

Abuse of Cryptocurrency to Funding International Terrorism Activities

Andhika Tegar Wardhana¹ Bambang Wahyu Nugroho²

¹Dept. of International Relations, Faculty of Social and Political Sciences, UMY, Yogyakarta, Indonesia, 55183

²Dept. of International Relations, Faculty of Social and Political Sciences, UMY, Yogyakarta, Indonesia, 55183

Email: andhika.tegar.isip17@mail.umy.ac.id; bambangwn@umy.ac.id

ABSTRACT

Terrorist organizations began to adjust themselves with the development of information and communications technology, especially in their efforts to finance their activities. **Cryptocurrency** is one of the latest advancement in financial technologies which is potentially support their actions. Even, it has already actualized in some cases. This research aims to examine what underlies terrorist organizations to start using **cryptocurrency** and to find forms of its recent activities and its further possibilities. This research uses qualitative approach through examining some sample cases and tries to extrapolate it into larger phenomena. The data obtained in the form of secondary data, namely data from books, articles, academic papers, journals, news, as well as electronic media. This research applies the theory of international crime to frame that terrorist organizations are illegal entities, theory of disruptive technology to describe the nature of cryptocurrency as a new form cyber-based financial technology, and theory of the diffusion of innovation to explain why in the recent internet era, cryptocurrency has a large potential to attract financial investments globally. This work found that terrorist organizations has been starting to use cryptocurrency to finance their activities based on its anonymous and less-regulated natures, both are delivering a new challenge of cybercrimes beyond the conventional scrutiny in finance and banking transfer, as well as counterattacks toward money counterfeit and money laundering.

Keywords: cryptocurrency, cybercrime, terrorism, terrorist organizations.

INTRODUCTION

Terrorist financing is a process by which terrorists obtain funds to carry out acts of terror. Terrorists need support and funds, both cash and non-cash, especially those not included in the conventional banking system. The larger the support they receive, the terrorist acts carried out will be more extensive and frequent. In obtaining support for carrying out acts of terror, terrorist organizations receive various forms of supply from multiple supporters. The assistance can be in the form of weapons, money, supplies, and many more. In addition to obtaining funds from donors or supporters, terrorist organizations also earn money through membership fees, drug transactions, fraud, human trafficking, and cybercrime (Irwin & Milad, 2016, p. 408).

Internet creates advancements in many aspect including economy, the cryptocurrency is one of the example. Cryptocurrency is a virtual currencies that created in public internet, not created by government or institution. Financial Action Task Force (FATF) describes cryptocurrency as a

exchange unit but not legally issued by any jurisdiction (Sountra, 2019). One of the example is bitcoin.

In the context of competition, when a new technology is born and carries characteristics that are superior to existing technology, it will trigger disruption (Smith, 2020). In this regard, cryptocurrencies challenge conventional financial systems with their simple and efficient characteristics. Its transactions are transnational in nature, fast, much cheaper fees, and are not controlled by any banking authorities. As consequence, a number of countries have banned cryptocurrencies in some or all of their uses. (Chohan, 2017). Furthermore, its pseudo-anonymity could be interesting to cybercriminals and terrorist organization. (Reddy & Minnaar, 2018) (Bray, 2016) (Brown, 2016) (Zhou, Zhuge, Fan, Du, & Lu, 2020) (Higbee, 2018).

More than its illegal activities, organized terrorism is also funded with financial sources which most of it are out of law. Some of the funds, indeed, come from "legal" sources such as donors or membership dues. However, terrorist organizations also get a supply of funds from the conduct of fraud, drug transactions, human trafficking, as well as cybercrime. (Irwin & Milad, 2016, p. 408)

The purpose of this paper is to provide evidence of how cryptocurrencies have been used to finance terrorist organizations and to discuss the possibilities for anticipating its further abuse.

PREVIOUS STUDY AND THEORITICAL FRAMEWORK

Terrorist groups have started to abuse cryptocurrencies as a means to carry out transactions. The scientific work by Raihan Zahirah Mauludy Ridwah entitled "The Utilization of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes". The research question of this paper is to find how does the terrorist organizations uses technology advancement such as cryptocurrency as an alternative way of *hawala* tradition for illicit purposes and to find how to tackle the problem it caused. Also, the paper explains this issue by applying the theory of criminal organization by Martha Crenshaw, this theory mainly discusses the objectives, actions and dynamics of the terrorist organizations. The second theory or concept applied in the paper is the concept of digital counterterrorism the efforts to combat against terrorism in digital world (online). From the paper it can be concluded that terrorist organizations need to withstand external pressures that threaten their operational activities, especially in their field like the presence of massive intelligence and military troops surrounding their environment making it became hostile to terrorist group to operate. Therefore, terrorist groups need to find alternatives to respond to these pressures and survive, one of which is

by abusing cryptocurrency as a means of their transactions and using advantages through darkweb. Also this paper mentions some of the example of cryptocurrency usage by terrorist group. The journal has a research subject in line with this research, namely researching the use of cryptocurrencies by terrorists, but this study will apply a different theoretical point of view by using the method listed below.

