# Legal Action Withdrawal of Assets Proceeding from Corruption Money Laundering through Cryptocurrency

Fidri Sahri[1], Hidayati[2]

{fidrisahri50@gmail.com[1], hidayati@borobudur.ac.id[2]}

Borobudur University, Jakarta, Indonesia[1], Borobudur University, Jakarta, Indonesia[2]

**Abstract.** Money laundering through Cryptocurrency in the form of digital commerce used in electronic transactions is an example of corruption that can harm state finances. The aim of this research is to save national wealth from Cryptocurrency crimes in order to improve the welfare of a socially just society. The method used is normative juridical with secondary data coming from a collection of literary documents, such as books, papers, constitutional laws, and scientific works. The results of this research conclude that the legal action for withdrawal of assets against perpetrators of state financial corruption is based on the applicable ITE Law states that cryptocurrency is lex especially because it regulates more specific matters regarding evidence in the Criminal Procedure Code. Article 73 regulates that electronic evidence can be used as legal evidence and is recognized in procedural law in Indonesia in cases of money laundering crimes.

**Keywords:** Cryptocurrency, Asset Confiscation, and Corruption.

## 1 Introduction

Pancasila is the source of all legal sources from various laws, but in fact, there are still citizens who do not comply with the principles of Pancasila, and there are still officials who violate laws and state mandates, such as corruption. Article 1 Law no. 39 of 1999 concerning Human Rights states that basic human rights are inherent in the person and existence of humans as creatures of God Almighty and are gifts that must be respected, upheld, and protected by the state, law, government and everyone for the sake of honour and protection of dignity. And human dignity. The three reasons for multilevel corruption are caused by greed and lack of resources which is a state of affairs; and third, corruption is caused by opportunity. The criminal act of corruption, as an extraordinary crime, has had various serious, systematic, and massive impacts on national development strategies, including the illegal transfer of state wealth into the hands of corruptors. Through various ways to transfer wealth to the private realm, for example, money laundering which is usually called cyberlaundering and cryptocurrency. Soerjono Soekanto believes that social and technological change will develop simultaneously. Social values, social norms, behavior patterns, organizations, and institutional structures of society can change society.[1] In particular, advances in computer and internet

ICL-C 2023, November 11, Jakarta, Indonesia

DOI 10.4108/eai.11-11-2023.2351302

technology have had a significant impact caused by the emergence of a new forum for criminal acts, known as cyberspace, also known as the virtual world.[2]

Economic crime is increasing throughout the world and there are no national borders. The more complex, organized, and systematic the action, the more difficult it is to investigate. Criminals always try to keep the money they obtain from crime in various ways, such as by laundering money obtained illegally into legal form. By carrying out money laundering, the perpetrator can hide the true origin of the assets obtained from improper profits or results, and by carrying out this activity, the perpetrator can enjoy the results freely as if the assets came from legal actions.[3] One of the new methods that can be used by someone to launder money resulting from criminal acts is laundering money with virtual currency. This technique uses technological advances in the cyber field, also known as cyberlaundering, where internet-based electronic transfer methods are used to disguise the source of illegal funds. This type of crime has increased due to the emergence of virtual currencies that have spread to various platforms. With increasing internet accessibility, many phenomena occur. One of the most prominent is the emergence of electronic currency or cryptocurrency.[4]

Using virtual money, or cryptocurrencies, offers speed, but also raises concerns about abuse that could happen in the unlikely event. All transactions related to cryptocurrency are carried out through digital systems that use electronic technology. The guarantee provides an indicator from a manual system switching to a Cryptographic technology system guarantee, at that time cryptography had a technological meaning that allowed more secure data transmission through a certain system.[5] Bitcoin is one of the most popular examples of virtual money known today. Bitcoin is a virtual currency consisting of crypto assets (cryptocurrency), which differentiates it from physical currency which is usually issued by banks. Because of its virtual form, there are several advantages to using it because there is no need to use third parties such as banks, and transactions can be carried out more quickly, easily, and across borders. In addition, Bitcoin offers confidentiality or anonymity, which provides a high level of protection to its users. In this case, there were several previous cases that occurred in Indonesia. One of them is the case of money laundering via Bitcoin against the fund and insurance finance manager of PT. ASABRI and theft of Citibank customer funds. This case is still difficult to solve until now because the real identity of the Bitcoin transaction perpetrator is still anonymous. In the process of recovering state assets, law enforcement faces challenges because of this problem. Asset recovery should be centered on the goal of distinguishing assets from perpetrators who own them as a result of criminal acts and returning these assets.[6] Bitcoin transactions are personal data that is confidential and therefore difficult to trace, making it difficult for law enforcement to uncover criminal cases via virtual or Bitcoin.

