

## REVIEW ARTICLE

# CRIMINAL LAW POLICY IN HANDLING DIGITAL ASSET-BASED MONEY LAUNDERING IN INDONESIA

Dipo Lukmanul Akbar<sup>1✉</sup>

<sup>1</sup>Managing Partners at Dipo & Partners Law Office, Jakarta

✉ [dipolukmanulakbar@gmail.com](mailto:dipolukmanulakbar@gmail.com)

## HOW TO CITE

Akbar, D.L. (2020). Criminal Law Policy in Handling Digital Asset-Based Money Laundering in Indonesia. *Journal of Law and Legal Reform*, 1(1), 129-176. DOI: <https://doi.org/10.15294/jllr.v1i1.35543>

---

## ABSTRACT

The rapid development of information technology has given birth to a variety of services with a variety of digital information facilities, where the sophistication of information technology-based products is able to integrate all information media so as to make the world become borderless and cause significant social, cultural, economic and law enforcement changes take place quickly. Nevertheless, the conditions in Indonesia which are growing and developing towards an information technology-based industrial society, in some cases are still lagging behind to follow the development of information technology. The concepts and theories used to analyze are Criminal Law Policy, Law Number 8 of 2010 concerning Money Laundering. The paper emphasized that the development of information technology that is developing now, especially in the field of digital assets is able to become an opportunity for money laundering. The paper highlighted that in the case of committing the crime of money laundering is carried out using the digital currency-based information technology method and can be used for cross-country trade. So that the crime of money laundering based on digital assets is very easy to do and can have a worldwide network.

**Keywords:** *Criminal Law Policy; Money Laundering Crime Handling; Digital Assets*

Submitted: 20 August 2019, Revised: 11 September 2019, Accepted: 28 October 2019

# TABLE OF CONTENTS

ABSTRACT .....	129
TABLE OF CONTENTS .....	130
INTRODUCTION .....	131
I. BACKGROUND .....	131
A. Technology Development and Crime Opportunities .....	131
B. Financial Technology in the Industrial Revolution .....	132
C. Renewal of Criminal Law in Technology Issues .....	132
II. RESEARCH PROBLEM IDENTIFICATION , LIMITATION AND FORMULATION .....	134
A. Identification of the Problems .....	134
B. Formulation of the Problems .....	134
C. Identification of the Problems .....	134
LITERATURE REVIEW .....	134
I. CRIMINAL LAW POLICY .....	134
A. The Foundation of Criminal Law Policy .....	134
B. Criminal Law Countermeasures .....	135
C. Policy Formulation .....	137
D. Law Enforcement Policy .....	139
E. Understanding of Criminal Law Policy .....	140
METHOD .....	142
DIGITAL ASSETS AND MONEY LAUNDERING IN INDONESIA .....	142
I. DIGITAL ASSETS BECOME OPPORTUNITIES FOR MONEY LAUNDERING .....	142
A. Development of Digital Assets .....	142
B. Blockchain Technology and Its Complexity .....	143
C. Crowd Funding .....	145
D. E-Money .....	145
E. Insurance .....	146
F. P2P Lending .....	147
G. Payment Gateway .....	147
H. Remittance .....	149
I. Securities .....	149
II. ACTS OF MONEY LAUNDERING USING DIGITAL ASSET MEDIA ..	150
A. Cases of Money Laundering Using Digital Assets Media .....	150
B. Bitcoin and Money Laundering in Indonesia .....	154
III. OPPORTUNITIES FOR DIGITAL ASSET-BASED MONEY LAUNDERING CRIME .....	157
A. CDD or EDD Obligations .....	158
B. Not Required To Report TKM .....	159
C. Illegal Fintech and Money Laundering .....	159
IV. PENAL POLICY IN THE HANDLING OF DIGITAL ASSET-BASED MONEY LAUNDERING CRIME .....	164
A. Current Criminal Law Policy towards Countering Money Laundering Crime .....	164

B. The Application of Money Laundering Crimes from The Perspective of The Money Laundering Act of 2010 .....	167
CONCLUSION .....	172
REFERENCES .....	172

## INTRODUCTION

### I.BACKGROUND

#### A. Technology Development and Crime Opportunities

The development of Information Technology that has developed now, has presented a variety of digital services, in which the technological information sophistication is able to easily integrate all fields of digital services so as to make the world become borderless, this has led to social, cultural, economic and economic changes. and fast and significant legal behavior. Nevertheless, the conditions in Indonesia that are growing and developing towards an information technology-based industrial society, in some respects, especially in the Legal Sector, are still lagging behind to keep abreast of such information technology.

The development of information technology which currently has many benefits for people in Indonesia, such as some development and advancement in facilities that occur in the fields of business, government, education, and many more. The ease in question is very young in interacting without having to deal directly with each other. So that this can have a negative advantage, on the other hand it also impacts the negative impact on the unprepared regulations that are proportional to the effects of criminal acts which will continue to grow and be misused by the community, resulting in unlawful acts.

Utilization of the development of information technology which has many positive impacts but also cannot be denied many also have negative impacts. Crime that uses information technology based is considered more effective and efficient, this is because it can easily access to all corners of the world, meaning conventional crime such as fraud, theft, threatening, embezzlement, gambling, defamation, money laundering to criminal acts of terrorism and attorney through the Information Technology media can be done *online* by individuals or groups and or a corporation, with the risk of being caught or in contact with a very small law with a result of greater losses for both society and the state. This causes the behavior of individuals and groups in committing criminal acts to be increasingly sophisticated by utilizing information-based information technology from the internet. Development is always evidenced by the existence of innovation and creativity, in this case in the field of information technology which has provided many conveniences for human life. The business world is increasingly competing to always innovate and win the market, where when business people do not do that, then they will always be left behind and businesses will not easily survive to face market demand.

Joseph Schumpeter (1934) has argued that based on his theory that “*creative destruction*” entrepreneurial values will bring up new markets through new methods. If Joseph Schumpeter's thoughts were clashed with legal instruments, then of course the law is not able to catch up with the dynamics of this very dynamic business. That what has been stated by Joseph Schumpeter the value of entrepreneurship is an innovation and creativity that is always developing in the business market using new methods, where the intuitive thing will greatly facilitate the community in using a population offered by Business Actors, so because it is product which has been introduced to the public by providing conveniences, then the legal basis or regulations or legislation may not necessarily be used as a legal basis for these stone products.

### B. Financial Technology in the Industrial Revolution

*Financial Technology* (Fintech) is a form of application of information technology in the financial sector. This is evidenced by the emergence of various digital financial innovation models that first started in 2004, financial institutions in the UK that run money lending services. Then the digital financial model through software, the cryptocurrency that was conceived by Satoshi Nakamoto in around 2008. In historical perspective, the core concept of the development of information technology is actually inseparable from the application of the concept of *peer-to-peer landing* (P2P) used by Napster in 1999 for *music sharing* (Pratama 2016).

The rapid development of the Investigation Technique was marked by the emergence of fintech, where the intended *fintech* is one of the digital currencies (cyrtocurrency) which in relation to the history of this currency was made by Satoshi Nakamoto in 2008, using a *peer-to-peer* (P2P) concept application), so that the development of the P2p technique is emerging, then there are financial service invasions in the field of financial services.

The Industrial Revolution has many new technical developments, as it develops, the forms of crimes are also developing, but generally the crimes are still conventional, only the methods applied always change with the times. Ronni R. Nitibaskara argued that: "Social interaction that minimizes physical presence is another feature of the information technology revolution. With this kind of interaction, social relations deviation in the form of crime will adjust its shape to that character. "

### C. Renewal of Criminal Law in Technology Issues

Reform in criminal law as part of a criminal law policy in which the rapid development of information technology is also important for the renewal of new norms that apply in accordance with existing values in Indonesian society. The importance of reforming a criminal justice system as a whole with due regard to legal culture, legal structure, and legal substance so that criminal law policy occupies a very strategic position in the development of modern criminal law to achieve certainty and usefulness of the law.

"That there are many reasons that can be cited as the cause of a change in society, but changes in the application of the results of modern technology are widely cited as one of the causes for social change (Raharjo, 1980). That the occurrence of these changes can be related to a social values, behavioral patterns, organization, arrangement of state / community institutions, and the authority of social interaction and so on where a change that occurs in the community will have an impact on the legal pattern in society.

The globalization process gave birth to a phenomenon that changed the conventional communication model by giving birth to reality in the virtual world (*virtual reality*) that is known today with the internet. The internet is developing so rapidly as a culture of modern society, said to be a culture because through the internet a variety of cyber community activities such as thinking, creating, and acting can be expressed in it, whenever and wherever. Its presence has formed a separate world known as cyber-space or pseudo world is a world of computer-based communication offers a new form of virtual reality (indirect and intangible) (Rahardjo, 2002)

As stated by Agus Rahardjo above, a globalization mechanism is shown by the initial to interact through conventional methods to change into interaction in cyberspace or interact using the internet, in relation to the internet, then a separate world directly or indirectly will occur a society and free to interact throughout the world.

Information technology is growing so rapidly that it must be made responsively related to the regulation, the law cannot be made before the problem, but in general the countermeasure is made first, and this will be much better. The development of digital crime has indeed been known as *cyber war or cyber law*, where there are so many positive impacts, but on the one hand there are also many negative impacts. This is in line with the term Barda Nawawi Arief which states that: *cybercrime identical with "criminal acts in cyber space" or "cyber space" or commonly also known as "cybercrime"* (Nawawi Arief, 2006)

Nawawi Arief (2003), Criminalization policy is a policy in determining an act that was not a criminal offense (not convicted) into a criminal act (an act that can be convicted). So in essence, the policy of criminalization of information technology crime is part of a criminal policy (*criminal policy*) using the means of criminal law (*penal*), and therefore includes part of the "criminal law policy" (*penal policy*), especially the formulation policy. Furthermore, according to the BNA, the criminalization policy is not just a policy of establishing or formulating what can be convicted (including criminal sanctions), but also includes the problem of how the formulation / legislation policy is arranged in a unified harmonious and integrated legal system (legislative policy).

## II. RESEARCH PROBLEM IDENTIFICATION , LIMITATION AND FORMULATION

### A. Identification of the Problems

From the background description above, problems can be identified , namely, starting from (1) Digital assets which are always developing rapidly can be used as a tool for money laundering; (2) The criminal law in force in Indonesia regulates the crime of money laundering, which does not mean that the regulation of the criminal act in force in Indonesia is carried out on the basis of digital assets; (3) The legal policy perspective is a legal renewal, in which criminal law must be able to keep up with the times as a form of countermeasures for a crime, especially in this case digital assets that are growing very fast.

### B. Limitation of the Problem

The problem is limited based on above problem identification, the research will focus on the "Criminal Law Policy Against Money Laundering Prevention-Based Digital Asset". With the limitation of this problem, it is hoped that researchers will focus more on studying and examining the problems that exist in the Criminal Law Policy Against Digital Asset-Based Money Laundering Crime.

### C. Formulation of the Problem

The problems studied will be more assertive and writing legal research to achieve the objectives it is necessary to formulate the problem as follows:

1. Does digital assets open up opportunities for money laundering;
2. Whether the current criminal law policy is a comprehensive provision in dealing with digital asset-based money laundering crimes;
3. What is the prospect of a comprehensive criminal law policy on the prevention of digital asset-based money laundering in the future

## LITERATURE REVIEW

### I. CRIMINAL LAW POLICY

#### A. The Foundation of Criminal Law Policy

National development is development that aims to realize people. Where is the national development of Indonesia to achieve a just, prosperous and prosperous society both materially and spiritually based on Pancasila and the 1945 Constitution. So that one part of national development is development in the field of law, which is known as *law reform*. . The renewal of national law as part of a series of national development is carried out thoroughly and integrated both criminal law, civil law, and administrative law, as well as formal law.

Efforts to reform the law are inseparable from public policies in controlling and shaping the pattern of how far the community is regulated and directed. Thus it is

very important to make the law makers and public policy even educators aware that the law and public policies that are published will have broad implications in the social, economic and political fields. Unfortunately, specialization both in work, education and research are based on these two disciplines (law and social science), so that various information sourced from the two do not always meet (*converge*) even often not the same and congruent (*incongruent*).

Fifth UN Congress (1976) stated that the term policy comes from English *policy* or in Dutch *politie*. Black's Law Dictionary identifies *Policy* as: The general principles by which a government is guided in its management of public affairs,... or principles and standards regarded by the legislature or by the policy should be coordinated and the whole should be integrated into a general social policy of each country. "

Sudarto (1965) stated that the crime prevention policy or commonly known as "criminal politics" according to Sudarto is a rational effort from the community in tackling crime. This definition is taken from the definition of Marc Ancel who formulated criminal politics as " *the rational organization of the control of crime by society* ", Marc Ancel, *Social Defense* (translation of *La Nouvelle Defense Sociale*),

The purpose of dealing with crime is to protect the community to achieve community welfare. The formulation of the objectives of such criminal politics is stated in one of the 34th training course reports organized by UNAFEI in Tokyo in 1973 as follows: *Summary Report, Resource Material Series Most of the group members agreed some discussion that "protection of the society" could be accepted as the final goal of criminal policy, although not the ultimate aim of society, which might perhaps be described by terms like "happiness of citizens", "a wholesome and cultural living", "social welfare" or "equality"* (UNAFEI, 1974: 95)

Agreement on the results of the course can be a foundation in criminal policy as an effort to tackle crime for *social welfare* and *social protection*.

## B. Criminal Law Countermeasures

The use of criminal law in regulating the public (through criminal legislation) is essentially part of a policy step (*policy*). Furthermore, to determine how a rational step (effort) in conducting a policy cannot also be separated from the objectives of the development policy itself integrally. Thus in an effort to determine any policy (including criminal law policy) is always related and cannot be separated from the national development goal itself, namely how to realize prosperity for the community.

Nawawi Arief (2006) stated that crime prevention policies or commonly known as "*penal policy*" According to GP Hoefnagles can be pursued by:

1. The application of criminal law (*criminal law application*)
2. Prevention without crime (*prevention without punishment*)
3. Influencing the public's view of crime and punishment through mass media (*influencing views of society on crime and punishment*)

The first category is categorized into efforts to overcome crime through the *penalty* line, while the second and third includes efforts to overcome crime through

the *non-penalty* line. With regard to the 2 (two) facilities, Muladi (2002) emphasized that: Criminal policy is a rational and organized effort of a society to tackle crime. Criminal policies aside from being repressive through the criminal justice system (the *penal* approach) can also be carried out by means of " *non-penal* " means through various prevention efforts without having to use the criminal justice system, for example efforts to improve community mental health, legal counseling, legal reform and civil law administration, and so on.

