The Utilization of Cryptocurrencies by the Terrorist Group as an Alternative Way of *Hawala* for Illicit Purposes

Raihan Zahirah Mauludy Ridwan

2016330021

Mahasiswa Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik

Universitas Katolik Parahyangan

Abstract

Kemajuan bidang teknologi dan komunikasi pada kenyataannya banyak disalahgunakan oleh kelompok teroris. Kelompok teroris menggunakan salah satu teknologi transaksi keuangan daring berupa *cryptocurrency* untuk tujuan ilegal. Hal ini dikarenakan tradisi *hawala* yang sudah tidak memungkinkan lagi untuk dilakukan dan terdapat beberapa prinsip *cryptocurrency* yang memberikan peluang lebih besar bagi kelompok teroris untuk bertransaksi serta mencari dana untuk kegiatan operasional mereka. Makalah ini ingin menjawab bagaimana kelompok teroris menggunakan kecanggihan teknologi saat ini berupa *cryptocurrency* sebagai jalan alternatif dari tradisi *hawala* untuk tujuan ilegal, dan apa bentuk tindakan penanganan yang baik bagi masalah ini. Makalah ini bertujuan untuk mengeksplorasi *cryptocurrency* dari sisi sistem, cara penggunaan, tradisi transaksi tradisional *hawala,* dan bentuk konkret penggunaan *cryptocurrency* oleh kelompok teroris. Makalah ini juga akan membahas tentang peluang aktor non negara lainnya seperti perusahaan teknologi swasta dalam membantu menangani penyalahgunaan *cryptocurrency*. Makalah ini menggunakan *organizational approach* terorisme dan konsep *digital counterterrorism.*

Keywords: Counterterrorism, Cryptocurrency, Digital, Illicit, Terrorist.

I. Introduction

Terrorism is one of the crucial problems in the world, especially in the globalization era. Terrorism is an act of anger and violence toward the disappointment of the political situation. Terrorist is a person who commits terrorism and involves in terrorist organization. When everything became easier to access and faster to connect, sometimes people misuse this time to create terrorism activities such as bombing, brainwashing, recruiting and war. Many terrorist organizations in the world especially Islamic terrorist groups which unites themselves into a single group, mostly called ISIS (Islamic State of Iraq and Syria). Besides the ISIS, there are *Al-Qaeda, Islamic Maghreb, Al-Murabitoun, ISIS in Libya, Ansar Al-Sunnah, Al-Qaeda of Arabian Peninsula in Yemen, Al-Shabaab, Haqqani Network, Mujahideen Shura Council, Fethullah Gullen Organization, Kataib Hezbollah, Moro Islamic Liberation Front, Abu Sayyaf, Boko Haram, Jamaah Islamiyah, Jamaah Ansharut Daulah*, etc. The devil is in the details. By the advancement of technology, it provides an opportunity for the terrorist organizations to

ISSN 0216-5031

conduct digital abuse such as the utilization of cryptocurrencies to gain financial resources as an alternative way of *hawala* and diversify their portfolio since the physical meeting for financial transaction by using broker no longer possible to be conducted due to the presence of massive intelligence and military troops.

The research question of this paper *inter alia* how does the terrorist organizations use technological advancement such as cryptocurrencies as an alternative way of *hawala* tradition for illicit purposes and how to tackle the problem. This paper uses the organizational theory of terrorism. This paper affirms that the terrorist organizations utilize the cryptocurrencies for fundraising, purchasing weaponry, illicit transactions and as the platform for crowdfunding to provide goods and incentives for their fighters. They launched a campaign and advertisement as well as attached their Bitcoin address. This paper recommends the creation of Crypto-Fintech Helix which based on the three dimensions of actors within a single partnership framework of "Digital Counterterrorism" and consist of government, international organizations and private sector. This partnership focuses on four sectors *inter alia* blockchain analysis; the capacity building and technological know-how; implementation of three cryptocurrencies system and banking sector innovation; and National Action Plan (NAP). To support the argument, this paper provides factual data and arguments from pieces of literature from a credible source. This paper aims to explore the cryptocurrencies, *hawala* traditional transaction, concrete utilization of cryptocurrencies by the terrorist organizations, and opportunities for the other non-state actors such as private technology companies in dealing with cryptocurrencies abuses. The reason why the writer chooses this topic because it is interesting to read, relevant and still happening until today. Counterterrorism refers to the action intended to prevent violence for political purposes.[1] Cryptocurrency means a digital currency produced by a public network, rather than any government, that uses cryptography to make sure payments are sent and received safely.[2] Digital refers to using an electronic system that uses a binary number to record sound or store information, and that gives high-quality results.[3] Illicit is something that not allowed by the law.[4] Terrorism is the use of violence for political purpose.[5]

II. Theoretical Framework

This paper uses the organizational theory of terrorism initiated by Martha Crenshaw. The organizational theory mostly discusses the objectives, actions and internal dynamics of the terrorist

[1] Cambridge Dictionary, "Counterterrorism," *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/counterterrorism (retrieved on May, 4th 2019)
[2] Cambridge Dictionary, "Cryptocurrency," *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/cryptocurrency (retrieved on May, 4th 2019)
[3] Oxford Learner Dictionary, *Fourth Edition* (China: Oxford University Press, 2008) 124.
[4] *Ibid.,* 219.
[5] *Ibid.,* 459.

