Innovation in Terrorist Financing: Interrogating Varying Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State

Department of Political Science

Haverford College

In Partial Fulfillment of the Requirements for the Degree of

Bachelor of Arts

Andrew Eaddy

May, 2019

To my loving parents Carolene and Richard, without whom this thesis would have been infinitely more difficult to write. You instilled in me a strong work ethic and spirited ambition, and for that I will be eternally grateful.

Contents

Chapter I: Introduction

Since their inception, terrorist organizations have embraced a culture of innovation. So why have terrorist organizations not yet integrated cryptocurrencies into their financing apparatus? Terrorist groups have been known to innovate with respect to both material capabilities, such as the advent of chemical and biological weapons, as well as shifts strategic capabilities, such as with the advent of airplane hijackings and suicide bombings.[1] Groups have also innovated in their ideology, with organizations being know to have shifting ideological orientations and group ethos as well. These sorts of material, ideological, and at times strategic breakthroughs will be examined over the course of this paper in order to answer the question of why terrorist organizations have not adopted cryptocurrency technology at a systematic level yet. These advances can also be readily observed in the early 2000s in the case of Al-Qaeda.[2]

In 2001, a series of letters laced with anthrax spores were sent to United States politicians and news personalities killing five people and injuring another twenty.[3] The attack was ultimately linked to Al-Qaeda, citing the content of the letters which read messages such as "Death to Israel" and "Death to America" as evidence for the claim.[4] Regardless of the perpetrator, however, the nature of the attack represented a drastic shift in terrorist technology. The attacks on September 11th were carried out with knives and box-cutters, while the attacks mere weeks later took the form of advanced bioweaponry. This incident was a signifier that the terrorist landscape was changing.

---

[1] Ungerer, Carl. "Terrorist Innovation and Methods" in "*Beyond bin Laden: Future trends in terrorism*." Canberra: Australian Strategic Policy Institute, 2001.
[2] Ibid
[3] Stern, Jessica, and Ronald Schouten. "Lessons from the Anthrax Letters." In *Insider Threats*, edited by Bunn Matthew and Sagan Scott D., 74-76.
[4] Ibid

Terrorist organizations adopting novel military strategy or implementing a new system of weaponry exist in copious amounts in the scholarship. These groups have both embraced innovation in their respective approaches to terrorism, and consequently found relative success. Innovation within terrorist groups is paramount - it is a means of survival and way to differentiate a group's identity from one another in a world riddled with terrorist groups. It is also a means of competition, as groups work to gain notoriety and recruits. Innovation and innovative principles rest centrally in the overarching mission of terrorist organizations. Analogous situations of terrorist organizations implementing a similar innovation in the realm of terrorist financing, however, are far less common.

Terrorists have innovated in the financial sphere, however as the current counter-terrorism financing regime grows larger and more knowledgeable, there will be urgency placed on these innovative endeavors. Right now, these innovations are rarely talked about in terrorist innovation literature. Reliable and consistent financing apparatuses are integral to the operations of all types of organizations: corporations, criminal enterprises, and terrorist groups are no exception to this rule. Terrorist organizations' response to financial strains due to the current counter-terrorism regime has revealed a dearth of scholarship on terrorist financing innovation and it is this dearth which acts as a driving force for this paper.

Specifically, one recent innovation in terrorist financing stands out as especially important, and that is the introduction of cryptocurrencies in to the terrorist financing ecosystem. Beginning in 2014, terrorist organizations have been using cryptocurrencies as a means of funding their operations.[5] Albeit sparingly, groups such as the Islamic State, al-Qaeda, and their

[5] Steven, Stalinsky. "Terrorists Have Been Using Bitcoin for Four Years, so What's the Surprise?" TheHill. March 08, 2018. Accessed November 02, 2018.

affiliates have sought funding in the form of cryptocurrencies for activities ranging from online server maintenance to violent campaigns. To this end, it has been reported that the 2015 Charlie Hebdo attacks were funded primarily through cryptocurrencies provided by Al-Qaeda on the Islamic Peninsula.[6]

Furthermore, as various pressures increase on traditional methods of terrorist financing, and as technologies become increasingly easier to use, it seems that cryptocurrencies will become both more appealing and more practical for a wide base of terrorist organizations around the world. As the world of possibilities for terrorist organizations continues to expand with advances in technology, innovation within these groups can be expected to occur with greater frequency and at a greater scale along with it. Just as businesses are working to remain relevant relative to current technological trends, terrorist organizations must do the same. They provide amenities to fighters, pay for travel, and maintain physical presences around the world, all while constantly competing and recruiting new fighters into their ranks. All of these operations in the current age require strong technical savvy and robust technological capacity which will be easier for terrorist organizations to procure as time progresses.

Despite existing in a technological age which seems receptive to innovation, along with being obstructed by an increasingly effective counter-terrorism financing regime, no terrorist organizations have not yet adopted cryptocurrencies at the system level.[7] Systematic adoption refers to the use of cryptocurrencies for executing operational expenditures and distributing funds to those on the payroll. While achieving adoption to this extent will take time, it does not

[6] Ibid

[7] Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3026.html.

appear that terrorist organizations are taking aggressive steps to arrive at this eventuality. The reason for this apparent risk aversion, and the resulting diversity of adoption levels among terrorist organizations, is puzzling and is the subject of my research.

Organization of the Paper

In my attempt to find a solution to the puzzle laid out above, I will discuss three cases of terrorist organizations who have used cryptocurrencies: al-Qaeda, Hezbollah, and the Islamic State. In the case of al-Qaeda, which is truly a transnational terrorist group, I will used data from al-Qaeda in the Arabian Peninsula (AQAP), al-Qaeda in the Islamic Maghreb (AQIM), and al-Shabaab as proxies for a single al-Qaeda entity. These are three of the most prominent, long-lasting al-Qaeda franchises and account for many of the fatalities and injuries caused by the group. As such, I found these groups to be adequately representative of the entire organization for the purposes of this study.

Against these cases I will test six hypotheses in the hopes of discerning a hypothesis that is validated by every case. Ultimately, I found that the primary feature of a terrorist organization which indicates potential cryptocurrency adoption is the status of the group's current financing techniques. If a group is experiencing a bottle neck of funding, either from sanctioned state sponsors or disrupted illicit commerce enterprises, they will turn to cryptocurrencies out of survival to finance their operations. Terrorist groups value fiscal capacity at a premium, and as such they will be forced into finding alternative sources of funding their operations. At the time, cryptocurrencies are the most convenient and beneficial technology capable of filling the void of fiat currency in terrorist organizations.

Finally, I will end my paper with a conclusion of the results of my research. I will also provide an overview of the potential policy implications of my findings. As the threat of cryptocurrencies in terrorist hands gradually becomes reality, it is critical that the United States national security apparatus be well-prepared.

Chapter II: Cryptocurrency Overview

A cryptocurrency is a virtual currency used to execute secure transactions between parties.[8] Similar to the American dollar, cryptocurrencies have value and are used to buy and sell goods and services through cyberspace, loosely defined as the environment where information is exchanged over computer networks.[9] Additionally, cryptocurrencies are 'soft' currencies meaning they are not supported by a stable government or available in physical form such as the American dollar, British pound, and Euro. While certain states have begun to adopt cryptocurrencies for their own purposes - Venezuela to combat rising inflation rates and North Korea to evade U.S. sanctions - the technology still operates within a decentralized network. Furthermore, for context, according to the Oanda Corporation, a foreign exchange company, the value of a single Bitcoin, the most prominent cryptocurrency in use, is in excess of $3,500 as of February 14th, 2019.[10]

Transactions using cryptocurrencies are carried out through blockchain technology, rendering each transaction immutable, anonymous, and secure. Each transaction is verified for

[8] Lennart, Ante. "Cryptocurrency, blockchain, and crime." In *The Money Laundering Market: Regulating the Criminal Economy*, edited by McCarthy Killian J., 171-198. Agenda Publishing, 2018.
[9] Ibid
[10] Ibid

authenticity using a series of mathematical formulas.[11] The blockchain is functionally a series of digital blocks, each containing information about transactions. In the case of Bitcoin, this information would include both the sender and receiver of the transaction (made cryptic through the use of public Bitcoin addresses), as well as the size of the transaction. Each block also contains a 'hash,' which refers to a unique code (similar to a fingerprint) that can be used to identify a transaction.[12] If the block is altered in anyway, its 'hash' would change, altering the relevant accounts of a breach in their security. Finally, each block also contains the 'hash' of the previous block, linking them together in cyberspace - a conceptual space connected by computer networks and accessed through various forms of digital technology.[13] This means that if a single block is tampered with, it will also alert each following block, and these blocks will not longer be valid as well.[14] When this happens, the transaction in the manipulated block will no longer have consensus from blockchain miners, and the blockchain would reject the block, getting rid of it permanently. To illustrate, the diagram below shows the connection of hashes within a blockchain.

[11] Ibid
[12] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Accessed February 12th, 2019. https://bitcoin.org/bitcoin.pdf
[13] Ibid
[14] Ibid

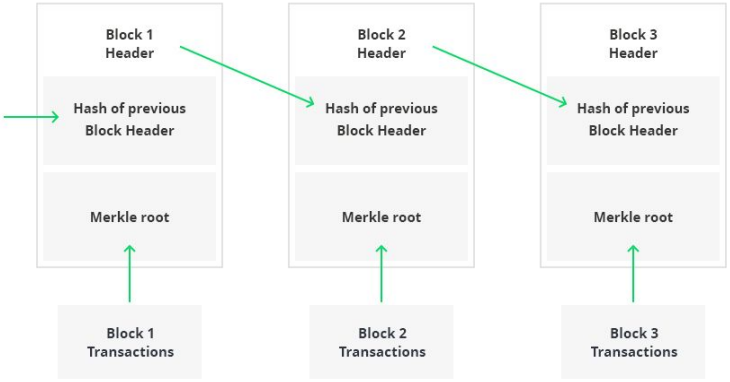

Diagram https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

The cryptocurrency landscape has been quite volatile since its introduction to the public.[15] In 2017 Bitcoin, the most popular cryptocurrency on the market currently, had a market capitalization 15 times greater than the previous year. The cryptocurrency market as a whole saw a spike of 3,400% in the same year.[16] Since then, both Bitcoin and the cryptocurrency market have dropped substantially, but still hold significant value. There are over one-thousand cryptocurrencies currently on the market, each with their own blockchains, and this wide array of currencies may very well account for the volatility of the technology.[17]

This large number of cryptocurrencies is due in part to general market trends and space for innovation in the cryptocurrency sector, and in part to specialization and differentiation within cryptocurrencies.[18] While coins such as Bitcoin and Ethereum remain the market leaders

[15] Spencer, Applebaum. "Analysis of the Cryptocurrency Exchange Landscape – Miami University Blockchain Club – Medium." *Medium.com*, Medium, 31 Dec. 2017
[16] Ibid
[17] Ibid
[18] "Why Are There So Many Cryptocurrencies?" Coindirect. September 26, 2018. Accessed April 11, 2019. https://blog.coindirect.com/so-many-cryptocurrencies/.

in the cryptocurrency industry, newer 'alt-coins' have been spreading which put a premium on privacy.[19] These include Dash, Zcash, and Monero. There are also industry-specific cryptocurrencies being developed on top of existing blockchains such as Bitcoin and Ethereum, which while connected to existing technologies do qualify as independent, discrete coins.[20] Coins also tend to differ in price, scalability, and anatomy, as the security schema of Dash, Zcash, and Monero are all markedly different.[21]

Diagram: https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited

The most popular of these however, including Bitcoin, Ethereum, and Rippel have all seemed to gain a larger market capitalization than the rest of the industry, rising to premier status in the cryptocurrency market.[22] In addition to a large number of cryptocurrencies on the market,

[19] Ibid
[20] Ibid
[21] Ibid
[22] Ibid

infrastructure for cryptocurrencies is also expanding. The number of cryptocurrency exchanges, where cryptocurrencies can be traded for various fiat, or government-backed, currency, is rapidly growing as well. This trend is expected to continue as more parties begin to use the technology.[23] By their nature, cryptocurrencies are not backed by any commodity or government, and its supply is not predicated on the decisions of central banks.[24] It is a purely virtual currency and can currently only be transmitted through this process which is founded on blockchain technology. It is commonly known, for example, that there are only 21 million Bitcoin in existence (including those coins which have not yet been mined) and that once they have all been mined, there will be no more Bitcoin in the world. This has led to an increased effort to mine Bitcoin, as individuals want to be in possession of the commodity before it becomes extremely sparse. These traits have been central to the widespread adoption of the technology by countries, companies, and individuals around the world.

To avoid tampering altogether, the Bitcoin blockchain implements a method called Proof-of-Work, or PoW. PoW is an algorithm that relies on consensus from decentralized members of the blockchain community. Although relatively timely, this process is the reason why Bitcoin is viewed as a secure cryptocurrency brand - in exchange for some work the network is able to disarm denial of service attacks on the servers and other harmful cyber behavior. Essentially, when a block of transactions is proposed, "miners," individuals who compete to process transactions into the blockchain for Bitcoin rewards, begin a process of generating a critical mass of random guesses to fit the frameworks set out by the Bitcoin blockchain.[25] This includes compiling hashes from the prior block, the transaction information

[23] Ibid
[24] Ibid
[25] Ibid

for the current block, and finding a random number that will result in a specific number of zeros in the new hash. Once this task is completed, a "miner" will receive Bitcoin in exchange for their services. This process is shown below:

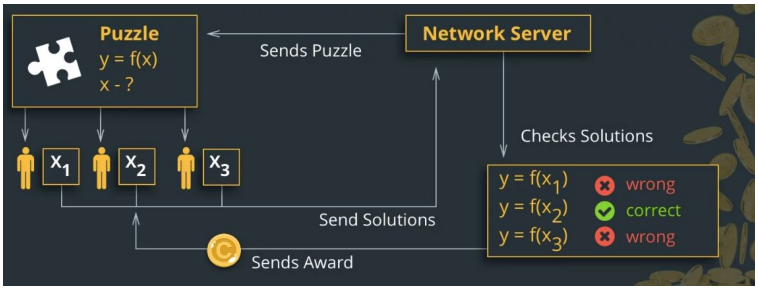

Diagram: https://cointelegraph.com/explained/proof-of-work-explained

According to Noelle Acheson, a blockchain capital markets researcher at CoinDesk, this process involved running approximately 10^{21} computations, which takes an average of ten minutes, although this can vary based on computer power.[26] It is this process of discovering hashes that allows for the title Proof-of-Work, as the process is both extremely time-intensive and expensive. PoW also prevents tampering, however, as altering the contents of a single block will require the altering of each following block in the blockchain. This would require going through this time-intensive and expensive process a prohibitive number of times. In addition to rehashing an enormous amount of blocks, an individual or group would have to gain control of over fifty-percent of the blockchain network, as each processed block goes through a consensus process carried out by each 'node,' or actor, in the network.[27] This sort of secure ledger has been used in contexts other than personal finance, such as to store medical records and create tax

[26] Acheson, Noelle. "How Does Proof of Work, Um, Work? – Decentralize Today." Decentralize Today. June 06, 2016. Accessed February 12, 2019.
[27] Ibid

ledgers. Its most popular use to date, however, has been through the use of cryptocurrencies such as Bitcoin.[28]

As demonstrated above, cryptocurrencies offer many benefits to their users. Transactions using cryptocurrencies such as Bitcoin are permanent, difficult to intercept due to their enigmatic and decentralized nature, relatively anonymous, and reasonably expedient compared to alternative options of decentralized payments. Additionally, using Bitcoin or similar cryptocurrencies inherently subverts traditional financial institutions, such as banks, which implement greater oversight and security measures over exchanges that happen through their platforms. Payments using cryptocurrency move through a completely different cyberspace than payments transacted through a traditional bank, which allows payments with cryptocurrency to often avoid detection, or at least be harder to trace. Cryptocurrency technology would afford terrorist organizations the ability to move money quickly, anonymously, and at scale amongst group members or even between groups. This shift in funding would not only allow for larger weapons shipments, for example, but also more frequent weapons shipments through more convenient payment methods which completely alters the organizational and material capacity of a terrorist organization.

As stated earlier, this technology has not yet been adopted on a systematic level by terrorist organizations, in spite of its many stated advantages. To determine why this might be the case, it is crucial to fully comprehend the current counter-terrorism financing regime in order to gain a more complete understanding of the relationship between financial regulatory bodies and the advent of this new currency. The current counter-terrorism financing regime has had

[28] Ibid

great effects on traditional means of financing used by terrorist organizations, and its reach into the realm of cryptocurrency has steadily grown over time. This can be most easily observed through the growing array of use cases for cryptocurrencies as demonstrated by both state and non-state actors alike.

