REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
	Master's of Military Studies	SEP 2017 - APR 2018

4. TITLE AND SUBTITLE

Beyond Bitcoin to the Blockchain: Security Implications of Blockchain Technology

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Pineda, David, Department of Homeland Security

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper focuses on the potential security implications from the emergence of cryptocurrencies, Blockchain technology, and its capabilities. This subject often is simplified to the bitcoin phenomenon and wrongly ignored. It should be noted that a significant portion of this subject has parallels to the cyber domain, of which some areas may be classified. However, this subject while nascent and obscure, warrants deeper dialogue to understand the future use cases of Blockchain technology along with the security implications which should be observed.

15. SUBJECT TERMS

Bitcoin; Blockchain; Technology; Decentralized; Cryptocurrency

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
Unclass					USMC Command and Staff College
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UU		**19b. TELEPHONE NUMBER** *(include area code)*
Unclass	Unclass	Unclass			(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

BEYOND BITCOIN TO THE BLOCKCHAIN:
Security Implications of Blockchain Technology

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: Mr. David Pineda

AY 2017-18

Mentor and Oral Defense Committee Member: LtCol BRAD PENNELLA
Approved: [signature]
Date: 20 April 2018

Oral Defense Committee Member: [signature]
Approved: [signature]
Date: 4/20/18

Executive Summary

Title: BEYOND BITCOIN TO THE BLOCKCHAIN: Security Implications of Blockchain Technology

Author: Mr. David Pineda, Department of Homeland Security.

Thesis: Technological innovations often benefit society writ large; however, the recent emergence of cryptocurrencies, underpinned by blockchain technology, presents a new domain that ought to be studied more closely, by federal regulatory and enforcement agencies, given the potential security implications that can span beyond the financial sector and well into any technologically dependent area.

Discussion: This paper focuses on the potential security implications from the emergence of cryptocurrencies, blockchain technology, and its capabilities. This subject often is simplified to the bitcoin phenomenon and wrongly ignored. It should be noted that a significant portion of this subject has parallels to the cyber domain, of which some areas may be classified. However, this subject while nascent and obscure, warrants deeper dialogue to understand the future use cases of blockchain technology along with the security implications which should be observed.

Conclusion: The United States Government should take a whole of government approach to understand and leverage capabilities within this new domain, just as it has in the cyber domain. Collaboration and knowledge sharing relationships should be established with key commercial blockchain organizations and subject matter experts on the cutting edge of innovations developing new systems and software. Furthermore, blockchain savvy, skilled, and trained United States Government personnel should be recruited into an interagency taskforce comprised of financial, science and technology, regulatory and law enforcement representatives. This whole of government posture should better enable the United States government to deter, combat and neutralize malign actors seeking to use this technology to their advantage to exploit vulnerabilities in various sectors of the homelands infrastructure.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Table of Figures

Table of Contents

Preface

This research project studies innovations in blockchain technology and cryptocurrencies, along with the potential associated security implication that should be monitored from a United States whole of Government perspective. Implication range from the financial technology sector to various data/technology dependent sectors. Federal regulatory, law enforcement, and science and technology organizations should devote time, resources, and personnel to understand and leverage this capability.

This subject is of great interest to me, as I feel we are currently in the middle of a paradigm shift in technology. I agree with many thought leaders in this space that overall technology is evolving from centralized information, internet, and data environment to a decentralized one. Many positives can be deduced from such a future. However, there are negative use cases, like exploitation of currency used to fund illegal activities and cryptographic communication technology that can be leveraged by criminals, terrorist and other malign actors.

A great deal of gratitude is due to Dr. John Gordon for his support, mentorship, and guidance during this process. Additionally, a special thanks to both Mr. Michael Cicere, who has been a wealth of knowledge on all matters related to the intelligence community.

We will encourage scientist in government, academia, and the private sector to achieve advancements across the full spectrum of discovery, from incremental improvements to game-changing breakthroughs. We will nurture a healthy innovation economy that collaborates with allies, partners, improves STEM education, draws on an advanced technical workforce, and invests in early-stage research and development (R&D).

–Donald Trump, 45th President of the United States
2017 National Security Strategy

I think the fact that within the bitcoin universe an algorithm replaces the functions of [the government] … is actually pretty cool. I am a big fan of Bitcoin.

–Al Gore, 45th Vice President of the United States

Context

The 2017 National Security Strategy emphasizes the priority of the United States to lead in research, technology, invention, and innovation; specifically, it highlights the need to maintain a competitive advantage by "prioritizing emerging technologies critical to economic growth and security, such as data science, encryption, autonomous technologies…advanced computing technologies, and artificial intelligence."[1] Factoring in the current terroristic landscape that keeps evolving and employing new technology, the United States' ability to meet these threats head-on requires it fully embrace, employ and execute the precepts within the National Security Strategy to ensure efforts to secure the homeland are agile and able to adapt to new and emerging threats.

There are new innovations in technology creating various new use cases, namely, cryptocurrencies and blockchain technology. However, they sadly are dismissed due to an oversimplification of this technology being labeled simply Bitcoin. But a closer study of this technology should be undertaken due to its disruptive potential and impact that spans beyond the financial sector. Bitcoin is the widely popular yet highly misunderstood technological phenomenon that grabbed headlines in 2017, due in part to its record-setting price of $19,783.06

per bitcoin, bringing the conversation about this technology out from the obscure *techy* circles and into the mainstream conversation, though, many would relegate it to an overhyped get rich quick scheme.[2] Moreover, various industries like banking, cyber, supply chain management, insurance, cloud storage, voting, public benefits, healthcare, energy management, retail, entertainment, real estate, and crowdfunding, to name a few, are extremely data dependent. Blockchain technology is creating ways for these industries and their respective organization to record and transfer data in a transparent, safe, auditable, and outage resistant manner. Furthermore, this technology may provide the ability to make the organizations that use the blockchain transparent, democratic, decentralized, efficient, and secure.[3]

Considering the wide reach of this technology, the United States government in accordance with the National Security Strategy as noted above, should take more deliberate steps to explore, understand, leverage and even exploit blockchain technology, which goes beyond Bitcoin. A benefit of understanding this technology will lead to improved crime, corruption, and fraud deterrence as well as crime fighting capabilities. However, a willful ignorance or disregard of this potential paradigm shift in technology is no different from ignoring the innovations that changed how wars were fought, via new vehicles, weapons, and technology. This paper explores, within a limited scope due to the complexity of the subject, the origins of Bitcoin, cryptocurrencies at large, the blockchain, mass adoption of blockchain technology, emerging threats domestically and abroad as they relate to crimes and terrorism, regulatory and security concerns, potential future use cases, and some thoughts for the road ahead. This paper should hopefully add to the conversation urging the need for government and law enforcement organizations to verse themselves in this technology that extends past Bitcoin or other similar digital currency, hereafter referred to as cryptocurrency, and their capabilities.

