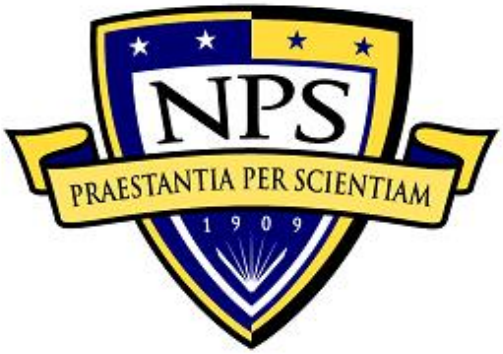
2018-12

A BIT OF RECENT GROWTH: THE EVOLVING RISK OF TERRORIST USE OF VIRTUAL CURRENCY

Ditamore, Stephen

Monterey, CA; Naval Postgraduate School



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A BIT OF RECENT GROWTH: THE EVOLVING RISK OF TERRORIST USE OF VIRTUAL CURRENCY

by

Stephen Ditamore

December 2018

Co-Advisors: Carolyn C. Halladay
Shannon A. Brown

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE A BIT OF RECENT GROWTH: THE EVOLVING RISK OF TERRORIST USE OF VIRTUAL CURRENCY	**5. FUNDING NUMBERS**
6. AUTHOR(S) Stephen Ditamore	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES 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.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The use of decentralized virtual currencies (DVCs) by terrorist organizations (TOs) on a significant scale could present unique challenges for regulators, policy makers, and law enforcement because they offer the potential for an illicit funding network that can be very difficult to disrupt or even detect. However, the body of existing research regarding the threat of terrorists' use of DVCs has determined that though it has become the payment method of choice for cybercriminals and many transnational criminal organizations, researchers do not believe that TOs will leverage DVCs on an appreciable scale in the near future. To justify their determinations, prior researchers cite insufficient market size, anonymity, and broad commercial acceptance, coupled with a perceived lack of TOs' technological sophistication, as limits to the practical use of DVCs over other better-established and less complicated terror funding methods. They further suggest that existing AML/CFT regulations, narrowly applied to DVC exchanges should be sufficient to catch terror financiers. However, this thesis identifies recent developments in DVCs and the ecosystems that support them that suggest all of the primary pillars on which prior research has been built may have eroded sufficiently to warrant further investigation into the potential threat posed by terrorist use of DVCs. The homeland security enterprise must not be lulled into complacency by what this thesis finds to be already outdated research.

14. SUBJECT TERMS virtual currency, cryptocurrency, cross-border payment systems, money laundering, terror finance, terrorism financing, financial technology, fintech, AML/CFT, bitcoin	**15. NUMBER OF PAGES** 77
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A BIT OF RECENT GROWTH: THE EVOLVING RISK OF TERRORIST USE OF VIRTUAL CURRENCY

Stephen Ditamore
Lieutenant, United States Navy
BS, Embry-Riddle Aeronautical University, 2015

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
December 2018**

Approved by: Carolyn C. Halladay
Co-Advisor

Shannon A. Brown
Co-Advisor

Afshon P. Ostovar
Associate Chair for Research
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The use of decentralized virtual currencies (DVCs) by terrorist organizations (TOs) on a significant scale could present unique challenges for regulators, policy makers, and law enforcement because they offer the potential for an illicit funding network that can be very difficult to disrupt or even detect. However, the body of existing research regarding the threat of terrorists' use of DVCs has determined that though it has become the payment method of choice for cybercriminals and many transnational criminal organizations, researchers do not believe that TOs will leverage DVCs on an appreciable scale in the near future. To justify their determinations, prior researchers cite insufficient market size, anonymity, and broad commercial acceptance, coupled with a perceived lack of TOs' technological sophistication, as limits to the practical use of DVCs over other better-established and less complicated terror funding methods. They further suggest that existing AML/CFT regulations, narrowly applied to DVC exchanges should be sufficient to catch terror financiers. However, this thesis identifies recent developments in DVCs and the ecosystems that support them that suggest all of the primary pillars on which prior research has been built may have eroded sufficiently to warrant further investigation into the potential threat posed by terrorist use of DVCs. The homeland security enterprise must not be lulled into complacency by what this thesis finds to be already outdated research.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AML	Anti-money laundering
BSA	Bank Secrecy Act
CFT	countering the financing of terrorism
DHS	Department of Homeland Security
DVC	decentralized virtual currency
DWM	dark web market
FATF	Financial Action Task Force
FI	financial institution
FinCEN	Financial Crimes Enforcement Network
Fintech	financial technology
HSC	Homeland Security Committee
HSSAI	Homeland Security Studies and Analysis Institute
IMF	International Monetary Fund
IP	Internet protocol
ISIS	Islamic State in Iraq and Syria
KYC	know your customer
Market cap	market capitalization
MSB	money services business
MVTS	money value transfer systems
NPPS	new payment products and services
P2P	peer-to-peer
RBA	risk-based assessment
RUSI	Royal United Services Institute
SEC	Securities and Exchange Commission
TCO	transnational criminal organization
TO	terrorist organization

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

To my wife, Mary Beth, and my son, Jack: I never could have endured this process without your constant love and support, and I'll never be able to thank you both enough for the sacrifices you made while I hid myself away to work for the duration of the time we lived in sunny California. I promised you both we would see and explore the West Coast to the fullest while we were here, and I hope you both enjoyed the scenic one block radius around our home.

Very sincere and special thanks to my co-advisors, Dr. Carolyn Halladay, and Dr. Shannon Brown, as well as to Chloe Woida at the Graduate Writing Center:

Dr. Halladay, your wisdom, humor, and unwillingness to have me thrown out of your classes for wielding my own brand of humor, were more than admirable, and I deeply appreciate you helping me stay focused on eating the elephant long after my appetite was spent.

Dr. Brown, I most appreciated your ability to recognize when I needed sufficient coddling to keep any number of veins from bulging right out of my forehead when my "superior writing abilities" would frequently falter and leave me staring at a blinking cursor for hours. Additionally, your willingness to subsist almost entirely on Starbucks' nutritional offerings on numerous occasions for my benefit did not go unnoticed.

Chloe, not only do I owe you many thanks for thoughtfully shepherding me from start to finish through a process I found entirely uncomfortable and alien, but also for taking the time to "try" to keep me focused and on task while I did my best to distract us both from any real work. Squirrel! Truly, your ability to balance real productivity with listening and laughing at my many complaints and rants helped keep me sane throughout my time at NPS. I appreciate your hard work.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Security analysts have assessed the threat posed by the potential use of de-centralized virtual currencies (DVCs), like Bitcoin (the oldest and most well-known DVC), by terrorist organizations (TOs) to be very low.[1] These recent assessments have been based in large part on four key assumptions about DVCs: limited market size, narrow range of mainstream acceptance, a lack of sufficient anonymity, and the presumed limits of terrorists' technological sophistication. But, in late 2017, DVCs experienced an exponential rise in market value, rapid growth in mainstream commercial acceptance, and tremendous investment devoted to new anonymizing technologies. Considering these recent developments, there is value in asking two questions: Will recent market growth, more mainstream acceptance, and advancements in anonymizing technologies make DVCs more attractive for use in financing terrorism; and how should regulators and law enforcement agencies respond to these developments, assuming that DVCs will, in fact, be adopted by criminal organizations and terrorists who seek to avoid financial surveillance by regulatory and law enforcement authorities?

A. SIGNIFICANCE OF THE RESEARCH QUESTION

A primary focus of U.S. counterterrorism strategy is detecting and disrupting the financing of terrorism.[2] Terror financing relies on numerous means to move money around the globe, including the traditional banking sector, informal cash courier systems like hawala networks, money services businesses (MSB) such as PayPal or Western Union, as well as new payment products and services (NPPS), including DVCs, that are part of a technologically-enabled "shadow banking" sector that poses a direct challenge to

[1] Zachary K. Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat" (Washington, DC: Center for a New American Security, May 2017), https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies; David Carlisle, "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic," Royal United Services Institute, www.rusi.org, March 2017, https://rusi.org/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic.

[2] Bennett Seftel, "Hawala Networks: The Paperless Trail of Terrorist Transactions," Cipher Brief website, www.thecipherbrief.com, March 16, 2016, https://www.thecipherbrief.com/article/middle-east/hawala-networks-the-paperless-trail-of-terrorist-transactions.

conventional financial institutions' business practices.[3] Though government institutions have developed a number of tools to combat terror financing, all of which are based on enhancing transparency within financial systems, any means of rapidly and anonymously moving large sums of money while simultaneously masking the identity and ownership interest of the parties involved is bound to catch the interest of TOs.[4] Indeed, DVCs and their supporting technologies promise low-cost, high-speed, secure, and anonymous financial transactions to anyone who can use a computer or smartphone. Coupled with the global, cross-border reach of DVCs' decentralized design, this same promise may make DVCs an attractive choice to TOs—increasingly even to those with little or no demonstrated technological savvy.

The use of DVCs by TOs on a scale that competes with cash, hawala transfers, or other readily available means of financing could present unique challenges for regulators, policy makers, and law enforcement because it offers the potential for an illicit funding network that can be very difficult to disrupt or even detect. However, the body of existing research regarding the threat of terrorists' use of DVCs all basically agrees that though virtual currencies are emerging as a payment method of choice for cybercriminals and such transnational criminal organizations (TCOs) as drug cartels, international smuggling rings, and organized crime syndicates, there is no evidence that TOs are leveraging DVCs on an appreciable scale, nor will they anytime in the near future.

This prior research suggests that insufficient market size, anonymity, and broad commercial acceptance, coupled with a perceived lack of TOs' technological sophistication, limits the practical use of DVC technology over other more well-established and less complicated terror funding methods. Furthermore, it suggests that existing anti-money laundering and countering the financing of terrorism (AML/CFT) regulations, narrowly applied to DVC exchanges (where users of DVCs "cash out" and convert their virtual currency into hard currency), should be sufficient to catch terror financiers.

[3] Ellie Maruyama and Kelsey Hallahan, "Following the Money: A Primer on Terrorist Financing" (Washington, DC: Center for a New American Security, June 2017), https://www.cnas.org/publications/reports/following-the-money-1.

[4] Maruyama and Hallahan.

However, considering recent developments in DVCs and the markets that support them, the pillars on which prior research has been built may have eroded sufficiently to warrant the United States and its allies taking another look at the potential threat.

This thesis builds on existing research on terror finance by highlighting recent technological developments in DVCs, how these developments might enhance the capabilities of terrorist organizations, and how states are responding to the advent of DVCs through regulation and enforcement policies (some of which may be in the earliest stages of development). The thesis also explores how recent broad acceptance, skyrocketing value, and rapidly evolving technology in support of existing and developing DVCs increases the likelihood that this technology will be used for money laundering, financing terrorism, and evading sanctions. Though only anecdotal evidence exists of recent attempted terrorist use of DVCs, the ongoing efforts by governments and financial institutions to address the possibility serves as significant evidence of their acknowledgement of the threat. Additionally, the possibility should not be ignored that TOs may now be more effectively leveraging dark web markets (DWMs) and utilizing anonymizing and obfuscating technology to more successfully evade detection. While this assertion may be difficult to prove, there is value in exploring the regulatory and enforcement steps that are being taken by governments and institutions—expressed in the form of policies, white papers, and international agreements—and understanding these measures as an effort to harness an otherwise unregulated field of financial activity, while simultaneously creating frameworks and mechanisms that disrupt the ability of criminal and terrorist actors to exploit rapidly-evolving financial technology (fintech), of which DVCs are an example.[5]

[5] The IMF provides a loose definition of what is often called "fintech," when Dong He et al. describes "A new wave of technological innovations…accelerating change in the financial sector. Fintech leverages the explosion of big data on individuals and firms, advances in artificial intelligence, computing power, cryptography, and the reach of the Internet. The strong complementarities among these technologies are giving rise to an impressive array of new applications touching on services from payments to financing, asset management, insurance, and advice. The possibility now looms that entities driven by fintech may emerge as competitive alternatives to traditional financial intermediaries, markets, and infrastructures." Dong He et al., "Fintech and Financial Services: Initial Considerations," Staff Discussion Notes (Washington, DC: International Monetary Fund, June 2017), 7, http://www.imf.org/en/Publications/SPROLLs/Staff-Discussion-Notes.

B. LITERATURE REVIEW

This literature review highlights some of the recent assessments of the risk DVCs pose as an instrument of terror financing and describes the assumptions that underpin those judgments.

1. High Threat Assessments

A number of authors have identified DVCs as a near-term, if not immediate, challenge for the homeland security enterprise charged with tracking questionable financial transactions. Jared Kleiman authored one of the earliest peer-reviewed papers about the threat of DVCs to national security in which he raises "Concerns about the government's ability to detect terrorist group financing."[6] He specifies the ability to conduct anonymous financial transactions as a serious hindrance to detecting illicit financing, and cites a 2012 case where Iranians traded DVC for normally unobtainable U.S. dollars and then held them in accounts outside of the country to avoid sanctions.[7] Ultimately, Kleiman assessed that governments should be "taking the threat of untraceable online transactions seriously, finding that DVCs may be used as a discrete method for financing terror groups."[8]

In the same year as Kleiman's assessment, the core findings of a Department of Homeland Security (DHS)—Homeland Security Studies and Analysis Institute (HSSAI) report on the *Risks and Threats of Cryptocurrencies* noted that DVCs "may in time represent a revolution in money laundering,"[9] but the report concludes that, due to the relatively small size of the DVC market, cash will likely continue to pose the greatest AML/CFT challenge for the foreseeable future. The report acknowledges, however, that TOs are quickly adapting to technology and increasing the sophistication of their financing methods, and further acknowledges that the use of DVCs by TOs would certainly increase if the popularity and mainstream acceptance of DVCs increased.

---

[6] Jared A. Kleiman, "Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger U.S. National Security and Welfare," *National Security Law Brief* 4, no. 1 (2013): 74.

[7] Kleiman, 74–75.

