HANG TUAH LAW JOURNAL

Volume 5 Issue 1 April 2021

Urgency of Cryptocurrency Regulation in Indonesia: The Preventive Action for Ransomware Crime

Winnie Stevani, Hari Sutra Disemadi[*]

Abstract

Disruption is a double-edged sword since, in addition to facilitating digitization, it also serves as a target for cybercriminals to conduct their schemes. Cryptocurrency is a type of virtual currency that uses cryptography technology to enable digital transactions in cyberspace. Ransomware is one type of crypto crime that has increased in 2020 occurrences. More over, ransomware is a way for cybercriminals to make money by threatening victims with access limitations, data deletion, and data dissemination in exchange for a ransom payment. Furthermore, the government hasn't provided recognition and protection for its inhabitants, the creation of a legal vacuum (*rechtsvacuum*) in Indonesia surrounding cryptocurrency regulation is seen to be damaging to digital users. In light of these issues, the goal of this research is to assist the Indonesian authorities in comprehending the fundamental issues surrounding crypto crimes such as ransomware. Then, to assess the prospects of cryptocurrency as a virtual currency in Indonesia, the research technique employed is a normative juridical research method with a conceptual approach and law. This paper demonstrates that the crime of ransomware will hinder cyber law enforcement in Indonesia, resulting in a detrimental impact on economic development and vulnerability to cyberattacks that harm national security. As a result, if cryptocurrency stays in a legal void or 'gray area', governments must be aware and prioritize preventive actions against ransomware attacks and their consequences. This preventative step could take the form of regulating cryptocurrency in Indonesia as virtual money and block ransomware activity.

Keywords

Cryptocurrency; Regulation; Ransomware Crime.

[*] Faculty of Law, Universitas Internasional Batam, Indonesia

Correspondence: Winnie Stevani, Fakultas Hukum, Universitas Internasional Batam, Batam, Indonesia. Email: 2051001.winnie@uib.edu

Introduction

The era of disruption provides a real digital transformation of world activities. Disruption is an innovation that replaces the old system with a new system that is more practical, simple, current, effective, efficient, and able to adapt to the demands of changing times (Priatna, 2019). The era of disruption has also started the industrial revolution 4.0 with the massive use of technological sophistication in almost all areas of life and refers to a world where the combination of technology in the physical, biological, and digital domains will be difficult to distinguish so that it is fundamentally different from the previous revolution (Schwab, 2016). The combination of technology also has a significant impact of 65% on the phenomenon of industrialization and economic growth in countries including Indonesia (Disemadi & Kang, 2021) This phenomenon provides a new contribution to cryptonomic as a companion to fiat currencies. Cryptocurrency is an alternative to virtual currency that applies the sophistication of cryptographic technology, where every financial transaction will be carried out by encoding and applying certain algorithms so that it is not easy to fake (Syamsiah, 2017). Cryptocurrency is different from other currencies because it is not produced by a central authority and there is no intervention or manipulation from the government (Dwicaksana & Pujiyono, 2020). Many types of cryptocurrencies are starting to develop in the community, namely Altcoin, Bitcoin, Bitshares, Dash, Dogecoin, Ethereum, Litecoin, Peercoin, Ripple, Stellar, NXT, and others (Kyriazis, 2021).

Sophisticated cryptography can control the circulation of new currency units and verify each transaction independently, without any intervention from third parties. However, the existence of cryptocurrencies is not recognized as a legal payment medium by Bank Indonesia due to several reasons, such as high risk, no official responsible administrator, highly volatile to price changes, and prone to crypto crime. Besides, the Chief Executive Director of the BI Legal Department, Rosalia Suci Handayani emphasized that cryptocurrencies are prohibited from being a legal payment medium in Indonesia for at least the next 10 years (Azhar, 2021). Then, Bank Indonesia as the central bank stated firmly to all digitalization users not to sell, buy, and trade cryptocurrencies as virtual currencies in Indonesia because it is contrary to Law No. 7 of 2011 concerning Currency. Bank Indonesia has issued various regulations regarding the prohibition of virtual currencies as payment media by financial technology providers, namely "BI Regulation No. 18/40/PBI/2016 concerning the Implementation of Payment Transaction Processing", "BI Regulation No. 19/12/PBI/2017 concerning the Implementation of Financial Technology", and "BI Regulation No. 20/6/PBI/2018 concerning Electronic Money". However, the Commodity Futures Trading Regulatory Agency (Bappebti) has recognized and legalized cryptocurrency as a crypto asset under the Indonesian Ministry of Trade in Permendagri No. 99 of 2018 concerning General Policy for the Implementation of Crypto Asset Futures Trading.

Behind the ban, cryptocurrencies during the Covid-19 pandemic experienced extraordinary developments because cryptocurrencies once reached a price of $64,800 million per chip or equivalent to IDR 939.6 million (exchange rate of IDR 14,500) (Ulya, 2021). However, anonymity and legal uncertainty in transactions are used by irresponsible people to commit crypto crimes. This is evidenced by the rise of crypto crime in various parts of the world, such as money laundering, ransomware, darknet markets, scams, stolen funds, and financing of terrorism and extremism. Then ransomware becomes an urgency that must be further considered by the Indonesian government for the security of digitizing users. Ransomware comes from the word "ransom", which means "forced ransom" and "malware", which means payment for stolen data or limited access via encryption. Ransomware is malware to extort money in the form of ransom from its victims by encrypting important files on the computer so that data access restrictions occur (Tajriyani, 2021). Extortionists ransom often use cryptocurrencies due to the anonymity of conducting financial transactions, making it difficult to track their whereabouts. Cases of ransomware increased dramatically in 2020 and will become critical if the government is not immediately prevented. Based on the report of crypto crime 2021 from Chainalysis, Blockchain shows that the total ransom paid by victims in 2020 increased by 311% or was worth $350 million (Chainalysis, 2021). This difference in numbers is crucial that ransomware requires a quick response from the government by establishing a legal regulation regarding this matter, so that it does not harm economic movements, legal certainty, and national security.

