



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**CRYPTOCURRENCY AND STATE SOVEREIGNTY**

by

Ryan L. Frebowitz

June 2018

Thesis Advisor:  
Second Reader:

Shannon A. Brown  
Erik J. Dahl

**Approved for public release. Distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
<b>1. AGENCY USE ONLY</b> (Leave blank)	<b>2. REPORT DATE</b> June 2018	<b>3. REPORT TYPE AND DATES COVERED</b> Master's thesis		
<b>4. TITLE AND SUBTITLE</b> CRYPTOCURRENCY AND STATE SOVEREIGNTY			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Ryan L. Frebowitz				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release. Distribution is unlimited.			<b>12b. DISTRIBUTION CODE</b> A	
<b>13. ABSTRACT (maximum 200 words)</b>  Since Bitcoin's release in late 2008, the cryptocurrency has grown and proven itself as a disruptive technology, resistant to sovereign law and international financial regulations, and an alternative to the sovereign state's concept of fiat money. The Wild West nature of cryptocurrency has enabled a number of individuals, criminal organizations, terrorist groups, and sovereign states to use Bitcoin, among other cryptocurrencies, to avoid detection, interference, or punishment from regulatory agencies to commit actions such as money laundering, trafficking narcotics, purchasing weapons, and bypassing international sanctions. This thesis addresses the disruptive nature of cryptocurrency by asking what legislative options are available to sovereign states to maximize the effectiveness of sovereign laws while limiting undesired cryptocurrency use. To tackle this question, this thesis breaks down the legislative actions countries may take into three categories—prohibition, regulation, and adoption—to investigate the benefits, limitations, and effects of each policy. By examining the legislative actions of countries like China, the United States, and Russia, this thesis finds that sovereign states have had limited success in preventing illicit cryptocurrency use; however, without implementing a refined, multifaceted global regulatory standard on cryptocurrency transactions in the near future, cryptocurrency will remain an unchecked means to transact on an international scale.				
<b>14. SUBJECT TERMS</b> cryptocurrency, cryptocurrencies, virtual currency, virtual currencies, Bitcoin, state sovereignty, banning cryptocurrency, economic and financial regulations, adopting cryptocurrency, blockchain			<b>15. NUMBER OF PAGES</b> 123	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UU	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release. Distribution is unlimited.**

**CRYPTOCURRENCY AND STATE SOVEREIGNTY**

Ryan L. Frebowitz  
Lieutenant, United States Navy  
BS, The Citadel, 2011

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES  
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL  
June 2018**

Approved by: Shannon A. Brown  
Advisor

Erik J. Dahl  
Second Reader

Mohammed M. Hafez  
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Since Bitcoin's release in late 2008, the cryptocurrency has grown and proven itself as a disruptive technology, resistant to sovereign law and international financial regulations, and an alternative to the sovereign state's concept of fiat money. The Wild West nature of cryptocurrency has enabled a number of individuals, criminal organizations, terrorist groups, and sovereign states to use Bitcoin, among other cryptocurrencies, to avoid detection, interference, or punishment from regulatory agencies to commit actions such as money laundering, trafficking narcotics, purchasing weapons, and bypassing international sanctions. This thesis addresses the disruptive nature of cryptocurrency by asking what legislative options are available to sovereign states to maximize the effectiveness of sovereign laws while limiting undesired cryptocurrency use. To tackle this question, this thesis breaks down the legislative actions countries may take into three categories—prohibition, regulation, and adoption—to investigate the benefits, limitations, and effects of each policy. By examining the legislative actions of countries like China, the United States, and Russia, this thesis finds that sovereign states have had limited success in preventing illicit cryptocurrency use; however, without implementing a refined, multifaceted global regulatory standard on cryptocurrency transactions in the near future, cryptocurrency will remain an unchecked means to transact on an international scale.

THIS PAGE INTENTIONALLY LEFT BLANK



## TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>MAJOR RESEARCH QUESTION.....</b>	<b>1</b>
<b>B.</b>	<b>SIGNIFICANCE OF THE RESEARCH QUESTIONS .....</b>	<b>2</b>
<b>C.</b>	<b>LITERATURE REVIEW .....</b>	<b>3</b>
1.	Illicit Uses of Bitcoin and Other Cryptocurrencies .....	4
2.	U.S. Regulation of Cryptocurrencies .....	10
3.	International Regulatory Propositions to Regulate Cryptocurrencies.....	13
<b>D.</b>	<b>POTENTIAL EXPLANATIONS .....</b>	<b>16</b>
<b>E.</b>	<b>RESEARCH DESIGN .....</b>	<b>16</b>
<b>F.</b>	<b>THESIS OVERVIEW AND DRAFT CHAPTER OUTLINE .....</b>	<b>17</b>
<b>II.</b>	<b>CRYPTOCURRENCIES AND THE BLOCKCHAIN .....</b>	<b>19</b>
<b>A.</b>	<b>BITCOIN AND “TRUST” .....</b>	<b>21</b>
<b>B.</b>	<b>SECURITY IN BITCOIN: HASH FUNCTIONS, MERKLE TREES, AND THE BLOCKCHAIN.....</b>	<b>22</b>
<b>C.</b>	<b>DECENTRALIZED PUBLIC LEDGER AND THE BITCOIN NETWORK: MINING AND NODES.....</b>	<b>26</b>
<b>D.</b>	<b>TRANSACTIONING WITH BITCOIN: VIRTUAL WALLETS, CRYPTOCURRENCY EXCHANGES, THE BITCOIN ECOSYSTEM, AND OTHER CRYPTOCURRENCIES .....</b>	<b>31</b>
1.	Virtual Wallets and Transactions .....	31
2.	Bitcoin Exchanges and the Cryptocurrency Ecosystem.....	33
3.	Other Cryptocurrencies .....	35
<b>E.</b>	<b>CONCLUSION .....</b>	<b>36</b>
<b>III.</b>	<b>BANNING CRYPTOCURRENCIES .....</b>	<b>37</b>
<b>A.</b>	<b>WHY STATES CHOOSE TO BAN VIRTUAL CURRENCIES.....</b>	<b>37</b>
1.	Bitcoin and Crime .....	38
2.	Increase the State’s Capital Controls.....	39
3.	To Limit Civil Rights .....	40
4.	To Introduce a State-backed Cryptocurrency .....	41
5.	To Eliminate the Excessive Energy Consumption in Mining .....	42
<b>B.</b>	<b>MECHANISMS TO BAN VIRTUAL CURRENCIES .....</b>	<b>43</b>
<b>C.</b>	<b>COUNTRIES THAT HAVE BANNED CRYPTOCURRENCIES. ....</b>	<b>44</b>

1.	Countries That Have Banned Bitcoin: Bangladesh, Bolivia, Ecuador, Kyrgyzstan, and Nigeria .....	45
2.	China .....	46
3.	A Partial Ban in Iceland.....	48
D.	THE EFFECTS OF BANNING CRYPTOCURRENCY .....	49
1.	China’s Impact on Cryptocurrencies .....	50
2.	Other States’ Effect in Banning Cryptocurrencies .....	52
3.	Banning Cryptocurrency Internationally .....	53
E.	CONCLUSION.....	53
IV.	THE REGULATION OF CRYPTOCURRENCY .....	55
A.	THE RATIONAL TO REGULATE VIRTUAL CURRENCIES .....	56
1.	Consumer Protection .....	56
2.	Money Laundering.....	56
3.	To Protect Monetary Policy .....	57
B.	DIFFICULTIES OF REGULATING CRYPTOCURRENCIES.....	57
C.	METHODS OF REGULATING CRYPTOCURRENCY .....	58
1.	Informational and Moral Suasion .....	59
2.	The Regulation of Specific Stakeholders .....	59
3.	Interpretation of Existing Regulations.....	59
4.	The Creation of Broader Regulation.....	60
D.	SELECTIVE SUMMARY OF CURRENT CRYPTOCURRENCY REGULATION .....	60
1.	The United States .....	60
2.	Regulation in the European Union.....	66
3.	International Regulation .....	67
E.	CONCLUSION .....	67
V.	THE ADOPTION OF CRYPTOCURRENCIES BY SOVEREIGN STATES .....	69
A.	REASONS FOR STATES TO USE CRYPTOCURRENCY .....	69
1.	To Incorporate the Unbanked .....	69
2.	Cheaper Transaction Costs.....	70
3.	To Bypass Sanctions .....	72
4.	The Auditability of Cryptocurrency .....	72
B.	STATES THAT ACCEPT, PLAN TO ADOPT, OR HAVE ISSUED STATE-BACKED CRYPTOCURRENCIES .....	73
1.	The Venezuelan Petro.....	73
2.	The Russian “CryptoRuble” .....	75

3.	Countries where Bitcoin Have Become the Trusted Currency .....	78
4.	The U.S. Fedcoin .....	80
5.	Other Countries Studying or Developing Cryptocurrencies.....	82
C.	POTENTIAL CHALLENGES TO ADOPTING CRYPTOCURRENCY .....	83
D.	CONCLUSION .....	87
VI.	CONCLUSION .....	89
A.	FINDINGS .....	90
B.	POLICY RECOMMENDATIONS .....	92
1.	Redefine Cryptocurrency .....	92
2.	New International Standards on Cryptocurrency Regulation.....	93
C.	RECOMMENDATIONS FOR FURTHER RESEARCH .....	93
D.	CONCLUSION .....	94
	LIST OF REFERENCES .....	95
	INITIAL DISTRIBUTION LIST .....	105

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

Figure 1.	A SHA256 Hash Generated from the Phrase “Naval Postgraduate School” .....	24
Figure 2.	The Hash Structure of the Block Chain and Merkle Tree .....	25
Figure 3.	Visual Differences between Centralized, Decentralized, and Distributed Networks. ....	27
Figure 4.	A Chain of Transactions Depicting the Ownership of Bitcoins with Public Keys and Private Keys .....	32
Figure 5.	“A Schematic Depiction of the Money Flow into and from CryptoRuble” .....	77

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS AND ABBREVIATIONS

AML	anti-money laundering
BIS	Bank for International Settlements
BSA	Bank Secrecy Act
BTC	Bitcoin
CEA	Commodity Exchange Act
CFTC	Commodity Futures Trading Commission
CPMI	Committee on Payments and Market Infrastructure
CRS	Congressional Research Service
CTF	counter-terrorist financing
DEA	Drug Enforcement Agency
DVC	decentralized virtual currencies
ECB	European Central Bank
ESMA	European Security and Markets Authority
EU	European Union
FBI	Federal Bureau of Investigations
FinCEN	Financial Crimes Enforcement Network
ICO	initial coin offering
IMF	International Monetary Fund
IRS	Internal Revenue Service
IS	Islamic State
OFAC	Office of Foreign Assets Control
PBoC	Peoples Bank of China
TCO	transnational criminal organizations
SEC	Security and Exchange Commission
SHA	secure hash algorithm
USD	U.S. dollars
VC	virtual currencies

THIS PAGE INTENTIONALLY LEFT BLANK



## **ACKNOWLEDGMENTS**

I would like to thank both my thesis advisor, Dr. Shannon Brown, and second reader, Dr. Erik Dahl, for their immeasurable guidance, time, expertise, and supervision during the thesis process. Without the input and assistance of Dr. Brown and Dr. Dahl, this academic achievement would not have been possible. To my girlfriend, Sophia, thank you for your unwavering patience and support; you made this accomplishment possible. I would also like to thank Dr. Carolyn Halladay for her leadership as my program academic associate and her advice in pursuit of my thesis topic. Finally, I would like to thank Carla, Chloe, Sasan, and Kate of the NPS Graduate Writing Center for their tireless aid in brainstorming, editing, and altering my chapters as I struggled toward a finished thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. MAJOR RESEARCH QUESTION

On October 31, 2008, the pseudonymous Satoshi Nakamoto released his proposal for an electronic cash system known as Bitcoin.<sup>1</sup> In the nine years that have passed since Bitcoin's proposal, Bitcoin<sup>2</sup> and other cryptocurrencies have gained popularity in the international community as a medium of transaction transcending current financial institutions and cross-border regulations. Additionally, state governments, banks, and investors have shown an increasing interest in using cryptocurrencies to enhance their own financial capabilities. Furthermore, because the blockchain technology used in cryptocurrency allows its users to "transact directly without the need for a trusted third party," the payee and recipient in transactions remain anonymous outside of their digital wallet signature.<sup>3</sup>

Despite the advantages that Bitcoin and other cryptocurrencies offer in the marketplace, cryptocurrencies also generate new sets of obstacles for international financial institutions and state governments regulating or monitoring transactions. The pseudonymity<sup>4</sup> provided to the users by cryptocurrencies, coupled with the ease of transaction, has proved to be a reliable tool for non-state and criminal networks pursuing methods to bypass taxes, governmental regulations, and international sanctions.

The questions in this thesis are built upon the premise that cryptocurrencies offer new and unprecedented challenges to sovereign states' ability to regulate and enforce laws governing its monetary policy, security, and trade; therefore, the state—and by extension the international community—will endeavor to develop policies to increase sovereign

---

<sup>1</sup> Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (white paper, Bitcoin, 2008), 1, <https://bitcoin.org/bitcoin.pdf>.

<sup>2</sup> In the literature reviewed, there is no standard among authors on whether Bitcoin is capitalized or not. For this thesis, the term *Bitcoin* is capitalized when discussing the cryptocurrency as a technology, system, or network, while units of the cryptocurrency as measurements of wealth or transaction costs use a lower case "b". This distinction is discussed in greater detail in Chapter II.

<sup>3</sup> Nakamoto, 1–2.

<sup>4</sup> The concept of pseudonymity (or pseudo-anonymity) is discussed in greater detail in Chapter II.

states' control on the use of cryptocurrency. The questions this thesis seeks to answer are: What options are available to the sovereign state to limit cryptocurrency's capacity to challenge domestic and international laws? What allows cryptocurrency to sidestep the established financial order and enforcement institutions? What are the challenges sovereign states face when introducing cryptocurrency legislation? Finally, as cryptocurrency technology becomes more popular and countries begin developing their own blockchain-based tools, what factors will inhibit or promote a sovereign state from developing their own sovereign cryptocurrency?

## **B. SIGNIFICANCE OF THE RESEARCH QUESTIONS**

Cryptocurrencies like Bitcoin challenge the post-Bretton Woods system of financial control on worldwide transactions. The bitcoin currency is decentralized and therefore is neither issued by any government nor stored in any one location. Decentralized currencies like Bitcoin utilize a distributed public ledger, barring the need for a trusted third party.<sup>5</sup> With cryptocurrencies, mints do not “print” cryptocurrency, banks are not required to store cryptocurrency, and escrow agents are unnecessary to verify transactions. To many consumers, decentralized cryptocurrency appears to be a superior method of transaction in terms of efficiency and transaction cost; however, to a state, the removal of the trusted and regulated third party carries significant drawbacks concerning government's control of commerce.

Since the emergence of Bitcoin, cryptocurrencies have weakened sovereign governments' capacity to protect their citizens from harm because they sidestep the regulations that monitor monetary transactions. During normal fiat<sup>6</sup> transactions, trusted third parties like banks, credit card companies, or escrow agents restrict and report transactions with ties to criminal or terrorist entities. As a result, individuals and organizations transacting with fiat are required to register with trusted third parties,

---

<sup>5</sup> Decentralized or distributed public ledgers are explained in Chapter II detailing how cryptocurrencies function.

<sup>6</sup> According to Investopedia, the definition of “Fiat money is currency that a government has declared to be legal tender, but it is not backed by a physical commodity” (e.g., the U.S. dollar). Brent Radcliffe, “Fiat Money,” Investopedia, November 20, 2003, <https://www.investopedia.com/terms/f/fiatmoney.asp>.

providing personal information to assist authorities in tracking and prosecuting individuals who commit illegal activities. Cryptocurrencies like Bitcoin bypass the difficulties in transactions that state governments have put in place to prevent illegal actions.

Herein lies the problem. Cryptocurrencies do not operate within the existing financial system, and the existing banking agreements and laws are unprepared to challenge cryptocurrency use. To counter illicit use, sovereign states must create new laws across the existing state and international financial institutions to limit cryptocurrency transactions. However, in the development of new legislation, lawmakers will be forced to wrestle between the limitations of sovereign laws on cryptocurrency and the needs of domestic and homeland security. Likewise, the government's pursuit of new laws will likely be restrained by the protection of liberties guaranteed to the citizens the anonymity inherent cryptocurrency's blockchain. Therefore, the significance of this thesis's research questions is to highlight the evolving challenges that sovereign states will encounter as cryptocurrencies become more mainstream. This thesis also analyzes the potential avenues of interaction and partnership between the existing financial intuitions and regulatory bodies as they seek to limit, regulate, and standardize transactions utilizing cryptocurrencies.

### C. LITERATURE REVIEW

The bulk of the literature available on cryptocurrency adoption is relatively new, with the first scholarly articles debuting in the years following Bitcoin traction as a traded commodity and method of transaction in 2011.<sup>7</sup> Most of the literature available also refers solely to Bitcoin, or uses the terms cryptocurrency and Bitcoin interchangeably. This is because Bitcoin is the first virtual currency to rely on *cryptography* as a means of security while implementing a *public distributed ledger* to track transactions (Chapter II of this thesis explains both ideas).<sup>8</sup> As of early 2018, there are nearly 1500 public

---

<sup>7</sup> Paul Vigna and Michael Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging The Global Economic Order* (New York: St. Martin's Press, 2015), 83–84.

<sup>8</sup> Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton, NJ: Princeton University Press, 2016), 1, 242.

cryptocurrencies, totaling a market cap of more than half a trillion dollars.<sup>9</sup> As noted in a 2017 study by the Cambridge Centre for Alternate Finance, there are “over 300 academic articles on the various aspects of bitcoin and other cryptocurrencies over the past several years.”<sup>10</sup> This thesis’s literature review surveys various authors’ studies and opinions relating to the illicit history of cryptocurrency and the role states and international institutions should take regarding cryptocurrency transactions.

The first section briefly covers the literature available on the historical use of Bitcoin as a means to conduct illegal transactions and bypass financial regulations. This section outlines some of the encounters law enforcement has had with cryptocurrency, and the methods cryptocurrency users have employed to bypass existing laws. The second section builds on the history of illegal activity using cryptocurrency and presents the literature detailing how the United States can potentially regulate cryptocurrencies within its existing legal frameworks. The third and final section expands upon the second by examining literature attempting to tackle cryptocurrency implementation on a global scale through the use of international financial institutions and international agreements.

## **1. Illicit Uses of Bitcoin and Other Cryptocurrencies**

A survey of recent research establishes that the lack of regulation in cryptocurrency has become a homeland security concern in addition to being a criminal one. In academia, there is little debate among scholars that individuals use cryptocurrencies to circumvent laws and commit illegal activities. Various publications from U.S. government reports and their various funded research groups to scholars and writers following the emerging cryptocurrency trends around the globe all acknowledge this. Furthermore, because cryptocurrency offers a combination of trust in value, anonymity, lack of regulation, and

---

<sup>9</sup> “Cryptocurrency Market Capitalizations,” CoinMarketCap, accessed March 5, 2018, <https://coinmarketcap.com/>.

<sup>10</sup> Garrick Hileman and Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (Cambridge: University of Cambridge Centre for Alternate Finance, 2017), [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf), 5.

transferability across borders, the authors who study cryptocurrency's impact to the state vary in their area of expertise.

The U.S. government has keenly noticed the capabilities virtual currencies provide to the illicit marketplace, but most of the government backed public research has just emerged in the past five years. The research conducted by the U.S. government agencies and various U.S. funded research groups tends to concentrate on the future potential threats that cryptocurrency may pose to the state's ability to impose financial restrictions, tax, and protect its citizens; however, this research has yet to reach a consensus of long-term solutions. As a 2015 Congressional Research Service report states, "in Congress, interest in virtual currencies is at the exploratory stage."<sup>11</sup> The 2015 *National Terrorist Financing Risk Assessment* report by the U.S. Treasury lists "new payment systems ... like Virtual Currencies (VC) such as Bitcoin and other emerging payment technologies" as potential future terrorist financing threats.<sup>12</sup> Additionally, the 2017 National Drug Threat Assessment produced by the DEA (Drug Enforcement Administration) writes that "TCO [transnational criminal organizations] are ... increasingly using virtual currencies due to their anonymizing nature and ease of use."<sup>13</sup> Likewise, the RAND corporation's *National Security Implications of Virtual Currency* highlights various methods how cryptocurrencies could "enhance non-state actor's political and/or economic power ... by means of illicit transfer, fundraising, or money laundering."<sup>14</sup>

Cryptocurrencies' connection to the illicit marketplace first received attention after the development of the Silk Road in 2013, a website only accessible through the Dark Web,

---

<sup>11</sup> Edward Murphy, Maureen Murphy, and Michael Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, CRS Report No. R43339 (Washington, DC: Congressional Research Service, 2015), <https://fas.org/sgp/crs/misc/R43339.pdf>, 10.

<sup>12</sup> Adam Szubin, *National Terrorist Financing Risk Assessment* (Washington, DC: Department of the Treasury, 2015), <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%932006-12-2015.pdf>, 56–57.

<sup>13</sup> Drug Enforcement Administration, *2017 National Drug Threat Assessment*, DEA-DCT-DIR-040-17 (Washington, DC: Drug Enforcement Administration, 2017), [https://www.dea.gov/docs/DIR-040-17\\_2017-NDTA.pdf](https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf), 130.

<sup>14</sup> Joshua Baron et al., *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actors Development* (Santa Monica, CA: RAND Corporation, 2015), ix–x, [https://www.rand.org/pubs/research\\_reports/RR1231.html](https://www.rand.org/pubs/research_reports/RR1231.html).

which is the part of the web users need special software to access and thus remain anonymous.<sup>15</sup> Nicolas Christin writes that during the Silk Road's period of operation between 2011 and 2013, it acted as an "infrastructure for sellers and buyers to conduct transactions ... similar to Amazon Marketplace, Craigslist, or eBay," but for both illegal and legal goods.<sup>16</sup> Christin estimates the Silk Road earned a monthly income of 1.2 million U.S. dollars (USD), stating that the dark website offered a variety of goods, mostly providing legal and illegal drugs, which the site categorized into 220 distinct groups for the ease of the dark website's users.<sup>17</sup>

Steven Brown directs his research toward how illegal use of Bitcoin affects the capability of state's law enforcement, arguing that Bitcoin "is the currency of choice for cybercriminals and Darknet entrepreneurs."<sup>18</sup> He writes that the lack of regulation in cryptocurrency transactions has created "attractive opportunities for criminal exploitation," and he lists a varying field of illegal activities available to Darknet users where Bitcoin is the primary method of payment.<sup>19</sup> He also lists the examples of illegal services transacting in bitcoins, including the laundering of fiat currencies, counterfeiting U.S. dollars, purchasing illegal drugs, and hiring assassination services.<sup>20</sup>

While the majority of literature expects to see increased incidents of terrorists using cryptocurrency, the actual capability of individuals and non-state actors to use virtual currencies to support terrorism is contested among academics. Scholars like William Mendel and Peter McCabe believe cryptocurrency is a current homeland security issue. They argue that Bitcoin offers new challenges to the U.S. mission to counter support and financing of the Islamic State (IS) that extends worldwide, citing a 2015 incident when the

---

<sup>15</sup> Vigna and Casey, *The Age of Cryptocurrency*, 84.

<sup>16</sup> Nicolas Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," in *Proceedings of the 22nd International Conference on World Wide Web (WWW '13)* (Rio de Janeiro, Brazil: ACM, 2013), 214.

<sup>17</sup> Christin, 222, 216–218.

<sup>18</sup> Steven Brown, "Cryptocurrency and Criminality: The Bitcoin Opportunity," *The Police Journal: Theory, Practice and Principles* 89, no. 4 (2016): 336.

<sup>19</sup> Brown, 327–328.

<sup>20</sup> Brown, 328.



U.S. resident Ali Amin was prosecuted for providing a “how-to” guide to support IS using Bitcoin as the method of finance.<sup>21</sup> Similarly, highlighting the Islamic State’s use of bitcoin “Sadaqa,” or donations, and an IS linked address worth \$3 million, Lewis Sanders argues there is a connection between IS and bitcoin.<sup>22</sup> Micah Zenko also agrees that cryptocurrencies are becoming more widespread among terrorist groups, emphasizing recent incidents of illicit transactions like the 2017 transfer of bitcoins to Islamist militants in Indonesia.<sup>23</sup>

On the other hand, some experts argue that the cryptocurrency-terrorist threat is not yet mainstream. Despite a growing number of incidents where terrorist organizations have used cryptocurrency as a means of finance, David Manheim et al. write, “[a]t present, cryptocurrencies are hardly a go-to solution for terrorist financiers.”<sup>24</sup> In their report for the RAND Corporation, Baron et al. provide a comprehensive analysis of the methods a non-state actor can use virtual currency, including the development, deployment, manipulation, and exploitation of virtual currencies to further non-state objectives.<sup>25</sup> They report that non-state actors face significant hurdles in using or implementing virtual currencies, especially when powerful opposing states seek to disrupt them.<sup>26</sup>

Like Manheim et al., Yaya Fanusie of the Foundation for Defense of Democracies writes that while terrorists have been mostly unsuccessful in their cryptocurrency endeavors, they will continue their attempts to use cryptocurrency. In his 2016 article, Fanusie found that the Ibn Taymiyya Media Center, an online media organization offering explosive training and support for the Islamic State (IS), ran “a social media fundraising

---

<sup>21</sup> William Mendel and Peter McCabe, eds., *SOF Role in Combating Transnational Organized Crime* (MacDill Air Force Base, FL: Joint Special Operations University Press, 2016), [http://cco.ndu.edu/Portals/96/Documents/books/JSOU%20SOF/JSOU16\\_MendelMcCabe\\_CTOC\\_final.pdf](http://cco.ndu.edu/Portals/96/Documents/books/JSOU%20SOF/JSOU16_MendelMcCabe_CTOC_final.pdf), 101.

<sup>22</sup> Lewis Sanders, “Bitcoin: Islamic State’s Online Currency Venture,” DW, September 20, 2015, <http://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856>.

<sup>23</sup> Micah Zenk, “Bitcoin for Bombs,” *Council on Foreign Relations* (blog), August 17, 2017, <https://www.cfr.org/blog/bitcoin-bombs>.

<sup>24</sup> David Manheim et al., “Are Terrorists Using Cryptocurrencies?,” *Foreign Affairs*, April 21, 2017, <https://www.foreignaffairs.com/articles/2017-04-21/are-terrorists-using-cryptocurrencies>.

<sup>25</sup> Baron et al., *National Security Implications*,” 19, 36.