Bitcoin Origins, Cryptocurrency, and the Blockchain

For many Bitcoin is this mysterious and techy digital money that is associated with individuals that may have gotten rich by investing in it early or as the form of money used on the Silk Road, the infamous dark web site, used by criminals.[4] Bitcoin and other various forms of cryptocurrencies are built on the principles of cryptography. A quick search of Dictionary.com or Merriam-Webster's dictionary, defines Cryptography is the science or study of the techniques of secret writing, especially code of cipher systems, methods and the like; essentially the art of writing or solving codes.[5] Some of the original forms of cryptocurrency began surfacing around the late 1980's, one notable instance was Digicash, created by David Chaum.[6] Various forms of electronic forms of cryptocurrencies, then called electric cash, all endeavored to reclaim financial ownership from the banking system or improve outdated practices in light of the growing computing power, gaining mainstream attention with the advancements of companies like Microsoft and Apple computer. [7] A central idea of some groups that were considered leftist movements was anonymity. The 1990's would usher in the cypherpunk movement, well before big data, Edward Snowden and knowledge of the NSA's capabilities were known.[8]

The cypherpunk movement sought to create various anonymous communication tools, for example email, information boards, messenger. These tools would limit the ability for governments and corporations from "snooping" on people's daily communications.[9] A notable figure that emerged from the cypherpunk movement was Julien Assange, the transparency crusader, who created Wikileaks, an expansion from the BlackNet project, which solicited secret information with the promise of encryption and payments in in untraceable digital money.[10] There were also other heinous offspring's of the cypherpunk movement, notably, Kuwabatake Sanjuro,

an anonymous market for assassinations. The Sanjuro market created a platform where anyone could anonymously contribute to a bounty that they would pay to have someone killed, remarkably this site had Ben Bernanke, the Chairman of the Federal Reserve, as having the highest bounty.[11] [12]

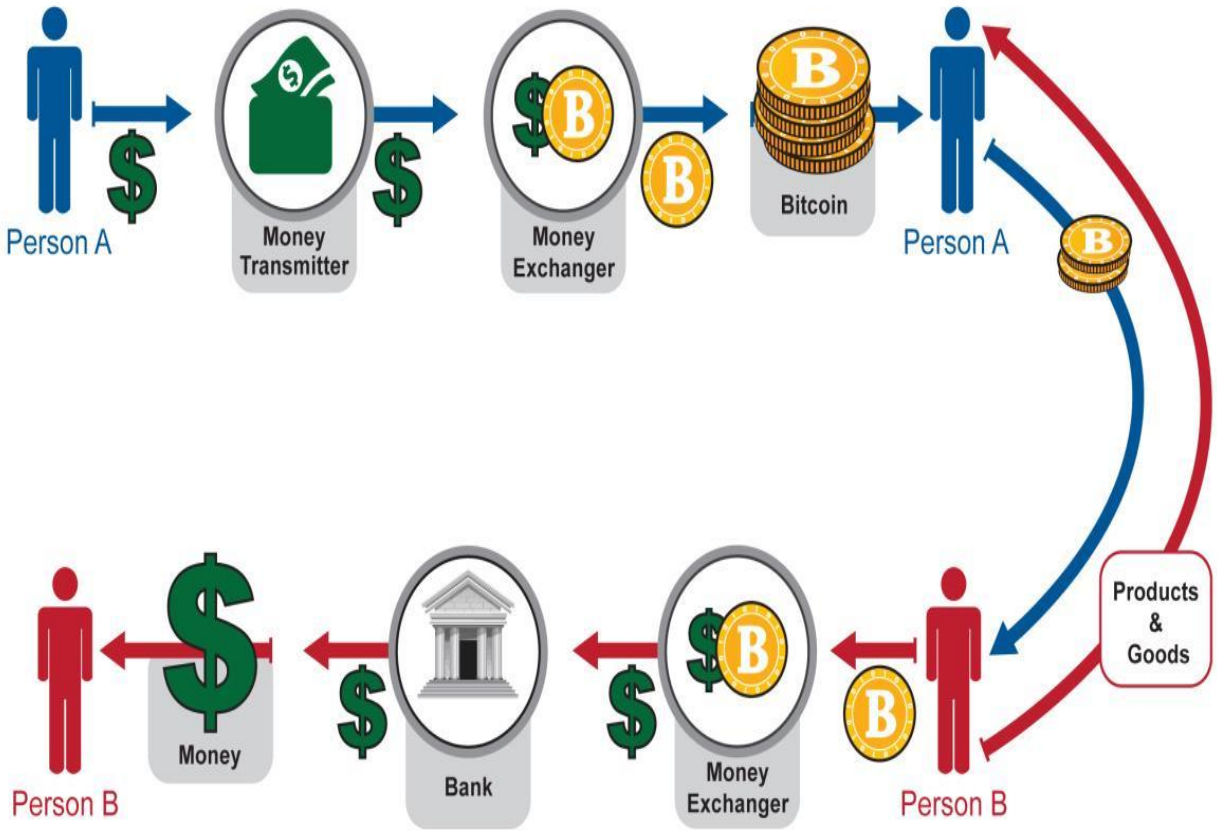
It is evident that there were good, questionable and even outrageous ideas that spawned from the cypherpunk movement, which was one of many. This was the bedrock from which Bitcoin emerged, fueled by the financial collapse of 2008. There are many descriptions of Bitcoin depending on who is asked or what aspect of this technology is considered. There are four general definitions for Bitcoin. First, it is a protocol or set of rules that govern how computers communicate with each other.[13] This protocol is how the universal distributed database (*the blockchain*) is parsed, and how transactions should be assembled and validated. [14] Second, is the network, which "is the peer-to-peer network to which nodes (*computers*) connect. Nodes in this peer-to-peer network exchange messages containing new blocks being added to the blockchain and new transactions being published to the universal network." [15] Third, is the currency, "a bitcoin, usually spelled with lower case 'b,' is a unit of the native currency of the Bitcoin network. There will be a total or max supply of roughly 21 million bitcoins created, mined, and issued. Although bitcoin is the main unit of account, each bitcoin is divisible into 100,000,000 pieces, called satoshis."[16] Last, is the open source implementation, which is the "the original open source project, written in C++ (*computer programming language*), implementing the protocol." [17] This is the segment of the technology that is open to everyone and a source of its growth over the years, due to its opensource nature allowing a collaborative community effort to implement updates, fixes and upgrades.