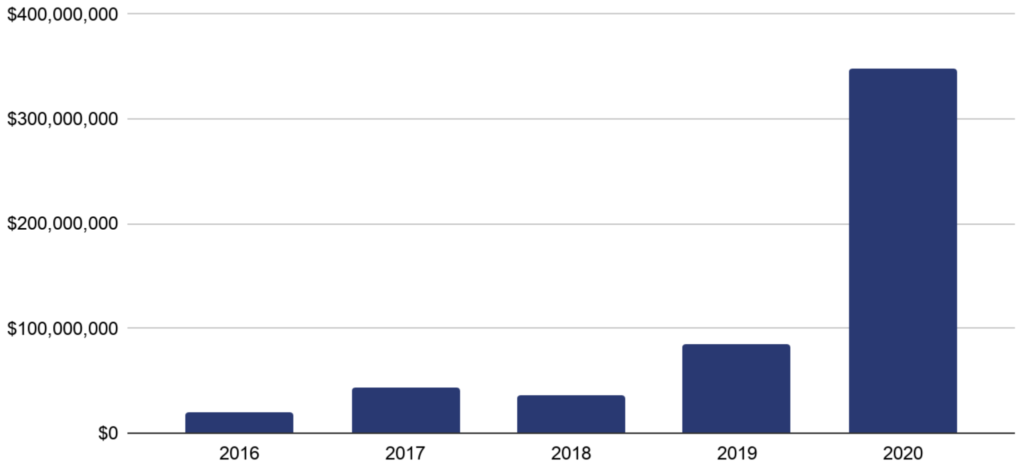

Figure 1. *Graph of Total Cryptocurrency Payments Due to Ransomware Crime*

Starting from the Covid-19 pandemic in 2020, there were 831,105 attacks on ransomware in Southeast Asia that were successfully blocked and 298,892 attacks on ransomware aimed at digitalization users in Indonesia (Wuragil, 2020). However, ransomware is increasingly troubling the public because a large country, as the United States, is attacked by a group of hackers called REvil. In April 2021, REvil was involved in a blackmail attempt with the Apple company and is now focused on attacking IT security management company Kaseya. The perpetrators tried to infect Kaseya's software, called

Vehicle Stability Assist (VSA) and it could spread to all users of the device (Hakim, 2021). The results of research from DigitalX Jakarta found that more than five state-owned and banking companies were detected by ransomware attacks on Kaseya's antivirus devices (Nugroho, 2021). Based on this phenomenon, Indonesia requires legality regarding cryptocurrency as virtual currency so that it is not used by hackers as a place to carry out illegal transactions in the form of extortion. Then, the status quo against the obscurity and absence of regulation related to cryptocurrency in Indonesia causes a legal vacuum (rechtsvacuum), making it difficult for law enforcement officials to handle. Although Indonesia already has several laws, such as the Criminal Code (KUHP) and Law No. 19 of 2016 concerning Information and Electronic Transactions (UU ITE) to impose sanctions on cases of threats/extortion. However, the law is not enough because the anonymity possessed by cryptocurrencies is not easy to trace, and it will only be a case of not being able to find out who the hacker is. As a result, cases of ransomware will never decrease. With this essence, the government needs to put the matter to a higher level and ensure the protection of legal rights of users of cryptocurrency consisting of communities and businesses in the transaction according to Article 28D and 28G of the Constitution NRI 1945 in each related regulation.

The previous study that examines the related themes has been carried out by Clara and Siti Nurbaiti in 2018 who reviewed "The Legal Position of Bitcoin as a Virtual Currency in Indonesia Based on Law Number 7 of 2011 concerning Currency" (Clara & Nurbaiti, 2018); Raafi Ghania Razzaq in 2018 who reviewed "The Legality of Virtual Currency in the Perspective of Indonesian Law" (Razzaq, 2018); F. Yudhi Priyo Amboro and Agustina Christi in 2019 who reviewed "The Prospects of Regulatory Cryptocurrency as a Virtual Currency in Indonesia (Comparative Study of Japanese and Singaporean Laws) (Amboro & Christi, 2019); Bart Custers et al. in 2020 who reviewed "Laundering the Profits of Ransomware: money Laundering Methods for Vouchers and Cryptocurrencies" (Custers et al., 2020); and Nur Syamsi Tajriyani in 2021 who reviewed "Criminal Accountability for the Crime of Extortion with the Operational Mode of Spreading the Cryptolocker Ransomware" (Tajriyani, 2021). Based on previous studies, the focus of this research is the urgency of regulation regarding cryptocurrencies in Indonesia as the preventive measure for ransomware crimes. For this reason, three main problems can be formulated that will serve as the basis for research and essential problems faced by digitalization users, namely the question of what cryptocurrency is, what are the implications of ransomware legal vacuum, and what is the urgency of regulating cryptocurrency in Indonesia as the preventive measure for ransomware crimes. The government must realize that the legal position on cryptocurrencies is important to be studied further and consider the government to look further into the issue of the legal vacuum of cryptocurrencies in preventing ransomware crimes.

