Journal of Social Research

P-ISSN: 2827-9832
E-ISSN: 2828-335x
http://ijsr.internationaljournallabs.com/index.php/ijsr

LEGAL PROTECTION OF CRYPTOCURRENCY USERS AGAINST CYBERCRIME ATTACKS

Adi Darmawansyah, Djunaedi, Kristiawanto
Universitas Jayabaya, Indonesia
202102026102@pascajayabaya.ac.id

ABSTRACT

The medium of exchange can be any object that can be accepted by everyone in society in the process of exchanging goods and services. Long before knowing money, humans had made transactions using barter practices, that is, the exchange of goods and/or services for the desired goods and/or services. In the preparation of this research, a normative juridical approach where approach is carried out based on the main legal material by examining theories, concepts, legal principles, and laws and regulations related to this research. Cryptocurrency assets don't just impact people who mine or trade crypto. It turns out that anonymous platforms that run crypto are also increasingly associated with cybercrime. A recent study *from Interisle Consulting Group* revealed that phishing attempts related to cryptocurrencies grew 257 percent compared to last year (compared to a 61 percent increase in phishing attacks overall), especially for attacks on wallets and exchanges. The rapid development of information and communication technology makes the journey of the development of crime in the virtual and digital world (*cybercrime)* sophisticated and complex.

Keywords: *cryptocurrency, cybercrime, barter practice*

INTRODUCTION

The medium of exchange can be any object that can be accepted by everyone in society in the process of exchanging goods and services (Lallie et al., 2021; Ostroy, 1989). Long before knowing money, humans had made transactions using barter practices, that is, the exchange of goods and/or services for the desired goods and/or services. For example, exchange a sack of rice for a bag of peanuts. The practice of barter began tens of thousands of years ago and still persisted until the beginning of modern man (Meloni & Swinnen, 2018). It's just that problems arise when two people who want to exchange do not agree on the exchange value. Especially if one of them doesn't really need the thing to be exchanged. Finally, this barter system was replaced with commodity currency, still using goods but these goods must be generally accepted as a medium of exchange and as a standard of value used in the exchange of goods by the community. For example, for hundreds of years gold can be directly used to buy goods, but gold also has other functions such as displays and jewelry.

At one time, precious metals such as gold were used as the main means of payment. Subsequently, paper assets such as cheques and banknotes began to be used as a means of payment and were considered money. Human development in meeting their needs is eventually followed by technological developments (Mishkin & Uang, 2010). As part of the development of information technology, a new type of financial instrument, cryptocurrency has been born and developed. This virtual currency can be used as a means of electronic transactions. In addition, the owners also use cryptocurrency to invest and trade. Now business transactions can be done online without involving intermediaries such as banks. Transactions are instantaneous, cross-border, transcontinental, faster, easier, cheaper, and more confidentially guaranteed Cryptocurrency has become the first implementation of Blockchain

technology and its potential is not limited to payment systems alone (Graham, 1995). Decentralized applications created can basically affect areas of life such as economics, science, education, art, culture and others The year 2008 marked the beginning of the cryptocurrency era with the release of a paper by someone under a pseudonym.

Before Bitcoin was born, digital currency experimentation actually existed in various forms, namely eCash, E-gold, Hashcash, B-money, and Bitgold. None of these experiments have resulted in exposure, but according to Cointelegraph, each had a significant influence on the creation of Bitcoin.

Bitcoin is actually a refinement of various experimentations of existing digital currencies. Satoshi Nakamoto, the creator of Bitcoin whose true identity is still unknown, once mentioned that Bitcoin is an implementation of the B-money and Bitgold proposals that are popular in the cryptography community. The Bitcoin proposal was first published by Satoshi on October 31, 2008 to a cryptography mailing list. In his proposal, Satoshi describes Bitcoin as an electronic payment system based on cryptographic proof rather than trust, allowing two parties to transact directly without having to involve a third party.