What some may not be aware of is that Bitcoin is underpinned by the blockchain technology, a universal ledger system. This is where the true innovation and disruptive dangers

lay that can affect various industries as introduced above. These range from banking and payments, cybersecurity, supply chain management, forecasting, networking, insurance, private transport and ride sharing, cloud storage, charity, voting, information management, government, public benefits, healthcare, energy management, online music, retail, real estate, and crowdfunding. Blockchain groups estimate that disruptions to the abovementioned fields could be realized within the next 5 to 10 years.[18] Considering the banking and finance industry, some like Dr. Henning Kehr an expert in the field of banking, deduces that "new technologies, such as the bitcoin blockchain, appear to be a viable solution in a lucrative position to revolutionize the financial sector just as the internet revolutionized the communication sector in the early 1990's."[19] Additionally, Dubai is aiming to integrate blockchain into their government infrastructure. Dubai wants all visa applications, bill payments, and license renewals to be transacted digitally via the blockchain by 2020.[20]

These are merely a few of the many examples of possible technological disruptions that span across all the industries listed above, many of which crossover into government infrastructure systems. Most of the current use cases of blockchain technology and cryptocurrencies revolve around currency applications. A simple illustration of a currency transaction between two individuals anywhere in the world can be found in figure 1. Here the steps highlight how money from person A can be transmitted from their bank to a money exchange for bitcoin then exchanged with person B for either products or goods. Person B can then exchange this money back into their desired currency, deposit it into their bank and go about their business. It should be stressed that many advocates of this technology maintain that once money is exchanged into a cryptocurrency, they have no reason to exchange it back to a bank recognized currency, essentially cutting out the

Figure 1 *Cryptocurrency Transaction*. Theguardianspro.com. January 2018. http://www.theguardianspro.com/how-bitcoin-works-and-how-its-worth-full



banking system and their respective oversight, protection and fees. This follows the notion of a crypto ecosystem, which involves retailers and customers.

Transactions like the ones above are not limited to Bitcoin alone; there are many alternative cryptocurrencies and tokens—used exclusively within an organization like a specific store credit—with proprietary uses. Within many circles, blockchain and cryptocurrency are widely regarded not only as an innovative technology but a genuine paradigm shift. A key vocal advocate of this technology is John McAfee, creator of McAfee computer security software systems. He believes it is a paradigm shift akin to the creations of the car, the airplane, the mobile phone, and even the internet which disrupted the horse and buggy, the transportation system, the telephone, and commerce, respectively. Conversely, others would regard these technological developments analogous to the Tulip mania of the 17th century—the first major financial bubble in which the

prices of tulip in the Netherlands ballooned up and crashed drastically bankrupting a majority of investors—or a new widespread Ponzi scheme taking the world by force and taking advantage of uninformed individuals.[21] Many government regulators and law enforcement officials around the world view this phenomenon as a safe haven for criminals that aim to use bitcoin and similar cryptocurrencies for "money laundering, illicit trade, and terrorism-related activities where users could hide under pseudo-anonymous identities, and stay under the radar for a long time before they get discovered."[22]

To get a holistic understanding of cryptocurrencies, the bedrock document that laid the foundation for bitcoin should be considered, which dates to the 2008 whitepaper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, anonymously written by an individual or group by the fictitious name Satoshi Nakamoto. Nakamoto, sought to present an alternative to the banking institution in light of the financial turmoil caused by the housing bubble collapse of 2007 and the subsequent bank bailouts frowned upon by many, which diminished trust in the financial establishment. Due to this loss of trust, many desired a more reliable monetary system, which was fertile ground for Bitcoin. Nakamoto proposed in his paper the foundation for what he believed was the need for an electronic payment system based on cryptographic proof instead of trust in a central banking entity susceptible to corruption, essentially allowing any two willing parties to transact directly with each other without the need for a trusted third party.[23] Nakamoto wrote:

> A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network

> itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.[24]

Essentially, he argued for using mathematical computations, cryptography, and computing power eliminating the middleman, which in this case were the banks, subsequently aiming to bypass many of the governmental oversight bodies, their respective regulations and charges. This would create a simple peer-to-peer version of electronic cash that would allow online payments to be sent from one party to another directly without having to go through a financial institution, as illustrated above in figure 1.[25] Adam Draper, a technology venture capitalist, fittingly described this concept by stating, "The Blockchain does one thing: It replaces third-party trust with a mathematical proof that something happened."[26] Furthermore, the record of all of these transactions would be recorded

Figure 2 *Distributed, Centralized, and Decentralization Comparison*. Dashbouquet.com. January 2018. https://dashbouquet.com/blog/blockchain/blockchain-solutions-the-way-to-transform-your-business-processes

on the blockchain, the decentralized, open and live public ledger, housed in various locations or nodes.

There are three types of frameworks when considering the types of systems that underpin how cryptocurrency or data is stored or shared. They are centralized systems, distributed systems and decentralized systems, illustrated in figure 2. A distributed system is not located in one location

but spread across many physical locations, with various part of the system holding key pieces of the data, however, a failure in key sections can cripple the system. A centralized system is dependent on a central location, an example being fiat currency, a legal tender whose value is backed by the government that issued it, like the U.S. Dollar, issued by the government with its supply managed by a central body; its dependence on a central source can also be a vulnerability given the reliance on a central location. A decentralized system has no central location; rather it maintains various functions, powers or things away from a central location or authority. Vitalik Buterin, the co-founder of Ethereum—the second largest blockchain distributed computing platform, asserts that there are three subtypes of decentralization: architectural decentralization, in which various physical computers are used; political decentralization, in which an individual or organization controls the computers; and logical decentralization, where the interface and data structures are independent of each other. A benefit of this type of system is the ability of the system to function with no operational loss, should parts of the network fail, or be cut in half for example.[27] The blockchain is a publicly shared immutable universal ledger that is cryptographically logged and stored encrypted data. It is shared among various individuals across the world, mostly those technologically inclined, willing to commit computing power. Transactions are contained in blocks which are linked together through a series of hash pointers, used to reference or link another piece of known information.