The *non-penal* approach covers a very broad area of *crime prevention* and covers both policy and practice. *Non-penal* means are basically preventive measures, starting from the education of the code of ethics to the renewal of civil law and administrative law. The policy varies from one country to another according to the cultural, political and intellectual backgrounds that exist in each society.

Furthermore, criminal policy (*criminal policy*) which includes a *penal* approach through the criminal justice system, it will naturally come into contact with criminalization that regulates the scope of acts that are against the law, criminal liability, and sanctions that can be imposed, both in the form of a criminal (*punishment*) and actions (*treatment*). It is means of crime prevention policies are carried out using the means of *penal* (criminal law), then criminal law policy (*penal policy*) must pay attention and lead to the achievement of the objectives of social policy in the form of *social welfare* and *social defense*.

Tackling crime must have a balance between the means of *punishment* and *non-reasoning* (integral approach). From the perspective of criminal politics, the most strategic policy is through *non-penal* means because it is more preventive. Even so, *penal* policies are still needed in the prevention of crime, because criminal law is one of the means of social policy to channel " *social dislike* " or *social disapproval/ social abhorrence* which is also expected to be a means of social protection (*social defense*). The means of " *penal* " is " *penal policy* " or " *penal law enforcement policy* " very vital role in the process of law enforcement to tackle crime. The 3rd criminology seminar in 1976 in one of its conclusions stated:

Criminal law should be maintained as a means of *social defense* in the sense of protecting the public against crime by repairing or *rehabilitating* the creator without reducing the balance of the interests of the individual (maker) and the community (Muladi & Nawawi Arief, 1998).

Muladi (2002) also emphasized political crimes committed by means of *penal* means the use of the criminal justice system, ranging from criminalization to the criminal execution. The approach by means of *punishment* must be continuously carried out through various efforts to improve the criminal justice system, both from the aspect of legislation (criminalization, decriminalization and *depenalization*), improvement of system infrastructure, improving the quality of human resources, and increasing public participation in the criminal justice system. Systemically, the criminal justice system includes a network of justice systems (with sub-systems of the



police, prosecutors, courts and penal) that utilize criminal law as its primary means. Criminal law in this case includes material criminal law, formal and criminal law.

The operationalization of legal policies by means of "penal" (criminal) can be done through a process that consists of three stages namely:

1. Formulation stage (legislative policy)
2. Application phase (judicial/judicial policy)
3. Stage of execution (executive/administrative policy).

Based on the description of the three stages of the criminal law enforcement policy contained within three powers/authorities, namely legislative/formulative authority in terms of determining or formulating what can be criminally oriented to the main problems in criminal law include acts that are against the law, error / responsibility what penalties and sanctions may be imposed by lawmakers. The application stage is the power in terms of implementing criminal law by law enforcement officers or the court and the executive/administrative stage in implementing criminal law by the executing / criminal execution apparatus.

### C. Policy Formulation

Judging from the perspective of criminal law, the formulation policy must pay attention to internal harmonization with the criminal law system or the general penal code in force today. It cannot be said that there is a harmonization/synchronization if the formulation policy is outside the current criminal law system

Formulation policy is the most strategic stage of the "penal policy" because at that stage the legislature has the authority to determine or formulate criminal actions which are oriented to the main problems of criminal law, including acts that are against the law, mistakes, criminal liability and witnesses what can be imposed. Therefore, efforts to tackle crime are not only the task of law enforcement officials but also the work of lawmakers (legislative apparatus) (Nawawi Arief, 2012).

Planning (*planning*) in combating crime with the criminal law system at the stage of formulation in essence according to Nils Jareborg covers three main problems in the structure of the criminal law system, namely the problem: Formulation of criminal acts / Criminalization and Criminal Threatened (*criminalization and threatened punishment*)

1. Criminalization (*adjudication of punishment sentencing*)
2. Criminal execution (*execution of punishment*)

In line with the above concept, the draft of the new Criminal Code is prepared by departing from 3 (three) main materials / substances / problems in criminal law, namely:

1. Criminal matters
2. Problems of error or criminal liability.
3. Criminal and criminal matters.

All material/substantive criminal law, formal criminal law and criminal implementation law can be seen as a single unit of the criminal system (*the sentencing*)

system). LHC Hulsman put forward the notion of a criminal system as “*Statutory rules relating to criminal sanctions and crimes*” (*the statute rules relating to penal sanctions and punishment*).

From the above understanding Barda Nawawi Arief provides a broad understanding of punishment as a process of giving or imposing a criminal sentence by a judge, it can be said that the criminal system includes the understanding of:

1. The whole system (laws and regulations) for criminalization;
2. The whole system (the rule of law) for granting or imposing and carrying out criminal offenses.
3. The whole system (statutory regulations) for the functioning or operationalization or concretization of crime;
4. The whole system (legislation) that regulates how the criminal law is enforced or operationalized concretely so that someone is given sanctions (criminal law).

The question of the formulation of a criminal act/criminalization arises when we are confronted with an act that is detrimental to another person or community whose laws do not yet exist or have not been found. In connection with the criminalization policy according to Sudarto, attention needs to be paid to the following core matters:

1. The use of criminal law must pay attention to the goals of national development, which is to realize a prosperous just society that is evenly materially and spiritually based on Pancasila; in connection with this (the use of) criminal law aims to tackle crime and make granting to the act of prevention itself, for the sake of welfare and community protection.
2. Actions that are endeavored to be prevented or endured by criminal law must constitute “undesirable acts”, such as acts that bring harm (material and spiritual) to the community members.
3. The use of criminal law must also take into account the principle of costs and results (*cost and benefit principle*)
4. The use of criminal law must also pay attention to the work capacity or capability of law enforcement agencies, namely the network until there is overloading of the workload (*overbelasting*).

Teguh Prasetyo and Abdul Halim Barkatullah (2005) based on the above considerations, it can be concluded that the reasons for criminalization in general are: The existence of victims:

1. Criminalization is not solely intended for retaliation;
2. Must be based on the principle of *principle ratio*; and
3. There is a social agreement (*public support*)

Criminal law policy issues related to the criminalization of what conduct is made criminal acts and *penalization* such as what should sanction imposed on the offender. Criminalization and *penalization* are central issues for which a *policy-oriented approach is needed*. Criminalization (*criminalization*) covering the scope of an unlawful act (*actus reus*), criminal liability (*mens rea*) and the sanctions to be imposed in the form of punishment (*punishment*) and action (*treatment*). Criminalization must be done carefully, not to create the impression of a repressive violation of the principle

of *ultimum remedium* ( *ultima ratio principle* ) and backfire in social life in the form of excessive criminalization ( *over-criminalization* ), which actually reduces the authority of the law. Criminalization in material criminal law will also be followed by pragmatic steps in formal criminal law for the purpose of investigation and prosecution (Muladi, 2003).

#### D. Law Enforcement Policy

Criminal law enforcement is part of criminal politics as one part of the overall crime prevention policy, indeed the enforcement of criminal law is not the only hope for being able to resolve or overcome the crime completely. This is reasonable because in essence the crime is a humanitarian and social problem that cannot be solved solely by criminal law.

Muladi, (1995: 25-26) highlighted that although criminal law enforcement in the context of overcoming crime is not the only hope, but its success is expected because in this field of law enforcement is at stake the meaning of the State based on law. The role of law enforcement officers in the State based on the law was also stated by Satjipto Rahardjo · Satjipto Rahardjo who stated, "*The law does not have any function, if it is not applied or enforced for lawbreakers, those who enforce the law in the field are law enforcement officers.*" Henry Campbell Black (1999: 797). The term enforcement in English is known as *enforcement* in the *black law dictionary*, meaning *the act of putting something as a law into effect, the execution of a law*. Whereas *law enforcement officer* means *those whose duty it is to preserve the peace*. In a large Indonesian dictionary,

Sudarto (1986) in the same context also emphasized that law enforcement is attention and cultivation, both acts that are against the law that actually happened (*onrecht in actu*) and acts against the law that might occur (*onrecht in potentie*). Meanwhile, according to Soerjono Soekanto, conceptually, the core of law enforcement lies in the activity of harmonizing the values relations that are set out in the rules that are solid and manifest and action attitude as a series of translation of the final stage values, to create, maintain, and maintain peace association of life.

For this reason, Adji (2005) concerned that part of *social policy*, this law enforcement policy covers the process of what is called *criminal policy*. This conception of law enforcement policies will later be applied through the institutional level through a system called the *Criminal Justice System*, hence there is a link between the Law Enforcement Policy and the Criminal Justice System, namely this sub-system of the Criminal Justice System will implement a law enforcement policy in the form of preventing and overcoming the occurrence of a crime in which the roles of this sub-system will become more acceptable together with the role of the community, and without the role of the community, law enforcement policies will not be optimized.

Soerjono Soekanto (2009) stated that the main problem of law enforcement actually lies in the factors that might influence it. According to Soerjono Soekanto the factors that influence law enforcement have a neutral meaning, so that the positive or negative impact lies in the contents of these factors, as follows:

1. The legal factor itself (the law)

2. Law enforcement factors are those who form and apply the law.
3. Factors of facilities or facilities that support law enforcement.
4. Community factors, namely the environment in which the law applies or is applied.
5. Cultural factors, namely as the results of works, inventions, and tastes based on human initiative in the association of life.

These five factors are closely interrelated, because it is the essence of law enforcement, also a measure of the effectiveness of law enforcement. Among all these factors, according to Soerjono Soekanto law enforcement factors occupy a central point as a measure of the extent to which contributions to the welfare of society. Law enforcement is very bound by criminal procedure and proof. Harahap (2000) stated that proof is a problem that plays a role in the process of hearing court hearings. Through proof, the defendant's fate is determined. If the results of the evidence using the evidence determined by the law "are not enough" to prove the guilt of the defendant, the defendant is "acquitted" of the sentence. On the other hand, if the defendant's guilt can be proven with evidence called Article 184 of the Criminal Procedure Code the defendant is declared "guilty". He will be sentenced.

Harahap also highlighted that the Criminal Procedure Code (KUHAP) explicitly mentions several pieces of evidence that can be submitted by parties who litigate before a trial. Based on Article 184 of the Criminal Procedure Code, the evidence is: (1) Witness statement; (2) Expert statement; (3) Letter; (4) Hints; and (5) Defendant's statement.

While the explanation of Article 184 of the Criminal Procedure Code is explained "*In the event of a quick examination, the judge's conviction was sufficiently supported by a valid piece of evidence*". Based on Article 184 and its explanation, it means that except for a quick examination, to support the judge's conviction, more than one or at least two valid evidences are needed. For this matter Article 183 of the Criminal Procedure Code Explanation of Article 184 of Law No.8 of 1981 concerning the Criminal Procedure Code of the State Gazette of the Republic of Indonesia Number 76 is explicitly formulated that "Judges may not impose a crime on a person except if at least two legitimate pieces of evidence he gained the conviction that a crime had actually taken place and that the defendant was guilty of it ". Thus in the Criminal Procedure Code explicitly provides legality that in addition to being based on the elements of the judge's conviction, proof with at least two valid evidences is necessary to support the element of error in determining whether a person is actually proven to have committed a crime or not.

### E. Understanding of Criminal Law Policy

The development of globalization and the advancement of information technology demand the renewal of criminal law as part of the applicable criminal law policy in accordance with the values of Indonesian society. Countermeasures against information technology criminal acts need to be balanced with improvement and development of the criminal law system as a whole, which includes the

development of culture, structure and substance of criminal law. In this case, criminal law policy occupies a strategic position in the development of modern criminal law.

Law policy (*legal policy*) within the meaning of state policies (*public policy*) in the field of law should be understood as part of social policy is the effort each society / government to improve the welfare of its citizens in all aspects of life. This can contain two dimensions that are related to each other, namely *social welfare policy* and *social protection policy*.

While the definition of criminal law according to Sudarto is to contain legal rules that bind to acts that meet certain conditions in the form of criminal consequences. The granting of criminal law in the general sense is a field of lawmakers based on the principle of legality, which originated from the Aufklarung era, which in short reads: *nullum crimen, nulla poena, sine praevia lege (poenali)*. In short, *nullum crimen sine lege* means there is no criminal offense without law and *nulla poena sine lege* means there is no criminal without law. So the law establishes and limits which actions and penalties (sanctions) can be imposed on violators. So to wear *poena* or criminal requires the law (criminal) first.

The definition of legal policy and criminal law above provides a definition of a criminal law policy (*criminal policy / strafrechtspolitik*) as, how to try or make formulate a good criminal law. Such an understanding can also be seen in the definition of "penal policy", proposed by Marc Ancel, that *penal policy* is a science as well as an art which ultimately has a practical goal to enable positive legal regulations to be formulated better and to provide guidance not only to legislators, but also to courts that apply the law and also to the organizers or executors of court decisions (Ancel, & Paul, 1965: 4-5). Ancel argued that the twentieth century criminal law system still had to be created. Such a system can only be devised and refined by the joint efforts of all people of good will and also by all experts in the social sciences.<sup>126</sup> The criminal law system consists of (1) criminal law regulations and sanctions; (2) a criminal law procedure; and (3) an implementation mechanism (criminal).

The definition of the "criminal law system" from Marc Ancel provides A. Mulder's foundation in providing a policy or political understanding of criminal law (*penal policy/Strafrechtspolitik*), to determine:

1. How far the applicable criminal provisions need to be changed or updated (*in welk opzicht de bestaande strafbepalingen herzien dienen te worden*);
2. What can be done to prevent the occurrence of criminal acts (*wat ganggrad worden om strafrechtelijk gedrad verkomen*);
3. The method of investigation, prosecution, trial and criminal conduct must be carried out (*hoe de operating, vervolging, acting en tenuitvoerlegging van straffen dient te verlopen*).

Based on the above policy, efforts and policies to make criminal law regulations which in essence cannot be separated from the purpose of crime prevention. So, the policy or politics of criminal law is also part of criminal politics. In other words, from

the perspective of criminal politics, the politics of criminal law is identical to the understanding of crime prevention policies with criminal law.

## METHOD

Legal research according to Cohen and Olson is "*Legal research is the process of finding the law that governs activities in human society*" legal research is a process that constructs the discovery of legal thinking that governs community activities. In line with this, P. Mahmud Marzuki stated "that legal research is a process to find the rule of law, legal principles and legal doctrines to answer the legal issues at hand".