ISSN 0216-5031

organization.[6] This theory emphasizes on the main goal of a terrorist organization which is the survival that could be illustrated as the state institution or commercial enterprise.[7] Terrorism could be inferred as the output of the struggle for survival within the competitive environment.[8] Likewise, this theory stresses that the terrorist organization could be illustrated as commercial enterprise or firms since the economic theory of the organization could be used to explain the activity and maintenance of the organization within the competitive environment.[9] For instance, one terrorist organization might perceive other terrorist organization as rivals within the marketplace e.g. Irish Republican National Army versus the Irish National Liberation Army.[10] Moreover, the leader of the terrorist organization usually delivers benefits and incentives to the members for the sake of survival.[11] The benefits or incentives could be in the form of goods (tangible and intangible goods).[12] In responding to the external pressures, the terrorist organization will change its incentives through an innovation.[13] Any actions conducted by the terrorist did not directly reflect their ideological values.[14] The terrorist organization typically self-sustaining and they are willing to do anything to survive.[15]

The reason why the terrorist organization could survive although they seldom to achieve their ultimate objectives is that the terrorist organization focuses on their material benefits and it administers financial resources for its members.[16] If they succeed in reaching their ultimate goals, the benefits will no longer exist and no incentives that could keep the organization together.[17] Thus, the function of the organization most likely to provide goods for its members.[18] For instance, the terrorist organization that gains financial support from illegal or illicit activities.[19] Furthermore, this theory argues that the terrorist organization uses peaceful means to provide goods for their members and provide externalities for the outsiders.[20]

III. Analysis

Defining terrorism, terrorism is an act of violence and anger of a person or group which aimed to show the disappointment of the political situation. Terrorism means the action of attacks of non-

[6] Ozgur Ozdamar, "Theorizing Terrorist Behavior: Major Approaches and Their Characteristics", *Defence Against Terrorism Review 1,* No. 2 (2008): 93-95.
[7] *Ibid.*
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*
[11] *Ibid.*
[12] *Ibid.*
[13] *Ibid.*
[14] *Ibid.*
[15] *Ibid.*
[16] *Ibid.*
[17] *Ibid.*
[18] *Ibid.*
[19] *Ibid.*
[20] *Ibid.*

ISSN 0216-5031

combatants which emerge fear within the society and political oriented.[21] Terrorism in history means revolution act by the opposition of the government. The root of terrorism can be traced back to the early twentieth century with the wave of revolutionary violence in Russia Revolution and the death of Prince Franz Ferdinand in Sarajevo by Gavrilo Princip which spurred the World War I.[22] Today, terrorism has changed in terms of its dimension, actors, platform, and activities. Terrorism is an act of cyber hackings, drug trafficking, guerilla warfare, insurgency, kidnappings, torture, assassinations, propaganda, sabotage, vandalism, aerial bombings, hijackings, suicide attacks which involved an act of violence toward the society.[23]

The advancement of technology enables people to conduct financial transaction easily (fin-tech) especially by the emergence of cryptocurrencies that uses the blockchain system (see appendix 1). Make a long story short, the cryptocurrency began to emerge in 1998 when Wei Dai (computer engineer) contrived an article in regards to the possibility of the new form of currency where he called it "b-money" which used the principle of anonymous and channeled through electronic cash system.[24] Practically, the analogy is like people paying for online things by using credit cards.[25] As time goes by, a computer scientist and legal scholar named Nick Szabo concocted "bit gold" as the first prototype of cryptocurrency.[26] Moreover, the decentralized cryptocurrency successfully produced a workable system called Bitcoin uses the system of SHA-256 (hash functions designed by United States National Security Agency) which contrived by Satoshi Nakamoto in 2009.[27] Since SHA-256 could ensure the proof of work of the cryptocurrency, so it could be inferred that the cryptocurrency itself is already reliable.[28] The proof of work in here refers to the system that avoids actions of scamming and fraud by obligating the proof of work from the person invoking the service so as the person could prove that he or she is aboveboard.[29] The "work" also created as the tricky system means that to prove the work, it required a difficult and time-consuming process so as we could determine their seriousness in proving the work.[30] For the service provider, it is easy to regulate and check-up the work.[31] Two years later, the Namecoin created and unleashed in the cryptocurrencies market which contrived to form a decentralized DNS which could make internet censorship harder to be implemented which means that the government could not supervise or even control our cryptocurrencies market activities *inter alia* trading, buying and