Another way to understand the blockchain logically, as illustrated in figure 3, is in seeing it as a triad of the known fields of 1) game theory, 2) cryptography science, and 3) software engineering. Separately, these fields have existed for a long time, but for the first time, they have together intersected harmoniously and morphed inside blockchain technology.[28] Blockchain, as noted above, extends in various areas that can be used to advance industries, but they can also

potentially hinder them as we will review below. Above a few industries were listed, however, blockchain technology can extend beyond them, a useful view is to consider six programmable concepts (assets, trust, ownership, money, identity, contracts) that can be used in any particular situation.[29]

Programmable Assets, namely digital assets "can be created, managed, and transferred on a blockchain network without incurring clearing-related delays due to the existence of intermediaries. Not requiring human or central database intervention to enforce verifiability is a

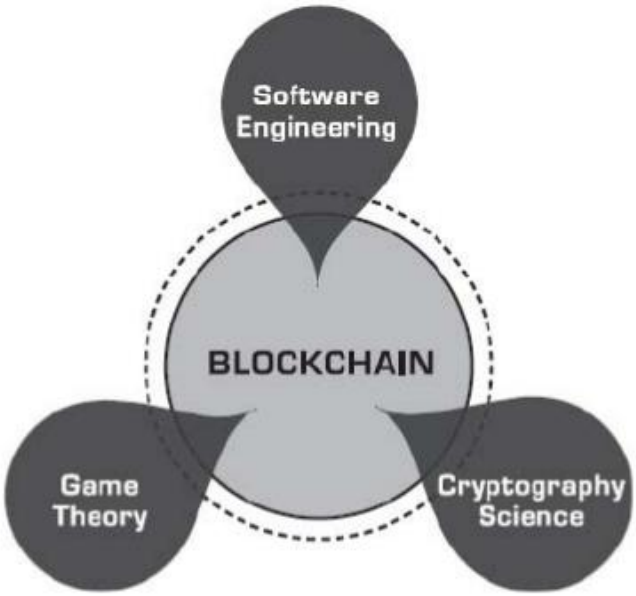


Figure 3 Vigna, Paul, and Michael J. Casey. *Blockchain*. In *The Age of Cryptocurrency*. New York, NY: St. Martin Press, 2015

fundamental novelty."[30] Programmable Trust inserts rules that represent trust inside transactions. Thus, the blockchain becomes a new way to validate these transactions via logic in the network, not via a database entry or central authority. Therefore, a new 'trust factor' is created that is part of the transaction itself."[31] Programmable Ownership enables the "blockchain to time-stamp documents representing rights or ownership, therefore providing irrefutable proofs that are cryptographically secure. This, in turn, can enable a variety of applications to be built on top of these new seamless verification capabilities."[32] Programmable Identity, offers "anonymous,

pseudonymous, or real identities that can be uniquely mapped on the blockchain, offering us the promise of owning our own identities, and not having them controlled by Google or Facebook. The vision of blockchain-based identity promises to empower users to be in complete control."[33] A more comprehensive illustration of the blockchain can be seen in figure 4, this example uses currency, but any data can be transmitted this way.

Mass Adoption

With a basic understanding of this technology and the various programmable areas that can affect different industries as noted above it is useful to understand how this technology might spread—this is also known as the diffusion of innovation. According to Everett Rogers, author of *Diffusion of Innovations*, diffusion is fundamentally how "innovation is communicated through certain channels over time among the members of a social system."[34] A significant aspect of innovation diffusion is how each member of a collective social system faces their respective

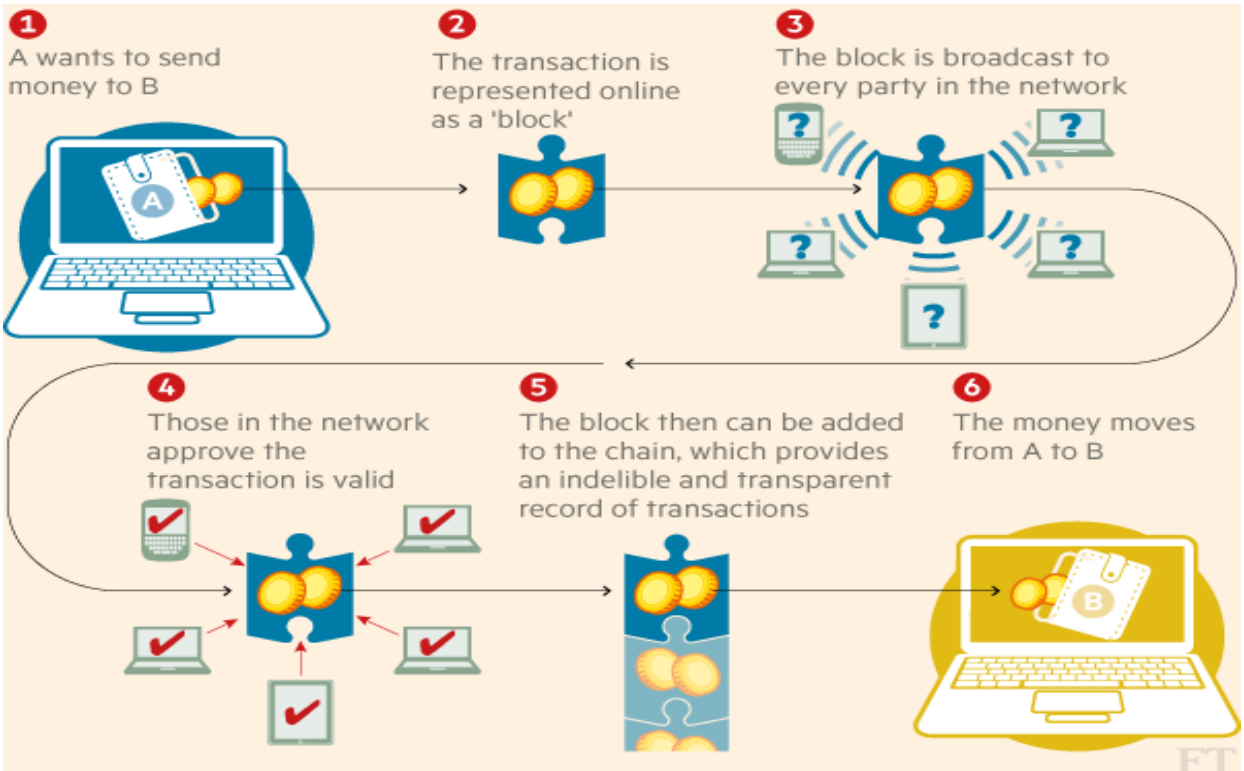


Figure 4 *Blockchain Overview*. Technofaq.com.com. January 2018. https://technofaq.org/posts/2016/08/blockchain-what-is-it-and-how-can-we-use-it/

innovation decision process or acceptance. Innovation decisions are believed to be made through a cost-benefit analysis when a great level of uncertainty exists as is the case with cryptocurrency and was the case with the internet; it is adopted as people believe that the innovation will enhance their utility, or rather provide a relative level of advantage to the status quo.[35] There are five general stages or groups individuals fall into when the adoption of a new technology is discussed, below illustrated in figure 5.