[8] Kleiman, 75.

[9] HSSAI, "Risks and Threats of Cryptocurrencies" (Falls Church, VA: Homeland Security Studies and Analysis Institute, December 31, 2014), 23.

In a 2016 issue of the *Journal of Money Laundering Control*, Irwin and Milad note that parties supporting the Islamic State in Iraq and Syria (ISIS) and other TOs had "posted YouTube videos, discussion forum links and links to research on the anonymity provided by Bitcoins"[10] to raise money for terror related activities. As an example, the authors refer to an article posted on-line in 2014 by an ISIS supporter that specifically instructs jihadist sympathizers how to utilize Bitcoin and third-party anonymizing software to fund jihadists, as well as how to access hidden DWMs to buy goods and services to benefit TOs. Additionally, the authors cite unverified reports by a reputable financial security firm, who in 2015 claims to have tracked millions of dollars of transfers and transactions in DVCs to numerous wallets they believed to be owned by ISIS.[11]

Irwin and Milad go further than reporting on just transactions and instructional material found online. They state that "there is evidence to suggest that Bitcoins have been utilized in a number of successful terror attacks,"[12] including the coordinated November 2015 attacks in France, to illustrate that DVCs are not just a future AML/CFT threat, but that cryptocurrencies are already in use by TOs. While they ultimately conclude that the scale of use is likely small compared to other funding methods, they assert the more important point is that these cases verify that TOs are actively "trying to understand new and evolving technologies" and that "it is likely that use of these mediums will only increase in the future."[13]

2. Low Threat Assessments

Following these early assessments, a recurring theme has emerged more recently from academic and professional discussions in 2016 and 2017 that DVCs should be acknowledged as a *potential* money laundering, terrorist financing, and sanctions-evasion threat, but that there is little reason to believe that DVCs will be used on a large scale; it is

[10] A.S.M. Irwin and G. Milad, "The Use of Crypto-Currencies in Funding Violent Jihad," *Journal of Money Laundering Control* 19, no. 4 (2016): 410.

[11] Irwin and Milad, 410.

[12] Irwin and Milad, 410.

[13] Irwin and Milad, 411.

more likely that regulators and law enforcement officials will note anecdotal, small-scale uses in the near future. One such assessment by Dong He et al. at the International Monetary Fund (IMF), notes that existing AML/CFT measures applied to DVC exchanges should be effective deterrents, considering TOs need to convert DVCs into fiat currency before they can use it.[14] However, this report goes on to say that "If the use of VCs becomes so widespread that there is no longer a need for participants to 'cash out' (that is, convert the DVCs into fiat currency), it may be necessary to extend regulation to other VC network participants…that operate entirely *within* the system."[15] Dong He and the IMF re-deliver nearly the same assessment, including a near identical caveat regarding the risk of more widespread use, in a June 2017 report on fintech and financial services.[16] These reports allude to the idea that an increased AML/CFT threat could arise if DVCs were to gain sufficient popularity to spawn a parallel economy that exists outside the purview of current regulatory authority.

David Carlisle of the Royal United Services Institute (RUSI) in the UK, published an assessment of DVCs and financial crime in March of 2017, where he states, "terrorist financing with VCs is best regarded as an emerging and potential risk, rather than a crystalised one."[17] He alludes to TOs' lack of technological abilities or possibly a lack of infrastructure when he says that TOs "may find VCs technically and practically difficult to use,"[18] and goes further to assert that they already have a number of other more established channels of finance and so likely have little need for DVCs.

Just a few paragraphs later, however, Carlisle cites a 2015 example of a U.S. teenager who was given jail time for "using Twitter to describe how to use Bitcoin to

---

[14] Dong He et al., "Virtual Currencies and Beyond: Initial Considerations," Staff Discussion Notes (Washington, DC: International Monetary Fund, January 2016), 27, http://www.imf.org/en/Publications/SPROLLs/Staff-Discussion-Notes?page=1.

[15] He et al., 27.

[16] He et al., "Fintech and Financial Services: Initial Considerations," 16.

[17] David Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities" (London: Royal United Services Institute, March 2017), 17, https://rusi.org/publication/occasional-papers/virtual-currencies-and-financial-crime-challenges-and-opportunities.

[18] Carlisle, 17.

support Daesh."[19] He further reports that a Daesh operative in Indonesia, alleged to have plotted a 2016 attack in Jakarta, used DVC to transact with other jihadis.[20] While Carlisle ultimately dismisses TOs' use of DVCs as anecdotal, he concedes that some experts believe that TOs "are becoming rapidly more technologically adept; as this trend continues, VCs could become an increasingly viable financing tool for terrorists."[21] Carlisle provided additional commentary about the subject on the RUSI website, where he reiterated that while many of the characteristics of DVCs may seem very appealing to ISIS and other TOs, "the threat landscape presents a more muted picture."[22] The title of the web article itself conveys RUSI and Carlisle's overall message on the subject: *Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic*.

Zachary Goldman et al., of the Center for a New American Security, provide one of the most recent studies, from May 2017, that builds on the same primary arguments presented in the years prior: DVCs are not yet as anonymous as cash and other more established methods of illicit finance; TOs lack technical sophistication or a broad peer-to-peer network of trust; and "Terrorists mostly need fiat currency to fulfill their funding requirements, so there is no reason to introduce the complications involved in using virtual currencies."[23] Additionally, Goldman et al. indicate that DVCs lack the market size and liquidity needed to be useful to TOs at scale. They specifically note that as of March 20, 2017, the market cap of the oldest and most widely known DVC, Bitcoin, was roughly $17 billion, while the market cap of newer, more anonymous DVCs such as Monero and ZCash were $340 million and $22 million, respectively.[24] Goldman et al. contrast these figures to the U.S. government's estimate that "illicit financing generates $300 billion per year,"[25]

[19] Carlisle, 18.

[20] Carlisle, 18.

[21] Carlisle, 18.

[22] Carlisle, "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic."

[23] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat," 26.

[24] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat."

[25] Goldman et al., 18.

alluding to the idea that DVCs lack sufficient scale and liquidity for terrorists use even in the unlikely event they may attempt to do so.

This brief review of the existing literature on the broad subject of DVCs and terror financing demonstrates that observers of this security challenge fall into one of two categories: those who see a near-term threat posed by a technology that is becoming more widely-accepted by the public, and those who see the possibility of risk in the future but note that there is no clear evidence that TOs will adopt the technology to support their operations when other less sophisticated (or more established) means of money transfer exist. This thesis explores both positions and identifies steps that regulatory and law enforcement authorities are taking to address the challenge presented by recent developments surrounding DVCs, since regardless of whether the threat is near-term or long-term, an argument can be made that if efforts to police DVCs are actively being developed by policy makers, then the risk is real.

C. RESEARCH DESIGN AND SOURCES

The research for this thesis involved a comprehensive analysis of the foundations upon which recent scholarly works built their modest assessments of the threat posed by DVCs to terror finance. These foundational arguments were evaluated using more recent information derived from numerous sources, including government data, academic publications, and open-source reports on the utility and deployment of DVCs. Subject-matter expert opinions and pre-existing interviews from officials at the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), the Securities and Exchange Commission (SEC), and developers of DVC related fintech were utilized whenever possible.

Data derived from government reports and estimates were used to establish a baseline for the amount of money TOs would need to operate annually, while open source data on the overall DVC market size and liquidity are used to determine if sufficient supply could be achieved to meet TO demand. These reports expound upon the U.S. financial system's regulatory framework, illustrating how the United States is attempting to respond to the challenges posed by DVCs, and illustrate why TOs might seek out weaker regulatory

environments to use DVCs with little fear of surveillance or confiscation by counter-terrorism authorities.

Academic publications on the subject of DVCs, and other open-source materials (trade and technical publications) established the growth trend of DVCs' mainstream acceptance around the world. However, any discussion of the growth of DVCs' adoption within DWM on the unindexed Internet and illicit communities relies almost entirely on news articles, and forum and blog posts due to a lack of access to the dark web.

Government reports, scholarly articles, white papers, and open source news reports provided information about the mechanisms that have been developed recently to address known vulnerabilities in older, more widely used pseudonymous DVCs. Government reports and some scholarly articles were also utilized for information on third party anonymizing web tools designed to further complicate and obfuscate DVC transactions.

This thesis relies on published primary sources including transcripts from congressional hearings, government agency reports, and industry publications; and published secondary sources such as peer-reviewed sources, open source material from news agencies and DVC industry stakeholders, and online DVC user sources (blog posts and discussion forums). Relevant AML/CFT laws and regulations, including the Bank Secrecy Act (BSA) and Title III of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USAPATRIOT) Act, are explored to the level of detail necessary to understand how DVC use and development is currently addressed by existing policy, and transcripts of supporting interviews with subject matter experts at federal law enforcement agencies are cited where appropriate.

The technology explored in this thesis is evolving rapidly, as is the response of governments to the uses and abuses of fintech. Every effort has been made to find and use the most credible and relevant information available; using primary and secondary sources in accordance with appropriate research protocols. The author did not have access to the so-called "dark web," or conduct anthropological research by attempting to contact actors who are working to hide their activities from the general public and law-enforcement officials.

Every attempt has been made to present broad-based and comprehensive information from the literature referenced for this thesis, however, new DVCs are being developed and marketed almost daily, making it difficult or impossible to assess DVCs as a group with accuracy or precision. The information used, and sources cited are as current as possible and deemed valid at the time of writing.

D. THESIS OVERVIEW AND CHAPTER OUTLINE

The first chapter of this thesis presents the primary research question and its importance to the homeland security enterprise, as well as the literature review and chapter outline. The second chapter provides background information regarding DVCs consisting of three primers on subjects necessary to understand the core matter of this thesis: contemporary terrorism finance, a fundamental explanation of what DVCs are, including the basics of how a virtual currency typically functions, and finally, a review of the current regulations and policies that have evolved to encompass DVCs. These sections are not meant to be an in-depth technical analysis, but rather practical explanations sufficient for the reader to understand how the nexus of the three are relevant. Additionally, this chapter expounds on the known traditionally utilized methods of terror finance and summarizes the reasons why prior research has determined that TOs are likely to continue these methods rather than engage in the use of DVCs on any meaningful scale. This context is important because "traditional" terror finance has been extensively studied by law enforcement and financial regulatory authorities, and DVCs represent a challenge to well-established mechanisms employed by governments around the world to surveille and interdict TO financial activities.

It is the goal of this thesis to determine whether recent developments in and around DVCs may be cause for a renewed investigation into the threat potential for TOs to use DVCs at scale. To accomplish this goal, Chapter III examines recent developments in scale of use and growth in value of DVCs, while Chapter IV deals exclusively with technological developments of newer DVCs, third-party fintech, and TO sophistication. These chapters focus on their respective changes in market developments and technological innovations that could affect, and potentially weaken, the four primary arguments on which the prior

research relied. Additionally, chapters III and IV examine how their respective developments could undermine the abilities of regulators and law enforcement to detect any increased use of DVCs, possibly increasing their potential to be exploited by TOs.

Building on any potential weaknesses in regulatory and enforcement mechanisms that may be exacerbated by the developments explored in chapters III and IV, Chapter V, the final chapter of the thesis, presents findings and conclusions based on the evidence presented in the prior chapters. The homeland security enterprise already focuses a great deal of counterterrorism manpower and resources to stemming the flow of terror finance. However, TOs are quickly adapting and flexing to meet their financial needs as governments and institutions aggressively make the traditional financial system more difficult for them to access. As we succeed in applying pressure to that end, it is of paramount importance to the homeland security enterprise, and to the people of the United States, that as innovation and technology open new possible avenues for alternate terror financing methods, that our policy makers stay up to date on the threats posed by these innovations and understand them in lock-step with those who would wish to support or perpetrate an agenda of terror.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND: VIRTUAL CURRENCY, CONTEMPORARY TERROR FINANCE, AND THE REGULATIONS DESIGNED TO KEEP THEM SEPARATE

A. INTRODUCTION

This chapter provides relevant background on three interrelated subjects that are at the core of this thesis: the design features of virtual currencies that may make them attractive to TOs; contemporary terror finance (how terror networks leverage the existing global financial system to move and convert currency without surveillance by state authorities); and U.S. financial regulations that aim to reduce the risk of a nexus forming between TOs and DVCs. The three sections of this chapter provide a context for understanding the mechanisms of terror finance and how TOs might find DVCs a useful alternative to conventional financial transactions, subject to the regulations that are described in this chapter. Virtual currencies are not a new invention, and financial regulators have been grappling with how best to address the evolving challenge of this technology, which has proliferated in the recent years. A survey of existing policies and laws make it clear that state authorities that have responsibility for oversight and enforcement of the financial sector are only now coming to realize the challenge posed by DVCs, and that additional regulation—underpinned by technical capabilities—will be necessary in the future.

B. THE DESIGN FEATURES OF DIGITAL VIRTUAL CURRENCIES

According to the Financial Action Task Force (FATF),[26] "Virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal

[26] FATF is regarded as the global leader in addressing AML/CFT issues, and the U.S. Department of the Treasury's FinCEN broadly utilizes FATF's guidance. As such, this thesis will attempt to adhere as closely as possible to key definitions and vocabulary used throughout both entities' publications with the intent of providing some common language to help better understand how DVCs operate.

tender status."[27] Virtual currency does not count as legal tender, which is likely the most important distinction from real currency, or *fiat currency*, which FATF defines as, "the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country."[28] Fiat currency also includes digital representations of legal tender, sometimes referred to as *e-money*, which may be used in electronic transfers.[29] Within the financial sector both e-money and virtual currency commonly fall under the broader category of *digital currency*; however, to prevent confusion, this thesis will not refer to e-money or digital currency and will only differentiate between fiat and virtual currency.