[21] Jeff Victoroff & Arie W. Kruglanski, *Psychology of Terrorism (*East Sussex: Psychology Press, 2009)
[22] *Ibid.*
[23] Richard Jackson, Lee Jarvis, Jeroen Gunning & Marie Breen-Smyth, *Terrorism: A Critical Introduction* (Palgrave Macmillan, 2011)
[24] Owen Hill, *Cryptocurrency Investing: Comprehensive Guide to Cryptocurrency* (Kindle Edition, 2019) 1-2.
[25] *Ibid.*
[26] *Ibid.*
[27] *Ibid.*
[28] *Ibid.*
[29] *Ibid.*
[30] *Ibid.*
[31] *Ibid.*

ISSN 0216-5031

spending.[32] Furthermore, the "altcoin" also created which able to modify further market such as Litecoin.[33] Litecoin used the script rather than SHA-256 to ensure regulation and credibility.[34] Currently, there are several cryptocurrencies being traded in the market *inter alia* Bitcoin, Bitcoin Cash, Ethereum, Litecoin, Ripple XRP, Stellar Lumens, Zcash, Ox, and Basic Attention Token.[35]

A little learning is a dangerous thing. Seeing that the government could not control and monitor the cryptocurrencies market activities, the action of abuse by non-state actors mostly terrorist organizations are proliferating especially for the illicit purposes. The Bitcoin continuously utilized by the purchasers and consumers of illicit goods on the Dark Web. Based on the CNAS report titled "Terrorist Use of Virtual Currencies: Containing the Potential Threat" stated that the terrorist organizations have used the cryptocurrencies to support the survival of their organizations. For instance, the terrorist organization in the Gaza Strip have used the cryptocurrencies to fund their operations as well as the Islamic State in Iraq and Syria (ISIS) members and supporters who particularly used the cryptocurrencies recorded in Indonesia and United States. Noting further that the substantial and abrupt loss of their physical territory, as well as the proliferation of strict military operations may limit their access and make them more difficult to move their cash across geographic areas and borders or the traditional financial transaction called *hawala* which refers to the physical financial transaction by using local broker to transfer money between locations.[36] Thus, this phenomenon potentially encourage the terrorist organizations to explore the new technology that could support their ability to move the funds through cryptocurrencies which make matter worse and add insults to injury.

There are several reasons that cryptocurrencies facilitate the terrorist organizations to move their funds across the border *inter alia* anonymity, rapid transaction settlement, decentralized, contained environment, self-governance model, financial integrity, tax evasion, treatment, enforcement of exchange controls, capital flow management, ease of use, independence from controls of legitimate financial system, and dark web access.[37] Anonymity means that cryptocurrencies offer various degrees of anonymity especially in name and transaction-level detail which contrary with the principle of "Know-Your-Customer" or "Customer Due Diligence," transaction reporting for both for anti-money laundering (AML) and countering the financing (CFT).[38] Moreover, the cryptocurrencies also

[32] *Ibid.*
[33] *Ibid.*
[34] *Ibid.*
[35] CNBC, "Markets Cryptocurrency," *CNBC*, https://www.cnbc.com/cryptocurrency/ (retrieved on May, 4th 2019)
[36] Antonia Ward, "Bitcoin and the Dark Web: The New Terrorist Threat?" *RAND Corporation*, January 22nd 2018, https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html (retrieved on May 4th, 2019)
[37] Everette J, *2017 Public-Private Analytic Exchange Program: Risks and Vulnerabilities of Virtual Currency* (Washington: Director of National Intelligence, 2017) 10-19.
[38] *Ibid.*