All transactions in cryptocurrency are carried out through digital systems that use electronic technology. The virtual currency itself means digital money created by technology that utilizes a cryptographic system to provide security that they cannot be copied or recreated. Cryptography allows safer data transactions with certain systems.[5] Both advantages and disadvantages can arise from cryptocurrency's relationship with the Indonesian legal system. From a profit point of view, it is easier in a business context, especially in terms of capital markets. However, from a negative perspective, there will be many losses for the country's economy, law, and security. The disadvantage is that cryptocurrency can be used as a new mode for criminal acts. Because there are many criminal acts of corruption involving money laundering which try to disguise funds as well as various information about transactions and where the money comes from, transactions are carried out using electronic systems that are

easily forged in the form of signatures or transaction account codes. The aim of this research is to save national wealth from Cryptocurrency crimes in order to improve the welfare of a socially just society. What is the legal action for withdrawing assets resulting from money laundering corruption via Cryptocurrency?

## 2 Method

The method used is normative juridical with secondary data originating from a collection of library documents, such as books, papers, constitutional laws, and scientific works. In this legal writing, a type of research called analytical descriptive is used. Analytical descriptive is a type of research that aims to describe, explain, and report the condition of an object or event while producing general conclusions about the research subject.[7] The policy of developing criminal law relating to the withdrawal of assets originating from the proceeds of non-corruption in Indonesia is the subject or regulation of the Supreme Court (Perma) adopted. The authors use a normative juridical approach, and secondary data sources that are closely related to their own research in this study. This secondary data source can be described as follows:[8] Primary legal materials include basic norms, such as the 1945 Constitution, basic regulations, statutory regulations, and customary law. The primary legal material used by the author is divided into three: 1) Law Number 2 of 2001 concerning Amendments to Law Number 31 of 1999 concerning the Eradication of Corruption Crimes; 2) Law No. 8 of 2010 amendments to Law number 25 of 2003 concerning Prevention of money laundering crimes; and 3) Law no. 19 of 2016 concerning Information and Electronic Transactions; the secondary legal materials that will be used to convey research results are descriptions that explain statutory or primary legal materials. This may include documents, books, or scientific works, as well as articles from the internet or print media related to the research topic.

## 3 Results and Discussion

### 3.1 Use of Cryptocurrency and Cybercrime Regulations in Business in Indonesia

The Bank Indonesia government is responsible for enforcing the law on the misuse of virtual currency also known as cryptocurrency as a means of payment in Indonesia. However, it is possible that other regulators from the financial services sector will cooperate in enforcing this law. In cases where cryptocurrency is used for money laundering or other crimes, the Financial Transaction Reports and Analysis Center (PPATK) together with the state police are responsible for investigating the case, and the perpetrator will be charged under Law no. 8 of 2010 concerning currency. Physical crypto asset traders can trade cryptocurrencies through Futures Exchanges, Futures Clearing Houses, and Physical Crypto Asset Brokers. This is because users have the ability to exchange Bitcoins with custom-sized wallets.

Commodity Futures Trading Supervisory Agency Regulation Number 5 of 2019 Technical Provisions for the Implementation of the Physical Market for Crypto Assets (Crypto Assets) have been made by the Commodity Futures Trading Supervisory Agency (PeBappebti) on the Futures Exchange. However, cryptocurrencies can only be used as commodities that can be traded on commodity futures exchanges, and may not be used as a means of payment. The purpose of limiting user types is to facilitate monitoring and prevent moral hazard. For example, PT insurance finance. ASABRI and theft of Citibank customer funds, carried out by irresponsible individuals with personal names, or certain collaborations. Therefore, Bappebti Regulation No. 5 of 2019 was created to protect users and traders from unforeseen

circumstances and minimize losses. This is done by ensuring that the market that will carry out trading, transactions or cryptocurrency trading has the funds first so that criminal acts committed by the perpetrators will be reduced or minimized.[9]