Uses of Cryptocurrencies

National governments such as Venezuela have created their own cryptocurrency to mitigate the devastating effects inflation has had on the country.[29] In December, 2017, president Nicolas Maduro announced the forthcoming Petro, a state-sponsored cryptocurrency which would be used to combat inflation and circumnavigate United States sanctions.[30] The currency was backed by 5 million barrels of oil allocated by the Venezuelan state, allowing each Petro to be worth a Petro of oil. The currency has seen middling success thus far - Petro is still be integrated into state institutions and was recently implemented into Venezuela's pension program.[31] Currency backed by commodities such as gold or oil can demonstrate volatile price trajectories, as commodities can be depleted. Currencies backed by law such as the United States dollar tend to be more reliable. Venezuela will now have to maintain the well-being of its oil reserves as well as reform their economic systems if it hopes to rectify the country's recent misfortunes.[32]

[29] David, Orrell, and Roman Chlupatý. "Changing the Dominant Monetary Regime, Bit by Bitcoin." In *The Evolution of Money*, 196-219. Columbia University Press, 2016.
[30] Daria, Dorovskaya, et al. "Inflation in Venezuela and Cryptocurrency. Influence of Hyperinflation in the Country on Cryptocurrency Prices." *The Coin Shark*, The Coin Shark, 11 Sept. 2018
[31] Ibid
[32] Ibid

States such as Iran and Russia have reportedly considered similar measures with their goal being to evade United States sanctions.[33] By implementing a currency which can act as an alternative to each country's respective fiat currency, Iran and Russia would have a vehicle for circumventing United States dollar-based economic regulation in addition to international banking institutions.[34] Often deemed as rogue states who act in discordance with the international community, Iran and Russia would both benefit greatly from the adoption of new, more elusive means of financing their operations.[35]

The Democratic People's Republic of Korea has also been a very visible user of cryptocurrencies in an effort to avoid United States sanctions.[36] By trading cryptocurrencies in a similar manner to commodities on a stock exchange, as well as through the creation of cryptocurrencies, North Korea has been able to generate funds in the face of monetary regulations. By launching their own cryptocurrencies and opening domestic cryptocurrency wallets, North Korea has been able to infiltrate cryptocurrency systems appearing as a non-threatening nation using cryptized communication.[37] North Korea also uses transaction mixers, which obscure the trail of a transaction in a blockchain by splitting linears paths of a single transaction to make the trail of money unclear.[38]

Finally, there are cryptocurrency shifting services which North Korea has used that change the nature of cryptocurrencies altogether, from Bitcoin to another cryptocurrency,

---

[33] Samburaj, Das. "Iran and Russia Consider Using Cryptocurrency to Evade US Sanctions: Report." *CCN*, CCN, 21 May 2018
[34] Ibid
[35] Ibid
[36] Chong, Nick. "Researchers: North Korea Is Trading Crypto To Undermine International Sanctions." Ethereum World News. September 25, 2018. Accessed April 11, 2019. https://ethereumworldnews.com/north-korea-crypto-sanctions/.
[37] Ibid
[38] Ibid

making the trail even more scarce. North Korea is then able to use this new cryptocurrency to exchange for fiat currency on any national market or exchange, procuring the American dollar free of sanction.[39] This is the same technique that many terrorist organizations use to launder money - move it, change it, clean it, and you can have it. By taking all of the aforementioned steps, a process which was once linear in a nature (literally a chain) is obscured and bent such that a cogent path of money is no longer recognizable.[40]

Cryptocurrencies have also been used by both companies and individuals for point-of-sale transactions as well as storing money and investing.[41] Companies such as Microsoft, Paypal, and sandwich chain Subway all accept cryptocurrency payments, and more companies are beginning to accept the technology as time continues. There is functionality to cryptocurrencies - its transactions are cheap, the pool of people with access to the technology is much greater than that with access to traditional banking apparatuses, and the pool of companies who can use the technology is also greater as risky business models may not be supported by traditional banks.[42] There is a universality to cryptocurrencies that make them so exciting to individuals and companies alike, and its adoption by the private sector as well as the public sector is expected to rise in the coming years. [43]

---

[39] Ibid
[40] Ibid
[41] Steinmetz, Fred. "Using Blockchain Technology for the Prevention of Criminal Activity." In *The Money Laundering Market: Regulating the Criminal Economy*, edited by McCARTHY KILLIAN J., 199-222. Agenda Publishing, 2018.
[42] Harrison, Kate. "Should Your Company Accept Bitcoin And Other Cryptocurrency Payments?" Forbes. September 19, 2018. Accessed April 11, 2019. https://www.forbes.com/sites/kateharrison/2018/09/10/should-your-company-accept-bitcoin-and-other-cryptocurrency-payments/#318bb9a43373.
[43] Ibid

Despite the gradual adoption of the technology, however, the cryptocurrency landscape has been quite volatile.[44] In 2017 Bitcoin, the most popular cryptocurrency on the market currently, had a market capitalization 15 times greater than the previous year. The cryptocurrency market more generally saw a spike of 3,400% in the same year.[45] Since then, both Bitcoin and the cryptocurrency market have dropped substantially, but still hold significant value, pricing at many thousands of United States dollars in the contemporary context. There are over one-thousand cryptocurrencies currently on the market, and this wide array of currencies may make any definitive statements on the future of cryptocurrencies difficult to come by.[46] The question of which cryptocurrencies will ultimately become more popular or gain the most market share is difficult to answer at this point, and only time will be able to accurately determine the future of the cryptocurrency landscape.

The most popular of these however, including Bitcoin, Ethereum, and Rippel have all seemed to gain a larger market capitalization than the rest of the industry, rising to premier status in the cryptocurrency market.[47] In addition to a large number of cryptocurrencies on the market, infrastructure for cryptocurrencies is also expanding. Both physical and digital infrastructure in the form of robust servers, cryptocurrency ATMs, cryptocurrency wallets, permissive regulatory apparatuses have expanded in recent years, preparing regions of the world for the advent of pervasive cryptocurrency adoption.[48] The number of cryptocurrency exchanges, where

[44] Spencer, "Analysis of the Cryptocurrency Exchange Landscape…"
[45] Ibid
[46] Ibid
[47] Ibid
[48] Ibid

cryptocurrencies can be traded for various fiat currency, is rapidly growing as more parties begin to use the technology.[49]

As early as 2014 terrorist organizations have been using cryptocurrencies, specifically Bitcoin, as a means of securing funding for their operations.[50] Albeit sparingly, groups such as the Islamic State, al-Qaeda, and affiliates of the aforementioned groups have sought funding through cryptocurrencies to finance their operations.[51] Furthermore, as various pressures increase on traditional methods of terrorism financing, and as technologies become increasingly easier to use, it seems that cryptocurrencies will become both more appealing and more practical for a wide base of terrorist organizations around the world.[52]

Within the world of terrorism, and as alluded to earlier in the paper, terrorist organizations are making strides to various degrees with respect to their adoption levels of cryptocurrencies. Some groups, like Hamas, have been very active in adopting cryptocurrency technology while other groups like al-Qaeda have been much less active in the space.[53] While on the whole there has been limited observation of cryptocurrencies being used by terrorist organizations, rendering the aforementioned examples slightly less significant, the threat of future use has been sufficient to spur abundant policy and literature about the subject.

[49] Ibid
[50] Steven, "Terrorists Have Been Using Bitcoin…"
[51] Ibid
[52] Ibid
[53] Cuen, Leigh. "Blockchain Analysis Links Hamas Fundraising to Coinbase Bitcoin Account." CoinDesk. February 07, 2019. Accessed April 20, 2019. https://www.coindesk.com/hamas-coinbase-bitcoin.

Chapter III: The Puzzle

Cryptocurrencies have the potential to serve many functions for terrorist organizations which may augment their current financing capabilities. For example, the hawala system requires face-to-face interaction which can add an unneeded element of risk to a transaction.[54] These meetings rid a transaction of its anonymity and can introduce the potential for physical harm, two concerns which do not exist with transactions carried out using blockchain technology. Additionally, oddly enough, this technology has marketed itself as one built on trust, as the consensus process of proof-of-work demonstrates. This is interesting because it seamlessly fits in alignment with the hawala system, a payment network used by terrorist groups today which heavily relies on trust as well.

Cryptocurrencies allow groups to bypass the interpersonal aspects of transferring funds that accompany such a system while maintaining this aforementioned premium on privacy. Cryptocurrencies can facilitate the illegal commerce which terrorist organizations often participate in as well. This can come in the form of creating a cryptocurrency wallet which is open for donations or conducting point-of-sale operations for contraband on the black market. Additionally, the reliability of these transactions provides an assuredness not often found in other financing methods.

For a number of terrorist groups who rely on state sponsors to fund their activities, cryptocurrency technology is especially beneficial. As countries are already beginning to recognize, such as North Korea, cryptocurrencies can be used to evade sanctions, making what

[54] Aman, Moustapha, Nikolay Nenovsky, and Ismaël Mahamoud. "The Informal System of Remittances and Currency Board: Complementarity or Antagonism? the Case of Hawala Transfers in Djibouti." Savings and Development 38, no. 1 (2014): 133-54. http://www.jstor.org/stable/savideve.38.1.133.

once was a relatively risky funding source more reliable.[55] Groups like Hamas and Hezbollah who rely on states like Iran, Palestine, and Lebanon for their funding, will now have greater assuredness in the future of their monetary well-being.[56] Many terrorist groups who do not rely on state sponsors for funding will be able to use cryptocurrencies to a similar end - dodging public ledgers that record banking transactions and instead conducting clandestine payment operations. Cryptocurrencies add a level of security and convenience to terrorist groups of all sorts, which poses an even larger threat to counterterrorism efforts being carried out today.[57]

This issue was discussed in-depth in a report entitled "Terrorist Use of Virtual Currencies: Containing the Potential Threat" written by Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss and published in the Spring of 2017 by the Center for a New American Security.[58] In Chapter 4, titled "Virtual Currency Abuse in the Future: Criminals vs. Terrorists," the report states that "if terrorist groups develop more of the characteristics of criminal enterprises, such as broader person-to-person networks of trust, technical sophistication, and the need for a wider funding base, virtual currencies might become more attractive" (26).[59] The report goes on to delineate five points about the value of the technology to illicit groups: 1. The greatest degree of anonymity for both users and transactions; 2. The ability to quickly and confidently move illicit proceeds from one country to another; 3. Low volatility (in technology stability or price), which results in lower exchange risk, increasing

[55] Chong, "Researchers: North Korea Is Trading Crypto..."
[56] Cuen, "Blockchain Analysis Links Hamas Fundraising…"
[57] Ibid
[58] Goldman, et al. Terrorist use of Virtual Currencies*: Containing the Potential Threat*. Report. Center for a New American Security, 2017. 9-16.
[59] Ibid

the virtual currency's ability to be an efficient means to transmit and store wealth; 4. Widespread adoption in the criminal underground; 5. Trustworthiness.

To this end, Gregory Nevano, Deputy Assistant Director of the Illicit Trade, Travel, and Finance Division of Homeland Security Investigations was quoted in a financial services committee press release in June, 2018, stating that "The pseudo-anonymity and ease of transfer cryptocurrency provides have led to expanded use by traditional criminal organizations with ample opportunity for expansion as it becomes more mainstream… Technology will inevitably continue to evolve, and law enforcement agencies everywhere must continue to adapt and evolve as well…"[60]

Furthermore, as stated earlier in the paper, innovation is essential to the identity of terrorist organizations. This can be seen clearly in the case of Aum Shinrikyo. In 1995 Aum Shinrikyo, a Japanese doomsday terror group based in Buddhist religious doctrine, carried out an orchestrated attack on multiple train cars in Tokyo, afflicting thousands with exposure to sarin gas.[61] Prior to 1993 Aum Shinrikyo operated primarily as a cult organization, proselytizing and subsequently retaining membership by way of exploitation and blackmail. Their central funding channels were tied to extortion of local business and hospitals, playing the role of mafia in 1980s and 1990s Shibuya, Tokyo. This transition from dangerous, albeit relatively stable religious crime organization to lethal terrorist group was as quick as it was unexpected. This transformation of organizational profile was a demonstration of intentional strategic and material

[60] "Combating the Illicit Use of Virtual Currencies." *Financial Services Committee*, The United States House Committee on Financial Services, 20 June 2018,
[61] Gunaratna, Rohan. "Aum Shinrikyo's Rise, Fall and Revival." *Counter Terrorist Trends and Analyses* 10, no. 8 (2018): 1-6.

innovation - Aum Shinrikyo spent copious resources and manpower to both develop usable sarin gas and in doing so created the requisite organizational capacity to carry out such an attack.[62]

Innovation can increase the profile and credibility of a group, as it did in the case of Aum Shinrikyo. It can happen in a short window of, and vastly increase the capabilities of an organization with respect to strategy, material ability, and ideology. In the same manner that weapons are an asset to a terrorist organization, so is the ability to innovate and move with changing times - remain relevant and threatening even as epochs and technologies develop and shift over time.[63] Innovation, for many groups, is a means of sustenance in a dangerous, anarchic international system. It is a means of survival. This was the case for Aum Shinrikyo, and this is what is available to terrorist groups today who are considering innovating and adopting cryptocurrency technology.[64]

Despite all of this, however, cryptocurrencies have yet to be implemented in terrorist organizations on a systemic level. Cryptocurrencies are not the central means of financing for any terrorist organization, and technology has yet to be fully integrated into the financial and operational infrastructure of these groups. Such integration might come in the form of using cryptocurrencies to pay out salaries for a group's payroll. Cases of its usage within terrorist groups are often anecdotal and relatively small in scale. This is my puzzle. Why, despite all of the potential benefits provided by cryptocurrencies, has nearly every major terrorist group

---

[62] Ibid
[63] Booker, Chaka. "Innovation Is A Fancy Word For Survival." Forbes. November 27, 2018. Accessed April 20, 2019. https://www.forbes.com/sites/chakabooker/2018/11/27/innovation-is-a-fancy-word-for-survival-baltimores-dirt-bike-culture/#4cfcb4fc4d10.
[64] Ibid

around the globe resisted its absolute adoption? And what accounts for the gradient in levels of adoption that we see by various terrorist groups today?

Chapter IV: Literature Review

One quite popular approach to this question is the study of terrorism innovation. Terrorism innovation explores the processes and prerequisites for innovation within terrorist organizations, using innovation and social theory to both predict and analyze adoption decisions. Most literature on terrorist innovation suggests that material resources and grand strategy are the most important factors to consider when predicting the innovation potential of a terrorist group. Essentially, a terrorist group must have access to, or the potential to gain access to things such as natural resources, trade routes, or strategic schema in order to innovate or develop. Magnus Ranstrop and Magnus Normark, editors of *Understanding Terrorism Innovation and Learning*, a key work in the discipline, argue that terrorists innovate when certain social and psychological benchmarks are met. To the editors, understanding why terrorist organizations may or may not adopt cryptocurrencies will go beyond strategic, capacity-related, or material aspects of analysis - immaterial aspects of terrorist organizations will play a role also.[65] This examination of social psychology can encompass issues of ideology, group history, and culture. Furthermore, Ranstrop and Normark delineate a set of steps necessary for the completion of an innovation within a terrorist organization as well as a list of 'delimiters' which would impede an adoption decision. There are two of these 'delimiters' in particular which I plan to use in this paper as potential answers for the question posed earlier.

[65] Magnus, Ranstrop, and Magnus, Normark, eds. *Understanding Terrorism Innovation and Learning*. Abingdon: Routledge, 2015: 5-10.

Ideology

First is the idea that the innovation must be within a groups technical abilities and resources, or at least within their expected capacity to acquire those resources.[66] This can be an issue for terrorist organizations based in areas without robust access to the computing power necessary to both mine and store cryptocurrencies securely. Second is the that "For adoption to be pursued the use of the proposed novel weapon or practice must not be anathema to deeply held cultural values or the worldview…of the terrorist group" (24).[67] It is possible that cryptocurrencies are viewed as an inherently Western technology, and therefore fundamentally incompatible with certain Jihadi sentiments. Unless a group that fits this archetype has carried out a number of operation which pose a similar dilemma to the group, thereby creating precedent for a decision like adopting cryptocurrency, then adoption of cryptocurrencies at a systemic level of a terrorist organization such as this one is very unlikely. In this way, institutional memory within terrorist groups is critical for innovation success. Moreover, simply the idea of innovation itself can be viewed as antithetical to a group's central values. Although these issues can potentially be assuaged using cost-benefit analyses, these 'delimiters' are important to consider when devising an answer to the proposed question.

Adam Dolnik, author of *Understanding Terrorist Innovation: Technology, tactics, and global trends*, on the other hand argues that terrorist innovations are a function of ideology, and more specifically levels of 'radicalism' within terrorist organizations.[68] Although Dolnik does

[66] Ibid
[67] Ibid
[68] Adam, Dolnik. Understanding Terrorist Innovation: Technology, Tactics and Global Trends. Place of Publication Not Identified: Routledge, 2013.

not operationalize this hypothesis directly, his findings are consistent with what seems to be the zeitgeist with respect to terrorist activities. Ranstrop and Normark reference Dolnik's work often throughout their own book, and rely on his initial research and inquiries to base their own analyses. While Dolnik's book also focuses on innovation with respect to the material capabilities of terrorist organizations, Dolnik explores the issues of ideology, group dynamics, and the future of terrorist technology more than the other two editors.

With respect to ideology, Dolnik states that "terrorists' innovation has been hypothesized to be driven by the need to achieve the capability necessary for reaching and sustaining the level of intensity preferred by the group" (146).[69] Essentially, if a group wants to be viewed as, and operate as a radical organization, than it will require capabilities which map to that identity. The innovations which this group chooses to make, then, will be determined by the capabilities needed by the group. This logical reasoning with respect radical organizations is central to the choice of adopting technology such as cryptocurrency within terrorist organizations and must be considered when doing this sort of research.[70]

Regarding group dynamics, Dolnik maintains that organizational capability, defined as an organization's ability to communicate without friction amongst the group, is key for innovation - a leader of a terrorist group must be able to both see value in a particular innovation and be able to "impose such a decision successfully on the rest of the group" (158). To this end group structure and hierarchy is key to achieving innovation.[71]

Finally, Dolnik writes about the future of terrorist innovation, noting that historically, innovation within terrorist organizations has been limited. As opposed to introducing radical

[69] Dolnik, 144-160
[70] Ibid
[71] Ibid

change which might alter the dynamics of a group structurally or otherwise, terrorist organizations have tended to improve and modify existing tactics and technologies to retain order.[72] This notion acts as a backdrop for discussion surrounding innovation in any area. However, linking with his earlier points, Dolnik claims that the terrorist organizations who are most likely to adopt new, radical technologies are also the groups with more extreme ideologies, who seek greater control in a region or seek to kill large numbers of people. Here, extremity of group is more relevant that the successfulness of a group - a group which has wrought a low-number of casualties but has ambitions to kill an immense number of people would still qualify to fit in this theory. With greater ambitions, Dolnik posits, come greater risks taken to achieve those ends.[73] While Dolnik is correct in creating a connection between ambitions and innovation, there are examples of radical groups who have not innovated radically with respect to various aspects of their organization. As a result it is fair to say that great ambitions and a radical ideology are necessary but not sufficient to drive radical innovation - there are other aspects that play an as large, if not larger role in a group's ultimate decision to innovate.

Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism by Michael C. Horowitz is another important voice within the scholarship.[74] While Horowitz's text focuses solely on the choice of terrorist groups to adopt suicide tactics, the methodology used to analyze this phenomenon are relevant to this study. Horowitz argues that groups with a small operational history, in this case groups who have not innovated on their financing strategies much in the past, will be more open to adopting new financing methods.[75] This is because prior

[72] Ibid
[73] Ibid
[74] Michael, C. Horowitz "Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism." *International Organization* 64, no. 1 (2010): 33-64.
[75] Ibid

approaches will not be privileged over newer ones, allowing for greater group flexibility. There is no system or precedent to be stuck in - terrorist groups will have freedom to innovate radically when they do not have a history of innovating and change.

This claim dialogues with that of Dolnik who states that more radical groups are more likely to innovate and at a great scale.[76] If more radical groups will innovate more, and more frequent innovation will lead to less innovation, then innovation within radical groups may not be sustainable, and moderate terrorist groups will be the primary actors in this narrative. It is very possible, with respect to Horowitz's argument, that groups who have not innovated in the past are simply stuck in their ways - stubborn and obstinate. However, Horowitz's theory still have import in the context of this study as the potential that a group with few innovative historical trends innovates in a radical way could greatly inform the cases that will be interrogated later in this paper.