ISSN 0216-5031

administer additional anonymity by the mixing services and location/identity hiding services.[39] The rapid transaction settlement means that the cryptocurrencies offer near real-time cross-border transaction settlement at a lower cost which attracts the global criminal and terrorist organizations to accelerate their borderless financial channels.[40] The decentralized and contained environments mean it is not clear who is the agent that responsible for hold the accountability in cryptocurrency networks even though there is a broad range of actors in cryptocurrency networks such as exchangers, miners, wallet providers, ATM providers, payment processors, etc (see appendix 2).[41] The transaction also not recorded such as what happened in the traditional financial system (no firms that regulate).[42] Moreover, the law enforcement agency unable to conduct an investigation for the exact location or asset confiscation.[43] The self-governance model means as the socio-technical trustless network without the institution which regulates the network, cryptocurrencies are formed and managed by the developers without clear and exact governance system.[44] The financial integrity means the cryptocurrencies open opportunities for global criminal and terrorist organizations to disguise their illicit transaction which could facilitate money laundering, sanctions evasion, cybercrime, fraud, and terrorist financing.[45] The tax evasion and treatment means that every element in the cryptocurrencies market could avoid tax which imposed by the government since the government itself could not control the market and there are no firms that regulate the cryptocurrencies network as it is based on the peer-to-peer system.[46] The enforcement of exchange controls and capital flow management means that cryptocurrency does not need any kind of circumvent exchange and capital flow management since it is a cross-border transaction of fiat currency.[47] The ease of use means that the cryptocurrencies offer user-friendly interfaces where the terrorist organizations could create automated and scalable payment interfaces that could be incorporated into ransomware and crimeware.[48] If the level of legitimate users of cryptocurrencies are higher and larger, the more this system offer a wide range of opportunities for the terrorist organizations to conduct illicit activities such as develop a criminal business model through ransomware to obtain money from the victims and hide the transactions.[49] The independence from controls of the legitimate financial system means that cryptocurrency cannot be regulated by financial firms.[50] In result, the banks and financial institutions seek to work on the risk-averse structure and try to create a system that could facilitate cash out cryptocurrencies and create their own cryptocurrencies

[39] *Ibid.*
[40] *Ibid.*
[41] *Ibid.*
[42] *Ibid.*
[43] *Ibid.*
[44] *Ibid.*
[45] *Ibid.*
[46] *Ibid.*
[47] *Ibid.*
[48] *Ibid.*
[49] *Ibid.*
[50] *Ibid.*

ISSN 0216-5031

markets.[51] Last, the Dark Web Access means that the cryptocurrencies already adopted as the suitable payment methods for illicit sites on the Dark Web since it offers multi-signature transaction and smart contracts which support the decentralized system and eradicate the level of trust between the illicit actors.[52] There are clouds on the horizon. There are several illicit purposes of the utilization of the cryptocurrencies by terrorist organizations such as purchasing drugs, selling drugs, weapons, and afford the illicit services in the Dark Web.[53] Moreover, the terrorist organization also launched its donation through the cryptocurrencies.[54] It could be inferred that cryptocurrencies could be turned into ransom payment.[55] In addition, there are several cryptocurrencies features which provide advantages for the users such as better than cash or credit, exchangeable for goods and services, convertibility, and stability of value (balance price volatility).[56]

An elephant in the room. Terrorist organizations have used cryptocurrencies to replace their traditional financial transaction called *hawala* where the physical financial transaction by using a local broker to transfer money between locations.[57] Bite the bullet, in 2014 ISIS already declared that they sought to raise funds through cryptocurrencies.[58] In 2016, *Mujahideen Shura Council* launched a fundraising campaign called *Jahezona* on Twitter and Telegram complete with the price list of weaponry such as rockets, rifles, grenades, and other gear for militants. They also attached their Bitcoin QR code.[59] In January 2017, Islamist militants, *Mujahideen Shura Council* (terrorist organization in Gaza Strip made by the US), and ISIS started to use Bitcoin as their funding methods for their operation and diversifying their portfolio.[60] Moreover, ISIS also posting their donation advertisement on the Dark Web complete with their Bitcoin address.[61] In the late November 2017, the pro-Islamic State contrived website called *Akhbar al-Muslimeen* which published Bitcoin address for donations.[62] They also frequently released ISIS attacks and propaganda.[63] It could be inferred that the physical fight and abolishment of terrorist organizations territory did not significant enough in eradicating the terrorist organizations until its root and cells since they still survive through utilizing the advancement of technology.[64] When it rains it pours. The terrorist organizations use Bitcoin to purchase a range of goods

[51] *Ibid.*
[52] *Ibid.*
[53] *Ibid.*
[54] *Ibid.*
[55] *Ibid.*
[56] *Ibid.*
[57] Antonia Ward, *Bitcoin and the Dark Web: The New Terrorist Threat.*
[58] Ankit Panda, "Cryptocurrencies and National Security," *Council on Foreign Relations,* February 28th 2018, https://www.cfr.org/backgrounder/cryptocurrencies-and-national-security (retrieved on May 4th, 2019)
[59] Yaya Fanusie, *Survey of Terrorist Groups and Their Means of Financing* (Washington, DC: House of Financial Services Committee USA, 2018) 3-4.
[60] Antonia Ward, *Bitcoin and the Dark Web: The New Terrorist Threat.*
[61] *Ibid.*
[62] Yaya Fanusie, *Survey of Terrorist Groups and Their Means of Financing,* 7.
[63] *Ibid.*
[64] Antonia Ward, *Bitcoin and the Dark Web: The New Terrorist Threat.*