Virtual currencies may be considered either convertible or non-convertible. FATF notes: "Convertible virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency,"[30] whereas non-convertible virtual currency "is intended to be specific to a particular virtual domain or world,"[31] such as the rewards points offered by commercial retailers or as may be used within online role-playing games. Lacking broad use in the global economy, TOs would likely find little or no utility in non-convertible virtual currency, consequently, this thesis will focus solely on the convertible varieties.[32]

Convertible virtual currency can finally be further divided into either centralized or de-centralized versions. Centralized virtual currencies rely on a single, controlling, administrative authority as a trusted third party that establishes the rules of a currency's

---

[27] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (Paris: FATF, June 2014), 4, http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html.

[28] FATF, 4.

[29] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks."

[30] FATF, 4.

[31] FATF, 4.

[32] "It should be noted that even where, under the terms set by the administrator, a non-convertible currency is officially transferrable only within a specific virtual environment and is not convertible, it is possible that an unofficial, secondary black market may arise that provides an opportunity to exchange the 'non-convertible' virtual currency for fiat currency or another virtual currency. Development of a robust secondary black market in a particular 'non-convertible' virtual currency may, as a practical matter, effectively transform it into a convertible virtual currency. A non-convertible characterisation is thus not necessarily static." FATF, 5.

use, maintains a single master ledger of transactions and accounts, and retains the authority to introduce or withdraw a currency from circulation.[33] Examples of centralized virtual currencies include Second Life Linden Dollars, World of Warcraft Gold, airline frequent flyer miles, and numerous retail store reward points. Prior to some of the first regulatory efforts encompassing virtual currencies in 2013, the level of control they offered made centralized virtual currencies prone to money laundering and terror finance activity, as was the case with the examples of both Liberty Reserve and e-gold Ltd.[34] However, it was the very existence of a central administrator, subject to the responsibility of ensuring compliance with AML/CFT regulation, that made these high-profile illicit-use cases relatively easy to pursue once regulatory or law enforcement authorities detected activity that met the threshold for an investigation. Consequently, centralized virtual currencies have become much less attractive to illicit actors compared to their de-centralized counterparts. Thus, this thesis focuses on the potential for TOs to exploit de-centralized virtual currency.

DVCs, unlike virtual currencies that make use of a central ledger and an administrator, utilize a framework of math-based internal protocols that rely on cryptography and a system majority consensus for transaction validation.[35] These systems are entirely decentralized: no single party maintains a ledger of transactions, and encrypted data is transmitted to populate decentralized ledgers housed on computers around the world. This reliance on cryptography is why DVCs are often referred to as *cryptocurrency* and is also what permits computational efforts by a broad and diffuse group of participants, known commonly as *miners*, to perform all necessary transaction validations.[36] These miners earn newly created units of DVCs as a reward for their work to verify and record transactions onto the system's publicly viewable distributed ledger.

---

[33] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat."

[34] In-depth explanations of enforcement actions against now defunct virtual currency administrators e-gold Ltd. and Liberty Reserve are well-documented in sections III. and VI. B. in: Stephen T. Middlebrook and Sarah Jane Hughes, "Regulating Cryptocurrencies in the United States: Current Issues and Future Directions," *William Mitchell Law Review* 40, no. 2 (2014): 813–48.

[35] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks."

[36] He et al., "Virtual Currencies and Beyond: Initial Considerations."

This distributed ledger, often referred to as a *blockchain*, is a publicly shared record of all the transactions that have ever occurred within a given DVC system. Once cryptographically signed, new transactions are aggregated by system protocols into blocks to be validated by miners before being added to a timestamped chain of previously existing blocks.[37] Identical copies of the blockchain are stored and shared on a peer-to-peer network of all computers that choose to run the publicly available software for a specific DVC.[38] Therefore, irreversible transactional security is ensured by majority consensus because, according to those who study blockchain technology like Alex Wilner, "any attempt to tamper with the blockchain would require the alteration of every block previously created, a near-impossibility given the decentralized nature of the technology."[39]

Publicly viewable DVC system addresses, which serve as account numbers, do not require names or any other type of identification to be attached to them to function in the system. Because, according to FATF, DVC protocols do "not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity,"[40] and with no central authority to monitor transactions and engage in AML/CFT reporting, DVC related investigations and asset seizure can become complicated for law enforcement.[41] However, even though users' identities may not be directly associated with their address(es), a complete and accurate history of all transactions associated with any and all addresses in the system are kept in public view on the blockchain.[42] These two competing features result in transactions with more anonymity than can be expected with credit cards, online services, or other traditional payment remittance methods—but certainly less than would be associated with the use of

[37] Ducas Evangeline and Alex Wilner, "The Security and Financial Implications of Blockchain Technologies: Regulating Emerging Technologies in Canada," *International Journal* 72, no. 4 (2017): 538–62, https://doi.org/10.1177/0020702017741909.

[38] Joshua Baron et al., National Security Implications of Virtual Currency-—Examining the Potential for Non-State Actor Deployment (RAND Corporation, 2015), https://doi.org/10.7249/j.ctt19rmd78.

[39] Evangeline and Wilner, "The Security and Financial Implications of Blockchain Technologies: Regulating Emerging Technologies in Canada," 4.

[40] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," 9.

[41] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks."

[42] He et al., "Virtual Currencies and Beyond: Initial Considerations."

cash. Thus, DVCs are said to provide "pseudonymity,"[43] rather than absolute "untraceability."[44]

C. CONTEMPORARY TERROR FINANCE

All TOs—regardless of size, structure, motivations, or methods—must raise and move the financial means to turn terrorist plots into actions.[45] TOs have exhibited great flexibility and variety in their funding methods and have proven that they are willing to use any and all means to raise and move money to support their agendas.[46] According to Maruyama and Hallahan of the Center for a New American Security, contemporary terror financing methods are "constantly evolving to avoid the restrictions imposed by governments, intergovernmental organizations, and the international financial system."[47]

Some of the more notable methods of raising money for and among TOs include: private donations, abuse and misuse of non-profit organizations, smuggling, drug trafficking, kidnapping for ransom, exploitation of natural resources, control of banks, involuntary extraction from local populations, legitimate commercial enterprise, and state sponsorship.[48] FATF's reports found that fully one third of all cases and prosecutions of terror financing in the United States since 2001 "involved direct financial support from individuals to terrorist networks."[49]

Regardless of how TOs acquire the money they raise, it must be moved and/or spent, often internationally, to facilitate and coordinate operations, create propaganda, successfully recruit new members, train and equip existing members, pay the salaries of members and leadership, and even provide social services to members and local

---

[43] Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities," 9.

[44] Thibault de Balthasar and Julio C. Hernandez -Castro, "An Analysis of Bitcoin Laundry Services," in *NordSec2017—Nordic Conference on Secure IT Systems, 8-10 Nov 2017, Tartu, Estonia* (2017). https://doi.org/10.1007/978-3-319-70290-2_18.2017, 23.

[45] FATF, "Emerging Terrorist Financing Risks" (Paris: FATF, 2015), www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.

[46] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat."

[47] Maruyama and Hallahan, "Following the Money: A Primer on Terrorist Financing," 2.

[48] FATF, "Emerging Terrorist Financing Risks."

[49] FATF, 13.

populations.[50] Terrorists today continue to rely primarily on traditional methods of moving money including services from banks within the formal banking sector, informal money value transfer systems (MVTS) like hawala networks, or such MSBs as Western Union, as well as the physical transportation of cash.[51] Indeed, while cash remains the simplest and most widely used method of purchasing goods and services within local economies, moving money across international borders in quantities sufficient to fund large-scale TOs is increasingly making the use of bulk cash impractical.[52] Thus, TOs have shown a willingness to delve into NPPS like prepaid cards and Internet-based payment systems, including DVCs, especially considering the increased anonymity, global reach, and faster speed these types of transactions can offer.[53]

As DVCs—the most well-known of which is Bitcoin—attract increasing attention from financial institutions (FIs), governments, and the general public, two narratives have taken shape. The first holds that DVCs represent an important innovation in the future of legitimate global payment products and services; the second, that DVCs represent a powerful new method for criminals, terrorist financiers, and sanctions-evaders to store and move money outside the reach of law enforcement and financial regulators.[54]

Indeed, a small minority of governments, with little appetite for complex financial innovations, have wholly banned DVCs as a potentially disruptive technology—acting on the latter narrative, or in response to the destabilizing effect DVCs can have on local economies (either because of the demand for electricity, which has the effect of driving up production costs and rates when miners are operating at scale, or because of the inflationary risks that come with price instability). Though such states as Russia and Bolivia have entirely disallowed the use of DVCs within their borders, after weighing the risks versus the potential benefits, the United States—and most states with well-developed financial infrastructures—have tentatively and cautiously developed some form of regulatory

[50] FATF, "Emerging Terrorist Financing Risks."

[51] FATF.

[52] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat."

[53] Goldman et al.

[54] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks."

enforcement and oversight capability in their approach to incorporating DVCs into the broader economy.[55]

D. EXISTING AML/CFT REGULATIONS

Illicit actors' potential use of early centralized virtual currencies for money laundering has been a concern of some of the world's largest financial institutions since at least 1996. In that year, a virtual currency offering, e-gold, appeared and was immediately subject to investigation and review by AML authorities.[56] Now defunct, e-gold nonetheless demonstrated that virtual currency could appeal to both mainstream investors and those seeking to use the currency for illicit purposes.[57] Early abuse of virtual currencies like e-gold forced regulators to add them to the language of existing AML/CFT policy, adding to the patchwork of financial sector laws and regulations that are still relied on today, either to rein in NPPS like DVCs, or shut them down when illicit use is suspected or discovered.[58]

According to the IMF, money laundering involves processing funds generated by criminal means in an effort to shroud any links between the funds and their illegal origin, while terrorism financing, a specific and separate issue, deals exclusively with raising money to support terrorist activity.[59] Though these two distinct and long existing issues have many differences, they often deal with very similar vulnerabilities in financial systems that allow transactions to occur anonymously or with an undesirable level of opacity.[60] Many tools and regulations designed to stave off both issues have seen significant modification and edits in order to be inclusive of the rapidly evolving landscape of NPPS,

---

[55] He et al., "Virtual Currencies and Beyond: Initial Considerations."

[56] Though regulators had monitored e-gold Ltd. since its inception in 1996, the federal government built their case for nine years before bringing charges against its administrators in 2007. In-depth detail of enforcement actions against the administrators of now defunct virtual currency e-gold Ltd. are well-documented in section III. in: Middlebrook and Hughes, "Regulating Cryptocurrencies in the United States: Current Issues and Future Directions."

[57] Middlebrook and Hughes.

[58] Middlebrook and Hughes; HSSAI, "Risks and Threats of Cryptocurrencies."

[59] International Monetary Fund, "Factsheet: The IMF and the Fight Against Money Laundering and the Financing of Terrorism," October 30, 2017, https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism.

[60] International Monetary Fund.

however, these methods continue to struggle to stay ahead of the innovations that illicit actors and terrorists exploit.[61] And while virtual currencies are not new, per-se, the AML/CFT regulations that the United States relies on to detect and prevent their illicit use are significantly older by comparison and likely in need of serious revision to remain wholly applicable to such a rapidly evolving technology.

The BSA of 1970, combined with the Money Laundering Control Act of 1986, and Title III of the USAPATRIOT Act of 2001, form the core of U.S. AML/CFT laws and regulations. This combination of regulations, as applied to banks and FIs, established requirements for suspicious transaction reporting, recordkeeping, and perhaps most notably, standards for identifying individuals participating in transactions, often referred to as know-your-customer (KYC) requirements.[62] However, on the heels of a growing number of headlines regarding criminal activity and money laundering involving the use of DVCs, these KYC requirements (last updated in 2001) drew increased attention—and some ire—from DVCs' proponents like developers and users, as well as more skeptical government leaders and financial institutions the world over.[63] Proponents of DVCs lament KYC requirements because they stifle anonymity—one of the primary libertarian motivations behind the original design of DVCs—while according to Jared Kleiman, many LEAs and policy makers argue that current KYC requirements do not go far enough and instead allow continue to allow DVCs to be utilized with sufficient anonymity that it creates "a means to transfer, launder, or steal funds as well as a means of making donations to groups participating in illegal activities."[64]

Especially following the rise of more organized terror groups like Al Qaida and ISIS, a renewed fervor over AML/CFT concerns made it apparent that clearer definitional and regulatory guidance would benefit those seeking more widespread adoption of

---

[61] Maruyama and Hallahan, "Following the Money: A Primer on Terrorist Financing."

[62] Victor Dostov and Pavel Shust, "Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?," *Journal of Financial Crime* 21, no. 3 (2014): 249–63, https://doi.org/10.1108/JFC-06-2013-0043.

[63] Kleiman, "Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger U.S. National Security and Welfare."

[64] Kleiman, 74.

developing fintech as well as ease the fears of those seeking to govern its use. Thus, in 2013, responding to calls for regulatory updates or clarifications, FinCEN released guidance that defined how the U.S. government would choose to align developers, exchangers, and users of DVCs into the framework of the BSA.[65] Shortly after the release of FinCEN's guidance, FATF released two reports; one in 2014 specifically addressing key definitions and the AML/CFT risks of virtual currencies, and another in early 2015 recommending a risk-based approach (RBA) for virtual currencies to FIs.[66] FinCEN and the BSA closely adhere to FATF's RBA, however, because these recommendations are non-binding, several other governments have taken very different actions to manage the use of DVCs because an outright ban of their use is untenable. This permissiveness complicates the enforcement of cross-border AML/CFT efforts between governments.[67]

The Bank Secrecy Act establishes requirements primarily for traditional banks as well as such MSBs as foreign currency exchanges and money transmitters. The current applicability of U.S. AML/CFT regulations to DVCs, therefore, relies on FinCEN having identified certain participants in the DVC ecosystem as MSBs. FinCEN determined in its 2013 guidance, and later in follow-on clarification efforts, that participants in the virtual currency ecosystem fall into one of three categories: users, administrators, and exchangers.[68] Following four administrative rulings intended to clarify their initial guidance, FinCEN currently defines a DVC exchanger as "a person engaged as a business in the exchange of virtual currency for [fiat] currency, funds, or other virtual currency,"[69]

---

[65] FinCEN, "Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Guidance (U.S. Department of the Treasury, March 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

[66] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks"; FATF, "Guidance for a Risk-Based Approach to Virtual Currencies" (Paris: FATF, June 2015), http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.

