all details of cryptocurrency transactions are carried out through blockchain technology that is open ledger through distribution to account holders in a major report, as well as cryptocurrency flows that always require consensus, the prosecutors in Indonesia, in addition to coordinating and cooperating with several prosecutors in several countries, can work together with other law enforcers in Indonesia, especially with tax authorities who have financial databases and have required recording and bookkeeping of every taxpayer who must report tax returns (SPT) in Indonesia (Hermawan & Sinaga, 2020), can use his discretion to carry out follow the money against suspicious transactions. So, it is very possible to uncover the pseudonym of the perpetrators of cryptocurrency transactions through transaction history which is always in the blockchain. The next step is to try to connect anonymously with actual people suspected of misusing cryptocurrency for criminal purposes. Of course, if the jurisdiction in Indonesia, cryptocurrency exchange can be traced to real currency in the legal territory in Indonesia. Because in the beginning real assets and/or real currencies are needed to obtain cryptocurrency, and in the end the cryptocurrency obtained will be exchanged for real assets and or real currencies considering that not all transactions carried out by these criminals in their daily lives can use cryptocurrency.

Regarding the consensus in cryptocurrency transactions. To anticipate and be able to immediately jump into analyzing suspicious transactions, the Prosecutors through their own unit can carry out official actions that explore the capability and utility-oriented controls (Li, 2014) in tackling cyberspace legal loopholes used by cryptocurrency criminals, such as coordinating with other law enforcers in order to open the account of an email so as to participate in conducting cryptocurrency transactions, so that they can always routinely analyze every transaction that occurs, can immediately assess the risk "nodes" which are most likely to be involved in cryptocurrency crime, and in the end the application of each type of responsibility to the perpetrators of cryptocurrency crimes and the parties involved in fulfilling equality, fairness, and public benefits.

Conclusion

This paper produces two main conclusions. First, in Indonesia cryptocurrency arrangements are only carried out on crypto-asset trading, but may not be used as a means of payment because virtual currencies have been banned by BI. Second, responsive prosecution discretion is needed in eradicating cryptocurrency crime in Indonesia through the application of accountability that exceeds liability based on faults, because liability based on faults will not be able to ensnare the actual beneficiaries, and only ensnare perpetrators of "puppets" who are already ready to put on the body receive punishment. The prosecution's discretion that fulfills responsive law is by implementing a "follow the money" and "trace the ICTs footprint" strategy to then apply strict liability, vicarious liability, and secondary liability to each party legally involved in the occurrence of a cryptocurrency crime. It is expected that the coordination of prosecutors and other law enforcement agencies through task forces, especially in preventing the occurrence of cryptocurrency crime, will actively participate in conducting cryptocurrency transactions, so that they can immediately manage risk through monitoring of suspicious “nodes” and implementing accountability rather than based on mistakes of each ICTs trader which does not implement strict registration of facilities that are at risk of being used in cryptocurrency transactions, such as laptops, cell phones, computers, and SIM Cards.

References

Arief, B.N. (2010). *Capita Criminal Law Selection*. Bandung: Citra Aditya Bakti.

Atmasasmita, R. (2009). *Comparison of Contemporary Criminal Law*. Jakarta: Fikahati Aneska.

Brown, S.D. (2016). Cryptocurrency and criminality: The Bitcoin Opportunity. *The Police Journal: Theory, Practice and Principles*, *89*(4), 327-339.

Central Bank of Indonesia (2018). *Bank Indonesia warns all parties not to sell, buy or trade virtual currency*. Jakarta: Press Release of Central Bank of Indonesia No. 20/4/DKom.

Chen, L.S. (2017). Internet Service Provider Copyright Infringement in Taiwan. In *Secondary Liability of Internet Service Providers*, Dinwoodie, G.B. (Ed.). Cham-Switzerland: Springer International Publishing, 343.

Cheng, Y. (2019). Review of Chinese Policy against Cryptocurrency Growth, *International Journal of Science and Society*, *1*(1), 38-45.