First, are the innovators, the small group of visionaries, the imaginative innovators who often spend excessive amounts of time, energy, and creativity on developing new ideas and gadgets. Second, are the early adopters, the ones on the lookout for apparent benefits of new technology and are quick to take leaps forward personally or professionally, making quick connections both in their personal needs or that of their businesses. Often, early adopters are quick to make connections between ingenious innovations that are hard for other to conceptualize. Third, are the early majority, the pragmatist, comfortable with moderate progressive ideas, but they will not leap without proof of proposed benefits. Fourth, are the late majority, the conservative pragmatists who dislike taking risks and are generally uncomfortable with new ideas. They are often influenced by the fears and opinions of the laggards. Last, are the laggards, the ones that will wait until the very end to embrace new things and are very risk adverse. Often the laggards are forced to assimilate or accept change once the change becomes the norm, for example those that hesitated the push toward the internet.[36]

Furthermore, Rogers also outlines a 5-step innovation decision process. First, is knowledge, which is when a person becomes aware of an innovation and has some idea of how it functions. Second, is persuasion, when a person forms a favorable or unfavorable attitude toward the innovation. Third, is decision, when a person engages in activities that lead to a choice to adopt or reject the innovation. Fourth, is implementation, when a person puts an innovation into use. Fifth, is confirmation, when a person evaluates the results of an innovation-decision already made.[37]

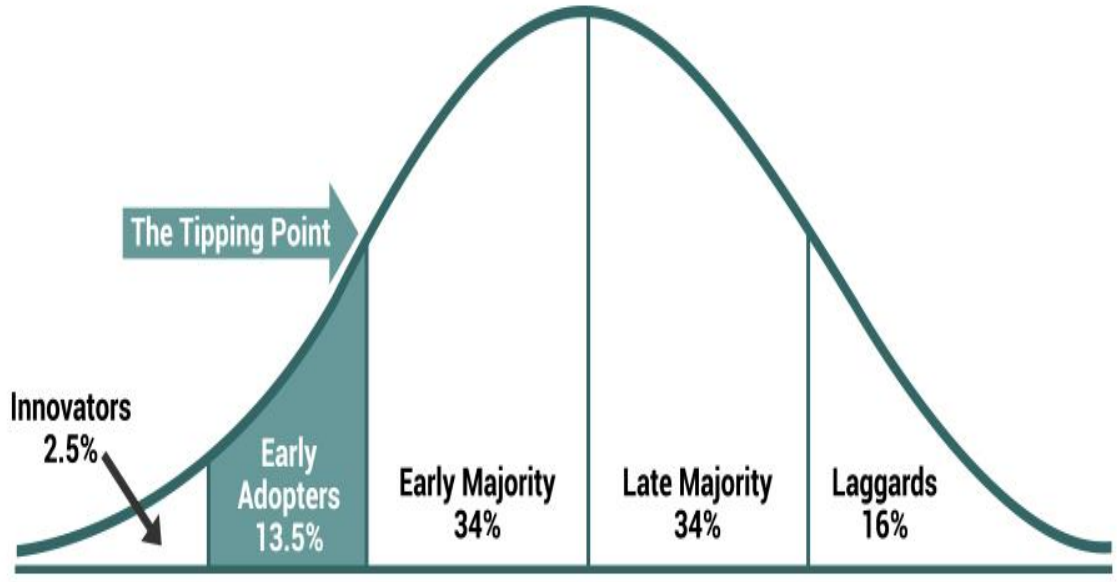


Figure 5 Rogers, Everett M. *Diffusion of Innovations*. In *Diffusion of Innovation*. New York: Free Press, 2003.

Remarkably, despite the various adoption groups useful in understanding how groups come to accept technological innovations, along with the innovation-decision process, there is a key role that opinion leaders play in accelerating the adoption process. Focusing on opinion leaders can speed up the rate of diffusion.[38] This is useful in leveraging how the masses adopt or disavow a technology. Arguably, regarding cryptocurrencies and blockchain, adoption is currently hovering between the innovators and early adopters stage. Many that fall into this category mean to do well and advance the narrative, but there is another side that must also be considered which is those that

seek to leverage these technological advancements for criminal or illegal motives. This leads to security implications for regulators and law enforcement officials, especially as the tipping point is crossed and adoption across the populace accelerates.

Emerging Threats in The Crypto Age

With a basic level of awareness of cryptocurrency and blockchain technology various use cases and the paths for adoption, many positives, can be inferred. This technology also potentially presents potential new threats that the U.S. government and law enforcement agencies, like the Department of Homeland Security (DHS), should pay attention to. The Rand Corporation has provided some key findings in their initial reports on the national security implication of virtual currencies and how non-state actors can potentially exploit these currencies. First, Rand assessed that, "non-state actors can use cryptocurrencies to disrupt sovereignty and increase their respective political and/or economic power."[39] Second, Rand assessed that, "decentralization affords more, though not total, resilience to disruptions from cyber-attacks; and the trend toward decentralized cyber service will only make it easier for unsophisticated cyber actors to have increasingly resilient access to cyber services, which is a two-way street that could enable unprecedented global access to information and communication services that, at its core, is agnostic to the national security interests of the United States." [40] These are alarming statements that lend more credence for this technologies disruptive capabilities, regardless of it being nascent.

From a homeland security perspective, the focus on information security has also been captured in the DHS' Strategic Plan. Specifically, the aim of the plan is to "continually increase and integrate domain awareness capabilities, as well as improve their ability to utilize vast amounts of intelligence and other information fully." [41] Additionally, deterrence and disruption of operations via the leveraging of intelligence along with, "information sharing, technological,

operational, and policy-making elements within DHS will facilitate a cohesive and coordinated operational response."[42]According to the Department of Homeland Security's 2014 Quadrennial Homeland Security Review, cyber threats are growing and "pose an ever-greater concern to our critical infrastructure systems as they become increasingly interdependent."[43] Furthermore, the mandate to DHS to "secure the Federal Government's information technology systems by approaching federal systems and networks as an integrated whole and by researching, developing, and rapidly deploying cybersecurity solutions and services at the pace that cyber threats evolve."[44] With technology advancing at the rate it is, cyber should not be the only concern, rather, as threats evolve, the position that the Department of Homeland Security should take is one that places attention, resources and funding to monitor, develop and ultimately leverage advancements in cryptocurrency and blockchain technology.