ISSN 0216-5031

and services *inter alia* weaponry, firearms, bomb-making materials, false passports, human trafficking, organ's trafficking, drug trafficking and other illicit activities that could generate profit for their operations.[65]

Based on the study conducted by RAND Europe titled "Behind The Curtain: The Illicit Trade of Firearms, Explosives, and Ammunition on The Dark Web," there is a direct link between Paris and Munich terrorist attack as well as the arms dealing within the Dark Web through cryptocurrencies.[66] The study shows that there were 24 French and British cryptocurrencies markets on the Dark Web along September 2016 where 75 percent of the transactions proved to conduct arms dealing.[67] The weapons used by the attackers and could be related to the ISIS propaganda which called for the proliferation of simplistic attacks by using vehicles, firearms, weaponry, chemical weapons, and knives.[68] Moreover, the al-Qaeda linked organization namely *al-Sadaqah* accused using Facebook and Telegram to launch their financial campaign through Bitcoin.[69] The evidence shows that about BTC 0.075 ($685) was sent by unknown and that funds were forwarded into another Bitcoin address.[70] In 2014, ISIS fighters in Raqqa proved to facilitate purchases and cross-border international transactions using cryptocurrencies.[71] In January 2015, ISIS fundraiser namely Abu Mustafa stated that since the United States law enforcement agency begun to shut down the traditional financial transaction platform, then Dark Web supposed to be their platform to raise funds through cryptocurrencies.[72] Before his account was closed, Abu Mustafa raised five Bitcoins valued $1,000. During the same year, a 17 years old Virginia man namely Shukri Amin accused of his promotion of e-donations to support ISIS through social media sites and cryptocurrencies.[73] [74] He was charged for his material support for ISIS by teaching how to use Bitcoin to fund the terrorist organizations.[75] In December 2017, a similar phenomenon happened where a woman was arrested in New York accused obtaining bitcoins valued $62,000 to support ISIS's operation.[76] Zoobia Shahnaz, 27-year-old resident of Long Island accused of wiring more than $150,000 to many individuals where she also accused to a scam involving money laundering and bank fraud including Chase Bank, TD Bank, American Express as well as Discover by obtaining six

[65] *Ibid.*
[66] *Ibid.*
[67] *Ibid.*
[68] *Ibid.*
[69] Nikita Malik, "How Criminals And Terrorists Use Cryptocurrency: And How To Stop It," *Forbes*, August 31st 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#6766399a3990 (retrieved on May 4th, 2019)
[70] *Ibid.*
[71] *Ibid.*
[72] *Ibid.*
[73] Nikita Malik, *How Criminals and Terrorists Use Cryptocurrency: And How To Stop It.*
[74] Ankit Panda, *Cryptocurrencies and National Security.*
[75] *Ibid.*
[76] *Ibid.*

ISSN 0216-5031

credit cards. She also bought Bitcoins valued $62,703 and converted into cash.[77] In the same year, she was trying to leave the United States and stay in Syria by obtaining a Pakistani passport.[78] She transferred the bitcoins through multiple Bitcoins accounts and sending it to Pakistan, China, and Turkey. [79]At the same time, another concrete utilization of cryptocurrencies proved by the existence of ISIS Dark Web site namely *Isdarat* which could be accessed through private The Onion Router (ToR) and the site sought for donations.[80] Based on the Europol report in 2015, over 40 percent of the illicit transaction through cryptocurrencies within European Union involved terrorist organizations.[81]

In the early March 2019, Hamas (terrorist organization in Gaza Strip) published a video showing that they urging their supporters to send financial support through cryptocurrencies especially Bitcoins.[82] Hamas started to raise funds through Bitcoins since January 2019 and raised a few thousand dollars.[83] Shreds of evidence show that the intersection of the terrorist organization and cryptocurrencies could support terrorist organizations in planning, financing and perpetrating attacks.[84] Cryptocurrencies also become the platform for terrorist organizations crowdfunding.[85] There should be more response from the states to respond to this significant threat which could be categorized as cybercrime and directly links to the cybersecurity of the citizens.[86] More weapons could guarantee that there will be further investigation to prevent abuse and simplistic attacks.[87]

Explaining the problem by using the organizational theory of terrorism, it could be inferred that by utilizing the cryptocurrencies, terrorist organizations are most likely operating as commercial enterprises where they publish and release campaign for fundraising complete with the price lists and Bitcoins address. Out of the frying pan and into the fire. The best of both worlds, the pieces of evidence show that through cryptocurrencies, terrorist organizations diversifying their portfolio for their survival within the competitive and hostile environment. The leader of the terrorist organization usually delivers benefits and incentives to the members for the sake of survival in the form of goods (tangible and intangible) could be seen from the distribution of money and range of weaponry. In responding to the external pressures especially losing territory and restricted financial regulation, the terrorist organization will change its incentives through innovation by diversifying their financial portfolio