This research uses the theory of international crime, the theory of disruptive technology, and the diffusion of innovation theory. First, the international crime itself is an act that is universally recognized as a crime. International recognition of this act shows that transnational crime is a problem that needs to be controlled. A criminal act is considered an international crime if: it has elements of threatening the peace and security of humanity. There is a transnational element that affects not only one country but also an aspect of necessity that encourages countries to fight crime (Wahjoe, 2011). Terrorism is an extraordinary crime that is included in international crimes because it poses threats and losses to various countries.

Disruptive technology is a theory by Clayton Christensen. Disruptive technology refers to a technology that can threaten the existence of current technology. It often contains characteristics that are unthinkable, innovative, and unexpected to attract people's interest. Disruptive technology is often considered interfering with existing technologies. It can affect consumer behaviour, industry, and how businesses operate because it is more profitable and practical. Because of this, disruptive technology has the potential to replace old technology over time (Limba, Stankevičius, & Andrulevičius, 2019). This theory explains the nature of cryptocurrency as a new form of cyber-based financial technology that may affect current financial procedures.

Diffusion of Innovation is a theory by E.M Rogers. Diffusion of innovation is a process where innovation is communicated through several channels over time among members of a social system (Rogers, 1962). E.M. Rogers also explains the process of innovation diffusion. There are five different groups of people. They are innovators, early adopters, early majority, late majority, and laggards.

METHOD

This research uses a qualitative approach and research methods through documents. The data obtained is in the form of secondary data through reading and analyzing. The data obtained is from books, articles, academic papers, journals, news, as well as electronic media.

RESULT

In historical context, the recent terrorist actions are “more of a galling nuisance than a truly destabilizing force, except for its psychological impact.” (Chaliand & Blin, 2007). So far, international counterterrorism enforcement has succeeded in preventing possible major acts of terror like 9/11 that occurred in 2001. So far, the enforcement of international counter-terrorism has succeeded in preventing the possibility of major acts of terror such as 9/11 that occurred in 2001. However, acts of terrorism on a small and medium scale still continue to occur in various places in the

world. In general, the “nuisance” is more directed at the interests of the United States as the leader of “free world” and its allies or supporters.

Of course, the terrorist groups need a lot of money to finance their networks and actions. The money is used to recruit and train new members, forged documents, to conduct bribery, to purchase logistics, equipment, and weapons, to support terrorist families, as well as fund the execution of terrorist acts and propaganda through media. The financial supports come from various sources, such as regimes in certain countries and non-state actors. States support began to diminish since the end of the Cold War (Triskaputri, Satrya, & Wardoyo, 2020), however, support from non-state actors still continues to exist in the form of collecting “charities”, donations from individuals or institutions. (Freeman, 2011).

Then, the movement of funds within a terrorist organization is also crucial in carrying out an attack. Transferring funds used by terrorist organizations include money couriers, hawala, financial services, trade misinvoicing, and banks. In addition, terrorist groups also carry out various criminal acts to raise funds. They justify fraud, robbery, ransom of hostages, and human trafficking. Their more colossal act in making a lot of money, however, is their involvement in the illicit drug trade. They are currently starting to incorporate the cryptocurrency business into it.

Cryptocurrency is a virtual currency or digital asset used as a medium of exchange with a cryptographic process. A cryptographic process is a method used to protect information and communication channels through codes, where the codes can only be read and processed by those who have exclusive access (Oliver, 2021).

The development of cryptocurrency began in 1980. David Chaum, a cryptographer from America, discovered an algorithm that allows a secure exchange of information called “blinded money”. 1989 David Chaum develops his findings into DigiCash, a payment system on the internet. DigiCash also issued cyberbucks, which is the currency used to transact in it. DigiCash went bankrupt in 1998 due to its non-decentralized nature, which resulted in a monopoly in supply control (Bowbrick, 2003). In the same year, Wei Dai published an article on the concept of a virtual currency, namely b-money. His writing describes a working concept like the concept of modern cryptocurrencies. Then other currencies began to appear, such as bit gold by nick Szabo, Hashcash, which uses proof of work algorithm to prevent DDoS attacks, and e-gold, which is a medium for buying and selling digital gold (Coinvestasi, 2018) (Reiff, 2019). The era of modern cryptocurrency begins with the emergence of bitcoin. Satoshi Nakamoto issued a draft in 2008. In early 2009, bitcoin was released to the public. By applying the innovation diffusion theory, this stage is the innovator stage.

Then other currencies began to appear, such as bit gold by nick Szabo, Hashcash, which uses proof of work algorithm to prevent DDoS attacks, and e-gold, which is a medium for buying and selling digital gold (Coinvestasi, 2018) (Reiff, 2019). The era of modern cryptocurrency begins with the emergence of bitcoin. Satoshi Nakamoto issued a draft in 2008. In early 2009, bitcoin was released to the public. By

applying the innovation diffusion theory, this stage is the innovator stage.