<sup>26</sup> Baron et al., 67.

campaign that is the first publicly verifiable instance of a terrorist group using bitcoin.”<sup>27</sup> He later reexamines terrorists’ attempt to use cryptocurrency in his December 2017 article, identifying numerous bitcoin “donation” addresses linked to IS and al-Qaeda backed groups advertised on both the Internet and Dark Web.<sup>28</sup> Moreover, he points out that Bitcoin is an attractive means of fundraising because of the assumed anonymity; however, the transactions stored on the public ledger provides an easy audit trail that traces the donation back to the source.<sup>29</sup> Fanusie concludes that while bitcoin “is still not a reliable source of funding for jihadists . . . this may change in the future” and points to the future potential for the acceptance of a new cryptocurrency offering more privacy or the creation of “online [cryptocurrency] exchanges that do not adhere to money laundering laws.”<sup>30</sup>

Rogue states seeking to bypass international sanctions have also demonstrated capacity to use cryptocurrency. In late 2017, White House Homeland Security Advisor Tom Bossert accused North Korea for the 2017 WannaCry ransomware attack, a cyber-attack that held infected computer systems hostage until the victim sent a payment of Bitcoin to a specific bitcoin address.<sup>31</sup> Nir Kshetri and Jeff Voas note that North Korea earned an estimated 120,000 USD in bitcoin, emphasizing that although most infected device users did not pay into the ransomware attack, the propensity for greater ransomware attacks using cryptocurrency is likely to increase in the future.<sup>32</sup>

Patrick Tucker argues that North Korea’s efforts to use cryptocurrency as an illegal source of income extends past simple ransomware attacks. He points out that North Korea

---

<sup>27</sup> Yaya Fanusie, “The New Frontier in Terror Fundraising: Bitcoin,” *The Cipher Brief* (blog), August 24, 2016, [https://www.thecipherbrief.com/column\\_article/the-new-frontier-in-terror-fundraising-bitcoin](https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin).

<sup>28</sup> Yaya Fanusie, “Terrorist Networks Eye Bitcoin as Cryptocurrency’s Price Rises,” *The Cipher Brief* (blog), December 21, 2017, <https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises>.

<sup>29</sup> Fanusie.

<sup>30</sup> Fanusie.

<sup>31</sup> Thomas P. Bossert, “It’s Official: North Korea Is behind WannaCry,” *Wall Street Journal*, December 18, 2017, <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537>, sec. Opinion.

<sup>32</sup> Nik Kshetri and Jeff Voas, “Do Crypto-Currencies Fuel Ransomware?,” *IT Professional* 17, no. Sep/Oct 2017 (2017): 3, 6.

was able to gain access illegally to South Korean cryptocurrency exchanges in 2017 by using phishing emails to obtain log in credentials.<sup>33</sup> Tucker states that North Korea can transfer the stolen cryptocurrency from the compromised exchange to other exchanges worldwide and then exchange the stolen cryptocurrency for more privacy based coins in an effort to launder the cryptocurrency, eventually withdrawing the funds in the form of fiat like the U.S. dollar or South Korean won. Because of becoming an intermediary between cryptocurrency and government backed fiat, Tucker explains, exchanges and their owners are under increased scrutiny and face shutdown or arrest for allowing illicit activities.<sup>34</sup>

The Russian Federation has also shown interest in the creation of a government backed cryptocurrency. Olivia Capozzalo writes that the Russian intentions for the development could be linked to bypass western sanctions Russia and is currently investigating possible implementation strategies using an official government working group.<sup>35</sup> Like Capozzalo, Shannon Liao is skeptical of Russian intention and sudden interest in cryptocurrency, highlighting Vladimir Putin's decree of five new presidential orders on 10 October 2017, which "demanded officials set up a legal framework to handle digital currencies ... that could solidify cryptocurrency acceptance within the Russian Federation."<sup>36</sup> Liao believes the development of the new Russian regulation would significantly increase regulations of cryptocurrency within the state, but she cites authors who have stated "fostering cryptocurrencies could be a means for Russian official's to skirt sanctions."<sup>37</sup> She concludes that although Russia has a long history of crime and money

---

<sup>33</sup> Patrick Tucker, "Russia, N. Korea Eye Bitcoin for Money Laundering, Putting It on a Crash Course with Regulators," *Defense One*, December 15, 2017, <http://www.defenseone.com/technology/2017/12/russia-n-korea-eye-bitcoin-money-laundering-putting-it-crash-course-regulators/144598/>.

<sup>34</sup> Tucker.

<sup>35</sup> Olivia Capozzalo, "Putin Adviser Says 'CryptoRuble' Will Circumvent Sanctions, Government Remains Divided," *Cointelegraph*, January 2, 2018, <https://cointelegraph.com/news/putin-adviser-says-cryptoruble-will-circumvent-sanctions-government-remains-divided>.

<sup>36</sup> Shannon Liao, "Inside Russia's Love-Hate Relationship with Bitcoin," *The Verge*, October 31, 2017, <https://www.theverge.com/2017/10/31/16387042/russia-putin-bitcoin-regulation-ethereum-blockchain-technology>.

<sup>37</sup> Liao.

laundering, “Russia also stands to legitimately benefit from the legalization of cryptocurrency.”<sup>38</sup>

Chris Telley is substantially less optimistic on the development of Russian cryptocurrency, believing Russia’s development of cryptocurrency laws and a state backed cryptocurrency likely has sinister intentions.<sup>39</sup> Highlighting Russia’s historical use of emerging technology, like social media, to disrupt and influence foreign affairs, Telley asserts that the Russian development of cryptocurrency will become another asset in Putin’s arsenal of state and economic manipulation aimed at promoting Russian influence globally.<sup>40</sup> Telley also comments that concerning the existing economic system, “few solutions exist to counter the specific capabilities of an adversary cryptocurrency network,” and he argues that the United States must urgently move to develop its own capabilities within the digital economic environment to protect U.S. national interests in the future.<sup>41</sup>

## **2. U.S. Regulation of Cryptocurrencies**

To understand the options available to sovereign governments like the United States to regulate cryptocurrencies, it is worthwhile to examine the literature detailing the opinions of scholars on the legal avenues the United States might take. This section presents a selection of peer-reviewed sources taking various legal approaches to regulate cryptocurrency. The majority of scholars who have studied the cryptocurrency movement since its debut believe that the current American legal system has been slow to adapt to the fast-moving digital world of virtual currencies and is ill prepared to prosecute illegal activity involving cryptocurrency under the existing framework of U.S. laws. Moreover, the avenues available to the United States for controlling or preventing illicit cryptocurrency use is widely debated among law scholars. As stated by Rainer Bohme et al., “a key challenge for prospective regulators is where to impose constraints.... While

---

<sup>38</sup> Liao.

<sup>39</sup> Chris Telley, “A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency,” *Small Wars Journal*, January 15, 2018, <http://smallwarsjournal.com/jrnl/art/a-coin-for-the-tsar-the-two-disruptive-sides-of-cryptocurrency>.

<sup>40</sup> Telley, 5.

<sup>41</sup> Telley, 5.

Bitcoin now appears to be subject to regulatory oversight, the authority of regulators face certain limits.”<sup>42</sup> For instance, many scholars point to the difficulty of controlling Bitcoin within the United States without imposing on citizens’ rights to privacy or unlawful searches and seizures.

One proposal to combat the illicit use of cryptocurrency is to expand the legal capability of law enforcement agencies to investigate illicit cryptocurrency use. Alice Huang argues that the current federal criminal subpoena standards are ill-equipped to prosecute the illicit uses of cryptocurrency, and she proposes enhancing the U.S. judicial power to “create a new criminal subpoena standard, modeled from current e-discovery laws, that targets criminal Bitcoin use.”<sup>43</sup> She also argues that the current subpoena process requires the government to “go through millions of transactions and hundreds of thousands of user accounts in order to pinpoint specific targets.”<sup>44</sup> Finally, she states that increasing the subpoena powers could become problematic because the new laws could infringe upon users who would want to maintain the anonymity and must therefore be carefully crafted to prevent governmental overstep.<sup>45</sup>

Similarly, Danton Bryans focuses on the interaction between Bitcoin and anti-money laundering (AML) laws, stating, “Bitcoin represents a disruptive financial technology that many AML and money transmitter statutes are ill prepared to deal with.”<sup>46</sup> Although Bryans asserts, “Bitcoin might be seen as illegal because it attempts to assume powers expressly reserved to the federal government under the U.S. Constitution,” he believes that emerging cryptocurrencies should continue to exist unhampered to its users.<sup>47</sup> Bryans instead argues that the most effective method of regulation is the regulation of the

---

<sup>42</sup> Rainer Bohme et al., “Bitcoin: Economics, Technology, and Governance,” *The Journal of Economic Perspectives* 29, no. 2 (Spring 2015): 231.

<sup>43</sup> Alice Huang, “Reaching within Silk Road: The Need for a New Subpoena Power That Targets Illegal Bitcoin Transactions,” *Boston College Law Review* 56, no. 5 (December 2015): 2097, 2119–2122.

<sup>44</sup> Huang, 2120.

<sup>45</sup> Huang, 2123–2124.

<sup>46</sup> Danton Bryans, “Bitcoin and Money Laundering: Mining for an Effective Solution,” *Indiana Law Journal* 89, no. 1, Article 13 (2014): 472, <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj>.

<sup>47</sup> Bryans, 447.

fiat-to-cryptocurrency exchanges, since exchanges already fall under existing money transmitter laws and require exchange users to identify themselves when they register and use exchanges.<sup>48</sup>

Like Bryans, Jonathan Turpin believes that the regulation of crypto-exchanges would be “the simplest and most likely route.”<sup>49</sup> Turpin writes that transactions using Bitcoin are not illegal but “operate in a legal gray area.... [where] no U.S. law currently on the books explicitly applies to Bitcoin.”<sup>50</sup> Due to the international applicability of using Bitcoin as a currency, he believes that Bitcoin will continue to grow unless the world governments move to regulate cryptocurrency; however, he recommends against an outright external restriction on cryptocurrencies. Turpin instead offers that the “wisest approach that governments might take to Bitcoin is to attempt to regulate the transactions that take place in Bitcoin (BTC), rather than the system itself,” arguing that a method of regulation inside of the blockchain would be far more effective than external regulation.<sup>51</sup>

Omri Marian offers a unique, less invasive solution a state could implement to regulate bitcoin-like cryptocurrencies, which incorporate a visible public ledger.<sup>52</sup> Marian’s conceptual framework exploits the cryptocurrencies’ public ledger—wherein every historical transaction is compiled—as a means of tracking licit and illicit cryptocurrency transactions. He argues that if the government were to enact an “elective anonymity tax” that enforces high taxes on merchants who transact in cryptocurrency with unknown users but offers tax relief to transactions with preidentified users, cryptocurrency users would be incentivized to register their identity.<sup>53</sup> As a result, customers who have been verified for the tax relief would reveal their identity through the process of associating

---

<sup>48</sup> Bryans.

<sup>49</sup> Jonathan Turpin, “Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework,” *Indiana Journal of Global Legal Studies* 21, no. 1 (2014): 364.

<sup>50</sup> Turpin, 352–353.

<sup>51</sup> Turpin, 367.

<sup>52</sup> Omri Marian, “A Conceptual Framework for the Regulation of Cryptocurrencies,” *University Of Chicago Law Review* 82, no. 53 (2015): 55–68, <https://scholarship.law.ufl.edu/facultypub/695/>.

<sup>53</sup> Marian, 63–64.

a name to their digital wallet, providing the businesses and regulatory bodies with a history of all transactions to and from that user.

Marian's proposed system has the unique advantage of permitting anonymous users to continue to use cryptocurrency to transact under regulation at the penalty of an additional financial fee imposed by the marketplace. He argues that law-abiding citizens will have no need to conceal their identity, and when these citizens are presented with the financial benefits of registration, they will register en masse, making the entire cryptocurrency network less anonymous while highlighting illicit transactions.<sup>54</sup> Marian concludes, "under such a framework, legitimate users [will] passively participate in regulatory efforts to prevent illicit behavior."<sup>55</sup>

### **3. International Regulatory Propositions to Regulate Cryptocurrencies**

The opinions of those debating the regulation of cryptocurrency in the international community fall on a spectrum between international oversight and adoption. On one end, the critics of cryptocurrency argue that cryptocurrencies threaten the existing financial order and state security and therefore need to be heavily regulated or prohibited through a framework of international governments. The cryptoanarchists and cypherpunks are on the other extreme, and they argue that the technology herald within the cryptocurrency movement will force political, financial, or social revolutions in the governments of the world. These opinions are both extreme, and the vast majority of scholarly views argue for minor regulation of cryptocurrency rather than prohibition and revolution.

Fiammetta Piazza believes that regulating cryptocurrency requires a coordination between international organizations to set the minimum for cryptocurrency regulation for sovereign states. She writes, "Given Bitcoin's great potential of being exploited not only by financial criminals but also Dark Web traffickers, an international agreement should be implemented."<sup>56</sup> Additionally, she argues that governments will need to establish

---

<sup>54</sup> Marian, 63.

<sup>55</sup> Marian, 63–64.

<sup>56</sup> Fiammetta Piazza, "Bitcoin in the Dark Web: A Shadow over Banking Secrecy and a Call for Global Response," *Southern California Interdisciplinary Law Journal* 26, no. 3 (2017): 545.

minimum international standards of registration that would lessen the anonymity in cryptocurrency but provide individual nations with the sovereign right to increase the regulation of cryptocurrencies as they see fit.<sup>57</sup> According to Piazza, these standards would “render Bitcoin less attractive to both Web and Dark Web criminals.”<sup>58</sup>

Nicholas Plassaras proposes that cryptocurrencies need to be reined in internationally through the International Monetary Fund (IMF), stating Bitcoin “poses an increasingly serious threat to the stability of the foreign currency exchange market and, by extension, international commerce.”<sup>59</sup> He believes that when cryptocurrencies like Bitcoin gain worldwide adoption, they can be used as a “speculative attack” on foreign currency and destabilize nations.<sup>60</sup> To counter Bitcoin’s threat of a speculative attack, Plassaras offers two solutions. First, the IMF could require member countries to purchase and contribute a percentage of bitcoins as part of each country’s required quota, thereby allowing the IMF to counter a Bitcoin speculative attack and stabilize individual countries.<sup>61</sup> Second, the IMF could simply purchase its own supply of bitcoins to be placed in reserve should a speculative attack occur.<sup>62</sup>

While Plassaras is not alone in his fear of cryptocurrency’s disruption of the international financial system, the IMF’s leadership dismisses the risks of virtual currency to the international financial order. In a speech to the Bank of England, the IMF managing director, Christine Lagarde, states, “[f]or now, virtual currencies such as Bitcoin pose little or no challenge to the existing order of *fiat* currencies... because they are too volatile, too risky, too energy intensive,... and not yet scalable.”<sup>63</sup> Similarly, the IMF’s book *Digital*

---

<sup>57</sup> Piazza, 545–46.

<sup>58</sup> Piazza, 545–46.

<sup>59</sup> Nicholas Plassaras, “Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF,” *Chicago Journal of International Law* 14, no. 1, article 12 (2013): 396.

<sup>60</sup> Plassaras, 398–400.

<sup>61</sup> Plassaras, 402–405.

<sup>62</sup> Plassaras, 406.

<sup>63</sup> Christine Lagarde, “Central Banking and Fintech—A Brave New World?” (speech at Bank of England Conference, London, September 29, 2017), <https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world>.



*Revolutions in Public Finance* offers a similar conclusion by dismissing the potential destabilizing effect of cryptocurrency adoption, proposing that blockchain is a tool for countries to amplify their respective capabilities of fiat currencies and data tracking.<sup>64</sup>

However, the emergence of distributed ledger cryptocurrencies, like Bitcoin, has also gained the attention of the Bank for International Settlements (BIS). The report on digital currencies produced by the BIS's Committee on Payments and Market Infrastructures (CPMI) provides a detailed analysis of potential benefits and drawbacks that digital distributed ledger currencies offer as a method of transaction.<sup>65</sup> The report also provides a list of potential regulatory actions a state or its central bank can take to control or weaken cryptocurrencies, and it analyzes a list of countries that have applied virtual currency regulations current to 2015.<sup>66</sup> <https://libguides.nps.edu/citation/rules-chicago-nb>

Paul Vigna and Michael Casey argue that Bitcoin will not tear down the existing Westphalian order upon which the world economy is built but instead will become a challenger and provide the “banking state . . . [with] some much-needed competition and discipline forced upon it.”<sup>67</sup> They explain there are three obstacles that Bitcoin, or any other cryptocurrency, must surmount to achieve the goal of widespread adoption. First, Bitcoin is stifled with the rocky history of scams and illegal activity, and its price tends to be volatile. Second, the deflationary nature of Bitcoin promotes hoarding over spending, and if adopted over the existing inflationary financial system, it could create another “Great Depression.”<sup>68</sup> Finally, if preexisting trusted companies developed their own direct competitor to Bitcoin with nearly the same benefits, consumers would likely prefer the trusted name-brand companies resulting in a decrease use of Bitcoin.

---

<sup>64</sup> Sanjeev Gupta et al., *Digital Revolutions In Public Finance* (Washington, DC: International Monetary Fund, 2017), 173–196.

<sup>65</sup> Committee on Payments and Market Infrastructures, *Digital Currencies* (Basel, Switzerland: Bank for International Settlements, 2015), <https://www.bis.org/cpmi/publ/d137.pdf>.

<sup>66</sup> Committee on Payments and Market Infrastructures, *Digital Currencies*, 12–13.

<sup>67</sup> Vigna and Casey, *The Age of Cryptocurrency*, 311.

<sup>68</sup> Vigna and Casey, 294.

## **D. POTENTIAL EXPLANATIONS**

Sovereign states have a host of legislative actions available to them to control cryptocurrencies; however, each state has unique challenges to implementing and enforcing these options. One potential challenge to applying laws on cryptocurrency is a state's capability to actually enforce policy against cryptocurrency, since cryptocurrency creation and transactions promote anonymity and complicates the identification and prosecution of offenders. Another probable challenge of a sovereign state control is if the legislation regarding cryptocurrency is compatible in the international community. In other words, a policy administering a total ban of cryptocurrency might be unenforceable if a host of other geographically near, or economically influential nations, permit the use of cryptocurrency by citizens.

From the ideas proposed by the authors in this thesis's literature review, it appears that the state and international financial institutions have three broad—but not separate—options available to control cryptocurrency. The three options are to ban cryptocurrency use; to instill regulations to control cryptocurrency use at level of the exchange or user; and to adopt cryptocurrencies as an accepted means of transaction. This thesis expounds upon the three options to determine what policies states could implement to control cryptocurrency and restrict illicit transactions as well as the incurring challenges and drawbacks of each action.

## **E. RESEARCH DESIGN**

To achieve a comprehensive analysis of the methods that sovereign states and international institutions could take to regulate cryptocurrency, this thesis surveys a combination of the available scholarly literature and historical incidents of government restrictions on cryptocurrency to draw conclusions about how effective controls on cryptocurrency are. This thesis does this by separating the potential avenues of controlling cryptocurrency into three groups (regulation, ban, and adoption) and analyzing methods of how the state and international community could implement controls.

## **F. THESIS OVERVIEW AND DRAFT CHAPTER OUTLINE**

The first chapter of this thesis consists of the thesis question and its importance, the literature review, and chapter outline. The second chapter is dedicated to describing the functionality of cryptocurrency, including the innovative technology that makes it an attractive method of transaction. Also, this chapter dissects blockchain technology into its key parts as a means to present the advantages, disadvantages and weaknesses inherent in blockchain based cryptocurrency.

It is this thesis's goal to analyze the potential impact that cryptocurrency has on the state's sovereignty and the methods the state and international institutions could take to manage cryptocurrency implementation. To do this, this thesis divides the potential actions a state may take into the last three chapters, Chapter III Banning Cryptocurrency, Chapter IV Regulating Cryptocurrency, and Chapter V Adopting Cryptocurrency. Chapter III focuses on listing the potential methods that states may take to regulate cryptocurrency and analyzes each method's effectiveness. Chapter IV lists and analyzes how different levels of a ban on cryptocurrency could affect a state's capability to prevent illicit activity and the consequences resulting from extreme measures. Chapter V discusses the possible implementation of cryptocurrency, either currently existing or those developed in the future, and the resulting impact that a government backed cryptocurrency could have on the international economic system. This thesis concludes with the analysis of each avenue the state and international community may take, as well as this thesis's opinion and ideas on potential future research.

THIS PAGE INTENTIONALLY LEFT BLANK

## II. CRYPTOCURRENCIES AND THE BLOCKCHAIN

To really understand what is special about Bitcoin, we need to understand how it works at a technical level.

—Narayanan et al.<sup>69</sup>

While this thesis focuses on the actions a state may take to manipulate and regulate cryptocurrencies, this chapter covers the relevant terminology, technology, concepts, and mechanics of cryptocurrencies. Additionally, this chapter provides the reader with the foundation of cryptocurrency knowledge that this thesis draws upon later and references when discussing the possibility of prohibition, regulation, or adoption of cryptocurrencies by state governments. However, it is important to note the limitations and constraints of this chapter.

There are many design elements of Bitcoin not covered in this thesis due to constraints of the length and detail. Many of the concepts and technologies utilized by Bitcoin are extremely complex—and far outside the scope of this thesis—therefore this chapter provides the requisite amount of information to explain the Bitcoin ecosystem without extending past the question asked in this thesis. This chapter examines Bitcoin exclusively due to Bitcoin’s popularity, market value, and abundance of published material; however, the technical discussion in this chapter applies to other cryptocurrencies as well.<sup>70</sup>

Another distinction is the difference between the phrases of “digital currencies,” “virtual currencies,” “decentralized virtual currencies,” and “cryptocurrencies.” To simplify the dissimilarity between them, this chapter offers the following assumptions exclusive to this thesis but may have exceptions in outside literature. As indicated in the literature reviewed in this thesis, there is no established preference of terms in use. The most common terms observed in regulatory literature are the phrases of “digital currency”

---

<sup>69</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, preface.

<sup>70</sup> CoinMarketCap, “Cryptocurrency Market Capitalizations.” At the time of writing this thesis, Bitcoin has the greatest market value of any cryptocurrency in USD per-coin, as well as being the first cryptocurrency ever adopted as a form of payment.

and “virtual currencies (VCs),” which can be used interchangeably as a blanket phrase under which to group all electronic currencies. Similarly, Eswar Prasad defines digital currency in his report as a “broad term that encompasses any form of currency that is not tangible.”<sup>71</sup>

On the other hand, cryptocurrencies are virtual currencies that specifically rely on cryptographic proof, and can be centralized, or decentralized.<sup>72</sup> Decentralized virtual currencies (DVC) are specifically decentralized digital currencies and may or may not be cryptocurrencies. For example, Bitcoin is considered both a cryptocurrency and a DVC. Because delineating between the terms can become confusing, this thesis adheres to the syllogism all cryptocurrencies are digital currencies; however, not all digital currencies are cryptocurrencies.

To explain the key parts of Bitcoin and to avoid confusion, this chapter builds upon the distinction Vigna and Casey use in their 2015 book, *The Age of Cryptocurrency*, to differentiate the Bitcoin technology from the currency.<sup>73</sup> They write that the word Bitcoin written with a capital “B” refers to the Bitcoin technology, system, or network; meanwhile, stating bitcoin with a lowercase “b” will reference the currency.

This chapter is organized into four sections; the first section discusses the relationship between trust and Bitcoin and why users can trust it without needing a governing body. The second section details the security and capabilities provided to Bitcoin by cryptographic functions and the blockchain. The third section outlines the Bitcoin network, the responsibilities of miners and nodes, and how transactions are stored on the blockchain. The fourth and final section discusses the security within a virtual wallet, storing and transacting with bitcoins, cryptocurrency exchanges, the bitcoin ecosystem, and a brief discussion of cryptocurrencies other than Bitcoin.

---

<sup>71</sup> Eswar Prasad, *Central Banking in a Digital Age: Stock-Taking and Preliminary Thoughts* (Washington, DC: Hutchins Center on Fiscal and Monetary Policy at Brookings, 2018), <https://www.brookings.edu/research/how-will-fintech-and-digital-currencies-transform-central-banking>, 5.

<sup>72</sup> The concepts of “cryptographic proof,” “centralized,” and “decentralized” currencies is discussed later in the chapter.

<sup>73</sup> Vigna and Casey, *The Age of Cryptocurrency*, 9.

## A. BITCOIN AND “TRUST”

The concept of *trust* is an essential to any currency’s adoption as a form of money. Under the classical model of fiat currency, the state builds and sustains public trust in the currency through the use of anticounterfeiting technology, central banks, third-party verification, and enforcement agencies to prevent cheating or tampering with the system. However, cryptocurrencies like Bitcoin promote a system of currency radically differing from traditional government backed fiat. As Vigna and Casey argue, “[f]or any currency to be viable, be it a decentralized cryptocurrency issued by computer program or a traditional “fiat” currency issued by a government, it must win the *trust* of the people.”<sup>74</sup> On the other hand, Bitcoin is not controlled by any government, organization, or person and must approach the dilemma of trust without the aforementioned tools available to state backed currency.

The design of Bitcoin is a departure from prior models of currency because Bitcoin purposely replaced the requirement for trusted third parties, instead instilling confidence in the currency through the reliance on virtually impervious mathematical functions. The pseudonymous founder of Bitcoin, Satoshi Nakamoto, acknowledges the challenges of the Bitcoin. He recognizes that prior to Bitcoin, “no mechanism [has existed] to make payment over a communication channel without a trusted third party.”<sup>75</sup> To conquer the problem of removing the middleman from transactions, Nakamoto proposed the Bitcoin whitepaper, a “peer-to-peer electronic cash system that uses ... cryptographic proof instead of trust” in financial institutions.<sup>76</sup> Vigna and Casey contend, “cryptocurrency systems imbue trust in an inviolable, decentralized computer program that is, in theory, incapable of defrauding people.”<sup>77</sup>

Some writers define cryptocurrencies as trustless; however, this is not the case. As Narayanan et al. note that the Bitcoin protocol is not trustless, but strives for a system of

---

<sup>74</sup> Vigna and Casey, 15.

<sup>75</sup> Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 1.

<sup>76</sup> Nakamoto, 1.

<sup>77</sup> Vigna and Casey, *The Age of Cryptocurrency*, 15.

“trust minimalization” to reduce the maximum amount of trust required of a currency to function.<sup>78</sup> Similarly, Vigna and Casey state

The simple genius of this technology is that it cuts away the middleman yet maintains an infrastructure that allows strangers to deal with each other. It does this by taking the all-important role of ledger-keeping away from centralized financial institutions and handing it to a network of autonomous computers, creating a decentralized system of trust that operates outside the control of any one institution.<sup>79</sup>

Bitcoin has removed many of the third party and regulatory bodies from its framework without removing trust. The replacement of trust is a key to why Bitcoin and other cryptocurrencies offer a viable and attractive alternative to the conventional model of government backed fiat.

## **B. SECURITY IN BITCOIN: HASH FUNCTIONS, MERKLE TREES, AND THE BLOCKCHAIN**

What is a cryptocurrency? Narayanan et al. identify the word “cryptocurrency” as a combination “cryptographic” and “currency,” wherein the “use of cryptography provides a mechanism for securely encoding the rules of a cryptocurrency system within the system itself.”<sup>80</sup> Bitcoin’s choice of cryptographic functions is the hash function, a cryptologic function that is used in Bitcoin to build many of the more complex data structures guaranteeing the security of the protocol.

Hash functions are important to discuss for two reasons. First, Bitcoin relies on the functionality and the output generated by the cryptographic hash to create many of the Bitcoin data structures, such as the Merkle tree, blockchain, mining, and the virtual wallet, each described in turn in the following text.<sup>81</sup> The second reason this chapter discusses the hash function is because cryptographic hashes are inherently robust in securing information, so that an adversary who wants to disrupt or manipulate the data contained in

---

<sup>78</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 280.