Pirlo stated that proof refers to the way a party exercises facts and rights related to its interests. However, according to Subekti, "proving" means convincing the judge about the truth of the arguments put forward by both parties in the dispute.[10] By considering these two meanings, it can be said that evidence in criminal cases is basically to prove that the defendant actually committed a criminal act, so law enforcement must collect evidence to prove the accusation. However, proof is not only finding someone's fault, but also seeking, discovering, and establishing the actual truth about the matter. Collecting and examining electronic evidence requires a long time and high costs because of its wide scope and various types. The use of electronic evidence must be adapted to the evidentiary system and standards of criminal procedural law in Indonesia. Although the Criminal Procedure Code does not regulate electronic evidence as valid evidence, several laws have regulated that electronic data can be used as valid evidence. Electronic evidence is evidence collected from a crime that uses technological tools to direct an event. This can be electronic data contained in certain technological devices, such as computers, hard disks, memory cards, SIM cards, or print outs, or that have been processed by certain technological devices, such as computers. Electronic evidence is currently evidence collected from or in other forms from traces or paths of technology use activities according to Makarim.[11] Judge Mohammed Chawki of the Computer Crime Research Center created three categories of electronic evidence namely:

a. Real Evidence

   "Direct evidence" is also direct evidence in the form of automatic recordings produced by the computer itself by running software and receiving information obtained from other devices, such as computer log files. Makarim considers electronic evidence to be valid and independent evidence. However, recording or copying data (data recording) must be done in the right way (programmed and calibrated) so that the results of the data printout can be accepted as case evidence.

b. Testamentary Evidence

   Witness statements and expert witnesses, namely expert witnesses, can be given during a trial based on a person's experience and observations. This statement is also known as witness evidence or Hearsay. In accordance with our statutory regulations, Law No. 8 of 1981 KUHAP, expert testimony is considered evidence that has the power of proof if it is given about something based on special expertise in the field they have and in the form of information "according to their knowledge" purely.[12] It is very important for judges deciding cybercrime cases if they are skilled at explaining the crime that occurred as well as providing explanations about electronic evidence.

c. Circumstantial Evidence

   According to his definition, provisional evidence is detailed evidence obtained from statements or observations about actual events that support a conclusion but do not prove it. "Circumstantial evidence, also called derived evidence, is a combination of real evidence and hearsay evidence."

Indonesia does not yet have a specific cyber law that regulates cybercrime. However, there are several other positive laws that apply generally and can be imposed on cybercrime perpetrators, especially those who use computers as a means, such as Criminal Code:

Because the Criminal Code involves many acts at once, it often uses more than one article. One example is the articles that can be applied to cybercrime in the Criminal Code.[13]

a. Article 362 of the Criminal Code applies in carding cases where the perpetrator steals another person's credit card number indirectly because only the card number is taken through card generator software available on the internet to carry out transactions in online stores. After the transaction is complete and the goods are sent, sellers who want to withdraw their money at the bank are rejected. This is because the card owner is not actually carrying out the transaction;

b. If someone pretends to offer and sell goods or services by placing an advertisement on a website so that people are interested in buying it, and then sends money to the advertiser, they could potentially be subject to Article 378 of the Criminal Code. However, this item is not there. After the money is sent, the ordered goods do not arrive, the buyer becomes deceived;

c. In carding cases, Articles 378 and 262 of the Criminal Code can be applied because the perpetrator commits fraud as if he wants to buy something and pays with a credit card whose number is stolen.

### 3.2 Proof in Corruption Crimes through Money Laundering and Legal Action through the validity of the Information & Electronic Transactions Law in Withdrawing assets resulting from corruption via cryptocurrency

Fraud is a type of criminal act that is included in money laundering in Article 2 Paragraph (1) Letter q, Law no. 8 of 2010, an amendment to Law number 25 of 2003 concerning the Prevention of money laundering, means that the law is the most effective for investigators in obtaining information about suspects who commit fraud via the Internet because it does not require long and time-consuming bureaucratic procedures. Investigators can ask the bank that received the transfer to provide the suspect's identity and banking data without having to comply with the regulations in the Banking Law. Because identity and banking data are part of bank secrecy, the procedures that are followed start from the investigator having to send a letter from the Regional Police Chief to the National Police Chief to obtain the information and data and then obtain the required data and information, this procedure takes quite a long time.[14]

Money laundering is processing money originating from criminal acts with unauthorised businesses so that the money looks clean or like halal money, so the source is closed. In Article 1, point (1) of Law no. 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundering, the three components of the crime of money laundering are transactions, wealth assets, and violations of the law, according to Tb. Irman.[15] Therefore, money laundering always occurs after an unlawful act, if there is no unlawful act that produces assets of wealth, money laundering will not occur. However, just because unlawful acts produce wealth, money laundering is not complete until the assets of wealth resulting from the crime are transacted in a disguised manner from the beginning. Money laundering originates from a criminal act, which contains elements such as error or negligence, intentionality, unlawful acts, the object of the criminal act, the consequences of the act, and circumstances

that accompany, assist, or order it to be carried out. An act does not have to be completely complete in order to be punished but must look at the formal formulation stated in the established rules. The criminal acts mentioned above are the beginning of the criminal acts that occurred. In a criminal act, there is always a perpetrator and a victim, even if it is only the perpetrator and the victim, the criminal act must be connected to an act, namely an act that violates the law so that a criminal act occurs. In this way, the consequences of criminal acts directed against the victim by the perpetrator arise.

