CNA
ANALYSIS & SOLUTIONS

August 2019

Cryptocurrency: Implications for Special Operations Forces

Megan McBride and Zack Gold

With contributions by Jonathan Schroden and Lauren Frey

CRM-2019-U-020186-Final

Abstract

Cryptocurrencies are strictly digital currencies, are typically overseen by a decentralized peer-to-peer community, and are secured through cryptography. Cryptocurrencies have relative benefits for those who engage in illicit activity. This paper includes: (1) a detailed taxonomy and examples of nefarious activities involving cryptocurrencies, such as funding terrorist activity, money laundering, cybercrimes, and regulatory crimes; (2) a discussion of state-actor engagement in the cryptocurrency arena that explores Iranian, North Korean, Russian, and Venezuelan activity in skirting sanctions, mining cryptocurrencies, participating in exchange hacking and ransomware, and using cryptocurrencies to fund information operations; (3) analysis attempting to anticipate the mid-term future of the cryptocurrency ecosystem; and (4) the tactical and strategic challenges and opportunities of cryptocurrencies for US special operations forces.

Distribution

Approved for public release. Unlimited distribution.

Cover image credit: "SOFWERX Hosts Cyber Capability Expo." Master Sgt. Barry Loo, US Special Operations Command, Oct. 20, 2017.

Approved by: **August 2019**

Jonathan Schroden, Research Program Director
Special Operations Program
Center for Stability & Development
Strategy, Policy, Plans, and Programs Division (SP3)

Request additional copies of this document through inquiries@cna.org.

Executive Summary

In March 2018, Merriam-Webster announced that it would add the word *cryptocurrency* to its dictionary.[1] They noted that the word had first been used in 1990, and the definition they offered mentioned three core characteristics:

> Any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.[2]

To increase understanding of the potential implications of cryptocurrencies, in 2018 the Joint Special Operations University (JSOU) asked for research on the topic, "The evolution of cryptocurrency: future challenges and opportunities for SOF [special operations forces]."[3] CNA initiated this study in response to that call for research.

As we conducted our research, we identified a gap in knowledge of cryptocurrencies among US military and government personnel. To fill this knowledge gap, we simultaneously published a companion piece to this study: "Cryptocurrency: A Primer for Policy-Makers." Readers new to cryptocurrencies, or interested in increasing knowledge in a specific area, are directed to the companion primer for a more detailed exploration.

This document assumes a baseline understanding of cryptocurrencies, and focuses on the four questions that motivated our analysis of the implications of cryptocurrencies for SOF:

1. What operational considerations are relevant as SOF considers action in this arena?
2. What is the range of concerning activities in which cryptocurrencies have been observed?
3. What are the likely next evolution(s) in the cryptocurrency ecosystem?
4. What challenges and opportunities do cryptocurrencies present to SOF given the current (and potential future) state of affairs?

[1] "The Dictionary Just Got a Whole Lot Bigger," Merriam-Webster, Mar. 2018, https://www.merriam-webster.com/words-at-play/new-words-in-the-dictionary-march-2018.

[2] "Cryptocurrency," Merriam-Webster, https://www.merriam-webster.com/dictionary/cryptocurrency.

[3] Joint Special Operations University, *Special Operations Research Topics 2018 (Revised Edition for Academic Year 2019)*, (MacDill AFB, FL: JSOU Press, 2018), https://jsou.libguides.com/ld.php?content_id=41898487.

Operational considerations

The dynamic nature of the cryptocurrency ecosystem makes it difficult to measure market penetration, but proxy measures—including the proliferation of new cryptocurrencies, the global network of access points, and survey data on cryptocurrency adoption—suggest that the market has not yet fully matured. In addition, cryptocurrencies are more vulnerable than popular culture suggests. In a discussion of common myths about, and weaknesses of, cryptocurrencies, this paper addresses 51 percent attacks, exchange hacking, technical vulnerabilities, human error and avarice, anonymity, and immutability.

Observed activities

The global response to cryptocurrencies has been varied, but to date Venezuela is the only nation confirmed to have launched its own cryptocurrency. That said, other nations of strategic significance to the US—Russia, Iran, and North Korea—are also active in this space. Additionally, cryptocurrencies are popular among criminals engaged in a wide variety of illegitimate activities that we assess to fall into three broad categories: regulatory crimes, conventional crimes (including terrorist activity), and cybercrimes.