Legal research is research to find a formulation of legal development. Research is a basic tool in the development of science and technology. This is because the research aims to reveal the truth systematically, methodologically and consistently. Through the research process, analysis and construction of the data that has been collected and processed is carried out. Legal research is a scientific activity that is based on certain methods, systematic and thinking, which aims to study one or several specific legal phenomena, by analyzing them. So that the legal facts are then used as a reference resolution for problems that arise in the symptoms in social and state life. Ashofa (2013: 20-21) states that a qualitative approach which means focusing on the general principles underlying the manifestation of symptom units in human life, or patterns that are analyzed by socio-cultural phenomena using the culture of the community concerned. to get a picture of the prevailing patterns. These patterns are analyzed again using objective theory.

## DIGITAL ASSETS AND MONEY LAUNDERING IN INDONESIA

### I. DIGITAL ASSETS BECOME OPPORTUNITIES FOR MONEY LAUNDERING

#### A. Development of Digital Assets

The industrial revolution has reached the era of 5.0 in which industry 5.0 conceptualized the continuation of the *cloud* and *computer*-based 4.0 industry. Technology 5.0 by using collaboration from biology, for example, is artificial intelligence AI, robotics, *internet of things* (IoT) and *big data*. Reported by *Bluenotes* (2019), according to a 2018 report by Japan's leading business body, the Japan Business Federation (Keidanren), Society 5.0 will depend heavily on AI, robotics, internet of things (IoT) and big data to provide excellence technology needed by Japan to overcome the problem of aging today.

The emergence of Society 5.0 that was echoed by Japan was considered inseparable from the condition of the population in the State of Sakura. The number of young Japanese who are shrinking into the workforce has found the prospect of

having to support a whole generation of old retirees. One of Japan's leading researchers on population trends is Professor Ryuichi Kaneko, a visiting professor at Meiji University and former Deputy Director General of the National Population and Social Security Research Institute. His research shows that based on current trends, Japan's population tends to shrink from 127 million in 2015 to 88 million in 2065 and 59.7 million at the turn of the next century in 2100. As people move towards the turn of the century, many other countries will face the challenges of a labor force that is declining and a rapidly growing population (TechnoZone, 2019).

Indonesia itself has entered the industrial revolution 4.0, in which the industry revolutionary presents disruptive technology that results in rapid changes and has the ability to undermine large companies that were previously pioneers in mastering technology. This phenomenon also allows people to invest in investments with a different model than before by utilizing digital technology as part of the development of information technology. In addition, digital assets are starting to feel the effects of industry development 4.0. One of them we can see from the development of crypto-currency that allows to be able to invest in digital currencies on a P2P basis and not be limited worldwide.

However, technological developments not only facilitate banking-based non-cash transactions, but give birth to financial digitalization in a new platform in the form of digital currency or crypto-currency. The practice developed by Bitcoin and Farad Egypt. In its development, digital-based currencies are able to show a more stable value compared to conventional currency rates. This currency has been used by some of the world community in trade transactions. OJK will only regulate *fintech* business actors whose core business includes deposits (lending funds), lending (fund distribution), capital raising (capital collection), and market provisioning (market provision). Whereas BI will regulate fintech business actors whose main business is in the form of clearing and settlement (settlement of payment transactions).

## B. Blockchain Technology and Its Complexity

As a vast country, Indonesia faces two main challenges in the midst of rapid economic development and national development, namely the urgency of an integrated infrastructure and the credibility of governance in various sectors. Lack of business infrastructure, high cases of corruption in many sectors and *human error* in managing data in both the government and private sectors are still common factors that shape Indonesia's reputation in the eyes of the global community. Regarding data management, the obstacle to achieving accuracy lies in the centralized approach of the internet-based system that was built. A software system that is basically designed to send data from one party to another requires a centralized *server* as a publisher and data manager. When there is a disruption to the *server*, the website cannot be accessed and automatically the user cannot use the service optimally.

*Blockchain* technology was born in response to the concerns of a number of parties about the workings of a centralized software. This technology was born in 2009 at the same time as the emergence of Bitcoin—a virtual currency that is

becoming the current trend. Technology blockchain is the underlying technology Bitcoin goes without relying on server centrally and thus avoid the risk of downtime. The blockchain system comes with changing the centralized approach to decentralized. In principle, blockchain technology conditions each *server* that runs this *software* to form a consensus network automatically to mutually replicate transaction data and mutually verify existing data. Therefore, when one *server* is *hacked*, the *server* can be ignored because it is considered to have data that is different from the majority of *the other server* networks .

This makes blockchain technology relatively far stronger against attacks than centralized technology because there is always at least 1 server running to handle transactions. Blockchain technology allows network consensus to record and validate each transaction so that data that has been entered cannot be falsified, lost or damaged so that it cannot be manipulated by the network provider.

The analogy of how a blockchain works is almost the same as a cash book in a bank which records all transactions made by its users. The difference is that only the authorities can access the transaction information in the bank cash book, while transactions through the blockchain can be seen by all users because the information collected is also distributed to everyone who runs the server. In addition, because server access is granted to everyone, no party can falsify or modify transactions.

The sector that first explored the blockchain was certainly the financial sector. Bank OCBC, for example, conducted a pilot transfer between Singapore and Malaysia branches which proved to only take 5 minutes. Bank Santander, one of the largest in the UK, projects that this technology can save bank operating costs by more than 20 billion dollars per year.

During its development, blockchain technology was also utilized by other sectors. Sony Global Education in collaboration with IBM published articles and diplomas on the blockchain network so that they could not be forged, damaged or lost. In the health sector, its application is carried out on a broader scale by several countries, one of which is Estonia. One patient's record or medical record at hospital A can be accessed by hospital B when the patient is treated at hospital B, in a short time because it has been recorded in the blockchain network .

In the food sector, IBM is collaborating with food manufacturers and distributors to reduce contamination in the global supply chain. Through the blockchain , food transactions around the world can be collected massively, so that if there is a case of food contamination, it is very easy for the relevant authorities to track the source and carry out rapid isolation. Another example is Alibaba in collaboration with Pricewaterhouse Coopers to help solve China's food security. Ernst & Young's accounting and consulting firm, in a different case, launched a blockchain platform to facilitate a shared car ownership scheme. Thus blockchain technology is basically a 'digital transcript' that was created to avoid fraud, but at the same time allows access for third parties as needed.

This technology, which is still very young, has not yet been applied in all fields, and many experiments continue to be carried out by many companies. But I believe in



the future, blockchain technology will change the way the system works as a whole, in the financial sector and also throughout the industrial sector. This system is believed to be effective in promoting transparency, security and accuracy of transaction data.

### C. Crowd Funding

Fundraising, charity, and other social activities can now also be done through startups engaged in *crowd funding*. More precisely, *crowd funding* is a startup that provides a fundraising platform to be channeled back to people in need, such as victims of natural disasters, victims of war, funding the creation of works, and so on. The fundraising is done *online*. One example of the biggest *crowd funding startup* is Kitabisa.com. This startup creates a place where we can help others in an easier, safer and more efficient way.

*bookisa.com* is a fintech startup that provides an internet-based platform for *online* fundraising. In the past, fundraising was generally done conventionally or took to the field, a website of Kitabisa.com now creates a forum for us to be able to help others in an easier, safer and more efficient way. In accordance with the culture in our country, Indonesia, which adheres to the philosophy of mutual cooperation, *Kitabisa.com* is an *online* mutual cooperation platform that allows many people to raise funds with various humanitarian objectives, such as social activities, funding the creation of works, and in the future not close the possibility of donations in order to realize creative ideas in the digital age. But broadly speaking, *Kitabisa.com* is more fundraising for social purposes.

Fundraising activities through Kitabisa.com also pay attention to the security aspect, where all fundraising activities carried out have been ensured to have followed the verification procedures or processes to ensure their accuracy. Besides that, *Kitabisa.com* also tries to monitor every fundraising activity that takes place. Fundraisers must also make financial use reports of funds collected so donors can clearly know where the money they have contributed, for example, is to help victims of natural disasters, medical assistance, various national issues, and other social or humanitarian activities.

### D. E- Money

E-Money or electronic money, as the name suggests, is money that is packaged into the digital world, so that it can be said to be an electronic wallet. This money can generally be used to shop, pay bills, etc. through an application. One of those electronic wallets is *Doku*. *Doku* is an application that can be easily uploaded on *smartphones*. *Doku* is equipped with a credit card link feature and electronic money or *cash wallet*, which we can use to shop both *online* and *offline* anytime and anywhere through the application.

*Doku* is an electronic wallet in the form of the *dokuwallet.com* application that can be easily uploaded on *smartphones*. *Doku* is equipped with a credit card link feature

and electronic money or *cash wallet*, which can be used to shop both *online* and *offline* at various *merchants* that have joined with Doku. The benefits of this service, we can use Doku anytime and anywhere through the application.

Besides that, even if we don't have a credit card or bank account, we can still make transactions *online*. We can also pay household bills such as electricity, telephone, PAM, installments and other payments through Doku. Uniquely, when you run out of cash or balance from your Doku account, you can also request and receive money from fellow Doku users, the way you can learn from the website. Doku is also trusted as a service that applies security standards in accordance with applicable regulations.

### E. Insurance

The type of startup engaged in insurance is quite interesting. Because usually insurance that we know so far is conventional insurance, where we set aside some money per month as a mandatory contribution to get benefits from such insurance in the future, this type of startup insurance does not all work that way. There is also an insurance startup that provides services to its users in the form of information about the nearest hospital, trusted doctor, hospital reference, and so on. *HiOscar.com* is a startup type like this. This startup was built with the aim of providing a simple, intuitive, and proactive way to help its customers navigate their health system. This startup collaborates with providers or with world-class doctors and the best hospitals who want to work together to help manage the health of their members.

*HiOscar.com* was founded in 2012 in New York, Texas and California, which provides a *platform* for your health care plan. How is this health insurance startup different from conventional insurance? *HiOscar.com* was built with the aim of providing a simple, intuitive, and proactive way to help its customers navigate their health system. The high cost of hospitals in the United States encourages this startup to provide services to the community to get easy access to better and more efficient health care. In order to meet the needs of these customers, *HiOscar.com* collaborates with providers or with world-class doctors and the best hospitals who want to work together to help manage the health of their members. Oscar also strives to be a provider of accurate and consumer-friendly health services. Oscar currently has 135,000 patients who prove that the startup is successful and will continue to grow in the future.

Through *HiOscar.com* we can do routine maintenance at an affordable cost. In addition, we can also get health guidance from expert doctors, nurses, and treatment guides as well as possible, and find doctors who understand the health schedule that you want to go through for the whole body, while saving money. Consulting or talking directly by phone for free with a great doctor is also not a taboo thing to do at *HiOscar.com*.

## F. P2P Lending

*Peer to peer* (P2P) Lending is a startup that provides an *online* loan platform. Capital affairs which are often considered the most vital part of opening a business, gave birth to the idea of many parties to set up this type of startup. Thus, for people who need funds to open or expand their businesses, now they can use startup services that are engaged in p2p lending. Uangteman.com is an example of a startup engaged in this field. This startup aims to meet the *financial needs of the* community by simply filling out a form on the Uangteman.com website in about 5 minutes, and fulfilling its requirements. Read:

Realizing your dream of opening a business or meeting your needs when finance is running low is now easier. Especially for those of you who don't have an account at a bank or other financial institution. How to? The answer is the startup Uangteman.com which provides a P2P Lending platform or *online* loans for various purposes, both consumptive and productive. Uangteman.com gives you the opportunity to be able to make loans *online*, for example to open a business. This startup aims to meet your *financial* needs in an easy way, and can be accessed anywhere and anytime.

How to get a loan by simply filling out a form on the Uangteman.com website in about 5 minutes, and fulfilling its requirements. The application filling process is up to the process of disbursing loan funds in just 2 working days. The establishment of P2P Lending startups like Uangteman.com makes people no longer need to worry to get the funds needed. Not only to open a business but also when not yet payday, to pay for children's schooling, buy electronic goods, and others. Even the nominal amount that we have to pay at the end of the loan period will be exactly the same as the original information when filling out the loan application.

## G. Payment Gateway

The growth of e-commerce companies also triggers more startups to become a bridge between e-commerce and customers, especially in the case of payment systems. The service provided by startup for e-commerce is called the payment gateway service. Payment gateways enable people to choose a variety of digital payment gateways (digital payment gateways) managed by a number of startups, thereby increasing e-commerce sales volume. Payment gateway one of which is *iPaymu*.

The proliferation of *online* businesses today has begun to change people's habits in shopping. No exception in the payment method. Now, the public is offered a variety of digital-based payment methods (*digital payment gateways*) that are managed by a number of *start-ups*. One of them is *iPaymu*.

*iPaymu* (PT Inti Prima Mandiri Utama) is a method of *online* payment or money transfer that serves to facilitate users in making transactions using internet services. Not only for shopping *online*, users can make payments for certain products, subscription products, donations, sending money, and withdrawing

money. Founded in 2012, iPaymu continues to improve its services. At the end of 2013, for example, iPaymu launched a Quick Response Code (QR Code) based payment solution. With iPaymu solution, in addition to being able to make *online* transactions faster, it is hoped that a sense of security, comfort and trust will be created between buyers and sellers.

The presence of the QR Code-based *mobile payment* feature is inseparable from one issue related to online shopping, namely payment system security. Although online stores already offer a method of payment with multiple layers of security, doubt still surrounds a number of people with its security.

So, with this service, iPaymu account holders can enjoy payment transactions, check balances, and withdraw cash orders directly from the cell phone quickly, safely, and comfortably. This service can also be an alternative device for payment of debit and credit card transactions with *Electronic Data Capture* (EDC) owned by banks in large companies. In addition, iPaymu uses 256 bit SSL *encryption* and has been verified by Thawte. But, users still have to maintain the confidentiality of the *username* and *password* and are advised to change the *password* regularly to prevent misuse by unauthorized parties.

To realize the speed, convenience, and security of the service, this startup has integrated its payment system with national and international banking networks and developed a payment system that guarantees the security and convenience of *online* transactions via the internet or *mobile phone*.

All *merchants* that have been certified by this startup will get a "Safe Shopping" Certificate from iPaymu. To get the certificate logo, the *merchant* must first apply for *merchant* certification to iPaymu. In addition, this startup has also collaborated with more than 21 thousand *ATM Bersama* networks, Link, Prima, Alto, Visa, Master Card, and JCB. Synergy is also carried out by iPaymu with Pos Indonesia. Concretely, iPaymu users can withdraw money through the post office. Not only that, now iPaymu also accepts transactions through PayPal.