<sup>79</sup> Vigna and Casey, *The Age of Cryptocurrency*, 5. The terms “decentralization” and “ledger” are explained later in this chapter.

<sup>80</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 1.

<sup>81</sup> Narayanan et al., 1.



a hash output could neither view the contents, nor the alter data inside without showing that someone tampered with the hash.<sup>82</sup> Narayanan et al. define the purpose of hash functions “to prevent tampering and equivocation, as well as to encode, in a mathematical protocol, the rules for creation of new units of currency.”<sup>83</sup> More importantly, cryptographically secure hash functions operate in one direction from input to output and cannot be *unhashed* by knowing the output.

All hashes are not the same, and to consider a hash function *cryptographically secure*, the hash must exhibit the three properties of collision resistance, hiding, and puzzle friendliness.<sup>84</sup> A collision occurs in a cryptographic function when two different inputs result in the same output. There are collisions for every hash function, regardless of its strength; therefore, a hash is considered *collision resistant* when it is virtually impossible to find a collision.<sup>85</sup> One reason why collision resistant hash functions are useful, particularly in the blockchain, is because they act as a summary of the input data, called a *digest*.<sup>86</sup> Best stated by Narayanan et al., a cryptographic hash is “a very efficient way to remember things [a user has] seen before and to recognize them again.”<sup>87</sup> The second property of cryptographically secure hash functions is *hiding*. Simplified for this thesis, hiding is achieved when the hash function secures the input data in such a way that an adversary can not guess the input data, even with knowledge of the output.<sup>88</sup> *Puzzle friendliness*—again, shortened for the purpose of this chapter—occurs when no known systematic method exists that would discover the input of a hash function faster than random guesswork.<sup>89</sup>

---

<sup>82</sup> Narayanan et al., 2–9.

<sup>83</sup> Narayanan et al., 1.

<sup>84</sup> Narayanan et al., 2.

<sup>85</sup> Narayanan et al. use a 256-bit hash as an example of collision resistance, stating, “if every computer made by humanity had been computing since the beginning of the universe, the odds that they would have found a collision by now are still infinitesimally small,” Narayanan et al., 3–4.

<sup>86</sup> Narayanan et al., 5.

<sup>87</sup> Narayanan et al., 5.

<sup>88</sup> Narayanan et al., 5.

<sup>89</sup> Narayanan et al., 8.

The majority of the Bitcoin protocol utilizes the particularly strong hash function of secure hash algorithm (SHA)-256,<sup>90</sup> which is described as virtually uncrackable unless the source of the information is already known.<sup>91</sup> The SHA-256 output presents itself as a fixed-length digest or an alphanumeric string that is 64 characters in length, regardless of the size input into the hash function.<sup>92</sup> For example, Vigna and Casey demonstrate that when one runs the entire contents of *War and Peace* and then a separate 13-word phrase through a SHA-256 generator, both of the outputs result in a 64 character string unique to their contents.<sup>93</sup> An example of a SHA-256 output is in Figure 1.

89F7901F20B05000FE48160DB5253561C322D6838164B2E157A76537F39441EF

Figure 1. A SHA256 Hash Generated from the Phrase  
“Naval Postgraduate School”<sup>94</sup>

The two hash-based data structures this chapter discusses are the block chain and the Merkle tree. As the word implies, the blockchain consists of multiple blocks of information chained together via a hash function (see Figure 2). Narayanan et al. further break down the components within each block, explaining, the “block chain [is] a clever combination of two different hash-based data structures. The first is a hash chain of blocks,

---

<sup>90</sup> As 3blue1brown estimates in his video, using the computing power as of the video’s production in 2017, to receive a 1-in-4 billion chance that SHA256 protection would be cracked over a period of 507 billion years, it would require four billion galaxies each filled with four billion planets, each planet containing four billion people, and with each person armed with the entire estimated processing power of all google servers combined with graphic processing units that are dedicated to cracking one specific SHA256 digest string. “How Secure Is 256 Bit Security?” YouTube video, 5:05, posted by 3blue1brown, July 8, 2017, [https://www.youtube.com/watch?v=S9JGmA5\\_unY&t=71s](https://www.youtube.com/watch?v=S9JGmA5_unY&t=71s).

<sup>91</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 110.

<sup>92</sup> Narayanan et al., 5.

<sup>93</sup> Vigna and Casey, *The Age of Cryptocurrency*, 129.

<sup>94</sup> Source: “SHA256 Hash Generator,” Password Generator, accessed April 29, 2018, <https://passwordsgenerator.net/sha256-hash-generator/>. To generate the same hash, type in “Naval Postgraduate School” exactly as written.

[and] ... the second data structure is a per-block [Merkle] tree of all transactions included in the block.”<sup>95</sup>

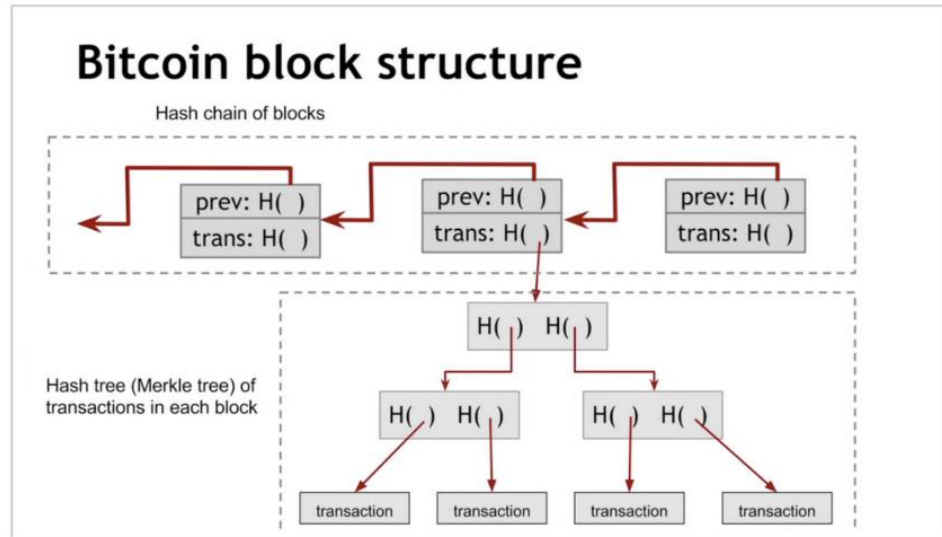


Figure 2. The Hash Structure of the Block Chain and Merkle Tree<sup>96</sup>

The purpose of the Merkle tree is to protect the data stored in each block of Bitcoin from tampering. Narayanan et al. states that the Merkle tree in Bitcoin groups “data blocks into pairs of two, and then for each pair ... [builds] a data structure that has two has pointers, one to each of the blocks.”<sup>97</sup> The process then repeats with the newly created data structure placed into another pair of two, repeating until the information reaches a single block, called the Merkle root.<sup>98</sup> According to Narayanan et al., since the Merkle tree is connected by hash pointers, “any attempt to tamper with any piece of data will be detected by just remembering the hash pointer at the top.”<sup>99</sup> A visual depiction of the Merkle tree is found in the bottom half of Figure 2.

<sup>95</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 64.

<sup>96</sup> Source: Suraj Kumar, “Merkle Trees—Introduction to Blockchain,” December 10, 2017, <https://medium.com/@skj48817/merkle-trees-introduction-to-blockchain-c80c0247046>.

<sup>97</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 13.

<sup>98</sup> “SHA256 Hash Generator.”

<sup>99</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 13.

The second hash-based data structure this chapter discusses is the blockchain. Much like the Merkle tree's protection of data within each individual block, the blockchain protects and links the most current block to each previous block, consequently protecting all of the historical Bitcoin data. The official website of the Bitcoin Core developers, Bitcoin.org, describes how the construction of the blockchain, stating

The merkle root is stored in the block header. Each block also stores the hash of the previous block's header, chaining the blocks together. This ensures a transaction cannot be modified without modifying the block that records it and all following blocks.<sup>100</sup>

The data stored within a blockchain can be any piece of information that a developer wishes to protect; however, in the case of Bitcoin, the data stored are the account balances of every bitcoin user in a system called a public ledger. Vigna and Casey explain, "The payee no longer has to trust 'third-party' institutions such as banks or governments to assure that the payer can deliver the agreed-upon funds."<sup>101</sup> A major benefit of storing the public ledger in the blockchain is that Bitcoin secures the information in a way that allows Bitcoin to self-police, thereby eliminating the problem of counterfeiting and providing an answer to the problem of double spending.<sup>102</sup>

### **C. DECENTRALIZED PUBLIC LEDGER AND THE BITCOIN NETWORK: MINING AND NODES**

The concept of decentralization is critical to the trust model of Bitcoin because decentralization allows access to the public ledger without the need for third parties (see Figure 3). Vigna and Casey write that traditionally, fiat "[m]onetary systems have been built on centralized ledger keeping" or a system wherein third parties are trusted to

---

<sup>100</sup> "How Does Bitcoin Work?," Bitcoin, accessed March 1, 2018, <https://bitcoin.org/en/developer-guide#block-chain-overview>.

<sup>101</sup> Vigna and Casey, *The Age of Cryptocurrency*, 11, 15.

<sup>102</sup> Narayanan et al. explain 'double spending' as spending a coin twice digitally. Double spending can occur, but only one coin will remain after multiple transactions. Any attempt to do so will result with only one expenditure to be validated after multiple confirmations on the longest block chain. Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 34–35.

maintain a record of monetary balances and are the solitary point of query for information on a user's account balance.<sup>103</sup>

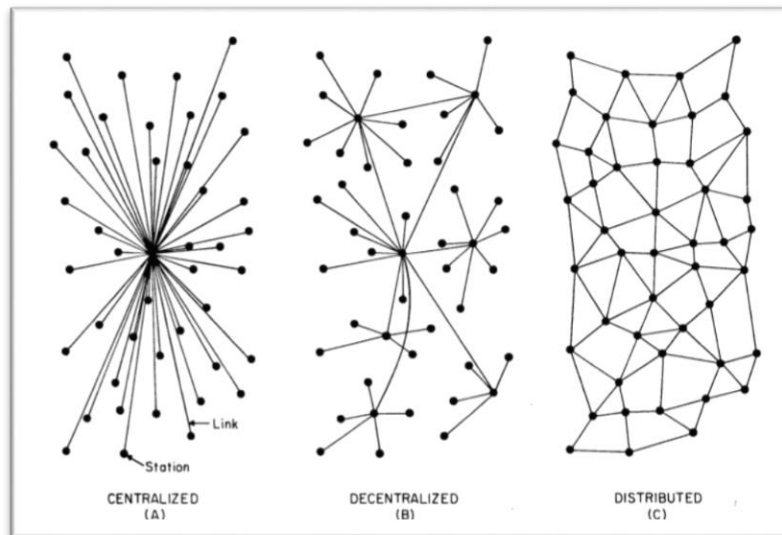


Figure 3. Visual Differences between Centralized, Decentralized, and Distributed Networks.<sup>104</sup>

However, Bitcoin achieves decentralization through the Bitcoin network consisting of individual *miners* and *nodes* that maintain copies of the public ledger worldwide.<sup>105</sup> This reflects a concept known as the *decentralized public ledger*. Any person who wants to join the Bitcoin network can turn her or his computer into a node or mining machine by downloading the Bitcoin protocol software onto a computer meeting the minimum hardware requirements and connect the computer to the Internet.<sup>106</sup> In addition to perpetuating the public ledger, the Bitcoin nodes and miners are responsible for a number

<sup>103</sup> Vigna and Casey, *The Age of Cryptocurrency*, 20.

<sup>104</sup> Source: Paul Baran, *On Distributed Communications: I. Introduction to Distributed Communications Networks*, RM-3420-PR (Santa Monica, CA: RAND Corporation, 1964), [https://www.rand.org/content/dam/rand/pubs/research\\_memoranda/2006/RM3420.pdf](https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf), 2.

<sup>105</sup> Vigna and Casey, *The Age of Cryptocurrency*, 120–137.

<sup>106</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 66–67.

of other tasks, including the verification and distribution of new transactions and prevention of hostile manipulation to the network.

Bitcoin nodes listen for new transactions on the network and propagate transactions to other nodes. To this end, each Bitcoin node institutes an independent check of any new transaction data to maintain the stability of the network. According to Narayanan et al., these checks, verify the transactions are valid in the blockchain, ensure the bitcoins in transactions have not already been spent (through double spending), ignore transactions that have already been seen by the node so that they are rebroadcasted, and ensure transactions are accepted according to a whitelist of scripts.<sup>107</sup> Nodes complete these tasks by sending and receiving network data to other nodes and miners around the world in a process that grows the Bitcoin blockchain and propagates transactions.

Like the nodes, Bitcoin miners have an important role in the Bitcoin network and are responsible for three functions pertinent to this thesis: continuing the blockchain by finding valid blocks, validating transactions that have been sent through the network, and providing consensus. Bitcoin miners find valid blocks by placing the pending transactions, which have been propagated via the nodes, into a block that will become validated as a part of the blockchain.<sup>108</sup> However, the process of finding a valid block is not solved but guessed, and moreover, it is mathematically unlikely that two separate miners are working on an identical approach to find blocks.<sup>109</sup>

This process of finding valid blocks is described in Bitcoin's terminology as mining, a phrase that Narayanan et al. compares to the mining the mineral gold due to the randomness and luck involved in the process.<sup>110</sup> As a result of the stochasticity of finding new valid blocks, mining Bitcoins becomes a system of chance and luck.<sup>111</sup> Mining is monitored autonomously by the Bitcoin protocol and altered accordingly so that blocks are

---

<sup>107</sup> Narayanan et al., 67.

<sup>108</sup> Narayanan et al., 64–68.

<sup>109</sup> Narayanan et al., 107.

<sup>110</sup> Narayanan et al., 104.

<sup>111</sup> Narayanan et al., 107.

made at an approximately steady rate. Bitcoin incorporates an algorithm that alters the difficulty of solving the next block based on the computing power of the entire Bitcoin network to ensure that new blocks are not created any slower or faster than roughly every 10 minutes.<sup>112</sup> Mining Bitcoin is considered competitive because even though there may be a huge number of computers worldwide dedicated to mining, there can only be one validated block found and rewarded in each interval.<sup>113</sup>

Miners are also responsible for finding a consensus in the blockchain through a mechanism called proof-of-work. By searching for the next valid block, miners also verify the last known distributed valid block in the network. Because the Bitcoin network is peer-to-peer and distributed throughout the globe, and there can only be one valid Bitcoin blockchain, Bitcoin miners seek to validate the longest chain available in a process called *distributed consensus*.<sup>114</sup> As long as a simple majority of miners and nodes in the network are honest in a distributed consensus, the blockchain is protected from malicious actors that seek to disrupt the network.<sup>115</sup>

Miners are incentivized to mine Bitcoin through two established system of rewards provided through the Bitcoin protocol. The first incentive and largest payoff for miners is the block reward. Since there are many miners competing to find the next valid block at an interval of every 10 minutes, the block reward essentially becomes “a payment to the [miner] in exchange for the service of creating a block on the consensus chain.”<sup>116</sup> In addition to incentivizing miners to mine Bitcoin, block rewards also act as Bitcoin’s only coin creation process by adding bitcoins at an established rate to add the total worldwide supply of the currency.<sup>117</sup>

---

<sup>112</sup> Narayanan et al., 107–8.

<sup>113</sup> There can be multiple blocks validated or relayed in Bitcoin in a phenomenon known as a “fork;” however, the Bitcoin protocol is designed to prevent a small number of forks from affecting its service. Note this thesis does not discuss blockchain forks in detail. Narayanan et al., 69, 73–74.

<sup>114</sup> Narayanan et al., 28–34.

<sup>115</sup> Narayanan et al., 34–38.

<sup>116</sup> Narayanan et al., 39.

<sup>117</sup> Narayanan et al., 39.

The second incentive for mining Bitcoin are transaction fees. When a transaction is made with bitcoin, a small transaction fee is also included. The miner who first places that transaction into a block that is included on the blockchain receives that transaction fee as payment for his or her service.<sup>118</sup>

Mining Bitcoin can be rather profitable. For example, in early March 2018, miners who found new blocks were given a block reward of 12.5 bitcoins, a total reward worth approximately 137,500 USD.<sup>119</sup> However, the supply of remaining bitcoins rewards is decreasing. Of the 21 million bitcoins that will ever be mined, only 20 percent remain.<sup>120</sup> As a result, mining has become a competitive business, and professional mining centers filled with computers dedicated to the Bitcoin mining process have been popping up around the globe.<sup>121</sup> These sophisticated mining centers are hundreds of thousands of times more efficient than the average household computers and have a much higher probability of finding the blocks; however, these centers have come at a cost to the Bitcoin ecosystem.

As discussed before, the Bitcoin protocol consistently increases the difficulty of finding new blocks so even with advances in computer efficiency and capabilities, computers still need to work harder to mine Bitcoins. As a consequence, large mining facilities require a significant amount of energy to operate, generate a large amount of heat, and have corresponding ecological impacts in the form of damage to the environment.<sup>122</sup>

---

<sup>118</sup> Narayanan et al., 39–40.

<sup>119</sup> On 1 March 2018, the approximate value for a single bitcoin was 11,000 USD. “Cryptocurrency Market Capitalizations;” “Bitcoin Block Reward Halving Countdown,” accessed March 5, 2018, <http://www.bitcoinblockhalf.com/>.

<sup>120</sup> Molly Jane Zuckerman, “80% of All Bitcoins Already Mined, Only 4.2 Million Coins Left until Supply Cap,” *Cointelegraph*, January 15, 2017, <https://cointelegraph.com/news/80-of-all-bitcoins-already-mined-only-42-million-coins-left-until-supply-cap>.

<sup>121</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 117–19.

<sup>122</sup> Narayanan et al., 119–124.



#### **D.     TRANSACTIONING WITH BITCOIN: VIRTUAL WALLETS, CRYPTOCURRENCY EXCHANGES, THE BITCOIN ECOSYSTEM, AND OTHER CRYPTOCURRENCIES**

This section of the chapter builds upon the previously discussed information in this chapter to outline the digital aspects of cryptocurrency that provide anonymity to the user, access to value stored in the blockchain, and the cryptocurrency ecosystem which has developed since Bitcoin's release.

##### **1.     Virtual Wallets and Transactions**

To transact with bitcoin, a user must first create a virtual wallet. A virtual wallet is software with a digital address that allows access to the Bitcoin blockchain for purchases, transfers, and store of bitcoins.<sup>123</sup> It would be a misnomer if a person was to say that he or she "sent" or "receive bitcoins" to a virtual wallet. During transactions, bitcoins are not sent to individual wallets—in actuality, bitcoins are not sent anywhere—but instead they are permanently listed on the blockchain's public ledger, noting that a bitcoins balance transfer has occurred.<sup>124</sup>

Virtual wallets are comprised of two hash outputs of 64-digit strings (see Figure 1.) which make up the public key and secret key. The virtual wallet allows Bitcoin users' identities to considered pseudonymous, because buyers and sellers are only identified by their public wallet address; moreover, a user is not restrained to a single wallet may choose to create an unlimited amount of wallets.<sup>125</sup> Narayanan et al. note that the public key acts as the "identity of a person or an actor in a system . . . [and] the consequence of treating public keys as identities is that you can make a new identity whenever you want."<sup>126</sup>

The secret key acts like a secret signature, which Narayanan et al. describe as "existentially unforgeable."<sup>127</sup> The private key's role is to verify the public key and to

---

<sup>123</sup> Narayanan et al., 77.

<sup>124</sup> Vigna and Casey, *The Age of Cryptocurrency*, 124–125.

<sup>125</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 139.

<sup>126</sup> Narayanan et al., 19.

<sup>127</sup> Narayanan et al., 15–16.

validate the transaction by the sender; therefore, for a transaction to occur, a sender of bitcoin must know the public and private key of the wallet she or he wishes to send from and the public identity of the recipient.<sup>128</sup> A visual of a transaction chain is depicted in Figure 4 from the original Bitcoin whitepaper.<sup>129</sup> The drawback of this system is that if malicious actors gain access to a linked public and private key, they can steal the identity of their victim as well as the entire balance of bitcoins out of the compromised wallet.<sup>130</sup>

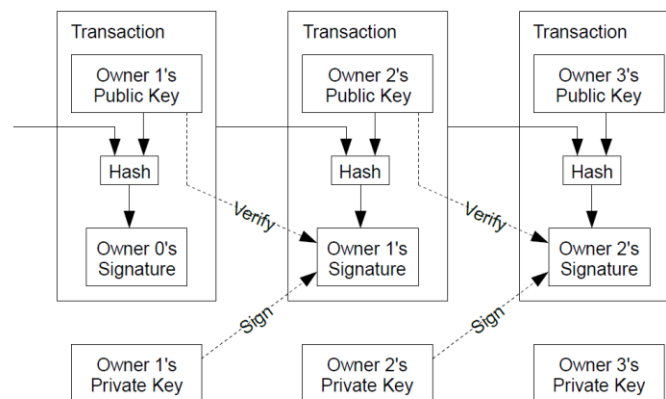


Figure 4. A Chain of Transactions Depicting the Ownership of Bitcoins with Public Keys and Private Keys<sup>131</sup>

Since virtual wallets are simply the combination of a private and public key providing access to the Bitcoin public ledger, the wallet can be stored either online, digitally on a computer, or completely separate from a computer on a piece of paper or physical device.<sup>132</sup> According to Narayanan et al., each of these methods offers its own advantages and disadvantages regarding availability, security, and convenience; however, the downside to all methods of storing bitcoin is that if a user loses or forgets his private

<sup>128</sup> Narayanan et al., 16.

<sup>129</sup> Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."

<sup>130</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 76.

<sup>131</sup> Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2.

<sup>132</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 76–83.

key, the user will lose access to his bitcoins.<sup>133</sup> When a user loses or forgets his or her private key, the bitcoins stored in that wallet become lost, unrecoverable or unspent and still apart of the total bitcoin supply. Lost bitcoins are somewhat common, and Roberts and Rapp, estimate there are nearly 4 million bitcoins or 23 percent of the total mined bitcoins that are lost forever.<sup>134</sup>

However, Bitcoin transactions are not completely anonymous and can still be tracked. Narayanan et al. explain

Linking a bitcoin address to real-world identities is often easy. If you interact with Bitcoin business—be it an online wallet service, exchange or other types of merchant—they usually want your real-world identity for transactions with them. For example, an exchange might require your credit card details, or a merchant will need your shipping address.<sup>135</sup>

Since the blockchain maintains a public historical record of every bitcoin transaction that has ever occurred, an entity like law enforcement could easily track the flow of bitcoins between known public addresses.<sup>136</sup> The true challenge of tracking the flow of bitcoins lies with linking addresses to real-world identities.

## **2. Bitcoin Exchanges and the Cryptocurrency Ecosystem**

According to Bitcoin.org, an individual may acquire bitcoins through purchase at a Bitcoin exchange, as a transaction for goods or services, through mining Bitcoins, and by exchanging fiat to bitcoins with another individual.<sup>137</sup> This chapter has already discussed mining, virtual wallets, and how to transact with bitcoins; this section focuses on the cryptocurrency exchanges.

---

<sup>133</sup> “Bitcoin Block Reward Halving Countdown,” 76.

<sup>134</sup> Jeff Roberts and Nicolas Rapp, “Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says,” *Fortune*, November 25, 2017, <http://fortune.com/2017/11/25/lost-bitcoins/>.

<sup>135</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 139.

<sup>136</sup> Narayanan et al., 139.

<sup>137</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 171; “FAQ—Bitcoin,” accessed April 3, 2018, <https://bitcoin.org/en/faq>.

Bitcoin exchanges, if legal in the individual's country, are arguably the easiest way to obtain bitcoins for fiat currency. Narayanan et al. describe

Bitcoin exchanges are businesses that—at least from the user interface standpoint—function in a similar way to banks. They accept deposits of bitcoins and will, just like a bank, promise to give them back on demand later. . . . You can also exchange bitcoins for fiat currency or vice versa. ... the big [advantage] is that exchanges help connect the Bitcoin economy and the flows of bitcoins with the fiat currency economy, so that it's easy to transfer value back and forth.<sup>138</sup>

Because cryptocurrency exchanges operate as private businesses, they are subject to the laws and regulations of the exchanges host nation. For example, a popular U.S. cryptocurrency exchange is Coinbase, which is based in San Francisco and available to 32 countries worldwide but subject to U.S. regulation.<sup>139</sup> If an individual would like to obtain bitcoin through Coinbase, she or he would first need to register with the company and then use a wire transfer, credit card, or bank account to exchange U.S. dollars for bitcoins.

Contrary to some opinions, Bitcoin is not a Ponzi or pyramid scheme. The currency obtains its value through the economic principles of supply and demand. As *Bitcoin Magazine* states, “Bitcoin derives its unique value from the fact that despite its lack of official backing or wide acceptance, it has generated an ecosystem in which many people are willing to trade and accept it.”<sup>140</sup> As a consequence of this system, the price of a single bitcoin often fluctuates and is considered volatile since the value of the cryptocurrency is not fixed to any physical commodity like gold is or guaranteed by any country.

Since the inception of Bitcoin, the cryptocurrency has had varying levels of acceptance worldwide as a currency. Vigna and Casey point out that major merchants have accepted Bitcoin as a form of payment, including “Overstock.com, the Sacramento Kings basketball team, Dell computers, and the travel site Expedia” for example and “sixty-seven

---

<sup>138</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 89.

<sup>139</sup> “About Coinbase,” Coinbase, accessed April 3, 2018, <https://www.coinbase.com/about?locale=en-US>.

<sup>140</sup> “What Makes Bitcoin Valuable?,” *Bitcoin Magazine*, accessed April 4, 2018, <https://bitcoinmagazine.com/guides/what-makes-bitcoin-valuable/>.

thousand [other] merchants by the end of June 2014.”<sup>141</sup> In addition to major retailers accepting bitcoin, every day users can interact, exchange, and store wealth in bitcoin via Bitcoin ATMs.<sup>142</sup> Bitcoin ATMs operate much in the same manner as bank ATMs, only that instead of transacting solely with a bank, a customer can also exchange wealth in the form of credit or debit cards from or into the Bitcoin blockchain. As of March 2018, there are 2648 Bitcoin ATMs worldwide in dozens of countries.<sup>143</sup>

### 3. Other Cryptocurrencies

Since the conception of Bitcoin, numerous other cryptocurrencies have emerged, each with their own unique approach as a type of currency. These alternative cryptocurrencies, or *altcoins*, can transact and trade on exchanges much of the same ways that Bitcoin can and have their own values separate from Bitcoin based on supply and demand.<sup>144</sup> Examples of other popular altcoins at the time of writing based on the total market capitalization of each coin include Ethereum, Litecoin, Ripple, and Bitcoin Cash (Bcash).<sup>145</sup>

Altcoins may have different properties from those listed in this chapter. For example, largely on the design of Bitcoin with a few exceptions, Litecoin mines new blocks at a rate of 2.5 minutes rather than Bitcoin’s 10 minute interval between mining blocks.<sup>146</sup> Another example is Ripple, a cryptocurrency that is open source, yet proposes a centralized governance through a parent company and corporate investors.<sup>147</sup> Despite different variations in how each altcoin functions, most coins enjoy many of same benefits of

---

<sup>141</sup> Vigna and Casey, *The Age of Cryptocurrency*, 103.

<sup>142</sup> Vigna and Casey, 103–105.