Criminals and terrorist of low to moderate technological sophistication are seeking ways to exploit cyber, cryptocurrencies or blockchain technology, this may give them the ability access more secure communications and other cyber services can make it increasingly difficult for the U.S. government to track and defeat them.[45] This aligns with the user maturity and experience dilemma, whereby there is an "increasing availability of well-designed cryptographic software—or, more generally, code—that was originally designed to support cryptocurrency, which can now be used by less sophisticated software developers to enable greater security," or undermine it.[46]

Considering how malign actors might use this technology across various industries as identified above, it further strengthens the need to train and equip law enforcement and counterterrorism professionals tasked with tracking and defeating these criminals, ensuring they more than a moderate level of technological sophistication. Most of the training in this space at best appears to be familiarity of the technology as shown within the Regional Organized Crime

Information Center's special research report titled, *Bitcoin and Cryptocurrencies: Law Enforcement Investigative Guide.* It covers an overview of what are cryptocurrencies, how they are used, a synopsis of alternative cryptocurrencies, an overview of blockchain technology, and a bitcoin investigative field guide.[47] Beyond a general orientation like this, training needs to address actual use of the various blockchain enabled programs, decentralized communication software, familiarity and hands on experience in the exchanges and information hubs of this space. This is no different than going beyond, for example, orientating drug enforcement agents to the various types of drugs, their classification and uses, then diving deeper into testing of substances, behavioral training to effectively deal with drug addicts, geographic orientation of high drug use areas and various tactics, training and protocols used by agents to effectively make arrest.

Regulatory and Security Concerns

While innovation may be trendy, interesting and exciting, there are significant issues and potential pitfalls that have arisen from this technology, regardless of the opinions of the crypto advocates. The creation of bitcoin, in essence, has slowly morphed into something much more significant than Nakamoto had ever envisioned. William Mougayar, a technology entrepreneur, referred to this metamorphosis as a "crypto-tech driven economy with its own value creation, not unlike the internet's own economy,"[48] which he dubbed the *cryptoconomy*. He further emphasized that this economy will not come from a takeover of current financial services, conversion of fiat money or recognized legal tender like the U.S. dollar, but rather by the creation of its own wealth, via new categories of services and businesses that extend beyond money transaction. [49] Herein lay many of the regulatory and security concerns that should not be ignored.

If within this new economy third-party oversight is absent, the question of safety and security must be addressed, regardless of the ideological views of the innovators pushing these

advancements. Don Tapscott, a technology and business leader, claimed that "governments that wish to repress the voices of citizens everywhere and have captured technologies like the Internet to silence dissidents and block outside media will find blockchain technology significantly more challenging."[50] While these views could be espoused by tyrannical regimes like Syria, China, and Russia for example that monitors closely or even close off outside media and information, this also would apply to democracies like the United States, Canada and other like-minded nations that have laws and regulatory bodies to ensure safety, compliance and encourage economic freedom. Furthermore, while many like Tyler Winklevoss, an early investor in Bitcoin, have decided to put their money and faith in a "mathematical framework that is free of politics and human error,"[51] this view dismisses the requirement for a free society to have political and human processes to maintains checks and balances. An extreme view of this virtual world would be to leave matters of the law to computer algorithms void of intelligent human input. However, the reality is that there are phases of adoption in any new technology and luckily cryptocurrency and blockchain technology is still for all intents and purposes a nascent technology.

Considering the diffusion of innovation phases discussed above, it would not be realistic for the government to be an innovator, though the National Security Strategy states otherwise, when it comes to some aspects of this technology, due in part to fiscal restraints. However, falling into the last group, the laggards, places those entrusted with drafting regulations and enforcing laws to be in a position of disadvantage. Criminals, however, will exploit technology to their benefit whenever possible. Some criminals have used cryptocurrencies to launder money, purchase and sell illegal drugs under the pretense that their activities are untraceable and completely anonymous which is not always the case. Though these technological advancements create means that the average criminal would not likely be able to develop on their own, they have learned to

use them for illegal means. That said, in the government, law makers and officials have begun taking notice.

The U.S. Senate Committee on Banking, Housing, and Urban Affairs convened on February 6, 2018, to hear statements from both the U.S. Securities and Exchange Commission (SEC) and the U.S. Commodity Futures Trading Commission (CFTC). CFTC Chairman Christopher Giancarlo testified that blockchain technology "promises enormous benefits to commercial firms and charities, it also promises assistance to financial market regulators in meeting their mission to oversee healthy markets and mitigate financial risk."[52] He goes on explain the difference this technology would have made during the financial crises of 2008; he claimed that the banks and even the securities exchange and other regulating bodies within the government would have had real-time trading data instead of having to piecemeal data as it was being taking place. Essentially, double spending and questionable lending practices could have been identified before they spiraled out of control. With an awareness of the benefit of this technology the stage is set for ways to potentially leverage this technology, which are currently being explored. However, because most of work in this space resides in the commercial space relationships need to be established with those who are creating these cutting-edge innovations.

The implications from a financial sector standpoint suggest leveraging this technology is worthy of further consideration, however, they arguably extend beyond the financial sector. Considering the increase over the past few years of hacks, data breaches, and theft, there are potential benefits that blockchain technology could produce to safeguard sensitive and critical government data better, moving away from current centralized frameworks. Notably, from a law enforcement perspective, the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations section recently announced they intend to make use of blockchain

technology to expose digital currency transactions made by illegal drug traffickers on what is known as darknet marketplaces in their efforts to combat the opioid crisis. Darknets are portions of the internet that have no active hosts and require specific software to be accessed. ICE has a goal to have more than 1,500 investigators trained on various forms of illicit payment networks and financial transactions.[53] This is an example of one agency taking steps to move forward in understanding and leveraging blockchain technology, but more needs to be done.

Future Concerns

Many nations are in discussion of the future of cryptocurrencies and blockchain technology, which will eventually lead to how they respond to it. The member countries of the G20, specifically, their finance ministers and central banking representatives met with the goal of sharing ideas and discussing blockchain technology and cryptocurrencies. They recognized their collective experience regulating a rapidly evolving technology market, along with their lessons learned. The consensus is that they are for the most part taking a hands-off approach and letting the technology mature so that it can flourish. This is positive but should be a warning that the sophistication and evolution of blockchain technology will continue, cautioning the United States to pay closer attention to this space.[54] The United States appears to be considering new laws, regulations and resolutions to strengthen the U.S. posture concerning cryptocurrency.