[67] An excellent summary of DVC regulation by nations other than the United States is available in section II. D. in: Sarah Hughes and Stephen Middlebrook, "Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries," *Yale Journal on Regulation* 32, no. 2 (2015): 495–559.

[68] FinCEN, "Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies"; Dostov and Shust, "Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?"

[69] Dostov and Shust, "Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?," 11.

leaving all others who transact in DVCs—not engaged as a business—defined simply as users. While users are the only category of the three not subject to BSA requirements, because DVCs lack any administrator by FinCEN's definition, at the time of this writing only DVC exchangers are required to register as a MSB.[70] In alignment with FATF's RBA, FinCEN's decision to only identify exchangers as MSBs—and thus make them the only DVC participants subject to the BSA—seems to agree with the IMF's position "that the most significant [AML/CFT] risks are concentrated in points of intersection between [virtual currencies] and the regulated fiat currency financial system. As such, it has only called for the regulation of…exchanges…that operate as 'gatekeepers' with the regulated fiat currency financial system."[71]

E. CONCLUSION

Digital virtual currencies are appealing to any individual or group that seeks to obscure the movement of funds across borders. TOs are especially interested in this kind of capability and have demonstrated the ability to take advantage of weaknesses in financial regulatory and oversight regimes by adopting new financial products and services. Virtual currencies can be understood as an innovative financial product that includes features to anonymize the locations and identities of parties to a transaction, and a review of existing government regulations written to monitor DVCs for AML/CFT abuse make it clear that the existing regimes for oversight and enforcement are relatively weak. Current U.S. laws and regulations are focused only on *registered* DVC exchangers to ensure BSA compliance. Thus, any changes to DVC technology, or to the tools and markets that support their use, that further enhance the anonymity of exchangers and alleviate their obligation to register with FinCEN as MSBs, may lead to both exchangers and users of these exchanges operating outside the scope of current regulatory oversight. This fact means that governments around the world that have an interest in KYC/AML and terror finance must respond quickly to the rapid innovation that is taking place in the financial services sector.

[70] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat."

[71] He et al., "Virtual Currencies and Beyond: Initial Considerations," 27.

The fact that the regulatory regime for these exchanges—and the currencies that are traded—are so weak is symptomatic of a larger problem: assumptions that regulatory authorities have made about the scalability, appeal, and speculative value of DVCs. The next chapter of this thesis examines these assumptions and demonstrates conclusively that there is considerable public interest in virtual currencies, and that the explosion of DVC offerings is a challenge that must be faced by regulators and LEAs who must become more responsive to the possibility that TOs will employ both DVCs and unregistered exchanges in the near future.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MARKET SIZE AND COMMERCIAL ACCEPTANCE SWELLS

A. INTRODUCTION

Many prior AML/CFT risk assessments cite the need for significant growth of the relatively small DVC market as a primary limiting factor to the widespread use and adoption of DVCs by TOs. Broadly, the size or *scale* of the DVC market can be viewed as a limiting factor because it determines how easily and reliably DVCs can be converted to or from fiat currency, and/or how easily DVCs can be spent directly on goods and services in the general economy. Convertibility relies on sufficient *liquidity*, the ability of the market to support a large volume of transactions, as well as on sufficient *market capitalization (market cap)*, the overall value invested in the market, to ensure the magnitude of currency required for large transactions is available. As the DVC market grows in size and scale, commercial interest attracts investment capital to fintech developers who create new applications and user interfaces designed to make DVCs easier to use, expanding and strengthening the support network intended to increase direct spending of DVCs in the general economy.[72] As previously mentioned, if the number of direct spending transactions using DVCs grows, so too does the parallel economy that exists outside the scope of current regulations, potentially making DVCs more attractive to illicit actors.[73]

Though prior assessments do not attempt to quantify what market size, level of commercial acceptance, or rate of growth should be considered a potential threat, they instead offer expected values for these data sets for the next several years. To determine if these values should reasonably be considered significant, this chapter examines some of the DVC market size statistics, figures, and expected rates of growth cited in recent low threat reports and compares them to current data to establish a position that, indeed, growth in all areas of market size, commercial use, and investment interest should reasonably be

[72] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat."

[73] He et al., "Virtual Currencies and Beyond: Initial Considerations."

considered significant. More specifically, this chapter argues that a recent rapid rise in value has led to a significant increase in DVC market cap and liquidity and has attracted a sudden influx of investment capital into the DVC ecosystem that has resulted in its increased commercial use. Indeed, in a very short period of time following the most recent 2017 assessments of TO interest in DVCs, due to the incredible growth of the overall market size and increased commercial acceptance, DVCs may now be more likely to attract TOs, and arguments that TOs are unlikely to adopt DVCs due to these limitations may no longer be valid.

B. GROWTH IN DVC MARKET CAPITALIZATIONS AND LIQUIDITY

David Cohen, the Obama Administration's Under Secretary of Terrorism and Financial Intelligence, U.S. Department of the Treasury, is quoted in a 2014 HSSAI report as saying that "we do not currently see widespread use of virtual currencies as a means of terrorist finance," in part, due to "its low capitalization and liquidity."[74] This same report cites an estimate from the same year that the total DVC market cap could likely "grow by 14 percent…topping $55.4 billion by 2017."[75] Comparatively, more recent data shows the total market cap of virtual currencies exceeded DHS's estimate by more than 1000 percent; in 2017 it peaked at more than $590 billion before declining rapidly to end the year, but then climbed beyond $800 billion just two weeks later.[76] Similarly, HSSAI cites data from CoinDesk in late 2014, regarding the astounding rate of growth in venture capital investment in virtual currencies at that time: "The amount of money invested…has increased significantly, from about $2 million in 2012 to…more than $250 million so far in 2014, representing an increase of more than 12,000 percent in three years."[77] More recently, venture capital investment in DVC related fintech has already exceeded $1.15 billion so far in 2018, representing an increase of more than 57,000 percent over the six

[74] HSSAI, "Risks and Threats of Cryptocurrencies," 108.

[75] HSSAI, 23.

[76] "Historical Snapshots," CoinMarketCap, 2018, https://coinmarketcap.com/historical/.

[77] HSSAI, "Risks and Threats of Cryptocurrencies," 16.

years since 2012, which shows that general interest in growing the scale, capitalization, and liquidity in DVC markets shows no sign of slowing.[78]

As noted, as recently as March 20, 2017, Zachary Goldman et al. indicated that DVCs lacked useful scale to support large TOs when they stated that the market cap of the oldest and most widely known and utilized DVC, Bitcoin, was roughly $17 billion, while such newer, more anonymous DVCs as Monero and ZCash had market caps of $340 million and $22 million, respectively.[79] Goldman et al. contrasted these figures to the U.S. government's estimate that TOs' "illicit financing generates $300 billion per year,"[80] suggesting that the total market cap of these three popular DVCs do not possess the scale needed to support the movement of TOs' illicit finance proceeds in totality. However, again illustrating the unprecedented exponential growth experienced by the overall DVC market in 2017, just nine months later at the end of 2017, Bitcoin's market cap exceeded $327 billion, while Monero and ZCash grew to $5.4 billion and $1.4 billion, respectively.[81] This data suggests that the market cap of these three DVCs alone could potentially more than support annual TOs' illicit finance requirements—and these three big players are only three of more than 1600 DVCs in the market at the time of this writing. Additionally, this data indicates subject matter experts misjudged the potential of DVC markets and regulators may have underestimated the broad appeal of DVCs.

Commanding more than 37 percent of the total DVC market to date, the original and oldest DVC, Bitcoin, is one of the few for which current and historical transactional data is readily available.[82] At the time of this writing, Bitcoin typically processes an average of 250 million transactions daily, and the underlying distributed ledger system is capable of supporting a peak capacity of nearly 500 million.[83] This transactional capacity

---

[78] "Bitcoin Venture Capital," CoinDesk, accessed May 11, 2018, https://www.coindesk.com/bitcoin-venture-capital/.

[79] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat."

[80] Goldman et al., 18.

[81] "Cryptocurrency Market Capitalizations."

[82] "Cryptocurrency Market Capitalizations."

[83] "Bitcoin Charts," Blockchain, accessed May 12, 2018, https://blockchain.info/charts.

equates to a single DVC with the potential to account for up to one third of the roughly 1.4 billion daily non-cash transactions occurring worldwide.[84] Again, though no specific threshold was established by prior research as to how much growth would bring DVCs to a scale considered to be a serious AML/CFT threat, it could be irresponsible not to take notice of this recent explosive growth trend and weigh the need for re-examination.

C. COMMERCIAL ACCEPTANCE AND NETWORK GROWTH

The primary reason for DVC market growth has not been attributable to its ease of use or a sudden wave of retail DVC spending. Instead, much of the meteoric rise in the total market cap and liquidity of DVCs is most likely attributed to the rise in popularity of investing in and speculating on its future value.[85] Still, the growing commercial and retail context in which users can transact in DVCs should not be ignored by those evaluating the growth of the DVC network since these characteristics tend to improve a payment product's ease of use—expanding the user base and the parallel DVC economy—more so than the overall size of the market, making it more accessible to legitimate consumers and illicit actors alike.

Though DVC payment systems still lag other more common forms of payment due to barriers created by limited retail acceptance and the complexity involved with obtaining and spending DVCs, great strides are being made in these areas. As an example of the growing retail use of DVCs, Marija Odineca at CoinTelegraph reports that the number of retailers accepting DVCs for payment in 2015 stood at just more than 7,000, while today more than 100,000 merchants now accept DVCs, including large well-known merchants like Amazon, Overstock, Microsoft, Expedia, and Subway.[86] However, DVC payment services can still only reach these larger retail and commercial audiences if the DVC

[84] "Total Global Non-Cash Payment Volumes," Worldpaymentreports.com, accessed May 12, 2018, https://www.worldpaymentsreport.com/reports/noncash.

[85] Alexander Kravets, "Institutional Investors Will Bet Big on Cryptocurrencies in 2018," Cointelegraph, January 18, 2018, https://cointelegraph.com/news/institutional-investors-will-bet-big-on-cryptocurrencies-in-2018.

[86] Marija Odineca, "Bitcoin Growth In 2016? Show Us Your Numbers!," Cointelegraph, January 19, 2016, https://cointelegraph.com/news/bitcoin-growth-in-2016-show-us-your-numbers; Jeremy West, "Largest Directory of Places to Spend Bitcoins," SpendBitcoins, accessed February 18, 2018, http://spendbitcoins.com/.

support network continues to grow and evolve to make obtaining and using DVCs more commonplace and convenient. Generally, consumers are not willing to attend a conference, read a tutorial, or watch a YouTube video—as was once a common requirement for first time users—to figure out how to buy a cup of coffee with Bitcoin, and so, it could be presumed that many TOs might not be willing to delve into the complexities of transacting in DVCs.[87] Indeed, even as commercial use of DVCs gains popularity and the numbers of full-service brokerages and exchanges have swelled to nearly 11,000, until recently, understanding, acquiring, and using DVCs remained too great a barrier to many people.[88]

To reach a larger audience, new technologies, services, and businesses have been created to begin to overcome the "complication barrier" and have begun integrating DVCs into more familiar forms of use through the proliferation of ATMs and smart phone applications in place of the—at times complex—desk-top computer programs once required to transact in DVCs. According to HSSAI, in July of 2014, there were just more than 120 DVC ATMs worldwide, designed to facilitate the exchange of fiat currency for Bitcoin.[89] By comparison, today there are more than 6,000 ATMs globally that service eight popular DVCs and the rate of new world-wide installations has reached nearly eight units per day.[90] Additionally, while early users of Bitcoin could only choose to store their private cryptographic keys (required to initiate and authorize transactions) in either paper *wallets*, downloadable computer software, or stand-alone hardware similar to USB thumb drives, smart phone wallet apps have been developed to bring ease of use for all DVCs to mobile networks and anyone who can use a modern cell phone.[91] At the end of 2017 there were more than 2,000 smart-phone applications on Google Play alone designed to enable fast and easy transactions between users, banks, merchants, exchanges, and all other types

[87] HSSAI, "Risks and Threats of Cryptocurrencies."

[88] "Cryptocurrency Market Capitalizations."

[89] HSSAI, "Risks and Threats of Cryptocurrencies."

[90] "Coin ATM Radar," Coinatmradar.com, accessed May 13, 2018, https://coinatmradar.com/charts/.

[91] Dostov and Shust, "Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?"

of wallets, with a more familiar interface, greatly expanding the possible DVC user base and nearly eliminating any complexities to obtaining and spending DVCs easily.[92]

At the beginning of 2018, some of the top DVC exchanges were adding 100,000 new users per day; unfortunately, not all of these new users, nor all recent DVC market growth can be attributed to legitimate commercial and retail networks.[93] The increase in DVCs' popularity for illegal purposes within criminal networks must also be accounted for. Cybercriminals and TCOs are in fact making use of DVCs on a significant scale.[94] Indeed, in an assessment from 2017, the U.S. Drug Enforcement Agency (DEA) stated that "TCOs are…increasingly using virtual currencies due to their anonymizing nature and ease of use. Bitcoin is the most common form of payment for drug sales on dark net marketplaces and is emerging as a desirable method to transfer illicit drug proceeds internationally. Bitcoin is the most widely used virtual currency due to its longevity and growing acceptance at legitimate businesses and institutions worldwide."[95]

Though this thesis and previous research keeps TOs, cybercriminals, and TCOs in distinctly different categories when assessing their individual scales of DVC use, when establishing the overall rise of DVC use cases and total market growth, it becomes difficult to ignore that both TOs and TCOs engage in drug trafficking, kidnapping for ransom, and money laundering associated with these activities. It is at the very least interesting to note that the U.S. House Homeland Security Committee has stated that "Terror financing experts assess that criminality and Islamist extremism are increasingly interconnected; ISIS actively seeks recruits with skills such as robbery and drug-dealing, that assist the group's

[92] Alyssa Hertig, "Crypto Mobile Apps Security Report," CoinDesk, November 29, 2017, https://www.coindesk.com/90-crypto-mobile-apps-trouble-security-report-claims/.