<sup>143</sup> “Bitcoin ATM Industry Statistics Charts,” accessed April 5, 2018, <https://coinatmradar.com/charts/>.

<sup>144</sup> Narayanan et al., Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 250–252.

<sup>145</sup> “Cryptocurrency Market Capitalizations.”

<sup>146</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 248.

<sup>147</sup> David Evans, “Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms” (working paper, Coase-Sandor Institute for Law and Economics at Chicago Unbound, 2014), [https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=2349&context=law\\_and\\_economics](https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=2349&context=law_and_economics), 16.

Bitcoin. Consequently, according to Narayanan et al., the cryptocurrencies compete on the free marketplace of cryptocurrency exchanges for dominance as the most valuable currency, and users choose the coin that they deem having the most valuable features.<sup>148</sup>

## **E. CONCLUSION**

This chapter's intent has been to provide a brief synopsis of how cryptocurrencies like Bitcoin operate and to link cryptocurrency functionality to the potential for governmental regulation. The different dimensions of the processes this thesis discusses build upon in later chapters to offer talking points for future regulations and restrictions to limit or adopt cryptocurrencies. Bitcoin has proven itself as an innovative and resilient form of currency promoting new challenges to the state's sovereign ability to regulate currency within its boundaries. The following chapters reference concepts of the blockchain, pseudonymous digital identities and wallets, cryptocurrency exchanges, the cryptocurrency ecosystem, and the altcoin.

The author chose this chapter's information under the pretense of linking cryptocurrency functionality to the potential for government enforcement of regulations or restrictions; therefore, the thesis references these concepts later. This chapter—by no means—completely covers the mathematics, technology, history, functionality, and applications of cryptocurrencies.<sup>149</sup>

---

<sup>148</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 251.

<sup>149</sup> For further reading on the Bitcoin ecosystem or the technology in cryptocurrencies, refer Narayanan et al., *Bitcoin and Cryptocurrency Technologies*.

### **III. BANNING CRYPTOCURRENCIES**

Chapter II explained the relevant basics of cryptocurrency and the aspects of the cryptocurrency ecosystem, which apply to this thesis. This chapter builds upon the information in the previous chapters, focusing on the interaction between cryptocurrency and the sovereign state to expound upon historical examples of states prohibiting virtual currencies and the reasons why and the methods how they have.

As stated in the introduction of this thesis, cryptocurrencies challenge the sovereignty of states due to the growing popularity of cryptocurrencies as an alternative—and unregulated—form of currency with which to transact. Consequently, this thesis assumes that states will attempt to gain control on cryptocurrency by passing legislation targeting cryptocurrency users, designers, or the cryptocurrencies themselves. However, this chapter specifically focuses on reasoning and methods of states that have partially or completely prohibited cryptocurrencies.

This chapter on banning cryptocurrency is divided into five sections, starting with the first section detailing the reasons why a country might opt for a partial or total ban of cryptocurrencies. The second section lists the different aspects of cryptocurrency a state could choose to regulate to limit domestic cryptocurrency use. The third section provides a limited list and background of the sovereign states with an official stance either partially or completely against cryptocurrency. The fourth section discusses the effectiveness state-backed regulation has had on prohibiting cryptocurrency transactions. The final section consists of the conclusion and key findings.

#### **A. WHY STATES CHOOSE TO BAN VIRTUAL CURRENCIES**

After surveying the literature available, this chapter identifies five common reasons why states might choose to ban cryptocurrencies. Although there are certainly other reasons that would drive a state toward the prohibition of virtual currencies, this chapter narrows its discussion to the five factors most frequently mentioned in this thesis's research. The five provocations that might lead a state to ban cryptocurrency are

- bitcoin's continued use as a method of payment within criminal networks
- the weakening of the state's ability to control the capital flow wealth, domestically and internationally, in decentralized cryptocurrency transactions
- to restrict citizens ability to rally against the state and reduce the civil rights of the people
- to eliminate competing virtual currencies in preparation for the release of a state-backed cryptocurrency
- to eliminate the major fiscal and infrastructure drains cause by miners on the state controlled energy grid

## 1. Bitcoin and Crime

One potential reason why a state might suppress cryptocurrencies is to reduce domestic crime, or at least make the payment for crimes less rewarding. One of the major reasons why Bitcoin gained popularity—and the eye of the U.S. government—has been the cryptocurrency's preference as a preferred currency in the Darknet.<sup>150</sup> For example, the Silk Road, which is considered by many scholars to have been the most infamous Darknet marketplace, exclusively accepted bitcoins for illicit drugs and services. In fact, the Silk Road operated unopposed for over two years—despite governmental knowledge of the website—until the Federal Bureau of Investigation (FBI) finally pinpointed and arrested the dark website's founder in October of 2013.<sup>151</sup> Moreover, by Lawrence Trautman's account, Bitcoin transactions have been tied to a number of illicit cases of the Darknet, including paid assassinations, attacks on businesses, child exploitation and pornography, corporate espionage, drugs, fake IDs and passports, investment schemes, sexual exploitations, and stolen credit cards.<sup>152</sup>

There are a number of reasons why illicit actors would choose cryptocurrencies to transact with over traditional fiat. In Trautman's research, he reveals the five reasons why the U.S. Secret Service views virtual currencies as a threat, stating they offer criminals:

---

<sup>150</sup> Christin, "Traveling the Silk Road."

<sup>151</sup> Vigna and Casey, *The Age of Cryptocurrency*, 86.

<sup>152</sup> Lawrence Trautman, "Virtual Currencies Bitcoin and What Nowafter Liberty Reserve, Silk Road, and Mt. Gox?," *Richmond Journal of Law & Technology* 20, no. 4 (2014): 2–5.



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, which results in lower exchange risk, increasing the digital currency's ability to be an efficient means to transmit and store wealth.
4. Widespread adoption in the criminal underground.
5. Trustworthiness.<sup>153</sup>

The correlation between Bitcoin and illicit activity has not gone unnoticed by the international community, and, as discussed later in the chapter, several governments blame the connection between Bitcoin and criminal enterprises as a motive for prohibiting virtual currencies.

## **2. Increase the State's Capital Controls**

One of the most attractive features that cryptocurrencies possess is the ability to transact seamlessly across sovereign state borders, intrinsically bypassing the regulations, taxes, tariffs, or sanctions to which traditional fiat currency is subject. By circumventing the fees associated with fiat, international cryptocurrency transactions are cheaper for both payees and recipients. Even though cryptocurrencies may provide substantial economic incentives for both merchants and customers, cryptocurrencies also possess significant negative drawbacks for the state. As Narayanan et al. point out, cryptocurrencies can defeat capital controls, which are defined as the “rules or laws that a country has in place that are designed to limit the flow of capital (money and other sets) into or out of the country.”<sup>154</sup> Capital controls are important and effective tools states, especially states in economic crisis, can use to stabilize the economy.

---

<sup>153</sup> Trautman, 3.

<sup>154</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 178.

Thus, a potential solution of a state fearing capital flight<sup>155</sup>—due to political or economic instabilities—could be to ban cryptocurrencies or cryptocurrency exchanges. Narayanan et al. surmise, “a government that wants to enforce capital controls in a world with Bitcoin has to try and disconnect the Bitcoin world from the local fiat currency banking system.”<sup>156</sup> Similarly, the IMF writes that “instead of purchasing foreign currency subject to government-imposed limitations, market participants can purchase VCs on the Internet and use them to conduct Internet-based foreign exchange transactions or make capital transfers that would otherwise be prohibited.”<sup>157</sup> By banning cryptocurrencies or enacting legislation that would increase the difficulty of exchanging fiat to cryptocurrency, sovereign states complicate the process by which wealth is exported outside of a nation. For example, China and Iceland both cite concerns about their right to control capital as a reason for their crackdown on cryptocurrencies, and this chapter discusses both countries in more detail later.<sup>158</sup>

### **3. To Limit Civil Rights**

Another potential motive for the state to impede the use of cryptocurrencies—exclusive to the more authoritarian systems of state control—would be to constrain or limit social movements or the peoples’ civil rights. The same benefits of anonymity, trustworthiness, and expediency that cryptocurrencies offer criminal networks could also benefit the civil rights movements within restrictive states. The unique features of cryptocurrencies could facilitate transactions for social movement leaders hiding from the heavy hand of the state. For example, Matthew Ponsford writes that the Chinese restriction

---

<sup>155</sup> According to Investopedia, “Capital flight is a large-scale exodus of financial assets and capital from a nation due to events such as political or economic instability, currency devaluation or the imposition of capital controls.” Elvis Picardo, “Capital Flight,” Investopedia, January 5, 2004, <https://www.investopedia.com/terms/c/capitalflight.asp>. To read more, also see “Capital Flight,” Investopedia, accessed October 15, 2017, <https://www.investopedia.com/terms/c/capitalflight.asp#ixzz5Czww8Th0>.

<sup>156</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 178.

<sup>157</sup> Dong He et al., *Virtual Currencies and beyond: Initial Considerations*, IMF Discussion Note SDN/16/03 (Washington, DC: International Monetary Fund, 2016), <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>.

<sup>158</sup> Primavera De Filippi, “Bitcoin: A Regulatory Nightmare to a Libertarian Dream,” *Internet Policy Review* 3, no. 2 (May 2014): 5, <https://doi.org/10.14763/2014.2.286>.

on Bitcoin is a byproduct of the restriction on the freedom of speech in China, remarking “bloggers, outspoken activists, or ‘revolutionaries’” could use technology like Bitcoin as methods of payment to skirt around the restrictive state controls on free speech.<sup>159</sup>

#### **4. To Introduce a State-backed Cryptocurrency**

One of the more interesting phenomenon research for this thesis discovered is the correlation between states choosing to prohibit aspects of decentralized virtual currencies that also plan to release their own respective state-controlled virtual currency. For example, in 2014, Ecuador enacted legislation that outlawed all cryptocurrencies, and then introduced its own electronic virtual currency.<sup>160</sup> Lawrence White of the Cato Institute points out that the legislation “gave the state a monopoly in electronic money ... [and] barred the private mobile phone companies and private financial institutions from providing competing systems.”<sup>161</sup>

Nonetheless, Ecuador’s experiment with electronic currency was short lived, lasting only four years and costing billions of dollars to upkeep.<sup>162</sup> White’s analysis of the Ecuadorian project points to a combination of factors that led to a lack of popularity and ultimately the electronic currency’s downfall and he cites a lack of trust in the central bank, a less than convenient exchange system, and a reluctance from the citizens to disregard the heavily used and trusted U.S. dollar.<sup>163</sup>

---

<sup>159</sup> Matthew P. Ponsford, “A Comparative Analysis of Bitcoin and Other Decentralized Virtual Currencies: Legal Regulation in the People’s Republic of China, Canada, and the United States,” *Jolt Digest* (blog), November 2015, <http://jolt.law.harvard.edu/digest/a-comparative-analysis-of-bitcoin-and-other-decentralized-virtual-currencies-legal-regulation-in-the-peoples-republic-of-china-canada-and-the-united-states>.

<sup>160</sup> “Ecuador Bans Bitcoin, Initiates Government-Run Digital Currency,” *PanAm Post* (blog), last updated July 25, 2014, <https://panampost.com/panam-staff/2014/07/25/ecuador-bans-bitcoin-initiates-government-run-digital-currency/>.

<sup>161</sup> Lawrence H. White, “The World’s First Central Bank Electronic Money Has Come—and Gone: Ecuador, 2014–2018,” *Cato at Liberty* (blog), April 2, 2018, <https://www.cato.org/blog/worlds-first-central-bank-electronic-money-has-come-gone-ecuador-2014-2018>.

<sup>162</sup> White.

<sup>163</sup> White.

Nevertheless, a sovereign state could attempt to introduce its own respective cryptocurrency and revise its approach to banning and adopting cryptocurrency from the lessons learned in Ecuador. For example, government officials in China announced in late March 2018 that the central bank intends to “launch a crackdown” on all virtual currencies, while simultaneously pushing “forward the research and development of its own digital currency.”<sup>164</sup>

## **5. To Eliminate the Excessive Energy Consumption in Mining**

As emphasized in Chapter II, mining Bitcoins can be extremely profitable but, as a requirement, the process requires a tremendous amount of energy. Depending on the price of electricity, the cost of power is often the largest expense in mining; therefore, miners will seek the greatest return on investment in countries where electricity is cheap, or the state subsidizes electricity to the people.<sup>165</sup> In such circumstances, mining becomes a physical and economic strain on the electrical grid, and a government could potentially outlaw or limit the mining of cryptocurrencies.

A recent example of this occurred in early 2018 when China began to reduce the available power output to miners as a part of a greater long-term cryptocurrency crackdown.<sup>166</sup> Similarly, Venezuela has taken actions against Bitcoin miners, despite an official government stance permitting cryptocurrency trading and ownership within the state. In 2017, Venezuela arrested Bitcoin miners, alleging they used 300 mining units to commit cyber fraud and power theft.<sup>167</sup>

---

<sup>164</sup> “China Central Bank Will Launch Crackdown on Virtual Currencies,” Reuters, March 29, 2018, <https://www.reuters.com/article/us-china-finance-digital-currency/china-central-bank-will-launch-crackdown-on-virtual-currencies-idUSKBN1H515L>.

<sup>165</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 121–123.

<sup>166</sup> Sara Hsu, “China’s Shutdown of Bitcoin Miners Isn’t Just about Electricity,” *Forbes*, January 15, 2018, <https://www.forbes.com/sites/sarahsu/2018/01/15/chinas-shutdown-of-bitcoin-miners-isnt-just-about-electricity/>.

<sup>167</sup> Tim Worstall, “Congratulations to Venezuela—Bitcoin Miners Arrested for Stealing Free Electricity,” *Forbes*, January 27, 2017, <https://www.forbes.com/sites/timworstall/2017/01/27/congratulations-to-venezuela-bitcoin-miners-arrested-for-stealing-free-electricity/>.

## B. MECHANISMS TO BAN VIRTUAL CURRENCIES

Regardless of the reason for banning cryptocurrencies, the end goal of a partial or complete ban on cryptocurrencies is to discourage the use of cryptocurrency as a medium of transactions within a sovereign state. From the literature this thesis research, there are two separate avenues a government must approach to achieve the intended results of prohibiting virtual currencies. The state's regulatory body must choose which aspects, if not all of them, to restrict, and then the state must determine how much punishment is required to enforce the policies.

According to a November 2015 digital currency report for the Bank for International Settlements (BIS), there are five restrictive areas a state could target to prohibit or discourage cryptocurrency: retail transactions, acceptance by retailers, use as financial instruments, currency exchanges, or transactions between banks.<sup>168</sup> The report also comments, "Authorities could seek to ban the use of digital currencies in their respective jurisdictions. Practically, this could imply a ban on any digital currency-based financial activities, as well as digital currency exchanges or digital currency acceptance by retailers."<sup>169</sup>

Even if a sovereign state chooses to restrict a specific area of cryptocurrency, the state must also demonstrate the means to enforce the policies if it is to be successful in disrupting domestic cryptocurrency use. Joshua Hendrickson and William Luther released a study titled "Banning Bitcoin," in which they analyze the size of the state needed and the punishments require, to stop alternative currencies from functioning within a state.<sup>170</sup> Hendrickson and Luther find that

A government can prevent an alternative [currency] from circulating if it is willing and able to mete out sufficiently severe punishments. ...

---

<sup>168</sup> Committee on Payments and Market Infrastructures, *Digital Currencies*, 12–13.

<sup>169</sup> Committee on Payments and Market Infrastructures, 12.

<sup>170</sup> Joshua Hendrickson and William Luther, "Banning Bitcoin," *Journal of Economic Behavior & Organization* 141 (September 2017): 194.

Sovereignty—that is, the ability of some agents to govern the behaviors of others—is a function of both size and power.<sup>171</sup>

Furthermore, Hendrickson and Luther conclude from their research that a government of a sufficient size can prevent cryptocurrencies from circulating as a form of money without the need for punishments and completely ban a virtual currency if it can effectively punish individuals challenging the ban.<sup>172</sup> Both the BIS report and “Banning Bitcoin” provide the hypothetical necessities required to prohibit cryptocurrencies. The next section of this chapter examines the countries that have implemented restrictions on cryptocurrencies.

### **C. COUNTRIES THAT HAVE BANNED CRYPTOCURRENCIES.**

Decentralized cryptocurrencies pose a new and dynamic challenge to sovereign states; thus, by nature of the cryptocurrencies novelty, the international community remains divided on what action should be taken to confront cryptocurrencies. To cover the various methods states can respond to lawlessness of decentralized cryptocurrencies, this chapter provides short case studies on sovereign states that have enacted laws partially or completely prohibiting the domestic use of virtual currencies.

The case studies in this section are divided into three groups: the sovereign states that have blanket legislation to prohibit cryptocurrencies, the systematic prohibition of cryptocurrencies in China, and the case of Iceland wherein separate aspects of cryptocurrencies are both banned and encouraged. Of the three case studies in this section, the discussion on China’s regulations provides the most detail and sections later in this chapter draw on it when discussing the effectiveness of banning cryptocurrencies.

This chapter focuses on China as the prime case study example for three reasons. First, China has approached the prohibition of cryptocurrency methodically, gradually instituting new laws since 2013. Second, China appears to have had success in disrupting

---

<sup>171</sup> Hendrickson and Luther, 194.

<sup>172</sup> Hendrickson and Luther, 194.

its domestic cryptocurrency networks. Finally, China's actions have had a notable corresponding effect on the international cryptocurrency marketplace.

### **1. Countries That Have Banned Bitcoin: Bangladesh, Bolivia, Ecuador, Kyrgyzstan, and Nigeria**

As of March of 2018, five countries have adopted legislation that makes owning or transacting with cryptocurrencies illegal. For example, in 2017, the country of Bangladesh has outlawed Bitcoin and other virtual currencies. According to Bangladeshi law, transactions using Bitcoin or other virtual currencies are illegal, and violators are subject to a sentence of up to 12 years in prison.<sup>173</sup> Kyrgyzstan also released similar guidance in 2014, when the Kyrgyz government barred its citizens from using virtual currencies.<sup>174</sup>

As discussed in the previous section, in Ecuador the “issuance, promotion or circulation of virtual currencies” is illegal.<sup>175</sup> Likewise, as per the Central Bank of Bolivia's directory resolution n044/2014, all “currency or coins not issued or regulated by the government, including a list of virtual currencies” are prohibited.<sup>176</sup> The Bolivian government has also proven itself keen to enforce the policy, arresting 60 of its citizens in May for using bitcoins and altcoins as investments.<sup>177</sup> Nigeria offers a more recent example of a state initiating an official stance on cryptocurrencies. As of early 2017, the Central Bank of Nigeria banned virtual currencies, stating “transactions in VCs are largely

---

<sup>173</sup> Abdur Rahim Harmachi, “Bangladesh Bank Warns against Transaction in ‘Illegal’ Bitcoin, Other Cryptocurrencies,” *Bbnews24*, December 28, 2017, <https://bdnews24.com/economy/2017/12/27/bangladesh-bank-warns-against-transaction-in-illegal-bitcoin-other-cryptocurrencies>, sec. Economy.

<sup>174</sup> “Warning of the National Bank of the Kyrgyz Republic: On the Spread and Use of the ‘virtual Currency,’ in Particular, Bitcoins (Bitcoin),” Kyrgyz Bank, July 18, 2014, <http://www.nbkr.kg/searchout.jsp?item=31&material=50718&lang=ENG>.

<sup>175</sup> “Digital Currencies: International Actions and Regulations,” Perkins Coie, last updated April 26, 2018, <https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html>.

<sup>176</sup> “Digital Currencies.”

<sup>177</sup> Aaron van Wirdum, “Bolivian Authorities Arrest 60 ‘Cryptocurrency Promoters,’” *Bitcoin Magazine*, May 29, 2017, <https://bitcoinmagazine.com/articles/bolivian-authorities-arrest-60-cryptocurrency-promoters/>.

untraceable and anonymous making them susceptible to abuse by criminals, especially in money laundering and financing of terrorism.”<sup>178</sup>

## **2. China**

Of all of the nations that have attempted to ban cryptocurrency, the People’s Republic of China (PRC) has taken the most substantial actions to limit domestic cryptocurrency use in what could be described as the systematic installment of laws to discourage cryptocurrency use inside of Chinese borders. Starting in 2013, the People’s Bank of China (PBOC)—the state controlled central bank of China—enacted the country’s first step toward prohibiting cryptocurrency use when the state barred Chinese based financial institutions from using bitcoin as a method of transaction.<sup>179</sup> By December 4, 2013, the PBOC had advised commercial banks to prohibit “settlement or payments related to bitcoin. It also barred trust companies and fund-management firms from making bitcoin-related investments and advised insurers not to insure bitcoins.”<sup>180</sup>

Matthew Ponsford points out that in addition to the new Chinese restrictions on Bitcoin in 2013, China also instituted new requirements to the financial sector, requiring all Chinese-based cryptocurrency exchanges and trading platforms to “register with the Ministry of Industry and Information Technology ... [and] Telecommunication Bureau.”<sup>181</sup> Shortly after the 2013 restrictions, China further clamped down on domestic cryptocurrencies use when it ordered that all bitcoin trading accounts to shut down by April 15, 2014.<sup>182</sup>

---

<sup>178</sup> Kevin Amugo, *Circular to Banks and Other Financial Institutions on Virtual Currency Operations in Nigeria* (Abuja, Nigeria: Central Bank of Nigeria, 2017), <https://www.cbn.gov.ng/out/2017/fprd/aml%20january%202017%20circular%20to%20fis%20on%20virtual%20currency.pdf>.

<sup>179</sup> “China Bans Financial Companies from Bitcoin Transactions,” Bloomberg News, December 5, 2013, <https://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions>.

<sup>180</sup> Grace Zhu, “China Central Bank Warns Banks on Bitcoin,” *Wall Street Journal*, May 7, 2014, <https://www.wsj.com/articles/china-central-bank-warns-banks-on-bitcoin-1399454876>, sec. Markets.

<sup>181</sup> Ponsford, “A Comparative Analysis.”

<sup>182</sup> Chao Deng and Lingling Wei, “China Cracks Down on Bitcoin,” *Wall Street Journal*, April 1, 2014, <https://www.wsj.com/articles/china-cracks-down-on-bitcoin-1396361492>, sec. Markets.



More recently, China has directed its laws toward the restriction of mechanisms in cryptocurrency allowing individuals to create or mine new currencies. In late 2017, Chinese regulators moved to ban Chinese public and corporate fundraising through initial coin offerings (ICO), a method commonly used to raise capital for new cryptocurrencies prior to release.<sup>183</sup> China has since doubled-down on its anti-ICO policy. Starting in February of 2018, the state officially discouraged Chinese companies abroad from issuing ICOs and started to block domestic Chinese Internet access to cryptocurrency development or trading websites.<sup>184</sup> These actions build upon a January 2018 act that limited electricity to cryptocurrency miners and ordered “local governments to make an ‘orderly exit’ from the [cryptocurrency] industry.”<sup>185</sup>

Grant Clark and Lulu Chen list several reasons why China has started to preclude cryptocurrencies, including “cleansing risk from financial markets,” which they describe as “a [Chinese] government mantra for more than two years.”<sup>186</sup> Also, they cite other possible reasons that China has taken such actions against cryptocurrencies, such as targeting the shadow banking sector, eliminating the source of unregulated domestic loans, and limiting methods of moving money internationally.<sup>187</sup>

A more transparent reason why the Chinese government assesses cryptocurrency as a threat is because of its ability to export capital overseas. Chinese regulation on capital controls limit the maximum outflow of yuan at 50,000 USD per person, per year.<sup>188</sup> Instead of storing wealth in Chinese banks where the currency inflation is greater than the interest

---

<sup>183</sup> Saheli Roy Choudhury and Barry Huang, “Chinese ICOs: China Bans Fundraising through Initial Coin Offerings, Report Says,” *CNBC*, September 4, 2017, <https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html>.

<sup>184</sup> Sara Hsu, “China Serious about Ending ICOs, Cryptocurrency Exchanges,” *Forbes*, February 7, 2018, <https://www.forbes.com/sites/sarahsu/2018/02/07/china-serious-about-ending-icos-cryptocurrency-exchanges/>.

<sup>185</sup> Hsu, “China’s Shutdown of Bitcoin Miners.”

<sup>186</sup> Grant Clark and Lulu Yilun Chen, “How China’s Stifling Bitcoin and Cryptocurrencies: QuickTake,” Bloomberg News, last updated February 27 2018, <https://www.bloomberg.com/news/articles/2018-01-09/how-china-s-stifling-bitcoin-and-cryptocurrencies-quicktake-q-a>, sec. Technology.

<sup>187</sup> Clark and Chen.

<sup>188</sup> Emily Parker, “Even China Can’t Destroy Bitcoin,” *MIT Technology Review*, December 11, 2017, <https://www.technologyreview.com/s/609320/can-china-contain-bitcoin/>.

gained, Chinese investors and businessmen can use cryptocurrencies as a means to deport wealth to other nations where their investments will be worth more. Ever vigilant to prevent capital flight, China views Bitcoin and other cryptocurrencies as a threat to the Chinese economy because it offers a new unregulated capital export option for wealthy Chinese citizens looking to invest abroad.

To date, even though it is illegal to transact with cryptocurrencies, the PRC still allows its citizens to own them; however, this may change in the future. In an effort to discourage the domestic attraction of cryptocurrencies, the Chinese government and central bank have attacked the aspects allowing cryptocurrencies to operate as money, including the cryptocurrency exchanges that offer Chinese citizens access to the monetary world outside of the communist state. In any event, the effect that China has had on the domestic and international cryptocurrency market, irrespective of the cause for the systematic prohibition of digital currency is significant (as this chapter discusses later in detail).

### **3. A Partial Ban in Iceland**

In contrast to the other countries discussed in this chapter, Iceland has taken a different administrative approach to Bitcoin and other virtual currencies. Jack Tatar explains that the Icelandic government—fearful of capital flight following the 2008 economic crisis—passed the 2013 Icelandic Foreign Exchange Act, which permits its citizens to legally own and mine cryptocurrencies yet prohibits “foreign exchange trading” with virtual currencies.<sup>189</sup> Despite the harsh international cryptocurrency trading platform maintained by the government, Iceland remains one of the top locations for mining Bitcoin and other cryptocurrencies.

As companies confront new regulations in their native countries, Iceland offers an attractive combination of cheap power generated by hydroelectric plants, a cold climate to deal with the heat generated during the mining process, and a friendly business environment

---

<sup>189</sup> Jack Tatar, “Iceland—Time to Free Bitcoin!,” The Balance, last updated March 17, 2017, <https://www.thebalance.com/iceland-time-to-free-bitcoin-4030896>.

that promotes the offshoring of international business to the Icelandic mainland.<sup>190</sup> Tatar asserts that although Iceland appears to remain firm in its cryptocurrency capital controls, Bitcoin may prove to be a valuable asset that could pay dividends if the government unshackled its policy on foreign cryptocurrency exchanges.<sup>191</sup>

#### **D. THE EFFECTS OF BANNING CRYPTOCURRENCY**

Gauging the effectiveness of individual state regulations on cryptocurrency is challenging because cryptocurrency ecosystems transcend state borders and provide a significant amount of anonymity to their users. Moreover, cryptocurrencies and cryptocurrency exchanges are commonly referred to as the “wild west,” an analogy comparing the figurative parallels of lawlessness and anarchy prevalent in the cryptocurrency ecosystem to that of the North American frontier.<sup>192</sup> Comparatively, it is these same factors of lawlessness and anarchy confounding how states approach the cryptocurrency dilemma, which also complicates the measurement of state regulation’s effects in the cryptocurrency ecosystem, or the corresponding compliance of citizens with sovereign state’s virtual currency laws.