Today's modern economy makes the role of money more crucial than ever. Money is no longer just a medium of exchange but also functions as a *unit of accounts*, *a store of value,* and a standard of deferred payments, and even today that can function as a commodity (Darmawan, 1992a). As part of the development of information technology, a new type of financial instrument, cryptocurrency has been born and developed. This virtual currency can be used as a means of electronic transactions. In addition, the owners also use cryptocurrency to invest and trade. Now business transactions can be done online without involving intermediaries such as banks. Transactions are instantaneous, cross-border, transcontinental, faster, easier, cheaper, and more confidentially guaranteed Cryptocurrency has become the first implementation of Blockchain technology and its potential is not limited to payment systems alone. Decentralized applications created can basically affect areas of life such as economics, science, education, art, culture and others The year 2008 was the beginning of the cryptocurrency era with the release of a paper by someone under the pseudonym (*anonymous).*

Today's modern economy makes the role of money more crucial than ever. Money is no longer just a medium of exchange but also functions as a *unit of accounts*, *a store of value,* and a standard of deferred payments, *and* even today that can function as a commodity (Darmawan, 1992b). *Cryptocurrencies* though are not classified as official currencies but have quite a global significance (Shanaev et al., 2020). This can be seen from the existence of crypto assets that occupy the eighth position in the category of the most popular commodities in the world. In the development *of cryptocurrency, each country sees that there are friendly and not, so countries have different regulations, especially* cryptocurrency *regulations as a means of payment.*

Attitudes and Regulations Related to *Cryptocurrency in Other Countries Will certainly also see how other countries' attitudes towards the development of* Cryptocurrency itself (Ferreira & Sandner, 2021). The attitude taken by other countries should be used as a benchmark for how a country responds to the phenomenon of new currencies *Cryptocurrency.* For example, Indonesia's neighboring country, Singapore also initially behaved the same as Indonesia towards this currency. They warn of the risks of using currencies. This warning also came directly from the state institution that is authorized to handle financial matters, The

Monetary Authority of Singapore (MAS) More or less the same thing happened to another close neighbor of Indonesia, namely Australia. In 2013 in June, the Australian Taxation Office (ATO) monitored how the cryptocurrency phenomenon was going. Also in December, the Reserve Bank of Australia issued a statement that cryptocurrencies do not pose a problem, but stressed the risks to speculators and said there was no way to stop transactions with other currencies including cryptocurrencies. Australia openly supports all aspects of cryptocurrencies and blockchain technology, from payment methods, NTF, and metaverse, and DeFi. Moreover, in March 2022, the country had declared a pro-regulation approach when a senator proposed a new regulatory framework.

South Korea currently has around 200 cryptocurrency exchange platforms. India is not closing all options when it comes to *cryptocurrencies*, including the use of *blockchain technology*. The Indian government will allow a number of places for people to experiment on blockchain and Cryptocurrency. However, what is the formulation for the development of *cryptocurrencies* is still in the rubbing stage. El Salvador made cryptocurrencies the official currency and legal tender of the country for the first time in the country's history starting on Tuesday. The digital currency is El Salvador's official currency alongside the United States (US) dollar, a move that is sure to draw attention to the opportunities and risks associated with cryptocurrencies.

Several countries in the world that are experiencing financial as well as banking crises, are looking at Blockchain technology and *Cryptocurrency* currencies as part of the solution to solve their problems (Sanka et al., 2021). Greece, the Marshall Islands and Venezuela are already trying *cryptocurrencies* as a way to solve their countries' economic problems. The Marshall Islands, which has a population of around 60,000, became the second country to create its own cryptocurrency as legal tender. They named their cryptocurrency SOV from the word "Sovereign" Along with Japan, the UK will also regulate this currency. The regulation not only focuses on financial aspects, but also on aspects of cybercrime, such as hacking and money laundering. Another country that has also given guidelines for the treatment of Cryptocurrency is the United States. In general, Cryptocurrency is recognized as a virtual currency that can be used as a medium of exchange. Exchangers are required to register as financial services or remittance entrepreneurs.