There are three types of user accounts offered, namely Personal, Business, and Enterprise. Interestingly, there are no monthly fees charged to users. Registration for all three types of users is also free. However, there are differences in withdrawing funds to a bank account. In the Personal type, withdrawing funds to a bank account takes seven days. In the type of business, the time required is three days. Funds withdrawals to bank accounts in *real time* can be enjoyed by Enterprise users. In order to enjoy *real time* services, users must *upgrade their* membership to a Business account with a minimum withdrawal of IDR 10 million or Enterprise with an unlimited number of withdrawals (terms and conditions apply). Other services that can be enjoyed by all three types of user accounts include transfers between *users*, bulk transfers, and sending bills. Each transaction is subject to a fee of 1% for users who use eWallet Debits. The percentage of transaction costs is greater if the user uses a credit card. Funds withdrawal or transfer through eWallet Debit and post offices are also subject to fees that vary in amount.

## H. Remittance

Remittance is a type of startup that specifically provides international money transfer services. Many of these startup *remittance* establishments are in order to help people who don't have an account or access to banking. The existence of this type of startup is very helpful for migrant workers or anyone who might be a member of his family abroad, because of the easy delivery process and lower cost. In Singapore, for example, stood a fintech startup named SingX. Fintech startup in Singapore SingX Pte Ltd has launched an *online remittance platform* that is faster, safer, more convenient and cheaper for consumers than they usually pay when sending money abroad.

The launch of the *online remittance* is supported by American Express Bank and DBS which aims to help consumers, small and medium businesses in order to save shipping costs by up to 90%. SingX also offers transaction advantages transparently.

SingX has launched the 2017 Singapore-India money transfer service .since mid-January, which allows Singapore-based consumers to send their funds to India. In the long run, SingX plans to expand *the money transfer platform* from Singapore to Malaysia, Hong Kong, Australia and other countries, where it also holds licenses. Atul Garg, SingX CEO said that: "*SingX technology can serve consumers in smarter, faster, smoother and cheaper ways. They no longer need to queue at the bank or fill out forms.*" SingX's *online remittance platform* is quite simple and *user-friendly*. Customers can register an account on the company's website. After document submission and face-to-face verification, his account will be approved and he can start using this service. The customer can send the amount of money he wants to send, to the SingX bank account, and the recipient will receive the money in his country within a few hours after the funds are received from the customer. SingX is a subsidiary of Easy Transfer Pte Ltd, licensed by the Singapore Monetary Authority. SingX also holds a *remittance* license in Hong Kong and Australia.

## I. Securities

Stocks, forex, mutual funds, etc., are investments that are already familiar to you. *Securities* can be said as a type of startup that provides a platform for investing in stocks *online*. An example of a startup is Bareksa.com. Founded on February 17, 2013 Bareksa.com is one of the first integrated *securities startups* in Indonesia that provides a platform for buying and selling mutual funds *online*, providing data services, information, mutual fund investment tools, stocks, bonds, etc. . Read: In line with the rapid development of *Financial Technology* (FinTech) startups in Indonesia, the capital market world has begun to look at these steps to make it easier for people to invest. Bareksa.com is present as an Indonesian online mutual fund marketplace.

Bareksa.com is under the auspices of PT Bareksa Investment Portal, which was established on February 17, 2013, is one of the first integrated *securities startup securities* in Indonesia that provides a platform for buying and selling *online* mutual funds , providing data services, information, investment fund tools, mutual funds ,

bonds and others. The creation of Bareksa.com as an Indonesian online mutual fund *marketplace* is expected to increase public participation in the capital market. Where the *startup* was founded and manned by young people who are experienced in the fields of capital markets, information technology, and digital media. Bareksa.com has a vision and mission to participate in developing the investment world among the people of Indonesia by utilizing information technology and the Internet. Bareksa.com also has ambitions to participate in increasing the world investment exposure to the global market. Even recently Bareksa.com collaborated with Bukalapak.com to sell mutual funds through *an online platform* under the name of BukaReksa service.

In *Bareksa.com*, we can see a variety of comprehensive, in-depth, and *updated* market data, including mutual fund, stock and bond data. In order to facilitate investors and potential investors, Bareksa.com develops and provides various digital tools and applications that are designed to facilitate, search, process, and analyze data relevant for investment decision making.

Latest and relevant news and information are also presented by Bareksa.com, moreover, it also provides a *platform* for investors and potential investors to join, discuss, and share with the investor community *online* so that they can increase our knowledge of each other in capital market world. So with the lack of significant regulation, digital assets are able to have the chance of money laundering.

## II. ACTS OF MONEY LAUNDERING USING DIGITAL ASSET MEDIA

### A. Cases of Money Laundering Using Digital Assets Media

The Center for Reporting and Analysis of Financial Transactions or PPATK found indications of the flow of funds in the crime of money laundering through digital currencies. Acting Director of PPATK Transaction Analysis, Danang Tri Hartono, who gave information to business tempo in central Jakarta Tuesday, December 19, 2019, said the indication was successfully traced because transactions in digital currencies were still carried out by conventional banks. indications of money laundering are from corruption to terrorism. But he was not yet willing to specify which digital currency provider site he intended. PPATK will continue to try its best to explore this indication.

The Center for Reporting and Analysis of Financial Transactions (PPATK) considers the development of virtual money including Bitcoin to be potentially used for money laundering and financing of terrorism. as a financial intelligence agency, PPATK has the attention and priority of tracking transactions that are allegedly related to money laundering and financing of terrorism by utilizing virtual money including Bitcoin.

PPATK formed a *financial technology* (fintech) and *cybercrime* desk , and increased cooperation with members of the National Coordinating Committee on Prevention and Eradication of Money Laundering (TPPU), namely Bank Indonesia (BI), the

Financial Services Authority (OJK), and Ministry of Trade (Ministry of Trade). PPATK also supports BI's policy as the payment system authority which is authorized to issue policies prohibiting the use of virtual money in processing payment transactions, as stipulated in Article 34 of Bank Indonesia Regulation (PBI) Number 18/40 / PBI / 2016 concerning the Implementation of Payment Transaction Processing and Article 8 paragraph (2) PBI Number 19/12 / PBI / 2017 concerning the Implementation of Financial Technology.

The step of the central bank to exercise its authority in accordance with the Law is considered as a progressive effort from the perspective of preventing money laundering and terrorism financing. Although it can be traced, it needs a very hard effort to detect identity, source of funds and the purpose of the transaction using virtual money. Therefore, PPATK as the authority in the field of prevention and eradication of the crime of money laundering and criminal acts of financing terrorism appealed to the public to be wiser in utilizing virtual money, including the use of Bitcoin and the like as digital assets, especially in the context of investment (*speculative investment purposes*).

The presence of the internet brings convenience in carrying out daily activities, including money launderers. Therefore, the term *cyber-laundering* then emerged, whose definition is simply the practice of money laundering carried out in cyberspace, namely through online transactions. In principle *cyber-laundering* is the same as the practice of conventional money laundering which consists of three stages:

1. Placement, placing dirty money into the legal financial system.
2. Layering, transferring or changing the form of money through complex transactions to obscure the origin of funds.
3. Integration, returning money that has been washed so that it can be used safely.

It's just that online transactions offer a wide range, speed, convenience, and low costs for money launderers. In any corner of the world, as long as there is internet access, money launderers can launch the action.

According to laws on crypto-currency such as Supervisory Board Commodity Futures Trading (Bappebti) finally issued Regulation No. 5 of 2019 on Technical Requirements Implementation of the Physical Markets Asset Crypto (Crypto Asset) in Stock Futures. In a statement Chief Bappebti, Indrasari Vishnu Ward signed the regulation on 8 February 2019 to Indotelko. That is regulated in Regulation of the Minister of Trade No. 99 of 2018 concerning General Policy for the Implementation of Crypto Asset Futures and Regulation of the Commodity Futures Trading Regulatory Agency Number 2 of 2019 concerning Operation of Commodity Physical Markets on the Futures Exchange, it is necessary to regulate the technical provisions for the implementation of physical asset market crypto (crypto asset) on the Futures Exchange.

In this rule, it is stated that Crypto Assets, hereinafter referred to as Crypto Assets, are intangible commodities in the form of digital assets, using cryptography, peer-to-peer networks, and distributed ledgers, to regulate the creation of new units, verify transactions, and secure transactions without interference from other parties. While Crypto Asset Physical Traders are parties who have obtained approval from the Head of CoFTRA to conduct Crypto Asset transactions both on their own

behalf, and / or facilitate Crypto Asset Customer transactions. Crypto Asset Customers are parties who use the services of Crypto Asset Traders to buy or sell Crypto Assets that are traded on the Crypto Asset Physical Market.

Crypto Asset Storage Manager is a party that has obtained approval from the Head of Bappebti to manage Crypto Asset storage for the storage, maintenance, supervision and / or transfer of Crypto Assets. Crypto Asset Proof is a document issued by the Depository Manager as proof of ownership of the stored Crypto Asset.

Wallet is a medium used to store crypto assets in the form of coins or tokens. Tokens are a form of Crypto Assets that are made as derivative products from coins. Coins are a form of Crypto Assets that have their own blockchain configuration and have characteristics like the Crypto Assets that first appeared, namely bitcoin. This regulation states that Crypto Assets can be traded if they meet the minimum requirements as follows:

1. Based on distributed ledger technology
2. In the form of Crypto utility (utility crypto) or Crypto Backed Asset
3. Market capitalization value (market cap) is ranked in the 500 (five hundred) large market capitalization of Crypto Assets for the Utility Asset Crypto
4. entered in the largest Crypto Asset exchange transaction in the world
5. has economic benefits, such as taxation, growing the information industry and the competence of experts in the field of information (digital talent).
6. risk assessments have been carried out, including the risks of money laundering and financing of terrorism and the proliferation of weapons of mass destruction. Crypto Assets can only be traded if they have been determined by the Head of CoFTRA in the list of Crypto Assets that are traded on the Physical Market of Crypto Assets. Business actors who have carried out Crypto Asset trading business activities before the enactment of this Agency Regulation must submit a request for registration to Bappebti.

Registration of prospective Crypto Asset Physical Merchants must meet the following requirements:

1. has paid up capital of at least Rp 100,000,000,000 (one hundred billion rupiah) and
2. maintain a final capital balance of at least Rp. 80,000,000,000.00 (eighty billion rupiah).

Crypto Asset Trading can only be facilitated by the Futures Exchange which has obtained approval from the Head of CoFTRA. To be able to obtain approval to facilitate Crypto Asset trading in addition to meeting the requirements as stipulated in the Bappebti Regulation governing the Commodity Physical Market Operation on the Futures Exchange, the Futures Exchange must meet the following requirements:

1. has paid up capital of at least Rp1,500,000,000,000.00 (one trillion five hundred billion rupiah)
2. maintain a final capital balance of at least Rp1,200,000,000,000.00 (one trillion two hundred billion rupiahs)
3. has at least 3 employees who are Certified Information Systems Security Professional (CISSP).

Whereas Crypto Asset Physical Merchants must meet the following requirements:



1. has a paid up capital of at least Rp1,000,000,000,000.00 (one trillion rupiah)
2. maintain a final capital balance of at least Rp. 800,000,000,000.00 (eight hundred billion rupiah)
3. has a minimum organizational structure Information Technology Division, Audit Division, Legal Division, Crypto Asset Customer Complaints Division, Client Support Division, Accounting and Finance Division;
4. have an online trading system and / or means used to facilitate the operation of the Crypto Asset Physical Market connected to the Futures Exchange and the Futures Clearing House
5. have a minimum standard operating procedure (SOP) governing the marketing and acceptance of Crypto Asset Customers, conducting transactions, controlling and supervising internally, settling Crypto Asset Customers disputes and implementing anti-money laundering programs and preventing terrorism funding and proliferation of weapons of mass destruction and
6. has at least 1 employee who is Certified Information System Security Professional (CISSP).
7. Crypto Asset Physical Merchants must save at least 70% of the total  
The Crypto assets it manages, offline or cold storage. Offline storage or cold storage can be done by:
  1. cooperate with the Manager of the Crypto Asset Depository in the context of using token or wallet storage services having their own token or wallet storage system or mechanism.
  2. The remaining Crypto Assets that are stored must be kept safe by the Crypto Asset Physical Traders taking into account risk management.

Based on the Financial Action Task Force (FATF) Report on Virtual Currencies Key Definitions and Potential AML/CFT Risks Bitcoin is one of the new payment methods ( NPM) which includes the use of internet-based payment services ( Internet-Based Payment Services ) is a digital representation of value that can be digitally traded and functions as: (1) a medium of exchange; and / or (2) a unit of account; and / or (3) a store of value, but does not have a legal tender status (ie, when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is neither issued nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users. Virtual currency is distinguished from fiat currency. It is also distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency.

Whereas based on Bank Indonesia Regulation Number 18/40/PBI/2016 concerning the Implementation of Payment Transaction Processing, the understanding of *virtual currency* is: digital money issued by parties other than monetary authorities obtained by means of *mining*, purchasing, or transfer of *rewards* ( *rewards* ) including Bitcoin , BlackCoin, Dash, Dogecoin, Litecoin, Namecoin, Nxt, Peercoin, Primecoin, Ripple, and Ven. Not included in the definition of *virtual currency* is electronic money.

In addition, Bitcoin uses *blockchain* technology that provides solutions to problems that exist in conducting transactions, which are not found in the financial

industry. *Blockchain* technology makes all financial transactions carried out in a *ledger* (digital *ledger*) digitally and not managed by one particular organization or party. This ledger record is distributed publicly and is managed by thousands of computers in the world at the same time, so everyone can know that a transaction has taken place and no one can oppose that fact. These things cause Bitcoin to be the most popular. Allen & Overy, *Virtual Currencies Mining the Possibilities*, 2015. Bitcoin was only developed in 2009 by someone under the pseudonym Satoshi Nakamoto, so that the true identity of the founder of Bitcoin has never been known.

Bitcoin is a *virtual web* currency and is an interesting economic experiment where many people now use it to buy *real items*. Simply put, Bitcoin is cash on the internet, which does not require banks, credit cards, fees, or fears of identity theft as is rife in the *online* world. Some people call it *cash for the internet*. Bitcoin is the latest digital *peer-to-peer* (P2P) currency that can be used to replace cash in *online* trading transactions (Bains, 2015).