[93] Joseph Young, "Exponential Growth: Cryptocurrency Exchanges Are Adding 100,000+ Users Per Day," Cointelegraph, January 7, 2018, https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day.

[94] DEA, "2017 National Drug Threat Assessment" (Washington, DC: U.S. Department of Justice Drug Enforcement Administration, October 2017), https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf.

[95] DEA, 130.

overall mission. One expert on Islamist radicalization has described jihadists' connections to criminality as 'an operational aspect of the Islamic State.'"[96]

Regardless of exactly who or what groups are responsible for the growth of the DVC market and its associated networks, tools, and technology, clearly the broader DVC ecosystem is growing, but will it now pose a greater threat? What we can safely surmise is that a growing commercial market, increasing acceptance of retail DVC point-of-sale transactions, an expanding illicit user base, and private peer-to-peer transactions all serve to decrease the need for TOs to exchange DVCs for fiat currency in order to conduct transactions in the general economy. Consequently, as this parallel virtual economy grows, eliminating the need to cash out DVCs for fiat currency, more and more transactions will inherently circumvent the narrow scope of AML/CFT scrutiny provided by licensed exchanges and MSBs.

D. CONCLUSION

The evidence presented in this chapter illustrates conclusively: the overall size of the DVC market has grown well beyond the expectations of both private and government subject matter experts; and commercial interest and acceptance of DVCs by a growing user base has exploded and shows little evidence of slowing. Though prior research did not attempt to establish any quantitative or qualitative goal posts for conditions or values at which they would no longer consider the limited market size and commercial acceptance of DVCs as barriers to TOs' interest or adoption, the rate of change of both factors has been significant enough to consider whether these two limiting factors may be nullified. Regardless, the next chapter will explore recent changes in the remaining two factors cited by researchers as barriers to adoption of DVCs by TOs: insufficient anonymity and the perceived lack of technological sophistication of TOs.

[96] Homeland Security Committee, "Cash to Chaos: Dismantling ISIS' Financial Infrastructure," House Homeland Security Committee Majority Staff Report (Washington, DC, October 2016), 15, https://homeland.house.gov/wp-content/uploads/2016/10/Dismantling-ISIS-Financial-Infrastructure.pdf.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. GREATER ANONYMITY AND TECHNOLOGICAL SOPHISTICATION OF TERRORIST ORGANIZATIONS

A. INTRODUCTION

The previous chapter addressed changes in market size and commercial acceptance of DVCs, undermining assumptions that these characteristics would limit TO adoption. The remaining assumptions to be addressed in this chapter are epitomized by the assessment of Goldman et al. who stated that, "without securing anonymity and increasing technological sophistication, systematic use of Bitcoin by terrorists remains unlikely."[97] Indeed, if Bitcoin were the only DVC at issue, this thesis could offer little in the way of rebuttal. However, due to recent developments in newer, more anonymous DVC technology, according to Olga Kharif, "Bitcoin is losing its luster with some of its earliest and most avid fans—criminals—giving rise to a new breed of virtual currency."[98] Furthermore, TOs are making strides in gaining technological sophistication while advancements in ease of use continue to lower technological barriers to utilizing DVCs.

The first segment of this chapter will address recent developments in anonymizing fintech fueled by an apparent arms race between privacy advocate DVC developers and LEAs determined to maintain or regain their ability to investigate, identify, and gather evidence against those who might use DVCs for nefarious purposes, including TOs. Additionally, as asserted by Goldman et al., developments in greater anonymity alone are unlikely to make DVCs more attractive to TOs if the technology remains too complicated to use for persons or groups who may have limited Internet access or limited technological sophistication. Thus, the second segment of this chapter addresses evidence that TO technological sophistication is on the rise, and, thanks in large part to the growth of commercial acceptance addressed in previous chapters, DVCs are increasingly easier to use.

---

[97] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat," 24.

[98] Olga Kharif, "The Criminal Underworld Is Dropping Bitcoin for Another Currency," Bloomberg, January 2, 2018, https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.

B. DEVELOPMENTS IN ANONYMIZING FINANCIAL TECHNOLOGY

During its infancy, Bitcoin appealed to those seeking privacy for both legitimate and illicit purposes because it was thought to offer greater anonymity than most traditional financial mechanisms. However, following several high-profile criminal prosecutions involving the use of Bitcoin, it became clear that law enforcement agencies had developed the means to follow the money through the known design limitations of the publicly viewable blockchain. As David Carlisle points out in his assessment for RUSI, "Law enforcement agencies are able to use a variety of new forensic techniques and tools alongside their traditional investigative methods to analyse and follow illicit flows of Bitcoin in support of criminal investigations."[99] However, encouraged by the recent and rapid influx of billions of dollars into the DVC market, developers are investing huge sums of capital into creating and marketing new anonymizing fintech aimed at consumers who value their privacy.

Developments in DVC related fintech include but are not limited to: third-party browser and IP address anonymizing software designed to complicate or completely obfuscate the location and identity of Internet users; the development and proliferation of private online marketplaces hidden from public view on the unindexed Internet, often referred to as dark web markets (DWMs); DVC privacy-enhancing tools designed to be used with existing DVCs; and finally, newly designed DVCs enabled with greater or total anonymity. This section discusses these developments individually but also illustrate how each of them build on one another to provide an enhanced level of anonymity that may prove sufficient to rebut arguments that DVCs cannot be made anonymous enough to attract the use of TOs.

1. Anonymizing Software

The reason for the development and use of anonymizing third-party software is best illustrated by David Carlisle, citing cryptocurrency researcher Malte Möser, who stated: "AML in Bitcoin has to deal with imperfect knowledge of identities, but may exploit

[99] Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities," viii.

perfect knowledge of all transactions."[100] Specifically, Möser meant that if anyone looking closely enough manages to connect someone's real identity to a specific DVC address or wallet, then that person's complete transaction history is viewable—for example, to authorities.[101] Revelations that the Bitcoin blockchain was not as infallible as was originally believed arose quickly after the 2013 arrest of Ross Ulbricht, the alleged mastermind behind the DWM known as *The Silk Road*,[102] and doubly so following the more recent 2017 arrests of the administrators of *AlphaBay* and *Hansa Market*, the most popular successors to the Silk Road.[103] Indeed, most DVC users have learned that the publicly viewable distributed ledger protocols underlying many of the most popular DVCs present a weakness that requires those seeking greater or total transactional anonymity to take additional precautions to safeguard their online identities.

One such effort to complicate an outside party's ability to follow DVC transaction histories involves the common practice of creating a new and unique public address for each and every individual transaction. However, though the ability to create an infinite number of new DVC wallets or addresses can make identifying a user *more* difficult, if investigators can determine the actual location of the device or physical address from which a user accesses the network, linking that device or location to a group or individual with *any* number of wallets or addresses becomes possible with enough effort through law enforcement's investigation of Internet protocol (IP) traffic analysis.[104] Therefore, if blockchain transaction histories can provide investigators with a perfect reconstruction of *how much* was transacted *when*, then protecting information regarding *what* was purchased from *where* or from which device, becomes crucial to maintaining the anonymity of *who*

---

[100] Carlisle, 9.

[101] Carlisle, 9.

[102] Details of the FBI's investigation, arrest, and prosecution of Ross Ulbricht are described in detail in section I.A.2. in: Nicole S. Healy and Emily N. Christiansen, "Anti-Money Laundering and Counter-Terrorist Finance," *ABA/Section of International Law Year in Review* 50 (June 2016): 426–38.

[103] Details of U.S. and European authorities' investigations, arrests, and seizures of AlphaBay and Hansa Market are detailed in: Nathaniel Popper and Rebecca R. Ruiz, "Authorities Shut Down Two Markets On Dark Net," *The New York Times*, July 20, 2017, sec. A.

[104] Pouyan Bohloul et al., "Anti-Money Laundering and Counter-Terrorist Finance," *ABA/Section of International Law Year in Review* 51 (June 2017): 431–46.

is transacting online. Disguising or complicating the where and the who of online activity is precisely the function of third-party anonymizing software.

To obscure a user's online activity, especially the where and the who, free and such publicly available browser applications as the Tor Browser from The Tor Project Inc. (formerly known as the The Onion Router) can be used by anyone with a computer to anonymize their IP address, and thus their location and identity.[105] According to the Tor Project's website, "Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location."[106] Tor is not the only browser or software designed to permit Internet anonymity and prohibit network tracking by investigators, but it is one of the oldest and most used, listed as an essential privacy enhancement tool by many privacy and fintech-centric forums and websites.[107] Indeed, since Tor's inception in the early 1990s, a number of both licit and illicit groups and individuals—from smugglers and drug dealers to LEAs and news reporters--have used the technology to establish encrypted and anonymous websites protected from monitoring and tracking by outside entities.[108]

2. Dark Web Markets

Anonymizing technology like Tor is essential for illicit actors to establish and access anonymous networks located on the unindexed Internet, or *deep web*. The deep

---

[105] DHS Science and Technology Directorate, "Cyber Security Division-Anonymous Networks and Currencies" (U.S. Department of Homeland Security, March 3, 2016), https://search.dhs.gov/search/docs?affiliate=dhs&dc=3634&query=cryptocurrency. Originally developed by the U.S. Naval Research Laboratory and the Defense Advanced Research Projects Agency (DARPA), Tor was intended to provide secure web-based communications for government and law enforcement personnel. "About Tor," Tor Project Inc., accessed May 20, 2018, https://www.torproject.org/about/overview.html.en.

[106] "About Tor."

[107] "Anonymity Tools," Dark Web News, accessed May 20, 2018, https://darkwebnews.com/category/anonymity-tools/; "The Best Free Privacy Software 2018: Top Tools for Anonymous Browsing," Tech Radar, accessed May 20, 2018, https://www.techradar.com/news/best-free-privacy-software.

[108] HSSAI, "Risks and Threats of Cryptocurrencies," 87.

web—which is not searchable or indexed by traditional search engines like Google or Bing—comprises as much as 96 percent of the total World Wide Web, according to estimates provided by one black market enthusiast website.[109] Primarily home to legitimate private corporate networks and other password protected sites designed specifically to provide secure communications and identity protection to users, the illicit side of the deep web is often referred to as the *dark web*.

The dark web is only accessible through the use of anonymizing software like Tor and requires users to know the specific web address of the site they intend to access, some of which change their address frequently and only post the latest dynamic address in heavily vetted, by-invitation-only, password protected forums and chat rooms.[110] It is here, in the lowest reaches of the dark web, where users can set up and access any one of several hundred DWMs for weapons, drugs, hitmen, explosives, stolen intelligence, financial data, human trafficking, and a near limitless range of black market goods and services, all anonymous and encrypted—and almost exclusively leveraging DVCs for transactions.

In addition to weapons, explosives, and other goods that TOs could choose to purchase anonymously directly from a DWM for the purpose of conducting attacks, a growing number of hidden, unlicensed, peer-to-peer (P2P) DVC exchanges on the dark web enable illicit actors to circumvent the AML/CFT protections placed on publicly utilized, legitimate DVC markets and exchanges. These secretive DWMs and unlicensed P2P DVC exchanges, which only exist with the successful use of anonymizing software, complicate AML/CFT regulation enforcement because they render exchange administrators, the only entities currently obligated with KYC and AML/CFT compliance, completely anonymous. As a result, even though the blockchain's exposed history allows LEAs to see that DVC has appeared in or been transferred from DVC wallets or addresses, if parties purchase DVCs in exchange for fiat currency through anonymous P2P exchanges, no identifying information will likely be forthcoming from an illegal exchange's

[109] "The Weird and Wonderful Deep Web," Dark Web News, accessed May 20, 2018, https://darkwebnews.com/deep-web/.

[110] HSSAI, "Risks and Threats of Cryptocurrencies."

administrators. LEAs would be unable to determine ownership of the exchange for enforcement actions due to the use of anonymizing software.[111]

As legitimate AML/CFT compliance becomes more complex and costlier for smaller businesses hoping to ride the wave of DVC exchange profitability, these businesses are increasingly apt to choose to operate under the shroud of DWMs where AML/CFT compliance is all but impossible to enforce. Though, the exact numbers of unlicensed exchanges operating within DWMs is unknown due to their inaccessibility to most researchers, according to a 2018 study by the Foundation for Defense of Democracies Center on Sanctions & Illicit Finance, "Darknet Markets are [a] key source of illicit funds," and "[t]he number of illicit entities sending bitcoins to conversion services has risen over time."[112] The study revealed a 500-percent increase in entities involved in the laundering of Bitcoin over a three-year period and notes: "Illicit activity originated overwhelmingly from darknet marketplaces."[113] Though the study's authors are quick to point out that the overall illicit use of Bitcoin specifically appears to be on the decline, they further illustrate the concentration of DVC launderers within DWMs when they note, "Nine of…102 illicit entities were the source of more than 95 percent of all laundered bitcoins in our study. All nine were darknet marketplaces."[114]

3. Privacy-Enhancing Tools for Early DVCs

In addition to supporting unlicensed P2P DVC exchanges and a variety of other nefarious goods and services, according to Ducas Evangeline and Alex Wilner, DWMs accessed through anonymizing software also "support a host of privacy enhancing tools known as 'tumblers' and 'mixers,' which can obscure value ownership and transaction histories on blockchain ledgers, rendering them highly vulnerable to abuse for money

---

[111] Kavid Singh, "The New Wild West: Preventing Money Laundering in the Bitcoin Network," *Northwestern Journal of Technology and Intellectual Property* 13, no. 1 (2015): 37–64.