Canada became the first country to implement special tax regulations for cryptocurrencies This tax system is applied to minimize the risks that often occur in transactions with virtual currencies, namely money laundering and financing for terrorists. Some countries have also rejected Bitcoin because it is wary of its volatility, decentralized nature, poses a threat to the monetary system, and is linked to illegal activities such as drug trafficking and money laundering. Some countries actually have restrictions and even ban the use of cryptocurrencies such as China, Russia, Algeria, and Bangladesh. Because it is considered to have a negative impact on the stability of state security.

China will provide tough "measures" for those who are still recalcitrant in crypto mining, aka crypto mining China's National Development and Reform Commission (NDRC), announced a crackdown will be imposed on commercial crypto miners and state-owned institutions. In Indonesia itself, the provisions regarding Cryptocurrency have not been specifically regulated. However, Law number 7 of 2011 affirms the legal currency in Indonesia. Currency is money issued by the Unitary State of the Republic of Indonesia hereinafter referred

to as Rupiah. Affirmation of the existence of rupiah is strengthened in article 21 of Law Number 7 of 2011 concerning Currency. In the Regulation issued by Bank Indonesia with Number 18/40/2016, the regulation explains that payment system service providers are prohibited from processing payments with Virtual Currency.

Legal subjects who are prohibited from processing transactions are banks or similar institutions in Bank Indonesia regulations, not individuals. Meanwhile, in Law Number 7 of 2011 concerning Currency, it is only affirmed that Rupiah must be used as a means of payment transactions in the territory of the Republic of Indonesia.

In Indonesia, Crypto Assets can be officially traded. This crypto asset is more of an investment asset, not a *currency*. In accordance with the Letter of the Coordinating Minister for Economic Affairs Number S-302 / M.EKON / 09/2018 dated September 24, 2018, regarding the Follow-up Implementation *of the Crypto Asset* Regulation Report as a Commodity Traded on the Futures Exchange, Crypto Assets are still prohibited as a means of payment, but as an investment tool can be included as commodities that can be traded on futures exchanges. With consideration, because economically the investment potential is large and if prohibited will have an impact on the number of investments that come out (*capital outflow)* because consumers will look for markets that legalize crypto transactions. Crypto Assets will first be regulated in the Minister of Trade which includes Crypto Assets as commodities traded on the Futures Exchange. Further arrangements related to technical matters and to accommodate inputs from Ministries/Institutions will be prepared to implement regulations in the form of Regulations of the Commodity Futures Trading Supervisory Agency (Bappeti). The results of a study from Bappeti concluded that Digital Commodities or Crypto Commodities from the *blockchain* system can be categorized as rights or interests, so they are categorized as Commodities in Law No. 10 of 2011 concerning Amendments to Law No. 32 of 1997 concerning Commodity Exchange Trading (PBK).

The development of Virtual Currency (cryptocurrency) then banyan also with the development of cybercrime in cybercrime (cybercrime). Cybercrime is a general term for crimes that attack computer systems or internet networks, with the aim of data theft, finance and the spread of malicious software code which is an illegal act in the field of information and communication technology as a modified form of conventional crime.

Cryptocurrencies exist in a decentralized and independent online environment, not held back by bank or government rules. While this makes them more accessible to people, it also exposes cryptocurrencies to a higher risk of cybercrime. Cybercriminals can hack trading platforms and steal funds. They typically use tactics such as cryptojacking, phishing, ransomware attacks, and extortion to steal cryptocurrencies. Cryptocurrency is already the most preferred form of exchange in ransomware attacks for cybercriminals.

A common pattern of cybercrime is carried out with ransomware, Cybercriminals can hide their identity while demanding a ransom in cryptocurrency. Furthermore, they can turn cryptocurrencies into traditional forms without ever being discovered. The ease of anonymity in cryptocurrency domains works for cybercriminals, which makes these domains even more vulnerable to cyber-attacks. It's easy for cybercriminals to be virtually untraceable in the cryptocurrency domain. They can attack any business and demand ransom in digital currency without fear of being tracked. With cryptocurrencies, there is no evidence pointing back to the

culprit. And with more and more businesses accepting cryptocurrencies across the business world, cybercrime has become a considerable threat.