Research Methods

The method used in this study is a normative juridical research method with conceptual approach and legislation to examine the prospects of the legality of cryptocurrency as a virtual currency in Indonesia to prevent the rise of ransomware. With this method, research is sourced from various literature studies as secondary material to find the main issues related to the legal vacuum of cryptocurrencies. Also, the statutory approach refers to various laws regarding the recognition and prohibition of cryptocurrencies, so that common ground is found to resolve the essence of the problem. The research will focus on crucial aspects of cryptocurrency regulation, so as not to be used as a medium for illegal ransomware transactions. The results of this study are presented descriptively and qualitatively, which clearly describes the importance of regulating cryptocurrencies as the preventive effort for ransomware in Indonesia and consider the government to look further into this issue.

Results and Discussion

1. Cryptocurrency at a Glance

Technological updates and developments in the financial world are increasing in line with the emergence of virtual currency innovations such as cryptocurrencies. According to Article 34 Letter a Bank Indonesia Regulation No. 18/40/PBI/2016 concerning Implementing Payment Transaction Processing, virtual currency is digital money issued by other parties outside the monetary authority and obtained through mining, rewards, purchases, or transfers, and is not included in the category of electronic money. In Greek, cryptocurrency comes from the root word "cryptos" which means secret. Cryptocurrency is a blockchain innovation that offers the formation of virtual coins or tokens through the sophistication of cryptography. Cryptocurrency is a further development of a digital financial system that is built with the computational sophistication of cryptology and a decentralized system (Li & Wang, 2017). Then cryptocurrency was first launched in 2009 by anonymity named Satoshi Nakamoto in his publication entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" (Addinanto, 2018). According to Satoshi Nakamoto, cryptocurrencies with distribution peer-to-peer are believed to protect sellers because computational transactions are difficult to reverse and protect buyers. After all, the mechanism of escrow is easy to implement (Nakamoto, 2008). All transactions will be carried out through a cryptographic mechanism that is distributed in nature and must carry out validation so that confidentiality can be guaranteed. Cryptocurrency is a representative of a financial taxonomy that previously did not exist in people's lives.

The financial taxonomy provides an overview of how the physical or digital currency specifications are visualized through a money tree or money interest. Therefore, the classification of why cryptocurrencies are different from other currencies can refer to four main criteria, namely the issuer: central bank or private (miner) form: physical or digital transaction processing: centralized or decentralized, and accessibility (Bech & Garratt, 2017). Based on these criteria, there are several justifications for cryptocurrencies: 1) private because they are issued privately without any central authority and are not part of any obligation or ransom that can be claimed. As a result, the transparency and predictability of the monetary policy of cryptocurrencies will increase, 2) the digital design of cryptocurrencies is similar to electronic money issued by central and commercial banks, as well as the absence of links to certain jurisdictions so that cryptocurrencies will be easily accessible in global trade, and 3) transaction settlement in a decentralized way because exchanges cryptocurrency use peer-to-peer and Decentralized Ledger Technology (DLT) so they are less vulnerable to malicious attacks. Although cryptocurrencies do not have a single responsible and authorized operating entity, they still require intermediaries to provide technical services, such as digital wallets cryptocurrency (Claeys et al., 2018).

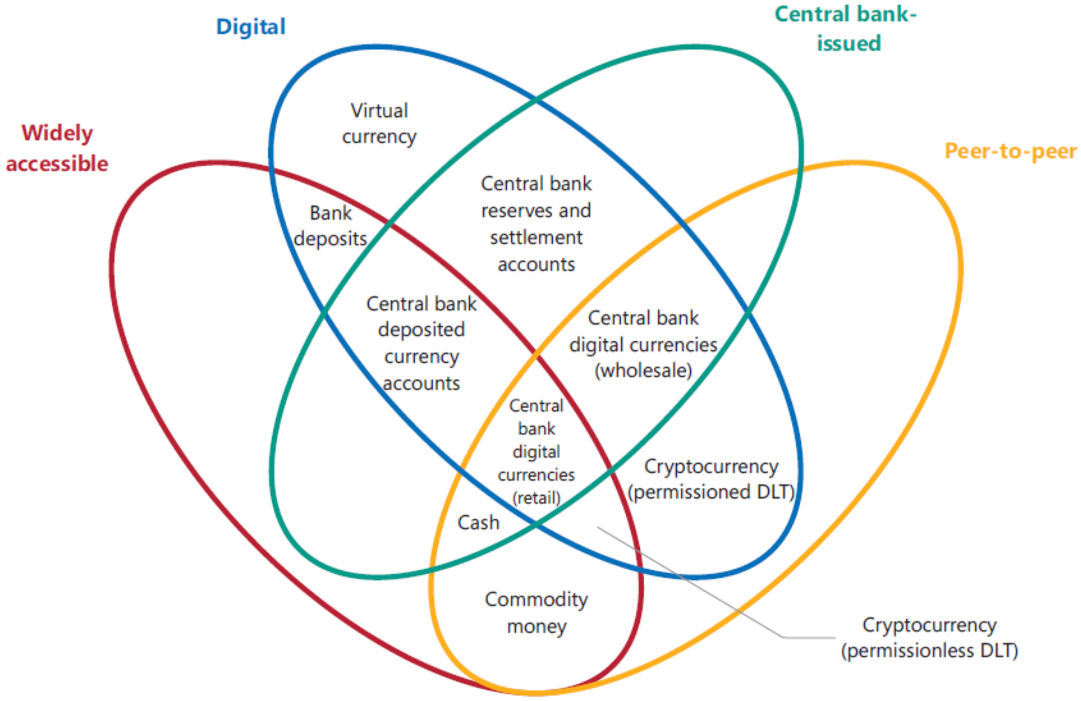
Digital
Central bank-issued
Widely accessible
Peer-to-peer
Virtual currency
Bank deposits
Central bank reserves and settlement accounts
Central bank deposited currency accounts
Central bank digital currencies (wholesale)
Central bank digital currencies (retail)
Cryptocurrency (permissioned DLT)
Cash
Commodity money
Cryptocurrency (permissionless DLT)