Horowitz also claims that networks are critical to adoption potential for terrorist organizations.[77] Connection with other terrorist groups who are similar with respect to geographic location or belief system can help facilitate and expedite innovation. If a terrorist organization witnesses a second group, who is similar, innovating or going through innovative processes, the first group will be more likely to innovate itself.[78] Horowitz does not specify in his book the degree to which groups must be similar in order for their to be a domino effect in innovation trends, but the nature of his argument suggests that there must be nominal similarities and few points of conflict for this theory to take effect.

[76] Ibid
[77] Ibid
[78] Ibid

Within the structuring of a terrorist organization, the decision-making process for adopting a new financing mechanism such as cryptocurrencies may be identical to that of material innovation such as introducing a new weapon into an arsenal. Terrorism is a dynamic phenomenon, and the key to its continued presence and success is its ability and willingness to adapt to changing environments.[79] In this way, the practice of innovation is baked into the fabric of terrorist practices in a way that cannot be said for other constitutive bodies such as NGOs or other institutions.

The approach of terrorism innovation, however, is not a perfect answer to the proposed question for a number of reasons, however. While it is a necessary explanation to explore when addressing these questions, it is not a sufficient answer to the question of terrorist innovation in the case of cryptocurrency adoption. As the authors demonstrate, terrorism innovation literature often relies on the idea that innovations within terrorist organizations are both 'recombinant' and 'recursive'. This is to say that innovations are always some combination of consolidation of currently existing technologies, and that these innovations exist in a gradual process. Essentially, innovations will continue to update and develop on older tactics or technologies, progressing in a linear fashion save for disruption to the chain. What is being explored in this study is a more radical innovation, one that is not recombinant nor recursive. Cryptocurrency technology presents a shift away from interpersonal forms of moving money. It also adds a greater element of risk to a terrorist group's operations, adding to the radical nature of adopting the technology.

While that analysis may be appropriate when considering material innovation such as the modification of a bomb or attack strategy, financing mechanisms are different. Such innovations

[79] Jacob N., Shapiro. "Terrorist Decision-Making: Insights from Economics and Political Science." *Perspectives on Terrorism* 6, no. 4/5 (2012): 5-20.

happen with less frequency, as financing can often be a more discreet practice than material operations, and often with different considerations than material innovations, adding nuance to my research relative to this school of thought. The Hawala system, for example, originated in the 8th century and is still used to this day by various terrorist organizations and criminal enterprises.

Criminal Enterprise

Another approach to the question of terrorist adoption of cryptocurrencies is the study of the terrorist enterprise scholarship. Understanding how terrorists collect funds through their business operations can inform both how cryptocurrencies might augment their current enterprise and why these groups have yet to systemically adopt the technology. Louise Shelley, author of *Dirty Entanglements: Corruption, Crime, and Terrorism* has explored this issue in detail.[80]

According to Shelley the business operations of terrorist organizations are not constrained to simply the creation and operation of business for the purposes of raising funds.[81] This notion of business operations can also carry over to criminal activity such as bank robberies and kidnapping which have become business themselves in many regions of the world. This expansion of the idea of business within the context of terrorist activity can increase the possible functions of cryptocurrencies for terrorist organizations exponentially.[82] Whereas business operations such as shell companies often receive greater scrutiny from national governments and agencies, individual payments are more inconspicuous, making enterprises such as kidnapping or murder more appealing as channel for receiving funds.

[80] Louise I., Shelley. *Dirty Entanglements: Corruption, Crime, and Terrorism*. New York, NY: Cambridge University Press, 2014: 259-280.
[81] Ibid
[82] Ibid

Shelly also discusses the trade of counterfeit and antique goods by terrorist organizations to fund their operations. According to Shelley these revenue streams are very poorly regulated which adds an element of appeal to them for terrorist groups.[83] Shelley claims that these poor regulatory efforts are due, in large part, to the international nature of the business endeavors. International trade has always been a pain point for the international community regarding the codification of legislation to adequately preside over the practice.[84] Because of this, terrorist organizations have been able to take advantage of holes in international trade enforcement and law in order to carry out their activity.[85]

If certains means of financing, through businesses or charities, has not been criminalized on the international stage (for example), groups can make use of these channels to finance their operations transnationally, without worry of persecution by international legislative bodies. Cryptocurrencies are in a similar space, where due to its recency, regulation surround the technology is sparse. Shelly provides examples in her book of innovation that is poorly regulated, such as the proliferation of improvised explosive devices (IEDs) and their subsequent relevant success.[86] Essentially, adoption is more likely to occur in the presence of weak regulatory regimes. This concept will also play a factor in this paper.

Shelly's focus, however, is on the transnational aspects of the crime and corruption that often accompany terrorist activity, and not the mechanisms by which these practices are conducted necessarily. While not focusing on the individuals manifestations of criminal

[83] Ibid
[84] Ibid
[85] Ibid
[86] Ibid

enterprises outlined in Shelley's book, my paper will focus on the potential to modify the practices Shelley discusses through the use of new technologies, specifically cryptocurrency.

A similar text that focuses more on the tracking of terrorist funding than the mechanisms by which terrorists acquire said funding is *Speculative Security: The Politics of Pursuing Terrorist Monies* by Marieke de Goede.[87] The book is based in the post-9/11 security landscape where de Goede claims that the fight against terrorist financing has shifted immutably.[88] More attention is paid to the various tactics which terrorist organizations use to finance their operations and new tools to combat these strategies have also arisen. Written in 2012, de Goede states that the United States, the United Kingdom, and the Netherlands have been at the forefront of this fight again terrorist funding.

The central claim of de Goede's book is that in the post-9/11 security landscape, and in the wake of the term "war on terror" descent from popularity, the fight against terrorist financing has gained steam. More resources and public approval have been allocated towards what de Goede terms the 'finance-security assemblage' of our current era.[89] This 'assemblage' refers to the securitization of financing in the international system that led to government crackdowns on illicit financing operations. These efforts alongside the preemptive nature of counterror analysts working around the world, de Goede believes, have had a large impact on the current mechanisms which terrorist organizations use to finance their operations. Not all of these efforts are equal however, as some are more effective than others, creating great variation in the usage

[87] Marieke De., Goede. *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press, 2012.
[88] Goede, 15
[89] Ibid

of cryptocurrencies by terrorist organizations. Where Shelley dives into these mechanisms, de Goede gives a thorough overview of how these tactics are being countered.

These texts are both central to my study, as an understanding of the ways in which terrorist organizations are able to secure funding is central to my research. The focus of the authors, especially de Goede, however, do not perfectly align with the tenor of my research. Terrorist funding will not undergo wholesale change due solely to external pressures from governments bent on impeding groups' funding mechanisms.[90] There must be a desire and ability to innovate within a terrorist organization in order to affect change. There can at times exist a causal effect between these two phenomena, but they are not always simultaneously present, and as such require qualification. I will explore these desires and abilities which allow innovation in this paper, however, in addition to the issues which de Goede brings up in her book.

Related to de Goede's work is *Illuminating Dark Networks: The Study of Clandestine Groups and Organizations* penned by Luke M. Gerdes.[91] In his book Gerdes explores the nature of terrorist groups as well as other 'clandestine groups' through a lens of social behavior analysis, as he tries to understand how these groups behave and what determines their decision making. Interestingly, within the text, authors Elisa Jayne Bienenstock and Michael Salwen pen a chapter titled "Covert Network Analysis: An Exchange Network Theory Perspective" in which they "question whether the same network metrics can be used to study any social structure regardless of the nature of the relationships" (3).[92] This is to say that Bienenstock and Salwen, in

[90] Merrick M., Yamamoto. *Terrorism Against Democracy: Based in Part on Stansfield Turner's University of Maryland Course, "Terrorism & Democracy"*. Report. Center for International & Security Studies, U. Maryland, 2017. 56-70.
[91] Luke M., Gerdes. *Illuminating Dark Networks: The Study of Clandestine Groups and Organizations*. New York: Cambridge University Press, 2015.
[92] Gerdes, 8

their chapter, explore the feasibility of comparing social groups using network metrics. This sort of study is extremely insightful with respect to my research as it affords me the opportunity of comparing terrorist groups' likelihood of adopting technologies such as cryptocurrencies with other social groups such as states and other variants of armed non-state actors. "Networks, as simplifications of complex sets of relations reveal patterns and provide clarity" (17).[93]

While this approach alone cannot always determine the the ability to compare the structure and design of various groups, it is a 'powerful tool' are doing such work. This is theory that I will use in my research to better understand the steps in the decision-making process for social groups and specifically terrorist organizations. This will also be extremely useful in turning a critical eye not only to the cases which I study in this paper, but also to the very nature of network comparisons in the context of terrorist organizations.[94] How great is the 'terrorist identity' in these groups that allows them to be grouped so freely? Are there distinctive aspects of groups that would make the poor comparative subjects? These are questions that will play a role in the discussion of my cases later in the paper.

Financial Literature

Another area of research that has relevance to my research question is financial cryptocurrency literature, specifically *Protean Power: Exploring the Uncertain and Unexpected in World Politics* edited by Peter J. Katzenstein and Lucia A. Seybert.[95] The chapter focuses specifically on Bitcoin. 'Protean power' as its described in the book illustrates an actor's ability

[93] Gerdes, 17
[94] David, Carslile. "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic." RUSI. March 02, 2017. Accessed November 02, 2018.
[95] Peter J., Kazenstein and Lucia A.. Seybert. Protean Power: Exploring the Uncertain and Unexpected in World Politics. Cambridge: Cambridge University Press, 2018.

to quickly adapt in situations of risk or unpredictability.[96] As de Goede illustrates in her book through the 'finance-security assemblage' of today's world, the basis for protean power is accurate. This is also similar to the notion of terrorist innovation proposed by Ranstrop, Normark, and Dolnik.

Bitcoin, as put by Katzenstein and Seybert, is a "cryptocurrency invented to bypass the political and financial centers of the world" (132).[97] Its genesis, the authors note, was in 2008-2009, a time of great risk and uncertainty given the financial crisis, and was also a prime example of protean power in practice. Much of the analysis of the authors results in the understanding that bitcoin and cryptocurrencies are 'social technologies' that are always evolving, making them difficult to adopt and also difficult to regulate. Its future cannot, at this point, be predicted. Its power to create a 'legitimate' currency outside of the purview of 'state-issued money' however cannot be understated. There is precedent, they state, for these alternative currencies in the form of 'mobile-minutes' in Africa and airline miles in other areas of the world, and so the authors believe the success of this new technology to be imminent.[98]

While Katzenstein and Seybert focus on Bitcoin from the lens of investors on Wall Street, states, and other private sector entities, the authors' analysis of the technology is apt. Much of the risk that companies and individuals face when considering investment in Bitcoin is the same mental process that leaders of terrorist organizations execute when considering the same possibility. Albeit the factors being considered in each case are vastly different, the notion being risk-loving or risk-averse and how that plays a role in the development of Bitcoin and other cryptocurrencies is both fascinating and very relevant to my research. The technology is

[96] Katzenstein and Seybert, 124
[97] Kazenstein and Seybert, 132
[98] "Airtime Is Money." The Economist. January 19, 2013. Accessed November 02, 2018.

ever-changing, which has large implications for my research. The technology is also difficult to regulate and also seemingly destined to succeed, which also speaks to the study I conduct.

Lastly, there have been a number of research papers written about the relationship between cryptocurrencies and ideas such as general governance, state sovereignty, and state economies. In one paper, entitled "The Economics of Cryptocurrencies – Bitcoin and Beyond," the authors examine the economic benefits and detriments of using cryptocurrencies.[99] According to the authors, there is relatively substantial deadweight loss (losses incurred due to economic inefficiencies) in the use of cryptocurrencies, and conclude that "a cryptocurrency works best when the volume of transactions is large relative to the individual transaction size" (1).[100] This finding is important because it suggests that if a terrorist organization adopts a cryptocurrency even partially, then there is incentive for that group to increase its adoption rates in order to combat this deadweight loss.[101] In that way partial adoption, according to this finding, is itself an indicator of potential systematic adoption and simultaneously suggests that sudden adoption should not be expected from terrorist organizations.

Counterterrorism Literature

Finally, the fourth primary category of literature being considered in this paper is that of counterrorism literature. Counterterrorism literature explores the efforts of national governments and agencies being implemented to stymie terrorist initiative. There are subsections of this literature that focus specifically on combating terrorist finance efforts. This literature is

[99] Chiu, Jonathan and Koeppl, Thorsten V., The Economics of Cryptocurrencies – Bitcoin and Beyond (September 1, 2017). Available at SSRN: https://ssrn.com/abstract=3048124 or http://dx.doi.org/10.2139/ssrn.3048124
[100] Ibid
[101] Ibid

interdisciplinary as it includes research and works from similar and related fields such as cyberinfrastructure and cyberterrorism. The primary difference between the fields is focus, however. Counterterrorism literature tends to explore trends and analyze behaviors while the other aforementioned fields tend to focus more on the mechanisms used to conduct terrorist activity. This literature is tied to my research as it will help paint a vivid picture of the counterterrorism regime that is currently in place around the globe, as well as inform many of my hypotheses relating to the state of terrorist funding.

For example, a recent trend that has been occuring in the international system is an expansion of the Islamic State into Southeast Asia - specifically Malaysia and the Philippines.[102] As a result, the Association of Southeast Asian Nations (ASEAN) has ramped up their counterterrorism efforts since their last updates in the post-9/11 era. Many of the group's efforts, however, have been unsuccessful. Successful counterterrorism, as asserted by Marguerite Borelli in her article, requires cooperation between states as terrorism is a transnational phenomenon.[103]

Cooperation between the member states of the ASEAN, countries such as Myanmar, the Philippines, Indonesia, Singapore, and Thailand has been hard to come by. Poor cooperation has led to slow decision making and ineffective enforcement mechanisms which has allows the Islamic State to see great successes in the region.[104] Finally, the ASEAN has had little success combating Southeast Asian terrorist radicalization because few of its counterterrorism efforts are preventative - rather they respond in an ad hoc manner to forthcoming threats. This is the case for most counterterrorism efforts in the international system and especially in the case of illicit

[102] Marguerite, Borelli. "ASEAN Counter-terrorism Weaknesses." *Counter Terrorist Trends and Analyses* 9, no. 9 (2017): 14-20.
[103] Ibid
[104] Ibid

financing means, prevention is critical.[105] The case of the ASEAN is relevant to my research but it exists as microcosm, an example, of a larger issue within the counterterrorism landscape: the lack of preventative counterterrorism options. The speed at which technologies such as cryptocurrencies are developing makes ad-hoc solutions to issues not sustainable. Prevention is the only way to combat such an impending threat. Ultimately the policy implications and recommendations which I cite at the end of my paper in addition to the way I approach the operationalization of my hypotheses will consider this idea thoroughly.

Others have written on terrorist expansion into Southeast Asia as well, such as Ryamizard Ryacudu, author of "Terrorism in Southeast Asia: The Need for Joint Counter-Terrorism Frameworks."[106] In this work Ryacudu contends that affected members of the Southeast Asian community have not been able to "devise joint intelligence mechanisms until the fall of Marawi city to IS in 2017" (2).[107] Lack of cooperation, again, seems to be the primary issue in failed counterterrorism efforts, especially in Southeast Asia.

If a known hotbed for terrorist activity has been able to both exist and thrive in Southeast Asia without being meaningfully disrupted by multilateral action, then more traditional means of terrorist financing are still functioning. If this the case, then risking the adopting a new, volatile technology over continuing to use effective financing methods would seem like an incredibly unwise decision.

Many reports have been written on this issue as well - the findings and focus of these reports tend to cross-cut the schools of thought delineated above. A report, titled

---

[105] Ibid
[106] Ryamizard, Ryacudu. "Terrorism in Southeast Asia: The Need for Joint Counter-Terrorism Frameworks." *Counter Terrorist Trends and Analyses* 10, no. 11 (2018): 1-3.
[107] Ibid

"Cyber-Terrorism Activities Report No. 4" published in the Spring of 2013, outlines a comprehensive timeline of cryptocurrencies that arose from January, 2009 until June, 2013.[108] In addition to discussing some of the earliest transactions and scandals during that time period, the article helps to provide a clear picture of the foundational years of cryptocurrencies and their rates of adoption. Having this early information will be important for my study.

Seperate from the aforementioned schools of thought is the white paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" penned by Satoshi Nakamoto, the purported founder of Bitcoin. This white paper is a foundational text in the realm of cryptocurrency scholarship, and goes into great detail regarding the backend functionality of blockchain technology, and the logic and computer science behind the innovation. Ultimately the white paper describes how technology is able to facilitate this trust-based peer-to-peer cash exchange system. This white paper in forms all of the hypotheses and operationalization choices made for those claims. Nakamoto's white paper also suggests a benchmark of resources and intelligence needed to operate this technology, and this fact will help when discerning adoption prerequisites for terrorist organizations.

From this literature are six hypotheses which embody six independent variables, each of which will be tested against my dependent variable which is represented by differing levels of cryptocurrency adoption in my case studies. My first and third hypotheses stem from the financial literature on cryptocurrencies, which often speaks about the volatility and logistical hurdles which accompany both mining and using cryptocurrencies in the financial sector. This

[108] ICT Cyber Desk. Report. International Institute for Counter-Terrorism (ICT), 2013.

includes general computing power needed to use the technology as well as the value of the technology as it fluctuates over time.

My second hypothesis, regarding ease of liquidity for cryptocurrency technology, is derived from the literature on criminal enterprises and their use of funds. For both criminal enterprises as well as terrorist organizations, liquid funds are crucial for a number of various expenditures. This hypothesis will use that fact to test if it effects the adoption of cryptocurrencies by terrorist organizations.

My fourth and fifth hypotheses, which deal with the effects of group radicalism and group ideology on cryptocurrency adoption. These hypotheses are heavily derived from the terrorist innovation literature which centers around ideology, as authors in this field have made claims of group ideology affecting its ability to innovate in many aspects of an organization.

Finally, my sixth hypothesis explores the current landscape of terrorist financing and how effective it is in the contemporary context. This hypothesis was borne out of literature on the current counter-terrorism financing regime and its efficacy.