From the research this thesis effort examines, there appears to be no definitive analysis on the effectiveness of governmental laws and regulations on Bitcoin’s users. The reactivity of markets, the value of bitcoin, fluctuations in user population, the number of daily transactions, and the locations of miners are all suggested methods to measure the pulse of cryptocurrency; however, the application of tools hiding users’ identities, like virtual private networks and the Darknet, can skew data. There are simply too many variables that go into the value of cryptocurrency to provide an in depth analysis in this thesis. Therefore, to steer the discussion toward the questions posed in this thesis, this section focuses on the authors who have made connections between the correlation on the price of bitcoin, response of

---

<sup>190</sup> Rick Noack, “Cryptocurrency Mining in Iceland Is Using So Much Energy, the Electricity May Run Out,” *Washington Post*, February 13, 2018, <https://www.washingtonpost.com/news/worldviews/wp/2018/02/13/cryptocurrency-mining-in-iceland-is-using-so-much-energy-the-electricity-may-run-out/>, sec. WorldViews.

<sup>191</sup> Tatar, “Iceland—Time to Free Bitcoin!”

<sup>192</sup> Steve Stecklow et al., “Chaos and Hackers Stalk Investors on Cryptocurrency Exchanges,” *Reuters*, September 29, 2017, <http://www.reuters.com/investigates/special-report/bitcoin-exchanges-risks/>.

domestic cryptocurrency miners, and exchanges in countries that choose to ban cryptocurrency.

## **1. China's Impact on Cryptocurrencies**

Of all the countries that have enacted laws to restrict virtual currencies, none have had a greater effect on the cryptocurrency ecosystem than China. According to many cryptocurrency enthusiasts and bloggers closely following cryptocurrencies, there is a seemingly apparent connection between the legislation that China passes (or announces), and the price of cryptocurrencies worldwide; however, this thesis could find no scholarly source that verifies, proves, or discredits the claim that China holds significant power over cryptocurrencies. Therefore, this section focuses on the impact Chinese legislation has had on Bitcoin miners and exchanges and the correlation between bitcoin price and news of new Chinese regulations.

China's laws on mining appear to have had an impact on Chinese miners and mining companies within the PRC borders. Grant Clark and Lulu Chen point out that China has changed the entire mining industry after its January legislation limiting electricity to Chinese miners. They explicate, "miners initially flocked to China because of its inexpensive power, local chipmaking factories and cheap labor—now they may have to look elsewhere."<sup>193</sup> Clark and Chen state

the moves [new legislation] are reshaping the Bitcoin mining industry and driving up costs. Bitmain, which runs China's two largest Bitcoin-mining collectives, is setting up regional headquarters in Singapore and now has mining operations in the U.S. and Canada. BTC.Top, the No. 3 mining pool, is also opening a facility in Canada. Bitcoin exchanges and wallet services in the country are also leaving, setting up over-the-counter shops in Hong Kong or looking at operating out of Singapore or South Korea.<sup>194</sup>

In addition, China also appears to have influenced the value of bitcoin worldwide. Andrew Marshall writes that China has had an invariably important relationship with Bitcoin, and he argues that "no other country's government has had such a consistent and powerful

---

<sup>193</sup> Clark and Chen, "How China's Stifling Bitcoin and Cryptocurrencies."

<sup>194</sup> Clark and Chen.

effect on Bitcoin price.”<sup>195</sup> He observes that China’s first impact on the cryptocurrency market occurred after the PBoC forbid Chinese financial institutions from using Bitcoin in late 2013, an occurrence that directly impacted the largest bitcoin exchange in the world, *BTC China*, and caused the price of Bitcoin to plummet to less than 50 percent over a period of two weeks.<sup>196</sup> Marshall reports that a similar occurrence in January 2017 when the PBoC bank executed on-site inspections on Chinese exchanges “to look into capital flight, money laundering and market manipulation” that resulted in a 10 percent decline in value.<sup>197</sup>

A similar occurrence appeared after China banned ICOs and shut down exchanges in September of 2017, appearing to cause a reactionary market decline of bitcoin’s value from 5000 USD to 3000.<sup>198</sup> The speculative market that drives the price of cryptocurrencies is volatile and is susceptible to rumors and regulations worldwide. Although the cryptocurrency market initially declined in the wake of the new Chinese regulation, the market quickly rebounded, skyrocketing back to 7000 USD in a few weeks’ time.<sup>199</sup>

There may be correlation between Chinese regulations and the price of bitcoin; however, gauging the Chinese impact on the international cryptocurrency ecosystem is not a simple matter; an entire thesis could be dedicated to quantitatively analyzing the cause and effect relationship. The research presented by this this, however, did not encounter any scholarly sources analyzing the effect that China’s prohibitive laws have had on its people, or how successful the enforcement of those policies have been. What is certain is that decentralized virtual currencies will continue to function despite the Chinese governmental animosity toward cryptocurrencies. As Vigna and Casey assert,

The Chinese government might bar its banks from handling bitcoin-related transaction services or declare that only the yuan be used within the nation’s

---

<sup>195</sup> Andrew Marshall, “How China Influences Bitcoin Price, Explained,” *Cointelegraph*, February 15, 2017, <https://cointelegraph.com/explained/how-china-influences-bitcoin-price-explained>.

<sup>196</sup> Marshall.

<sup>197</sup> Marshall.

<sup>198</sup> Panos Mourdoukoutas, “Bitcoin Prices Still Firmly above \$7,000, without China,” *Forbes*, November 4, 2017, <https://www.forbes.com/sites/panosmourdoukoutas/2017/11/04/bitcoin-prices-still-firmly-above-7000-without-china/>.

<sup>199</sup> Mourdoukoutas.

borders, but it can't shut down bitcoin, which resides nowhere and everywhere. The same challenge faces any government.<sup>200</sup>

In the future, China may choose to prohibit individual ownership of cryptocurrencies, but as of now, it seems intent on denying its citizens access to the cryptocurrency ecosystem.

## **2. Other States' Effect in Banning Cryptocurrencies**

Outside of China, sovereign states that have banned cryptocurrencies appear to have had mixed domestic result in their efforts to prevent their citizens from obtaining Bitcoin and other cryptocurrencies. Again, one such case is in Nigeria where cryptocurrencies like Bitcoin have been deemed illegal. Even so, the Nigerian government and central bank both acknowledge that they are nearly powerless to enforce cryptocurrency laws, admitting in a governmental conference in 2018 that the "Central bank cannot control or regulate bitcoin. Central bank cannot control or regulate blockchain. Just the same way no one is going to control or regulate the Internet. We don't own it."<sup>201</sup> In the case of Nigeria, the state can tell its citizens that cryptocurrencies are illegal, but given the combination of an economic opportunity investing in bitcoin and the lack of sufficient state power to find and punish violators, it is unlikely that the country will be able to eliminate cryptocurrency users under its sovereignty.

A similar case to Nigeria can be found in Ecuador, where Bitcoin has been illegal for four years to date. Alexandra Veloz writes in mid-2017 "even if the law only allows the flow of electronic backed money backed by the Central Bank, people are using and buying bitcoin increasingly often."<sup>202</sup> Likewise in Venezuela, where the country has arrested Bitcoin miners in the past, the citizens continue to risk prosecution by mining and transacting bitcoins to survive in the hyperinflated economy.<sup>203</sup>

---

<sup>200</sup> Vigna and Casey, *The Age of Cryptocurrency*, 66.

<sup>201</sup> Kevin Helms, "Central Bank of Nigeria Says 'We Can't Stop Bitcoin,'" *Bitcoin News* (blog), March 5, 2017, <https://news.bitcoin.com/central-bank-of-nigeria-says-we-cant-stop-bitcoin/>.

<sup>202</sup> Alexandra Veloz, "Ban Fails to Halt Bitcoin in Ecuador," *Antigua Report* (blog), May 24, 2017, <http://antiguareport.com/2017/05/ban-fails-to-halt-bitcoin-in-ecuador/>.

<sup>203</sup> Rene Chun, "Big in Venezuela: Bitcoin Mining," *The Atlantic*, September 2017, <https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/>.

A more striking development is a surge in demand for bitcoin in countries that have clamped down on the legality of cryptocurrencies. For example, one local Nigerian exchange in late December 2017 valued of bitcoin 15 percent higher than exchanges outside of the country, in the face of then-new governmental warnings on cryptocurrency.<sup>204</sup>

### **3. Banning Cryptocurrency Internationally**

A sovereign state that chooses to ban cryptocurrency may find the enforcement of anti-cryptocurrency policies difficult, especially when cryptocurrency is accepted internationally. There is not internationally recognized regulatory standard for the regulation and prosecution of cryptocurrencies. While countries like Bangladesh, China, Ecuador, and Nigeria may choose to outlaw cryptocurrencies, the vast majority of other nations have yet to adopt such a critical stance on cryptocurrencies, thereby fueling the cryptocurrency ecosystem to thrive internationally in the face of nations seeking prohibit its use. Matthew Ponsford, comments, “inconsistencies in regulation have posed many challenges for jurisdictions currently attempting to mitigate regulatory deficiencies,” highlighting the difficulties of international cooperation to obtain records and prosecute violators internationally.<sup>205</sup> A sovereign state prohibiting cryptocurrencies may be surrounded geographically by countries accepting of them or be interdependent economically with sovereign entities embracing virtual currencies. As a consequence, individual admission to the cryptocurrency ecosystem only requires Internet access and a willingness to participate, regardless of the state laws to which citizens are subordinate.

## **E. CONCLUSION**

Banning cryptocurrencies may be a tool for sovereign states that want to contain or restrict its citizens from using cryptocurrency, but there is still no clear defined verdict on how effective the measures are internal to the state. Of the countries identified in this chapter, the gradual implementation of anti-cryptocurrency laws in China appears to have the greatest

---

<sup>204</sup> Aline Oyamada and Camila Russo, “Bitcoin Trading Thrives Wherever Regulators Crack Down Most,” Bloomberg News, December 14, 2017, <https://www.bloomberg.com/news/articles/2017-12-14/bitcoin-trading-thrives-wherever-regulators-crack-down-most>.

<sup>205</sup> Ponsford, “A Comparative Analysis of Bitcoin.”

affect international market for cryptocurrencies, but only because the Chinese labor and power costs have been conducive to a growing cryptocurrency ecosystem.

A sovereign state may attempt to ban aspects of cryptocurrencies to regain its controls on the monetary supply, but there will always be individuals and organizations that will find illegal methods to move money away from the prying eye of the state. If anything, the research has shown that a sovereign state wherein cryptocurrencies are considered illegal may not have the capacity to prevent or prosecute individuals within its jurisdiction. This conclusion is justified by the thriving cryptocurrency ecosystem in sovereign states where cryptocurrencies are considered illegal and highlights to the inability of the state to enforce laws against domestic cryptocurrency users.<sup>206</sup> If a sovereign state was to become truly successful at regulating or prohibiting cryptocurrency, the state would need to completely control or deny its citizens access to the Internet.

Another conclusion is that it may not be feasible for solitary, less developed nation to ban cryptocurrencies while other nations regulate or adopt them. Weaker, less developed states may find themselves unable to enforce their anti-cryptocurrency policies and lacking the technology or capability to find and prosecute individuals or organizations violating their anti-virtual currency laws. Likewise, BIS offers the suggestion that any unitary attempt by individual states to ban cryptocurrencies may be less than effective, observing that “given the nature of digital currencies, which are typically online and therefore not limited to national jurisdictions, a coordinated approach at a global level may be important for regulation to be fully effective.”<sup>207</sup> However, banning cryptocurrency is just one answer to how sovereign states can deal with the challenges posed by decentralized virtual currencies. In the next chapter, this thesis illuminates how states can regulate the cryptocurrency ecosystem to minimize its impact to the sovereign functions of the state.

---

<sup>206</sup> Oyamada and Russo, “Bitcoin Trading Thrives.”

<sup>207</sup> Committee on Payments and Market Infrastructures, *Digital Currencies*, 12.



## **IV. THE REGULATION OF CRYPTOCURRENCY**

Chapter III explored the methods of sovereign states in banning cryptocurrencies. This chapter approaches the regulation of cryptocurrency in a similar approach to Chapter III; however, state-backed regulation of cryptocurrency differs in rationale and implementation from the states that choose to ban virtual currencies. For purposes of this chapter, cryptocurrency regulations are the potential methods by which a state allows its citizens to legally obtain, transact, and develop cryptocurrencies without the state actually recognizing, adopting, or banning aspects of virtual currencies. At the time of writing, no clear virtual currency regulation exists on a supranational level. Even states with strong economic and political ties have shown little similarity in the methods by which they choose to target the emerging cryptocurrency ecosystem.

As discussed in Chapter II, cryptocurrency's peer-to-peer nature transcends physical state borders, transacting across a range of sovereign entities, each with its own take on the how to regulate cryptocurrencies. Because the question of cryptocurrency and state sovereignty surpasses individual states, there are a number of regulatory responses drawn on an international, multistate level. To explore state-backed regulation in cryptocurrency, this chapter is divided into five sections. First, this chapter presents the rationale as to why a state would choose to regulate cryptocurrencies over banning or over adopting its own state-backed cryptocurrency. The second section explains the difficulties of regulating cryptocurrency within a sovereign state. The third section outlines a range of broad methods that sovereign states could use to approach the question of regulation and cryptocurrency. The fourth section presents the regulatory action taken by the United States as a case study because of the sophisticated and intricate regulatory response taken. The fourth section also discusses the regulatory action taken on a supranational level by the European Union (EU), and the guidance provided from the international institutions of the IMF and BIS. The fifth and final section of this chapter offers concluding thoughts on sovereign states' regulation of cryptocurrency.

## **A. THE RATIONAL TO REGULATE VIRTUAL CURRENCIES**

The rationale to regulate cryptocurrencies is not unlike the reasons listed for banning cryptocurrency presented in Chapter III. However, by allowing cryptocurrencies to function legally within the sovereignty of the state, the governing body also assumes the risks associate with cryptocurrency, which may challenge the state’s economic, political, and law enforcement capabilities.<sup>208</sup> This section discusses the three reasons why a state would choose to regulate cryptocurrencies: consumer protection, the prevention of money laundering, and fiscal policy protection.

### **1. Consumer Protection**

Sovereign states often quote *consumer protection* as a fundamental reason to regulate cryptocurrencies due to the risks inherent in the unregulated cryptocurrency market. As the BIS states, “central banks typically have a responsibility to promote safe and efficient payment systems.”<sup>209</sup> For instance, investors could face the potential for loss due to the volatility of value in cryptocurrency markets. The BIS also points out that due to the relative anonymity in cryptocurrency transactions, there is a large risk of fraud in digital currency markets.

### **2. Money Laundering**

The pseudoanonymity inherent in cryptocurrency has generated a number of difficulties for law enforcement agencies. As stated by the 2015 BIS report, the “relative anonymity of digital currencies may make them especially susceptible to money laundering and other criminal activities.”<sup>210</sup> Cryptocurrencies can easily be transferred from fiat to cryptocurrency, transferred through a number of virtual wallets, and then exchanged back into fiat currency via an exchange or via a transfer of cryptocurrency to another user’s

---

<sup>208</sup> The reasons why sovereign states may choose to ban cryptocurrency presented in Chapter III are: to reduce crime, to regain the capital controls of the state, to limit or restrict the citizens civil rights, to develop and introduce a state-sanctioned cryptocurrency, and to eliminate cryptocurrency mining as a major drain on the energy grid.

<sup>209</sup> Committee on Payments and Market Infrastructures, *Digital Currencies*, 14.

<sup>210</sup> Committee on Payments and Market Infrastructures, 15.

virtual wallet in exchange for cash. While trackable through the blockchain, this process complicates the legal requirements that permit law enforcement to track and prosecute money launderers. A sovereign state could attempt to regulate cryptocurrency exchanges or require its citizens to register cryptocurrency accounts to increase the visibility of transactions.

### **3. To Protect Monetary Policy**

In the theoretical event that that a non-sovereign cryptocurrency becomes widely accepted and used without adequate state-controlled regulations in place, the citizens could bypass the sovereign state and central bank completely. If such an event was to occur, the result could be a weakening of the sovereign government and central bank to issue and control interest rates and the weakening of monetary policy. The CPMI report explains, “a widespread substitution of banknotes with digital currencies could lead to a decline in central bank non-interest paying liabilities. . . . The result could be a reduction in central bank earnings that constitute central bank seigniorage revenue.”<sup>211</sup> Likewise, if cryptocurrency becomes widespread, citizens would no longer require the use of banks in favor of the peer-to-peer nature of the blockchain. The result would be a change in the central bank’s monetary policy.

## **B. DIFFICULTIES OF REGULATING CRYPTOCURRENCIES**

States face an inherent challenge in regulating cryptocurrencies—finding an appropriate level of regulation that minimally infringes on the citizens’ rights to own or use cryptocurrency but also retaining a level of control over cryptocurrencies meeting sovereign state needs. The needs of individual states vary and are dependent upon the political, economic, and law enforcement requirements. Because cryptocurrencies themselves do not pose an inherent threat to the state or its citizens, some law scholars argue that it is beyond the control of the state to prohibit ownership or transactions with virtual currencies. For example, Bryans writes:

---

<sup>211</sup> Committee on Payments and Market Infrastructures.

In an increasingly digital world, it makes perfect economic and societal sense to allow digital currencies, government-backed or otherwise. . . . Regulation of such currencies should occur at the point where law enforcement can most effectively punish civil and criminal violations with the least overhead.<sup>212</sup>

More importantly, cryptocurrencies are difficult to define, and therefore, they are difficult to regulate. The IMF asserts that cryptocurrencies “combine properties of currencies, commodities, and payment systems, and their classification as one or the other will often have implications for their legal and regulatory treatment.”<sup>213</sup> Additionally, Bohme et al. affirm, “it is infeasible to regulate all peers in the Bitcoin network due to their quantity, their geographic distribution, and the privacy protections in the network. Instead, regulators are naturally drawn to key intermediaries.”<sup>214</sup> The lack of an established definition or regulation to group cryptocurrencies under, coupled with the transnational reach of virtual currencies and the difficulty of monitoring transactions, has shaped a multitude of sovereign responses internationally, diverse in methods that are used to restrain cryptocurrencies. As a consequence, the regulatory approaches level of intrusiveness vary by regulation on cryptocurrencies on a case-by-case basis and are explored later in the chapter.

### **C. METHODS OF REGULATING CRYPTOCURRENCY**

The 2015 CPMI report for the BIS also lists four broad classifications detailing how a sovereign state can regulate—without banning—virtual currencies. This section is divided upon the four broad classifications listed and complements the information provided by the BIS with other scholarly sources to provide an analysis of the regulatory actions available to sovereign states. The four broad categories of regulation are: informational/moral suasion, the regulation of specific entities, interpretation of existing regulations, and the creation broader regulations to target cryptocurrencies.

---

<sup>212</sup> Bryans, “Bitcoin.”

<sup>213</sup> He et al., *Virtual Currencies and beyond*, 24.

<sup>214</sup> Bohme et al., “Bitcoin,” 231.

## **1. Informational and Moral Suasion**

The moral suasion regulatory option presented by the BIS proposes highlighting the risks and dangers of investing, transacting with, and mining cryptocurrency to the general public, indirectly weakening the appeal of cryptocurrencies to the public.<sup>215</sup> Examples of the informational approach include public warnings, promoting general information on investing and buying cryptocurrencies, and providing research papers to the public.<sup>216</sup>

As outlined in Chapter II, Bitcoin and other currencies obtain their value through a system of supply and demand, and by many individuals and businesses view them as an investment rather than a currency. As a result, the value of cryptocurrency is *reactionary* to potential news that might affect its wealth. A sovereign state could use cryptocurrency's reactionary value to pass new cryptocurrency restrictions, or simply suggest implementing new cryptocurrency regulations, to indirectly discourage citizens' use of cryptocurrencies by reducing its investment potential.

## **2. The Regulation of Specific Stakeholders**

A governing body could also create regulations on specific stakeholders, such as targeting the privately owned financial institutions functioning as key parts of a cryptocurrency network.<sup>217</sup> For example, a cryptocurrency exchange is considered a financial based institution, and an example of a regulation in this category would be the creation of minimum consumer protection requirements to which the exchange or other institution would be subject. Another example would be the requirement of locally owned exchanges to keep and provide records to regulatory bodies when necessary.

## **3. Interpretation of Existing Regulations**

Another method by which a government could regulate cryptocurrencies would be to interpret the existing laws of the state so that cryptocurrencies would fall under the

---

<sup>215</sup> Committee on Payments and Market Infrastructures, *Digital Currencies*, 12.

<sup>216</sup> Committee on Payments and Market Infrastructures, 13.

<sup>217</sup> Committee on Payments and Market Infrastructures, 12.

existing legislative framework.<sup>218</sup> For instance, in the United States, federal entities have taken advantage of the lack of a clear definition of what a virtual currency is (e.g., security, currency, property), allowing a range of cooperating government organizations to enforce standards upon cryptocurrency users under the prior-existing laws.

#### **4. The Creation of Broader Regulation**

Sovereign governments may enact new, broader legislation that combines or covers the larger aspects of cryptocurrency listed like consumer protection, organizational rules for stakeholders, and specific operating rules.<sup>219</sup> For instance, the CPMI suggests that state authorities could create broad AML and counter-terrorist financing (CTF) regulations that would cover all cryptocurrency transactions, as well as payment methods, and cryptocurrency exchanges under a single regulatory law.<sup>220</sup>

### **D. SELECTIVE SUMMARY OF CURRENT CRYPTOCURRENCY REGULATION**

This section focuses almost exclusively on the regulation that the United States has enacted on cryptocurrency to serve as an example of a state that has regulated cryptocurrency. This thesis focuses on the United States because arguably the United States has some of the most complex and complicated virtual currency regulation, with regulatory bodies releasing new regulations and virtual currency guidance nearly every month. This section also briefly discusses the regulatory actions and lack of action taken by the EU and on an international level.

#### **1. The United States**

The United States arguably has one of the most complicated and robust standards on virtual currencies. Because cryptocurrencies are neither easily defined, nor easily categorized under existing laws, multiple regulatory bodies within the United States have released their own guidance for the conduct of cryptocurrency transactions, investments,

---

<sup>218</sup> Committee on Payments and Market Infrastructures, 13.

<sup>219</sup> Committee on Payments and Market Infrastructures, 13.

<sup>220</sup> Committee on Payments and Market Infrastructures, 12.

and ownership for U.S. citizens. As stated by a 2018 Commodity Futures Trading Commission (CFTC) report, “US law does not provide for direct, comprehensive federal oversight of underlying Bitcoin or virtual currency spot markets. As a result, U.S. regulation of virtual currencies has evolved into a multifaceted, multi-regulatory approach.”<sup>221</sup> Under U.S. law, virtual currencies are considered to be as either property, commodity, or security, dependent upon which U.S. regulatory body is charged with the regulation.

**a. Law Enforcement Agencies**

The FBI is responsible for shutting down the Silk Road, an illicit Dark Web marketplace that used bitcoin as the only accepted method of payment.<sup>222</sup> After two years of searching, on October 1, 2013, the FBI was finally able to pinpoint and arrest the founder and operator of the Silk Road, Ross Ulbricht, on the charges of “narcotics trafficking and money laundering conspiracies through creating and operating Silk Road. The FBI seized all the bitcoins stored on the website,” allowing federal marshals to later sell 29,655 bitcoins at auction.<sup>223</sup> The arrest of Ulbricht and downfall of the Silk Road was the first large-scale criminal investigation of criminal acts involving cryptocurrencies. As a result, the 2013 case of the Silk Road has become widely associated with illicit cryptocurrency use and has focused the attention of lawmakers and scholars towards studying the legality of bitcoin.

**b. Internal Revenue Service**

In March 2014, the Internal Revenue Service (IRS) released tax guidance for virtual currencies like Bitcoin and defined virtual currency as property under U.S. federal law.<sup>224</sup>

---

<sup>221</sup> U.S. Commodity Futures Trading Commission, *CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets* (Washington DC: U.S. Commodity Futures Trading Commission, 2018), [https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder\\_virtualcurrency01.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf), 1.

<sup>222</sup> Huang, “Reaching within Silk Road,” 2105.

<sup>223</sup> Huang, 2105.

<sup>224</sup> Internal Revenue Service, *IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply* (Washington DC: Internal Revenue Service, 2014), <https://www.irs.gov/newsroom/irs-virtual-currency-guidance>.

Under the IRS guidance, individuals who transact, pay, or trade cryptocurrency are responsible for reporting capital gains made during transactions or trades with cryptocurrencies. Likewise, payments for services with virtual currencies are liable to the same U.S. tax law as payments made with property.

*c. Commodity Futures Trading Commission*

The CFTC is an independent regulatory organization of the United States responsible for monitoring and regulating the wide assortment commodity markets “to foster open, transparent, competitive, and financially sound markets.”<sup>225</sup> The CFTC “declared virtual currencies to be a ‘commodity’<sup>226</sup> subject to oversight under its authority under the Commodity Exchange Act (CEA)” in 2014.<sup>227</sup> Since then, the CFTC has held a significant role in shaping public awareness and the current U.S. regulations in the cryptocurrency ecosystem.

The CFTC divides its approach on the regulation of virtual currencies into five categories: *consumer education* to provide greater public information on virtual currencies; *asserting legal authority* to provide anti-fraud and manipulation regulations on virtual currency derivatives; obtaining *market intelligence* to gather information and data on virtual currency derivative; *robust enforcement* “to enforce the law and prosecute fraud, abuse, manipulation or false solicitation in markets for virtual currency derivatives and underlying spot trading;” and *government-wide coordination* of virtual currencies with other federal regulators.<sup>228</sup>

Under the authority bestowed by the CEA, the CFTC has taken a number of enforcement actions on cryptocurrencies, including acting against unregulated exchanges

---

<sup>225</sup> “Mission & Responsibilities,” U.S. Commodity Futures Trading Commission, accessed April 22, 2018, <https://www.cftc.gov/About/MissionResponsibilities/index.htm>.

<sup>226</sup> The “CFTC Glossary” defines commodity as “(2) A physical commodity such as an agricultural product or a natural resource as opposed to a financial instrument such as a currency or interest rate.” “CFTC Glossary,” U.S. Commodity Futures Trading Commission, accessed April 22, 2018, <https://www.cftc.gov/ConsumerProtection/EducationCenter/CFTCGlossary/index.htm>.

<sup>227</sup> U.S. Commodity Futures Trading Commission, *CFTC Backgrounder*, 1.