Figure 2. *Money Flower: A Financial Taxonomy*

As an innovation that is currently viral, cryptocurrency is believed to be a support and alternative for digital economic transaction payments without the role of a third party. Cryptocurrencies have a decentralized nature because they are not issued by any financial institution and are universally accessible. Besides, blockchain technology is the origin of cryptocurrency and acts as a distribution balance that records all digital traces of users, so that new blocks will merge with previous blocks and form a linear series (Fernández-Villaverde & Sanches, 2018). Data components such as receiver, sender, and coin value will be stored by the blockchain. In general, there are several mechanisms used by blockchain, namely using harsh techniques that identify transaction blocks with unique values, mechanisms of proof-of-work that aim to slow down the creation of new blocks while making it difficult to change blocks, and distribution management mechanisms with networks peer-to-peer by sending valid node information of the new block to all crypto users. In a borderless world, confirmation of crypto transactions is very important because all users will receive transaction confirmations from other users. Cryptocurrency activity will be a blockchain history that cannot be changed by other parties. Then the confirmation will be carried out by the miner, starting from accepting new transactions, validating them, spreading them to the entire network of users. Since the Covid-19 pandemic, cryptocurrency users have increased dramatically and provided extraordinary developments for cryptonomics. Based on the results of Onfo's research in 2020, Indonesia with a population of ± 270 million has 11% of crypto users, comparable to 14% of crypto users in the United States (Bitocto, 2021). The importance of the legality of cryptocurrencies in the era of cryptonomic has not been well considered because the government only recognizes it as an investment commodity, not as a medium of payment like the Rupiah currency.

Bank Indonesia strictly prohibits the existence of cryptocurrency as a medium of exchange or unit of value. The risks that are factors for the prohibition of cryptocurrencies in Indonesia are the risk of the payment system and the management of the Rupiah currency if crypto is used as a payment medium, the risk of capital outflows that can affect BI's monetary policy, the risk of financial system stability, the risk of violating the AML-CFT principles, the risk of violating consumer protection, and the protection of personal data. However, the prohibition of cryptocurrencies is not explicitly stated in the Currency Law, which states that "currency is money issued by the Republic of Indonesia, here in after referred to as Rupiah". Also, the Bank Indonesia Law explains that "Rupiah is a legal tender in the territory of the Republic of Indonesia". Thus, the constitution does not prohibit using cryptocurrencies in people's lives, but all risks related to ownership and threats are their responsibility because no law regulates it. The importance of cryptocurrency regulation has been recognized by several countries in the world. In Japan, the recognition began with the crypto crime incident in 2014 at the Mt. Gox, which holds about 80% of Bitcoin trades in the world and suffered losses of around $500 Million due to hacking (Amboro & Christi, 2019). In maintaining national security, Japan has legalized cryptocurrency through the Financial Services Agency (FSA), as well as implementing anti-money laundering regulations on cryptocurrency exchange platforms by knowing your customers during account creation, user verification, maintenance of transaction history, actively reporting suspicious transactions, system internal controllers, as well as affirmation of the category of criminal acts when using someone else's ID. Then, Singapore through the Monetary Authority of Singapore (MAS) also recognized cryptocurrency as a service provider that was subject to a Goods and Services Tax (GST) of 7% on buying and selling profits (Yohandi et al., 2017). Furthermore, El Salvador has legalized Bitcoin as a legal tender in its territory at the proposal of President Nayib Bukele (Ramli, 2021). Bitcoin Law in El Salvador states several things: Bitcoin will be an unrestricted legal tender; not limited in any transaction; must be accepted by the public, private companies, and legal entities; will not be subject to capital gains; promote training and mechanisms required by the community; and the creation of an institutional structure by the executive for implementing the law (Roy, 2021). Thus, the phenomenon of cryptocurrency requires a quick response from the government to keep up with blockchain and prevent crypto crime.

2. Ransomware as Implications of a Cryptocurrency Legal Void

The Covid-19 pandemic has provided an unusual impetus to technological developments and digitization. Along with these developments, borderless space is increasingly being felt by the world so that there is a warm trend to use cyptocurrency as a payment medium, like fiat currency. However, cryptocurrencies are used by cyber actors as a medium of crypto crime that has the potential to threaten the security of technology users. One form of crypto crime that has experienced a drastic increase due to the Covid-19 pandemic is ransomware. Ransomware crime is malware that restricts access to a victim's device or data and demands a ransom in exchange for stolen functionality. In general, two types of ransomwares are often used by criminal's crypto: 1) locker ransomware which locks the victim's computer access so that after the screen is locked, the perpetrator asks the victim to pay money to restore access to resources these; 2) cryptolocker ransomware that encrypts digital data from the victim's computer so that the perpetrator will ask for a ransom of money to get the encryption key (Tajriyani, 2021). From the second of this type, the most common is ransomware with a symmetric encryption scheme. Ransomware acts by encrypting the public key of crypto user data through a mechanism of command-and-control (C&C) or remote command and control (Palisse et al., 2017). When executing the ransomware action, the perpetrator will provide certain sites to provide ransom and how to pay the ransom. There are several mechanisms of ransomware ranging from distribution, infection, C&C, search for crucial data, data encryption, and demand for money as ransom for encrypted data. Then, the perpetrators will avoid using bank transfers or prepaid cards so as not to be tracked by law enforcement officials so that cryptocurrencies such as Bitcoin become the choice for perpetrators to transacting with victims because of its advantages, namely confidentiality, transfer speed, and no central bank (Palisse et al., 2017). The phenomenon of ransomware must be further understood by regulators because perpetrators will target important data belonging to digital users and threaten victims to make payments via cryptocurrency. Also, ransomware perpetrators will more often target specific companies and organizations than individual users because they will get a much higher ransom (Richardson & North, 2017).