[112] Yaya Fanusie and Tom Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services" (The Foundation for Defense of Democracies Center on Sanctions and Illicit Finance, January 12, 2018), 5, http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.

[113] Fanusie and Robinson, 5.

[114] Fanusie and Robinson, 6.

laundering and other forms of financial crime."[115] These types of tools are designed to enhance the security and anonymity of Bitcoin, and other early DVCs built on its underpinning basic protocols, since LEAs and the security research community have demonstrated an ability to analyze these early blockchains using transaction times, amounts, and patterns of use.[116]

Brill and Keene explain in the *Defense Against Terrorism Review* that tumblers are designed to enhance the privacy of DVC transactions by sending "payments through a complex, semi-random series of dummy transactions"[117] that complicate and obscure the link between wallets or addresses involved in transactions, "making it fruitless to use the 'Blockchain' to follow the money trail involved in the transaction."[118] Mixers, by comparison, attempt to anonymize transactions by aggregating multiple real transactions of varying quantities into larger third-party transactions that are then dispersed by this third party, for a fee, to the actual intended recipients using newly created addresses.[119] Because most DVC tracking efforts rely on matching transaction amounts with a specific time and address on the blockchain, these services obfuscate the true individual transaction amounts and make it more difficult to trace transactions to individual addresses or wallets.[120]

Some new DVC electronic wallet services provide multiple layers of anonymity by combining the features of third-party mixers and tumblers into a convenient browser-based extension.[121] According to Goldman et al., one such electronic wallet service, known as Dark Wallet, has a stated goal of making de-anonymizing DVC transactions impossible "by combining random contemporaneous transactions and then encrypting recipients'

---

[115] Evangeline and Wilner, "The Security and Financial Implications of Blockchain Technologies: Regulating Emerging Technologies in Canada," 11.

[116] Baron et al., National Security Implications of Virtual Currency—Examining the Potential for Non-State Actor Deployment.

[117] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," 6.

[118] Alan Brill and Lonnie Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing?," *Defense Against Terrorism Review* 6, no. 1 (2014): 21.

[119] Baron et al., National Security Implications of Virtual Currency—Examining the Potential for Non-State Actor Deployment.

[120] Baron et al.

[121] FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks."

information so it does not appear on the blockchain."[122] Irwin and Milad state that Dark Wallet and other services like it "enhance anonymity of transactions by allowing illicit transactions to digitally 'piggyback' on non-illicit transactions,"[123] resulting in a type of layering, or comingling of funds, that would be typical of contemporary money laundering techniques, such as when ill-gotten funds are carefully mixed with legitimate business funds and then deposited into an unsuspecting FI. Dark Wallet has a similar effect as mixing and tumbling combined in that the true amount of a transaction is obfuscated, as is the actual address of both the sender and the receiver, since the wallet produces new, unique, and unrelated addresses for each new transaction.[124] Indeed, Dark Wallet founder Cody Wilson, of 3-D gun printing fame, has stated quite bluntly: "It's just money laundering software."[125]

Summarizing the evolving technology being developed to support the private and anonymous use of the DVC Bitcoin, Irwin and Milad state, "It is feared that Dark Wallet services combined with a Tor Browser may allow Bitcoins to be transferred with complete anonymity."[126] However, this statement alludes to the fact that the majority of these services were designed to support and mask the known privacy deficiencies of public blockchains like those specifically underpinning Bitcoin. Unfortunately, though Bitcoin is still by far the most used DVC on the market, other DVCs are being developed with untraceability properties embedded into the currency. As de Balthasar and Hernandez-Castro state, there are "alternative cryptocurrencies that offer improved anonymity and untraceability properties such as Monero or Zcash,"[127] that LEAs should be more concerned with.

---

[122] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat," 15.

[123] Irwin and Milad, "The Use of Crypto-Currencies in Funding Violent Jihad," 419.

[124] Irwin and Milad, "The Use of Crypto-Currencies in Funding Violent Jihad."

[125] Andy Greenberg, "'Dark Wallet' Is About To Make Bitcoin Money Laundering Easier Than Ever," Wired Magazine Online, April 29, 2014, https://www.wired.com/2014/04/dark-wallet/.

[126] Irwin and Milad, "The Use of Crypto-Currencies in Funding Violent Jihad," 419.

[127] de Balthasar and Hernandez-Castro, "An Analysis of Bitcoin Laundry Services," 23.

4. Newer Privacy Enhanced DVCs

During his testimony to a U.S. Senate Judiciary Committee on S.1241: Modernizing AML Laws to Combat Money Laundering and Terrorist Financing, Matthew Allen of DHS Immigration and Customs Enforcement, Homeland Security Investigations, acknowledges that newer more anonymous DVCs have been designed around a focus of more complete anonymity "to better obfuscate transaction information."[128] A prime example of an anonymity enhancing DVC includes Monero, which, as Zachary Goldman et al. explains, "attempts to ensure users' privacy by combining multiple transactions," making it impossible to isolate and pinpoint any one specific transaction.[129] Additionally, unlike Bitcoin's blockchain—which accurately records the involved addresses, times, and amounts of all transactions for public scrutiny—Monero, according to Olga Kharif, "encrypts the recipient's address on its blockchain and generates fake addresses to obscure the real sender" as well as "the amount of the transaction."[130] Similarly, ZCash makes use of a next generation of DVC technology called Zero-proof to remove any identifying information from transactions, and according to Pouyan Bohloul et al., "renders the transaction untraceable."[131] Indeed, the need for additional, complex, third-party anonymizing techniques, tools, or software is no longer required of these newer DVCs, making them far simpler to use and thus far less prone to user errors that could lead to investigational vulnerabilities. It could be argued then, that any reasonably well-informed TO would not likely opt to continue to try to use Bitcoin for illicit activity over newer DVCs with greater or complete anonymity built right in.

---

[128] Matthew Allen, "S.1241: Modernizing AML Laws to Combat Money Laundering and Terrorist Financing," § Judiciary (2017), https://www.dhs.gov/news/2017/11/28/written-testimony-ice-senate-committee-judiciary-hearing-titled-s1241-modernizing.

[129] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat," 15.

[130] Kharif, "The Criminal Underworld Is Dropping Bitcoin for Another Currency."

[131] Bohloul et al., "Anti-Money Laundering and Counter-Terrorist Finance," 432.

C. GROWTH OF TO TECHNOLOGICAL SOPHISTICATION AND DVCS EASE OF USE

Though growth and development in the scope of TOs' technological capabilities have likely been far less explosive than in the fintech sector, evidence exists that TOs are making strides in their abilities to access and understand how to leverage diverse new technological means to achieve their objectives. Though previous assessments' dismissive treatment of the anecdotal cases of DVC use by TOs may paint a less than compelling picture of terrorists undertaking large-scale adoption of DVCs, what these cases do infer is that TOs are gaining confidence in the use of emerging technologies and are actively acquiring technological sophistication.

This section will revisit many of the same anecdotal use cases cited in previous assessments, as well as examine more recent developments, to aggregate a body of evidence that suggests that TO technological sophistication is growing steadily. Additionally, this body of evidence also suggests that the ease of use of DVCs has improved sufficiently to lower the bar of technological sophistication required to use them effectively and routinely. These developments serve to counter arguments that TOs lack the technological sophistication required to undertake large-scale DVC adoption.

1. TO Technological Sophistication Grows

Goldman et al. insist, "Many terrorist groups…operate in areas with poor infrastructure and low penetration of modern technical and telecommunications tools."[132] Certainly, as much of this body of research insists, technical infrastructure may be lacking in such remote TO haunts as the Horn of Africa, Yemen, or sub-Saharan Africa, presenting a barrier to reliably using a strictly Internet based financial mechanism. However, not all TOs operate in such technology-austere environments, and even fewer TO supporters and financiers, located outside of these specific locations, contend with any kind of technological limitations. Indeed, Goldman et al. concede that many—arguably most—TOs and their supporters are rarely left wanting for "[i]nternet access, computing

[132] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat," 6.

capabilities, or knowledge of sophisticated tactics to evade regulatory detection of electronic money movements."[133] With the rising risks associated with traditional terror finance methods, many TOs are actively seeking to leverage emerging fintech.[134]

Some of the earliest known cases of efforts by TO supporters and would-be-financiers suggest that illicit actors have the technological prowess to utilize DVCs as a mechanism to fund terror operations. For instance, an article posted on-line in 2014 by an author who identified himself as Taqi'ul-Deen al-Munthir specifically instructs jihadist sympathizers how to buy and transfer DVCs using third party anonymizing software, through countries with weak regulatory oversight to directly fund jihadists, or to buy weapons and supplies on hidden dark web marketplaces.[135] According to Andy Greenberg of Wired Magazine, Dark Wallet was commended by name in several papers and blogs known for supporting ISIS.[136] David Carlisle mentions a 2015 example of a U.S. teenager who was given jail time for "using Twitter to describe how to use Bitcoin to support Daesh."[137] Irwin and Milad cite unverified claims by Ghost Security Group who in 2015 claim to have tracked DVC transactions to numerous wallets they believed to be owned by ISIS, containing up to $15.7 million.[138] Moreover, some additional research goes further than reporting on just transactions and instructional material found online and instead point to specific terror operations that were directly funded utilizing DVCs.

Irwin and Milad state that "there is evidence to suggest that Bitcoins have been utilized in a number of successful terror attacks,"[139] including the coordinated November 2015 terror attacks in France. Carlisle's assessment supports this claim when he reports that a Daesh operative in Indonesia, alleged to have plotted a 2016 attack in Jakarta, used

---

[133] Goldman et al., 6.

[134] Irwin and Milad, "The Use of Crypto-Currencies in Funding Violent Jihad."

[135] Taqi'ul-Deen al-Munthir, "Bitcoin and the Charity of Violent Physical Struggle," July 2014, https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf.

[136] Greenberg, "'Dark Wallet' Is About To Make Bitcoin Money Laundering Easier Than Ever."

[137] Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities," 18.

[138] Irwin and Milad, "The Use of Crypto-Currencies in Funding Violent Jihad," 410.

[139] Irwin and Milad, 410.

DVC to transact with other jihadis.[140] Further, he acknowledges that "[t]errorists us[e] VCs to purchase illegal firearms or explosive material on the dark web, as well as travel documents or other items to facilitate operations."[141] Though Carlisle suggests there is no indication that TOs use DVCs "as a payment tool with regularity,"[142] if he and other security experts agree that TOs are already technologically capable of making purchases on DWMs, then there is little to stop them from utilizing unlicensed DVC exchanges and other anonymizing tools located there to effectively mask the indications that Carlisle and other researchers are looking for.

As Maruyama and Hallahan stated in their CNAS primer on terrorist financing, "terrorist groups have displayed a remarkable ability to adapt and innovate to meet their financing needs."[143] Indeed, Joshua Baron et al. state in their report published by the RAND Corporation that "some non-state actors, in particular terrorist organizations, seem to have at least a limited ability to create secure cyber services, such as encryption platforms."[144] These reports suggest that it could be a mistake to dismiss TOs as technologically inept or as less capable than the TCOs that researchers suggests are using DVCs regularly.[145] The U.S. Department of the Treasury agrees and has observed that TOs and TCOs have increasingly similar and at times interconnected complex business models.[146] Indeed, few sustainable businesses can survive in the global economy without some level of knowledge about technology and web-based services, and as Healy and Christiansen suggest, "large-scale terrorist organizations are sophisticated modern

[140] Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities," 18.

[141] Carlisle, 18.

[142] Carlisle, 19.

[143] Maruyama and Hallahan, "Following the Money: A Primer on Terrorist Financing," 9.

[144] Baron et al., National Security Implications of Virtual Currency—Examining the Potential for Non-State Actor Deployment, 36.

[145] U.S. Department of the Treasury, "National Money Laundering Risk Assessment" (Washington, DC, June 12, 2015).

[146] U.S. Department of the Treasury, "National Terrorist Financing Risk Assessment" (Washington, DC, June 12, 2015).

businesses with accounting and finance staff, spreadsheets and financial reports, social media fundraising platforms, and complex financial networks."[147]

ISIS specifically draws attention in all of the research referenced for this thesis because they have repeatedly proven to be an organization which remains incredibly flexible in their methods of finance, using effective modern accounting methods to support what is widely regarded as a financial operation of significant sophistication.[148] According to the U.S. House Homeland Security Committee (HSC), "ISIS is unique in comparison to other terror groups in that it runs a state-like infrastructure designed to raise revenue and support government functions, such as providing social welfare services and waging war."[149] Their ability to support such complex infrastructure and utilize modern financial tools and methods suggests that they are not a group that should be considered constrained by a lack of technological sophistication or capability.

Indeed, ISIS and its supporters have repeatedly demonstrated their ability to use Internet-based platforms like PayPal, GoFundMe, and CASHU, and have set up websites soliciting donations using Facebook, Twitter, and Skype.[150] According to HSC, ISIS has displayed proficiency in utilizing these Internet-based technologies "to circumvent formal financial system controls and preserve anonymity," and has also "used WhatsApp or Kik and messenger applications to coordinate drop-off points for cash or in-kind payments."[151] Though these examples all involve publicly available, indexed-Internet hosted platforms, they demonstrate that as an organization, ISIS possesses the necessary technical acumen and infrastructure to use fintech and secure communication platforms. While there are few known cases that directly link ISIS to using DVCs on any meaningful scale with any regularity, it becomes difficult to say that they are not organized or technologically sophisticated enough to use a Tor browser and newer DVCs in DWMs carefully enough to have just not been caught.

---

[147] Healy and Christiansen, "Anti-Money Laundering and Counter-Terrorist Finance," 435.

[148] Maruyama and Hallahan, "Following the Money: A Primer on Terrorist Financing."

[149] Homeland Security Committee, "Cash to Chaos: Dismantling ISIS' Financial Infrastructure," 3.

[150] Homeland Security Committee, "Cash to Chaos: Dismantling ISIS' Financial Infrastructure."