Chuen, D.L.K., Guo, L., & Wang, Y. (2017). Cryptocurrency: A New Investment Opportunity?. *Journal of Alternative Investments, 20*(3), 16–40.

Cipher Trace. (2019). *Cryptocurrency Anti-Money Laundering Report, 2019 Q3*. https://ciphertrace.com/wp-content/uploads/2019/12/CipherTrace-Cryptocurrency-Anti-Money-Laundering-Report-2019-Q3-2.pdf.

Dinwoodie, G.B. (2017). *A comparative analysis of the secondary liability of online service providers.* In Secondary Liability of Internet Service Providers, Springer, Cham, 1-72.

DPR. (2017). *Rancangan laporan singkat Pembahasan Rancangan Kitab Undang-Undang Hukum Pidana*. http://www.dpr.go.id/doksileg/proses3/RJ3-20190430-114030-5314.pdf.

Drozd, O., Lazur, Y., & Serbin, R. (2017). Theoretical and Legal Perspective on Certain Types of Legal Liability in Cryptocurrency Relations. *Baltic Journal of Economic Studies*, *3*(5), 221-228.

Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. *International Journal, 72*(4), 538–562.

Engle, E. (2016). Is Bitcoin Rat Poison? Cryptocurrency, Crime, and Counterfeiting (CCC). *Journal of High Technology Law*, *16*(2), 340-393.

Frank, J. (1932). Mr. Justice Holmes and Non-Euclidean Legal Thinking. *Cornell Law Review*, *17*(4), 586.

Frunza, M.C. (2016). Cryptocurrencies: A new monetary vehicle. In *Solving modern crime in financial markets: Analytics and case studies*, Frunza, M.C. (Ed.). MA: Elsevier Inc., 40.

Fuller, L.L. (1934). American Legal Realism. *Univ. PA. Law Review*, *82*(5), 462.

Gawas, V.M. (2017). Doctrinal legal research method a guiding principle in reforming the law and legal system towards the research development. *International Journal of Law*, *3*(5), 128-130.

Greene, B. (2017). *Optimize Tort Law*. London: Taylor & Francis Ltd.

Hermawan, A.W., & Sinaga, H.D.P. (2020). Public Benefit Principle in Regulating E-Commerce Tax on Consumer’s Location in Indonesia. *International Journal of Advanced Science and Technology*, *29*(8), 1212-1222.

Kelly, J., & Wilkes, T. (2018). *Exclusive: Coincheck hackers trying to move stolen cryptocurrency-executive*. https://www.reuters.com/article/us-japan-cryptocurrency-cybercrime/exclusive-coincheck-hackers-trying-to-move-stolen-cryptocurrency-executive-idUSKBN1FJ28Y.

Levine, K., & Feeley, M. (2015). Prosecution. In *International Encyclopedia of the Social & Behavioral Sciences Volume 19*, 2nd ed. MA: Elsevier Ltd, 210–215.

Li, X. (2014). Exploring into regulatory mode for social order in cyberspace. *Webology 11*(2), 1-8.

Mabunda, S. (2018). Cryptocurrency: The new face of cyber money laundering. *In IEEE International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, 1-6.

Makarov, I., & Schoar, A. (2020). Trading and Arbitrage in Cryptocurrency Markets, *Journal of Financial Economics*, *135*(2), 293-319.

Matharu, A. (2019). *Understanding cryptocurrencies: The money of the future*. New York: Business Expert Press.

Meteab, A.A. (2020). Effect of Continuous Improvement of Information Technology Applications on E-Costumer Behavior in Social Media. *Webology, 17*(1), 19-29.

Nakamoto, S.B. (2019). *A Peer-to-Peer Electronic Cash System*. https://nakamotoinstitute.org/bitcoin/

Nonet, P., & Selznick, P. (2010). *Responsive Law*. Bandung: Nusa Media.