METHOD

In the preparation of this research, a normative juridical approach where the approach is carried out based on the main legal material by examining theories, concepts, legal principles and laws and regulations related to this research. This approach is also known as the literature approach, namely by studying books, and other documents related to this research. In this research also through the statutory approach (*statue approach*), conceptual approach (*conceptual approach*) and Comparative Law.

RESULTS AND DISCUSSION

Cryptocurrency assets don't just impact people who mine or trade crypto. It turns out that anonymous platforms that run crypto are also increasingly associated with cybercrime. A recent study *from Interisle Consulting Group* revealed that phishing attempts related to cryptocurrencies grew 257 percent compared to last year (compared to a 61 percent increase in phishing attacks overall), especially for attacks on wallets and exchanges. Cybercriminals use the same techniques they use in other online financial crimes on virtual currencies, and they have great success in their efforts.

The international community has also taken a serious look at *cybercrime. Cybercrime* using *crypto (cryptocurrency)* reached US $ 8.6 billion or Rp 123 trillion last year. These digital assets are obtained from hacking or other criminal acts. "That figure is up 30% compared to 2020," blockchain analysis firm *Chainalysis* said. Overall, money laundering using crypto has exceeded $33 billion or Rp 473 trillion since 2017. According to *Chainalysis,* the perpetrators targeted centralized exchanges. *Chainalysis* said money laundering using crypto is a process of disguising the origin of money obtained illegally. Then, the perpetrator transfers it to a legitimate business. The company noted that $8.6 billion of money laundering last year was funded by *crypto-native crimes.* These funds come from the sale of data stolen by the *darknet* and ransomware attacks.

Various forms of cybercrime that are often used by perpetrators include email spoofing is forgery of email headers. The received email message appears to have been sent by a genuine, actual and trusted source. This mode is usually used in spam or phishing campaigns. The target may open the email thinking that the email has been sent by a legitimate source. Hacking is a secret breach of a computer system and stealing valuable data from the system without permission. The spread of a virus or malware is a set of cyber instructions capable of performing some malicious operation. Viruses and malware stop the normal functioning of system programs and insert some abnormalities from the performance of the affected system. Viruses and malware can spread through email, chat messages, data storage, multimedia, the internet and other electronic media. Phishing is the act of stealing personal information such as passwords, credit card details, victim user data targeted over the internet (Nian & Chuen, 2015). This form of cybercrime is carried out by spoofing emails and instant messages to victims. Hackers create direct links that direct targeted victims to fake web pages that look identical to real websites. Stalking is the use of the internet for other electronic means to stalk or spy on someone who is victimized. Stalking can be harassment, hate speech, or cyberdefamation in

cyber scope. Stalking generally involves harassing, threatening or terrorizing behavior that a person performs repeatedly, such as making phone calls, texting and other types of bullying or terror. Defamation is the desecration of the dignity of victims in cyberspace that harms the reputation of a person or organization in the public eye through cyber space. Desecration of dignity is done by making defamatory statements to bring down the reputation of an individual or company as a victim. Website scripting is a type of computer or system security vulnerability usually found on websites that allows code or script injection by cybercriminals. The website script vulnerability is exploited by perpetrators to request access control to website servers.

The money laundering crime utilizes technological sophistication ranging from manual to complicated or super sophisticated by utilizing cyberspace and money laundering crime known as *cyber loundering* is a *cybercrime* supported by knowledge of banks, business, and *electronic banking* Established and with technological advances already exist, this is done easily, where actors can store or send money through banks using electronics and can be done anywhere and anytime. Money launderers can also deposit the money in a bank without having to include their identity (Singh & Best, 2019).