[151] Homeland Security Committee, 16.

2. DVCs' Ease of Use Improves

Broadly speaking, based on many of the developments in DVC market support, anonymizing tools and software, and newer, easier to use, fully anonymous DVCs discussed in this and earlier chapters, perhaps it is prudent to reassess just how much technological sophistication is actually required to use DVCs today. Smartphones and other wireless or cellular devices are operating more like full-fledged computers with every new iteration and anonymizing software like the Tor browser is already compatible with most smartphones.[152] The number of DVC smartphone apps and smartphone-based wallets continues to multiply, and wireless coverage is steadily expanding to cover an ever-greater footprint across the globe. Because of these factors, Baron et al. suggest, "the usage of mobile phones to conduct everyday VC transactions should be viewed as feasible,"[153] and add that a growing number of people are utilizing mobile money services requiring similar infrastructure in a number of developing countries such as Kenya, Somalia, Pakistan, Iran, and the Philippines. Dong He et al. with the IMF go further than discussing similar mobile money services and assert that "in the Philippines and Kenya, blockchain-based intermediaries offer money transfer services via Bitcoin and subsequent conversion of Bitcoins back into fiat currency for withdrawal by recipients through…their mobile phones."[154] It seems even in relatively remote locations around the globe, if a person has the technological sophistication to use a web browser or a smart phone, he or she can anonymously transact in DVCs.

Smartphones, wallets, and apps are not the only means by which DVCs can easily be anonymously converted in remote locations by those who may lack considerable technical acumen. According to Irwin and Milad a rapidly growing number of DVC "ATMs and…exchanges are located in countries that have seen significant numbers of foreign fighters join ISIS in the Middle East and are also positioned in countries that have

---

[152] "About Tor."

[153] Baron et al., National Security Implications of Virtual Currency - Examining the Potential for Non-State Actor Deployment, 39.

[154] He et al., "Virtual Currencies and Beyond: Initial Considerations," 22.

seen increased risk of terror attack."[155] DVC ATMs in the United States are considered money transmitters under the BSA and as such are subject to AML/CFT regulations. However, because it is up to the individual owner/operator to enforce compliance, it is possible for anyone, including TOs to purchase and operate these ATMs in any country or jurisdiction, some lacking proper AML/CFT enforcement, where they may choose to simply overlook compliance measures.[156] Again, referring to ATMs, Irwin and Milad further clarify the TO and DVC link when they state that "[t]hese present a significant risk because they allow for the seamless, anonymous transfer of funds to and from terrorist groups and their supporters."[157] As an example of the growing ease of use of DVCs, the use of an ATM kiosk is not today typically considered technologically arduous.

For all the expansion of technology and the growth of cellular and wireless networks, an argument can still be made, that there will remain those few unconnected, remote areas where electricity and network connectivity for ATMs may not be available, and mobile phones may be unreliable. In these areas, TOs will be more likely to use more proven, traditional methods of illicit funds transfer such as informal MVTS like hawala networks.[158] However, even low-tech money laundering methods could be augmented by DVCs. For example, some hawaladars who frequently travel to more urban and sophisticated areas to transfer and exchange their funds may elect to utilize DVCs somewhere within that system. Hawaladars could choose to utilize DVCs, as Goldman et al. suggests, to "effectively build a digital platform on top of established systems that currently allow terrorists, and others, to transfer cash on an international scale,"[159]

Traditionally operated hawalas are already an AML/CFT threat, and the U.S. Homeland Security Committee has stated that, "Gaping weaknesses in reporting and oversight standards for hawala transactions hamper efforts to identify ISIS financiers and

---

[155] Irwin and Milad, "The Use of Crypto-Currencies in Funding Violent Jihad," 407.

[156] Irwin and Milad, "The Use of Crypto-Currencies in Funding Violent Jihad."

[157] Irwin and Milad, 407.

[158] Details of the trust-based money value transfer system known as hawala are covered in detail in: Seftel, "Hawala Networks: The Paperless Trail of Terrorist Transactions."

[159] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat," 4.

hold financial institutions accountable."[160] Potentially compounding the issue, even in areas where terrorist A may not be able to directly transact DVC with terrorist B, their hawaladars who may have occasional access to the Internet or wireless networks could elect to utilize DVCs at any point within the network. If instead of carrying large quantities of bulk cash, hawaladars choose to try to reduce their risk by utilizing the security, speed, and cross-border capabilities of DVCs to augment or replace their use of cash, this could provide additional layering and anonymity to an already difficult to track method of terror finance.[161]

The latest assessments regarding TOs' use of DVCs, such as David Carlisle's report to RUSI, warn that as organizations become more technologically adept, DVCs "could become an increasingly viable financing tool for terrorists."[162] Additionally, referring to ISIS, Zach Goldman et al. state that "a number of forum discussions on websites affiliated with the group show efforts by more technical members to educate their peers on the use of virtual currencies."[163] And indeed, evidence suggests that TOs are proving willing and increasingly able to effectively utilize many new payment products and services (NPPS) including DVCs. However, suggesting that vast improvements in technological abilities are required before TOs can effectively use and transfer DVCs to meet their needs, may go too far in making it seem as though an incredible level of technological ability is needed. The relative ease of use of anonymizing DVC apps, browsing software allowing access to DWMs, and fully anonymous DVCs has recently come down to the level of less tech savvy users as evidenced by the expanding, increasingly uncomplicated, network of connected devices like ATMs and mobile phones. As the convenience of technology expands to serve the greater licit masses, so too grows the opportunity for illicit actors to take advantage.

---

[160] Homeland Security Committee, "Cash to Chaos: Dismantling ISIS' Financial Infrastructure," 23.

[161] Seftel, "Hawala Networks: The Paperless Trail of Terrorist Transactions."

[162] Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities," 18.

[163] Goldman et al., "Terrorist Use of Virtual Currencies: Containing the Potential Threat," 12.

D. CONCLUSION

Contrary to the findings of recent prior threat assessments, this chapter conclusively illustrates that the final two pillars on which low threat evaluations of DVC use by TOs were based—insufficient anonymity and a perception of technological sophistication among TOs being too low—may no longer support such dismissive arguments. After rebuttal of all four primary reasons cited by previous researchers, even with only anecdotal cases of DVC use by TOs, assumptions made by this most recent research may already be outdated. While difficult to prove, it is at least possible that the level of anonymity offered by newer DVC technology—including third-party tools designed to anonymize IP addresses, browsers, and existing DVCs—combined with the improving ease of use of DVCs and increasing TO technological acumen, regulators and LEAs may already be unable to monitor DVCs for illicit use. The following concluding chapter will explore the limited information available on reported LEA capabilities at detecting and tracking illicit flows of DVCs and offer a final determination on whether or not TOs may now find DVCs more attractive for current or future use.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION: LAW ENFORCEMENT CAPABILITIES AND THE NEED TO REEVALUATE THE THREAT

This chapter, in conclusion, asserts that: LEAs must continue their efforts to develop new investigational techniques to monitor DVCs for illicit use, policy makers need to reconsider whether current AML/CFT regulations are sufficient to deter illicit use of DVCs, and that further and continuing research is needed to ensure that TOs are not able to take advantage of blind spots created by policy makers' current belief of a low-threat assessment. In the most recent assessment considered for this thesis, Goldman et al. state: "as new cryptocurrencies become more anonymous, and if terrorist groups develop more of the characteristics of criminal enterprises, such as broader person-to-person networks of trust, technical sophistication, and the need for a wider funding base, virtual currencies might become more attractive,"[164]—very nearly predicting the precise developments that unfolded within twelve months of that report. Indeed, much of the research completed as recently as mid-2017 that purports TOs are not capable of—or interested in—utilizing DVCs is already dated and based on assumptions inconsistent with the current state of TO capabilities and the DVC market, and could potentially lead to dangerous oversights by the U.S. homeland security enterprise and unacceptable vulnerabilities to U.S. national security.

Though the growth of DVC markets, broader commercial acceptance, improvements in anonymity, greater ease of use, and the increasing technological capabilities of TOs may have come to fruition just after much of the existing research relied on in this thesis went to print, LEAs and security experts have been making some efforts to contain the potential threat. Indeed, a sort of arms race between developers of anonymizing fintech, security researchers, and law enforcement has inevitably developed, but because law enforcement is typically on the reactionary side of the race, fintech developers tend to stay one step ahead, innovating new privacy centric tools and methods

[164] Goldman et al., 26.

faster than law enforcement can cope.[165] While LEAs and fintech developers seem to be taking their opposing roles in AML/CFT compliance and financial transaction transparency seriously, and in a timely manner, researchers and policy makers that rely on that research have been somewhat slower to respond.

A. LAW ENFORCEMENT CAPABILITIES OR LACK THEREOF

In what should be good news for AML/CFT regulators, recent law enforcement actions suggest that DVCs, Tor, and other anonymizing tools are not necessarily impenetrable. Starting as early as October 2013, when U.S. authorities shut down and arrested the administrator of the DWM Silk Road,[166] and as recently as July 2017, when DWMs AlphaBay and Hansa Market were taken down and their administrators arrested,[167] law enforcement appears to be making some progress in investigating DVC transactions as well as DWMs created with and operated using Tor. It remains unclear, however, whether LEAs have actually made progress in cracking open blockchains and DWMs using new, breakthrough, technologically developed methods or if perhaps these cases may have been a result of simple user error on the side of inexperienced or careless criminals.

According to University of Michigan researchers cited in the HSSAI assessment, "offenders use Tor inconsistently" and "[o]ver 90 percent of regular Tor users send traffic from a non-Tor IP at least once after first using Tor."[168] HSSAI's report implies that prosecutions of DWMs utilizing Tor are most likely due to carelessness on the part of the site's administrator rather than because of any new tools or techniques leveraged by law enforcement. The *New York Times* story on the takedown of AlphaBay and Hansa Market confirm that carelessness and misuse of Tor was indeed the case with at least one of the apprehended administrators.[169] While such working groups as the DHS Science and Technology Directorate, which enlists the help of one of the original developers of Tor--

[165] Carlisle, "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic."

[166] HSSAI, "Risks and Threats of Cryptocurrencies."

[167] Popper and Ruiz, "Authorities Shut Down Two Markets On Dark Net."

[168] HSSAI, "Risks and Threats of Cryptocurrencies," 121.

[169] HSSAI, "Risks and Threats of Cryptocurrencies"; Nathaniel Popper and Rebecca R. Ruiz, "Authorities Shut Down Two Markets On Dark Net."

the Naval Research Laboratory--have been created to develop tools and techniques needed to covertly access and investigate DWMs, the continued operation of such markets as the now popular *Dream Market*, serve as evidence that authorities do not yet have unfettered access to the dark web, lest Dream Market and many others like it would also be shut down. Indeed, following the demise of AlphaBay and Hansa Market, former FBI Deputy Director Andrew McCabe stated, "Critics will say that as we shutter one site, another will emerge, and they may be right…there is always a new player waiting in the wings ready to fill those shoes."[170] While it remains unclear whether or not LEAs possess the tools needed to infiltrate DWMs, either way, authorities likely lack the manpower, budget, or technology to quickly and easily pursue them all considering the rate at which countless new DWMs are springing up.[171]

If Tor and DWMs remain a DVC market variable that cannot yet be fully rendered non-threatening, perhaps investigational access will be gained through monitoring DVC blockchains for suspicious activity? Unfortunately, this also does not seem likely since as David Carlisle notes in a 2017 assessment by Europol: "the majority of law enforcement currently has its attention focused on Bitcoin, a fact which is not lost on the criminal community."[172] Certainly following the takedown of several high profile individuals and DWMs, TOs and the criminal community have come to realize that law enforcement, working with numerous analytic firms, have gained proficiency at flagging suspicious Bitcoin transactions and are now better able to track and monitor its users, as is evidenced by the trove of data compiled by Fanusie and Robinson in their study for the Foundation for Defense of Democracies.[173] These same analysis and monitoring techniques are apparently not yet as effective with such privacy enhanced DVCs like Monero or Zcash, however, and could potentially be a contributing factor in why data from this same study of Bitcoin indicated a "sharp drop in 2016 that mirrored an across-the-board decline in the

[170] Popper and Ruiz, "Authorities Shut Down Two Markets On Dark Net."

[171] Evangeline and Wilner, "The Security and Financial Implications of Blockchain Technologies: Regulating Emerging Technologies in Canada."

[172] Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities," 16.

[173] Fanusie and Robinson, "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services."

proportion of illicit transactions."[174] Interestingly, Zcash first began trading in late October of 2016 when it was met by an immediate buying frenzy according to the *New York Times*,[175] and though Monero had been on the market since 2014, its market cap grew by nearly 2,800 percent in 2016 alone, and was up over 115,000 percent from its 2015 price by the end of 2017.[176] These developments suggest that while LEAs and security researchers were still primarily focused on Bitcoin, TOs and other criminal networks may have quietly adopted other, harder to investigate DVCs.

Though some regulatory technology has been developed in an effort to at least flag suspicious transactions utilizing privacy enhanced DVCs, specifically discussing the opaque blockchain of Monero, Olga Kharif asserts that its underlying protocols are effective enough to confuse regulatory technology software created by companies such as Coinfirm, a company which "helps exchanges and other companies avoid tainted money,"[177] into flagging every transaction as a risk, effectively negating the software's ability to prove or disprove that funds originated from known illegal sources. As David Carlisle concludes, "The use of highly anonymized VCs on encrypted dark web platforms raises the prospect that law enforcement may be operating with blind spots."[178]

However, even with the relative ease of use offered by these newer, more anonymous DVCs, coupled with the encryption and privacy available to users of network masking tools such as Tor, previous assessments cling to the fragile hope that TOs do not possess, and will not develop, the infrastructure or technological sophistication required to utilize DVCs on a meaningful scale. Unfortunately, as previously noted, TOs are measurably gaining technological sophistication while the level of sophistication required to utilize DVCs is simultaneously being lowered.

---

[174] Fanusie and Robinson, 7.