The release of bitcoin was well received by its fans. Hal Finney is known as an early adopter of this currency. Hal Finney received 50 BTC from Satoshi for his support, making it the first transaction on the bitcoin blockchain network and being the first recipient of BTC. Peter Saddington, an entrepreneur, bought BTC when the price was \$2.52 in 2011. Peter bought about 45 BTC at that time and made a significant profit in 2017 when the price of BTC started to soar since this is Peter became a bitcoin investor (The Guardian, 2020). In 2010, bitcoin was used for the first time as a transaction tool, namely in purchasing two Papa John's pizza pans, to be exact 22 May 2010. Lazlo Hanyecz paid 10,000 bitcoins (which is currently worth 25 dollars) for the pizza. This event was later remembered as "bitcoin pizza day" (Hankin, 2019). This stage is the early adopter stage. The popularity of bitcoin has also led the birth of other cryptocurrencies with a working base like bitcoin, such as Ethereum, Litecoin, Dogecoin, Binance Coin, Cardano Coin, and so on.

Bitcoin became a hot topic of conversation by the media after its emergence. In addition, the price continues to rise. 2 years after its appearance, the cost of bitcoin reached 1 dollar per BTC. Bitcoin also began to accept exchange for other currencies such as British pounds, Brazilian reals, and euros, making the scope of its trade wider (Makhul, 2011). In late 2012 WordPress became the first company to accept bitcoin for payment, followed by Expedia, Microsoft, and Tesla recently. PayPal also uses cryptocurrencies so that users can make transactions using that currency directly through their accounts. In addition, users can also monitor the current price through the PayPal application. The cryptocurrencies supported by PayPal are bitcoin, Ethereum, Litecoin, and bitcoin cash (Lyles, 2021). The use of cryptocurrency by large companies indicating the early majorities in the diffusion of innovation process.

Cryptocurrency has become a disruption to the conventional banking system. Cryptocurrencies have characteristics such as faster international transactions, no additional fees, and are not regulated by third parties, making them more efficient. When a technology has superior features to existing technology, it will trigger disruption (Smith, 2020). Some countries have banned cryptocurrencies from being used as legal tender for fear that it will bring instability to the payment system in the country that triggers inflation. Then concerns about its relationship with criminal activity. Indonesia is one of the countries that prohibits cryptocurrency as a means of payment (Widyastuti & Antara, 2021) (Friana, 2021). Not all people know or use cryptocurrency. Some countries consider this currency to be illegitimate as a means of payment. Then, some people are still sceptical to cryptocurrencies because of their association with illegal acts, money laundering and their unstable value. It takes time, communication channels, and social conditions that begin to adapt to spread to the next population in the innovation diffusion model.

Cryptocurrencies are being misused by criminals for illegal actions. Cryptocurrencies are related with the darknet because of their anonymity and unregulated nature. Due to that characteristic, cryptocurrencies can be used to trade

illicit goods on the internet's black market. In addition, another misuse of cryptocurrencies is ransomware. Ransomware is a computer virus that victim's computer data. One example of a ransomware attack is WannaCry in 2017, where the perpetrators asked for a reward in the form of bitcoins to recover the victim's data (Rooney, 2021). Next, there was a case of fraud with cryptocurrency through hacking a public figure's Twitter account. The hacked accounts spread tweets about bitcoin frauds. Other crimes have also begun to take advantage of cryptocurrencies, such as money laundering and terrorism financing.

In this context, there was concerns in the US Congress against the use of cryptocurrencies by terrorist groups as expressed in a document entitled "Survey of Terrorist Groups and Their Means of Financing". In the introduction, the Chair of the Subcommittee on Terrorism and Illicit Finance, Stefan Pearce, stated that Al-Qaida conducted fundraising and campaign with cryptocurrencies. (Survey of Terrorist Groups and Their Means of Financing, 2018). Furthermore, the document is also revealing the other terrorist group, Hezbollah, for its proliferation in financing its activities, includes the possibilities to use cryptocurrencies. (Ibid, 2018).

Fundraising through cryptocurrency is a practice that terrorist organizations often use. This will facilitate donors who want to support terrorists without worrying about their identity being exposed. Backers can transfer their cryptocurrency directly or through a broker.

The United States Department of Justice, on Thursday, August 13, 2020, managed to confiscate and dismantle cryptocurrency transactions used by terrorist organizations. United States authorities seized millions of dollars, more than 300 cryptocurrency accounts, four websites, four Facebook accounts linked to a cryptocurrency scheme run by Al-Qaeda, ISIS, and the Al-Qassam Brigades (Savage, 2020).