From this thought, it can be seen that the government must know the plan of the perpetrators of ransomware and how the crime itself works. The following is a brief explanation of the criminal process of ransomware: 1) perpetrators of ransomware will try to infect the victim's device through websites, certain networks, download drives, or fake e-mails from official agencies (Ferdiansyah, 2018). The infection begins by asking the victim to download the attached file containing cryptolocker ransomware in a portable executable format (.exe); 2) if the file is already on the victim's device, the cryptolocker ransomware will automatically install and immediately connect to the perpetrator's network. Next, the perpetrator sends Shamir Adleman's Revest (RSA-2048) key to encrypt the victim's data (Kumar Sharma & Kant Verma, 2017); 3) if the cryptolocker ransomware manages to take over the device, the perpetrator will use RSA-2048 to insert a numeric code into the binary code of the victim's file, resulting in a damaged or compromised device system; 4) the initial stage of infection cryptolocker ransomware in the form of closing the entire device screen with the perpetrator program and the victim cannot access the device because they do not enter password the right; 5) after that, various information will appear from the perpetrator such as a message that your device has been infected, the count of time the data is permanently deleted, the count of the time when the ransom payment is increased, and the procedure for payment via cryptocurrency to exchange the description code; 6) to re-access the infected device, the victim must have a description code that is only owned by the perpetrator so that they are given the option to immediately make a ransom payment so that it can be exchanged for a description code; 7) as for the consequences of the victim if he does not pay, namely the permanent deletion of data. However, it was also found that the victim did not receive the description code after paying the ransom to the perpetrator. Thus, the criminal process of ransomware can be visualized in the following flowchart:

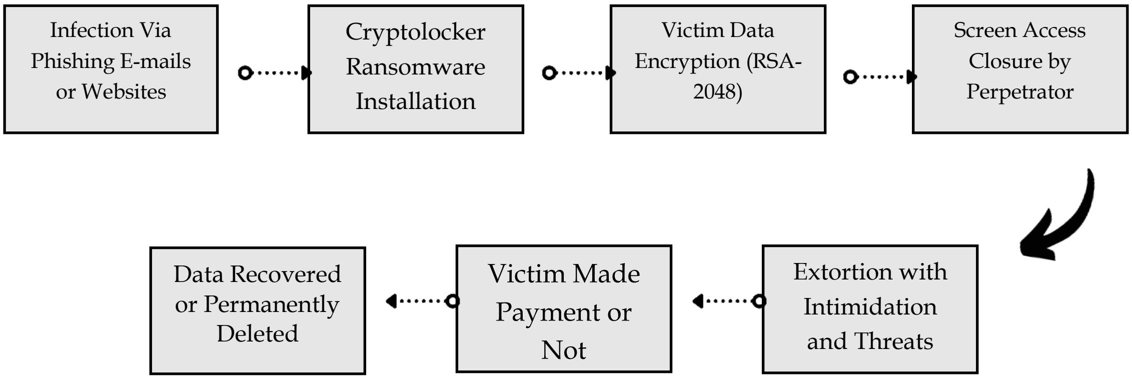
Infection Via Phishing E-mails or Websites
Cryptolocker Ransomware Installation
Victim Data Encryption (RSA-2048)
Screen Access Closure by Perpetrator
Extortion with Intimidation and Threats
Victim Made Payment or Not
Data Recovered or Permanently Deleted

Figure 3. *Crime Ransomware Process Flow*

It is undeniable that ransomware will always lurk for technology users in the digital world. This is exacerbated by the condition that Indonesia is not ready to take a stand against the phenomenon of cryptocurrency as a legal virtual currency, resulting in a legal vacuum (*rechtsvacuum*). Law or *recht* is a collection of coercive-life rules and contains orders, permits, or prohibitions to act or not to regulate public order (Nasution & Lubis, 2016). Law is defined as all rules with considerations of decency that refer to individual behavior in society and guidelines for the state to carry out their duties (Subiharta, 2015). Meanwhile, emptiness or vacuum in the Big Indonesian Dictionary (KBBI) means "emptiness". Therefore, it can be concluded that a legal vacuum is a condition of a state government related to the absence of laws and regulations in society. Then, the causes of the legal vacuum are divided into three: 1) the preparation of laws and regulations by state institutions (legislative and executive) takes a long time so that something that is intended to be regulated by regulations has changed; 2) a legal vacuum can be caused by something that has not yet been regulated in-laws and regulations; and 3) the ambiguity and incompleteness of something that wants to be regulated in the legislation (Nasir, 2017). Thus, the legal vacuum regarding cryptocurrency is caused by things that cannot be regulated in-laws and regulations because the government has not taken a firm stand regarding the position and legality of cryptocurrencies in Indonesia. Furthermore, a legal vacuum will result in legal uncertainty (*rechtsonzekerheid*) and fatally can lead to legal chaos (*rechtsverwerking*). This incident will have implications for an increase in cases of ransomware in Indonesia because the perpetrators are not bound by law and technology users have no guarantee of protection against them. With these implications, the government must provide a clear position regarding cryptocurrencies. Although cryptocurrencies have not been able to become legal tender in Indonesia, at least the government can provide regulations with strict sanctions for perpetrators of ransomware who collect ransom payments through cryptocurrencies. To overcome the legal vacuum in Indonesia, policies and initiatives from regulators are needed following Article 20 Paragraphs (1) and (2) of the 1945 Constitution of the Republic of Indonesia which states that, "The House of Representatives has the power to form laws" and "Every draft law is discussed by the DPR and the President for mutual approval. There are important points that the government must pay attention to regarding the regulation of cryptocurrencies as an effort to prevent crimes, ransomware namely making further studies of ransomware cases in the world and the experience of the WannaCry case because the global scale applied by actors can target industrial companies such as state-owned enterprises, thus threatening economic growth and cybersecurity in Indonesia.