Unlike other *online* currencies that are related to banks and use payment systems such as PayPal, Bitcoin is directly distributed between users without the need for intermediaries. Bitcoin combines cryptography and *peer-to-peer* architecture to avoid oversight of financial authorities. Thus, transactions using Bitcoin do not leave a trail because there is no need to pass intermediary institutions such as banks. Bitcoin can be transferred to any country in the world if connected to the internet. Bitcoin will be saved into a bitcoin wallet. The wallet application must be installed on both parties' devices with personal computers or laptops, tablets or smartphones. After installing the wallet application, the user will get a bitcoin address.

At present, the use of Bitcoin is free to operate and has been used by many countries, both as a commodity and to be equalized as a currency in conducting transactions. However, Bitcoin is often misused by criminals to carry out criminal acts (Irwin, 2014).

## B. Bitcoin and Money Laundering in Indonesia

In Indonesia, Bitcoin is widely used by business people in investing and even because it is *pseudonym* (does not use real identity) and decentralized (there is no financial authority or third party who oversees and controls transactions) so that it is often used by criminals in committing criminal acts. Like, money laundering (a process in which the proceeds of crime are then transformed as if it were net money or bought assets). Terrorism funding (providing funds for terrorist activities), and other criminal acts that use the Bitcoin media in transactions. This is a problem for a country in eradicating money laundering and financing of terrorism.

Indeed there are no international rules or standards that apply globally related to *virtual currencies*, especially Bitcoin. However, some countries are currently trying to regulate *virtual currencies* and there are also other countries, such as the United States, China, and Japan, which have regulated them. Based on the recommendations of the *Financial Action Task Force* (FATF) No. 15 it is regulated that each country is required to make comprehensive rules regarding the *New Payment Method* (NPM)

including *Internet-Based Payment Services* (FATF 2015) and each country is required to apply a *risk assessment* before establishing a related business NPM technology (FATF 2012). The need to look at policies or rules made by other countries and FATF recommendations is to find out what and how to regulate *virtual currency* in Indonesia.

Regulations in force in Indonesia related to *virtual currencies* are only prohibited, which refers to Bank Indonesia Regulation Number 18/40 / PBI / 2016 concerning the Implementation of Payment Transaction Processing. Article 34 letter a of Bank Indonesia Regulation states that Payment System Service Providers (PJSPs) are prohibited from processing payment transactions using *virtual currency*. In other words, Bank Indonesia (BI) does not prohibit the use of *virtual currency*, but prohibits PJSPs that have obtained licenses from BI to process payment transactions using *virtual currency*.

The *virtual currency*, specifically Bitcoin, is not a legal payment instrument in Indonesia as regulated in Act Number 7 of 2011 concerning Currency and BI is not responsible for risks arising from the use of *virtual currency* by the public. This regulation does not regulate the risk of using *virtual currency* in criminal financing of terrorism and other criminal acts that use Bitcoin as a transaction medium so that it becomes a loophole for terrorists and other perpetrators to commit their crimes.

In addition, Bank Indonesia Regulation Number 19/12 / PBI / 2017 concerning Financial Technology Implementation has also been issued. In Article 8 paragraph (2) of this regulation it is stated that, "In addition to the obligations referred to in paragraph (1), Providers of Financial Technology are prohibited from carrying out payment system activities using *virtual currenc*." Prohibition of conducting payment system activities using this *virtual currency* is due to *virtual currency* is not a legal payment instrument in Indonesia

There is already a *Bitcoin Exchange* in Indonesia which is an *intermediary* between buyers and sellers of Bitcoin that can make *online* transactions through the indodax.com site (previously: bitcoin.co.id) and allows someone to withdraw rupiah from their *bitcoin wallet* account. *Bitcoin Exchange* in Indonesia provides Bitcoin exchange services in rupiah, and vice versa, although there are no rules that regulate it so that it becomes an attraction for terrorists and other perpetrators in funding terrorism and other criminal acts. In addition, its *pseudonym* and *borderless transaction* are of particular interest because terrorists can transfer Bitcoin across countries easily and quickly without being able to trace their identity.

Seeing this fact, if it is not a concern of the government in terms of regulations, it will be difficult to eradicate funding of terrorism and other crimes because they freely use the internet network used by the *Bitcoin Exchange* and *Bitcoin trading websites* to commit crimes and there is no obligation for *Bitcoin Exchange* to report any suspicious transactions and there is no obligation to implement *Know Your Customer* (KYC). So, as long as the Indonesian government does not recognize the existence of Bitcoin, the application of KYC has no meaning as long as it has not been regulated by the authorities in Indonesia.

There have been a number of cases that have occurred in Indonesia related to the use of Bitcoin as a tool for committing crimes, namely narcotics and terrorism. The use of Bitcoin to launch criminal financing for terrorism has been a concern for a long time by law enforcers around the world. Moreover, since the ISIS (*Islamic State of Iraq and Syria*) uprising in Syria many Bitcoin transactions are used by ISIS groups to fund acts of terrorism. Bitcoin is also widely used by terrorists as a transfer media to fund terrorist activities in Indonesia and to fund foreign terrorists who want to join ISIS.

Examples of terrorism cases related to Bitcoin that have been decided by the Tangerang District Court in 2016 are in the name of Leopard Wisnu Kumala, a suspected bomber in Mal Alam Sutera, who blackmailed mall managers with money requests in the form of Bitcoin. He sent an *e-mail* to the mall manager to ask for money in the amount of Rp300 million in the form of Bitcoin. Because the mall manager only sent a small portion of bitcoin to the suspect's account then the suspect blew up Mal Alam Sutera.

With such a mode, it is feared that it will become a trend of further threats from other terrorists and then the results of the transfer of Bitcoin to terrorists will be used to fund acts of terrorism in Indonesia, such as carrying out bombings in Indonesian territory or other terrorist activities. This is a mechanism for funding terrorism through *self-funded* fundraising.

Recently the Minister of Trade issued Regulation of the Minister of Trade No. 99 of 2018 concerning General Policy for the Implementation of *Crypto Asset*. With the existence of these rules, then bitcoin and other virtual currencies are commodities worth trading as subjects of Indonesian futures contracts on the Futures Exchange. However, is this regulation sufficient to overcome the current situation, where criminals use bitcoin and other virtual currencies to carry out their crimes?

The absence of legislation in force in Indonesia related to *virtual currencies* such as Bitcoin will provide a loophole for perpetrators of crime in committing crimes. The prohibition on using *virtual currency* in Indonesia only causes problems and does not support efforts to prevent and eradicate criminal acts such as terrorism and narcotics.

In addition, the prohibition of Bitcoin in Indonesia has caused economic losses because domestic investors will buy digital assets abroad that have legalized Bitcoin transactions. Finally, many domestic assets flow to other countries. Technology continues to develop and cannot be avoided. When referring to the *principle of neutrality of e-commerce technology* that applies globally, technology can be used for useful purposes as well as for committing criminal acts. That is, the technology itself is innocent, the guilty are individuals who use the technology for illegal activities.

Thus, the government needs attention in terms of *virtual currency* regulation so that the government can monitor as well as obtain digital money transaction data which will later be used to prevent and minimize acts of terrorism and narcotics as well as other financial related crimes. In addition, the government can also prepare to face the development of financial technology in the future.

### III. OPPORTUNITIES FOR DIGITAL ASSET-BASED MONEY LAUNDERING CRIME

If previously the money laundering mode was developed through splitting funds into a number of bank accounts, now as various new business models grow such as *peer to peer lending*, online loans, buying and selling online investments, online insurance policies, the mode of smuggling illicit funds originating from *predicate crime* has great potential to target the *financial technology* (fintech) sector, especially *fintech* which is not registered with state authority (illegal fintech).

Anticipating various modes of money laundering, the *Financial Action Task Force* (FATF) has issued 40 recommendations related to international standards in the area of money laundering and financing of terrorism adopted by the majority of world jurisdictions through the supervision of FATF- *style Regional Bodies* (FSRBs). FSRBs for countries in the Asia Pacific region are handled by the *Asia Pacific Group on Money Laundering* (APG). APG is tasked with evaluating compliance with the fulfillment of 40 FATF recommendations for members, both in terms of *technical compliance assessment* and *asset effectiveness* through *mutual evaluation reviews* (MER) of members every 4 years. Indonesia itself has been a member of the APG since 1999.

In the 2017-2018 range, Indonesia has shown quite good results with improved *ratings* obtained for 2 (two) Recommendations, namely Recommendation 4 regarding the legal framework for confiscation and seizure of assets and Recommendation 8 regarding the legal framework for non-profit organizations, and 2 (two) Immediate Outcome (IO), namely IO2 related to the effectiveness of international cooperation and IO8 related to the effectiveness of confiscation and seizure of assets.

To note, the legal basis for implementing anti-money laundering and preventing terrorism financing (PPT) in Indonesia is contained in several regulations such as Law No.8 Year 2010 concerning Prevention and Eradication of Money Laundering (TPPU) Act, Law No.9 Year 2013 concerning Prevention and Eradication of Terrorism Funding Crime (TPPT), PP No.43 of 2015 concerning Reporting Parties in PPTPPU and POJK No. 12 of 2017 concerning the Implementation of the PPT APU Program in the FSS. Specifically *fintech* P2P lending, its specific arrangement in relation to anti money laundering regulations refers to POJK No. 12 of 2017. It's just that, for reasons of time adjustment, the POJK only came into force in the coming year 2021.

Referring to Article 1 *a quo* POJK, the fintech industry which is an information technology lending and borrowing service provider is categorized as a Financial Services Provider (PJK) in the non-bank financial industry sector. Consequently, Fintech (PJK) must identify, assess and understand the risks of TPPU and / or TPPT related to customers, countries or geographical areas, products, services, transactions or distribution networks.

In addition, the fintech industry will also be required to document TPPU / TPPT risk assessments; consider all relevant risk factors before determining the overall level of risk, as well as the level and type of risk mitigation sufficient to be applied; updating risk assessments regularly; and has an adequate mechanism related to providing risk assessment information to the authorized agencies.

### A. CDD or EDD Obligations

Analyst Senior Executive in Functional Quality Control and Monitoring Supervision Sector-Group Handling APU PPT Financial Services Authority (FSA), Dewi Fadjarsarie Handajani, explained that there are several divisions obligation execution due diligence *customer* by the bank *fintech*, the CDD (*customer due diligence*) in a simple and EDD (*enhance due diligence*). Simple CDD, must be *fintech* PJK for low-risk customers TPPU / TPPT, while EDD must be done for high-risk customers / customers. The CDD and EDD processes are included in the APU PPT implementation scheme as stipulated in POJK No.12 of 2017 concerning the Implementation of the PPT APU Program in the FSS. It is important to note, Dewi said that the implementation of the PPT APU obligation specifically for P2P Lending fintech will only take effect in the coming year 2021. The CDD process includes identification, verification and monitoring by the PJK to ensure the transaction is in accordance with the profile, characteristics and / or transaction patterns of Prospective Customers, Customers or WIC. Whereas EDD is a more in-depth CDD action undertaken by PJKs against high-risk prospective customers/clients/WIC such as having background, identity and history that are considered high risk of conducting TPPU and / or PEP, including *Political Expose Person* (PEP). For example, to conduct EDD, PJK can create a customer profile. From that profile, PJK must know the funding portfolio of both lenders and debtors. Not just the background / identity of lenders and debtors, PJK also needs to make a range of transactions. For ranges below Rp. 50 million, for example, they are classified as low risk transactions so there is no need to get extra supervision. If transactions in the range of Rp 50 million to Rp 500 million are categorized as medium risk, while high risk that requires extra strict and important supervision by EDD is in the range of transactions above Rp 500 million.

Furthermore, the risk also depends on the nominal, then monitoring is done afterwards. There it can be seen that what is called the risk base approach is not necessarily beaten all flat. It can be seen in accordance with the profile. In addition to the nominal transaction value, the high risk AML category can also be seen from the size of the company, the form of the company (foundation/cooperative/limited company), customer profile, regional location, the field of corporate services to the *Beneficial Owner* (actual beneficial owner / BO) of the corporation.

A clear example, foundation customers are considered to be at higher risk of being exposed to TPPU/TPPT if affiliated with NGOs engaged in activities related to radicalism, otherwise if the foundation is engaged in education the risk is moderate. Another example, large companies with more employees, subsidiaries

spread across several regions and have a more *sophisticated* transaction system can also be categorized as *high risk* AML.

Each OJK supervisor, will make an individual risk assessment of all PJKs and do a mapping related to the level of transaction risk *safety* in all of these lines. When the transaction category is in the form of a *high risk* AML, OJK will conduct PPT APU checks every year. For AML the *middle risk* category, the inspection is conducted every 2 years, while for *low risk* in the range of 3 years.

With regard to foreign PEPs, in addition to implementing CDD, the PJK fintech also needs to conduct EDD periodically, at least by analyzing information about customers or *beneficial owners*, sources of funds and sources of wealth. Even if CHD fintech business relations or transactions originating from High-risk countries published by the FATF, it is important take preventive measures (*countermeasures*). There, PJK is not only required to do EDD, but also must ask for confirmation and clarification from the competent authority.

### B. Not Required To Report TKM

The obligation to report suspicious financial transactions (TKM) by *fintech* P2P Lending to the *Financial Intelligence Unit* (FIU), namely PPATK, has yet to be regulated. Supposedly, said Dewi, PJK fintech P2P was also required to report to PPATK, only then was PPATK and law enforcement officers working and ascertained whether in a TKM the TPPU and TPPT practices were actually carried out. The importance of reporting TKM to PPATK, he said because OJK only functions as a supervisor who ensures that PJK fintech has implemented APU PPT properly.

When referring to the definition of PJK in Article 1 paragraph (4) Perka PPATK No. PER-09 / 1.02.2 / PPATK / 09/12 concerning Procedures for Submitting Suspicious Financial Transaction Reports and Cash Financial Transaction Reports for Financial Service Providers Customers, indeed P2P Lending is not included in the PJK category which is required to report TKM based on the *a quo* PPATK Perka, only the fintech *payment gateway* entity is regulated. Although there is no P2P obligation as a reporter, there is still no obstacle for the public to report to PPATK.

When confirmed, the Head of PPATK Ki Agus Ahmad Badaruddin said his party was still in the process of reviewing the reporting obligations of TKM by fintech P2P Lending to PPATK. "There is no regulation about Tkm to PATPK.