2019 Al-Qassam Brigades group formed a fundraising scheme through cryptocurrency. This group made posts on their social media pages asking for donations in bitcoins for terror activities. This fundraiser is also uploaded to their official website. Al-Qassam Brigades emphasizes that donations via bitcoin are undetectable. Their website attached a video instruction on how to donate anonymously using a unique bitcoin address created for each donor. Each individual will get a different bitcoin address making it difficult to track. The site is also available in seven languages (Popper, 2019).

Jonathan Xie was arrested for attempting to provide material support for the terrorist organization Al-Qassam. In April 2019, he offered the Al-Qasam website link to one of the online FBI agents undercover. Xie referred to the Hamas website and explained that he had previously sent donations to the terrorist organization. Xie then sent a screenshot of the website to an undercover agent and demonstrated how to use a new feature on the website that allows donations to be sent via bitcoin. On 26 April 2019, Xie sent a gift of 20 dollars in bitcoin (including tax) via the website to check that the donation via bitcoin feature is working correctly (The United States Departement Of Justice, 2019).

Al-Qaeda, a terrorist based in Syria, is also suspected of using a cryptocurrency fundraising scheme through social media. In some cases, the organization stated that fundraising was done for charity, but the funds raised were used to buy weapons. An organization within the Al-Qaeda network, Al-Sadaqqah, has also been accused of using Facebook and Telegram to raise funds with bitcoin to finance jihadists in Syria. Reports show that around 0.075 bitcoins were sent by anonymous donors (Malik, 2018). At the start of his campaign, Al-Sadaqqah asked for \$750 to fund the camp, and their bitcoin address accepted \$685 worth of bitcoins. The group continues to solicit funds for various purposes, sometimes sending videos showing the conditions of their camp in the mountains. Al-Sadaqqah does not only accept bitcoin as a means of raising funds. In early 2018 they started accepting other cryptocurrencies such as Monero, Dash, and Verge. These cryptocurrencies have a stronger level of anonymity than bitcoin.

In mid-2018, Mahlama Tactical Group, another Syrian militant group inspired by Al-Sadaqqah's methods using cryptocurrency. The group's funding sources came from contracts to train terrorist soldiers and military aid, then began soliciting donations during the financial crisis in 2017. The founder of the Mahlama Tactical was reportedly killed in 2017, and Abu Salman Belarus leads the group. Abu Salman Belarus is a follower of the social media Al-Sadaqqah. He uses Twitter to provide updates on Mahlama Tactical. In 2018, Abu Salman sent his group's bitcoin address asking for donations, after that the tweet was later deleted. According to Yaya Fanusie's report, the address found bitcoin worth less than \$100 (Fanusie, Survey of Terrorist Groups and Their Means of Financing, 2018).

The former affiliate of Al-Qaeda, namely Hay'at Tahrir Al-Sham (HTS), which controls the Idlib region, Syria, is openly pro-cryptocurrency. In 2019 HTS called bitcoin the currency of the future economy and released a 26-minute video of HTS clerics discussing bitcoin's compatibility with Sharia law. HTS also regularly promotes BitcoinExchange, a cryptocurrency community run by HTS that accepts buying and selling cryptocurrencies with cash since June 2019 (O'Leary, 2021).

Like the Al-Qassam Brigades (Hamas) and Al-Qaeda and its former affiliate HTS, ISIS has also begun to involve themselves in cryptocurrency schemes. ISIS has a dark website called Isdarat, which can only be accessed through the TOR (The Onion Router) network. Apart from spreading propaganda, the site also asks for donations, one of which is through cryptocurrency (Ridwan, 2019). This site utilizes several Telegram channels to send propaganda in videos and others (Mohammed, 2015).

Al Khilafah Aridat: The Caliphate Has Returned is a pro-ISIS blog that explains how bitcoin can be used to finance them. The blog also explains that bitcoin cannot be tracked by the government, has a decentralized nature, and facilitates cross-border transactions (Charles, 2014). The blog also describes the use of DarkWallet. DarkWallet can provide bitcoin users with additional protection for their privacy and identity. In January 2015, a cell from ISIS held a fundraiser via the darkweb, via bitcoin. Fundraiser Abu Mustafa managed to collect five bitcoins, which cost around

\$ 1000 before his account was successfully blocked by the FBI (Harman, 2015).

The Ibn Taymiyya Media Center (ITMC) is an online jihadist propaganda unit based in the Gaza Strip. This group is the media wing of the Mujahideen Shura Council (MSC). The Mujahideen Shura Council was categorized as a terrorist organization by the United States Department of State in 2014. ITMC launched an online campaign called Jahezona (equip us in Arabic) which began in 2015. This campaign invites Muslims around the world to send donations to each other. This campaign also regularly sends infographics regarding the need for weapons and ammunition as well as their prices. At the end of June 2016, this campaign added the option of paying via bitcoin, an infographic regarding this payment was posted on Twitter and a QR code for the bitcoin wallet address. The campaign aims to raise \$2500 for each militant. The address has only received 0.929 BTC (approximately \$540) of bitcoin through two transactions with an interval of six days (0.893 BTC on the first transaction and 0.0359 BTC on the second) (Fanusie, The New Frontier in Terror Fundraising: Bitcoin, 2016).