Therefore, the perpetrator who violates the law aimed at the victim is the cause and effect that arises. Criminal acts against humans can cause pain, humiliation, loss of things, and even lives. Criminal acts against objects can cause damage, unusability, alteration, or the emergence of new objects. All the consequences that arise and if these consequences are in the form of money or generate money, and the money is stored in a money storage place that is regulated by regulations, such as a bank or financial service provider, then money laundering is the beginning. Directly, no particular individual or company is harmed by money laundering. This crime has no victim, so it is different from robbery, theft, or murder which damages the victim. To obtain evidence, as regulated in Article 73 of Law no. 8 of 2010 concerning the Prevention and Eradication of the Crime of Money Laundering, Investigators can request information from Financial Service Providers regarding wealth assets that are indicated as money laundering which PPATK has reported, or have Suspect or Defendant status as regulated in Article 72 paragraph (2) of Law no. 8 of 2010, namely by requesting this information, investigators must pay attention to the provisions governing bank secrecy and financial secrecy. Legal action through the validity of the information & electronic transactions law in withdrawing assets resulting from corruption via cryptocurrency:

1. UU no. 19 of 2016 concerning Information and Electronic Transactions explains that electronic printouts are valid evidence

   Included in the Criminal Procedure Code. New rules regarding evidence recognized in Indonesia, especially in criminal procedural law, were created with the enactment of Law No. 19 of 2016 concerning Information and Electronic Transactions (UU ITE). This evidence includes electronic documents. Article 73 of the ITE Law regulates electronic evidence, which states that electronic information, electronic documents, and/or printed results are valid legal evidence if used with an electronic system in accordance with the regulated provisions. According to Article 5 Paragraph (1) of the ITE Law, information, documents, and electronic printouts are valid evidence. In accordance with applicable procedural law in Indonesia, information, documents, and electronic printouts are an extension of this evidence. UU no. 19 of 2016 concerning Electronic Information and Transactions, Article 44 stipulates that: “Evidence for investigations, prosecutions and examinations at court hearings according to the provisions of this law are as follows: a) Evidence as intended in the provisions of the law; and b) Other evidence in the form of information and/or electronic documents as intended in Article 1 paragraph (1) and Article 2; and c) Other evidence in the form of information and/or electronic documents Bank Indonesia strictly prohibits people from using virtual currency or cryptocurrency as a means of payment because it does not have elements of consumer protection, risk reduction, and supervision of overall macroeconomic stability.

   In addition, they have the characteristics of a practical cryptosystem, which makes them capable of being misused for criminal acts such as terrorism, firearms sales, drugs, and money laundering. According to the Indonesian Banking Regulations issued by Bank

Indonesia, payment system service providers or financial technology providers are prohibited from using virtual currency for payment transactions. According to the Executive Director of the Head of the Legal Department of Bank Indonesia, there are five threats to cryptocurrency in Indonesia: 1) if crypto assets or cryptocurrencies are used for payment transactions, it will disrupt the payment system and rupiah management; 2) an increase in the number of crypto asset transactions could affect Bank Indonesia's monetary policy and disrupt capital outflows; 3) and crypto asset transactions are increasingly complicated and disruptive to banking. Because it increases the risk to the stability of the Indonesian financial system; 4) increased cryptocurrency transactions in Indonesia, changes to anti-money laundering regulations, and the prevention of terrorist financing all pose risks; 5) Bank Indonesia also anticipates significant violations of consumer protection and personal data.[16] The Bank Indonesia government is responsible for law enforcement in the misuse of virtual currency also known as cryptocurrency as a means of payment in Indonesia. However, other regulators from the financial services sector may cooperate in enforcing this law. In cases where cryptocurrency is used for money laundering or other crimes, PPATK together with the state police is responsible for investigating the case, and the perpetrator will be charged under Law no. 8 of 2010 concerning the Crime of Money Laundering.