[77] Dan Mangan, "New York woman pleads guilty to using bitcoin to launder money for terror group ISIS," *CNBC,* November 26th 2018, https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html (retrieved on May 4th, 2019)
[78] *Ibid.*
[79] *Ibid.*
[80] *Ibid.*
[81] *Ibid.*
[82] Yaya Fanusie, "Jihadists Upping Their Bitcoin Game," *Forbes,* March 29th 2019, https://www.forbes.com/sites/yayafanusie/2019/03/29/jihadists-upping-their-bitcoin-game/#7006834f79bc (retrieved on May 4th 2019)
[83] *Ibid.*
[84] Antonia Ward, *Bitcoin and the Dark Web: The New Terrorist Threat.*
[85] Yaya Fanusie, *Jihadists Upping Their Bitcoin Game.*
[86] Antonia Ward, *Bitcoin and the Dark Web: The New Terrorist Threat.*
[87] *Ibid.*

ISSN 0216-5031

through cryptocurrency and Dark Web to sustain their balance. Any actions which conducted by the terrorist do not directly reflect their ideological values as well as the terrorist organization typically self-sustaining and they are willing to do anything to survive also could be proven by their willingness to explore the new financial technology where people out there most likely think that terrorist organizations are far from advanced technology. Thus, it could be inferred that the function of the organization most likely to provide goods for their members by gaining profit from illicit activities and peaceful means for the sake of their survival.[88] Know which way the wind is blowing, a perfect storm might be like the terrorist organizations will survive and launch a series of attacks even though they already lost their territory.

IV. Conclusion

In conclusion, the terrorist organizations utilize the cryptocurrencies as an alternative way of *hawala* due to the presence of massive intelligence and military troops which turn the surrounding environment into competitive and hostile. There are many terrorist organizations which utilize cryptocurrencies for their crowdfunding during fundraising such as ISIS, *Mujahideen Shura Council*, al-Qaeda, Hamas, etc. Due to the external pressures, such as losing territory and restricted financial regulation, the terrorist organizations diversifying their financial portfolio through Dark Web and cryptocurrencies to sustain their operations and maintain their survival. In here, we could see the tendency that terrorist organizations most likely operating as commercial enterprises where they publish and release campaign for fundraising complete with the price lists and Bitcoins address as well as distributing money and goods for their fighters.

V. Recommendation

There has been certain regulation imposed by the government especially United Kingdom that seeks to disclose the user identities so as the measures in line with the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF).[89] A stitch in time saves nine. This paper would like to propose a solution to be considered by the government, private sectors and international organizations which focus on partnership and capacity building especially for the developed, developing and least developed countries to avoid miss the boat and bite the bullet. Hit the nail on the head, the better way to eradicate terrorism until its root especially abolishes their financial transactions is through the concept of Cryptocurrency-Fintech Helix which based on the three dimensions of actors within single partnership framework of "Digital Counterterrorism". The Crypto-Fintech Helix will consist of government, international organizations, and the private sector. The government could from police and national

[88] Ozgur Ozdamar, *Theorizing Terrorist Behavior: Major Approaches and Their Characteristics.*
[89] Nikita Malik, *How Criminals And Terrorists Use Cryptocurrency: And How To Stop It.*

ISSN 0216-5031

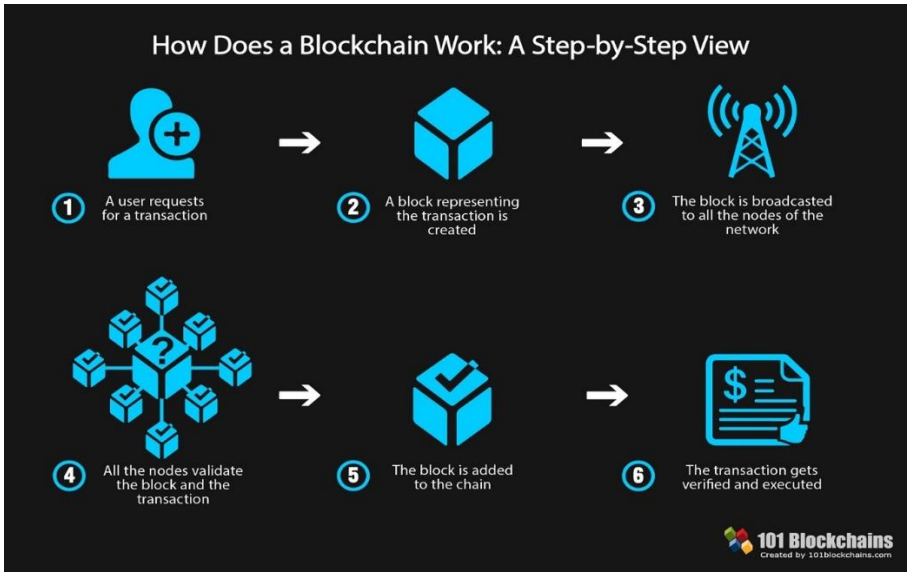
intelligence as well as security agency while the organizations could be INTERPOL and the private sector could be the technology companies and banking sector.