<sup>228</sup> U.S. Commodity Futures Trading Commission, 1–2.



domestically and abroad, enforcing laws prohibiting illegal trading on derivative platforms, and issuing guidance on regulatory matters involving virtual currencies.<sup>229</sup> The CFTC has also created a virtual currency self-certification process to enforce the regulations put forth by the CFTC, while allowing U.S. exchanges access to Bitcoin future contracts.<sup>230</sup> The self-certification process has since allowed two large market exchanges—the Chicago Mercantile Exchange Inc. and the Chicago Board of Options Exchange—to offer bitcoin future contracts as of December 1, 2017.<sup>231</sup>

*d. Security and Exchange Commission*

One of the more recent U.S. agencies to offer guidance on cryptocurrency is the Security and Exchange Commission (SEC), whose mission statement “is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation” in the buying and selling of stocks.<sup>232</sup> In a move to promote investor awareness and protection in the cryptocurrency market, the SEC has recently released public guidance on the conduct of cryptocurrency initial coin offerings (ICO). Similar to the concept of IPOs, developers use ICOs to raise capital in the form of U.S. dollars or other cryptocurrency in return for the pre-public release of the developer’s token or cryptocurrency at an established price.<sup>233</sup> The company promoting the ICO benefits by raising capital prior to the official release, and the customers can often buy the proposed cryptocurrency at a value less than expected, offering the potential of a quick profit to investors.

---

<sup>229</sup> U.S. Commodity Futures Trading Commission, 1.

<sup>230</sup> According to the “CFTC Glossary,” the definition of futures contract is “An agreement to purchase or sell a commodity for delivery in the future: (1) at a price that is determined at initiation of the contract; (2) that obligates each party to the contract to fulfill the contract at the specified price; (3) that is used to assume or shift price risk; and (4) that may be satisfied by delivery or offset.” “CFTC Glossary,” U.S. Commodity Futures Trading Commission.

<sup>231</sup> U.S. Commodity Futures Trading Commission, *CFTC Backgrounder*, 2.

<sup>232</sup> “SEC What We Do,” U.S. Security and Exchange Commission, June 10, 2013, <https://www.sec.gov/Article/whatwedo.html>.

<sup>233</sup> Jay Clayton, “Statement on Cryptocurrencies and Initial Coin Offerings,” U.S. Security and Exchange Commission, December 11, 2017, <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>.

Although the SEC has released strenuous guidance for ICOs, the organization has yet to clarify if cryptocurrencies are considered securities, which leaves ambiguity for future possible SEC intervention into the cryptocurrency market.<sup>234</sup> For example, after weighing the pros and cons of cryptocurrency use in the official 2017 public statement on cryptocurrencies and ICOs, SEC Chair Jay Clayton writes:

It has been asserted that cryptocurrencies are not securities and that the offer and sale of cryptocurrencies are beyond the SEC's jurisdiction. Whether that assertion proves correct with respect to any digital asset that is labeled as a cryptocurrency will depend on the characteristics and use of that particular asset.<sup>235</sup>

Since the 2017 public release, the SEC has provided further guidance outlining investor considerations for cryptocurrency trading. The most recent (March 7, 2018) public release by the SEC, a report, has since turned to cryptocurrency exchanges, highlighting that there are a number of cryptocurrency exchanges that do not adhere to the SEC standards. Thus, the unregistered exchanges do not receive the SEC established investor protections.<sup>236</sup> Moreover, the SEC declares, “a number of these platforms provide a mechanism for trading assets that meet the definition of a ‘security’ under the federal securities laws.”<sup>237</sup> Finally, this report announces that cryptocurrency exchanges may be required—depending on the circumstances—to register with the SEC and adhere to federally established minimums set by the SEC for securities and exchanges.

*e. Office of Foreign Assets Control*

The U.S. Treasury's Office has also released new requirements through the Office of Foreign Assets Control (OFAC), mandating U.S. cryptocurrency exchanges and

---

<sup>234</sup>According to Investopedia, security is defined as “A security is a fungible, negotiable financial instrument that holds some type of monetary value. It represents an ownership position in a publicly-traded corporation (via stock), a creditor relationship with a governmental body or a corporation (represented by owning that entity's bond), or rights to ownership as represented by an option.” “Definition of a Security,” Investopedia, November 26, 2003, <https://www.investopedia.com/terms/s/security.asp>.

<sup>235</sup> Clayton, “Statement on Cryptocurrencies.”

<sup>236</sup> “Statement on Potentially Unlawful Online Platforms for Trading Digital Assets,” U.S. Securities and Exchange Commission, March 7, 2018, <https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading>.

<sup>237</sup> “Statement on Potentially Unlawful Online Platforms for Trading Digital Assets.”

investors to blacklist specific cryptocurrency addresses that the OFAC deems as a threat to the United States.<sup>238</sup> The list, referred to by OFAC as the specially designated nationals, targets individuals, groups, and companies that do not necessarily need to be a part of a sovereign state.

*f. Financial Crimes Enforcement Network*

The Financial Crimes Enforcement Network (FinCEN) operates as the U.S. Treasury's law enforcement arm, and it is responsible for directing regulation and enforcement of virtual currencies. According to the FinCEN official website, "FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."<sup>239</sup> FinCEN considers virtual currency to be "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of a real currency. In particular, virtual currency does not have legal tender status in any jurisdiction."<sup>240</sup> However, FinCEN's interest in virtual currencies stems from users' ability to exchange U.S. fiat dollars for cryptocurrency and vice versa readily and quickly.

Virtual currencies are subject to the laws contained in the Bank Secrecy Act (BSA), an act FinCEN explains as the "[United States] first and most comprehensive Federal anti-money laundering and counter-terrorism financing statute."<sup>241</sup> The 2013 guidance, which officially applies the FinCEN regulations to virtual currencies, expands upon the laws contained in the BSA to delineate the key participants subject to FinCEN regulations. As such, the various participants of virtual currencies are arranged into three categories

---

<sup>238</sup> Olly Jackson, "Ofac's Crypto Blacklist Could Drive Investors to Riskier Exchanges," *International Financial Law Review*, April 6, 2018, <http://www.iflr.com/Article/3799007/%5bOPEN-ACCESS%5d-Ofacs-crypto-blacklist-could-drive-investors-to-riskier-exchanges.html>.

<sup>239</sup> "What We Do," United States Department of the Treasury Financial Crimes Enforcement Network, accessed April 22, 2018, <https://www.fincen.gov/what-we-do>.

<sup>240</sup> Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Washington, DC: Department of the Treasury, 2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, 1.

<sup>241</sup> Financial Crimes Enforcement Network, *Application of FinCEN's Regulations*.

FinCEN defines as *users*, *administrators*, and *exchangers* of virtual currency (defined in the footnotes).<sup>242</sup> Moreover, the enforcement of FinCEN regulations only apply to virtual currency administrators and exchangers since they are considered money transmitters.<sup>243</sup> As of now, the FinCEN regulations are only applicable to the administrators and exchangers of virtual currencies because they are classified as money service businesses, and therefore, they are subject to the registration, reporting, and recordkeeping stipulated under the BSA.

## 2. Regulation in the European Union

As of the time of writing, virtual currencies are completely legal under the supranational guidance of the EU, allowing the EU member nations to regulate cryptocurrency as they see fit. Compared to the United States, the EU's Central Bank (ECB) has taken a laissez-faire approach to virtual currencies, officially stating, "it is not in the ECB's responsibility to ban or regulate bitcoin or other cryptocurrencies."<sup>244</sup> The ECB has instead elected to provide the public with an informational approach highlighting the risks of investing and using cryptocurrencies. Furthermore, the ECB also argues Bitcoin and other virtual currencies are not actually considered currency, citing the following four reasons as justification: first, Bitcoin lacks a central authority. Second, Bitcoin has a limited following of customers and merchants. Third, cryptocurrency transactions lack any legal protection by the EU. Finally, the volatility of cryptocurrency is too unstable to be predicted or used as a form of reliable payment.

---

<sup>242</sup> FinCEN defines *user* as "a person that obtains virtual currency to purchase goods or services," and it further states, "obtaining" as an all-encompassing phrase that contains any or all of the following words to describe virtual currency use: the "earning," "harvesting," "mining," "creating," "auto-generating," "manufacturing," or "purchasing" of virtual currencies. Also according to FinCEN, an *exchanger* is "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." Finally, according to FinCEN, an *administrator* is associated with any persons "engaged as a business in issuing (putting into circulation) virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency." Financial Crimes Enforcement Network, *Application of FinCEN's Regulations*, 2–3.

<sup>243</sup> Financial Crimes Enforcement Network, *Application of FinCEN's Regulations*, 2.

<sup>244</sup> "What Is Bitcoin?," European Central Bank, February 13, 2018, <https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.en.html>.

Likewise, in November 2017, the EU has also released public guidance from the European Security and Markets Authority (ESMA) providing EU citizens with the risks associated with ICOs.<sup>245</sup> The ESMA has since expanded the precautions to citizens of virtual currencies, releasing another round of public awareness to pan-EU consumers on the risks associated with buying and trading virtual currencies.<sup>246</sup>

### **3. International Regulation**

The current focus by many of the international standard setting institutions like the IMF and the BIS appears to be a research and wait-and-see response. In this thesis, most of the cited potential issues that cryptocurrency poses to the sovereign state are drawn from the research reports released by the IMF and BIS. For example, writing for the IMF, Dong He et al. note, “the Financial Action Task Force (FATF)—the AML/CFT standard-setter—and the United Nations Office on Drugs and Crime (UNODC) have focused on the prevention and law enforcement response to the money laundering risks posed by VCs” on an international level.”<sup>247</sup> Even if new standards were created, the reach of international regulators only extend as far as the countries that choose to adhere to the proposed standards. Outside the creation of law enforcement standards for money laundering and terror financing, there is little coordination against cryptocurrency on a multinational level.

## **E. CONCLUSION**

Sovereign state regulatory agencies walk a tightrope between restricting and adopting cryptocurrency. He et al. explain, “[t]he challenge for policymakers has often turned on finding a balance between addressing the risks and vulnerabilities posed by VCs while not stifling innovation.”<sup>248</sup> Moreover, one could make the case that restricting or

---

<sup>245</sup> “ESMA Highlights ICO Risks for Investors and Firms,” European Securities and Markets Authority, November 13, 2017, <https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms>.

<sup>246</sup> “ESAs Warn Consumers of Risks in Buying Virtual Currencies,” European Securities and Markets Authority, February 12, 2018, <https://www.esma.europa.eu/press-news/esma-news/esas-warn-consumers-risks-in-buying-virtual-currencies>.

<sup>247</sup> He et al., *Virtual Currencies and Beyond*, 26.

<sup>248</sup> He et al.

prohibiting cryptocurrency in liberal democracies, which are founded on the ideals of individual liberties, is an impracticality. Therefore, states will need to implement restrictions on virtual currencies through the interpretation of existing laws, like in the United States, or choose to create new, all-inclusive regulation mitigating the negative attributes of cryptocurrency use.

Cryptocurrencies are an unprecedented step toward a new method of transaction used both legally and illegally; therefore, sovereign governments will inevitably need to pursue new regulations on virtual currencies to minimize illicit activities. Governing bodies, regardless of their policy toward virtual currencies, need to address money laundering, fiscal policy, and consumer protection. The route of regulation on cryptocurrency will depend on a number of social, political, and economic factors. Whether virtual currency regulations be a hands-on, multifaceted approach as seen in the United States, less obtrusive moral suasion approach by the EU, or a new creation of broader regulation, a state's likely approach to cryptocurrency regulation is reflective of how much the state views cryptocurrency as a threat. This chapter has focused on the reasons why a sovereign state would seek to regulate cryptocurrency and outlined a number of possible regulatory actions available to the state. The next chapter expands upon the adoption of cryptocurrency by the sovereign state and explores how cryptocurrencies can officially acclimate as a part of the state.

## **V. THE ADOPTION OF CRYPTOCURRENCIES BY SOVEREIGN STATES**

Chapter IV explored the rationale, methods, and real-world cases of regulating cryptocurrency by sovereign states. This chapter directs its focus toward the adoption of cryptocurrency within sovereign states. There are two distinct categories of state-sponsored cryptocurrency. The first is the sovereign states that recognize prior-existing stateless cryptocurrencies (e.g., Bitcoin) as a form of legal tender, and second is the cryptocurrencies specifically developed by a sovereign state that supplants or supplements the existing sovereign currency. This chapter begins with a brief discussion of the benefits a sovereign cryptocurrency could provide to a state. The second section expands on the development and implementation of state-sponsored cryptocurrency by analyzing the sovereign states that plan to adopt or issue a state-backed cryptocurrency. The third section details a selection of political and social obstacles of incorporating a sovereign-state cryptocurrency.

### **A. REASONS FOR STATES TO USE CRYPTOCURRENCY**

Whether a state adopts a preexisting stateless cryptocurrency or decides to create a new state-backed virtual currency, there are a number of reasons why a sovereign state might choose to incorporate a blockchain-based virtual currency into its financial system. This section highlights the potential benefits for sovereign states should they choose to adopt or create their own cryptocurrency with four examples: the inclusion of the unbanked costs, cheaper transaction costs, cryptocurrency's ability to bypass sanctions, and cryptocurrency's feature, which permits the state access to the full transaction history.

#### **1. To Incorporate the Unbanked**

A state cryptocurrency, adopted (Bitcoin) or created by a central bank, could be used by less-developed countries to include the citizens who are not connected with banking institutions, decreasing the poverty stricken individuals in a country while driving economic growth. These people remain isolated from bank access due to a number of reasons: lack of access to standing banking infrastructure, some countries have a weak

institutional identification process that creates risk for banks to invest in people, and then there are the lack of profits when investing in the poor vice richer people elsewhere in the world.<sup>249</sup> Vigna and Casey write that there are “roughly 2.5 billion adults in the world . . . that are cut off from a financial system that the rest of us take for granted.”<sup>250</sup> They describe the excluded people—those without access to banking services such as saving accounts, checking accounts, and credit cards—as the *unbanked*. The unbanked are unable to store and secure money in banks, make purchases on the Internet, or effectively transact outside of their local area, and therefore, are a huge untapped market for services and goods.

On the other hand, cryptocurrencies only require the Internet to move money, and does not require identification for access. If a less-developed or developing state decided to adopt and accept cryptocurrency as a form of money, theoretically, the unbanked citizens would be granted access to every other cryptocurrency user. As Vigna and Casey highlight, “financially integrating a third of humanity could create vast new opportunities for world trade and for attacking poverty.”<sup>251</sup> By including the lower socioeconomic classes that have been historically barred from participating in the global financial order, the state can simultaneously uplift the poorest parts of its population, connect those individuals with the state and global economy, and develop the resident human capital as greater economic participants within the state. Ultimately, by implementing a state sanctioned cryptocurrency system easily accessible to all individuals regardless of income, the people can benefit from what this thesis discusses next, cheaper transaction costs.

## **2. Cheaper Transaction Costs**

Additionally, a state-adopted or developed cryptocurrency could substantially reduce the cost to move money transnationally over other money wire services Western Union. According to Vigna and Casey, when using traditional fiat currencies there can be up to seven paid intermediaries in a traditional credit card transaction between a customer

---

<sup>249</sup> Vigna and Casey, *The Age of Cryptocurrency*, 190.

<sup>250</sup> Vigna and Casey, 186.

<sup>251</sup> Vigna and Casey, 191.



and a merchant, agents who are responsible for either recording the identities of the users or verifying that the appropriate funds are transferred from payee to merchant.<sup>252</sup> A bank or credit card company charges merchants small fees for the intermediary service; however, as Vigna and Casey illuminate, transactions across sovereign currencies (e.g., from U.S. dollar to euros or pesos) incur additional exchange fees, adding up to roughly an eight percent fee per transaction.<sup>253</sup> Moreover, if an individual chooses to send money directly through a service like western union, the fee could be as high as 11 percent.<sup>254</sup> The end result is a process that makes credit card transactions trustworthy but timely and costly since the merchants often pass that third-party costs to the customer in a process that can take days to complete.

In contrast, purchases with cryptocurrencies like Bitcoin remove the third parties from the transaction process. As discussed in Chapter II, cryptocurrencies replace expensive intermediaries with the blockchain, permitting cryptocurrency users to transact on a peer-to-peer basis with nearly no fees. Likewise, the transaction process with cryptocurrencies is often significantly quicker and more secure since the transaction data is permanently recorded within the blockchain and protected by cryptographic algorithms. Therefore, coupled with the decreased cost of transacting, incorporating cryptocurrency into the payment structure would decrease the costs of doing business, which could lead to more purchasing power of the customers.

The merchants and customers are not the only beneficiaries from a cryptocurrency adoption. Vigna and Casey point out that individuals reliant on global remittance—when migrant workers are sent abroad for work to send money via international transfer services to relatives in their home countries—would become a major benefactor from a state accepted cryptocurrency. They write of traditional currency transactions, “fees for money sent from the United States often hit 10 percent; from . . . other countries it can be double that. With exchange-rate costs, the total friction in the transaction can run as high as 30

---

<sup>252</sup> Vigna and Casey, 99.

<sup>253</sup> Vigna and Casey, 100.

<sup>254</sup> Vigna and Casey, 194

percent.”<sup>255</sup> For individuals who rely on out-of-country remittance(s), the money saved through the use of cryptocurrency would be a substantial gain in purchasing power as the recipients could in-turn use the increase available money within their local economy or as savings.

Ultimately, sovereign states could use cryptocurrency to increase economic opportunities and support their citizens. The adoption or creation of a sovereign cryptocurrency would indirectly facilitate state interests by providing extra money to the transactors, money that would normally lost to fiat transaction costs, but that citizens could then return to the local or regional economy, eventually bolstering the economic capacity of the state.

### **3. To Bypass Sanctions**

Authors in this thesis’s literature review generally view the capability for cryptocurrency to easily bypass sanctions negatively; nevertheless, for states on the receiving end of economic sanctions, cryptocurrency offers a form of economic relief. For one, cryptocurrency’s ability to transact and move wealth internationally without utilizing third parties offers sovereign states—and ostensibly those countries currently under international sanctions like Venezuela or Russia—the capability to ignore international laws and policies. States can take advantage of the disruptive enterprise that cryptocurrency promotes by creating a state-backed cryptocurrency controlled by the state, or likewise, incorporate a stateless cryptocurrency as an additional form of money.

### **4. The Auditability of Cryptocurrency**

Another use of cryptocurrency is that sovereign states could use cryptocurrency’s ability to maintain a ledger of every transaction to its advantage by adopting a state-created cryptocurrency to audit money flows and enhance AML/CTF laws. Sovereign states could create a trackable cryptocurrency, similar to Bitcoin; however, the proposed state cryptocurrency system would need to maximize the identification of users and require cryptocurrency users to register with the government. The government cryptocurrency

---

<sup>255</sup> Vigna and Casey, 189–190.

would incentivize users to register due to cryptocurrency's capacity to transact more cheaply on a peer-to-peer basis than other electronic methods of transaction (as mentioned earlier). Additionally, a proposed state-sponsored cryptocurrency would encourage legal employment of the cryptocurrency while discouraging the illegal use of other cryptocurrencies. By requiring users to register, the system would discourage illegal actors from using cryptocurrency. In contrast, licit actors have no need to hide their identity and should comply with the registration policy.

## **B. STATES THAT ACCEPT, PLAN TO ADOPT, OR HAVE ISSUED STATE-BACKED CRYPTOCURRENCIES**

Currently, there are no known states that have adopted Bitcoin or any other stateless cryptocurrency as their national currency; however, there are several states that have released or are developing their own state-backed cryptocurrency. This section outlines a selection of countries that have released a sovereign cryptocurrency and are working on their own bitcoin-like state-backed cryptocurrency. Also, it examines the real-world cases where Bitcoin has become the preferable form of money.

### **1. The Venezuelan Petro**

In the beginning of 2018, President Nicolas Maduro of Venezuela announced to the world that Venezuela would issue a cryptocurrency that pegs its value to the price of a barrel of oil.<sup>256</sup> The Venezuelan *Petro*, which is named after the commodity it represents, is designed by the Venezuelan government as a cryptocurrency to be bought, sold, and exchanged for other cryptocurrencies like Bitcoin. Moreover, Venezuela promoted a public presale of the state-backed cryptocurrency to obtain capital prior to the official release, successfully raising approximately 735 million USD for the government on opening day.<sup>257</sup> The Venezuelan government claims that the state-backed cryptocurrency will

---

<sup>256</sup> Fabian Cambero and Girish Gupta, "Maduro Says Venezuela Will Issue \$5.9 Billion in Oil-Backed Cryptocurrency," Reuters, January 6, 2018, <https://www.reuters.com/article/us-venezuela-economy/maduro-says-venezuela-will-issue-5-9-billion-in-oil-acked-cryptocurrency-idUSKBN1EV02S>.

<sup>257</sup> Lesley Wroughton and David Alexander, "U.S. Bans Transactions with Venezuela's Digital Currency," Reuters, March 20, 2018, <https://www.reuters.com/article/uk-crypto-currencies-venezuela-usa/u-s-blocks-use-of-venezuelas-digital-currency-white-house-idUSKBN1GV2AX>, sec. Foreign Exchange Analysis.

become widely accepted within the country, allowing the citizens of Venezuela “to make payments to public institutions, including tax payments, according to official documents explaining the initiative.”<sup>258</sup>

The release of the Petro, however, has had a number of critics internationally, and the future of the Petro is uncertain as hyperinflation and a weak economy continue to take their toll on the U.S. sanctioned country. Robert Looney asserts that Venezuela is plagued by a series of poor economic choices, which have resulted in the hyperinflation of the state fiat currency, the bolivar, with an inflation rate expected to reach over 3400 percent by 2019.<sup>259</sup> He explains, “The Petro’s primary function would be to secretly move cash out of a collapsing economy and convert it into foreign currency, making a Petro a digital money laundering tool for government insiders and their cronies.”<sup>260</sup> Moreover, There are a number of countries that argue the petro is a simply a ploy by the Venezuelan government to raise capital and skirt international sanctions in the process. For instance, via executive order, the United States has released guidance on the petro prohibiting U.S. citizens from purchasing or trading with the Venezuelan virtual currency.<sup>261</sup> Because the cryptocurrency is peer-to-peer, Venezuela can transfer wealth in and out of the state without dealing with the institutions that assist in enforcing international sanctions.

Another interesting revelation is that the Venezuelan government was not acting unilaterally in the design and release of the state backed cryptocurrency. According to a March exclusive issue by *Time*, the Petro release is a joint experiment between Russia and Venezuela to design and test a virtual currency in a sanctioned country.<sup>262</sup> The exclusive

---

<sup>258</sup> Rachele Krygier, “Venezuela Launches the ‘Petro,’ Its Cryptocurrency,” *Washington Post*, February 20, 2018, <https://www.washingtonpost.com/news/worldviews/wp/2018/02/20/venezuela-launches-the-petro-its-cryptocurrency/>, sec. WorldViews.

<sup>259</sup> Robert Looney, “Hyperinflation Is Crippling Venezuela, but Maduro Has No Interest in Fixing It,” *World Politics Review*, January 23, 2018, <https://www.worldpoliticsreview.com/articles/24035/hyperinflation-is-crippling-venezuela-but-maduro-has-no-interest-in-fixing-it>.

<sup>260</sup> Robert Looney, “Venezuela’s Economic Collapse,” *Milken Institute Review*, February 28, 2018, <http://www.milkenreview.org/articles/venezuelas-economic-collapse>.

<sup>261</sup> Wroughton and Alexander, “U.S. Bans Transactions.”

<sup>262</sup> Simon Shuster, “Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions,” *Time*, March 20, 2018, <http://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/?iid=sr-link1>.

notes that Russia has expressed interest in creating its own official “CryptoRuble;” however, the Russians are concerned about the economic and political backlash they might face. Simon Shuster comments, “instead of putting the ruble at risk, Russia encouraged its ally in Latin America to run the experiment on itself.”<sup>263</sup> Ultimately, the pending success or failure of the Venezuelan cryptocurrency and its effectiveness in dodging U.S. sanctions may pay dividends to other internationally-sanctioned countries, as the Petro becomes a baseline test that other countries—like Russia—can use in the development of their own cryptocurrency.

The Petro may not be an ideal example of a state-backed cryptocurrency due to the unique circumstances around its development and the economic status of its backer nation; nonetheless, its emergence is the first case of a state-backed cryptocurrency to be sold as a part of the cryptocurrency ecosystem. One day after the launch of the Petro and after raising a proclaimed 735 million USD, Maduro announced the *Petro Gold*, a cryptocurrency that is planned to be backed by the Venezuela’s gold commodity.<sup>264</sup> Irrespective of the intentions for its use, the Petro as a state-backed cryptocurrency, has proven that a state can develop and market a cryptocurrency internationally.

## **2. The Russian “CryptoRuble”**

The Russian Federation has also announced it is interested in the creation of a state-backed cryptocurrency. As a complement to Russia’s evolving cryptocurrency initiative, President Putin recently introduced five directives in October 2017 ordering the creation of new domestic legislation to tax and regulate cryptocurrency, specifically targeting the Russian miners, ICOs, and exchanges in Russia.<sup>265</sup> Following the announcement by its president, Russia has been swept by a wave of cryptocurrency acceptance within the country. According Shannon Liao, businesses have started accepting cryptocurrency as a payment method and graphics cards essential to mining cryptocurrency are in short supply

---

<sup>263</sup> Shuster.

<sup>264</sup> Brian Ellsworth and Ana Isabel Martinez, “Venezuela Aims for Crypto Alchemy with New ‘Petro Gold’ Token,” Reuters, February 22, 2018, <https://www.reuters.com/article/uk-crypto-currencies-venezuela/venezuela-to-launch-petro-gold-cryptocurrency-backed-by-gold-maduro-idUSKCN1G52S2>.

<sup>265</sup> Liao, “Inside Russia’s Love-Hate Relationship with Bitcoin.”

across the country.<sup>266</sup> Also according to Liao, Russia's official stance on cryptocurrency has been increasingly unclear over the past few years as it ranges from appearing increasingly restrictive toward cryptocurrency users whereby the state threatened jail time to cryptocurrency users, to meeting with prominent founders of cryptocurrency outside of the state. Liao writes that these new initiatives are "likely part of the digital ruble initiative that the Russian Central Bank has been pursuing."<sup>267</sup> By regulating the existing miners, traders, and exchanges that deal with cryptocurrency, Russia would be better prepared to introduce and market its own state-backed cryptocurrency.

As aforementioned in the discussion on the Venezuelan Petro, Russia has an expressed interest in exploring how cryptocurrencies can bypass sanctions and state borders. Zura Kadushadze and Jim Kyung-Soo Liew write in detail on the CryptoRuble and Russia's motivations behind the development of a state-issued cryptocurrency. They argue, "Russia's . . . primary goal in issuing a government cryptocurrency is to free their monetary system from the controls exerted by the Federal Reserve (Fed), European Central Bank (ECB), and their allied central banks."<sup>268</sup> They also argue that the Cryptoruble unchains itself from the western countries banks by "[creating] a buffer layer that only the Russian government has control over with pertinent information inaccessible to the Fed/ECB, . . . the U.S., the E.U., etc."<sup>269</sup> (see Figure 5). In the form imagined by Kadushadze and Liew, the CryptoRuble would be able to effectively launder money through the Russian central authority and subject to manipulation at the hands of the Russian oligarchs.

---

<sup>266</sup> Liao.

<sup>267</sup> Liao.

<sup>268</sup> Zura Kakushadze and Jim Kyung-Soo Liew, "CryptoRuble: From Russia with Love," November 2, 2017, <https://arxiv.org/ftp/arxiv/papers/1801/1801.05760.pdf>, 3.

<sup>269</sup> Kakushadze and Liew, 20.