(Likely) futures of cryptocurrency

Predicting the future of cryptocurrency is a precarious undertaking, but we assess that two major variables will shape the future of cryptocurrencies: regulation and adoption. Each of these variables may either increase or stall, and our analysis explores the four possible permutations this would produce:

1. Scenario 1: Increased adoption and stalled regulation
2. Scenario 2: Increased adoption and increased regulation
3. Scenario 3: Stalled adoption and increased regulation
4. Scenario 4: Stalled adoption and stalled regulation (i.e., the status quo)

Implications for SOF

This paper concludes by considering the tactical and strategic challenges and opportunities of cryptocurrencies for SOF.

Challenges include:

- **Fractured regulatory environment.** The regulatory environment for cryptocurrencies is currently fractured, and is thus an obstacle to tracking and interdicting the financial activities of threat groups.

- **Evolution of technology (and nefarious behaviors).** Although government actors have increased their attention to the nefarious use of cryptocurrencies, the ecosystem is evolving at a faster rate than the government's capacity to stop this behavior.[4]
- **Lack of knowledge, training, and education.** It is not clear that any part of the US government—including the SOF enterprise—is prepared to fully address the national security challenges posed by cryptocurrencies. As a result, SOF should not assume that some other part of the US government will take care of these issues for them. This means that SOF will need to deepen their own knowledge, which should entail developing forms of education and training on cryptocurrencies and likely future trends, as well as actively folding lessons from ongoing operations that encounter cryptocurrencies into training for future missions.

Opportunities include:

- **Exploit vulnerable existing technology.** The existing technology is clearly vulnerable to exploitation, and SOF might mine information via at least two distinct vectors: cryptocurrency exchanges and user identities.
- **Collaborate with (or lead) new partners.** Because relatively few US government entities are knowledgeable about the cryptocurrency ecosystem, SOF have an opportunity to (1) collaborate with new partners, (2) maximize the collective ability to track activity, and (3) assume the role of knowledge leader.
- **Shape the future environment.** As the ecosystem evolves, SOF will have a chance to advocate for regulatory actions that might be helpful from an operational standpoint. Alternatively, SOF might argue against certain potential regulatory actions.
- **Exploit the vulnerabilities of cryptocurrencies as users.** Many features of cryptocurrencies make them particularly compelling for nefarious actors. Many of these same features, however, are also available to SOF (until regulatory frameworks and/or more restrictive authorities prevent such activities).

The challenges and opportunities that SOF will confront in this space vary considerably across the possible futures we outlined. However, our analysis shows that the lack of knowledge, training, and education is problematic regardless of how the future takes shape. It also shows that there is no future in which SOF is unable to exploit this technology (see the figure on the next page).

[4] Megan McBride and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

Likely futures of cryptocurrencies and potential implications for SOF

		Scenario 1: Increased adoption/ Stalled regulation	Scenario 2: Increased adoption/ Increased regulation	Scenario 3: Stalled adoption/ Increased regulation	Scenario 4: Stalled adoption/ Stalled regulation
Challenges	Fractured regulatory environment	↓	↔	↑	↔
	Evolution of technology (and nefarious behaviors)	↓	↔	↑	↔
	Lack of knowledge, training, and education	↓	↓	↓	↓
Opportunities	Exploitable existing technology	↑	↑	↔	↑
	Underdeveloped partnerships	↑	↑	↑	↑
	Malleable future environment	↔	↑	↑	↔
	Underexplored potential applications	↑	↔	↔	↑

Mid-term implications for SOF given its existing posture	
↓	Negative
↔	Neutral
↑	Positive

Source: CNA

At present, widespread expertise regarding cryptocurrencies is lacking in the US government, and more detailed analysis of the specific issues raised above is needed to fully explore and understand them. But there is also a clear path forward and thus little doubt that SOF should be looking at cryptocurrencies in more detail, to both mitigate the challenges and exploit the opportunities that we identified in our research.

Contents

Introduction

In March 2018, Merriam-Webster announced that it would add the word *cryptocurrency* to its dictionary.[5] They noted that the word had first been used in 1990, and the definition they offered mentioned three core characteristics:

> Any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.[6]

By the time the term was introduced into the *Merriam-Webster Dictionary*, it was already circulating through popular culture. It had been mentioned in multiple episodes of *The Simpsons* (as well as episodes of *CSI*, *Family Guy*, and *The Big Bang Theory*), it had made its appearance in major Hollywood films (including *Horrible Bosses 2* and *Deadpool*), and it had even appeared as an answer on an episode of *Jeopardy* (in 2014).[7] Moreover, in 2017 the value of one Bitcoin skyrocketed to more than $20,000 resulting in widespread media coverage and a virtual gold rush of new investors. Even people who did not join the frenzy became aware of the trend, and by 2018 nearly 80 percent of Americans reported having heard the term "Bitcoin."[8] Despite this familiarity, relatively few people actually understand the technology or its potential implications.