### C. Illegal Fintech and Money Laundering

To note, Indonesia through the Financial Services Authority (FSA) has now stopped the operation of 803 *illegal fintech* entities. So far, Dewi also mentioned that sanctions obtained by *illegal fintechs* were indeed limited to stopping company activities such as blocking in collaboration with the Ministry of Information and Communication (Communication and Information). While the United States (US) did not even hesitate to take legal action against *fintech* entities that do not comply with

federal *Anti-Money Laundering* (AML) provisions. The action was taken through the US financial audit authority, the *Financial Crimes Enforcement Network* (FinCEN) which is under the Ministry of Finance.

The first *Fintech* said to have to deal with US AML law enforcement in the form of fines worth US \$ 700 thousand, namely Ripple Labs. Ripple Labs at that time carried out its activities without being *legally* registered. So firmly the US law provides sanctions against *illegal fintech* in line with the high awareness of the US authorities about the dangers of the circulation of funds from money laundering in the *fintech* industry. If registered, it is clear that it will make it easier for FinCEN to detect sources and inflows of funds in and out, so that the money supply chain from TPPU can be easily broken.

TPPU expert, Yenti Ganarsih, said that any industry based on digital technology would indeed be very vulnerable to being a means of money laundering if the government control function did not go well. In the politics of anti-money laundering law, all business activities that can raise funds and enter capital must be applied to reporting obligations. If technically the transfer of funds is done through a bank, the bank should automatically be obliged to report the transaction to PPATK if the transaction value is above Rp 500 million.

It is a problem, he said, if P2P Lending does not cooperate with the Bank in conducting transactions, so PPATK will have difficulty *sniffing out* indications of AML violations because it does not get reports from the Bank. Conversely, the origins of large amounts of transactions thought to originate from proceeds of crime can be easily tracked by the formal system of government through reporting obligations. Finally, through its data, authorities can track the source of the flow of funds more quickly and efficiently.

The Chairperson of the OJK Investment Alert Task Force, Tongam Lumban Tobing, reminded that all P2P Lending *fintechs* were required to register their company in the OJK in accordance with POJK No. 77 / POJK.01 / 2016 concerning Information Technology-Based Money Lending and Borrowing Services. The reason for the compulsory registration is called Tongam, which cannot be separated from fears of the tearing of TPPU / TPPT practices in the *fintech* industry. If it is not registered with the OJK, he said, financial statements related to *fintech* funding sources will be difficult to trace.

The Task Force's steps to anticipate this, the Task Force announced to the public that the community does not participate in *illegal fintech* activities as well as blocking related to illegal *fintech* sites or applications through the Ministry of Communication and Information. After that, Tongam said that his party would submit information related to the TPPU's indication to law enforcement.

Regarding sanctions, there are no specific criminal provisions governing the matter of *fintech*. So that when a crime occurs, he explains that the sanctions are still included in the category of general criminal offenses that are snared using the Criminal Code, be it fraud fraud. If the billing is disturbing then it can be included in the snare of unpleasant acts or even can be sanctioned using the provisions of the ITE Law.



Bank Indonesia (BI) prohibits the use of virtual currencies like Bitcoin as a means of payment. In its policy, other than rupiah, there is no other legal currency as a means of payment. Responding to this, the CEO of Bitcoin Indonesia, Oscar Darmawan said that his company strongly supports BI's policies. Oscar also said that his company agreed that transactions in Indonesia must use Rupiah.

Quoted from Indoprimer that the last few years, we often hear about cryptocurrency or known as digital currency. Cryptocurrency is a technology making digital currencies that uses cryptography for security that makes it, so it cannot be falsified. Over time, this technology is increasingly popular and continues to be developed by various companies and teams of experts in various parts of the world to be able to cause a 'hot fund' raising trend where a start-up generates millions of dollars in capital by issuing virtual tokens to investors in exchange for money. The company offers digital tokens (ICOs) that can be used to pay for goods and services on their platforms or saved as investments using blockchain technology, create whitepapers as platforms, software or products they want to build, then people buy these tokens using crypto received broadly (like bitcoin) or fiat currencies for example USD.

In cryptocurrency, the price value is determined by the 'buy and sell' power of the users of this technology, meaning that we can buy at low prices and sell at high prices or buy when there is an opportunity to rise and sell when prices are higher than the purchase price. But because the basic value of cryptocurrency is purely based on the strength of 'buy and sell' and the absence of supervision from the relevant financial departments and clear legal rules, it is not uncommon for cryptocurrency to have a value of more than 20% down in a trading day that is actually used to make a profit. According to Smith + Crown, a blockchain research and consultancy group, said that start-ups have raised more than one billion dollars this year in coin sales and in recent months, only four crypto projects have raised more than \$ 660 million combined. Since the birth of bitcoin digital currency and blockchain technology in 2008, the two jargons have been quite controversial, due to their pseudonym, decentralized and encrypted nature, making it difficult to track every transaction made, and the individuals behind it. In addition, cryptocurrency uses peer-to-peer technology so that the process of sending money is faster, cheaper, more extensive and safer than using ordinary banking services, especially utilizing Western Union services. Theoretically, anyone who has an internet connection and a digital wallet can be part of a coin sales event.

But the ease with which this technology is triggered concerns for many because it can be used as a money laundering facility or to fund terrorist activities and engage in other fraudulent behavior - especially in countries where corruption is rampant. On August 1, the Singapore Monetary Authority (MAS) as the financial regulatory body and Singapore's central bank said in a newspaper that the ICO "is vulnerable to the risk of money laundering and terrorist risk because it is anonymous in conducting transactions, and concerns the ease of large and fast amounts of money. go up in no time. Meanwhile, a legal entity in the United States, the Securities and Exchange Commission (SEC) provides guidance on its website so that investors can consider before participating in the sale of digital tokens. The SEC

asks potential buyers to look carefully and identify investment schemes that are not true.

Although terrorism financing is not uncommon in Asia Pacific compared to the Middle East or North Africa, experts told CNBC that crypto-essence money laundering was a major concern among the authorities. To avoid fraud or money laundering, fundraising companies are asked to do customer due diligence, certify their identity and track their source of wealth and require companies to arrange their products, a process that is sometimes expensive according to Phillipps, who previously worked with Australian regulators Securities and Investments Commission. Phillipps said ICO and cryptocurrency were only new avenues for old age problems: "People are endlessly looking for ways to avoid going through all the efforts of regulation, compliance and so on."

Responding to concerns about cryptocurrency opportunities as a money laundering container, this blockchain-based system is actually considered to be uncomfortable for 'unscrupulous individuals' who want to try to misuse because every digital token transaction is recorded permanently in a digital ledger that can be seen publicly, allowing investigators to track the person who has done a transaction and what matters related to their activities regarding the cooperation.

To the CNBC, the experts also added that with the inclusion of ICO on a large scale, it means that there are now hundreds of obstacles that can be imitated by criminals. At the same time, there have been developments in exchanges that may have tended not to cooperate with the authorities. It has already recorded more than 500 cryptocurrency created based on coinmarketcap.com. Even Google Ventures also invests in one of these Cryptocurrency technologies. Some cryptocurrency has a variety of different concepts and some have concepts that mimic other coins. Experts say the process on the ground makes ICO a perfect vehicle for money laundering, for example when Innocent Bob buys a digital token in the hope he can sell his shop later at a higher price on the main exchange (which spends money to record customer information to match regulatory regulations), or he can switch to fly-by-night exchanges where prices are better. Prices are better on the second exchange because of money laundering candidates, Dirty Harry is willing to pay a premium to launder their funds. Dirty Harry, who wanted to make his dirty money look clean, bought a digital token from Bob. Then Bob makes more money than he has on a more regular exchange, and Harry now has digital tokens that are not related to criminal companies. Harry can then go to any exchange and sell his digital tokens for digital currencies or general fiat according to the prevailing currency in the country.

Alternatively, criminals could have bought the ICO themselves, hoping that novice technology would not have strong know-the-customer practices. In order to track and prevent and protect investors from fraud, many argue that emergency crypto requires some form of regulation - especially digital coins which sometimes act like securities but are not subject to strict main regulations. Seriously addressing the issue, late last month, the Securities and Exchange Commission released an investigative report that said companies planning to use ledgers or buffering devices that could be used to raise capital should take appropriate steps to comply with US federal securities laws Union. The Singapore MAS also clarified this week that it

would regulate the sale of digital tokens in the city-state if the product is regulated in Singapore's securities and futures regulations. After regulatory oversight of the ICO, several sources told CNBC that the benefits would be seen clearly. Most agree that having the right rules can protect investors in the same way that is maintained in the securities market.

Having the right regulations is expected to gain more traction, especially among retail investors. This can be seen from the Data Tokens released by Smith + Crown, which show that in the first half of 2017, there were more sales than in 2016, with the number of fundraising increasing from month to month since March. Data Tokens are another site that tracks future token sales, listing dozens of ICOs in the coming months.

Kapron explained that, at present, to invest in ICO, people need to have some technical understanding and interest in this matter. This is needed to buy ethereum or bitcoin and then invest in coin sales. While the current environment is limited to a subset of investors, he said regulations would be very useful when investing in ICO so that it would be easier to invest and therefore more people would be involved without having to realize the risks or challenges behind several platforms.

However, there are also many general criticisms made on the sale of tokens because it is believed that many beginners 'play' but do not have the experience or a decent business model. In other words, there is a possibility that bigger businesses fail and investors cannot return their money. In contrast, in a venture fundraising round, investors consider the viability of a start-up business plan as an executive strategy before supporting it. VC-supported founders are obliged to answer their investors.

"Tokens are not dilutive, (usually) do not have voting rights, and have very few rights, if any, attached to them. They are not in debt, who enjoy mandatory payments in the event of failure, and also their equity. Give the privileges of some shareholders ordinary vis-a-vis preferred," Justin Hall, principal at the early stage Golden Gate Ventures venture capital, told CNBC.

On the other hand, critics would call back investor protection to dispute the rules, he said, adding it might be difficult to reconcile the two parties. Moreover, Hall said, given how new the technology was, many regulators still "did not fully understand this developing industry." Implementing unplanned policies can be more dangerous than good, he said. To be sure, the SEC and MAS have learned a lot of crypto-crypto. MAS issued a notice in early March 2014 saying that virtual currencies are not regulated, but that virtual currency intermediaries will be regulated for the risk of money laundering and the risk of terrorism. "

That all, of course, raises the question of why someone is interested in buying an ICO that has been overlooked. For most people, the answer is simple: They think there is money to be made. Tee, a veteran of the banking industry, explained to CNBC that a digital token is "a representation of contractual rights in an easily transferable form of media. If the rights associated with tokens fall into the latter category, most jurisdictions will consider it security, "regardless of whether the rights are digital tokens, written contracts or formal security such as stock or debt instruments," Tee said.

At present, to overcome regulatory oversight, many ICOs prevent residents of the United States and Singapore from participating in the sale of their tokens - either by blocking internet protocol addresses from these locations or by relying on self-declarations from participants. But experts told CNBC that people could easily overcome it by using virtual private network connections to cover their locations or simply by asking third parties in different places to participate on their behalf.

#### IV. PENAL POLICY IN THE HANDLING OF DIGITAL ASSET-BASED MONEY LAUNDERING CRIME

##### A. Current Criminal Law Policy towards Countering Money Laundering Crime

The eradication of money laundering in Indonesia has begun with Law No. 15 of 2002 concerning Criminal Acts of Money Laundering. The law has stated that the act of money laundering is a criminal offense. The new thing about this law is the birth of a new institution called the Financial Transaction Reports and Analysis Center (PPATK). Travel Law No. 15 of 2002 a year later amended by Law No. 25 of 2003 concerning Prevention and Eradication of Money Laundering (PPTPPU). Lapse of 8 years later, the Parliament passed Law No. 8 of 2010 concerning Prevention and Eradication of Money Laundering (PPTPPU), Money Laundering cannot be separated from the formulation of criminal law. Criminal law formulation policy is defined as an effort to make and formulate a good criminal law.

This understanding can also be seen in the definition put forward by Marc Ancel which states that *penal policy* as a science as well as art which aims to enable positive legal regulations to be better formulated and to provide guidance not only to the legislators, but also to the courts that apply The law and also to the organizers or executors of court decisions (Nawawi Arief, 2008).

The philosopher Aristotle states that "*a supremacy of law will be far better than compared to the rule of rampant tyranny*". This translation reads, "it is more proper that law should govern than any of the citizens: upon the same principle, if it is advantageous to place the supreme power in some particular persons, they should be appointed to be only guardians, and the servants of the laws"(Aristotle, Politics).

that in the legislative legislation of the Government of Indonesia together with the House of Representatives in the context of handling *money laundering* crimes has formed several legal products to deal with money laundering issues including Law Number 15 of 2002 which has been amended by Law Number 25 of 2003 concerning Eradication of the Criminal Act of Laundering money, and last amended by Act No. 8 of 2010. Crime is a portrait of the concrete reality of the development of the life of society, directly or indirectly, or being sued condition of society, that in social life there is undoubtedly potential vulnerability gap child birth deviant individuals. In society there are struggles of interests that are not always filled with the right path, meaning that there are ways that are not right and violate the law carried out by a person or group of people to fulfill their interests (Wahid & Labib, 2005).

The threat of transnational crime, transnational, has become one of the world's main concerns. Region Southeast Asia or East Asia, which includes Indonesia as

a whole relatively vulnerable to the threat of transnational crime, such as money laundering activities of money laundering almost always involve banks because of the globalization of the banking system through the payment system, especially that of electronic equipment (*electronic funds transfer*), proceeds crimes which in general will flow in large numbers or even move beyond national borders by utilizing bank secrecy factors that are generally upheld by banks. Likewise, not only the legal aspects related to this crime, but also other non-legal aspects such as economic, political, and social culture. Various crimes both committed by individuals and companies within national borders or across national borders are increasing. The aforementioned crimes are in the form of liquor trading, gambling, arms trafficking, corruption, and smuggling. In order not to be easily traced by law enforcers regarding the origin of the crime funds, the perpetrators do not directly use the funds referred to but are attempted to disguise / hide the origin of these funds in the traditional way, for example through casinos, horse racing or entering these funds into the financial system or banking. Efforts to conceal or disguise the origin of funds obtained from these criminal acts are known as *money laundering*.