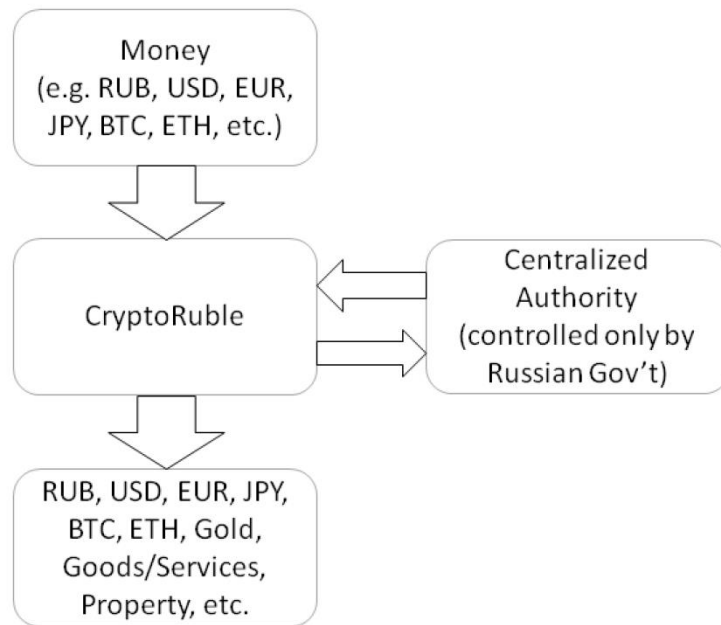


Figure 5. “A Schematic Depiction of the Money Flow into and from CryptoRuble”<sup>270</sup>

Russia has also announced a CryptoRuble registration system to combat the anonymity inherent in stateless cryptocurrency systems; however, that too, appears to be dubious in execution. According to news reports released in 2017 by local Russian media, the proposed CryptoRuble would have a 13 percent tax applied to all unregistered exchanges of currency.<sup>271</sup> Kakushadze and Liew write that the unregistered user tax is “akin to a government-mandated money laundering machine and with such a low overhead should be extremely attractive to all sorts of shady players.”<sup>272</sup> Furthermore, since the ledger that records all transactions would be maintained by the government, Kakushadze and Liew assert that Russia could later blackmail unsuspecting illicit actors using the CryptoRuble to launder money.

---

<sup>270</sup> Source: Kakushadze and Liew, 20.

<sup>271</sup> Devin Coldewey, “Russia May Soon Issue Its Own Official Blockchain-Based Currency, the CryptoRuble,” *TechCrunch* (blog), October 15, 2017, <http://social.techcrunch.com/2017/10/15/russia-may-soon-issue-its-own-official-blockchain-based-currency-the-cryptoruble/>.

<sup>272</sup> Kakushadze and Liew, “CryptoRuble: From Russia with Love,” 3.

Russia's proposed CryptoRuble would differ in function from Bitcoin's to ensure that the Russian government have complete and solitary control over the cryptocurrency. As discussed in Chapter II, Bitcoin's model revolves around a decentralized public ledger stored within the blockchain and managed by a volunteer ecosystem of incentivized miners and nodes which expand the blockchain by validating bitcoin transactions. Conversely, the CryptoRuble would be centralized whereby the Russian government would be solely responsible for maintaining the cryptoruble ledger and controlling access to the cryptocurrency. Kakushadze and Liew assert the CryptoRuble would be more efficient than Bitcoins and the "central banks and sovereign governments . . . more control, not less, than with the current banking system."<sup>273</sup> The CryptoRuble has yet to be released, and the conclusion of many authors concerning the intent of the CryptoRuble are speculative in nature; nevertheless, the development and future release of a Russian cryptocurrency provides insight into how a state-backed cryptocurrency could become disruptive to the international financial system.

### **3. Countries where Bitcoin Have Become the Trusted Currency**

Bitcoin has become a major store of value and trusted money supply for the citizens of Kenya, Sudan, South Africa, and Zimbabwe. Currently, none of the four countries governments support Bitcoin; however, Bitcoin's ability to transact internationally and peg its value to the supply and demand outside of the secluded African countries has made the cryptocurrency an attractive choice for a store of wealth. Matina Stevis-Gridneff and Georgi Kantchev note that Bitcoin "is often viewed as a haven from political and economic turmoil" that plagues many less developed or developing nations.<sup>274</sup> These cases of bitcoin adoption by the people of the country without the consent of the sovereign government provides insight to how an actual state-sponsored cryptocurrency might function under similar circumstances.

Cryptocurrencies are often cited as a means to bypass sanctions as a negative, but for the citizens of Sudan, Bitcoin offers a way to transact internationally bypassing the

---

<sup>273</sup> Kakushadze and Liew, 3.

<sup>274</sup> Stevis-Gridneff and Kantchev, "Bitcoin Is a Hit in Countries."



sanctioned Sudanese government.<sup>275</sup> Similarly, in Zimbabwe where hyperinflation runs rampant, the classically volatile value of bitcoin has become a source of reliability in comparison. MacDonald Dzirutwe asserts that inflation in the country has risen to nearly 50 percent per month—despite switching to the U.S. dollar as the official currency for the country—making bitcoin the de facto currency for many people.<sup>276</sup> In both cases, cryptocurrency has proven itself to be a reliable supply of money for the people and a trusted medium of exchange.

Similar to the situation outlined in African countries, Bitcoin has become an outlier currency among Argentines who are frustrated with the government's money controls over the state-backed fiat, the peso. Elena Moreno asserts, "For some Argentines, bitcoin is a legitimate alternative to state backed currency. According to one estimate, bitcoin users in Argentina trade \$70,000–\$80,000 over the counter per day."<sup>277</sup> As the time of writing, Argentina's official stance on virtual currencies is that they are "not legal tender under the country's National Constitution, which designated the Central Bank as the only authority that may issue legal tender."<sup>278</sup> While 70–80 thousand USD a day may not be a huge amount, Argentina still stands as a case study of a state wherein the people have chosen bitcoin as their choice of money over their sovereign currency.

Jill Carlson studies the case of outlier Bitcoin adoption in Argentina and has attributed four variables why cryptocurrencies could see outlier adoption in a state that does not currently support virtual currencies. She suggests that the factors of "capital control circumvention, . . . tax evasion, . . . cultural and ideological factors . . . and the presence of multiple accepted currencies and exchange rates may play a critical role in

---

<sup>275</sup> Stevis-Gridneff and Kantchev.

<sup>276</sup> MacDonald Dzirutwe, "Think Bitcoin's Getting Expensive? Try Zimbabwe," Reuters, November 12, 2017, <https://www.reuters.com/article/us-zimbabwe-bitcoin/think-bitcoins-getting-expensive-try-zimbabwe-idUSKBN1DD0NF>.

<sup>277</sup> Elena Christine Moreno, *Bitcoin in Argentina: Inflation, Currency Restrictions, and the Rise of Cryptocurrency* (Chicago: University of Chicago Law School, 2016), [https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1017&context=international\\_immersion\\_program\\_papers](https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1017&context=international_immersion_program_papers).

<sup>278</sup> "Digital Currencies," Perkins Coie.

acceptance of a new entrant into the economy.”<sup>279</sup> Although cryptocurrency use in countries like Kenya, Sudan, South Africa, Zimbabwe, and Argentina are not sanctioned by the governments, an analysis of how bitcoin became a preferred currency would prove useful for a sovereign state in a similar situation that chooses to implement or adopt a cryptocurrency; however, such an analysis is outside the scope of this thesis and is one of the areas this thesis recommends for future research in the conclusion.

#### **4. The U.S. Fedcoin**

The U.S. dollar is arguably the most widely used currency on earth. As Kimberly Amadeo writes, the U.S. dollar “makes up 64 percent of all known central bank foreign exchange reserves. That makes it the def facto global currency.”<sup>280</sup> As a result of its importance to the global economy, the U.S. dollar has become trusted, but what if the United States builds on the earned trust to promote its own sovereign-cryptocurrency for worldwide use? Enter the fedcoin.

The idea for an official Federal Reserve cryptocurrency (fedcoin) has been widely explored by scholars who study banking, economics, and virtual currencies. In 2014, JP Koning first pitched the fedcoin, and among scholars, the idea has since gained popularity to become the default title of a theoretical U.S. backed cryptocurrency.<sup>281</sup> From the literature this researcher examined, most authors envision the theoretical fedcoin as blockchain based, centralized in control, and pegged to the U.S. dollar. As stated Morten Bech and Rodney Garratt on the behalf of the BIS,

[T]he idea is for the Federal Reserve to create a cryptocurrency that is similar to bitcoin. However, unlike with bitcoin, only the Federal Reserve would be able to create Fed Coins and there would be one-for-one convertibility with cash and reserve. Fedcoins would only be created (destroyed) if an equivalent amount of cash or reserves were destroyed

---

<sup>279</sup> Jill Carlson, *Cryptocurrency and Capital Controls* (Oxford: University of Oxford, 2016), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3046954](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046954), 13–14.

<sup>280</sup> Kimberly Amadeo, “Global Currency: Definition, Role of the Dollar,” The Balance, last updated February 19, 2018, <https://www.thebalance.com/world-currency-3305931>.

<sup>281</sup> JP Koning, “Fedcoin,” *Moneyness* (blog), October 19, 2014, <http://jpkoning.blogspot.com/2014/10/fedcoin.html>.

(created) at the same time. Like cash, Fedcoin would be decentralised in transaction and centralised in supply.<sup>282</sup>

Although Bech and Garratt envision the Fedcoin as a “third component of the monetary base, alongside cash and reserves,”<sup>283</sup> not all researchers believe that a Fedcoin is feasible.

Berentsen and Schar have come to the conclusion that a central bank cryptocurrency permitting anonymity is unrealistic. They write, “no reputable central bank would issue a decentralized virtual currency where users can remain anonymous.”<sup>284</sup> Instead, they argue in favor for “Central Bank Electronic Money,” which is comprised of a centralized and not anonymous, virtual, and monopolized by the central bank. Figure 6 depicts the different structures between a central bank cryptocurrency and central bank electronic money by Berentsen and Schar. Nevertheless, scholars agree that there is breathing room in the global economy for the creation of a U.S.-backed digital currency, cryptocurrency, or otherwise. As Vigna and Casey state,

the dollar is already the world’s primary reserve and commercial currency, but this [a U.S. digital dollar] would give it an even bigger edge. That’s because people in countries whose currencies aren’t trusted or who are barred or restricted from buying foreign currencies—think China, Argentina, Russia—Could now easily obtain the one currency that has long symbolized international stability.<sup>285</sup>

In the near future, it is likely that the United States will be forced to confront new virtual challenges as individuals worldwide find new and cheaper methods to transfer money and transact. Chris Telley argues, “the U.S. national security community must understand the power of cryptocurrencies, recognize threat adaptations, and invest in capabilities to influence the digital economy environment.”<sup>286</sup> The development of a

---

<sup>282</sup> Morten Bech and Rodney Garratt, “Central Bank Cryptocurrencies,” *BIS Quarterly Review* (September 2017), [https://www.bis.org/publ/qtrpdf/r\\_qt1709f.pdf](https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf), 63.

<sup>283</sup> Bech and Garratt, 61.

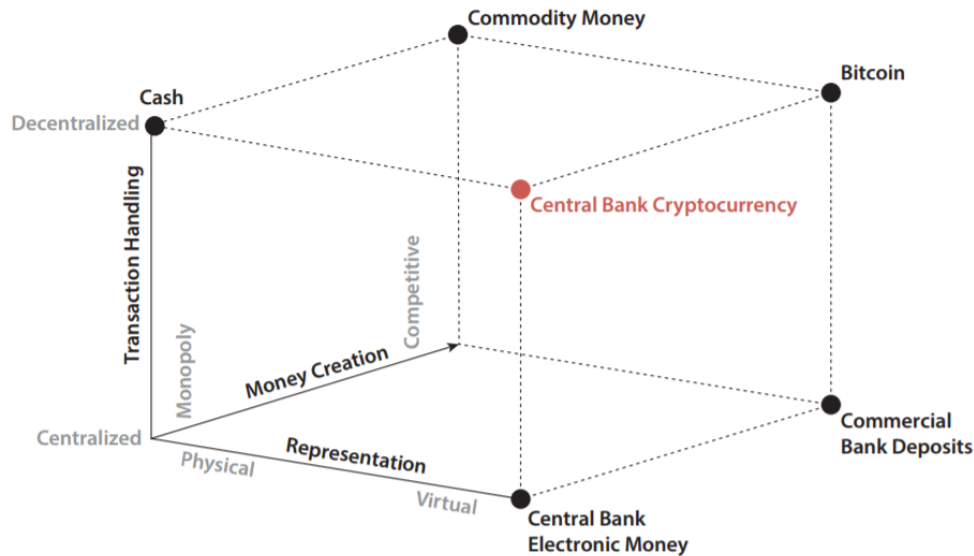
<sup>284</sup> Aleksander Berentsen, and Fabian Schar, “The Case for Central Bank Electronic Money and the Non-Case for Central Bank Cryptocurrencies.” *Economic Research: Federal Reserve Bank of St. Louis* 100, no. 2 (February 2018): 104.

<sup>285</sup> Vigna and Casey, *The Age of Cryptocurrency*, 304.

<sup>286</sup> Telley, “A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency,” 4.

cryptocurrency fedcoin—centralized or decentralized, pseudonymous or otherwise—would enable the United States to influence the digital economy and provide it an advantage over sovereign countries that have proposed their own sovereign virtual currencies, such as Russia’s CryptoRuble.

#### Control Structure of Currencies



NOTE: Adapted from Berentsen and Schär (2017).

Figure 6. The Control Structure of Currencies<sup>287</sup>

## 5. Other Countries Studying or Developing Cryptocurrencies

Venezuela, Russia, and the United States are not the only countries interested in studying and developing cryptocurrency. Prasad writes that in addition to Venezuela, Russia, and the United States, the countries of China, Japan, France, Canada, United Kingdom, Brazil, Australia, South Africa, Singapore, Hong Kong, Sweden, Philippines, Indonesia, India, Lebanon, Eastern Caribbean, South Korea, Israel, and the Netherlands, all have active programs exploring blockchain technology as a currency or have officially

<sup>287</sup> Source: Berentsen and Schar, “The Case for Central Bank,” 98.

announced plans to release their own virtual currency based on the blockchain.<sup>288</sup> Another future application of cryptocurrency could be a regional supranational cryptocurrency, like a virtual euro coin, which would encompass an entire region and be accepted by a number of sovereignties.

### **C. POTENTIAL CHALLENGES TO ADOPTING CRYPTOCURRENCY**

A state adopting an existing cryptocurrency or creating its own must also confront a number of variables to protect its economic and political wellbeing. This section provides a selective list of four obstacles or vulnerabilities that can hinder the cryptocurrency adoption process: a speculative attack on a sovereign state's central bank, domestic pushback on cryptocurrency acceptance within a sovereign state, the pushback from the third-party institutions that stand to lose profits from the implementation of a peer-to-peer state-backed cryptocurrency, and the 51 percent vulnerability that malicious actors could use to disrupt or discredit a sovereign-state's cryptocurrency system.

#### **1. Speculative Attack**

One weakness of a sovereign state adopting or recognizing a stateless cryptocurrency like Bitcoin is that the adopting country then becomes vulnerable to a speculative attack. Nicholas Plassaras explicates “a speculative attack on a currency occurs when an investor wishes to take advantage of a ‘weak currency,’ a currency that has depreciated in value relative to other currencies.”<sup>289</sup> The objective of a speculative attack is that it takes advantage of a discrepancy called a *maturity mismatch* of funds, a term used in this case when the bank is forced to buy the weaker currency at a loss. Plassaras asserts, “This discrepancy [maturity mismatch] gradually depletes the bank's supply of the attacked currency over time,” and if not properly protected against, the attack could “[trigger]

---

<sup>288</sup> Prasad, *Central Banking in a Digital Age*, 34–39.

<sup>289</sup> Plassaras describes the speculative attack, writing “the attack begins by taking what is known as a ‘short position’ in the currency. To do this, the attacker borrows a sum of the weak currency and sells it for a stronger (more valuable) currency, with the intention of buying the weak currency back for less than the attacker sold it for. If the currency continues to depreciate in value after the short sale, the attacker makes a profit when they buy it back.” Plassaras, “Regulating Digital Currencies.”

destabilization in the foreign currency exchange market.”<sup>290</sup> Plassaras highlights that traditionally, international institutions like the IMF keep reserves of currencies to provide assistance to the banks when needed and to protect against speculative attacks. However, the IMF does not currently hold any supply of cryptocurrency, and therefore it cannot assist banks with absorbing a maturity mismatch involving cryptocurrencies.<sup>291</sup>

Although Plassaras’s solution of the banks vulnerability to maturity mismatch would be for the IMF to hold a reserve stock of cryptocurrency, he also notes there are obstacles to this proposal.<sup>292</sup> First, he notes that that Article VII of the IMF’s Articles of Agreement “only authorizes the IMF to collect currency from member nations.”<sup>293</sup> Second, if cryptocurrencies become a part of the IMF reserves, who would be responsible for the purchase of the cryptocurrency? If sovereign states were to adopt or accept a stateless cryptocurrency like Bitcoin before adequate measures are put in place to protect banks from maturity mismatches, they would find themselves at higher risk to speculative attack.

## **2. Domestic Pushback as an Accepted Currency**

Adopting a state-approved cryptocurrency carries significant hurdles in both implementation and adoption. As highlighted in Chapter II, the concepts of the Bitcoin protocol and blockchain are complex. As a consequence of the intricacies of cryptocurrency, citizens, unfamiliar with cryptocurrency technology, may refuse to trust cryptocurrencies over a money supply that can be physically seen or held. Likewise, Vigna and Casey highlight that unique to each country, there are significant social and cultural barriers that a state-sanctioned cryptocurrency must overcome to become widely accepted and adopted.<sup>294</sup> The adoption of a cryptocurrency by the state would only be successful if the citizens trust and use the cryptocurrency as a form of money.

---

<sup>290</sup> Plassaras, 398.

<sup>291</sup> Plassaras, 399.

<sup>292</sup> Plassaras, 400.

<sup>293</sup> Plassaras, 401.

<sup>294</sup> Vigna and Casey, *The Age of Cryptocurrency*, 194.

### **3. Resident Institutional Pushback**

Even if a cryptocurrency similar in concept to Bitcoin was adopted by a sovereign state, a number of institutional pushbacks internal to the state could disrupt the adoption process. As Chapter II discusses, cryptocurrency is peer-to-peer and avoids the traditional third-parties associated with fiat currencies; those third-parties, like banks, stand to lose profits if a state-sanctioned cryptocurrency is introduced into the economy. In Prasad's 2018 study of how cryptocurrency would alter central banking, he comes to the conclusion that

Financial institutions, especially banks, could face challenges to their business models, as new technologies facilitate the entry of institutions (or decentralized mechanisms) that can undertake financial intermediation and overcome information asymmetries. Banks will find it difficult to continue collecting economic rents on some activities that cross-subsidize other activities. The emergence of new institutions and mechanisms could improve financial intermediation but will pose significant challenges in terms of regulation and financial stability.<sup>295</sup>

As a consequence, sovereign states may find significant political barriers to the implementation of cryptocurrency erected by political lobbyists representing the businesses that stand to lose revenue from the introduction of cryptocurrency.

### **4. 51 Percent Attack**

One of the most discussed weaknesses in cryptocurrencies like Bitcoin is the notion of a 51 percent attack. As discussed in Chapter II, Bitcoin miners achieve consensus on the correct blockchain and valid transactions through a distributed network of individual miners building the blockchain on top of the longest branch of valid transactions.<sup>296</sup> In theory, a 51 percent attack occurs when a malicious actor gains control of the majority (51 percent) of the network to obtain mining consensus on future transactions of the system.<sup>297</sup> Recall as discussed in Chapter II, miners will by default attempt to build on the longest blockchain; thus, as a result of controlling the majority of the network, a malicious attacker

---

<sup>295</sup> Prasad, *Central Banking in a Digital Age*, 4.

<sup>296</sup> Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 28–34.

<sup>297</sup> Narayanan et al., 48.

could likely succeed in creating the longest branch of the blockchain.<sup>298</sup> The malicious actor could then add new invalid blocks with invalid transactions to the blockchain to manipulate the public ledger.<sup>299</sup> Cryptocurrencies like Bitcoin are praised for their resilience to outside attack, but the 51 percent attack is one the greatest weaknesses of decentralized virtual currencies. Similarly, Vigna and Casey submit that the 51 percent attack “eats at a lot of bitcoin intellectuals. Why? Because it’s the one irrefutable structural weakness in the bitcoin system.”<sup>300</sup>

However, the 51 percent attack is limited to manipulating the future creation of blocks and cannot alter the protocol by which Bitcoin operates, nor can it alter public ledger prior to the attack. The security inherent in Bitcoin’s blockchain protocol that controls the rules of the system and the distributed public ledger is virtually uncrackable due to safety guaranteed by the hash function (as highlighted in Chapter II).<sup>301</sup> According to Narayanan et al., if an attacker in control of 51 percent of the nodes were to attempt to manipulate the system, such as to steal bitcoins from another user, to spend bitcoins that the attacker does not own, or to change the block reward to a greater quantity of bitcoins, the Bitcoin network on the honest nodes would ignore the invalid actions.<sup>302</sup> More importantly, if attackers were to somehow gain control of at least 51 percent of the network, their attack would be evident to the honest nodes. Narayanan et al. assert, “If there were, in fact, actual signs of a 51 percent attack, what would probably happen is that the developers would notice it and react.”<sup>303</sup> The attack would have little bearing on the network’s users or capacity; instead, it would damage Bitcoin’s trust, an injury that would fair far worse to the cryptocurrency than a temporary disruption in services.

As stated in the second chapter of this thesis, the concept of trust is essential to any currency’s adoption as a form of money. Narayanan et al. argue, “It is not only possible,

---

<sup>298</sup> Narayanan et al., 48.

<sup>299</sup> Narayanan et al., 48.

<sup>300</sup> Vigna and Casey, *The Age of Cryptocurrency*, 155.

<sup>301</sup> Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, 1.

<sup>302</sup> Narayanan et al., 48–49.

<sup>303</sup> Narayanan et al., 49.



but in fact likely, that a 51 percent attacker of any sort will destroy confidence in the system.”<sup>304</sup> Accounting for the fact that bitcoin’s value relies on the principles of supply and demand principles, if the cryptocurrency were to lose trust, the likely effect would result in the decline in value of bitcoin. Narayanan et al. emphasize that the point of a 51 percent attack is one of disruption to “destroy confidence” because no other reason really “make[s] sense from a financial point of view.”<sup>305</sup> To achieve the majority control of the network is no small feat, considering the Bitcoin network is rather large and interconnected worldwide by anonymous individual users who choose to participate in the process; however, the task is not impossible, especially for a sovereign state with a large amount of fiscal resources that is set on disrupting cryptocurrencies. As a result, the 51 percent attack remains a valid concern for any state adopting a decentralized, proof-of-work cryptocurrency.

#### **D. CONCLUSION**

Currently, no state other than Venezuela has released its own cryptocurrency, but it is likely that other states will develop and release their own version of the blockchain-based virtual currency in the near future. Cryptocurrency’s potential to interconnect the globe and uplift the unbanked in poverty-stricken states, or to be used by sanctioned countries to bypass international laws, makes cryptocurrency a potentially powerful and disruptive tool for sovereign states. Its adoption is a double edge sword carrying a number of benefits and vulnerabilities in implementation and use. Venezuela is one of the first states to take advantage of a sovereign cryptocurrency. Additionally, with dozens of countries investigating the prospects of cryptocurrency, it is very likely that other countries will develop and introduce their own sovereign cryptocurrencies in the near future. This chapter has discussed the advantages and drawbacks in a sovereign cryptocurrency. Next chapter is this thesis’s conclusion, and it draws on the discussions in Chapter III, IV, and V to analyze how cryptocurrencies affect sovereign states.

---

<sup>304</sup> Narayanan et al., 49.

<sup>305</sup> Narayanan et al., 51.

THIS PAGE INTENTIONALLY LEFT BLANK

## VI. CONCLUSION

Cryptocurrency is a disruptive technology easily accessible by illicit actors, resilient to sovereign state and international laws, and it is a capable medium to transfer wealth from person-to-person across multiple jurisdictions. Therefore, it is necessary that sovereign states carefully consider the best approach to limit illegal or disruptive cryptocurrency use. As Vigna and Casey assert,

the decentralized bitcoin network and its public ledger, the blockchain, are at their essence a radical new way of dealing with information. . . .[I]t takes information about monetary transactions and economic exchanges out of the hands of monopolist institutions and creates a decentralized mechanism for society to judge the validity of that information.<sup>306</sup>

As a consequence of cryptocurrency's ability to subvert domestic and international economic models and law enforcement structure, sovereign states have issued a variety of legislation—varying by country—to limit cryptocurrency's impact on the state. To address the relationship between the sovereign state and cryptocurrency technology, this thesis asked the following primary question: What options are available to the sovereign state to limit cryptocurrency's capacity to challenge domestic and international laws? To further explore the main question, this thesis also examines the following three subquestions. First, what allows cryptocurrency to sidestep the established financial order and enforcement institutions? Second, what are the challenges sovereign states face when introducing cryptocurrency legislation? Finally, as cryptocurrency technology becomes more popular and countries begin developing their own blockchain-based tools, what factors would inhibit or promote a sovereign state from developing its own sovereign cryptocurrency?

To address these questions, this thesis is divided into six chapters. After a detailed literature review in the first chapter, the thesis's second chapter dissect the technology behind Bitcoin and other cryptocurrency ecosystems. Chapters III, IV, and V detail banning, regulating, and adopting cryptocurrency by sovereign states to highlight the consequences of each action by providing real-world examples of each approach. In

---

<sup>306</sup> Vigna and Casey, *The Age of Cryptocurrency*, 310.

addition to finding states can ban, regulate, or adopt cryptocurrency, this thesis recommends that states carefully consider these options and develop a combination of the three approaches appropriate to political, economic, and fiscal interests. Additionally, this thesis recommends three specific approaches the international community could take to better mitigate the potential for cryptocurrency to be used disruptively.

## **A. FINDINGS**

Cryptocurrency's ability to transact from peer-to-peer while prioritizing anonymity has complicated the enforcement of previously established sovereign and international laws. Alone, cryptocurrencies are not illicit tools, but their features allow them to be used as a tool to transact without governmental oversight. As this thesis highlights in the literature review, the reduction of country's sovereign power to enforce laws and prosecute illicit actors have also reduced countries' capability to enforce domestic, homeland security, and homeland defense policies. The benefits offered in cryptocurrency transactions have allowed organized crime and drug traffickers, terrorist groups, rouge states like North Korea, and sanctioned countries like Russia to conduct transactions without U.S. or other international interference. To examine how cryptocurrency provides near anonymous, stateless, peer-to-peer transactions, Chapter II of this thesis dissects the cryptocurrency Bitcoin and the Bitcoin ecosystem to analyze the technology permitting Bitcoin to operate without the need of a sovereign government.