Chapter V: Hypotheses and Operationalization

I have identified six potential reasons explaining why terrorist groups may or may not be adopting cryptocurrencies systematically. Each of the hypothesis implies that a terrorist group will try to adopt this technology, and explores the gradient of adoption that exists within the groups. In this paper, my dependent variable is level of cryptocurrency adoption within a terrorist group. As will be discussed further in this section, this 'level of adoption' is being operationalized using an assessment of terrorist operations with cryptocurrency developed by

RAND Corporation. Additionally, the time frame of these hypothesis span to the genesis of Bitcoin. Bitcoin was created in 2009, as stated earlier in the paper, but the earliest adoption point for the technology would not have been expected until 2011, when Silk Road, a black market sales platform, was founded.[109] This was the initial and primary vehicle for Bitcoin transactions in its early years, and put the currency at the center of international attention.

The research in this paper will be conducted via a comparative study. I chose this specific research method for two primary reasons. The first is that given absence of freedom to conduct an experimental design (given geographical limitations and safety risk) a comparative study provides the opportunity to hone in on an issues from a multitude of lenses. Secondly, my question at its essence calls for a study of a single phenomena is different contexts, a circumstance which lends itself perfectly to a comparative case study. Ultimately, for reasons of convenience and beneficence, a comparative case study seemed to be the optimal approach for this research.

First I will layout my hypotheses and both the literature and theory from which they are derived. I will then discuss the operationalization of those hypotheses and introduce a discussion of my dependent and independent variables. I will then explore my three cases of al-Qaeda, Hezbollah, and the Islamic State, juxtaposing each hypothesis against each case. Finally, I will close with a summary of my cases and the outcome of the hypotheses which I tested.

[109] Winston, Ali. "How a Dark Web Drug Ring Was Uncovered After Suspicious A.T.M. Withdrawals." The New York Times. April 16, 2019. Accessed April 20, 2019. https://www.nytimes.com/2019/04/16/nyregion/dark-web-drug-dealing.html.

H1: The higher the level of computing power in a region, the more likely terrorist groups there are to adopt cryptocurrencies.

Many authors writing about the relationship between terrorist groups and cryptocurrency usage, especially Katzenstein, have mentioned the necessity of computing power to properly access the technology. For this reason I have hypothesized that a group needs to have a high level of computer power relative to the global average in order to seriously consider adopting cryptocurrency technology to a great extent. While mining cryptocurrencies requires a massive investment of energy, and often leaves a large carbon footprint, simply using and transacting through the technology requires substantial computer power as well. This will test not only a group's ability to use the currency, but at higher benchmarks produce the currency as well.

To operationalize my first hypothesis I plan to use the ICT Development Index (IDI), a dataset published by a branch of the United Nations which ranks countries based on benchmarks related to information and communication technology. Many of the metrics used in this index are excellent proxies for computing power such as "Percentage of individuals using the Internet" and "International internet bandwidth per Internet user (Bit/s)."

These proxies will allow me to observe if there is a relationship between levels of computing power and the likelihood of cryptocurrency adoption in a given region. This hypothesis may also be conflated with the presence of cryptocurrency technology already in place in a given region. Cryptocurrencies have been used to help developing countries by attacking poverty, access to banks, and job insecurity. It is likely that if this infrastructure is already in place, a terrorist group in the same region will have the computing power needed to adopt the technology.

There are circumstances in which a government may possess greater computing power relative to a terrorist group within its jurisdiction, and through that government a terrorist group is able to access cryptocurrency technology. In this case, that of state-sponsored terrorism, the data compiled regarding computer power from the ICT Development Index would be less revealing. Transnational groups or groups that use lone-wolf attackers also pose risk to this theory. Instances of groups with regional headquarters who fund themselves are more common however, and as such they will be the focus of this study.

H2: The harder it is to convert cryptocurrencies into fiat currencies, the less likely terrorist groups are to adopt cryptocurrencies.

As mentioned earlier, Katzenstein discusses the difficulties in the transference of cryptocurrency to cash. Often times cash is needed to make a transaction, he writes, because cryptocurrencies have not be adopted into society at a full-scale yet, making the currency unusable at many vendors. While a number of companies in the United States and Europe have begun to accept cryptocurrencies, as their technology is far advanced relative to that in Iran and Palestine, other companies have not, making cryptocurrency an inadmissible payment in many transactions. For this reason I hypothesize that having a convenient way to exchange these currencies is needed for a group to adopt the technology to a greater extent.

There are many ways to convert cryptocurrencies into cash. Cryptocurrency exchanges such as Coinbase or Kraken, Bitcoin ATMs, and cryptocurrency wallets are all examples of both physical and online infrastructure that would allow for such a conversion. Conversion apparatuses also exist in some traditional banks. For my second hypothesis I will research the

existence of these institutions in various regions where terrorist organizations are active and observe if a lack of these devices has resulted in a lack of cryptocurrency adoption, or adoption to a lesser extent than other areas.

Additionally, this hypothesis will address the question of goals for terrorist organization. Terrorist groups would pursue cryptocurrency technology, and generally use funds, for two primary purposes. The first is to execute short-term expenditures. This can range from payroll spending to weapon purchases. The second use is often storage and investments. This allows a group's funds to be self-sustaining, similar to the operation of a college or university endowment fund, and it lets the group attain greater ambitions in the future. Both goals rely on being able to convert cryptocurrencies to fiat currencies, but to varying extents. More urgency is placed on this conversion mechanism if a terrorist groups needs to use the funds for short-term expenditures, and it is less urgent in cases of long-term investment planning as the money does not need to be liquid for long stretches of time. This hypothesis will seek account for these different funding goals also analyzing whether groups with either goal are more likely to adopt the technology and observe if there is a pattern.

H3: The more volatile that cryptocurrency prices are, the less likely terrorist organizations are to adopt cryptocurrencies.

Many of the authors mentioned above discussed the volatility of cryptocurrencies in the market, and the effects that a volatile commodity might have within the structure of a terrorist organization. For this reason, and other more intuitive reasons, I hypothesize that groups will be

less likely to adopt the technology if the price of the currency has risen recently, as many of the rises in the currency's history have follow dips in price, creating a volatile price trend.

An analog for this strain of volatility is the volatility observed in global food prices.[110] Trends in this space are similar to cryptocurrencies in their tendency to rise and fall sporadically, with prices generally remaining high and volatile.[111] Global food prices also are subject to a number of extraneous factors like crop yields and petroleum prices just as cryptocurrencies are subject to various legislation and political events.[112] As long as demand is higher than supply, prices will rise as seen in both examples.

To operationalize my third hypothesis I hope to find cases of terrorist organizations using cryptocurrencies to various extents, and map those uses to the market price a given cryptocurrency at that time. If terrorist groups are using cryptocurrencies while their price is in heavy flux, then information can be gleaned regarding how terrorist groups perceive the price volatility of cryptocurrencies as well as the potential bifurcation of risk loving and risk averse terrorist groups.

H4: The more radical terrorist organizations are, the more likely it is for them to adopt cryptocurrencies.

Dolnik, Ranstrop, and Normark all discuss the ideological factors of innovation, as mentioned earlier, and their relative effects on innovation and adoption by terrorist organizations. From their literature on these topics, I hypothesize that the more radical a terrorist group, the

[110] Ghanem, Hafez. "How to Stop the Rise in Food Price Volatility." Carnegie Endowment for International Peace. January 31, 2011. Accessed April 22, 2019. https://carnegieendowment.org/2011/01/13/how-to-stop-rise-in-food-price-volatility-pub-42292.
[111] Ibid
[112] Ibid

more likely they will be to adopt cryptocurrency technology and to a larger scale. The rationale here is that radicalism implies a set of more ambitious goals that a group hopes to achieve. Typically to achieve very ambitious goals, a group will be required to take larger risks to achieve those goals. Consequently, a more radical terrorist group will be more likely to take the risk of adopting cryptocurrency technology.

To operationalize this hypothesis, I plan to use the Global Terrorism Database published by the University of Maryland to look at number of incidents, number of fatalities, and number of injuries for each of the cases being studied in this paper. I will also create conformity in the data by procuring data for each groups number of fatalities and injuries per attack, in an effort to make the results of each group comparable. Time frame is also very relevant for this hypothesis - many groups shift ideologically and strategically over time due to both external and internal pressures. Additionally I will be comparing the data I collect about these groups to global averages which I will calculate in order to put these groups' activities in context of global terrorism trends. Data demonstrating behavior more egregious than the global average will indicate that a group is leaning radical, especially if the data greatly deviates from the means. A group that either matches or falls below these global averages presented will be categorized as more moderate in this paper.

For the purposes of this study, I will look at group behavior between the years 2010 and 2016. I chose this range because there is ample data for this period in time. I also chose it because these years encompass the height of the Islamic State's reign in Syria and Iraq, the genesis (or close to it) of a number of al-Qaeda franchises, and the return of Hezbollah to global relevance in 2012.

H5: The more anti-Western sentiment that exists in a terrorist organization's doctrines, the less likely they are to adopt cryptocurrencies.

Also stemming from research conducted by Dolnik, Ranstrop, and Normark, anti-Western sentiments, they claim, can affect adoption rates of new technology. Technology itself, as well as cryptocurrencies such as Bitcoin, are often associated with the West and Western influence. According to the aforementioned authors, this association can lead a group with anti-Western sentiments to resent and ultimately reject the technology. For this reason I hypothesize that groups with very anti-Western sentiments within their belief system, to the point that they regularly act on their beliefs, will leads to a lower adoption rate of cryptocurrency technology.

For my fifth hypothesis I plan to examine the platforms of these groups as well, specifically regarding their views on the West and Western influences, to determine if there is a correlation between the groups' beliefs about the West and their usage of cryptocurrencies. Cryptocurrencies, and innovation writ large, have often been associated with Western powers and their attempt to gain influence over the globe. There may be a relationship between groups who hold this sentiment closely and those who choose not to adopt cryptocurrencies.

I also hope to explore the propaganda and messaging put out by terrorist organizations preceding a cryptocurrency usage, to determine whether the gradual adoption of this technology has any effect on group messaging, cohesion, or organizational capabilities.

H6: If a terrorist organization's traditional means of financing their operations seem to be operating well, they will be less likely to adopt cryptocurrencies.

While not stemming from any research directly, I hypothesize that while traditional means of terrorist financing are operational and not being impeded greatly by global counter-financing efforts, terrorist groups will be less likely to fully adopt cryptocurrency technologies and instead maintain their current financing apparatuses. This is a null hypothesis of sorts, and also a relatively obvious possibility. There may be no need to innovate at all if the current system of financing is still intact. Examples of phenomena that might force groups to change their financing strategy include updates in counter-terrorism financing policy, violent outbreaks, and economic crisis.

There are issues with this theory, however. For example, a terrorist group's traditional means of financing maybe be operational, but that technique no longer matches the ambitions of the group and as such there is need for an upgrade in financing technology. Additionally, many groups may want to have access to a second, alternative channel of funding even if their funding sources already in place are still working.

Finally, to operationalize traditional means of financing, I plan to look at reports of terrorist group wealth over time as well as assets seized by government or private enterprise operations, and identify trends from which to draw from. These findings should provide some sense of how successful traditional financing mechanisms have been over time, and also of how successful counter-terrorism financing efforts have been.

Furthermore, my universe of cases is comprised of terrorist organizations who are known to have adopted cryptocurrencies to some extent. These groups have either used them once, or

multiple times, to fund operations or carry out an attack. The groups I will examine in this study are Al-Qaeda, The Islamic State, Hamas, Al-Shabab, and Boko Haram. These are a collection of the deadliest and most well-funded terrorist groups in the world.[113] If full adoption of cryptocurrencies is to occur, it logically follows that adoption would be observed in one of these organizations.

Hypotheses	***Independent Variable***	***Dependent Variable***
H1	*Computing power*	*Level of Crypto Adoption*
H2	*Barriers to Currency Conversion*	*Level of Crypto Adoption*
H3	*Price Flux of Crypto*	*Level of Crypto Adoption*
H4	*Level of Radicalism*	*Level of Crypto Adoption*
H5	*Ideological Platform*	*Level of Crypto Adoption*
H6	*Level of Success with Traditional Method*	*Level of Crypto Adoption*

[113] Manheim, David, Patrick Johnston, Josh Baron, and Cynthia Dion-Schwarz. "Are Terrorists Using Cryptocurrencies?" Foreign Affairs. April 21, 2017. Accessed March 02, 2019. https://www.foreignaffairs.com/articles/2017-04-21/are-terrorists-using-cryptocurrencies.

Cryptocurrency Functionalities

1. Mining Cryptocurrency (2)
2. Point-of-Sale transactions (purchases) (2.6)
3. Payment of employees (1.4)
4. Maintenance of illicit enterprises (1.4)
5. Investments (1.8)
6. Private transactions between group members (2)
7. Travel and other operational expenses (1.4)

Lastly, for the purposes of this paper, terrorist organizations will fall on a spectrum of low, medium, and high with respect to their usage of cryptocurrencies. Using the list above as a reference, terrorist organizations who reach a sum value of 1 or lower will be categorized as 'low usage groups'. Terrorist organizations who reach of a sum value between 1 and 2 will be categorized as 'medium usage groups'. Terrorist organizations reach a sum value of over 3 will be categorized as 'high usage groups". The above functionalities each represent a single use of cryptocurrency for an organization. The idea here is that as a terrorist group is found to use cryptocurrencies for another function, that function is added to their sum value which ultimately determines their categorization of cryptocurrency usage.

Furthermore, not all of these functionalities are equal. Paying employees and making important purchases is more valuable to a terrorist group than travel or mining more cryptocurrency. For this reason certain variables are weighted relative to their importance in a terrorist organization. To weight these functionalities, I used a weighting conducted in a book by

the RAND Corporation which looked at similar functions of cryptocurrencies.[114] In this book, functionalities were weighted on a scale of "lesser importance" to "critical importance," in relation to various tasks a terrorist organization may want to carry out. For the purposes of this study, I will average the "importance" of each functionality across all tasks valuing "lesser importance" as a 1 and "critical importance" as a 3. I will then apply the values to each above functionality as closely as possible.

While these functionalities represent neither dependent nor independent variables, they help in the categorization of terrorist organizations which is important for the synthesis of my hypotheses. Regardless of what my hypotheses find, if they cannot connect back to the central question of cryptocurrency usage by terrorist organizations than the information has little significance.

Table 3.1
Assessment of Terrorist Finance Activities with Respect to Cryptocurrency Properties

	Fundraising	Illegal Drug and Arms Trafficking	Remittance and Transfer	Attack Funding	Operational Funding
Anonymity	Moderate importance	Critical importance	Moderate importance	Critical importance	Lesser importance
Usability	Critical importance	Lesser importance	Lesser importance	Lesser importance	Lesser importance
Security	Moderate importance	Critical importance	Critical importance	Critical importance	Critical importance
Acceptance	Lesser importance	Lesser importance	Lesser importance	Moderate importance	Moderate importance
Reliability	Lesser importance	Moderate importance	Critical importance	Critical importance	Moderate importance
Volume	Moderate importance	Lesser importance	Critical importance	Lesser importance	Critical importance

Diagram: Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3026.html. Pp. 34.

[114] Dion-Schwarz, et al. Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats

While not a perfect compartmentalization of terrorist organizations, these categories can also speak to the orientation of particular terrorist organizations towards cryptocurrencies as well. If a group makes use of one function of the technology, it may just be a result of experimentation without any mission attached to the adoption. This usage gradient will correlate to a progression of both frequency and scale of cryptocurrency usage as well. As the use of this technology increases, so does the implied commitment to both the technology and what the technology represents which is also important in the discipline of security studies and armed non-state actors.

Chapter VI: The Current Counter-Terrorism Financing Regime

Currently terrorist organizations primarily rely on three methods of financing in order to carry out their operations.[115] 'Operations' in the broadest sense can range in definition from paying for utilities at a headquarters to purchasing biological weaponry in order to execute an attack. For all of these uses, however, these three central models of funding have seen great success for a number of terrorist organizations including the Islamic State and Al-Qaeda.

The first is charitable donations, which are often contributed in the name of religious orthodoxy. These charities can be real or feigned, and often attract donations on the basis of a pro-Islam agenda, collecting zakat (Islamic tithe) from devout Muslims.[116] Often these 'charities' are simply extensions of criminal enterprises of terrorist organizations, and funds collected through the aforementioned charity will go directly to the controlling group. Other times,

[115] Nikos, Passas. "Hawala and Other Informal Value Transfer Systems: How to Regulate Them?" *Risk Management* 5, no. 2 (2003): 49-59.
[116] Simon, Norton, and Paula Chadderton. *Detect, Disrupt and Deny: Optimising Australia's Counterterrorism Financing System*. Report. Australian Strategic Policy Institute, 2016. 10-17.

individuals will simply donate without the existence of a charity. In the United States, policy has been implemented in the hopes of preventing this tactic such as policy that states "U.S. policy is very clear that no charity can provide money to any organization that may have terrorism as part of their agenda" according to Lee Wolosky, a former government official working on the National Security Council.[117]

The second is illegal commerce. This method of financing can manifest itself the creation of a business (real or fabricated) which is established for the purpose of money laundering. This method of financing can also refer to selling of narcotics, oil, or other contraband.[118] In some of the sources which will be expounded on later, the definition of illegal commerce has expanded to payment in exchange for acts such as kidnapping and murder. While this practice is relatively new as a means of financing terrorist activity, it falls within the category of illegal commerce.

The third is through the hawala system, a trust-based system of transferring funds without the actual conveyance of money. In this system Individual A communicates with his local hawala dealer about a forthcoming transaction.[119] That dealer will then correspond with a fellow hawala dealer in another location, sharing the details of the transaction. The second hawala dealer will fulfill the requisite payment to Individual B, asking for proper compensation from the first hawala dealer once the transaction is complete. Transactions carried out using this system are typically small in value, and as such are kept track of via informal journals and notebooks.

---

[117] Eben, Kaplan. "Tracking Down Terrorist Financing." Council on Foreign Relations. April 4, 2006. Accessed December 21, 2018.
[118] Zachary K., Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. *Terrorist Use of Virtual Currencies Containing the Potential Threat*. Report. Center for a New American Security, 2017. 9-16.
[119] Dulce M., Redin, Reyes Calderón, and Ignacio Ferrero. "Exploring the Ethical Dimension of "Hawala"." *Journal of Business Ethics* 124, no. 2 (2014): 327-37.

This can be very beneficial to terrorists as no transactions and recorded on public ledgers, visible by government agencies and private organizations. This level of anonymity and security (through trust) is very rare - as such it makes sense that the hawala system is such a long-standing and relied-upon institution. Finally, all deals between hawala dealers are completed in property, goods, and cash, keeping in line with the clandestine nature of the transactions.[120]

Governments around the world have been extremely active in their work to stop terrorist financing in the post-9/11 era.[121] Specifically, a number of multilateral organizations have pressured their member states to crackdown on financing channels for terrorist groups.[122] According to a report from the Council on Foreign Relations, this has come in the form of "criminalizing terrorist financing, requiring financial institutions to report suspicious transactions, creating a greater degree of international cooperation in tracking down terrorist financiers, and ratifying the UN convention on financing terrorism, a step that has been taken by 150 countries."[123] These actions are being used to combat illegal commerce as well as donations to fake charities and to disrupt hawala systems.