Nonet, P., & Selznick, P. (2003). *Responsive Law: Choices in Transition*. Jakarta: Huma.

Nykodym, N., & Taylor, R. (2004). Control of Cyber crime: The world's current legislative efforts against cyber crime. *Computer Law & Security Review*, *20*(5), 390–395.

Prasetyo, H.M. (2019). *Remarks by the Attorney General of the Republic of Indonesia at the opening of an integrated training of law enforcement officers between countries with the theme of anticipating the development of cryptocurrency crimes*. Jakarta: Kejaksaan Agung.

Priyambudi, Arief, B.N., Putera, N.S.J., Sularto, R.B., & Sinaga, H.D.P. (2020). Political Corruption and the Role of Public Prosecutors in Indonesia. *Tes Engineering & Management*, *83*, 11981–11992.

Priyambudi, Sinaga, H.D.P., & Bolifaar, A.H. (2020). Managing Plea Bargaining Risk in Indonesia: An Effort to Overcome the Corporate Corruption. *Tes Engineering & Management*, *83*, 11993–12005.

Raymaekers, W. (2015). Cryptocurrency Bitcoin: Disruption, challenges and opportunities. *Journal of Payments Strategy & Systems*, *9*(1), 30–40.

Salter, M., & Mason, J. (2007). *Writing Law Dissertations: An Introduction and Guide to the Conduct of Legal Research*. Essex: Pearson Education Limited.

Sinaga, B.R.P., & Sinaga, H.D.P. (2020). Secondary Criminal Liability in the Customs Field: An Effort of Handling of E-Commerce Challenges in Indonesia. *In International Postgraduate Students Conference (INGRACE) on Legal Challenges and Opportunities in the Fourth Industrial Revolution: Sustainability*, Human Rights and Social Justice Perspectives in Asia Pacific at Faculty of Law, Universitas Gadjah Mada, Yogyakarta, Indonesia on January 20th-21th, 2020.

Sinaga, H.D.P. (2019). Regulation of the Absolute Accountability of Taxpayers in Indonesia from the Perspective of Justice and Public Benefit. *Jurnal Hukum & Pembangunan*, *49*(3), 517-546.

Sinaga, H.D.P. (2017). Liability of Substitutes in Tax Law in Indonesia. *Masalah-Masalah Hukum*, *46*(3), 206–217.

Sinaga, H.D.P., & Sinaga, B.R.P. (2018). *Reconstruction of Accountability Models in the Tax and Customs Sector*. Yogyakarta: PT. Kanisius.

Sinaga, H.D.P., Wirawan, A., & Pramugar, R.N. (2020). Recontruction of Corporate Criminal Liability in Indonesia. *International Journal of Advanced Science and Technology*, *29*(8), 1231-1240.

Sterling, T. (2016). *Dutch arrest 10 men suspected of using Bitcoin to launder money*. https://www.reuters.com/article/us-netherlands-crime-bitcoin-idUSKCN0UY0V8.

Thompson, M. (2018). *The US and Cryptocurrency Crime*. https://axcessnews.com/national/breaking-national/us-cryptocurrency-crime_6635/.

Tisnadibrata, I.L. (2017). *PPATK: Funding Terrorism in Indonesia, Bahrun Naim Uses Paypal and Bitcoin*. https://www.benarnews.org/indonesian/berita/aliran-dana-terorisme-01092017160938.html.

Ferguson, G. (2015). Criminal Liability and Criminal Defenses. *In International Encyclopedia of the Social & Behavioral Sciences*, *19*, 2nd ed. MA: Elsevier Ltd, 219–226.

Jones, L. (2013). *Introduction to Business Law*. Oxford: Oxford University Press.

Thomas, K.D. (2011). The Case Against A Strict Liability Economic Substance Penalty. *University of Pennsylvania Journal Business Law*, *13*(2), 445–497.

Thamer, K.A. (2020). Method of artificial neural networks teaching. *Webology*, *17*(1), 43-64.