This illustrates that *money cybercrime* is not solely a crime that is local but can also be international. In general, developing countries do relax some of their financial rules and regulations. This easing is carried out with the deliberate intention of inviting the flow of funds from outside into their countries to carry out development in their countries and the agendas of the intended country or government. This attitude is certainly highlighted by the international community, especially the *FATF (Financial Action Task Force).*

A digital ledger system where cryptocurrencies are built into the blockchain, which has anonymity in it. Ransoms paid in cryptocurrencies such as bitcoin can be run through "cryptocurrency mixers", which obscure the ownership trail by combining it with someone else's ownership.

Although the practice itself is not considered illegal, mixer operators can get into trouble if found to have laundered illegally obtained money (Bueger & Edmunds, 2020). And cryptocurrencies have truly become the new favorite way for cybercriminals to launder funds. Another option to maintain this anonymity is to convert the ransom payment to a different cryptocurrency through a crypto exchange. For this, so-called money mules can be recruited on dark web forums and directed to withdraw Bitcoins from certain accounts, while keeping their identities completely secret and untraceable.

For the digital currency domain, ransomware attacks experienced their first spike in 2020, when victims paid more than $406 million ions in cryptocurrency to attackers, according to blockchain analytics firm *Chainanalysis* Inc. This year, cybercriminals have taken at least $81 million from victims as of May, according to company estimates. The cybersecurity firm said the company had paid millions of dollars more for an undisclosed ransom (Perwej et al., 2021). Being insured against cybercrime can make individuals and businesses more willing to pay the ransom if they are covered under an insurance policy, because they know that they will get that money back from the policy. This is why cybercriminals who specialize in ransomware are actively looking for targets that have insurance to maximize the chances of getting paid (Choo, 2011).

For cryptocurrency investors, here are some of the most common cybersecurity risks:

1. Cryptojacking – Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by making victims click on malicious links in emails that load crypto mining code on computers or by infecting websites or online ads with JavaScript code that executes automatically after loading in the victim's browser.
2. Phishing – Phishing campaigns target trading platforms with the primary purpose of stealing user credentials which fraudsters can then use to demand profits or ransom
3. Hacked trading platforms – Cybercriminals compromise trading platforms by stealing funds from users.
4. Compromised registration forms – Cybercriminals steal user information and then sell it on the black market for profit.
5. Third-party apps – Cybercriminals hack other apps to then steal user data and use it to target further attacks.

Given that crypto cybercrime losses have increased tremendously, there is great pressure on international organizations and governments to legislate to regulate these virtual currencies. In April 2021, a private-public partnership called the Ransomware Task Force published an 81-page report with recommendations on how governments can protect against and deal with ransomware attacks. The group urged governments to expand Know Your Customer (KYC), Anti-Money Laundering (AML), and Combating the Financing of Terrorism (CFT) requirements, which are typically imposed by national and international authorities on banks in their jurisdictions, to crypto exchanges, kiosks and over-the-counter trading desks.

Businesses and individuals need a way to combat cybercrime in cryptocurrencies urgently as they look to improve their investment prospects. Businesses and individuals – who invest in cryptocurrencies – need training to recognize the latest threats used by hackers. It's important to make simulated phishing a part of their overall security training. One should also gain a solid understanding of cybersecurity methods to protect cryptocurrency investments.

With businesses using high-level cybersecurity protections, cybercrime can be mitigated. Just as cybercrime is on the rise, so are initiatives to ensure that cryptocurrency exchanges are regulated and monitored in the most secure way possible.

The best way to protect against these cyberattacks is to implement proper crypto cybersecurity protocols and practices as well as be extra careful with the apps and sites you use.

Cybercrime is an act carried out by perpetrators to destroy an organization's network by stealing valuable data, documents, hacking bank accounts and transferring them to their accounts To study these crimes, cyber criminology is needed which is a combination of knowledge from criminology, psychology, sociology, computer science, and cybersecurity to provide an in-depth understanding of cybercrime. Some of the main factors that cause cybercrime to develop rapidly are the tools, ways and media of cybercrime are very easily accessed and learned on the internet, rapidly increasing technological improvements related to

the speed of processing, data processing and analysis, internet bandwidth and other internet network activities and affordable manual access to information sources or servers.