At present the perpetrators of crimes have many choices about where and how they want the proceeds of crime to be seen as "clean" and "lawful". The development of international banking technology that has given way to the growth of local / regional banking networks into a global financial institution has provided opportunities for *money laundering* actors to utilize the service network which results in money from illegal transactions becoming legal in the business world on international financial markets. At present money laundering activities have crossed the jurisdiction's limits offering a high level of confidentiality or using a variety of financial mechanisms where money can 'move' through banks, *money transmitters*, business activities and can even be sent abroad so that it becomes *clean laundered money*.

The crime of money laundering or *money laundering* is increasingly getting special attention from various groups ranging from the community, academics and state administrators who are not only on a national scale, but also regional and globalized through cooperation between countries. This movement was triggered by the fact that nowadays *money laundering* crimes are rife, while most countries have not established a legal system to combat or define them as crimes that must be eradicated. Such a large negative impact on a country's economy, so that countries in the world and international organizations feel moved and motivated to draw more serious attention to the prevention and eradication of money laundering crimes, so that the creation of law enforcement. Law enforcement in eradicating money laundering in Indonesia is still not optimal. As the main problem in the matter of law enforcement and awareness, it can be pointed out that there is a lack of a harmonious relationship between laws and regulations, law enforcement behavior, law enforcement facilities, and public expectations. As the development of perpetrators and types of crimes of money laundering is not balanced with the human resources of the law enforcers, more and more *money laundering* cases cannot be resolved and dealt with quickly and appropriately because of the lack of quality human resources from the law enforcers themselves. so that if there is a new mode and type of crime for which there is no way

to deal with it and the articles in the Criminal Code that ensnare many law enforcers are inadequate in imposing criminal acts which should be alleged to ensnare them, so that it is necessary to improve the quality of law enforcers themselves to realize law enforcement officials professional.

Improving the quality of law enforcement officers in the framework of the realization of professional law enforcement officers, realized through efforts:

1. provide opportunities for law enforcement officials to attend education and vocational training;
2. organize education and training among fellow investigators in certain cases in order to obtain a common perception in handling criminal cases;
3. collaboration with tertiary institutions to provide education and training in order to increase the knowledge of the investigating apparatus related to the implementation of the task;
4. develop a transparent and professional human resource management system;
5. establish guidelines and procedures for coaching members; and
6. supervise the performance of law enforcement officers fairly.

Improving coordination between law enforcement institutions in order to create synergistic cross-agency relations through:

1. Mapping the problems that arise related to cross-agency coordination;
2. Increasing the formation of cooperation institutions between related agencies;
3. Form a supervisory institution in charge of overseeing the implementation of the tasks of each institution;
4. Integrating and synchronizing community services so that service mechanisms can run simply, quickly and without overlapping;
5. Each agency meets periodically both formally and informally to discuss various problems that arise related to coordination problems as well as finding solutions;
6. Increasing discussion forums and meetings between law enforcement officials aimed at obtaining common ground in carrying out investigative tasks;
7. Prepare MoU which contains cooperation and coordination across agencies related to law enforcement. Seek to establish and / or improve legislation related to law enforcement in order to realize legal certainty.

In terms of state financial interests, the PPATK is given authority by Law No. 8 of 2010 concerning the Prevention and Eradication of Criminal Acts of Money Laundering, to make a temporary stop or delay in transactions containing suspicious transactions. The suspension or postponement is intended to save the state money that is suspected of being the result of *predicate crime* or to cut off the operations of crime organizations to expand their crime networks.

The policy of criminal law enforcement against the handling of money laundering in the context of criminal law reform in Indonesia can be started with the establishment of appropriate legal products through the government and is endorsed by the House of Representatives so that Law Number 8 of 2010 is formed in addition to the products of money laundering crime when this has received special attention from various groups ranging from the community, academia and state administrators who are not only on a national scale, but also regional and globalized through cooperation between countries so that requires the readiness of law enforcement

officials, police, prosecutors, special judges such as PPATK, and One of the significant policies in money laundering is the burden of reverse proof which is considered the most revolutionary policy .

Constraints faced in the application of criminal law enforcement policies against tackling money laundering in the context of reforming criminal law in Indonesia and how to overcome them. The crime of money laundering is increasing and the effect is very large not only is a problem in the field of law enforcement, but also concerns the threat of national and international security of a country, obstacles in dealing with money laundering in addition to investigator resources that are still very limited but also lack of coordination between law enforcement agencies, as well as legislation that overlaps and conflicts with one another.

## B. The Application of Money Laundering Crimes from The Perspective of The Money Laundering Act of 2010

Law No. 8 of 2010 (UUTPPU) is a means to realize the expectations of many parties as a law to anticipate various patterns of crime that lead to money laundering activities. As for who is being targeted in This TPPU Law is to prevent and eradicate money laundering systems or processes in the form of placement, layering and integration. Then because the main targets in money laundering activities are bank and non-bank financial institutions, the regulatory objectives of the UUTPPU include the active roles of these institutions to anticipate money laundering crimes.

Bank and non-bank financial institutions are identified in the regulation of UUTPPU with Financial Service Providers. Financial Service Providers are defined as service providers in the financial sector or other services related to finance including but not limited to banks, financial institutions, securities companies, mutual fund managers, custodians, trustees, depository and settlement institutions, foreign exchange traders, pension funds, insurance companies and post offices. Then many crime handling systems in this law are processed with special criminal procedure law, because the legal principles are *lex specialis* .

Article 68 of this Law stipulates that investigations, prosecutions and examinations are carried out based on the provisions of the Criminal Procedure Code, unless otherwise specified in this Law. From this arrangement it appears that lawmakers want the law to be adjusted more to the nature of the development of the problem of money laundering crimes

Problems are governed by legislation other. Thus it appears that this law does indeed have a *lex specialis* nature and the principles in this law can be exceptions to the provisions of other laws based on the *lex specialis derogate legi lex generalis* principle

Furthermore, crimes that are threatened against those who carry out trials, assistance or conspiracy in money laundering are equated with criminal threats against criminal offenses that have been completed as regulated in article 3, article 4, and article 5 of the UUTPPU. In other words the threat of sanctions that are threatened in article 3, article 4, and article 5 from those contained in article 10 is not distinguished.

The provisions in article 10 of this UUTPPU differ or deviate in principle from the provisions in the Criminal Code, because in articles 53 and 57 of the Criminal Code stipulates that qualifications for trial, assistance or conspiracy are distinguished from qualification from criminal acts that have been completed.

In this UUTPPU INTRAC function becomes wider than sub - earlier law which functions such as :

1. Prevention and eradication of money laundering.
2. Management of data and information obtained by PPATK.
3. Supervision of the reporting party's compliance.
4. Analysis or examination of reports and information on financial transactions that indicate money laundering and / or other criminal acts. With the existence of these functions, the PPATK's authority becomes wider in order to carry out these functions.

The act of blocking of the assets of a suspect or defendant can be carried out if the assets are known or reasonably suspected to be the proceeds of crime. Article 71 UUTPPU determines that investigators, public prosecutors and judges are authorized to order Financial Service Providers to block the assets of every person that has been reported by PPATK to investigators who are known or reasonably suspected to be the result of a criminal offense. In Article 73 of Law No. 8 of 2010 which is evidence in the examination are:

1. evidence as referred to in the Criminal Procedure Code.
2. other evidence in the form of information that is spoken, sent, received, or stored electronically with optical devices or similar devices such as optics and documents; and
3. documents as referred to in article 1 number 16

The provisions in article 1 number 16 of Law No. 8 of 2010 are:

"Documents are data, records or information that can be seen, read, and / or heard, which can be issued with or without the aid of a means, whether stated on paper, any physical object other than paper, or recorded electronically, including but not limited to:

- a. writing , sound or image
- b. map, design, photograph or the like;
- c. letters, signs, numbers, symbols or perforations that have meaning or can be understood by people who are able to read or understand them. "

Evidence used in the examination of a crime of money laundering according to article 73 of Law no. 8/2010 is indeed very diverse. This is clearly a necessity in eradicating money laundering because the problem of money laundering is a very complex problem because of the mode and the crime system practiced by money launderers has involved high-tech equipment.

Unlike the Criminal Code, this UUTPPU determines the minimum and maximum criminal threats. We can see this, among others, in article 3, article 4,



article 5, and article 7 of this law which sets the threat of imprisonment for a minimum of 5 years and a maximum of 20 years and a minimum fine of Rp. 1,000,000,000 (one billion rupiah) and a maximum of Rp. 100,000,000,000 (one hundred billion rupiah).

The specificity of criminal procedure law used by Law no. 8 of 2010 is the implementation of the justice system *in absentia*. Justice *in absentia* is justice done by a court decision in which the defendant was not present although it has been summoned legally in accordance with applicable regulations.

The regulation of the judicial system *in absentia* regulated in article 79 of the Law on Laws is aimed at making the judiciary run smoothly even without the presence of the accused. Another objective is to save property from the proceeds of crime committed by the defendant. Law No.8 of 2010 also adopts a reverse proof system, in which the defendant himself is required to prove his innocence. The provisions in article 77 state: "*For the purpose of examining the court, the defendant must prove that his assets are not the result of a criminal offense.*"

In article 79 paragraph (4) of Law No.8 Year 2010 it is stated that if a defendant dies before a judge's decision is handed down, where there is convincing evidence that the accused committed the crime, then the judge can make a determination regarding the assets of the defendant that has been confiscated to be seized and owned by the state. The provisions of article 79 paragraph (4) are very contrary to the principle of the *presumption of innocence*, where a person cannot be found guilty before a judge's decision states that he is guilty of the charges charged with him.

In contrast to Law No.15 of 2002, in Law No.25 of 2003 there are articles that explain the meaning of money laundering, whereas in Law No. 8 of 2010 the definition of Money Laundering was expanded again to read "Money Laundering is all acts that meet the elements of criminal acts in accordance with the provisions in this Law". In Law No. 15 of 2002, the notion of money laundering is not explicitly explained but only given its categorical meaning (in article 2 of Law No. 15 of 2002). The meaning of money laundering as explained in article 1 paragraph (1) of Law No.25 of 2003 is:

"The act of placing, transferring, paying, spending, granting, donating, depositing, bringing abroad, exchanging, or other acts of assets that are known to be or suspected to be the result of a criminal offense with the intent to conceal or disguise the origin of the assets so that as if it were a legitimate asset . "

In Article 2 of Law No. 8 of 2010 is set on the types of criminal offenses the results of these actions are assets as referred to in Law No.8 of 2010. This is a unique feature of the Money Laundering Law, because this crime is related to other criminal acts referred to as *predicate offences*. As stated in article 2 of Law No.8 of 2010 are: Results of Criminal Acts are Assets obtained from criminal acts, corruption, bribery narcotics, psychotropics, labor smuggling, migrant smuggling, in the banking sector, in the capital market, in the insurance sector, customs, excise,

human trafficking, illegal arms trade, terrorism, kidnapping, theft, embezzlement, fraud, money fraud, gambling, prostitution, in the field of taxation, in the field of forestry, in the field of the environment, in the field of maritime affairs and fisheries; or other criminal offenses threatened with imprisonment of 4 (four) years or more, committed in the territory of the Unitary State of the Republic of Indonesia or outside the territory of the Republic of Indonesia and such crimes are also criminal acts under Indonesian law.

A *financial intelligent unit* usually performs several tasks and authorities, namely the regulatory task, regulating cooperation in the framework of law enforcement, cooperating with the financial sector, analyzing incoming reports, securing all available data and assets, conducting international cooperation and administrative functions general. PPATK as a *financial intelligent unit* also carries out such functions. To carry out its role as a *financial intelligent unit* in efforts to prevent and eradicate money laundering in Indonesia, the PPATK was given the duty and authority of Law No. 8 of 2010 as regulated in Article 39, Law No. 8 of 2010 the main task of PPATK is to prevent and eradicate money laundering. While the PPATK function as regulated in Article 40 of Law no. 8/2010 includes the prevention and eradication of money laundering crimes Management of data and information obtained by the PPATK *Administrative model*, with variations: it is an independent institution under the government, such as AUSTRAC, FINTRAC, FINCEN or under a Central Bank such as in Malaysia (Husein, 2003).

In the provision of Article 41 of Law No. 8/2010, PPATK in carrying out the function of prevention and eradication of the crime of money laundering, PPATK is authorized:

1. request and obtain data and information from government agencies and / or private institutions that have the authority to manage data and information, including from government agencies and / or private institutions that receive reports from certain professions;
2. establish guidelines for identifying Suspicious Financial Transactions;
3. coordinate efforts to prevent money laundering with related agencies;
4. provide recommendations to the government regarding efforts to prevent money laundering;
5. represent the government of the Republic of Indonesia in international organizations and forums relating to the prevention and eradication of the crime of money laundering;
6. organizing anti-money laundering education and training programs; and
7. organize socialization of prevention and eradication of the crime of Money Laundering.

In carrying out the function of data and information management, in accordance with the provisions of Article 42 of Law No. 8 of 2010, PPATK has the authority to administer information systems. What is meant by the information system as set out in the explanation of Article 42 of Law No. 8 of 2010 include:

1. Build, develop and maintain application systems;
2. Build, develop, and maintain computer and database network infrastructure;

3. Collecting, evaluating data and information received by PPATK manually and electronically;
4. Storing, maintaining data and information into a database;
5. Present information for analysis needs;
6. Facilitating the exchange of information with relevant institutions both domestically and abroad; and
7. Promote the use of application systems to the reporting party.

In carrying out the supervisory function on the compliance of the reporting party as regulated in Article 43 of Law No. 8 of 2010, PPATK is authorized:

1. Establish provisions and guidelines for reporting procedures for the reporting party;
2. Establishing service user categories that have the potential to commit money laundering crimes;
3. Carry out a compliance audit or special audit;
4. Delivering information from the results of the audit to the institution authorized to supervise the reporting party;
5. Give a warning to the reporting party that violates the reporting obligations;
6. Recommend to the authorized institution to revoke the business license of the reporting party; and
7. Establish provisions for implementing the principle of recognizing service users for reporting parties who do not have a supervisory and regulatory body.

In carrying out the function of analysis or examination of reports and information, in the provisions of Article 44 of Law No. 8 of 2010 it is regulated that the PPATK can:

1. Request and receive reports and information from the reporting party;
2. Request information from related institutions or parties;
3. Request information from the reporting party based on the development of PPATK analysis results;
4. Request information from the reporting party based on requests from law enforcement agencies or overseas partners;
5. Forward information and / or results of analysis to the requesting agency, both at home and abroad;
6. Receive reports and / or information from the public regarding the alleged crime of money laundering;
7. Request information from reporting parties and other parties related to alleged money laundering crimes;
8. Recommend to law enforcement agencies about the importance of interception or wiretapping of electronic information and / or electronic documents in accordance with statutory provisions;
9. Requesting financial service providers to temporarily stop all or part of a transaction that is known or suspected is a criminal offense;
10. Request information on the progress of investigations and investigations carried out by investigators of original crime and money laundering;
11. Carrying out other administrative activities within the scope of duties and responsibilities in accordance with the provisions of this law; and
12. Forward the results of the analysis or examination to the investigator.