The current ordering of the counter-terrorism financing regime has been constructed to combat these methods of financing. Spearheaded by organizations such as the Financial Crimes Enforcement Network (FinCEN), a government bureau under the United States Department of the Treasury, and the Financial Action Task Force (FATF), a multinational organization aiming to create policy to combat money laundering, numerous efforts have been implemented since the

[120] Ibid
[121] Ibid
[122] Ibid
[123] Ibid

September 11th attacks. Made up of many sub-organizations and groups, these efforts have been aimed primarily to intercept wire transfers with greater consistency and to limit both imports and exports for commodity-based funding approaches.[124]

In addition to organizations with a focus on combating terrorism financing, many international organizations also play a large role. In fact, Section III, paragraph 8 of the UN Global Counter-Terrorism Strategy, which was adopted in 2006, works to try and encourage "...the International Monetary Fund, the World Bank, the United Nations Office on Drugs and Crime and the International Criminal Police Organization to enhance cooperation with States to help them to comply fully with international norms and obligations to combat money-laundering and the financing of terrorism." Other ancillary organizations that are relevant in the global fight against terrorist financing include the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organization (INTERPOL), and other criminally-oriented groups. [125] Many counter-terrorism financing reforms have been implemented on a global scale as a result of the work of these groups. These reforms include advocating for stronger compliance regulations for commercial transactions in countries, providing training to intelligence agencies on " terrorist financing risks, asset freezing, information sharing and disrupting terrorist financing," and expanding the membership of nations who cooperate with the FATF. The FATF has also made counter-terrorism financing recommendations related to the interception of fund transfers suspected of being tied to terrorist networks.[126]

[124] Gardner, Kathryn L. "Fighting Terrorism the FATF Way." *Global Governance* 13, no. 3 (2007): 325-45.
[125] Kozlowski, Andrzej. "Cross-Border Philanthropy and Counterterrorism Regulations: Guidance for U.S. Grantmakers." PEAK Grantmaking. February 08, 2018. Accessed February 12, 2019.
[126] Ibid

Groups like the FATF, the UNODC, INTERPOL, and FinCEN are only able to do the work which they do, however, due to three pieces of legislation put in place following the attacks on September 11th. The first is Executive Order 13224, an order put in place less than two weeks after the attacks by then President George W. Bush.[127] The order, entitled "Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit, or Support Terrorism," gave the United States government permission to freeze the assets of any persons or organization aiming to assist or interact with any entity connected to terrorist networks. The second piece of legislation, commonly known as the USA PATRIOT Act, allowed for more grave penalties after being charged with working to aid or support terrorist sentiments. The attacks of September 11th upended the practice of counter-terrorism as it was known, and many countries adopted a similar hardening approach to the practice.[128] Finally, two resolutions adopted by the United Nations Security Council, adopted in 1999 and 2001 respectively, have played a large role in the current ordering of the contemporary counter-terrorism regime.

The first is UN Security Council Resolution 1269, published in 1999, which sought to promote international peace by both condemning terrorist attacks at the time of the document's penning as well as encouraging greater state cooperation in the international system. The document was significant is highlighting the importance of counterterrorism efforts around the globe, and its effects have been borne out in many of the counterterror measures being implemented by states today. The second UN Security Council Resolution which more directly tied to the attacks of September 11th is resolution 1368 which was adopted the the day following the attacks. Resolution 1368 builds on the sentiments of 1269 in its call for international

[127] Ibid
[128] Ibid

cooperation and action against terrorist threats. Citing the 1999 resolution, 1368 calls for international action, a call for those countries to "redouble their efforts to prevent and suppress terrorist acts…" Both resolution 1269 and resolution 1368 have played major roles in the shaping the conversation around counterterrorism measures on the global stage. Counterterrorism policy has a long and legacied history in the United States and the state of the current counter-terrorism regime is very much predicated on historical developments in the international arena.

Similar to the changes that occured in United States foreign policy post-9/11 which resulted in a new regulatory regime to crack down on terrorist financing, there is a history of precedent for the regulation of cryptocurrencies specifically as well. Central to many of the legislative efforts aimed at regulating the cryptocurrency landscape is the Howey Test, which defines what constitutes a "security."[129] The test, named after the 1946 Supreme Court case *SEC v. W. J. Howey Co.*, is used to determine whether assets which do not look like a traditional security can be legally deemed as a security for regulatory purposes. A security is a financial tool that has inherent value, and can be traded between two or more entities.[130] Common examples of securities are common stocks, bonds, and futures. Resulting from the decision of the case, the test sets out a tripartite criteria for what constitutes a security. First, there must be an investment of money. Second, the investment must be made with an expectation of future profits. Finally, these future profits must have an expected derivation from the efforts of a third party.[131]

This test provides legislators and regulatory bodies both discretion and flexibility in their capacity to crack down on malicious financial activity. If a regulatory body is able to

---

[129] Van Valkenburgh, Peter. *Framework for Securities Regulation of Cryptocurrencies*. Washington D.C.: Coin Center, 2018. February, 2019. https://coincenter.org/files/securities-cryptocurrency-framework-v2.1.pdf
[130] Kenton, Will. "Security." Investopedia. December 13, 2018. Accessed March 02, 2019. https://www.investopedia.com/terms/s/security.asp.
[131] Van Valkenburgh, *Framework for Securities Regulation of Cryptocurrencies*.

characterize the purchase or exchange of cryptocurrencies as the purchase or exchange of a security, it will be able to legally intervene. This is important because many of the primary duties of the United States Securities and Exchange Commission (SEC) revolve around enforcing federal security laws, and more generally regulating the securities industry. As cryptocurrencies become more ubiquitous, the SEC will likely turn to the Howey Test as a tool to have greater regulatory capabilities in the future.

A robust approach to counter-terrorism financing has not necessarily resulted in success however. In Peter R. Neumann's 2017 *Foreign Affairs* article "Don't Follow the Money The Problem With the War on Terrorist Financing," Neumann states that "In 2015, for example, the self-proclaimed Islamic State (also known as ISIS) had a budget of up to $1.7 billion, according to a study by King's College London and the accounting company Ernst & Young, making it the world's richest terrorist group. That same year, the total amount of all frozen terrorist assets amounted to less than $60 million. Only three countries—Israel, Saudi Arabia, and the United States—had seized more than $1 million." Through illicit commerce, donations, and other forms of funding, terrorist groups have been growing richer over the past forty years while global counter-terrorism financing efforts to mitigate this funding have been mediocre at best. As these organizations continue to play catch-up with terrorist funding mechanisms, the potential exists for terrorist groups to take advantage of the situation and innovate so to further avoid regulatory apparatuses.

Chapter VII: Cases

For my cases, I decided to observe the behavior of al Qaeda, the Islamic State (ISIS), and Hezbollah. I chose these cases for two main reasons. The first is that each of these groups has been reported to have used cryptocurrency technology, which itself is cause to include as cases. Second, these three groups were observed in a recent study conducted by RAND Corporation entitled *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*.[132] The book describes these groups as in need of "anonymous, secure, and ready streams of funding," (xii) and claims that, while the missions of each group are varied, their need for these funding streams unites them as cases for a study such as this one. There does exist some selection bias here, as these groups require large amounts of funding relative to many other, smaller, terrorist organizations around the world. This, however, is another reason for the selection of these three cases: it will be helpful for my sample of cases to contain these group groups because they are some of the biggest, most ambitious and visible terrorist groups on the planet with abundant public data about their movements. For a study of a technology that is still new and burgeoning, it will be helpful to explore groups that facilitate research and inquiry due to their public nature.

Against each of these cases I will test the six independent variables I have outlined as part of my hypotheses. I will the aggregate the results of each test in order to determine which of the original hypotheses, and in turn independent variables, have legs as potential explanations for the varied adoption rates of cryptocurrency technology by the aforementioned organizations. Based on my findings, I plan to posit policy recommendations for how to best combat the advent of cryptocurrencies as a terrorist capability.

[132] Dion-Schwarz, et al. Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats

Case 1: Al Qaeda

Before the attacks on September 11th, 2001, al Qaeda derived most of their funds through charitable donations, oftens transferred via a hawala system.[133] After the attacks took place, however, the group was forced to innovate, as their "market share" was jeopardized by successful counter-financing efforts by the United States and its allies. Al Qaeda proper began to move into the criminal enterprise business discussed by Shelley earlier. The group's affiliates in Somalia also adapted, creating "the most diversified and innovative funding method, a combination of taxes and checkpoint fees, diaspora remittances, and a charcoal trade-based money laundering scheme" according to Juan C. Zarate in his book *Treasury's War: The Unleashing of a New Era of Financial Warfare*.[134]

This innovation has carried over until today where al Qaeda and affiliates of the terrorist group have been reported to have used or attempted to use cryptocurrency technology to raise funds for the group's fighters.[135] Like the other cases which will be examined in this study, however, al-Qaeda has yet to fully adopt cryptocurrency technology into its infrastructure. Full adoption would take the form of cryptocurrencies being used at the same rate as traditional means of financing such as the hawala system and donations.[136] Cryptocurrency usage would have to equal the usage of those techniques both in scale and magnitude of money being transacted. Based on reports of al-Qaeda's dealings with cryptocurrency technology, the group

[133] Ibid
[134] Juan C. Zarate, "Learning Curve," in Treasury's War: The Unleashing of a New Era of Financial Warfare, New York: Public Affairs, Perseus Book Group, 2013, pp.362–363.
[135] Baydakova, Anna. "Crypto Use A 'Fringe Activity' Among Terrorists, Says Think Tank." CoinDesk. September 11, 2018. Accessed April 03, 2019.
https://www.coindesk.com/crypto-use-is-a-fringe-activity-among-terrorists-says-think-tank.
[136] Ibid

would be categorized as a moderate-usage group, as it has only been reported to have used the currency to pay its fighters.[137]

The dependent variable for this case is the group's low-usage rate of cryptocurrency technology. Against this variable we will test each of the six independent variables listed earlier to determine which of these potential reasons would explain the groups' moderate-usage rate of the technology.

The first independent variable is the measure of computing power where al-Qaeda resides. For the purposes of this study, I will use Afghanistan as the testing destination for computing power, as that is the home for al-Qaeda's base network, as would most likely be the location of the largest and most important transactions. There are other terrorist groups and violent organizations in Afghanistan, but given the nature of the study - exploring the nation's computing power - allows the data to be relevant to al-Qaeda as well as other groups in the region such as the Taliban. According to the ICT Development Index, an index which ranks countries based on information and communication technology metrics. Afghanistan ranks 159th in the world on the ICT Index, with a rank of 1.95.[138]

Furthermore, the index states that in Afghanistan, as of 2017, only 4.8% of households have internet access, with less than 3.5% of households in the country even having a computer. Finally, according to the index, the average international internet bandwidth per internet user is 11966.64 (Bit/s) or bits (units of information) processed per unit of time.[139] For reference, the country that mined the most Bitcoin in 2017 was China, and at that time they possessed an

[137] Ibid
[138]"2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&AFG.
[139] Ibid

average international internet bandwidth per internet user of 4906022.95 (Bit/s).[140] Iceland is also a well-known destination for Bitcoin mining, and they topped the 2017 ICT Index with an average international internet bandwidth per internet user of 997829.92, over 83 times that of Afghanistan at the same time.[141] This hypothesis is supported because the group's use of cryptocurrencies align with its very low national computer power, and general access to basic computing requirements. These levels of computing power are much too low to mine cryptocurrency reliably, and in many areas most likely to low to easily use cryptocurrencies for other purposes.

The second independent variable relates to restrictions on currency conversion, in this instance in Afghanistan. According to coinatmradar.com, there are currently 4626 Bitcoin ATMs in the world, spanning across 78 countries.[142] Numbers for other ATM services are not very public, especially those that are relatively new in the cryptocurrency scene and only have a few in place. According the website, of the 4626 Bitcoin ATMs around the world, none exist in Afghanistan, and only two exist in the Middle East, specifically Saudi Arabia.[143] This lack of infrastructure to easily turn cryptocurrency into cash while subverting traditional banking mechanisms is potentially a large deterrent to adopting the technology on a larger scale. In addition to a dearth of easy ways to convert cryptocurrencies to fiat currencies, the presence of an ATM itself is at odds with the anonymous benefits of the technology. Without both easy and

[140] "2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&HKG
[141] "2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&ISL
[142] "Bitcoin ATM Map – Find Bitcoin ATM, Online Rates." – Find Bitcoin ATM, Online Rates. Accessed April 20, 2019. https://coinatmradar.com/.
[143] Ibid

secure ways to convert cryptocurrencies, such as in this case, groups will not be very likely to adopt the technology.

The third independent variable discusses cryptocurrency price volatility in relation to adoption frequency within terrorist organizations, in this case al-Qaeda. To test this, we will match reported uses of cryptocurrencies by al-Qaeda to the technologies price at the time of the usage to see if price of the currency affected usage rate. The most notable reported usage of the technology by al-Qaeda occurred January 7th, 2015 with the attacks on the offices of newspaper Charlie Hebdo in Paris.[144] On January 1st of that year, Bitcoin was priced at $383.[145] This marked over a 65% decrease in the technology's price from January 1st of the prior year, when the technology was priced at $1099.04.[146] This behavior demonstrates buying practices connected to volatility because the group bought in at a time when the currency had not undergone massive price flux - the price had been relatively stable and presumably safe to invest in. If the price had undergone more radical shifts in price during the time preceding al-Qaeda's use of the technology, the group may not have found it wise to invest.

[144] Steven, "Terrorists Have Been Using Bitcoin for Four Years…"
[145] "Bitcoin Historical Price & Events" https://99bitcoins.com/price-chart-history/
[146] Ibid

Diagram: https://99bitcoins.com/price-chart-history/

It also marked a valley in the technology's price, as Bitcoin skyrocketed to nearly $20,000 three years later.[147] While the group could not have, and most likely did not predict the price of the technology in the coming months and years, it is probable that they noticed the price of the technology decline such that investing in it would not be as risky after it fell.

The fourth independent variable tackles the issue of varying levels of radicalism within terrorist organizations and their ties to potential cryptocurrency adoption. In the case of al-Qaeda, the total number of incidents carried out by the group between 2010 (a significant year for United States counterterrorism operations in response to increase al-Qaeda activity around the globe) and 2016, as well as the average number of deaths and injuries resulting from these attacks, will be compared to global averages in that same time frame and examined as a measure

[147] Ibid

of radicalism within al-Qaeda. Due to the franchised and transnational nature of al-Qaeda, I have aggregated data from al-Qaeda in the Islamic Maghreb (AQIM), al-Qaeda in the Arabian Peninsula (AQAP), and al-Shabaab as a representative sampling for the operationalization of this hypothesis.[148] Between 2010 (a year near the inception of many of the al-Qaeda franchises) and 2016 al-Qaeda (specifically the three aforementioned franchises) carried out 3815 attacks, totalling 16,459 deaths and 11,302 injuries.[149] These numbers are equivalent to 4.3 deaths per attack, slightly less than twice the 2.4 global average in that time frame, and 2.9 injuries per attack.[150] Relative to the Islamic State, as will be presented later, these numbers are relatively low. However compared to the global average, and to Hezbollah, these numbers are very high.

It is important to note here that the activities of al-Shabaab greatly propped up these statistics, as the number of incidents carried out by al-Shabaab was 223% greater than the incidents conducted by AQIM and AQAP combined.[151] Furthermore, the group's fatalities nearly doubled the that of AQIM and AQAP put together, and their injury numbers were higher than the aggregate of the other two groups as well.[152]

Ultimately, this hypothesis does not work in the case of al-Qaeda, as the radicalism demonstrated by the aforementioned injury and fatality numbers do not match the group's current adoption levels of cryptocurrencies. Perhaps, although the benefits of cryptocurrencies for transnational terrorist groups are great, the logistical hurdles of adopting this sort of

[148] Fishman, Brian. "Using the Mistakes of Al Qaeda's Franchises to Undermine Its Strategies." The Annals of the American Academy of Political and Social Science 618 (2008): 46-54. http://www.jstor.org/stable/40375774.
[149] National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). Global Terrorism Database [Perpetrators: AQIM, AQAP, Al-Shabaab]. Retrieved from https://www.start.umd.edu/gtd
[150] Roser, Max, Mohamed Nagdy, and Hannah Ritchie. "Terrorism." Our World in Data. July 28, 2013. Accessed April 20, 2019. https://ourworldindata.org/terrorism.
[151] Ibid
[152] Ibid

technology across such differently performing franchises makes the technology more difficult to implement.

The fifth independent variable deals with anti-Western sentiments held by terrorist organizations and their effects on adoption of cryptocurrency technology. In this case, messaging and propaganda put out by al-Qaeda affiliated media sources will be examined to determine how much anti-Western sentiment is a part of the group's ideology. Al-Qaeda's messaging and mission for a long time has been to destroy the West, especially after the global retaliation against the group after the September 11th attacks.[153] Recently, however, the group has not done much in the way of aggression towards the global hegemon.[154] The only attack of recent on Western soil by al-Qaeda was the 2015 Charlie Hebdo attacks. This is a drastic decline from the previous number of attacks and fatalities wrought by the group.[155] In this way, al-Qaeda can be viewed as a group with a low amount of anti-Western sentiment, which according to the fifth hypothesis, would explain its low cryptocurrency usage.

The sixth independent variable explores the current, traditional methods of financing used by al-Qaeda and their current success. If their current success is not very high, then they can be expected to adopt cryptocurrency technology to a great extent. If their current levels of success are high, then the risky adoption of cryptocurrencies is less likely. Despite global efforts to combat terrorist financing operations, specifically within the al-Qaeda network, the group has still been able to accrue funds and resources. In 2017 Qatar was accused of aiding, funding, and

[153] Hamming, Tore Refslund. "With Islamic State in Decline, What's Al-Qaeda's Next Move?" War on the Rocks. April 27, 2018. Accessed April 03, 2019. https://warontherocks.com/2018/04/with-islamic-state-in-decline-whats-al-qaedas-next-move/.
[154] Ibid
[155] Ibid

housing members of terrorist organizations such as al-Qaeda, ISIS, and Hamas.[156] It was also recently reported that £80 million of British taxpayer money has been channeled to al-Qaeda over the past twenty years through a British gang with connections to the group's members.[157] Al-Qaeda has been able to receive funds through its traditional means of money laundering, zakat donations, and even state-sponsored monetary aid. This fact supports the sixth hypothesis in that al-Qaeda's traditional means of financing work well, making a transition to a riskier currency less appealing.