Several individuals linked to ISIS also played a role in the scheme of using this currency. An example is Ali Shukri Amin, a 17-year-old Virginia resident who provides support and instruction to ISIS and its supporters by teaching them how to use bitcoin and the encryption platform to hide it. Ali used his Twitter account @Amreekiwitness to give ISIS supporters a guide on using bitcoin to hide donations. Since 2014, this young man has been posting bitcoin usage guides for extremist groups (Abutaleb & Cooke, 2016). Ali also wrote an essay in the blog entitled "Bitcoin and The Charity of Jihad". The paper explains that bitcoin is an alternative currency for ISIS after criticizing foreign currency as a transaction tool (Sanders, 2015). Ali was arrested in Virginia in February 2015 and sentenced to 11 years in prison and fined \$100,000.

In 2017, Zoobia Shahnaz, a woman from Long Island, New York, was sentenced to 13 years in prison for providing material support to ISIS (Mangan, 2018). From March to July 2017, Shahnaz was involved in a fraudulent scheme against several financial institutions to obtain money for ISIS, one of which illegally borrowed \$22,500 from a Manhattan bank. Shahnaz was engaged in a fraudulent scheme against Chase Bank, TD Bank, American Express, and Discover by illegally obtaining six different credit cards. The credit card received was used to buy bitcoin and other cryptocurrencies for over \$62,703. After getting money with the scheme, he made wire transfers (money transfers between banks for different countries) of \$150,000 to various ISIS sympathizers in Pakistan, China, and Turkey. Shahnaz then plans to go to Syria with a Pakistani passport and quit his job. July 31, 2017, Shahnaz was arrested at John F. Kennedy airport in New York (The United States Department of Justice, 2020).

Then acts of terrorism-related to cryptocurrencies also occurred in Indonesia. One of them is the bombing at Mall Alam Sutera on October 28, 2015, by Leopard Wisnu, a lone terrorist. His terrorist act was motivated by extortion by asking the mall management for 100 bitcoins and threatening to bomb the mall. Mall Alam Sutera gave the

perpetrator 0.25 bitcoins (worth 700.000 rupiahs at the time), the bomb placed by the perpetrator exploded in the mall employee cafeteria (Cahaya, 2015). In addition to economic reasons, the perpetrators also often saw and followed news related to ISIS before carrying out the bombing. The perpetrator was also inspired by the bomb at ITC Depok (Tempo, 2015). In 2016, a pro-ISIS party based in Majalengka, West Kalimantan, proposed the idea of raising funds through bitcoin but was discontinued because it was deemed too complicated. October 2018, ` Abu Ahmed Foundation, an extremist charity in Indonesia that supports the Hay'at Tahrir Al-Sham (HTS) rebel group in Syria. The charity raises funds using cryptocurrencies, encouraging supporters to donate using cryptocurrencies such as bitcoin, monero, dash, and verge. In 2016, a pro-ISIS party based in Majalengka, West Kalimantan, proposed the idea of raising funds through bitcoin but was discontinued because it was deemed too complicated. October 2018, ` Abu Ahmed Foundation, an extremist charity in Indonesia that supports the Hay'at Tahrir Al-Sham (HTS) rebel group in Syria. The charity raises funds using cryptocurrencies, encouraging supporters to donate using cryptocurrencies such as bitcoin, monero, dash, and verge.

Bahrn Naim, one of the Indonesian militants who fought with ISIS in the Middle East, uses online payment services such as PayPal and bitcoin to transfer money to his colleagues back home to finance terrorist activities, especially in Java. In 2016, in an online manual written by Bahrn Naim, he listed bitcoin as a method of transferring funds to launder the proceeds from carding. PPAATK reported that Bahrn Naim had transferred money to his partner using PayPal, where the funds came from bitcoin. The funds were used to fund a suicide attack at the Solo Police Headquarters, Central Java, in July 2016. The total amount of funds was not explained by PPAATK according to PPAATK's director of inspection and research, Ivan Yustiavand, that PayPal and bitcoin were used so that terrorists could evade the monitoring of law enforcement who traced their path. Transactions through the banking system (Arianti & Yaorren, 2020).

May 2020, the Philippine Institute for Peace, Violence, and Terrorism Research (PIPVTR) reported that terror groups linked to IS were conducting transactions with cryptocurrencies, according to reports of terrorist-related money laundering acts involving cryptocurrencies. The proceeds were used to finance terror networks' activities in the Mindanao region, Southern Philippines, where still under conflict at that time (Philippine Institute for Peace, Violence, and Terrorism Research, 2020).