There are two PPATK tasks that are very prominent in relation to efforts to prevent and eradicate money laundering in Indonesia. The first task is to detect the occurrence of money laundering, and the second is the task to assist law enforcement related to money laundering and *predicate crimes*. In carrying out its duties as an independent institution that aims to prevent and eradicate money laundering activities in Indonesia, PPATK will cooperate with many parties. In addition to the police and prosecutors as law enforcement agencies who are authorized to conduct investigations and prosecutions in money laundering, PPATK will also collaborate with Bank Indonesia, the Director General of Taxes, the Director General of Customs and Excise, the Capital Market Supervisory Agency, the Ministry of Finance, the public and other institutions both from within and outside the country. Seeing so many parties involved in the effort to prevent and eradicate money laundering, it can be realized that money laundering is a very dangerous threat that requires cooperation from many parties to be able to deal with it.

## CONCLUSION

The research concluded and highlighted that in order to optimize the results of the research in this paper a number of suggestions are put forward to increase concrete efforts in the politics of criminal law against the handling of digital asset-based money laundering. The development of information technology that is developing now, especially in the field of digital assets is able to become an opportunity for money laundering. The case of committing the crime of money laundering is carried out using the digital currency-based information technology method and can be used for cross-country trade. So that the crime of money laundering based on digital assets is very easy to do and can have a worldwide network. Whereas in the case of the crime of money laundering currently regulated as in Law No. 8 of 2010 concerning TPPU, it is felt to be highly irrelevant, because basically digital assets in Indonesia have no regulations yet.

That politics is a legal product, which in this case digital assets using Blockchain technology based on information technology has been very fast developing in developed countries there are already their own authorities. Because the velocity of money is so extraordinary that it will have an impact on the country. Digital assets should have been made in legislation in order to obtain certainty, usefulness and fairness to their users, and not to use them for money laundering

## REFERENCES

- Adji, I.S. (2005). *Korupsi Sistematis dan Kendala Penegak Hukum di Indonesia*. Jakarta: CV. Restu Agung.
- Ali, A. (2009). *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicial Prudence) Termasuk Interpretasi Undang-Undang (Legisprudence)*. Jakarta: Kencana Prenada Media Group.

- Amrani, H. (2015). *Hukum Pidana Pencurian Uang: Perkembangan Rezim Anti-Pencucian Uang dan Implikasinya terhadap Prinsip Dasar Kedaulatan Negara, Yurisdiksi Pidana, dan Penegakan Hukum*. Yogyakarta: UII Press.
- Amirullah, A. (2003). *Money Laundering, Reorientasi Kebijakan Penanggulangan dan Kerjasama Internasional*. Malang: Bayu Media Publisng.
- Bains, T. (2015). Bitcoin Digital Currency: A Portend for India's National Security, *CLAWS Journal*, Winter 2015, 170-178. [https://archive.claws.in/images/journals\\_doc/1620376481\\_BitcoinDigitalCurrency.pdf](https://archive.claws.in/images/journals_doc/1620376481_BitcoinDigitalCurrency.pdf).
- Bassiouni, M.C. (1978). *Substantive Criminal Law*. Holland: Kluwer Deventer.
- Bellefroid. (1953). *Inleidag tot de Rechtswetenschap in Nederland*
- De Feo, M.A. (1990). Depriving International Narcotics Traffickers and Other Organized Criminals of Illegal Proceeds and Combatting Money Laundering. *Den J.Int LL & Pol'y*, 18(3), 413-446.
- Djamali, R. A. (2003). *Pengantar Hukum Indonesia*. Jakarta: RajaGrafindo Persada.
- Fajar ND, M., et.al. (2010). *Dualisme Penelitian Hukum, Normatif dan Empiris*. Yogyakarta: Pustaka Pelajar.
- FATF. (2014). *Financial Action Task Force (FATF) Report on Virtual Currencies Key Definitions and Potential AML/CFT Risks*, June 2014.
- Fuady, M. (2004). *Bisnis Kotor Anatomi Kejahatan Kerah Putih*. Bandung: Citra Aditya Bakti.
- Harahap, M.Y. (2000). *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang Pengadilan, Banding, Kasasi, dan Peninjauan Kembali*. Bandung: Sinar Grafika.
- Hartono, S. (1991). *Politik Hukum Menuju Satu Sistem Hukum Nasional*. Bandung: Alumni.
- Hardiman, B. (2009). *Demokrasi Deliberatif*. Yogyakarta: Kanisius.
- Hartono, M.D. (1997). *Lima Langkah Membangun Pemerintah Yang Baik*. Jakarta: Ind Hill Co.
- Hoefnagel, G.P. (1973). *The Other Side of Criminology*. Holland: Kluwer Deventer.
- Husein, Y. (2005). *Negeri Sang Pencuci Uang*. Jakarta: Pustaka Juanda Tigalima.
- Husein, Y. (2003). PPAATK: Tugas, Wewenang dan Peranannya dalam Memberantas Tindak Pidana Pencucian Uang. *Paper*, presented on Seminar of Money Laundering, Jakarta, May 6, 2003.
- Indrati, M.F. (2007). *Ilmu Perundang-Undangan: Proses dan Teknik Pembentukannya* Yogyakarta: Kanisius.
- Irwin, A.S.M., et.al. (2014). Money Laundering and Terrorism Financing in Virtual Environments: A Feasibility Study, *Journal of Money Laundering Control*, 17(1), 50-75.
- Irman, T.B., (2001). *Hukum Pembuktian Pencucian Uang*. Jakarta: MQS Publishing & AYYCCS Group.
- Ismawan, I. (2001). *Derivatif Modus Favorit Pencuciang Uang*. Jakarta: Bisnis Indonesia.
- Jaya, N.S.P. (2006). *Bahan Kuliah Sistem Peradilan Pidana*. Semarang: Master of Laws Program Universitas Diponegoro.
- John, G. et al. (2005). *Sejarah Hukum: Suatu Pengantar*. Bandung: Refika Aditama.

- Kaelan. (2001). *Pendidikan Pancasila*. Yogyakarta: Paradigma.
- Kusumaatmadja, M. (1986). *Hukum, Masyarakat dan Pembinaan Hukum Nasional: Suatu Uraian Tentang Landasan Pikiran, Pola Dan Mekanisme Pembaharuan Hukum Di Indonesia*. Bandung: Binacipta.
- Laksmi, S.W. (2017) Terrorism Financing and the Risk of Internet-Based Payment Services in Indonesia. *Counter Terrorist Trends and Analyses*, 9(2), 21-25. Retrieved from [www.jstor.org/stable/26351496](http://www.jstor.org/stable/26351496)
- Mansur, D.M.A., & Gultom, A. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.
- Marzuki, P.M. (2014). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.
- Marzuki, P.M. (2008). Karakteristik Ilmu Hukum. *Yuridika*, 23(2), 15-38.
- Marzuki, P.M. (2014). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.
- Martojo. (2000). *Politik Hukum dalam Sketsa*. Semarang: Faculty of Law Universitas Diponegoro.
- Muladi, M., & Nawawi Arief, B. (1984). *Teori-teori dan Kebijakan Pidana*. Bandung: Alumni.
- Mergenovna Sat, D., Krylov, G.O., Evgenyevich, K., Bezverbnyi, B., Alexander Borisovich Kasatkin, A.B., & Kornev, I.A. (2016). Investigation of Money Laundering Methods Through Cryptocurrency, *Journal of Theoretical and Applied Information Technology*, 83(2), 244-254.
- Mulder, A. (1980). *Strafrechtspolitik. Delic en Delinkwen*.
- Nawawi Arief, B. (2006). *Sari Kuliah: Perbandingan Hukum Pidana*. Jakarta: PT.Raja Grafindo Persada.
- Nawawi Arief, B. (2003a). *Kapita Selekta Hukum Pidana*. Bandung: PT.Citra Aditya Bakti.
- Nawawi Arief, B. (2003b). *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*. Bandung: PT.Citra Aditya Bakti.
- Nawawi Arief, B. (1996). *Bunga Rampai kebijakan Hukum Pidana*. Bandung: Citra Aditya Bakti.
- Nawawi Arief, B. (2010). *Tindak Pencucian Uang, Perkembangan Pembahasan Pencucian Uang Sejak RUU Sampai UU No. 25 Tahun 2003*. Semarang: Badan Penerbit Undip.
- Nawawi Arif, B. (2002). *Bunga Rampai Kebijakan Hukum Pidana*. Bandung: PT. Citra Aditya Bakti.
- Nazir, M. *Metode Penelitian*. Jakarta: Ghalia Indonesia.
- Nitibaskara, T.R.R. (2001). *Ketika Kejahatan Berdaulat : Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi*. Jakarta: Peradapan.
- Nurmalawaty, N. (2006). Faktor Penyebab Terjadinya Tindak Pidana Pencucian Uang (Money Laundering) dan Upaya Pencegahannya. *Jurnal Equality*, 11(1), 12-18.
- PPATK . (2018). *Indonesia Melawan Praktik Pencucian Uang*. Jakarta: PPATK.
- Rahardjo, S. (1985). *Beberapa Pemikiran tentang Rancangan Antardisiplin dalam Pembinaan Hukum Nasional*. Bandung: Sinar Harapan Baru.
- Rahardjo, S. (2009). *Negara Hukum Yang Membahagiakan Rakyatnya*. Yogyakarta: Genta Publishing.

- Rahardjo, S. (2000). *Ilmu Hukum*. Bandung: Citra Aditya Bakti.
- Rahardjo, A. (2002). *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*, Bandung: PT.Citra Aditya Bakti.
- Rahardjo, S. (1980). *Hukum dan Masyarakat*. Bandung: Angkasa.
- Rahardjo, S. (1983). *Hukum dan Perubahan Sosial*. Bandung: Alumni.
- Rajagukguk, E. (2004). *Tindak Pidana Pencucian Uang (Money Laundering) Peraturan Perundang-Undangan*. Jakarta: Lembaga Studi Hukum dan Ekonomi.
- Republic of Indonesia. (2002). *Law Number 15 of 2002 concerning Money Laundering*, LN No. 30 of 2002, TLN No. 4191.
- Republic of Indonesia (1945). *The 1945 Constitution of the Republic of Indonesia and its Amendments*
- Republic of Indonesia. (2010). *Law Number 8 of 2010 concerning Prevention and Eradication of Money Laundering Crimes*.
- Republic of Indonesia (1998). *Law No. 10 of 1998 concerning Amendment to Law No. 7 of 1992 concerning Banking*
- Republic of Indonesia (2009). *Law No. 6 of 2009 concerning Government Regulation in Lieu of Law No. 2 of 2008 concerning the Second Amendment to Law No. 23 of 1999 concerning Bank Indonesia Becomes Law*
- Republic of Indonesia. (2010). *Criminal Law Act Number 8 of 2010 concerning Prevention and Eradication of Money Laundering Crimes*.
- Remy, S. (2005). *Pencucian Uang: Pengertian, Sejarah, Faktor-Faktor Penyebab, dan Dampaknya Bagi Masyarakat*. *Jurnal Hukum Bisnis*, 22(2), 35-52.
- Sasangka, H., & Rosita, L. (2003). *Hukum Pembuktian Dalam Perkara Pidana*. Bandung: Mandar Maju.
- Setiyadi, M.W.R., & Siregar, M.D.A. (2008). *Naskah Akademik Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi*, <http://www.gipi.or.id>
- Shaw, M.M. (1986). *International Law*. London: Butterworths.
- Sherman, T. (1993). "International Efforts to Combat Money Laundering: The Role of the Financial Task Force", on MacQueen L (ed.), *Money Laundering*. Edinburgh, 1993.
- Siahaan, N.H.T. (2002). *Money Laundering dan Kejahatan Perbankan*. Jakarta: Pustaka Sinar Harapan.
- Soewarsono, H., & Manthovani, R. (2004). *Pemberantasan Tindak Pidana Pencucian Uang di Indonesia*. Jakarta: CV.Malibu.
- Soekanto, S., Liklikuwata, L., & Kusuma, M.W. (1981). *Kriminologi Suatu Pengantar*. Jakarta: Ghalia Indonesia.
- Steel, B. (2018). *Laundering-What is Money Laundering*. <http://www.laundryman.u-net.com>.
- Sudarto. (1977). *Hukum dan Hukum Pidana*. Bandung: Alumni.
- Sutedi, A. (2008). *Hukum Perbankan: Suatu Tinjauan Pencucian Uang, Merger, dan Kepailitan*. Jakarta: Sinar Grafika.
- Sutedi, A. (2010). *Aspek Hukum Pengadaan Barang dan Jasa*. Bandung: Refika Aditama.
- Sutedi, A. (2008). *Tindak Pidana Pencucian Uang*. Bandung: PT. Citra Aditya Bakti.

- Syafrudin, A. (2000). Menuju Penyelenggaraan Pemerintahan Negara yang Bersih dan Bertanggung Jawab. *Jurnal Pro Justisia*, 4(2), 125-140.
- Taylor, T. (1999). *Follow The Money Methods in Crime Control Policy, A Study prepared for the Nathanson Centre for the Study of Organized Crime and Corruption*. York University: Toronto.
- Utari, I.S. (2017). *Menyibak Money Laundering & Penangulangannya*. Semarang: BPFH UNNES.
- Von Schmid, J.J. (1958). *Ahli-Ahli Pikir Besar Tentang Negara dan Hukum*. Jakarta: PT. Pembangunan.
- Wahid, W., & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama.
- Warasih, W. (2005). *Pranata Hukum Sebuah Telaah Sosiologis*. Semarang: CV. Suryandaru Utama.
- Wiyono, R. (2014). *Pembahasan Undang-Undang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang*. Jakarta: Sinar Grafika.
- Yuhassarie, E. (2005). *Tindak Pidana Pencucian Uang: Prosiding Rangkaian Lokakarya Terbatas Masalah-Masalah Kepailitan dan Wawasan Hukum Bisnis Lainnya*. Jakarta: Pusat Pengkajian Hukum.