Similarly, the US Department of Defense (DOD) is aware of cryptocurrencies, but often lacks a thorough understanding of their potential implications in the national security space. To increase knowledge on this issue, in 2018 the Joint Special Operations University (JSOU) asked for research on the topic "The evolution of cryptocurrency: future challenges and opportunities for SOF [special operations forces]."[9]

---

[5] "The Dictionary Just Got a Whole Lot Bigger," Merriam-Webster, Mar. 2018, https://www.merriam-webster.com/words-at-play/new-words-in-the-dictionary-march-2018.

[6] "Cryptocurrency," Merriam-Webster, https://www.merriam-webster.com/dictionary/cryptocurrency.

[7] Julia Herbst, "A Comprehensive Guide to Crypto References in Pop Culture," *BREAKERMAG*, Oct. 29, 2018, https://breakermag.com/a-comprehensive-list-of-crypto-references-in-pop-culture/.

[8] Nikhilesh De, "Survey: Nearly 80% of Americans Have Heard of Bitcoin," Coindesk, Sept. 6, 2018, https://www.coindesk.com/survey-nearly-80-of-americans-have-heard-of-bitcoin.

[9] Joint Special Operations University, *Special Operations Research Topics 2018 (Revised Edition for Academic Year 2019)*, (MacDill AFB, FL: JSOU Press, 2018), https://jsou.libguides.com/ld.php?content_id=41898487.

This CNA-initiated study responds to that call for research by exploring the cryptocurrency ecosystem and helping SOF consider the implications of cryptocurrencies on its missions.

In the process of researching this topic, however, we realized that—with the exception of a few pockets of expertise—most US military and government personnel lack an understanding of how cryptocurrencies work. To fill this knowledge gap, we simultaneously published a companion piece to this study: "Cryptocurrency: A Primer for Policy-Makers." Readers new to cryptocurrencies, or interested in increasing knowledge in a specific area, are directed to the companion primer for a more detailed exploration. The primer contains: (1) a brief history of cryptocurrencies and the problems that cryptocurrencies were designed to solve; (2) an exploration of the key differences between cryptocurrencies and conventional currencies; (3) an explanation of how cryptocurrencies work that addresses mining, market volatility, transaction times, cryptocurrency use, wallets, and regulation; (4) a section on common myths and weaknesses of cryptocurrencies (that is also included in this document); and (5) recommendations to policy-makers of areas in which more research and analysis on the impact of cryptocurrency is required.

This document, by contrast, assumes a baseline understanding of cryptocurrencies. As such, it focuses on the four questions that motivated our analysis of the implications of cryptocurrencies for SOF:

1. What operational considerations are relevant as SOF considers action in this arena?
2. What is the range of concerning activities in which cryptocurrencies have been observed?
3. What are the likely next evolution(s) in the cryptocurrency ecosystem?
4. What challenges and opportunities do cryptocurrencies present to SOF given the current (and potential future) state of affairs?

We began this work with a literature review assessing the current state of cryptocurrencies (both technologically and financially), and then we interviewed government, military, and private industry experts engaged in daily work that touches on cryptocurrencies. With this information in hand, we identified and theorized a series of likely mid-term evolutions of the cryptocurrency ecosystem. Finally, we used the totality of this information—our assessment of the current state of affairs, and the potential futures we assessed to be most likely—to identify and explore potential implications for SOF mission areas.

In the course of our analysis, we found that the literature on cryptocurrencies was somewhat polarized, with some individuals clearly championing the technology and other individuals clearly denigrating its potential. We negotiated this landscape by avoiding these competing waves of enthusiasm and skepticism. We did this, in part, by taking pains to normalize cryptocurrencies whenever possible. And specifically, we found that cryptocurrencies could be normalized in three registers.

First, understanding the technology is not a prerequisite to taking advantage of its benefits. As one analyst thoughtfully argued, cryptocurrencies are the microwaves of the 21st century.[10] Just a few decades ago microwaves represented an incredible innovation. Very few people understood how the technology worked, and many expressed apprehension and uncertainty about heating their food via this unfamiliar piece of equipment. And yet today, microwaves are almost ubiquitous despite the fact that most people remain ignorant of how the technology works. People adopted microwaves because they became common and familiar, not because they became easier to understand. In other words, mastery of the technological features of cryptocurrency is critical in some arenas, but it is not necessary for widespread global adoption and it is not necessary for SOF exploitation.