India's National Investigation Agency (NIA) claims in its formal accusation that one of the IS (Islamic State) individuals, namely Jahanzaib Sami, is accused of using cryptocurrencies in terror activities in India. Jahanzaib Sami and his wife Hina Bashir were arrested in Delhi on March 8, 2020. According to an NIA report, the two perpetrators received bitcoin wallet addresses via Threema, an instant messaging app from an account called "Caged Pearls," whose owner is a British woman based in Syria. "Caged Pearls" gave Sami the wallet's address and asked him to send money into it. Then Sami also asked his colleagues to send money into the wallet. In addition, Sami also has relations with Libyan-based IS individuals with the identity

of "Sech Tech". "Sech Tech" is a member of the intel and IS media unit and tells Sami that he works on the darkweb and provides bitcoins to fund the organization. Sami and "Sech Tech" discussed fund management through the blockchain system and discussed its potential to purchase explosive weapons and raw materials. The two also discussed the use of stolen credit cards for weapons procurement (Chauhan, 2020).

The use of cryptocurrency by terrorist organizations above has shown that technological advances and innovations bring convenience for ordinary people to help with daily activities. This progress can also be a steppingstone for criminals and terrorists to simplify their operations, especially with the internet making it easier to exchange information. The existence of darknets and VPNs also helps them move online undercover and expand the scope of operations between countries, and this is an additional challenge in dealing with terrorism, not only directly in the field but also requires attention in cyberspace.

CONCLUSION

Despite its high-cost operations, the governments supported by professional bodies and private financial institutions apply stricter regulations and law enforcement to counter money laundering, illegal transaction, and suspicious money transfer activities. (Leong, 2007). On the one hand, it can suppress the financial capacity of terrorist organizations. However, on the other hand, it can trigger them to intensify their efforts in financing their activities in the "blue ocean" of the anonymous, poorly regulated, and uncontrolled realm of the cryptocurrency.

The nature of anonymity, however, will remain the most important attraction of cryptocurrencies in the context of cybercrimes, especially to funding terrorist organizations.

Three targets of terrorism that must be anticipated are, first, hacking actions to disrupt, weaken, or damage official government websites, especially those of strategic and critical value. This can be overcome by continuously improving the quality of cybersecurity protection. Second, in the "real world" outside cyberspace, acts of terror are the end of a series of pre-actions that require material equipment. Therefore, what needs to be monitored is the use of cryptocurrencies to exchange into "real" currencies or to purchase tools to support any acts of terror. It is easier, indeed, to find those patterns so it can be prevented using counterterrorism operations, far more possible than finding out the identity of the terrorist behind the hash code of a cryptocurrency transaction which is almost impossible to do. In conclusion, therefore, national authorities along with its international bodies of counterterrorism now deal with a new kind of money laundering, say, a "cryptolaundrying". This laundering happens when a cryptocurrency is transferred to many persons who act as shadow businesspersons and cover it with legal businesses.

REFERENCE

Abutaleb, Y., & Cooke, K. (2016, June 6). *Extremists Among Us: A teen's turn to radicalism and the U.S. safety net that failed to stop it*. Retrieved