There are four sectors of partnerships that could be conducted. First, the blockchain analysis which will focus on research and development as well as the periodical risk assessment regarding the financial transaction within the cryptocurrencies market. Second, the capacity building and technological know-how which focus on the implementation of different blockchain system within the cryptocurrencies market by using three options *inter alia* permissioned versus less-permission, "Know-Your-Miner", or shut down entirely. You cannot make an omelet without breaking some eggs. The "Know-Your-Miner" system will decrease the degree of anonymity and forge the private sector to have information sharing. Third, the implementation of public policy regarding the cryptocurrencies accounts by choosing between "state-by-state licensing" or "the aggressive de-risking" by banking sector systems. Moreover, in this sector of partnership, there will be an assessment on the possibility of the banking sector in forging the incentives and innovation to detect the terrorist financing as well as adopting the information sharing strategy with related government bodies. The government should support the banking sector in initiating the trusted new payment technologies and contrive their own promising virtual currency that could persuade and attract the new customers with balance volatility, competitive as well as prevent them from ransom payment. In addition, there should be more strong coordination and well-structured chain of command with the law enforcement and intelligence agency since several national police agency already possessed the cyber police. Fourth, the manifestation of the three sectors of partnerships into the National Action Plan (NAP). Lastly, the collaboration between the cryptocurrencies traders also necessary since they could help the law enforcement agency and government in noticing the illicit users and transactions.

Appendix

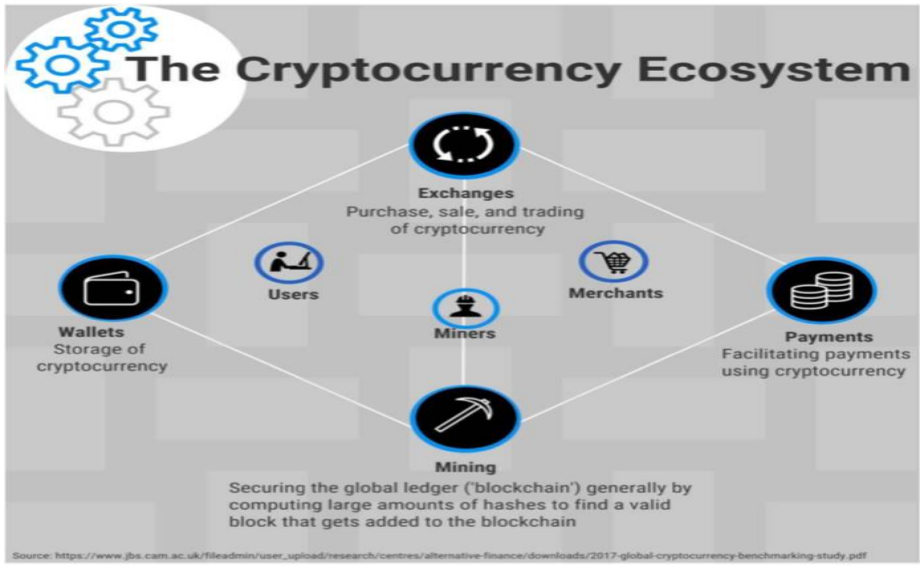
Appendix 1

ISSN 0216-5031



Source: Hasib Anwar, "The Ultimate Blockchain Technology Guide: A Revolution to Change the World," *101 Blockchains*, July 13th 2018, https://101blockchains.com/ultimate-blockchain-technology-guide/ (retrieved on May 4th, 2019)