3. The Urgency of Cryptocurrency Regulation in Indonesia

The technological speed that is not matched by legalization and explicit regulation will harm the country's cybersecurity. One of the impacts caused by the lack of clarity about cryptocurrency regulation is the increase in ransomware attacks. Currently, ransomware is a major threat in several countries and the growth of such attacks is still ongoing due to the small chance of catching the perpetrators and becoming very popular (Morse & Ramsey, 2016). It should be emphasized that ransomware is not just financial extortion in the form of cryptocurrency, but this crime can extend beyond the business industry, government, academia, to geographical boundaries. During the Covid-19 pandemic, ransomware became very dangerous and had a devastating impact on vital sectors of the country, such as health and the economy. Also, money from ransomware crimes can be misused by hackers to finance illicit activities ranging from human trafficking to the development and proliferation of weapons of mass destruction (Force, 2021). Most of the perpetrators of ransomware operate with impunity due to jurisdictions making it difficult for law enforcement officials to bring cases to court. The problem is further exacerbated by the illegal use of cryptocurrencies as a medium for paying ransom by perpetrators. Then the emergence of the model "ransomware as service" (RaaS) allows actors without technical sophistication to carry out attacks. The complexity of ransomware requires a comprehensive approach that affects the behavior of actors on all sides of the ecosystem. This approach can be implemented by blocking, disturbing the perpetrators, preparing the response of potential victims, involving important figures such as regulators, law enforcement, and national security experts. Without preventive measures, ransomware is not only risking money but will also affect people's lives, critical infrastructure, public confidence in the legitimacy of state institutions, education systems, health, economic industries, and so on. Besides, the crime of ransomware on a global scale will be fatal to countries because it threatens critical infrastructure such as military facilities and energy networks, endangers public health, diverts vital public resources, risks data loss or privacy, disrupts schools and colleges, and crippled the economy.

Ransomware attacks present urgency and national security risk in all countries, including Indonesia. As a country that uses blockchain technology, Indonesia has not recognized the existence of cryptocurrency as a legal transaction medium and has not placed it as a payment medium. This uncertainty has implications for weak enforcement of cybercrimes such as ransomware. Although Indonesia already has many regulations, such as the Criminal Code and Law No. 19 of 2016 concerning Information and Electronic Transactions, the law is not enough to solve cases of ransomware. As for the reasons why the current law does not provide justice for digitalization users, especially victims of ransomware: 1) the unclear position of cryptocurrency as a payment medium and is only considered a commodity so that it is used by criminals to carry out illegal transactions, 2) lack of competence of law enforcement officers regarding crypto crimes such as ransomware which results in ineffective law enforcement; and 3) the government's lack of attention to the crime of ransomware which is at the root of global-scale anonymous hacker attacks. In May 2017, ransomware types such as WannaCry shocked Indonesia because they infected the queue system of Harapan Kita Hospital, Dharmais Hospital, and Jember University (Indonesia, 2019). This incident is not only caused by the absence of regulation, but the behavior of the community also has a big influence on the increase in cases because most individuals tend to have low awareness of ransomware and often access adult sites. The lack of education about crypto crime is also the reason Indonesia is a target for cyberattacks. The impunity and anonymity of the perpetrators of ransomware complicate the tracking process, so the best way to do this is to take preventive measures through the legal stipulation of cryptocurrency as a transaction medium that is recognized by the state. With this legality, the perpetrator will be difficult to launch the action because it no longer has a ransom payment medium such as cryptocurrency.

Using cryptocurrencies in ransomware is a fact that must be handled responsively by the government to protect its citizens. The time effectiveness and confidentiality offered by cryptocurrencies add to the challenge of identifying the perpetrators of the ransomware as the payments are difficult to associate with any individual. Often extortion money does not flow directly from victims to perpetrators because it goes through a series of multi-step processes involving new financial entities and is not part of the standard or illegal payment market. Then, the perpetrator will apply the method-chain hopping, namely the ransom fund escape method as quickly as possible to avoid detection and tracking (Force, 2021). In this method, the perpetrators also use the method of mixing services to disrupt the public ledger by mixing legitimate traffic with extortion funds. Therefore, the following are the mechanisms for prevention efforts ransomware in Indonesia: 1) proactively carrying out well-coordinated diplomatic and international law enforcement efforts by prioritizing prevention ransomware through a comprehensive resource strategy; 2) implement aggressive and comprehensive sustainable actions; 3) voice the campaign anti-ransomware; 4) strengthening existing institutions or agencies to protect cybersecurity by prioritizing ransomware; 5) collaborate with state and industry players; 6) establish an organization related to response crypto crime and recovery funds to support cyber activity surveillance with a mandate that victims must report ransom payments and consider alternatives before making payments; 7) seek international coordination through developing systems that are clear, accessible, and capable of being widely adopted by countries to help agencies be prepared and able to respond to attacks ransomware; and 8) the sector cryptocurrency which pays medium for crimes ransomware must be regulated more strictly and firmly by requiring cryptocurrency exchanges, crypto kiosks, and mechanisms over-the-counter as transaction media to follow established regulations, including procedures know your customer and Anti-Money Laundering and Combating the Financing of Terrorism (AML-CFT) laws. As such, the threat of ransomware on a global scale of crime requires dedication, coordination, and attention from experts from policymakers to security engineers and industry leaders.