2. Legal action through withdrawal of assets caused by cryptocurrency

   Furthermore, Articles 39 to 42 of the Criminal Code regulate the basic principles of confiscation and confiscation of items that can be withdrawn. These provisions can be described as follows: items that can be withdrawn are items owned by the convict that were obtained from a crime or were used intentionally to commit a crime. In cases of conviction for violations or crimes that were not committed intentionally, a withdrawal decision can also be imposed based on matters specified in the law, namely: a) withdrawal can be carried out against the person involved in the violation; b) If a person under the age of sixteen years owns, enters or transports goods in violation of shipping control regulations in certain parts of Indonesia or forwards the goods, then the judge can impose a penalty of towing the goods; c) The withdrawal of previously confiscated items can be replaced by imprisonment if the legal action taken against the items does not meet the requirements; and d) The State is responsible for all costs of imprisonment and confinement, and all profits from fines and withdrawals. Asset withdrawal arrangements relate to efforts to maximize the withdrawal of assets resulting from crime.

   MA Regulation (Perma) Number 1 of 2013 stipulates procedures for resolving requests for withdrawal of assets in cases of Money Laundering (TPPU) via cryptocurrency. With this Perma, PPATK can handle assets without first asking permission from the district court. To provide information to parties who feel they own and wish to recognize the account, PPATK will later announce the existence of the unclaimed account. Unused accounts are intended to be found for their owners. However, if no one admits it within the specified time limit, the assets in the account are declared state-confiscated assets by a trial court in the district court. If someone objects to the existence of the account, a trial will be held with a single panel (fast trial) to prove whether he is the owner. However, the judge will also consider the account owner's confession of good faith as part of the decision. This regulation applies to all levels of the Supreme Court and lower courts.

   CoFTRA Regulation No. 3 of 2019 concerning Commodities stipulates that Bitcoin can be traded on futures exchanges because it is included in the commodity category.

Therefore, as one way to uncover crimes of corruption, optimization of digital forensic methods is needed. This can be achieved through strengthening regulations, increasing the capabilities of forensic accountants in the digital world, and strengthening cooperation between institutions such as "PPATK with the Corruption Eradication Commission and the Prosecutor's Office." By optimizing these efforts for digital forensic methods, it may be easier to find assets belonging to criminals who launder money into Bitcoin. In practice, this can be seen in cases of corruption and TPPU regarding the management of PT insurance funds and finances. ASABRI and theft of Citibank customer funds. In this case, the suspects committed money laundering by channelling funds generated from corruption to carry out transactions using Bitcoin. This becomes very difficult to uncover in this case because the perpetrator will have the facility to anonymize his real identity when making Bitcoin transactions. The suspects in this case agreed to exchange some of their shares for shares in their company's portfolio. The suspects manipulated share prices when they were exchanged to maintain a positive image of the company's portfolio. To protect the Company from losses, the suspects bought back shares that had been sold at low prices in their names and then bought them again through underlying mutual funds, which were apparently owned by the suspects.

There are no Indonesian laws that specifically regulate Bitcoin. However, the suspects in this case were finally charged with subsidiary charges, namely Article 2 paragraph (1) as the primary indictment, and subsidiary charges, namely Article 18 Law no. 20 of 2001 concerning Eradication of Corruption. Because of this, law enforcers have difficulty taking action and giving appropriate punishment to individuals involved in criminal acts of corruption who have laundered their assets into Bitcoin. The author therefore proposes that the government can create laws to supervise Bitcoin operations. In addition, all institutions must cooperate with each other to optimize the recovery of state assets through digital forensics. PPATK must cooperate with the Corruption Eradication Commission and the Prosecutor's Office in this matter. Organizations have the authority to investigate and collect evidence, primarily using digital forensic techniques.

Withdrawing assets through legal action caused by money laundering through cryptocurrency in the form of Bitcoin, the perpetrator can hide the true origin of the assets obtained from improper profits or proceeds, and by carrying out this activity, the perpetrator can enjoy the results freely as if The assets come from legal actions. Applying Article 18 Paragraph (1) of Law No. 20 of 2001 concerning the Eradication of Corruption can help restore state losses. With the merger of Law No. 8 of 2010 concerning the Crime of Money Laundering and Law No. 19 of 2016 concerning Information and Electronic Transactions (UU ITE) PPATK will later announce the existence of unclaimed accounts at banks. The unused account is intended to be found for its owner within a certain time limit, then the assets can be withdrawn as state-confiscated assets by a trial court in the district court. The legal consequences of acts of corruption that "can harm state finances or the state economy". Corruption defendants who are proven to have caused state financial losses must pay compensation. The court decision determines this penalty as an additional type, and the amount of replacement is very dependent on state losses. Recovering state losses and maintaining economic stability are also criminal responsibilities. Money from the withdrawal of assets as a replacement for those paid by convicts is very important to support the APBN which is experiencing a deficit due to high levels of state spending and corrupt practices in many places. Therefore, the success

of law enforcement in retrieving state money through the crime of Bitcoin cryptocurrency money laundering is very important for the prosperity of society.[17]