- from Reuters Investigates:
<https://www.reuters.com/investigates/special-report/usa-extremists-teen/>
- Arianti, V., & Yaorren, K. Y. (2020, June 30). *How Terrorists Use Cryptocurrency in Southeast Asia*. Retrieved from The Diplomat:
<https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia/>
- Bauer, K. (2018, September 7). *Survey of Terrorist Groups and Their Means of Financing*. Retrieved from washingtoninstitute.org website:
<https://www.washingtoninstitute.org/media/1321>
- Bowbrick, S. (2003, February 25). *Past Currency*. Retrieved from The Guardian:
<https://www.theguardian.com/technology/2003/feb/25/comment.comment>
- Bray, J. (2016, August). *Anonymity, Cybercrime and the Connection to Cryptocurrency*. Retrieved from ProQuest:
<https://www.proquest.com/openview/6b6b90e3ec22811be1f2cf6f6a060a52/1?pq-origsite=gscholar&cbl=18750>
- Brown, S. D. (2016, July 25). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal: Theory, Practice and Principles*, 327-339.
doi:<https://doi.org/10.1177/0032258X16658927>
- Cahya, K. D. (2015, October 29). *Teroris Peras Mall Alam Sutera dengan Minta Tebusan Bitcoin*. Retrieved from Kompas:
<https://megapolitan.kompas.com/read/2015/10/29/16441531/Teroris.Peras.Mall.Alam.Sutera.dengan.Minta.100.Bitcoin>
- Chaliand, G., & Blin, A. (Eds.). (2007). *The History of Terrorism From Antiquity to Al Qaeda*. (E. Schneider, K. Pulver, & J. Browner, Trans.) Berkeley and Los Angeles: University of California Press, Ltd.
- Charles, B. S. (2014, October 29). *ISIS. Are they Using Bitcoins to Fund Criminal Activities?* Retrieved from Security Intelligence:
<https://securityintelligence.com/isis-are-they-using-bitcoins-to-fund-criminal-activities/>
- Chauhan, N. (2020, October 23). *IS operative caught in Delhi used Bitcoins to fund terrpr. Its India's first: NIA*. Retrieved from Hindustan Times:
<https://www.hindustantimes.com/india-news/nia-charge-sheet-alleges-bitcoins-used-by-is-operatives-to-fund-terror-activity/story-1qVgzJ5Ipi3t2DCrPmWpvO.html>
- Chohan, U. W. (2017, September 20). *Assessing the Differences in Bitcoin & Other Cryptocurrency Legality across National Jurisdictions*. Retrieved from SSRN:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3042248
- Coinvestasi. (2018, September 3). *Proof-of-Work vs Proof-of-Stake: Panduan Dasar Mining*. Retrieved from Coinvestasi:
<https://coinvestasi.com/belajar/proof-of-work-vs-proof-of-stake-panduan-dasar-mining/>
- Fanusie, Y. (2016, August 24). *The New Frontier in Terror Fundraising: Bitcoin*. Retrieved from The Cipher Brief:
https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin
- Fanusie, Y. (2018, 7 September). *Survey of Terrorist Groups and Their Means of Financing*. Retrieved from
https://financialservices.house.gov/uploadedfiles/09.07.2018_yaya_fanusie_testimony.pdf
- Freeman, M. (2011). The Sources of Terrorist Financing: Theory and Typology. *Studies in Conflict & Terrorism*, 34, 461-475.
doi:10.1080/1057610X.2011.571193
- Friana, H. (2021, Februari 26). *Uang Digital Bank Sentral, Upaya BI Bendung Bitcoin*. Retrieved from CNN Indonesia:
<https://www.cnnindonesia.com/ekonomi/20210226062635-78-611113/uang-digital-bank-sentral-upaya-bi-bendung-bitcoin>
- Hankin, A. (2019, June 25). *Bitcoin Pizza Day: Celebrating the \$80 Million Pizza Order*. Retrieved from Investopedia:
<https://www.investopedia.com/news/bitcoin-pizza-day-celebrating-20-million-pizza-order/>
- Harman, D. (2015, January 29). *U.S.-based ISIS Cell Fundraising on the Dark Web, New Evidence Suggests*. Retrieved from Haaretz:
<https://www.haaretz.com/.premium-isis-uses-bitcoin-for-fundraising-1.5366305>
- Higbee, A. (2018, July). The role of crypto-currency in cybercrime. *Computer Fraud & Security Vol. 2018, Issue 7*, 13-15.
doi:[https://doi.org/10.1016/S1361-3723\(18\)30064-2](https://doi.org/10.1016/S1361-3723(18)30064-2)
- Irwin, A. S., & Milad, G. (2016). The use of cryptocurrencies in funding violent jihad. *Journal of Money Laundering Control*, 407-425.
- Leong, A. V. (2007, May 15). Chasing dirty money: domestic and international measures against money laundering. *Journal of Money Laundering Control Vol. 10, No. 2*, 140-156.
doi:<https://doi.org/10.1108/13685200710746857>
- Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). Cryptocurrency As Disruptive Technology: Theoretical Insight. *Journal of Entrepreneurship And Sustainability Issues*, 6(4), 2068-2080.