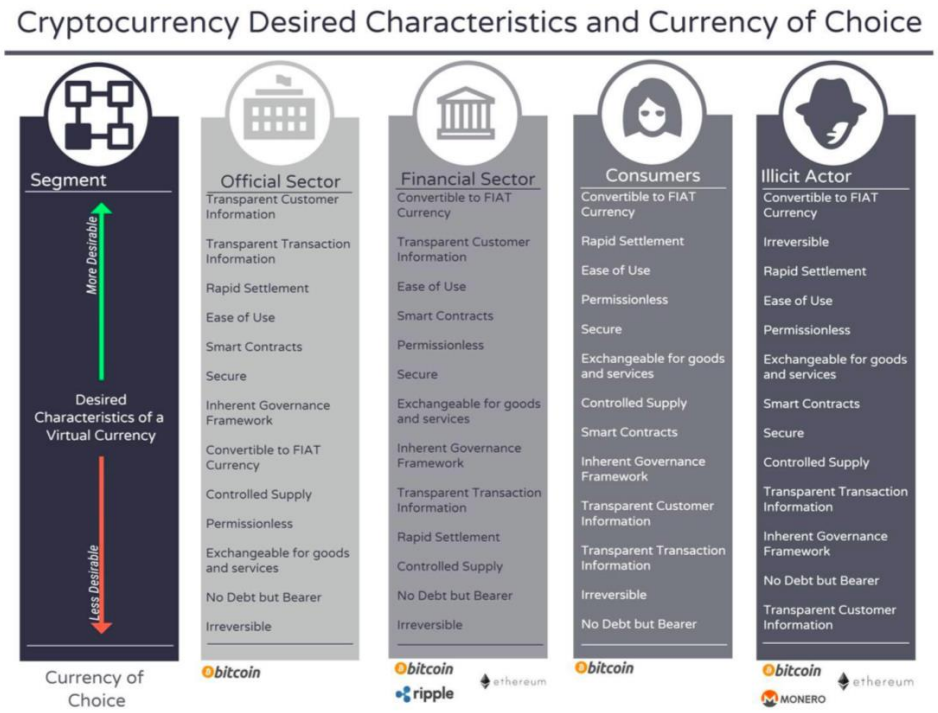
Appendix 2



Source: Everette J, *2017 Public-Private Analytic Exchange Program: Risks and Vulnerabilities of Virtual Currency* (Washington: Director of National Intelligence, 2017)

ISSN 0216-5031

Appendix 3



Source: Everette J, *2017 Public-Private Analytic Exchange Program: Risks and Vulnerabilities of Virtual Currency* (Washington: Director of National Intelligence, 2017)

ISSN 0216-5031

Works Cited

Victoroff, Jeff, and Arie W. Kruglanski. 2009. *Psychology of Terrorism.* East Sussex: Psychology Press.

Jackson, Richard, Lee Jarvis, Jeroen Gunning, and Marie Breen-Smyth. 2011. *Terrorism: A Critical Introduction.* Palgrave Macmillan.

Cambridge Dictionary,. n.d. *Counterterrorism.* Accessed May 4, 2019. https://dictionary.cambridge.org/dictionary/english/counterterrorism .

Cambridge Dictionary. n.d. *Cryptocurrency.* Accessed May 4, 2019. https://dictionary.cambridge.org/dictionary/english/cryptocurrency .

Oxford Learner Dictionary. 2008. *Fourth Edition .* Oxford University Press.

Ozdamar, Ozgur. 2008. "Theorizing Terrorist Behavior: Major Approaches and Their Characteristics." *Defence Against Terrorism Review* 1 (Fall): 93-95.

Victoroff, Jeff, and Arie W. Kruglanski. 209. *Psychology of Terrorism .* East Sussex: Psychology Press.

Jackson, Richard, Lee Jarvis, Jeroen Gunning, and Marie Breen-Smyth. 2011. *Terrorism: A Critical Introduction.* Palgrave Macmillan.

Hill, Owen. 2019. *Cryptocurrency Investing: Comprehensive Guide to Cryptocurrency .* Kindle Edition.

CNBC. n.d. *Markets Cryptocurrency.* Accessed May 4, 2019. https://www.cnbc.com/cryptocurrency/ .

Ward, Antonia. 2018. *Bitcoin and the Dark Web: The New Terrorist Threat?* January 22. Accessed May 4, 2019. https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html .

J, Everette. 2017. *2017 Public-Private Analytic Exchange Program: Risks and Vulnerabilities of Virtual Currency .* Director of National Intelligence, Washington DC: Director of National Intelligence, 10-19.

Panda, Ankit. 2018. *Cryptocurrencies and National Security.* February 28. Accessed May 4, 2019. https://www.cfr.org/backgrounder/cryptocurrencies-and-national-security .

Fanusie, Yaya. 2018. *Survey of Terrorist Groups and Their Means of Financing.* House of Financial Services Committee USA, Washington DC: House of Financial Services Committee USA, 3-7.

Malik, Nikita. 2018. *How Criminals And Terrorists Use Cryptocurrency: And How To Stop It.* August 31. Accessed May 4, 2019. https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#6766399a3990 .

Mangan, Dan. 2018. *New York woman pleads guilty to using bitcoin to launder money for terror group ISIS.* November 26. Accessed May 4, 2019. https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html .

Fanusie, Yaya. 2019. *Jihadists Upping Their Bitcoin Game.* March 29. Accessed May 4, 2019. https://www.forbes.com/sites/yayafanusie/2019/03/29/jihadists-upping-their-bitcoin-game/#7006834f79bc .

ISSN 0216-5031