## 4 Conclusion

Legal action for the withdrawal of assets against perpetrators of state financial corruption results from cooperation between law enforcers based on the ITE Law. The applicable Law on Money Laundering and Eradication of Corruption Crimes states that cryptocurrencies are legal, let alone regulate more specific matters regarding evidence in the Criminal Procedure Code. Article 73 regulates that electronic evidence can be used as legal evidence and is recognized in procedural law in Indonesia in money laundering criminal cases.

## References


[1] Josua Sitompul, *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa, 2012.

[2] H. Djanggih, "The Phenomenon of Cyber Crimes Which Impact Children As Victims in Indonesia," *Yuridika*, vol. 33, no. 2, p. 212, 2018, doi: 10.20473/ydk.v33i2.7536.

[3] R. Raihana, T. E. K. Sari, and F. Fanny, "Tindak Pidana Pencucian Uang Perspektif Hukum Pidana Dan Perkembangan Teknologi," *SEIKAT J. Ilmu Sos. Polit. dan Huk.*, vol. 2, no. 3, pp. 347–355, 2023, doi: 10.55681/seikat.v2i3.639.

[4] H. Amrani, *Hukum Pidana Pencucian Uang*. Yogyakarta: UII Press, 2010.

[5] B. Kelly, *The Bitcoin Big Bang : How Alternative Currencies Are about to Change the World*, 1st ed. Wiley, 2018.

[6] M. R. Imbar, "Peran Jaksa terhadap Asset Recovery dalam Tindak Pidana Pencucian Uang," *Lex Crim.*, vol. IV, no. 1, pp. 87–96, 2014, doi: 10.1080/10246029.2005.9627584.

[7] B. Waluyo, *Penelitian Hukum dalam Praktek*. Jakarta: Sinar Grafika, 1991.

[8] P. M. Marzuki, *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group, 2005. doi: 9793925256.

[9] D. A. F. Nitha and I. K. Westra, "Investasi Cryptocurrency Berdasarkan Peraturan Bappebti No. 5 Tahun 2019," *J. Magister Huk. Udayana (Udayana Master Law Journal)*, vol. 9, no. 4, p. 712, 2020, doi: 10.24843/jmhu.2020.v09.i04.p04.

[10] R. Subekti, *Hukum Pembuktian*. Jakarta: Pradya Paramita, 1995.

[11] E. Makarim, "Tindak Pidana Terkait Dengan Komputer dan Internet: Suatu Kajian Pidana Materiil dan Formil," in *Seminar Pembuktian dan Penanganan Cyber Crime di Indonesia*.

[12] M. Y. Harahap, *Pembahasan Permasalahan dan Penerapan KUHAP Penyidikan dan Penuntutan*. Jakarta: Sinar Grafika, 2012.

[13] D. Setiawan, *Sistem Keamanan Komputer*. Jakarta: PT Elex Media Komputindo, 2005.

[14] H. S. Jannah and M. Naufal, "Penegakan Hukum Cyber Crime ditinjau Dari Hukum Positif dan Hukum Islam," *Al-Mawarid*, vol. 12, no. 1, pp. 69–84, 2012.

[15] I. S, *Hukum Pembuktian Pencucian Uang*. Bandung: MQS Publishing, 2006.

[16] T. Rahayuningsih, "Perampasan Aset Hasil Tindak Pidana Perbankan Dalam Rangka Pemberantasan Tindak Pidana Pencucian Uang," *Rechtidee*, vol. 8, no. 2, pp. 1–20, 203AD, doi: https://doi.org/10.21107/ri.v8i2.693.g613.

[17] A. Mahmud, "Urgensi Penegakan Hukum Progresif Untuk Mengembalikan Kerugian Negara Dalam Tindak Pidana Korupsi," *Masal. Huk.*, vol. 49, no. 3, pp. 256–271, 2020, doi: 10.14710/mmh.49.3.2020.256-271.