In the United States a significant Bill was introduced to the House is the Financial Technology Innovation and Defense Act—HR 4752, which seeks to "establish an Independent Financial Technology Task Force, to provide rewards for information leading to convictions related to terrorist use of digital currencies, to establish a FinTech Leadership in Innovation Fund to encourage the development of tools and programs to combat terrorism and illicit use of digital currencies, and for other purposes."[55] This Task Force consist of the Secretary of the Treasury who

will serve as the head of the task force, along with the Attorney General, the Director of the CIA, the Director of the Financial Enforcement Network, Director of the Secret Service, the Director of the Federal Bureau of Investigations and appointed private sector individuals. One critical aspect of this Bill is the proposed reward, which welcomes the crypto community to police up their space from bad actors, it states, "The Secretary of the Treasury, in consultation with the Attorney General to establish a program to pay a reward to any person who provides information leading to the conviction of an individual involved with terrorist use of digital currencies."[56] There needs to be means and avenues to share and disseminate the governments position and initiatives to gain support from the active users and those well versed in this space, similar to the common police *see something say something* initiatives. To gain traction in this space, there needs to be a deeper level of commitment from law makers and law enforcement officials to blockchain technology, which will result in a better reception from the crypto community that is hands-on and able to support the government's plans. This interactive relationship should facilitate communication and not create a "big brother is watching and here to take your toys away" feel, which is part of the narrative many within this space.

Noticeably, HR 4752 provides no inclusion of any representatives of the Department of Homeland Security, which is tasked with similar duties in another bill, the Homeland Security Assessment of Terrorists Use of Virtual Currencies Act—HR 2433, that were passed to the Senate. It authorizes the Under Secretary of Homeland Security for Intelligence and Analysis with "coordinating with appropriate Federal partners, to develop and disseminate a threat assessment regarding the actual and potential threat posed by individuals using virtual currency to carry out activities in furtherance of an act of terrorism, including the provision of material support or resources to a foreign terrorist organization.[57] This again furthers the need to allocate resources

and personnel from within DHS to ensure they not only understand the landscape but are well versed to ensure it fulfills its mission of thwarting any use of this technology to elicit threats to the homeland. Most of the language in these proposed Bills makes little mention of training U.S. government personnel to specialize in this technology compared to cyber security specific Bills.

Conclusion

As blockchain technology and cryptocurrencies become more advanced, and mass adaption on a global scale continues to materialize the concepts of deeper research, familiarization and training in blockchain technology and cryptocurrencies, introduced here should be closely monitored and studied by regulating and law enforcement agencies. The United States and key law enforcement agencies must take a forward-thinking posture with the goal of understanding the blockchain and cryptocurrency space. While it is possible to manage and mitigate threats within this space successfully, the level of sophistication and expertise of law enforcement and security professionals should increase beyond familiarity. This shift toward decentralized blockchain operations which will enhance cyber operations will potentially empower the relatively unsophisticated cyber actors to have access to increasingly sophisticated cyber services. The national security community will have to contend with the challenge of thwarting these cyber actors over the coming years.[58] It is helpful to recognize this reality as it is becoming a reality so that the appropriate steps can be taken to leverage these advancements going forward.

Regarding information, the potential free flow of information that may very well come from "uninterruptible news sites and web forums, breaking down national firewalls, such as China's Great Firewall, but also enable even greater access to extremist rhetoric and tactics"[59] is a paradigm shift that requires the United States change its views on this subject and how it assess the enemy both domestically and even abroad. Leveraging this technology would also enable the

United States to defeat international censorship, thereby enabling the projection of American propaganda to countries that were previously denied such information.[60]Conversely, this also will enable malign and terrorism propaganda to be spread and accessed by populations that were inaccessible.

Regardless of the views or positions held when it comes to the subject of cryptocurrencies, the reality is that this dimension or crypto space, which totaled a market capitalization of over 800 Billion dollars in January 2018, should not be ignored. There are many benefits as we have briefly covered but there are also dangers and new possible threats.

Subscribing to the National Security Act and the mission of DHS for example, of securing of the homeland, innovations in decentralized technology must be considered, not minimized to a temporary bitcoin phenomenon. Priority should be given to collaboration with inventors and innovators within industry and academia. The aim of the United States to leverage private expertise to build and innovate, requires as stated in the National Security Strategy, that the "United States regain the element of surprise and field new technologies at the pace of modern industry…government agencies must shift from an archaic R&D process to an approach that rewards rapid fielding and risk-taking."[61]

A whole-of-government approach requires that not only a few agencies like ICE work toward these goals but that DHS and other key agencies—FBI, Department of Treasury, Securities and Exchange Commission, not only take steps to understand and embrace this technology, exploiting where possible the potential benefits but also explore ways to effectively leverage it against adversaries aiming to exploit its capabilities to threaten and attack the homeland across the various forms of industries and technology. This phenomenon extends beyond bitcoin to the blockchain and warrants that options for the road ahead be considered and discussed. Working

groups comprised from the various regulatory and law enforcement agencies should be assembled along with leaders from within the blockchain space, that are on the cutting edge of new breakthroughs to establish new ways to nurture innovation while ensuring criminal and terrorist activities are combated effectively, so that present and future security implications of blockchain technology are mitigated.

Endnotes

[1] Trump, "National Security Strategy," 20.

[2] Morris, “Bitcoin Hits a New Record High.”
[3] Future Thinkers, “Industries the Blockchain Will Disrupt.”
[4] Roberts, “Silk Road.”
[5] Dictionary.com, “Cryptography.”
[6] Levy, “E-Money.”
[7] *Ibid*.
[8] Vigna and Casey, *The Age of Cryptocurrency*, 49.
[9] *Ibid*, 51.
[10] *Ibid*, 42.
[11] Greenberg, “Assassination Market.”
[12] Vigna and Casey, *The Age of Cryptocurrency*, 42.
[13] Merriam-Webster, “Protocol.”
[14] Franco, Understanding Bitcoin, 18.
[15] *Ibid*.
[16] *Ibid*, 19.
[17] *Ibid*.
[18] Future Thinkers, “Industries the Blockchain Will Disrupt.”
[19] Kehr, Tonkin, and Bihler, “The Unbanked.”
[20] D’Cunha, “Dubai.”
[21] Shane, “Tulip Mania: Bitcoin Vs History's Biggest Bubbles.”
[22] Mougayar and Buterin, The Business Blockchain, 53.
[23] Nakamoto, “Bitcoin.”
[24] *Ibid.*
[25] Mougayar and Buterin, The Business Blockchain, 21.
[26] Kendall, “Whatever Happened to Bitcoin?”
[27] Buterin, “The meaning of Decentralization.”
[28] Mougayar and Buterin, *The Business Blockchain*, 26.
[29] *Ibid*, 48.
[30] *Ibid*.
[31] *Ibid*.
[32] *Ibid*.
[33] *Ibid*.
[34] Rogers, *Diffusion of Innovations*, 5.
[35] *Ibid*, 208.
[36] *Ibid*, 262.
[37] *Ibid*, 163.
[38] *Ibid*, 331.
[39] Baron, “Virtual Currency,” 2.
[40] *Ibid*, xiv.
[41] Department of Homeland Security Strategic Plan: Fiscal Years. 2014-18.
[42] *Ibid*.
[43] Department of Homeland Security, “Quadrennial Homeland Security Review.”
[44] *Homeland Security Act of 2002*, (2015).
[45] Baron, “Virtual Currency,” 62.
[46] *Ibid*.
[47] Regional Organized Crime Information Center, “Bitcoin.”