Conclusion

Cryptocurrency as a sophisticated form of blockchain technology is part of the financial taxonomy and fully contributes to the formation of cryptonomics. Also, the absence of third parties, the speed of transactions, and the guarantee of confidentiality provide distinct advantages to the existence of cryptocurrencies. Cryptocurrency has a significant difference from other currencies because it is not issued by the central bank, holding the role of a miner in digital form with a decentralized system, and accessible globally. The Covid-19 pandemic has also had a tremendous impact on the increase in the number of users of cryptocurrency so that Indonesia is said to be ready to enter a cryptocurrency and will accompany people's lives in legal transactions. Then the attraction offered by this currency attracts the attention of criminals and uses it as an illegal medium for payment of ransom. This is also caused by the government's lack of awareness of cryptocurrencies position, which has implications for the status of a legal vacuum and triggers extortion through ransomware. Ransomware is a cybercrime by infecting the victim's device and encrypting the data so that the victim has to pay a certain amount of money in crypto to get the decryption code. The mechanisms of ransomware are distribution, infection, command-and-control, search for crucial data, data encryption, and demand for money as ransom for encrypted data. With this mechanism, the victim will channel the ransom funds to the perpetrators, who then apply the technique of chain hopping, which is to escape the ransom funds as quickly as possible to avoid detection and tracking. Ransomware is not just financial extortion in the form of cryptocurrencies, but this crime can extend beyond the business industry, government, academia, to geographical boundaries. Several considerations can be used as the basis for making cryptocurrencies regulation in Indonesia, namely, requiring a cryptocurrency exchange policy, crypto kiosks, and over-the-counter mechanisms as transaction media to follow established laws including procedures for knowing your customers and AML-CFT. Therefore, regulating cryptocurrency as the ransomware prevention effort requires dedication, coordination, and attention from experts ranging from regulators to security engineers and industry leaders.

References

Addinanto, H. (2018). Determinan Penggunaan Mata Uang Kripto di Indonesia. In *Skripsi Universitas Islam Indonesia*. Universitas Islam Indonesia.

Amboro, F. Y. P., & Christi, A. (2019). Prospek Pengaturan Cryptocurrency sebagai Mata Uang Virtual di Indonesia (Studi Perbandingan Hukum Jepang Dan Singapura). *Journal of Judicial Review*, *21*(2), 14–40. https://doi.org/10.37253/jjr.v21i2.665

Azhar, S. (2021). *BI Tegaskan Minimal 10 Tahun ke Depan Cryptocurrency Tidak Boleh Jadi Alat Pembayaran*. Kontan. https://nasional.kontan.co.id/news/bi-tegaskan-minimal-10-tahun-ke-depan-cryptocurrency-tidak-boleh-jadi-alat-pembayaran#:~:text=BI tegaskan minimal 10 tahun ke depan cryptocurrency tidak boleh jadi alat pembayaran,-Minggu%2C 30 Mei&text=Sampai saat ini cryptocurrency tidak,tahun 2011 tentang Mata Uang.

Bech, M., & Garratt, R. (2017). Central bank cryptocurrencies. *BIS Quarterly Review*, *September*, 55–70. https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

Bitocto. (2021). *Perkembangan Cryptocurrency di Indonesia Sangat Pesat*. Bitocto.Com. https://bitocto.com/perkembangan-cryptocurrency-di-indonesia-sangat-pesat/

Chainalysis. (2021). *The 2021 Crypto Crime Report*. *February*.

Claeys, G., Demertzis, M., & Efstathiou, K. (2018). Cryptocurrencies and Monetary Policy. *Bruegel*, *10*. https://doi.org/10.1142/9789811201783_0022

Clara, & Nurbaiti, S. (2018). Kedudukan Hukum Bitcoin sebagai Mata Uang Virtual di Indonesia Berdasarkan Undang-Undang Nomor 7 Tahun 2011 tentang Mata Uang. *Jurnal Hukum Adigama*, *1*(1), 1–26. https://doi.org/10.24912/adigama.v1i1.2215

Custers, B., Oerlemans, J. J., & Pool, R. (2020). Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies. *European Journal of Crime, Criminal Law and Criminal Justice*, *28*(2), 121–152. https://doi.org/10.1163/15718174-02802002

Disemadi, H. S., & Kang, C. (2021). Tantangan Penegakan Hukum Hak Kekayaan Intelektual dalam Pengembangan Ekonomi Kreatif di Era Revolusi Industri 4.0. *Jurnal Komunikasi Hukum*, *7*(1), 54–71. http://dx.doi.org/10.23887/jkh.v7i1.31457

Dwicaksana, H., & Pujiyono. (2020). Akibat Hukum Yang Ditimbulkan Mengenai Cryptocurrency Sebagai Alat Pembayaran Di Indonesia. *Jurnal Privat Law*, *8*(2), 187. https://doi.org/10.20961/privat.v8i2.48407

Ferdiansyah. (2018). Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware. *JUSIFO (Jurnal Sistem Informasi)*, *2*(1), 44–59. https://doi.org/10.19109/jusifo.v4i1

Fernández-Villaverde, J., & Sanches, D. (2018). On the Economics of Digital Currencies. *Federal Reserve Bank of Philadelphia*, *7*(February).

https://doi.org/10.21799/frbp.wp.2018.07

Force, R. T. (2021). Combating Ransomware. In *Intel Security Group*.