In the case of al-Qaeda, every hypothesis fit the case. The group is in a region with very poor computing power and essentially no Bitcoin ATMs in the vicinity. The group also made a price-conscious decision to invest in the currency for a one-time attack while it was at its price valley, and has presented a fairly moderate Western stance, especially in the age of the Islamic State. Finally, the group's traditional methods of financing their operations have persisted through global efforts to combat the group's financing endeavors, making the switch to cryptocurrency technology less appealing. For these reasons it makes sense that the group is registered as a low-usage entity of the technology.

Case 2: Hezbollah

Hezbollah, a terrorist group based in Lebanon, has historically received a large amount of its funding from state-sponsored entities such as the Iranian and Venezuelan governments. It is important to note that the contributions of these governments, historically, have not been equal,

[156]Press Release - March 28, 2019. "Qatar: Extremism & Counter-Extremism." Counter Extremism Project. January 02, 2018. Accessed April 03, 2019. https://www.counterextremism.com/countries/qatar.
[157] Williams, Sara Elizabeth. "£80m of British Taxpayers' Money 'funnelled to Al-Qaeda' in Decades-long Scam." The Telegraph. March 31, 2019. Accessed April 03, 2019. https://www.telegraph.co.uk/news/2019/03/31/80m-british-taxpayers-money-funnelled-al-qaeda-decades-long/.

with Iran providing much greater support to Hezbollah in the past than Venezuela, who have played a 'sympathizer' role to the organization.[158] This is due to an alignment of mission, especially with respect to their campaign against the neighboring Israel. After Iran was burdened with sanctions following President Trump's withdrawal from the Joint Comprehensive Plan of Action in 2018, and the sanctions which existed before the plan was put in place in 2015, that funding declined dramatically.[159] Additionally, Venezuela's oil troubles and dramatically high inflation rates have also affected the country's ability to provide monetary aid to the terrorist group.[160] As a result Hezbollah was forced to innovate with respect to their funding mechanisms, adopting illicit commerce vehicles, money laundering, and criminal enterprises.

Hezbollah, like it's anti-Israeli counterpart Hamas, have been reported to be using cryptocurrencies in the as recent as 2018.[161] Given their status as a state-sponsored terrorist organization, it follows that the group has received its cryptocurrency funding and education at least partially through the Iranian government, who has been reported to be using and creating cryptocurrencies within its borders.[162]

Additionally, Hezbollah is one of the most transnational terrorist organizations in the world, spanning both countries and continents with its reach.[163] Because of this, it is probable that the group will adopt cryptocurrencies to a substantial extent soon, relative to other groups,

---

[158] Clarke, Colin P. "Hezbollah Is in Venezuela to Stay." Foreign Policy. February 09, 2019. Accessed April 18, 2019. https://foreignpolicy.com/2019/02/09/hezbollah-is-in-venezuela-to-stay/.
[159] "Iran Nuclear Deal: Trump Pulls US out in Break with Europe Allies." BBC News. May 09, 2018. Accessed April 18, 2019. https://www.bbc.com/news/world-us-canada-44045957.
[160] Scott, Heather, and Agence France-Presse. "What Does 10,000,000 Percent Inflation Look Like? See Venezuela." ABS. October 09, 2018. Accessed April 18, 2019. https://news.abs-cbn.com/business/10/09/18/what-does-10000000-percent-inflation-look-like-see-venezuela.
[161] Jetencila. "Hamas Turns to Bitcoin (BTC) to Fund Its Terror Activities • Live Bitcoin News." Live Bitcoin News. February 04, 2019. Accessed April 03, 2019. https://www.livebitcoinnews.com/hamas-turns-to-bitcoin-btc-to-fund-its-terror-activities/.
[162] Dion-Schwarz, et al. Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats
[163] Ibid

and as such makes the group an interesting case study. While relative to al-Qaeda and the Islamic State, Hezbollah is a relatively low user of the technology today, the group has a larger potential of using cryptocurrencies to a great scale in the coming years. Its use of the technology is less of a threat today, and more of an impending threat in the future.[164]

According to reports, their usage of the technology has been primarily for storage as opposed to operational use.[165] Like al-Qaeda, however, the group is very far from adopting the currency to a more systematic level. As such, the group will be categorized as a moderate-usage group the same as al-Qaeda, since their primary use of the technology has simply been storage and investments, putting the group's value at a 1.8. This moderate-usage will be tested against all six of my hypotheses to see which fit the case of Hezbollah.

For reference, it was recently reported that Hamas, a terrorist group based in Palestine which controls the Gaza Strip, initiated a Bitcoin campaign in January of 2019.[166] Discussion of Hamas is relevant because, while it is not a case being studied, it does dwell in a similar region to groups being studied in this paper, and can provide additional context and information for my examination of those groups. The group raised a few thousand dollars in their first round of donations, and is working to improve their profits in the coming months, learning more about the technology and expanding their reach.[167] The group has begun to teach its supporters about its uses and benefits as well, as it works to expand its technological capacity. A much weaker entity

[164] Ibid
[165] Ibid
[166] Fanusie, Yaya J. "Jihadists Upping Their Bitcoin Game." FDD. April 01, 2019. Accessed April 03, 2019. https://www.fdd.org/analysis/2019/03/29/jihadists-upping-their-bitcoin-game/.
[167] Ibid

than Hezbollah, Hamas' foray into the cryptocurrency space has been very impressive, and as such their success might affect Hezbollah's in the coming years.[168]

The first hypothesis, related to the computing power of the Hezbollah and in turn their capabilities with respect to mining cryptocurrencies, is very revealing about the organization's future in the cryptocurrency space. The ICT Development Index ranks Hezbollah 64th in the world with an ICT Index rating of 6.30.[169] This is a large jump from Afghanistan's 165th ranking, and speaks to the difference in cryptocurrency exposure between the two groups. According to the ICT Index, 77.7% of households in Lebanon have internet access, and an even larger 78.09% of households in Lebanon have a computer.[170] Furthermore, the international internet bandwidth per internet user in Lebanon is 55086.32 (Bits/s), a much larger processing rate than that of Afghanistan in 2017 which was 11966.64 (Bit/s).[171] This finding fits the hypothesis that greater computing power leads to a greater chance of adopting cryptocurrencies on a larger scale, as Hezbollah's forays into the crypto space have mirrored that of Hamas while dwarfing that of al-Qaeda thus far.

The second hypothesis pertains to Lebanon's infrastructure with respect to cryptocurrencies, and ease of exchanging cryptocurrencies for fiat currencies in the country where Hezbollah resides. According to coinatmradar.com, there are no Bitcoin ATMs in either Lebanon or Palestine, making turning cryptocurrencies into fiat currencies very difficult.[172] Perhaps, given Hezbollah's relationship with Saudi Arabia, and the presence of Bitcoin ATMs in

---

[168] Ibid
[169] "2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&LBN
[170] Ibid
[171] Ibid
[172] "Bitcoin ATM Map – Find Bitcoin ATM, Online Rates." – Find Bitcoin ATM, Online Rates. Accessed April 20, 2019. https://coinatmradar.com/.

Saudi Arabia, these exchanges might be slightly easier. Nonetheless, the lack of facilitating infrastructure for cryptocurrency exchange, in tandem with Hezbollah's relatively advanced entry into the crypto space, speaks to the waning significance of these machines in a country. For reference, Iceland, which in 2017 according to the ICT Development Index had the highest computing power and greater percentage of their population connected to the internet, only had one Bitcoin ATM in its territory.[173]

The third hypothesis speaks to the volatility of cryptocurrency prices and its relationship to instances of usage of the technology. In February of 2018, near the time that Venezuela announced the creation of the 'Petro,' Hezbollah was reported to have used cryptocurrencies to store funds for the group's operations.[174] The report was that the storage was very small in scale, and Venezuela's move to its own, commodity-backed cryptocurrency would allow the country to more readily aid Hezbollah in the future.[175] However, the simultaneous timing of the United States President Donald Trump backing out of the Joint Comprehensive Plan of Action with Iran made the move to crypto relatively appealing.[176] In February of 2018, Bitcoin was worth just over $17,000. At this time, the price of Bitcoin was reaching its peak. Individuals and conglomerate entities were still buying into the technology, however, as the pricing mechanism had become bubble, with people buying into the technology for the sole purpose of not missing out on potential profits in the long-run. Nonetheless, Hezbollah buying in at such an unsure time for the technology means that the hypothesis does not fit this case.

---

[173] "2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&ISL

[174] Floyd, David. "Venezuela's Petro Isn't Oil-Backed. It's Not Even a Cryptocurrency (Opinion)." Investopedia. March 12, 2019. Accessed April 03, 2019. https://www.investopedia.com/news/venezuela-petro-not-cryptocurrency/.

[175] Ibid

[176] Ibid

Diagram: https://99bitcoins.com/price-chart-history/

The fourth independent variable examines the level of radicalism of terrorist groups and its relevance to the conversation of adopting cryptocurrency technologies. To determine this level of radicalism, it is helpful to examine records displaying the number of terrorist incident perpetrated by Hezbollah between 2010 (near the time of its resurgence to relevance) and 2016. Between 2010 and 2016, Hezbollah reportedly participated in the execution of 35 terrorist attacks.[177] Of those attacks, an average of one person died per attack, and an average of 2.1 individuals were injured per attack.[178] For reference, the global average for fatalities as a result of a terrorist attack between 2010 and 2016 was 2.1. In the span that 75,915 terrorist attacks were perpetrated between 2010 and 2016, Hezbollah only committed 35.[179] And whereas 172,057 fatalities were attributed to terrorist attacks around the globe in the time frame, on 35 were a result of Hezbollah's actions.[180] Hezbollah, relative to the average performance of terrorist

[177] National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). Global Terrorism Database [Perpetrators: Hezbollah]. Retrieved from https://www.start.umd.edu/gtd
[178] Roser, et al. "Terrorism."
[179] Ibid
[180] Ibid

groups with respect to deaths and injuries, is not a very radical group. As such, this hypothesis makes sense. Hezbollah is a prime candidate for future adoption of cryptocurrencies, but their adoption to this point has not been significant, which matches their level of radicalism relative to global norms between 2010 and 2016.

The fifth hypothesis explores the ideological platform of Hezbollah, and more specifically the presence of anti-Western rhetoric and actions within the group's core mission. While Hezbollah is heavily affiliated with Iran and their political agenda, Hezbollah itself has not recently conducted any attacks on Western soil.[181] Additionally, its anti-Israeli platform has seemed to take precedent in the group's recent messaging over its anti-Western sentiments.[182] In this way, the fifth hypothesis does fit this case, as Hezbollah's cryptocurrency usage aligns with its relatively moderate stance towards the West. Were the case of Hezbollah not to fit this hypothesis, it would have a much more hostile stance towards the West, and perhaps would have claimed responsibility for a number of the attacks carried out in the region over the last half-decade.

The sixth hypothesis tackles the question of traditional financing methods within the Hezbollah financial infrastructure. Hezbollah has had great success with their traditional means of financing as of recent. Venezuelan moves to reboot their economy, Iran's own use of cryptocurrency to create more economic autonomy within the state, and recent partnerships with Sunni groups in the Middle East have all helped the terrorist group sustain itself.[183] Granted, some of these partnerships and shifts in economic autonomy are a result of the current

[181] Katz, Brian. "Will Hezbollah's Rise Be Its Downfall?" Foreign Affairs. March 08, 2019. Accessed April 03, 2019. https://www.foreignaffairs.com/articles/israel/2019-03-08/will-hezbollahs-rise-be-its-downfall.
[182] Ibid
[183] Dion-Schwarz, et al. Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats

counter-terrorism finance regime that is in place, the effects they have had on Hezbollah economic strategy are fascinating all the same. This hypothesis seems to fit the case of Hezbollah as the group's use of cryptocurrency technology seems to scale with the relative success of financing intervention put in place by groups like the Financial Action Task Force (FATF).[184] As counter-terrorism financing success increases, so will Hezbollah's innovation rates as they seek to maintain their group's integrity by finding alternative funding sources in the vicinity.

Ultimately, only three of the hypotheses laid out at the outset of the case section fit the case of Hezbollah and their relatively high cryptocurrency usage compared to al-Qaeda. Despite being both "moderate-usage" groups, the value for Hezbollah's usage is higher than that of al-Qaeda, and reports seem to take their usage of the technology more seriously than al-Qaeda's. This may be influenced by Hamas' rampant use and development of cryptocurrencies in Palestine, and the relationship between Hamas and Hezbollah, but the results of the study are still significant.

It seems that level of computing power, ideological platform, and efficacy of traditional financing methods are the most significant factors in determining whether a terrorist organization will ultimately adopt the technology. Both al-Qaeda and Hezbollah have behaved according to each of these hypotheses. Higher computing power has resulted in higher cryptocurrency usage, moderate anti-Western sentiments have led to moderate adoption of the technology, and functional traditional methods of terrorist financing have led to a tempered adoption of newer, more risky technologies such as cryptocurrencies.

[184] Ibid

Case 3: The Islamic State

The Islamic State, like many terrorist organizations, has historically funded itself for much of its existence.[185] Having learned from its predecessor in al-Qaeda, the Islamic State has traditionally focused on an economic model similar to that of a state. It purchased and sold both goods and oil at an impressive rate in order to generate funds.[186] The Islamic State also used robust tax regimes within civil systems to fund their expansion, taxing agricultural products and other goods.[187] Funds generated by garbage collection and motor vehicle transportation in Iraq and Syria, while not taxes, were collected for the group as well. Water, electricity, and income were all taxed to high rates (10% in the case of income taxes), even charging vendors exorbitant rates to set up stalls at central marketplaces.[188] Cryptocurrencies would have made these financing tactics more centralized, having payments come through a single system as opposed to multiple, poorly tracked interactions. For a group with such diversified funding channels, a single payment platform through which to operate anonymously would beneficial for all parties involved.

While the group's expansion plans have all but ceased after the recent crackdown on the group by multi-national counterterrorism initiatives, cryptocurrencies will serve important functions for the group on digital platforms as well.[189] As the Islamic States moves to relying more heavily on lone-wolf actors operating in a number of countries, being in possession of a

[185] Terrill, W. Andrew. Report. Strategic Studies Institute, US Army War College, 2017. http://www.jstor.org/stable/resrep11436.
[186] Ibid
[187] Perper, Rosie. "ISIS Made Millions from Taxes That It Then Used to Run Garbage Collections and Even a DMV." Business Insider. April 06, 2018. Accessed April 18, 2019. https://www.businessinsider.com/islamic-state-used-taxes-to-grow-power-and-offer-services-2018-4.
[188] Ibid
[189] Ibid

means by which the Islamic State can transfer funds across national borders anonymously is incredibly valuable.

The group's focus on physical expansion played to its benefit after 2013, allowing the group to expand in power and influence. The group conquered and maintained land throughout the Middle East for years.[190] This approach to funding was checked however by great powers like the United States in 2017 and 2018. A unified global effort to combat the Islamic State and its violence revealed shortcomings in the Islamic State's strategy. Physical expansion made the group vulnerable to military might, a commodity which the United States, France, Britain, and many other countries have in great abundance.[191] Additionally, as the Islamic State continued to expand, its financial and operational needs grew with it, creating multiple pain points for the organization which were taken advantage of by counterterrorism initiatives.[192]

Now the Islamic State is in financial turmoil.[193] Their physical expansion has been readily stopped, and the group has been reduced to extremely small, disparate factions - territory which is many times smaller than the pseudo-empire it once used to rule.[194] The group has also made enemies with many other terrorist organizations in the region, like al-Qaeda and Hezbollah, which makes proximity trading and general tradecraft among terrorist organizations increasingly difficult.[195] It seems as though the Islamic State is primed to adopt cryptocurrency technology,

[190] Gunaratna, Rohan. "Global Threat Forecast The Rise of ISIS." *Counter Terrorist Trends and Analyses* 8, no. 1 (2015): 6-11. http://www.jstor.org/stable/26369557.
[191] Ibid
[192] Ibid
[193] Sherlock, Ruth. "U.S.-Backed Forces Declare Defeat Of ISIS 'Caliphate'." NPR. March 23, 2019. Accessed April 20, 2019. https://www.npr.org/2019/03/23/706147761/u-s-backed-forces-declare-defeat-of-isis-caliphate.
[194] Ibid
[195] Ibid

but only testing the various independent hypotheses will show if it is a plausible eventuality for the group.

The Islamic State is arguably the largest user of cryptocurrency technology of the cases being examined in this study.[196] The Islamic State has reportedly used both Bitcoin and Zcash, an "altcoin" which, while similar to Bitcoin, purportedly has greater privacy and security features attached to the currency.[197] Because Bitcoin is an open source platform, meaning that its algorithms are public information, many individuals and groups have developed the technology - sometimes getting rid of the consensus trait of proof-of-work, and other times building a new cryptocurrency altogether. The coins are also much less energy-intensive than Bitcoin with respect to mining and general functionality, making them more appealing to many groups.[198] The group has used these currencies to purchase website domains, transfer funds between the group's members, lone-wolf attacks, and travel expenses.[199]

Consequently, the group would be categorized as a high-useage group with a value of at least 6 based on the functionalities weights listed in the previous chapter. This value speaks to the extensive nature of the group's usage of cryptocurrency (frequency of use) as well as the significance of the use and how that use might reflect future ambitions of the group. Now the group will be tested up against each independent variable to observe if the patterns witnessed with the prior two cases stay consistent in the case of the Islamic State.

---

[196] Canellis, David. "Europol: Criminals Are Still Using Bitcoin, but ISIS Loves Zcash." Hard Fork | The Next Web. September 21, 2018. Accessed April 03, 2019. https://thenextweb.com/hardfork/2018/09/19/europol-cryptocurrency-cybercrime/.
[197] Ibid
[198] Ibid
[199] Ibid

With respect to the first hypothesis, Syria will be used as the country which represents the Islamic State, as Syria is the group's home country and base. While there are other groups in this region that are not the Islamic State, this information about Syria will provide a blanket set of statistics through which many groups can be analyzed. This includes the Islamic State, as well as Hayat Tahrir al-Sham. Here, the issue of transnational groups comes up again, as testing an organization known for its transnational tendencies make the findings of this particular hypothesis difficult to extrapolate. According to the ICT Development Index, Syria is ranked 126th in the world with an ICT Index rating of 3.34.[200] This sits in the middle of Afghanistan's startlingly low rating and Lebanon's surprisingly high ICT Development Index rating mentioned earlier in this section. Regarding the specifics of Syria's ranking, according to the index 43.62% of households in Syria have internet access, and 49.90% of households in Syria have computers in their homes.[201] Additionally, the international internet bandwidth per internet user in Syria is 12813.18 (Bit/s). These numbers are incredibly surprising at first glance.