As discussed in Chapter III, cryptocurrencies like Bitcoin will continue to flourish regardless of whether or not a country incorporates a complete ban on cryptocurrency transactions. Sovereign states have the option to outlaw cryptocurrency mining, exchanges, trading, or fundraising through ICOs; however, the stateless nature of cryptocurrency makes it accessible to any individual with access to the Internet. Chapter III notes that China's government and central bank have all but outlawed ownership of cryptocurrency in an effort to gain greater command over domestic capital controls and the export of Chinese wealth, forcing the majority of Chinese based cryptocurrency mining companies and exchanges to migrate to less restrictive countries, like Singapore and Canada. Despite the heavy Chinese restrictions on cryptocurrency, the stateless cryptocurrency network

continued to thrive, and the citizens of China will continue to access and transact with cryptocurrency unless the government successfully bans access to digital wallets and exchanges.

This thesis also has found a number of technical and political hurdles challenging sovereign states' ability to regulate cryptocurrency. Chapter IV notes that since cryptocurrency has emerged, countries have struggled to define or categorize it under the framework of existing laws. Depending on the country and regulatory agency, virtual currencies—the category cryptocurrency falls under—are classified as either a security, currency, property, or commodity. Moreover, the term cryptocurrency is often referred to in the pejorative, insinuating that cryptocurrency is a form of money that is unregulated and associated with illicit circles; however, owning, investing in, or transacting with cryptocurrency is not inherently criminal in nature. To date, there has yet to be any internationally agreed upon method, minimum standard, metric, or guidance for countries to pursue cryptocurrency legislation. Ultimately, cryptocurrency remains an amorphous system of electronic money still unrecognized by the majority countries as official method of transaction.

This thesis has also examined the advantages, disadvantages and limitations in the introduction of a state-backed sovereign cryptocurrency in Chapter V. This thesis finds that countries can introduce a sovereign cryptocurrency developed specifically for official use as an attractive and reliable form of virtual money. Sovereign cryptocurrencies, much like Bitcoin, are efficient, unforgeable, and easily auditable characteristics provided through blockchain; however, unlike stateless cryptocurrencies, state-backed cryptocurrencies would be centrally controlled by the sovereign government or central bank and would likely minimize or actively disincentivize user anonymity through required registration or taxing anonymous transactions. Moreover, countries facing international economic sanctions, like Russia and Venezuela are, could use the disruptive features of cryptocurrency to their advantage, bypassing sanctioning institutions or countries during international transfers of wealth. To ensure the state-sponsored cryptocurrency is accepted transnationally, a sovereign country could buy back or link the value of a state produced

commodity like petroleum, natural gas, or gold, forcing other countries to buy in to or exchange for the sanctioned state cryptocurrency to purchase the given resource.

## **B. POLICY RECOMMENDATIONS**

After this thesis's in-depth analysis, this thesis recommends two specific policy actions that sovereign states and the international community can take to address future cryptocurrency strategy. The policy recommendations are to redefine cryptocurrency as its own category under sovereign law to promote awareness of the laws and drawbacks on cryptocurrency as well as to create an international standard comprising of a composition of banning, regulating, and adoption standards that would enable states to reign in and prosecute undesired cryptocurrency usage under their sovereignty.

### **1. Redefine Cryptocurrency**

To ease the legislative process of introducing new laws and clarify the rules for domestic companies and citizens, sovereign states could clearly define cryptocurrencies and other virtual currencies in their own category. This thesis points out that cryptocurrency is a revolutionary new step forward in innovative, open-source technology, and unless laws drastically change to restrict cryptocurrencies, companies and businesses are likely to continue refining blockchain technology well into the future. However, in countries that embrace technological developments, virtual currency regulations are often convoluted, ambiguous, and contradictory. The United States is a prime example as it classifies cryptocurrency as property, a security, or commodity to fit under existing laws and enumerates a variety of regulatory agencies to individually develop new, state-wide cryptocurrency guidance. Rather than allowing individual regulatory bodies to interpret cryptocurrency under their jurisdictions, the creation of an all-encompassing categorization for virtual currencies with clearly distinct and subordinate legislation, specifically distinguishing licit and illicit cryptocurrency actions, would prevent confusion regarding cryptocurrencies among citizens and businesses.

## **2. New International Standards on Cryptocurrency Regulation**

A new transnational or international set of regulatory minimums and information sharing could minimize the disruptive capacity of stateless and state-backed cryptocurrency transactions. Despite proposals to regulate cryptocurrency on an international level, there still remains a lack of international standards or minimum requirements—outside of AML/CTF regulations—for countries to reference when dealing with limiting, prohibiting, reporting, or using cryptocurrency exchanges, users, and miners. A common framework of cryptocurrency regulation, possibly enforced by international organizations and agreements (such as the IMF or Basel banking accords), would allow governments to work together to monitor and track illicit transactions occurring across sovereign borders. Furthermore, international institutions will be forced in the near-future to create guidelines or restrictions for transactions with sovereign cryptocurrency. Sovereign cryptocurrencies, like the Petro and CryptoRuble, facilitate new means for countries to move money that they otherwise would be unable to using traditional fiat, thus avoiding transnational banking oversight and imposed sanctions. The creation of internationally agreed upon regulatory minimums for cryptocurrencies could potentially alleviate the disruptive effects from the introduction of new sovereign cryptocurrency.

### **C. RECOMMENDATIONS FOR FURTHER RESEARCH**

This thesis discusses a number of current regulatory actions taken by different countries but is unable to provide analysis of the effectiveness of cryptocurrency legislation. For future research, this thesis recommends research into the development of a metric to measure the effectiveness of existing legislation to determine if sovereign states have prevented illicit transactions in accordance with AML/CTF standards. Additionally, new laws and regulations need to be designed to counter sovereign-state developed cryptocurrencies, therefore warranting research into how disruptive state cryptocurrencies, such as the Petro or CryptoRuble, could be contained, exploited, or challenged. Another potential research topic could analyze how the regime type of government (democratic, authoritarian, etc.) correlates to how the government is to regulate cryptocurrency. For example, Russia, Sudan, China, and Venezuela all have aspects of authoritarianism in their

governmental structures; however, their approaches to cryptocurrency widely differs. Scholars could potentially use this prospective research question to predict future regulatory responses by sovereign states concerning new innovative and disruptive technologies like cryptocurrency.

#### **D. CONCLUSION**

The propensity of individuals, criminal organizations, terrorist groups, and sovereign states to use cryptocurrency to ignore domestic and international laws and reduce the security of sovereign states prompts action by countries around the globe. Keeping in mind cryptocurrencies' ability to challenge sovereign states' capacity to enforce domestic and international laws, individual countries would be wise to develop their own legislative approach combining regulating, adopting, and banning specific aspects, while participating in an international discussion to develop a global cryptocurrency standard.



## LIST OF REFERENCES

- 3blue1brown. "How Secure Is 256 Bit Security?" YouTube video. 5:05. July 8, 2017.  
[https://www.youtube.com/watch?v=S9JGmA5\\_unY&t=71s](https://www.youtube.com/watch?v=S9JGmA5_unY&t=71s).
- Amadeo, Kimberly. "Global Currency: Definition, Role of the Dollar." The Balance. Last updated February 19, 2018. <https://www.thebalance.com/world-currency-3305931>.
- Amugo, Kevin. *Circular to Banks and Other Financial Institutions on Virtual Currency Operations in Nigeria*. Abuja, Nigeria: Central Bank of Nigeria, 2017.  
<https://www.cbn.gov.ng/out/2017/fprd/aml%20january%202017%20circular%20to%20fis%20on%20virtual%20currency.pdf>.
- Baran, Paul. *On Distributed Communications: I. Introduction to Distributed Communications Networks*. RM-3420-PR. Santa Monica, CA: RAND Corporation, 1964. [https://www.rand.org/content/dam/rand/pubs/research\\_memoranda/2006/RM3420.pdf](https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf).
- Baron, Joshua, Angela O'Mahony, David Manheim, Cynthia Dion-Schwarz. *National Security Implications of Virtual Currency: Examining the Potential for Non-State Actors Development*. Santa Monica, CA: RAND Corporation, 2015.  
[https://www.rand.org/pubs/research\\_reports/RR1231.html](https://www.rand.org/pubs/research_reports/RR1231.html).
- Bech, Morten, and Rodney Garratt. "Central Bank Cryptocurrencies." *BIS Quarterly Review* (September 2017): 55–70. [https://www.bis.org/publ/qtrpdf/r\\_qt1709f.pdf](https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf).
- Berentsen, Aleksander, and Fabian Schar. "The Case for Central Bank Electronic Money and the Non-Case for Central Bank Cryptocurrencies." *Economic Research: Federal Reserve Bank of St. Louis* 100, no. 2 (February 2018): 97–106.
- Bitcoin Magazine*. "What Makes Bitcoin Valuable?" Accessed April 4, 2018.  
<https://bitcoinmagazine.com/guides/what-makes-bitcoin-valuable/>.
- Bloomberg News. "China Bans Financial Companies from Bitcoin Transactions." December 5, 2013. <https://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions>.
- Bohme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, Technology, and Governance." *The Journal of Economic Perspectives* 29, no. 2 (Spring 2015): 213–238.
- Bossert, Thomas P. "It's Official: North Korea Is behind WannaCry." *Wall Street Journal*, December 18, 2017. <https://www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537>.

- Brown, Steven. "Cryptocurrency and Criminality: The Bitcoin Opportunity." *The Police Journal: Theory, Practice and Principles* 89, no. 4 (2016): 327–339.
- Bryans, Danton. "Bitcoin and Money Laundering: Mining for an Effective Solution." *Indiana Law Journal* 89, no. 1, Article 13 (2014): 441–472.  
<https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11100&context=ilj>.
- Carlson, Jill. *Cryptocurrency and Capital Controls*. Oxford: University of Oxford, 2016.  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3046954](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046954).
- Camero, Fabian, and Girish Gupta. "Maduro Says Venezuela Will Issue \$5.9 Billion in Oil-Backed Cryptocurrency." Reuters, January 6, 2018. <https://www.reuters.com/article/us-venezuela-economy/maduro-says-venezuela-will-issue-5-9-billion-in-oil-acked-cryptocurrency-idUSKBN1EV02S>.
- Capozzalo, Olivia. "Putin Adviser Says 'CryptoRuble' Will Circumvent Sanctions, Government Remains Divided." *Cointelegraph*, January 2, 2018.  
<https://cointelegraph.com/news/putin-adviser-says-cryptoruble-will-circumvent-sanctions-government-remains-divided>.
- Choudhury, Saheli Roy, and Barry Huang. "Chinese ICOs: China Bans Fundraising through Initial Coin Offerings, Report Says." *CNBC*, September 4, 2017.  
<https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html>.
- Christin, Nicolas. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." In *Proceedings of the 22nd International Conference on World Wide Web (WWW '13)*. Rio de Janeiro, Brazil: ACM, 2013.
- Chun, Rene. "Big in Venezuela: Bitcoin Mining." *The Atlantic*, September 2017.  
<https://www.theatlantic.com/magazine/archive/2017/09/big-in-venezuela/534177/>.
- Clark, Grant, and Lulu Yilun Chen. "How China's Stifling Bitcoin and Cryptocurrencies: QuickTake." Bloomberg News, last updated February 27 2018.  
<https://www.bloomberg.com/news/articles/2018-01-09/how-china-s-stifling-bitcoin-and-cryptocurrencies-quicktake-q-a>.
- Clayton, Jay. "Statement on Cryptocurrencies and Initial Coin Offerings." U.S. Security and Exchange Commission. December 11, 2017. <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>.
- Coldewey, Devin. "Russia May Soon Issue Its Own Official Blockchain-Based Currency, the CryptoRuble." *TechCrunch* (blog), October 15, 2017.  
<http://social.techcrunch.com/2017/10/15/russia-may-soon-issue-its-own-official-blockchain-based-currency-the-cryptoruble/>.

- Committee on Payments and Market Infrastructures. *Digital Currencies*. Basel, Switzerland: Bank for International Settlements, 2015. <https://www.bis.org/cpmi/publ/d137.pdf>.
- De Filippi, Primavera. “Bitcoin: A Regulatory Nightmare to a Libertarian Dream.” *Internet Policy Review* 3, no. 2 (May 2014): 1–11. <https://doi.org/10.14763/2014.2.286>.
- Deng, Chao, and Lingling Wei. “China Cracks Down on Bitcoin.” *Wall Street Journal*, April 1, 2014. <https://www.wsj.com/articles/china-cracks-down-on-bitcoin-1396361492>.
- Drug Enforcement Administration. *2017 National Drug Threat Assessment*. DEA-DCT-DIR-040-17. Washington, DC: Drug Enforcement Administration, 2017. [https://www.dea.gov/docs/DIR-040-17\\_2017-NDTA.pdf](https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf).
- Dzirutwe, MacDonald. “Think Bitcoin’s Getting Expensive? Try Zimbabwe.” Reuters, November 12, 2017. <https://www.reuters.com/article/us-zimbabwe-bitcoin/think-bitcoins-getting-expensive-try-zimbabwe-idUSKBN1DD0NF>.
- Ellsworth, Brian, and Ana Isabel Martinez. “Venezuela Aims for Crypto Alchemy with New ‘Petro Gold’ Token.” Reuters, February 22, 2018. <https://www.reuters.com/article/uk-crypto-currencies-venezuela/venezuela-to-launch-petro-gold-cryptocurrency-backed-by-gold-maduro-idUSKCN1G52S2>.
- Evans, David. “Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms.” Working paper, Coase-Sandor Institute for Law and Economics at Chicago Unbound, 2014. [https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=2349&context=law\\_and\\_economics](https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=2349&context=law_and_economics).
- Fanusie, Yaya. “The New Frontier in Terror Fundraising: Bitcoin.” *The Cipher Brief* (blog), August 24, 2016. [https://www.thecipherbrief.com/column\\_article/the-new-frontier-in-terror-fundraising-bitcoin](https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin).
- Fanusie, Yaya. “Terrorist Networks Eye Bitcoin as Cryptocurrency’s Price Rises.” *The Cipher Brief* (blog), December 21, 2017. <https://www.thecipherbrief.com/terrorist-networks-eye-bitcoin-cryptocurrencys-price-rises>.
- Financial Crimes Enforcement Network. *Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001. Washington, DC: Department of the Treasury, 2013. <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.
- Gupta, Sanjeev, Michael Keen, Alpa Shah, and Genevieve Verdier. *Digital Revolutions in Public Finance*. Washington, DC: International Monetary Fund, 2017.

- Harmachi, Abdur Rahim. “Bangladesh Bank Warns against Transaction in ‘Illegal’ Bitcoin, Other Cryptocurrencies.” *Bbnews24*, December 28, 2017. <https://bdnews24.com/economy/2017/12/27/bangladesh-bank-warns-against-transaction-in-illegal-bitcoin-other-cryptocurrencies>.
- He, Dong, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad et al. *Virtual Currencies and beyond: Initial Considerations*. IMF Discussion Note SDN/16/03. Washington, DC: International Monetary Fund, 2016. <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>.
- Helms, Kevin. “Central Bank of Nigeria Says ‘We Can’t Stop Bitcoin,’” *Bitcoin News* (blog), March 5, 2017. <https://news.bitcoin.com/central-bank-of-nigeria-says-we-cant-stop-bitcoin/>.
- Hendrickson, Joshua, and William Luther. “Banning Bitcoin.” *Journal of Economic Behavior & Organization* 141 (September 2017): 188–195.
- Hileman, Garrick, and Michel Rauchs. *Global Cryptocurrency Benchmarking Study*. Cambridge: University of Cambridge Centre for Alternate Finance, 2017. [https://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf](https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf).
- Hsu, Sara. “China’s Shutdown of Bitcoin Miners Isn’t Just about Electricity.” *Forbes*, January 15, 2018. <https://www.forbes.com/sites/sarahsu/2018/01/15/chinas-shutdown-of-bitcoin-miners-isnt-just-about-electricity/>.
- Huang, Alice. “Reaching within Silk Road: The Need for a New Subpoena Power That Targets Illegal Bitcoin Transactions.” *Boston College Law Review* 56, no. 5 (December 2015): 2093–2125.
- Internal Revenue Service. *IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*. Washington, DC: Internal Revenue Service, 2014. <https://www.irs.gov/newsroom/irs-virtual-currency-guidance>.
- Jackson, Olly. “Ofac’s Crypto Blacklist Could Drive Investors to Riskier Exchanges.” *International Financial Law Review*, April 6, 2018. <http://www.iflr.com/Article/3799007/%5bOPEN-ACCESS%5d-Ofacs-crypto-blacklist-could-drive-investors-to-riskier-exchanges.html>.
- Kakushadze, Zura, and Jim Kyung-Soo Liew. “CryptoRuble: From Russia with Love.” November 2, 2017. <https://arxiv.org/ftp/arxiv/papers/1801/1801.05760.pdf>.
- Koning, JP. “Fedcoin.” *Moneyness* (blog), October 19, 2014. <http://jpkoning.blogspot.com/2014/10/fedcoin.html>.

- Krygier, Rachelle. "Venezuela Launches the 'Petro,' Its Cryptocurrency." *Washington Post*, February 20, 2018. <https://www.washingtonpost.com/news/worldviews/wp/2018/02/20/venezuela-launches-the-petro-its-cryptocurrency/>.
- Kshetri, Nik, and Jeff Voas. "Do Crypto-Currencies Fuel Ransomware?" *IT Professional* 17, no. Sep/Oct 2017 (2017): 1–6.
- Lagarde, Christine. "Central Banking and Fintech—A Brave New World?" Speech at Bank of England Conference, London, September 29, 2017. <https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world>.
- Liao, Shannon. "Inside Russia's Love-Hate Relationship with Bitcoin." *The Verge*. October 31, 2017. <https://www.theverge.com/2017/10/31/16387042/russia-putin-bitcoin-regulation-ethereum-blockchain-technology>.
- Looney, Robert. "Hyperinflation Is Crippling Venezuela, but Maduro Has No Interest in Fixing It." *World Politics Review*, January 23, 2018. <https://www.worldpoliticsreview.com/articles/24035/hyperinflation-is-crippling-venezuela-but-maduro-has-no-interest-in-fixing-it>.
- Looney, Robert. "Venezuela's Economic Collapse." *Milken Institute Review*, February 28, 2018. <http://www.milkenreview.org/articles/venezuelas-economic-collapse>.
- Manheim, David, Patrick Johnson, Josh Baron, and Cynthia Dion-Schwartz. "Are Terrorists Using Cryptocurrencies?" *Foreign Affairs*, April 21, 2017. <https://www.foreignaffairs.com/articles/2017-04-21/are-terrorists-using-cryptocurrencies>.
- Marian, Omri. "A Conceptual Framework for the Regulation of Cryptocurrencies." *University Of Chicago Law Review* 82, no. 53 (2015): 55–68. <https://scholarship.law.ufl.edu/facultypub/695/>.
- Marshall, Andrew. "How China Influences Bitcoin Price, Explained." *Cointelegraph*, February 15, 2017. <https://cointelegraph.com/explained/how-china-influences-bitcoin-price-explained>.
- Mendel, William, and Peter McCabe, eds. *SOF Role in Combating Transnational Organized Crime*. MacDill Air Force Base, FL: Joint Special Operations University Press, 2016. [http://cco.ndu.edu/Portals/96/Documents/books/JSOU%20SOF/JSOU16\\_MendelMcCabe\\_CTOC\\_final.pdf](http://cco.ndu.edu/Portals/96/Documents/books/JSOU%20SOF/JSOU16_MendelMcCabe_CTOC_final.pdf).
- Moreno, Elena Christine. *Bitcoin in Argentina: Inflation, Currency Restrictions, and the Rise of Cryptocurrency*. Chicago: University of Chicago Law School, 2016. [https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1017&context=international\\_immersion\\_program\\_papers](https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1017&context=international_immersion_program_papers).

- Murphy, Edward, Maureen Murphy, and Michael Seitzinger. *Bitcoin: Questions, Answers, and Analysis of Legal Issues*. CRS Report No. R43339. Washington, DC: Congressional Research Service, 2015. <https://fas.org/sgp/crs/misc/R43339.pdf>.
- Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." White paper, Bitcoin, 2008. <https://bitcoin.org/bitcoin.pdf>.
- Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ: Princeton University Press, 2016.
- Noack, Rick. "Cryptocurrency Mining in Iceland Is Using So Much Energy, the Electricity May Run Out." *Washington Post*, February 13, 2018. <https://www.washingtonpost.com/news/worldviews/wp/2018/02/13/cryptocurrency-mining-in-iceland-is-using-so-much-energy-the-electricity-may-run-out/>.
- Oyamada, Aline, and Camila Russo. "Bitcoin Trading Thrives Wherever Regulators Crack Down Most." Bloomberg News, December 14, 2017. <https://www.bloomberg.com/news/articles/2017-12-14/bitcoin-trading-thrives-wherever-regulators-crack-down-most>.
- PanAm Post* (blog). "Ecuador Bans Bitcoin, Initiates Government-Run Digital Currency." Last updated July 25, 2014. <https://panampost.com/panam-staff/2014/07/25/ecuador-bans-bitcoin-initiates-government-run-digital-currency/>.
- Parker, Emily. "Even China Can't Destroy Bitcoin." *MIT Technology Review*, December 11, 2017. <https://www.technologyreview.com/s/609320/can-china-contain-bitcoin/>.
- Piazza, Fiammetta. "Bitcoin in the Dark Web: A Shadow over Banking Secrecy and a Call for Global Response." *Southern California Interdisciplinary Law Journal* 26, no. 3 (2017): 521–546.
- Picardo, Elvis. "Capital Flight." Investopedia, January 5, 2004. <https://www.investopedia.com/terms/c/capitalflight.asp>.
- Plassaras, Nicholas. "Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF." *Chicago Journal of International Law* 14, no. 1, Article 12 (2013): 377–407.

- Ponsford, Matthew P. "A Comparative Analysis of Bitcoin and Other Decentralized Virtual Currencies: Legal Regulation in the People's Republic of China, Canada, and the United States." *Jolt Digest* (blog), November 2015. <http://jolt.law.harvard.edu/digest/a-comparative-analysis-of-bitcoin-and-other-decentralized-virtual-currencies-legal-regulation-in-the-peoples-republic-of-china-canada-and-the-united-states>.
- Prasad, Eswar. *Central Banking in a Digital Age: Stock-Taking and Preliminary Thoughts*. Washington, DC: Hutchins Center on Fiscal and Monetary Policy at Brookings, 2018. <https://www.brookings.edu/research/how-will-fintech-and-digital-currencies-transform-central-banking>.
- Radcliffe, Brent. "Fiat Money." Investopedia, November 20, 2003. <https://www.investopedia.com/terms/f/fiatmoney.asp>.
- Roberts, Jeff, and Nicolas Rapp. "Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says." *Fortune*, November 25, 2017. <http://fortune.com/2017/11/25/lost-bitcoins/>.
- Reuters. "China Central Bank Will Launch Crackdown on Virtual Currencies." March 29, 2018. <https://www.reuters.com/article/us-china-finance-digital-currency/china-central-bank-will-launch-crackdown-on-virtual-currencies-idUSKBN1H515L>.
- Sanders, Lewis. "Bitcoin: Islamic State's Online Currency Venture." DW. September 20, 2015. <http://www.dw.com/en/bitcoin-islamic-states-online-currency-venture/a-18724856>.
- Shuster, Simon. "Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions." *Time*, March 20, 2018. <http://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/?iid=sr-link1>.
- Stecklow, Steve, Alexandra Harney, Anna Irrera, and Jemima Kelly. "Chaos and Hackers Stalk Investors on Cryptocurrency Exchanges." Reuters, September 29, 2017. <http://www.reuters.com/investigates/special-report/bitcoin-exchanges-risks/>.
- Szubin, Adam. *National Terrorist Financing Risk Assessment*. Washington, DC: Department of the Treasury, 2015. <https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%932006-12-2015.pdf>.
- Tatar, Jack. "Iceland—Time to Free Bitcoin!" The Balance. Last updated March 17, 2017. <https://www.thebalance.com/iceland-time-to-free-bitcoin-4030896>.
- Telley, Chris. "A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency." *Small Wars Journal*, January 15, 2018. <http://smallwarsjournal.com/jrnl/art/a-coin-for-the-tsar-the-two-disruptive-sides-of-cryptocurrency>.

- Trautman, Lawrence. "Virtual Currencies Bitcoin and What Nowafter Liberty Reserve, Silk Road, and Mt. Gox?" *Richmond Journal of Law & Technology* 20, no. 4 (2014): 1–73.
- Tucker, Patrick. "Russia, N. Korea Eye Bitcoin for Money Laundering, Putting It on a Crash Course with Regulators." *Defense One*. December 15, 2017. <http://www.defenseone.com/technology/2017/12/russia-n-korea-eye-bitcoin-money-laundering-putting-it-crash-course-regulators/144598/>.
- Turpin, Jonathan. "Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework." *Indiana Journal of Global Legal Studies* 21, no. 1 (2014): 335–368.
- U.S. Commodity Futures Trading Commission. *CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets*. Washington, DC: U.S. Commodity Futures Trading Commission, 2018. [https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder\\_virtualcurrency01.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/%40customerprotection/documents/file/backgrounder_virtualcurrency01.pdf).
- van Wirdum, Aaron. "Bolivian Authorities Arrest 60 'Cryptocurrency Promoters.'" *Bitcoin Magazine*, May 29, 2017. <https://bitcoinmagazine.com/articles/bolivian-authorities-arrest-60-cryptocurrency-promoters/>.
- Veloz, Alexandra. "Ban Fails to Halt Bitcoin in Ecuador." *Antigua Report* (blog), May 24, 2017. <http://antiguareport.com/2017/05/ban-fails-to-halt-bitcoin-in-ecuador/>.
- Vigna, Paul, and Michael Casey. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging The Global Economic Order*. New York: St. Martin's Press, 2015.
- White, Lawrence H. "The World's First Central Bank Electronic Money Has Come—and Gone: Ecuador, 2014–2018." *Cato at Liberty* (blog), April 2, 2018. <https://www.cato.org/blog/worlds-first-central-bank-electronic-money-has-come-gone-ecuador-2014-2018>.
- Worstell, Tim. "Congratulations to Venezuela—Bitcoin Miners Arrested for Stealing Free Electricity." *Forbes*, January 27, 2017. <https://www.forbes.com/sites/timworstell/2017/01/27/congratulations-to-venezuela-bitcoin-miners-arrested-for-stealing-free-electricity/>.
- Wroughton, Lesley, and David Alexander. "U.S. Bans Transactions with Venezuela's Digital Currency." *Reuters*, March 20, 2018. <https://www.reuters.com/article/uk-crypto-currencies-venezuela-usa/u-s-blocks-use-of-venezuelas-digital-currency-white-house-idUSKBN1GV2AX>.
- Zenk, Micah. "Bitcoin for Bombs." *Council on Foreign Relations* (blog), August 17, 2017. <https://www.cfr.org/blog/bitcoin-bombs>.



Zhu, Grace. "China Central Bank Warns Banks on Bitcoin." *Wall Street Journal*, May 7, 2014. <https://www.wsj.com/articles/china-central-bank-warns-banks-on-bitcoin-1399454876>.

Zuckerman, Molly Jane. "80% of All Bitcoins Already Mined, Only 4.2 Million Coins Left until Supply Cap." *Cointelegraph*, January 15, 2017. <https://cointelegraph.com/news/80-of-all-bitcoins-already-mined-only-42-million-coins-left-until-supply-cap>.

THIS PAGE INTENTIONALLY LEFT BLANK

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California