- Lyles, T. (2021, March 30). *PayPal will let US users pay with Bitcoin, Ethereum, and Litecoin starting today*. Retrieved from The Verge: <https://www.theverge.com/2021/3/30/22357246/paypal-buy-with-bitcoin-litecoin-ethereum-crypto-checkout>
- Makhul. (2011, April 05). *BitMarket.Eu has Closed Down*. Retrieved from Bitcoin Forum: <https://bitcointalk.org/index.php?topic=5441.0>
- Malik, N. (2018, August 31). *How Criminals And Terrorists Use Cryptocurrency: And How To Stop It*. Retrieved from Forbes: <https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-usecryptocurrency-and-how-to-stop-it/#6766399a3990>
- Mangan, D. (2018, November 26). *New York woman pleads guilty to using bitcoin to launder money for terror group ISIS*. Retrieved from CNBC: <https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-usingbitcoin-to-launder-money-for-isis.html>
- Mohammed, R. (2015, November 3). *ISIS Has a New Favorite Social Media Network*. Retrieved from The Fiscal Times: <https://www.thefiscaltimes.com/2015/11/03/ISIS-Has-New-Favorite-Social-Media-Network>
- n.n. (2018). *Survey of Terrorist Groups and Their Means of Financing*. Washington, D.C.: The U.S. Government Publishing Office. Retrieved from <https://www.govinfo.gov/content/pkg/CHRG-115hhrg31576/html/CHRG-115hhrg31576.htm>
- O'Leary, R.-R. (2021, March 31). *The bitcoin terrorists of Idlib are learning new tricks*. Retrieved from Wired: <https://www.wired.co.uk/article/bitcoin-crypto-terrorism-syria>
- Oliver, A. (2021, January 19). *Kenali Kriptografi, Sistem Pengkodean yang Dapat Melindungi Data-Data Penting*. Retrieved from glints: <https://glints.com/id/lowongan/kriptografi-adalah/#.YDJpdtXitPY>
- Philippine Institute for Peace, Violence, and Terrorism Research. (2020, May 20). *Terrorism Financing Continues Unabated During the Covid 19 Pandemic*. Retrieved from Philippine Institute for Peace, Violence, and Terrorism Research: <https://pipvtr.wordpress.com/2020/05/20/terrorism-financing-continues-unabated-during-the-covid-19-pandemic/>
- Popper, N. (2019, Agustus 18). *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*. Retrieved from The New York Times: <https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html>
- Reddy, E., & Minnaar, A. (2018, September 1). *Cryptocurrency : a tool and target for cybercrime. Acta Criminologica : African Journal of Criminology & Victimology Vol. 31, No. 3*. Retrieved from <https://hdl.handle.net/10520/EJC-14d902942d>
- Reiff, N. (2019, June 25). *Were There Cryptocurrencies Before Bitcoin?* Retrieved from Investopedia: <https://www.investopedia.com/tech/were-there-cryptocurrencies-bitcoin/>
- Ridwan, R. Z. (2019). *The Utilization of Cryptocurrencies by the Terrorist Group as an Alternative Way of Hawala for Illicit Purposes. Jurnal Sentris KSMPMI, 2, 1-14.*
- Rogers, E. M. (1962). *Diffusion Of Innovations* (3rd ed.). New York: The Free Press.
- Rooney, K. (2021, January 24). *Overall bitcoin-related crime fell last year, but one type of crypto hack is booming*. Retrieved from CNBC: <https://www.cnbc.com/2021/01/24/overall-bitcoin-related-crime-fell-last-year-but-one-type-of-crypto-hack-is-booming.html>
- Sanders, L. (2015, September 20). *Bitcoin: Islamic State's online currency venture*. Retrieved from Deutsche Welle (DW): <https://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856>
- Savage, C. (2020, August 13). *U.S. Seizes Bitcoin Said to Be Used to Finance Terrorist Groups*. Retrieved from The New York Times: <https://www.nytimes.com/2020/08/13/us/politics/bitcoin-terrorism.html>
- Smith, T. (2020, March 21). *Disruptive Technology*. Retrieved from Investopedia: <https://www.investopedia.com/terms/d/disruptive-technology.asp#:~:text=Disruptive%20technology%20is%20an%20innovation,attributes%20that%20are%20recognizably%20superior.>
- Sountra, M. A. (2019). *Cryptocurrency as a Modern Technique of Money Laundering and Terrorism Financing. LGU International Journal for Electronic Crime Investigation, 3(4), 1-16.*
- Tempo. (2015, October 30). *Pengebom Mall Alam Sutera Tangerang Terinspirasi ISIS*. Retrieved from Tempo: <https://metro.tempo.co/read/714500/pengebom-mal-alam-sutera-tangerang-terinspirasi-isis>
- The Guardian. (2020, October 31). *Early Adopters Of Bitcoin*. Retrieved from The Guardian: <https://guardian.ng/technology/early-adopters-of-bitcoin/#:~:text=Hal%20Finney%20is%20known%20for,being%20the%20first%20Bitcoin%20recipient.>

The United States Department Of Justice. (2019, May 22). *Somerset County Man Charged With Attempts To Provide Material Support To Hamas, Making False Statements, And Making Threat Against Pro-Israel Supporters*. Retrieved from United States Department of Justice: <https://www.justice.gov/usao-nj/pr/somerset-county-man-charged-attempts-provide-material-support-hamas-making-false>

The United States Department of Justice. (2020, March 13). *Long Island Woman Sentenced to 13 Years' Imprisonment for Providing Material Support to ISIS*. Retrieved from The United States Department of Justice: <https://www.justice.gov/opa/pr/long-island-woman-sentenced-13-years-imprisonment-providing-material-support-isis>

Triskaputri, R. M., Satrya, A., & Wardoyo, B. (2020). 372-379. doi:DOI 10.4108/eai.6-11-2019.2297285

Wahjoe, O. (2011). *Hukum Pidana Internasional Perkembangan Tindak Pidana Internasional dan Proses Penegakannya*. Jakarta: Penerbit Erlangga.

Widyastuti, R., & Antara. (2021, June 15). *BI Tegas Melarang Kripto Digunakan sebagai Alat Pembayaran*. Retrieved from Tempo: <https://bisnis.tempo.co/read/1472893/bi-tegas-melarang-kripto-digunakan-sebagai-alat-pembayaran/full&view=ok>

Zhou, G., Zhuge, J., Fan, Y., Du, K., & Lu, S. (2020, February 1). A Market in Dream: the Rapid Development of Anonymous Cybercrime. *Mobile Netw Appl* 25, 259-270. doi:<https://doi.org/10.1007/s11036-019-01440-2>