As mentioned earlier, for a group known to be the most active users of cryptocurrencies of the terrorist organizations currently in the space, the numbers presented by the Islamic State in this index are closer to those of Afghanistan, where al-Qaeda is not a very active user of the technology, than Lebanon, where Hezbollah is using it slightly more. For the case of the Islamic State it seems that this hypothesis does not fit, as computing power does not correlate to their activity in the crypto space. It is important to note, however, that the Islamic State has promoted the popularity of lone-wolf attacks around the globe, which is what some of the cryptocurrency

[200]"2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&SYR
[201] Ibid

funding goes towards.[202] In this case, the funding and attacks may not be based in Syria, allowing for greater use of the technology.

For the second hypothesis, and as mentioned above, there are no cryptocurrency ATMs in Syria.[203] Again, the Islamic State's use of lone-wolf attacks complicates this analysis slightly, as there are ATMs in countries where the Islamic State has claimed damages such as Turkey, France, the United States, Belgium, and other countries. But in Syria there are none, and they would most likely not be aided by Saudi Arabia to convert cryptocurrency to fiat currency, where there are two known cryptocurrency ATMs.[204] In late 2018 it was reported that a woman was found guilty of supporting Islamic State affiliates in China and Turkey, regions where there are cryptocurrency ATMs, which speaks to the deviation of lone-wolf attack results versus initiatives based in Syria proper.[205] This hypothesis also does not fit the case of the Islamic State. Without proper infrastructure such as cryptocurrency ATMs, the Islamic State has still managed to make effective use of the technology, and has for some time. This does not match what the second hypothesis predicted.

For the third hypothesis which looks at the price flux of cryptocurrencies in the market in relation to adoption probability by terrorist organizations, two instances of the Islamic State using the technology will be examined. The first instance of the Islamic State engaging in activity with cryptocurrencies is January 15th, 2019, when the website for Akhbar al-Muslimin opened a coin wallet on the homepage of their website, formally asking for Bitcoin donations to

---

[202] Gelvin, James L. "What Draws 'lone Wolves' to the Islamic State?" PBS. November 05, 2017. Accessed April 20, 2019. https://www.pbs.org/newshour/nation/what-draws-lone-wolves-to-the-islamic-state.
[203] https://coinatmradar.com/countries/
[204] Ibid
[205] Mangan, Dan. "Bitcoin, Bank Fraud and Bloodshed: New York Woman Pleads Guilty to Supporting ISIS Terror Group." CNBC. November 27, 2018. Accessed April 03, 2019. https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html.

help support the website.[206] It is reported that law enforcement believe the funds will be used to reinforce the organization and fund terrorist activities.[207] At the start of January, 2019, Bitcoin was priced at $4,177.35.[208] This came as Bitcoin was on a sharp decline, coming from its peak price of nearly $20,000.[209] The price was stabilizing at this time, and was a great bargain given the price of the currency only months earlier, so the purchase and investment in cryptocurrency technology at this time aligns with the hypothesis.

Diagram: https://99bitcoins.com/price-chart-history/

[206] Bitcoin Exchange Guide News Team. "ISIS Affiliated Website Akhbar Al-Muslimin Takes Bitcoin Donations to Make Use of BTC Anonymity." BitcoinExchangeGuide. February 17, 2019. Accessed April 03, 2019. https://bitcoinexchangeguide.com/isis-affiliated-website-akhbar-al-muslimin-takes-bitcoin-donations-to-make-use-of-btc-anonymity/.
[207] Ibid
[208]"Bitcoin Historical Price & Events" https://99bitcoins.com/price-chart-history/
[209] Ibid

The second instance the Islamic State using cryptocurrencies that will be examined in this study took place in January of 2017, when the Islamic State was accused of using Bitcoin to send money to operatives in Indonesia both as payment and for the carrying out of operations such as the 2016 bombing and shooting in Jakarta, Indonesia.[210] For the purpose of this study, the date that will be analyzed is that of the Jakarta attacks, as the report implied that the funding it was discussing happened in the past, most likely around the time of the attack.[211] The attacks in Jakarta, Indonesia took place on January 14th, 2016.[212] The price of Bitcoin at this time was $463.92, in the same price valley as when al-Qaeda made use of the technology leading up to the Charlie Hebdo attacks.[213] This purchase and investment in the technology also makes sense with the hypothesis as it was purchased at a not very volatile, inexpensive time in the technology's lifetime. Prices were low as was risk, and the Islamic State decided to investment in the technology as a result. These instances, while discrete in nature, do provide helpful information when considering the systematic use of cryptocurrencies.

These instances are some of the biggest, and therefore more risky investments and uses of cryptocurrencies used by terrorist organizations. Due to the scale of the usages, exploring the circumstances surrounding such significant instances of cryptocurrency usage by terrorist organizations provides insight into what considerations these groups make they invest in the technology. These instances can be representative of larger trends or manners in which groups

[210] Rizzo, Pete, and Pete Rizzo. "Indonesia's AML Watchdog Links Bitcoin to Islamic State." CoinDesk. January 09, 2017. Accessed April 03, 2019. https://www.coindesk.com/indonesias-aml-agency-links-bitcoin-islamic-state-terrorism.
[211] Ibid
[212] Ibid
[213] "Bitcoin Historical Price & Events" https://99bitcoins.com/price-chart-history/

approach cryptocurrencies which, at such an early stage in the technology's development, is significant information.

Diagram: https://99bitcoins.com/price-chart-history/

The fourth independent variable explores the issue of radicalism in terrorist groups and how it might relate to cryptocurrency adoption. To determine this level of radicalism I will again look at records discussing the number of attacks perpetrated by the Islamic State since its inception in 2013, and the average deaths and injuries per attack relative to global norms in the same time frame. According to the Global Terrorism Database, a database managed by the University of Maryland, College Park, since 2013 the Islamic State has carried out, or claimed responsibility for, 5676 terrorist attacks.[214] The attacks resulted in an average of 7.2 deaths per incident as well as 5.7 injuries per attack.[215] These number are very high given global averages in

[214] National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). Global Terrorism Database [Perpetrators: The Islamic State]. Retrieved from https://www.start.umd.edu/gtd
[215] Ibid

the same time span. From 2013 to 2016 the average number of deaths per terrorist attack in the world was 2.4 - the fatality rate of the Islamic State was triple the global average.[216]

For reference, Hezbollah, another well-known terrorist organization, averaged one death per attack over a time period which was three years longer than that of the Islamic State. Both the magnitude of fatalities and injuries exacted by the Islamic State, in tandem with the short time period in which these acts were carried out, would categorize the Islamic State as a very radical organization who tactics have wrought incredible damage around the world. Given their level of radicalism, their level of cryptocurrency adoption makes sense. The Islamic State is one of the most well-adapted terrorist groups to this technology in the contemporary context, and it makes sense given their very radical agenda. They have ambitious goals and require radical innovation to attain them.

The fifth hypothesis deals with ideological platforms of the Islamic State and their sentiments towards the West more specifically. The Islamic State is known for being extremely anti-Western, even more so than al-Qaeda. The group feels this intensely about the West so much so that in an August 1st briefing by Tony Blair Institute for Global Change in 2016, it was reported that Islamic State magazine Dabiq published an article "Why We Hate You & Why We Fight You," an article where "the group sets out six points explaining the justifications for their hatred of the West. It mentions, in order, the West's disbelief in Islam, the prevalence of secularism, atheism, 'transgressions' against Islam, military operations, and territorial incursions."[217]

---

[216] Roser, et al. "Terrorism."

[217] "In Their Own Words: Why ISIS Hates the West." Institute for Global Change. August 1, 2016. Accessed April 03, 2019. https://institute.global/insight/co-existence/their-own-words-why-isis-hates-west.

The Islamic State is also known for either directly carrying out attacks on United States soil, or claiming responsibility for attacks that have taken place in the United States and across the Western world as well.[218] For these reasons, the Islamic State does not fit the fifth hypothesis, as its usage of cryptocurrency is relatively high given its very extreme anti-Western views. If the hypothesis were to fit this case, the Islamic State's hatred of the West would manifest itself in the rejection of Western technologies including cryptocurrency technology in exchange for more Eastern, fundamentalist practices.[219]

The sixth hypothesis regards the traditional means of financing employed by the Islamic State and its status in the contemporary context. As mentioned in the RAND Corporation's book, the Islamic State has had its traditional means of financing rendered essentially useless. The land it once held has been stripped from the group, leaving it with little room to obtain and sell oil. It's finances have been spent battling the Kurds and other forces in a global effort to destroy and dismantle the group.[220] The group's geographic location makes it difficult to access traditional banking mechanisms as well, even if the group did eventually decide to use them. As such, the Islamic State is in a state of transition - moving from physical space to a more digital one, and altering its funding mechanisms as well.

In the end, only the hypotheses related to the pricing of Bitcoin at the time of its use by the Islamic State, and the groups need for innovation in the face of extreme counter-terrorism financing intervention fit the case of the Islamic state. The groups ideology and computing

[218] Gilsinan, Kathy. "The 'Caliphate' Is Dead, but Americans Might Not Be Any Safer." The Atlantic. March 24, 2019. Accessed April 20, 2019. https://www.theatlantic.com/politics/archive/2019/03/us-safer-islamic-state-gone/584110/.
[219] Ibid
[220] Dion-Schwarz, et al. Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats

power, as well as the infrastructure in Syria do not match the group's use of cryptocurrency technology today. The group's more frequent use of lone-wolf attackers compared to al-Qaeda and Hezbollah make these determinations slightly more shaky, as the international nature of this strategy allows for the use of infrastructure, computing power, and ideology outside of the Syrian context, which might play a big role is the Islamic State's success thus far. However, there is still significance in the narrowing of options which has come out of the cast studies.

Case Summary

Ultimately, only one hypothesis has prevailed through the three cases, that being the hypothesis related to the traditional means of financing already in place by terrorist organizations. For the groups who have not faced much adversity in the way of their financing - al-Qaeda and Hezbollah - there has not been a huge adoption of cryptocurrency technology. There are not many anecdotal cases of adoption for these groups and their messaging does not seem to suggest that this phenomenon should change in the near future. For the group that has faced the greatest adversity and is undergoing a large shift in strategy and identity - the Islamic state - adoption of cryptocurrency has looked much larger.

The results of these studies become murkier when we consider the existence of lone-wolf attackers however. If we were to globalize the Islamic State as a result of their use of lone-wolf attackers, we would see the first hypothesis (related to computing power) and the second hypothesis (related to infrastructure) fit the Islamic State case. While the second hypothesis did not fit the case of Hezbollah, the first hypothesis would then fit each case, making it, like the

sixth hypothesis, a strong contender as a legitimate reason for lack of full adoption of cryptocurrency technology today.

The issue of transnational terrorist organizations is also very significant in the operationalization of many of my hypotheses. Regarding issues of computing power in various countries, the presence of cryptocurrency ATMs in select countries, and even in an exploration of radicalism amongst terrorist groups, transnationality complicates the research. Now-a-days, terrorist groups can be quite disparate, dwelling on a number of continents with varying levels of computer power and infrastructure, with, at times, no true headquarter or home base. Within the framing of these hypotheses, accounting for transnational terrorist groups is quite difficult, and should be the subject of future research on this topic.

Below is a table displaying the three cases and the six hypotheses, significantly truncated so as to account for limited space. The left hand side will represent the three cases and the top will represent the hypotheses. The goal is to depict the relationship between the cases and the hypotheses to see which independent variables best account for each of the cases:

	Computing Power	Infrastructure	Price Flux	Radicalism	Ideology	Traditional Methods
Al-Qaeda	Yes	Yes	Yes	No	Yes	Yes
Hezbollah	Yes	No	No	Yes	Yes	Yes
Islamic State	No	No	Yes	Yes	No	Yes

Another interesting wrinkle to this study would be to replace Hezbollah, which after some consideration, feels a bit like an anomaly, with another terrorist organization with even

greater ties to the technology such as Hamas. As Hamas has entered the cryptocurrency space for a longer period of time, and arguably has a deeper adoption of the technology already underway, it would be interesting to plot their experience with the technology within these data to see if new findings arise. Their usage and understanding of the technology, from reports, rivals that of the Islamic State, and they would therefore make an appealing case to research in the future.

Finally, it is important to analyze the positive data which we do have and understand the implications of them. The common factor among these cases is that with greater disruption to traditional means of terrorist financing comes a greater likelihood of innovation and adoption cryptocurrency technology. Does this mean that governments should stop disrupting flows of money to and from terrorist organizations? No. This simply means that, as it has been, government approaches to these issues must be two fold. First, the must address the traditional means of financing that are allow groups like al-Qaeda and Hezbollah to persist without needing to drastically innovate their financing methods.

Second, they must also crack down on the proliferation of cryptocurrency technology around the world. It will require a massive multilateral effort, but governments must learn to regulate this technology and work with other countries to create a standard of policing illicit financial activities.

It is important to note that the cases examined in this study only encompass one region of the world. This fact was not inconsequential in the research. All of the cases being housed in the Middle East meant that none of the groups had the proper infrastructure to convert cryptocurrency into fiat currency efficiently. Were the study to have research Russian, Spanish, American, or Chinese terrorist groups, the infrastructure for these exchanges would have been

plentiful, and possibly have changed the tenor of the conclusions of the study. This is to say that policy to combat terrorist financing must be region-specific. What works to stop terrorists from abusing cryptocurrency technology in the Middle East may not, and most likely will not work for terrorist organizations in other areas of the world. This is an important realization and one that often goes unmentioned in literature on the topic.

Chapter VIII: Conclusions

Many of the common beliefs regarding how to best prevent the abuse of cryptocurrencies by terrorist organizations are wrong. There are no distinctive traits that would mark a terrorist organization of being more likely to adopt the technology. Even ISIS' recent uses of cryptocurrencies do not guarantee, or necessarily even indicate, that the group is near adopting cryptocurrencies on a systemic level within their organization. What seems to be the greatest indicator of a group which is likely to adopt cryptocurrencies, is their ability to efficiently use their other funding mechanisms.

The current systems in place for terrorist organizations fit the needs of these organizations to a satisfactory level, such that they need not search out alternative funding apparatuses. If the funding channels which are currently in place are disrupted, groups will be forced to find funding elsewhere. Fiscal capacity is one of the most important characteristics of a terrorist organization. Finances allow terrorist groups to operate: pay fighters, purchase weapons, travel. Efficient and friction-less financing will always be the preferred course for terrorist organizations.

In addition to these challenges, future topics of research should focus on the issue of lone-wolf attackers and transnational terrorist organizations. These are two characteristics, or tactics, of terrorist groups that may have a large influence on whether a group decides to adopt cryptocurrency technology on a systematic level. While challenging to observe within the framework of my research, cryptocurrencies offer many benefits to these factions - they allow for easier cross-continental transactions, and subsequently more difficult-to-track funding channels. As some groups move closer to these approaches to terrorist activity, research should focus on the empirical effects of this shift on the cryptocurrency landscape.

This is the task that faces governments around the world. Regulatory instruments are being made to latch onto moving targets -- always amending policies trying to pin down an ever-evolving technology. Additionally, every new technology will not be adopted by terrorist groups, making the work of policy creation difficult. When is it appropriate to regulate a technology? Will time be wasted crafting policy towards a fruitless end? While governments are moving in the right direction with respect to corralling the proliferation of cryptocurrencies in terrorist hands, cryptocurrencies themselves are advancing; becoming more secure and bearing greater anonymity. What is more, states such as North Korea are equally abusing cryptocurrencies in an effort to evade United States sanctions, making the work of regulatory policy extremely complicated. First, effective policy must mitigate the use of cryptocurrencies by both state and non-state actors. Secondly, in the case of terrorist organizations, effective policy must also regulate both a terrorist organization's traditional financing methods as well as its impending transition to cryptocurrencies.

With regard to the potential policy implications of these findings, certain issues must be weighted more heavily than others. First, United States policy needs to put a focus first on Hezbollah and Hamas, not other actors such as al-Qaeda and the Islamic State. Through heavier Iranian restriction, and more expansive regulatory action against patrons of Iran such as Syria and Russia, Iran's influence in the Middle East can be stymied.

Iran has undergone significant sanctions in the past half-decade. As a result, Iran has been forced to sell its natural resources like a rentier state to maintains its integrity as it did in November, 2018, when Russia was caught facilitating oil sales between Iran and the Assad regime in Syria.[221] Iran's ability to sponsor terrorist groups and implement military proxies has been greater weakened, making groups like Hezbollah and Hamas prime for adopting cryptocurrency technology to a great scale.[222] A focus on Iranian sanctions would not only alleviate the fear of crypto-adoption within Hezbollah and Hamas, but it would also ameliorate tensions in Syria and allow the conflict greater chance of coming to a close. Heavier Iran sanctions must be accompanied by robust interventionary policy to combat the cryptocurrency usage that might follow such sanctions.

The issue of creating 'robust inventionary policy' ties directly to certain policy enacted by the United States Treasury, specifically its program the Terrorist Finance Tracking Program (TFTP).[223] The TFTP derives much of its intel from the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which it regularly subpoenas for information of terrorist

[221] Office of the Spokesperson. "Sanctions Announcement on Iran." *United States Department of State*, November 20, 2018.
[222] Ibid
[223] "U.S. Department of the Treasury." Terrorist Finance Tracking Program (TFTP). Accessed April 17, 2019. https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp.

financing activity.[224] SWIFT is a Belgian company that houses a "messaging system used to transmit financial transaction information" according to the treasury department. The problem with the treasury department's TFTP is that the information it gets from SWIFT and certain data hosted in the European Union, which only tracks transactions carried out through traditional banking channels.[225] This means that anonymized cryptocurrencies transactions might not fall within the purview of the TFTP and the banks which oversee SWIFT including the United States Federal Reserve and the Bank of England.[226]

The United States government needs to allocate resources towards partnering with organizations such as Chainanalysis which has found ways to link cryptocurrency exchange wallets to real identities in an effort to combat criminal activity and financing.[227] The European Union Agency for Law Enforcement Cooperation (Europol) has already began working with the company to augment the European Union's cryptocurrency regulation policy, but the United States must follow suit if it hopes to make a dent in the world of terrorist group financing through cryptocurrency.[228] Additionally, there is an imperative to act quickly. As cryptocurrencies such as Zcash and Monero continue to gain market share and become more popular, government crypto wallets will be faced with attacking a new wave of more private, more secure cryptocurrencies. Getting ahead of trends in the cryptocurrency landscape is difficult, and so is keeping up with developments which occur in the space.