Due to the autonomous, anonymous, and permanent nature of crypto transactions, cryptocurrencies act as the perfect escape car for cybercriminals. Crypto has become an invaluable vehicle for hackers. This is based on:

1. No oversight: authorities such as banks or government agencies that usually act as intermediaries in financial transactions are not involved in crypto transactions.
2. Bad actors remain anonymous: crypto transactions do not convey identity details in any way, such as names, email addresses, or other background information. There is only a wallet address, and it is just a string of unrecognizable letters and numbers. And hackers often use multiple wallets to help "launder" further transactions.
3. Transactions are permanent: in crypto, when money is sent from one person to another, it is irreversible. Just like using cash, transactions are out of your control. And for attacks like ransomware, it's easy for hackers to flee the scene without being tracked.

As cryptocurrency prices continue to fall, wiping out hundreds of billions of dollars in value, cybercriminals who thrive in ransomware attacks are forced to rethink how they collect their ransom, and how much they might ask for. The crypto crash has pushed many dark web-based crypto-exchange markets, where cybercriminals manage their money, out of business. Last year, for example, more than 30 smaller dark web exchanges have shut down.

Ultimately, cybercriminals still have the mindset of traditional investors: if the value of an asset starts to fall, they tend to cash out quickly to mitigate losses. As a result, this has forced these bad actors to consider switching back to traditional digital crimes like corporate phishing and dollar-impacted malware, rather than crypto.

CONCLUSION

The rapid development of information and communication technology makes the journey of the development of crime in the virtual and digital world (*cybercrime)* sophisticated and complex. The existence of reliable and effective cybersecurity is needed to overcome cybercrime so that people can feel protected against their cyptocurrency assets. The challenge in the future of cybercrime in cryptocurrency is to make cybercrime regulations against cryptocurrencies so that cybercrime patterns against cryptocurrencies such as Cryptojacking, Phishing, Compromised registration forms, Hacked trading platforms which are patterns of cybercrime crimes against cryptocurrencies can be overcome optimally. Strengthening regulations in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions is absolutely necessary in order to dynamically carry out cybercrime response to cryptocurrency assets.

REFERENCES

Bueger, C., & Edmunds, T. (2020). Blue crime: Conceptualising transnational organised crime at sea. *Marine Policy*, *119*, 104067.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731.

Darmawan, I. (1992a). Pengantar Uang dan Perbankan. *Jakarta: PT Rineka Cipta*.

Darmawan, I. (1992b). Pengantar Uang dan Perbankan. *Jakarta: PT Rineka Cipta*.

Ferreira, A., & Sandner, P. (2021). Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law & Security Review*, *43*, 105632.

Graham, S. (1995). From urban competition to urban collaboration? The development of interurban telematics networks. *Environment and Planning C: Government and Policy*, *13*(4), 503–524.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Meloni, G., & Swinnen, J. (2018). Trade and terroir. The political economy of the world's first geographical indications. *Food Policy*, *81*, 1–20.

Mishkin, F. S., & Uang, E. (2010). Perbankan, dan Pasar Keuangan Buku I, alih bahasa Lana Soelistianingsih dan Beta Yulianita. *Salemba Empat, Jakarta*.

Nian, L. P., & Chuen, D. L. K. (2015). Introduction to bitcoin. In *Handbook of digital currency* (pp. 5–30). Elsevier.

Ostroy, J. M. (1989). The informational efficiency of monetary exchange. In *General Equilibrium Models of Monetary Economies* (pp. 113–128). Elsevier.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management*, *9*(12), 669–710.

Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications*, *169*, 179–201.

Shanaev, S., Sharma, S., Ghimire, B., & Shuraeva, A. (2020). Taming the blockchain beast? Regulatory implications for the cryptocurrency Market. *Research in International Business and Finance*, *51*, 101080.

Singh, K., & Best, P. (2019). Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, *34*, 100418.