Hakim, A. R. (2021). *200 Perusahaan di Amerika Serikat Jadi Korban Ransomware*. Liputan6. https://www.liputan6.com/tekno/read/4598221/200-perusahaan-di-amerika-serikat-jadi-korban-ransomware

Indonesia, G.-C. (2019). *Hati-Hati! Serangan Ransomware Wannacry Belum Berakhir*. Govcsirt.Bssn.Go.Id. https://govcsirt.bssn.go.id/hati-hati-serangan-ransomware-wannacry-belum-berakhir/

Kumar Sharma, G., & Kant Verma, K. (2017). Ransomware Attack in Cyber Security: A Case Study. *Technical Research Organisastion India*, *4*(10), 103–106. http://troindia.in/journal/ijcesr/vol4iss10part4/103-106.pdf

Kyriazis, N. A. (2021). A Survey on Volatility Fluctuations in the Decentralized Cryptocurrency Financial Assets. *Journal of Risk and Financial Management*, *14*(7), 1–46. https://doi.org/10.3390/jrfm14070293

Li, X., & Wang, C. A. (2017). The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin. *Elsevier*, *95*(3), 49–60. https://doi.org/10.1016/j.dss.2016.12.001

Morse, E. A., & Ramsey, I. (2016). Navigating the Perils of Ransomware. *The Business Lawyer*, *72*(1), 287–294. https://ssrn.com/abstract=2909280

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin*, 1–9. https://bitcoin.org/bitcoin.pdf

Nasir, G. A. (2017). Kekosongan Hukum & Percepatan Perkembangan Masyarakat. *Jurnal Hukum Replik*, *5*(2), 172. https://doi.org/10.31000/jhr.v5i2.925

Nasution, M. S. A., & Lubis, Z. P. (2016). *Hukum dalam Pendekatan Filsafat*. Kencana.

Nugroho, A. (2021). *Terkait Serangan ke Kaseya VSA, Bank dan BUMN Indonesia Juga Ditarget Ransomware REvil*. Cyberthreat.Id. https://cyberthreat.id/read/12018/Terkait-Serangan-ke-Kaseya-VSA-Bank-dan-BUMN-Indonesia-Juga-Ditarget-Ransomware-REvil

Palisse, A., Bouder, H. Le, Lanet, J.-L., Guernic, C. Le, & Legay, A. (2017). Ransomware and the Legacy Crypto API. *International Conference on Risks and Security of Internet and Systems*. https://doi.org/10.1007/978-3-319-54876-0_2

Priatna, T. (2019). Disrupsi Pengembangan Sumber Daya Manusia Dunia Pendidikan di Era Revolusi Industri 4.0. In *UIN Sunan Gunung Djati*. http://digilib.uinsgd.ac.id/id/eprint/29541

Ramli, R. R. (2021). *Resmi, El Salvador Jadi Negara Pertama yang Gunakan Bitcoin sebagai Alat Pembayaran*. Kompas. https://money.kompas.com/read/2021/06/10/105111126/resmi-el-salvador-jadi-negara-pertama-yang-gunakan-bitcoin-sebagai-alat

Razzaq, R. G. (2018). Legalitas Mata Uang Virtual dalam Perspektif Hukum Indonesia. *Lontar Merah*, *1*(2), 108–122. http://jom.untidar.ac.id/index.php/lontarmerah/article/view/346

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, *13*(1), 10–21. https://digitalcommons.kennesaw.edu/facpubs/4276/

Roy, A. (2021). *El Salvador's Bitcoin Law: Full English Text*. Freopp.Org. https://freopp.org/el-salvadors-bitcoin-law-full-proposed-english-text-9a2153ad1d19

Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.

Subiharta. (2015). Moralitas Hukum dalam Hukum Praksis sebagai Suatu Keutamaan (Legal Morality in Practical Law as a Virtue). *Jurnal Hukum Dan Peradilan*, *4*(3), 385–398. https://doi.org/10.25216/jhp.4.3.2015.385-398

Syamsiah, N. O. (2017). Kajian Atas Cryptocurrency Sebagai Alat Pembayaran di Indonesia. *Indonesian Journal on Networking and Security*, *6*(1), 53–61. https://doi.org/10.2311/ijns.v6i1.1449

Tajriyani, N. S. (2021). Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker. *Jurist-Diction*, *4*(2), 685. https://doi.org/10.20473/jd.v4i2.25785

Ulya, F. N. (2021). *Harga Bitcoin Perlahan Turun dari Rekor Tertinggi Sepanjang Sejarah*. Kompas. https://money.kompas.com/read/2021/04/19/082101426/harga-bitcoin-perlahan-turun-dari-rekor-tertinggi-sepanjang-sejarah?page=all

Wuragil, Z. (2020). *Enterprise Target Utama Serangan Ransomware di Indonesia, WFH Jadi Celahnya*. Tempo. https://tekno.tempo.co/read/1382050/enterprise-target-utama-serangan-ransomware-di-indonesia-wfh-jadi-celahnya

Yohandi, A., Truhastuti, N., & Hartono, D. (2017). Implikasi Yuridis Penggunaan Mata Uang Virtual Bitcoin Sebagai Alat Pembayaran Dalam Transaksi Komersial (Studi Komparasi Antara Indonesia-Singapura). *Diponegoro Law Journal*, *6*(2), 1–19. https://doi.org/10.1017/S0269888907001014