---

[224] Ibid
[225] Ibid
[226] Ibid
[227] Hrones, Matthew. "Yes, Your Bitcoin Transactions Can Be Tracked - and Here Are the Companies That Are Doing It." Bitcoinist.com. June 28, 2018. Accessed April 17, 2019. https://bitcoinist.com/yes-your-bitcoin-transactions-can-be-tracked-and-here-are-the-companies-that-are-doing-it/.

[228] Ibid

Ultimately, United States policy related to combating the financing of terrorist operations is outdated given the current threats which face the United States. Cryptocurrencies are an impending threat, especially as the Trump administration continues to administer a robust and prolific sanction regime on countries such as North Korea and Iran. Both of these countries have been involved in either acquiring or facilitating the transaction of cryptocurrencies within their jurisdiction in response to heavy sanctions. The United States first needs to reinforce its policies which put pressure on contemporary methods of terrorist financing, and they must also cooperate with multinational cooperatives such as the European Union to develop adequate follow-up measures to tackle the subsequent cryptocurrency adoption which often follows sanction regimes.

This is especially important because, as Horowitz mentions, innovation without terrorist organizations has a duplicating effect. Once one group adopts the technology on a systemic level, more groups will follow suit as their conditions allow them greater capacity to adopt the technology. If this occurs, the speed at which both the technology is developing and groups are adopting the technology will be exceedingly high such that legislation and regulation will ultimately prove too slow and encumbered to effective address the issue at hand. The solution for this aforementioned problem is a mystery, and the focus at this point in time should be on mitigating traditional financing mechanisms while also preparing for shifts to cryptocurrency adoption. Terrorist groups need money, and if their primary channels of acquiring said funds are disrupted, they will be forced to seek out new financing techniques. The United States government must take this threat of adoption seriously, and update its policies to address the issues at hand.

Bibliography

"2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&AFG.

"2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&HKG

"2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&ISL

"2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&LBN

"2017 Global ICT Development Index." ITU. Accessed April 20, 2019. http://www.itu.int/net4/itu-d/idi/2017/index.html#idi2017economycard-tab&SYR

"Airtime Is Money." The Economist. January 19, 2013. Accessed November 02, 2018.

Acheson, Noelle. "How Does Proof of Work, Um, Work? – Decentralize Today." Decentralize Today. June 06, 2016. Accessed February 12, 2019.

Adam, Dolnik. Understanding Terrorist Innovation: Technology, Tactics and Global Trends. Place of Publication Not Identified: Routledge, 2013.

Aman, Moustapha, Nikolay Nenovsky, and Ismaël Mahamoud. "The Informal System of Remittances and Currency Board: Complementarity or Antagonism? the Case of Hawala Transfers in Djibouti." Savings and Development 38, no. 1 (2014): 133-54. http://www.jstor.org/stable/savideve.38.1.133.

Baydakova, Anna. "Crypto Use A 'Fringe Activity' Among Terrorists, Says Think Tank." CoinDesk. September 11, 2018. Accessed April 03, 2019. https://www.coindesk.com/crypto-use-is-a-fringe-activity-among-terrorists-says-think-tank.

Booker, Chaka. "Innovation Is A Fancy Word For Survival." Forbes. November 27, 2018. Accessed April 20, 2019. https://www.forbes.com/sites/chakabooker/2018/11/27/innovation-is-a-fancy-word-for-survival-baltimores-dirt-bike-culture/#4cfcb4fc4d10.

"Bitcoin ATM Map – Find Bitcoin ATM, Online Rates." – Find Bitcoin ATM, Online Rates. Accessed April 20, 2019. https://coinatmradar.com/.

Bitcoin Exchange Guide News Team. "ISIS Affiliated Website Akhbar Al-Muslimin Takes Bitcoin Donations to Make Use of BTC Anonymity." BitcoinExchangeGuide. February 17, 2019. Accessed April 03, 2019. https://bitcoinexchangeguide.com/isis-affiliated-website-akhbar-al-muslimin-takes-bitcoin-donations-to-make-use-of-btc-anonymity/.

“Bitcoin Historical Price & Events” https://99bitcoins.com/price-chart-history/

Canellis, David. "Europol: Criminals Are Still Using Bitcoin, but ISIS Loves Zcash." Hard Fork | The Next Web. September 21, 2018. Accessed April 03, 2019. https://thenextweb.com/hardfork/2018/09/19/europol-cryptocurrency-cybercrime/.

Chiu, Jonathan and Koeppl, Thorsten V., The Economics of Cryptocurrencies – Bitcoin and Beyond (September 1, 2017). Available at SSRN: https://ssrn.com/abstract=3048124 or http://dx.doi.org/10.2139/ssrn.3048124

Chong, Nick. "Researchers: North Korea Is Trading Crypto To Undermine International Sanctions." Ethereum World News. September 25, 2018. Accessed April 11, 2019. https://ethereumworldnews.com/north-korea-crypto-sanctions/.

Clarke, Colin P. "Hezbollah Is in Venezuela to Stay." Foreign Policy. February 09, 2019. Accessed April 18, 2019. https://foreignpolicy.com/2019/02/09/hezbollah-is-in-venezuela-to-stay/.

“Combating the Illicit Use of Virtual Currencies.” *Financial Services Committee*, The United States House Committee on Financial Services, 20 June 2018,

Cuen, Leigh. "Blockchain Analysis Links Hamas Fundraising to Coinbase Bitcoin Account." CoinDesk. February 07, 2019. Accessed April 20, 2019. https://www.coindesk.com/hamas-coinbase-bitcoin.

Daria, Dorovskaya, et al. “Inflation in Venezuela and Cryptocurrency. Influence of Hyperinflation in the Country on Cryptocurrency Prices.” *The Coin Shark*, The Coin Shark, 11 Sept. 2018

David, Carslile. "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic." RUSI. March 02, 2017. Accessed November 02, 2018.

David, Orrell, and Roman Chlupatý. "Changing the Dominant Monetary Regime, Bit by Bitcoin." In *The Evolution of Money*, 196-219. Columbia University Press, 2016.

Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3026.html.

Dulce M., Redin, Reyes Calderón, and Ignacio Ferrero. "Exploring the Ethical Dimension of "Hawala"." *Journal of Business Ethics* 124, no. 2 (2014): 327-37.

Eben, Kaplan. "Tracking Down Terrorist Financing." Council on Foreign Relations. April 4, 2006. Accessed December 21, 2018.

Fanusie, Yaya J. "Jihadists Upping Their Bitcoin Game." FDD. April 01, 2019. Accessed April 03, 2019. https://www.fdd.org/analysis/2019/03/29/jihadists-upping-their-bitcoin-game/.

Fishman, Brian. "Using the Mistakes of Al Qaeda's Franchises to Undermine Its Strategies." The Annals of the American Academy of Political and Social Science 618 (2008): 46-54. http://www.jstor.org/stable/40375774.

Floyd, David. "Venezuela's Petro Isn't Oil-Backed. It's Not Even a Cryptocurrency (Opinion)." Investopedia. March 12, 2019. Accessed April 03, 2019. https://www.investopedia.com/news/venezuela-petro-not-cryptocurrency/.

Gardner, Kathryn L. "Fighting Terrorism the FATF Way." *Global Governance* 13, no. 3 (2007): 325-45.

Gelvin, James L. "What Draws 'lone Wolves' to the Islamic State?" PBS. November 05, 2017. Accessed April 20, 2019. https://www.pbs.org/newshour/nation/what-draws-lone-wolves-to-the-islamic-state.

Ghanem, Hafez. "How to Stop the Rise in Food Price Volatility." Carnegie Endowment for International Peace. January 31, 2011. Accessed April 22, 2019. https://carnegieendowment.org/2011/01/13/how-to-stop-rise-in-food-price-volatility-pub-42292.

Goldman, et al. Terrorist use of Virtual Currencies*: Containing the Potential Threat*. Report. Center for a New American Security, 2017. 9-16.

Gilsinan, Kathy. "The 'Caliphate' Is Dead, but Americans Might Not Be Any Safer." The Atlantic. March 24, 2019. Accessed April 20, 2019. https://www.theatlantic.com/politics/archive/2019/03/us-safer-islamic-state-gone/584110/.

Gunaratna, Rohan. "Aum Shinrikyo's Rise, Fall and Revival." *Counter Terrorist Trends and Analyses* 10, no. 8 (2018): 1-6.

Gunaratna, Rohan. "Global Threat Forecast The Rise of ISIS." *Counter Terrorist Trends and Analyses* 8, no. 1 (2015): 6-11. http://www.jstor.org/stable/26369557.

Hamming, Tore Refslund. "With Islamic State in Decline, What's Al-Qaeda's Next Move?" War on the Rocks. April 27, 2018. Accessed April 03, 2019. https://warontherocks.com/2018/04/with-islamic-state-in-decline-whats-al-qaedas-next-move/.

Harrison, Kate. "Should Your Company Accept Bitcoin And Other Cryptocurrency Payments?" Forbes. September 19, 2018. Accessed April 11, 2019. https://www.forbes.com/sites/kateharrison/2018/09/10/should-your-company-accept-bitcoin-and-other-cryptocurrency-payments/#318bb9a43373.

Hrones, Matthew. "Yes, Your Bitcoin Transactions Can Be Tracked - and Here Are the Companies That Are Doing It." Bitcoinist.com. June 28, 2018. Accessed April 17, 2019. https://bitcoinist.com/yes-your-bitcoin-transactions-can-be-tracked-and-here-are-the-companies-that-are-doing-it/.

ICT Cyber Desk. Report. International Institute for Counter-Terrorism (ICT), 2013.

"In Their Own Words: Why ISIS Hates the West." Institute for Global Change. August 1, 2016. Accessed April 03, 2019. https://institute.global/insight/co-existence/their-own-words-why-isis-hates-west.

"Iran Nuclear Deal: Trump Pulls US out in Break with Europe Allies." BBC News. May 09, 2018. Accessed April 18, 2019. https://www.bbc.com/news/world-us-canada-44045957.

Jacob N., Shapiro. "Terrorist Decision-Making: Insights from Economics and Political Science." *Perspectives on Terrorism* 6, no. 4/5 (2012): 5-20.

Jetencila. "Hamas Turns to Bitcoin (BTC) to Fund Its Terror Activities • Live Bitcoin News." Live Bitcoin News. February 04, 2019. Accessed April 03, 2019. https://www.livebitcoinnews.com/hamas-turns-to-bitcoin-btc-to-fund-its-terror-activities/.

Juan C. Zarate, “Learning Curve,” in Treasury’s War: The Unleashing of a New Era of Financial Warfare, New York: Public Affairs, Perseus Book Group, 2013, pp.362–363.

Katz, Brian. "Will Hezbollah's Rise Be Its Downfall?" Foreign Affairs. March 08, 2019. Accessed April 03, 2019. https://www.foreignaffairs.com/articles/israel/2019-03-08/will-hezbollahs-rise-be-its-downfall.

Kenton, Will. "Security." Investopedia. December 13, 2018. Accessed March 02, 2019. https://www.investopedia.com/terms/s/security.asp.

Kozlowski, Andrzej. "Cross-Border Philanthropy and Counterterrorism Regulations: Guidance for U.S. Grantmakers." PEAK Grantmaking. February 08, 2018. Accessed February 12, 2019.

Lennart, Ante. "Cryptocurrency, blockchain, and crime." In *The Money Laundering Market: Regulating the Criminal Economy*, edited by McCarthy Killian J., 171-198. Agenda Publishing, 2018.

Louise I., Shelley. *Dirty Entanglements: Corruption, Crime, and Terrorism*. New York, NY: Cambridge University Press, 2014: 259-280.

Luke M., Gerdes. *Illuminating Dark Networks: The Study of Clandestine Groups and Organizations*. New York: Cambridge University Press, 2015.

Magnus, Ranstrop, and Magnus, Normark, eds. *Understanding Terrorism Innovation and Learning*. Abingdon: Routledge, 2015: 5-10.

Mangan, Dan. "Bitcoin, Bank Fraud and Bloodshed: New York Woman Pleads Guilty to Supporting ISIS Terror Group." CNBC. November 27, 2018. Accessed April 03, 2019. https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html.

Manheim, David, Patrick Johnston, Josh Baron, and Cynthia Dion-Schwarz. "Are Terrorists Using Cryptocurrencies?" Foreign Affairs. April 21, 2017. Accessed March 02, 2019. https://www.foreignaffairs.com/articles/2017-04-21/are-terrorists-using-cryptocurrencies.

Marguerite, Borelli. "ASEAN Counter-terrorism Weaknesses." *Counter Terrorist Trends and Analyses* 9, no. 9 (2017): 14-20.

Marieke De., Goede. *Speculative Security: The Politics of Pursuing Terrorist Monies*. Minneapolis: University of Minnesota Press, 2012.

Merrick M., Yamamoto. *Terrorism Against Democracy: Based in Part on Stansfield Turner's University of Maryland Course, "Terrorism & Democracy"*. Report. Center for International & Security Studies, U. Maryland, 2017. 56-70.

Michael, C. Horowitz "Nonstate Actors and the Diffusion of Innovations: The Case of Suicide Terrorism." *International Organization* 64, no. 1 (2010): 33-64.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Accessed February 12th, 2019. https://bitcoin.org/bitcoin.pdf

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). Global Terrorism Database [Perpetrators: AQIM, AQAP, Al-Shabaab]. Retrieved from https://www.start.umd.edu/gtd

National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2018). Global Terrorism Database [Perpetrators: Hezbollah]. Retrieved from https://www.start.umd.edu/gtd

Nikos, Passas. "Hawala and Other Informal Value Transfer Systems: How to Regulate Them?" *Risk Management* 5, no. 2 (2003): 49-59.

Office of the Spokesperson. “Sanctions Announcement on Iran.” *United States Department of State*, November 20, 2018.

Perper, Rosie. "ISIS Made Millions from Taxes That It Then Used to Run Garbage Collections and Even a DMV." Business Insider. April 06, 2018. Accessed April 18, 2019. https://www.businessinsider.com/islamic-state-used-taxes-to-grow-power-and-offer-services-2018-4.

Peter J., Kazenstein and Lucia A.. Seybert. Protean Power: Exploring the Uncertain and Unexpected in World Politics. Cambridge: Cambridge University Press, 2018.

Press Release - March 28, 2019. "Qatar: Extremism & Counter-Extremism." Counter Extremism Project. January 02, 2018. Accessed April 03, 2019. https://www.counterextremism.com/countries/qatar.

Roser, Max, Mohamed Nagdy, and Hannah Ritchie. "Terrorism." Our World in Data. July 28, 2013. Accessed April 20, 2019. https://ourworldindata.org/terrorism.

Rizzo, Pete, and Pete Rizzo. "Indonesia's AML Watchdog Links Bitcoin to Islamic State." CoinDesk. January 09, 2017. Accessed April 03, 2019. https://www.coindesk.com/indonesias-aml-agency-links-bitcoin-islamic-state-terrorism.

Ryamizard, Ryacudu. "Terrorism in Southeast Asia: The Need for Joint Counter-Terrorism Frameworks." *Counter Terrorist Trends and Analyses* 10, no. 11 (2018): 1-3.

Samburaj, Das. “Iran and Russia Consider Using Cryptocurrency to Evade US Sanctions: Report.” *CCN*, CCN, 21 May 2018

Scott, Heather, and Agence France-Presse. "What Does 10,000,000 Percent Inflation Look Like? See Venezuela." ABS. October 09, 2018. Accessed April 18, 2019. https://news.abs-cbn.com/business/10/09/18/what-does-10000000-percent-inflation-look-like-see-venezuela.

Sherlock, Ruth. "U.S.-Backed Forces Declare Defeat Of ISIS 'Caliphate'." NPR. March 23, 2019. Accessed April 20, 2019. https://www.npr.org/2019/03/23/706147761/u-s-backed-forces-declare-defeat-of-isis-caliphate.

Simon, Norton, and Paula Chadderton. *Detect, Disrupt and Deny: Optimising Australia’s Counterterrorism Financing System*. Report. Australian Strategic Policy Institute, 2016. 10-17.

Spencer, Applebaum. “Analysis of the Cryptocurrency Exchange Landscape – Miami University Blockchain Club – Medium.” *Medium.com*, Medium, 31 Dec. 2017

Steinmetz, Fred. "Using Blockchain Technology for the Prevention of Criminal Activity." In *The Money Laundering Market: Regulating the Criminal Economy*, edited by McCARTHY KILLIAN J., 199-222. Agenda Publishing, 2018.

Stern, Jessica, and Ronald Schouten. "Lessons from the Anthrax Letters." In *Insider Threats*, edited by Bunn Matthew and Sagan Scott D., 74-76.

Steven, Stalinsky. "Terrorists Have Been Using Bitcoin for Four Years, so What's the Surprise?" TheHill. March 08, 2018. Accessed November 02, 2018.

Terrill, W. Andrew. Report. Strategic Studies Institute, US Army War College, 2017. http://www.jstor.org/stable/resrep11436.

Van Valkenburgh, Peter. *Framework for Securities Regulation of Cryptocurrencies*. Washington D.C.: Coin Center, 2018. February, 2019. https://coincenter.org/files/securities-cryptocurrency-framework-v2.1.pdf

Ungerer, Carl. “Terrorist Innovation and Methods” in “*Beyond bin Laden: Future trends in terrorism*.” Canberra: Australian Strategic Policy Institute, 2001.

"U.S. Department of the Treasury." Terrorist Finance Tracking Program (TFTP). Accessed April 17, 2019. https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp.

"Why Are There So Many Cryptocurrencies?" Coindirect. September 26, 2018. Accessed April 11, 2019. https://blog.coindirect.com/so-many-cryptocurrencies/.

Williams, Sara Elizabeth. "£80m of British Taxpayers' Money 'funnelled to Al-Qaeda' in Decades-long Scam." The Telegraph. March 31, 2019. Accessed April 03, 2019. https://www.telegraph.co.uk/news/2019/03/31/80m-british-taxpayers-money-funnelled-al-qaeda-decades-long/.

Winston, Ali. "How a Dark Web Drug Ring Was Uncovered After Suspicious A.T.M. Withdrawals." The New York Times. April 16, 2019. Accessed April 20, 2019. https://www.nytimes.com/2019/04/16/nyregion/dark-web-drug-dealing.html.

Zachary K., Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. *Terrorist Use of Virtual Currencies Containing the Potential Threat*. Report. Center for a New American Security, 2017. 9-16.