[175] Nathaniel Popper, "Zcash, a Harder-to-Trace Virtual Currency, Generates Price Frenzy," The New York Times, October 31, 2016, https://www.nytimes.com/2016/11/01/business/dealbook/zcash-a-harder-to-trace-virtual-currency-generates-price-frenzy.html.

[176] "Cryptocurrency Market Capitalizations."

[177] Kharif, "The Criminal Underworld Is Dropping Bitcoin for Another Currency."

[178] Carlisle, "Virtual Currencies and Financial Crime: Challenges and Opportunities," 16.

Ultimately, while law enforcement and security researchers have had some limited success in penetrating certain individual, stand-alone anonymizing services, as evidenced by de Balthasar and Hernandez-Castro's detailed efforts at defeating numerous tumblers, mixers, and privacy enhanced DVCs, these narrow-field, isolated successes do not mean that these kinds of anonymizing tools have been rendered impotent.[179] In fact, as recently as January 2018, at a workshop for financial investigators organized jointly by Europol, Interpol, and the Basel Institute on Governance, due to their broad effectiveness in anonymizing transactions, "which burdens the work of law enforcement agencies to detect and trace suspicious transactions,"[180] the need to take action specifically against mixers and tumblers was among the top four concerns. Additionally, this group showed great concern for the need to develop and apply regulations not only to DVC exchanges, as is currently the case in most jurisdictions, but for wallet providers as well.[181]

B. FURTHER RESEARCH AND INVESTIGATION ARE NEEDED

Recent developments in DVCs and the ecosystems that support them suggests that the primary pillars on which prior research has been built may have eroded sufficiently to warrant further and continued investigation of the potential threat posed by terrorist use of DVCs. The body of existing research regarding the threat of terrorists use of DVCs has determined that though it has become the payment method of choice for cybercriminals and many TCOs, researchers do not believe that TOs will leverage DVCs on an appreciable scale in the near future. To justify their determinations, the authors of this prior research focused on four primary reasons why TOs are more likely to exploit other less complicated, time tested methods of moving money. First, the authors assert that the overall size of the DVC market is too small to support the typical scale and liquidity required to reliably finance large scale terror operations. Second, the commercial contexts in which DVCs are

[179] de Balthasar and Hernandez - Castro, "An Analysis of Bitcoin Laundry Services."

[180] Europol, "Global Workshop for Financial Investigators on Detection, Investigation, Seizure and Confiscation of Cryptocurrencies," Europol Newsroom, January 26, 2018, https://www.europol.europa.eu/newsroom/news/global-workshop-for-financial-investigators-detection-investigation-seizure-and-confiscation-of-cryptocurrencies.

[181] Europol.

accepted are so limited that terrorists will be forced to make use of exchanges to acquire fiat currency for use in local transactions, exposing them to the scrutiny of AML/CFT regulations that registered DVC exchanges must currently operate under. Third, the most well-known and broadly accepted DVC, Bitcoin, has proven not to be as anonymous as terrorists require for successful evasion of detection and identification. Fourth and finally, TOs tend to lack the technological infrastructure and sophistication required to effectively utilize a strictly Internet-based currency.

As discussed in this and previous chapters, however, following recent developments on all four fronts, the rapidly growing utility of DVCs is not likely to go unnoticed by either legitimate or illicit communities hoping to capitalize on a faster, cheaper, more anonymous method to move funds globally. The homeland security enterprise, therefore, should not allow itself to be lulled into complacency or otherwise pacified by existing and already outdated research. Indeed, if LEAs let their guard down and inadvertently enable the use of DVC by TO on a scale that competes with cash or other readily available means of financing, such a development could present unique challenges for regulators, policy makers, and law enforcement because it offers the potential for an illicit funding network that can be very difficult to disrupt or even detect.

LIST OF REFERENCES

al-Munthir, Taqi'ul-Deen. "Bitcoin and the Charity of Violent Physical Struggle," July 2014. https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf.

Allen, Matthew. S.1241: Modernizing AML Laws to Combat Money Laundering and Terrorist Financing, § Judiciary (2017). https://www.dhs.gov/news/2017/11/28/written-testimony-ice-senate-committee-judiciary-hearing-titled-s1241-modernizing.

Balthasar, Thibault de, and Julio C. Hernandez-Castro. "An Analysis of Bitcoin Laundry Services." In *NordSec2017—Nordic Conference on Secure IT Systems, 8-10 Nov 2017, Tartu, Estonia* (2017). https://doi.org/10.1007/978-3-319-70290-2_18.

Baron, Joshua, Angela O'Mahony, David Manheim, and Cynthia Dion-Schwarz. *National Security Implications of Virtual Currency—Examining the Potential for Non-State Actor Deployment*. RAND Corporation, 2015. https://doi.org/10.7249/j.ctt19rmd78.

Blockchain. "Bitcoin Charts." Accessed May 12, 2018. https://blockchain.info/charts.

Bohloul, Pouyan, Gabriela Chambi, Sandra Fadel, Nicole S. Healy, Eunjung Park, and Christina Robertson. "Anti-Money Laundering and Counter-Terrorist Finance." *ABA/Section of International Law Year in Review* 51 (June 2017): 431–46.

Brill, Alan, and Lonnie Keene. "Cryptocurrencies: The Next Generation of Terrorist Financing?" *Defense Against Terrorism Review* 6, no. 1 (2014): 7–30.

Carlisle, David. "Cryptocurrencies and Terrorist Financing: A Risk, But Hold the Panic." Royal United Services Institute. www.rusi.org, March 2017. https://rusi.org/commentary/cryptocurrencies-and-terrorist-financing-risk-hold-panic.

Carlisle, David. "Virtual Currencies and Financial Crime: Challenges and Opportunities." London: Royal United Services Institute, March 2017. https://rusi.org/publication/occasional-papers/virtual-currencies-and-financial-crime-challenges-and-opportunities.

Coinatmradar.com. "Coin ATM Radar." Accessed May 13, 2018. https://coinatmradar.com/charts/.

CoinDesk. "Bitcoin Venture Capital." Accessed May 11, 2018. https://www.coindesk.com/bitcoin-venture-capital/.

CoinMarketCap. "Historical Snapshot." 2018. https://coinmarketcap.com/historical/.

Dark Web News. “Anonymity Tools.” Accessed May 20, 2018. https://darkwebnews.com/category/anonymity-tools/.

Dark Web News. “The Weird and Wonderful Deep Web.”. Accessed May 20, 2018. https://darkwebnews.com/deep-web/.

DEA. “2017 National Drug Threat Assessment.” Washington, DC: U.S. Department of Justice Drug Enforcement Administration, October 2017. https://www.dea.gov/docs/DIR-040-17_2017-NDTA.pdf.

DHS Science and Technology Directorate. “Cyber Security Division-Anonymous Networks and Currencies.” U.S. Department of Homeland Security, March 3, 2016. https://search.dhs.gov/search/docs?affiliate=dhs&dc=3634&query=cryptocurrency.

Dostov, Victor, and Pavel Shust. “Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?” *Journal of Financial Crime* 21, no. 3 (2014): 249–63. https://doi.org/10.1108/JFC-06-2013-0043.

Europol. “Global Workshop for Financial Investigators on Detection, Investigation, Seizure and Confiscation of Cryptocurrencies.” Europol Newsroom, January 26, 2018. https://www.europol.europa.eu/newsroom/news/global-workshop-for-financial-investigators-detection-investigation-seizure-and-confiscation-of-cryptocurrencies.

Evangeline, Ducas, and Alex Wilner. “The Security and Financial Implications of Blockchain Technologies: Regulating Emerging Technologies in Canada.” *International Journal* 72, no. 4 (2017): 538–62. https://doi.org/10.1177/0020702017741909.

Fanusie, Yaya, and Tom Robinson. “Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services.” The Foundation for Defense of Democracies Center on Sanctions and Illicit Finance, January 12, 2018. http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf.

FATF. “Emerging Terrorist Financing Risks.” Paris: FATF, 2015. www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.

FATF. “Guidance for a Risk-Based Approach to Virtual Currencies.” Paris: FATF, June 2015. http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.

FATF. “Virtual Currencies: Key Definitions and Potential AML/CFT Risks.” Paris: FATF, June 2014. http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html.

FinCEN. “Guidance: Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.” Guidance. U.S. Department of the Treasury, March 18, 2013. https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

Goldman, Zachary K., Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. “Terrorist Use of Virtual Currencies: Containing the Potential Threat.” Washington, DC: Center for a New American Security, May 2017. https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies.

Greenberg, Andy. “‘Dark Wallet’ Is About To Make Bitcoin Money Laundering Easier Than Ever.” Wired Magazine Online, April 29, 2014. https://www.wired.com/2014/04/dark-wallet/.

He, Dong, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, et al. “Virtual Currencies and Beyond: Initial Considerations.” Staff Discussion Notes. Washington, DC: International Monetary Fund, January 2016. http://www.imf.org/en/Publications/SPROLLs/Staff-Discussion-Notes?page=1.

He, Dong, Ross Leckow, Vikram Haksar, Tommaso Mancini-Griffoli, Nigel Jenkinson, Mikari Kashima, Tanai Khiaonarong, Celine Rochon, and Herve Tourpe. “Fintech and Financial Services: Initial Considerations.” Staff Discussion Notes. Washington, DC: International Monetary Fund, June 2017. http://www.imf.org/en/Publications/SPROLLs/Staff-Discussion-Notes.

Healy, Nicole S., and Emily N. Christiansen. “Anti-Money Laundering and Counter-Terrorist Finance.” *ABA/Section of International Law Year in Review* 50 (June 2016): 426–38.

Hertig, Alyssa. “Crypto Mobile Apps Security Report.” CoinDesk, November 29, 2017. https://www.coindesk.com/90-crypto-mobile-apps-trouble-security-report-claims/.

Homeland Security Committee. “Cash to Chaos: Dismantling ISIS’ Financial Infrastructure.” House Homeland Security Committee Majority Staff Report. Washington, DC, October 2016. https://homeland.house.gov/wp-content/uploads/2016/10/Dismantling-ISIS-Financial-Infrastructure.pdf.

HSSAI. “Risks and Threats of Cryptocurrencies.” Falls Church, VA: Homeland Security Studies and Analysis Institute, December 31, 2014.

Hughes, Sarah, and Stephen Middlebrook. “Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries.” *Yale Journal on Regulation* 32, no. 2 (2015): 495–559.

International Monetary Fund. “Factsheet: The IMF and the Fight Against Money Laundering and the Financing of Terrorism,” October 30, 2017. https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism.

Irwin, A.S.M., and G. Milad. “The Use of Crypto-Currencies in Funding Violent Jihad.” *Journal of Money Laundering Control* 19, no. 4 (2016): 407–25.

Kharif, Olga. “The Criminal Underworld Is Dropping Bitcoin for Another Currency.” Bloomberg, January 2, 2018. https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.

Kleiman, Jared A. “Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger US National Security and Welfare.” *National Security Law Brief* 4, no. 1 (2013): 59–78.

Kravets, Alexander. “Institutional Investors Will Bet Big on Cryptocurrencies in 2018.” Cointelegraph, January 18, 2018. https://cointelegraph.com/news/institutional-investors-will-bet-big-on-cryptocurrencies-in-2018.

Maruyama, Ellie, and Kelsey Hallahan. “Following the Money: A Primer on Terrorist Financing.” Washington, DC: Center for a New American Security, June 2017. https://www.cnas.org/publications/reports/following-the-money-1.

Middlebrook, Stephen T., and Sarah Jane Hughes. “Regulating Cryptocurrencies in the United States: Current Issues and Future Directions.” *William Mitchell Law Review* 40, no. 2 (2014): 813–48.

Odineca, Marija. “Bitcoin Growth In 2016? Show Us Your Numbers!” Cointelegraph, January 19, 2016. https://cointelegraph.com/news/bitcoin-growth-in-2016-show-us-your-numbers.

Popper, Nathaniel. “Zcash, a Harder-to-Trace Virtual Currency, Generates Price Frenzy.” The New York Times, October 31, 2016. https://www.nytimes.com/2016/11/01/business/dealbook/zcash-a-harder-to-trace-virtual-currency-generates-price-frenzy.html.

Popper, Nathaniel, and Rebecca R. Ruiz. “Authorities Shut Down Two Markets On Dark Net.” *The New York Times*. July 20, 2017, sec. A.

Seftel, Bennett. “Hawala Networks: The Paperless Trail of Terrorist Transactions.” Cipher Brief website. www.thecipherbrief.com, March 16, 2016. https://www.thecipherbrief.com/article/middle-east/hawala-networks-the-paperless-trail-of-terrorist-transactions.

Singh, Kavid. “The New Wild West: Preventing Money Laundering in the Bitcoin Network.” *Northwestern Journal of Technology and Intellectual Property* 13, no. 1 (2015): 37–64.

Tech Radar. “The Best Free Privacy Software 2018: Top Tools for Anonymous Browsing.” Accessed May 20, 2018. https://www.techradar.com/news/best-free-privacy-software.

Tor Project Inc. “About Tor.” Accessed May 20, 2018. https://www.torproject.org/about/overview.html.en.

U.S. Department of the Treasury. “National Money Laundering Risk Assessment.” Washington DC, June 12, 2015.

U.S. Department of the Treasury. “National Terrorist Financing Risk Assessment.” Washington DC, June 12, 2015.

West, Jeremy. “Largest Directory of Places to Spend Bitcoins.” SpendBitcoins. Accessed February 18, 2018. http://spendbitcoins.com/.

Worldpaymentreports.com. “Total Global Non-Cash Payment Volumes.” Accessed May 12, 2018. https://www.worldpaymentsreport.com/reports/noncash.

Young, Joseph. “Exponential Growth: Cryptocurrency Exchanges Are Adding 100,000+ Users Per Day.” Cointelegraph, January 7, 2018. https://cointelegraph.com/news/exponential-growth-cryptocurrency-exchanges-are-adding-100000-users-per-day.

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