[48] Mougayar, "How the Cryptoconomy Will Be Created."
[49] *Ibid*.
[50] Boring, "Blockchain Revolution."
[51] Guard, "Bitcoin Blockchain Thoughts."
[52] U.S. Senate Committee on Banking, Housing, & Urban Affairs, "Virtual Currencies."
[53] Nevano, "*Combating the Opioid Crisis.*"
[54] Torque Capital Partners, "G20 Member States."
[55] Financial Technology Innovation and Defense Act. HR 4752. 115th Cong., (Introduced to the House, January 10, 2018).
[56] *Ibid*
[57] Homeland Security Assessment of Terrorists Use of Virtual Currencies Act. HR 2433. 115th Cong., (Referred to the Senate, September 13, 2017).
[58] Baron, "Virtual Currency," 64.
[59] *Ibid,* 65.
[60] *Ibid*
[61] Trump, "National Security Strategy," 21.

Bibliography

Baron, Joshua, Angela O'Mahony, David Manheim, and Cynthia Dion-Schwarz. *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actor Deployment*. RAND Corporation, 2015. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf

Buterin, Vitalik. "The Meaning of Decentralization." Medium. Last modified February 6, 2017. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

D'Cunha, Suparna D. "Dubai Sets its Sights on Becoming the World's First Blockchain-Powered Government." Forbes. Last modified December 18, 2017. https://www.forbes.com/sites/suparnadutt/2017/12/18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/#58a91b05454b.

Department of Homeland Security Strategic Plan: Fiscal Years. 2014-18. *United States. Department of Homeland Security*. 2014. https://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.

Department of Homeland Security. *2014* Quadrennial Homeland Security Review. 2014. http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA596238.

Dictionary.com. "Cryptography." Dictionary.com. Accessed April 10, 2018. http://www.dictionary.com/browse/cryptography?s=t.

Franco, Pedro. *Understanding Bitcoin: Cryptography, Engineering, and Economics*. Chichester: Wiley, 2015.

Future Thinkers. "19 Industries the Blockchain Technology Will Disrupt." Future Thinkers Podcast. Last modified February 24, 2018. https://futurethinkers.org/industries-blockchain-disrupt/.

Greenberg, Andy. "Meet The 'Assassination Market' Creator Who's Crowdfunding Murder with Bitcoins." Forbes. Last modified February 3, 2014. https://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/#4efa59103d9b.

Homeland Security Act of 2002. September 22, 2015. https://www.dhs.gov/homeland-security-act-2002.

Kehr, Henning, Graham Tonkin, and Reiner Bihler. "The Unbanked Don't Need More Brick and Mortar Banks." Shaping the Digital Enterprise, 2016, 139-156. doi:10.1007/978-3-319-40967-2_7.

Kendall, Marisa. “Whatever Happened to Bitcoin? Adam Draper Has the Answer.” The Mercury News. Last modified November 12, 2016. https://www.mercurynews.com/2016/11/11/whatever-happened-to-bitcoin-adam-draper-has-the-answer/.

Levy, Steven. “E-Money (That's What I Want).” WIRED. Last modified December 1, 1994. https://www.wired.com/1994/12/emoney.

Merriam-Webster. “Definition of Protocol.” Dictionary by Merriam-Webster: America's Most-trusted Online Dictionary. Accessed March 19, 2018. https://www.merriam-webster.com/dictionary/protocol.

Morris, David Z. “Bitcoin Hits a New Record High, But Stops Short of $20,000.” Fortune. Last modified December 17, 2017. http://fortune.com/2017/12/17/bitcoin-record-high-short-of-20000.

Mougayar, William, and Vitalik Buterin. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Hoboken: John Wiley & Sons, Inc., 2016.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. https://bitcoin.org/bitcoin.pdf.

Nevano, Greg. “Combating the Opioid Crisis.” Immigration Customs Enforcement. Last modified March 16, 2018. https://www.ice.gov/features/opioid-crisis.

Regional Organized Crime Information Center. *Bitcoin and Cryptocurrencies: Law Enforcement Investigative Guide*. Regional Organized Crime Information Center, 2018. http://www.riss.net.

Roberts, Jeff J. “Judge Sinks Dread Pirate of Silk Road with Life Sentence.” Fortune. Last modified May 29, 2015. http://fortune.com/2015/05/29/ulbricht-sentenced-silk-road-crimes.

Rogers, Everett M. *Diffusion of Innovations*. 5th Ed. ed. New York: Free Press, 2003.

Shane, Daniel. “Tulip Mania: Bitcoin Vs History's Biggest Bubbles.” CNNMoney. Last modified December 8, 2017. http://money.cnn.com/2017/12/08/investing/bitcoin-tulip-mania-bubbles-burst/index.html.

Torque Capital Partners. “A Snapshot of Current Crypto Regulations of All G20 Member States.” Medium. Last modified March 14, 2018. https://medium.com/@Torquecapital/a-snapshot-of-current-crypto-regulations-of-all-g20-member-states-3b5f80ffac81.

Trump, Donald. *National Security Strategy of the United States*. Washington, DC: White House, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

US Congress. House. Financial Technology Innovation and Defense Act. HR 4752. 115th Cong., (Introduced to the House, January 10, 2018).

US Congress. House. Homeland Security Assessment of Terrorists Use of Virtual Currencies Act. HR 2433. 115th Cong., (Referred to the Senate, September 13, 2017).

Vigna, Paul, and Michael J. Casey. *The Age of Cryptocurrency How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York, NY: St. Martin Press, 2015.