Second, the types of illicit activities outlined below are not the result of the cryptocurrencies. The criminal (and terrorist) community is often at the forefront of adopting new technologies such as cryptocurrency.[11] However, cryptocurrencies have not revolutionized activity in this arena. Criminals were exchanging funds digitally—via video games, gift cards, online poker games, etc.—long before cryptocurrencies arrived on this scene.

Third, it is important to adapt our approach to cryptocurrency proportionately. Cryptocurrency is an innovation that facilitates and complicates the types of activities that nefarious state and non-state actors might undertake. It does not, however, fundamentally change the nature of criminal and terrorist activity. Given this, we should "avoid inventing duplicitous systems" when tackling this challenge and instead leverage the systems already in place.[12]

Based on these considerations, we approach cryptocurrencies as a potentially significant evolution, not as a game-changing revolution. Keeping this in mind, the remainder of this document offers readers the following:

- An explanation of the operational considerations relevant to cryptocurrencies (including a discussion of the different types of cryptocurrencies, the market penetration of cryptocurrencies, common myths about cryptocurrencies, and the relevant weaknesses of cryptocurrencies);
- An assessment of cryptocurrency activities likely of concern to SOF (including a summary of state-sponsored cryptocurrency activity, and a detailed taxonomy of nefarious criminal and terrorist cryptocurrency activity);

[10] Megan McBride and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

[11] Megan McBride, conversation with SOCOM personnel, Jan. 25, 2019.

[12] Chris Telley, "A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency," *Small Wars Journal*, https://smallwarsjournal.com/jrnl/art/coin-tsar-two-disruptive-sides-cryptocurrency.

- Analysis attempting to anticipate the mid-term future of the cryptocurrency ecosystem; and
- An exploration of the tactical and strategic challenges and opportunities that cryptocurrencies present for the SOF community.

We conclude the paper with a summary of our thoughts on the future of the cryptocurrency ecosystem and what this means for SOF.

Operational Considerations of Cryptocurrencies

In the sections below, we explore three operational considerations that inform our analysis of the potential implications of cryptocurrency for SOF. Specifically, we discuss cryptocurrency penetration, common myths about cryptocurrencies, and weaknesses of cryptocurrencies.

How widespread is cryptocurrency use?

The dynamic nature of the cryptocurrency ecosystem makes it difficult to measure market penetration. And because the actual number of cryptocurrencies is in flux (with some analysts speculating that over 800 cryptocurrencies are effectively dead), assessing the degree to which cryptocurrencies are going mainstream is difficult.[13] That said, some potential proxy measures—including the proliferation of new cryptocurrencies, the global network of access points, and survey data on cryptocurrency adoption—suggest a growing global market.

Different types of cryptocurrencies

As the first functional cryptocurrency, Bitcoin (BTC) is not only the most popular, but also the technological and functional standard for many other cryptocurrencies. Other popular cryptocurrencies include Ethereum (ETH), Ripple (XRP), Litecoin (LTC), Bitcoin Cash (BCH), Dash (DASH), and privacy coins including ZCash (ZEC) and Monero (XMR).[14]

Although these "altcoins" (so called because they are alternatives to Bitcoin) have core structures similar to that of Bitcoin, they have marketed themselves in part based on their notable differences from Bitcoin. For example, the Ether cryptocurrency is tied to the Ethereum blockchain, which itself functions as a distributed data storage service.[15] Ripple's popularity is driven by its use as an intermediary for international conventional currency transfers (Figure

[13] Arjun Kharpal, "Over 800 Cryptocurrencies Are Now Dead as Bitcoin Is 70 Percent off Its Record High," CNBC, Jul. 2, 2018, https://www.cnbc.com/2018/07/02/over-800-cryptocurrencies-are-now-dead-as-bitcoin-feels-pressure.html.

[14] See section "The myth of anonymity" for additional information on privacy coins.

[15] Steve Fiorillo, "What Is Cryptocurrency? Everything You Need to Know," The Street, Aug. 14, 2018, https://www.thestreet.com/investing/bitcoin/what-is-cryptocurrency-14679467.

1).[16] Bitcoin Cash, Dash, and Litecoin claim that their verification process is faster, making their transaction times shorter.[17] And the privacy coins ZCash and Monero emphasize personal anonymity.

Figure 1. Conventional currencies

*We use the phrase **conventional currencies** to refer to fiat currencies, which are currencies backed by the governments that issue them. Importantly, this type of currency is not tied to a physical good. The linen of a US dollar itself has no intrinsic value. The value of the US dollar is not tied to an intrinsically valuable commodity (such as gold), and the US dollar cannot be exchanged for gold at a fixed rate (as was the case when the US used the gold standard).*

Source: CNA.

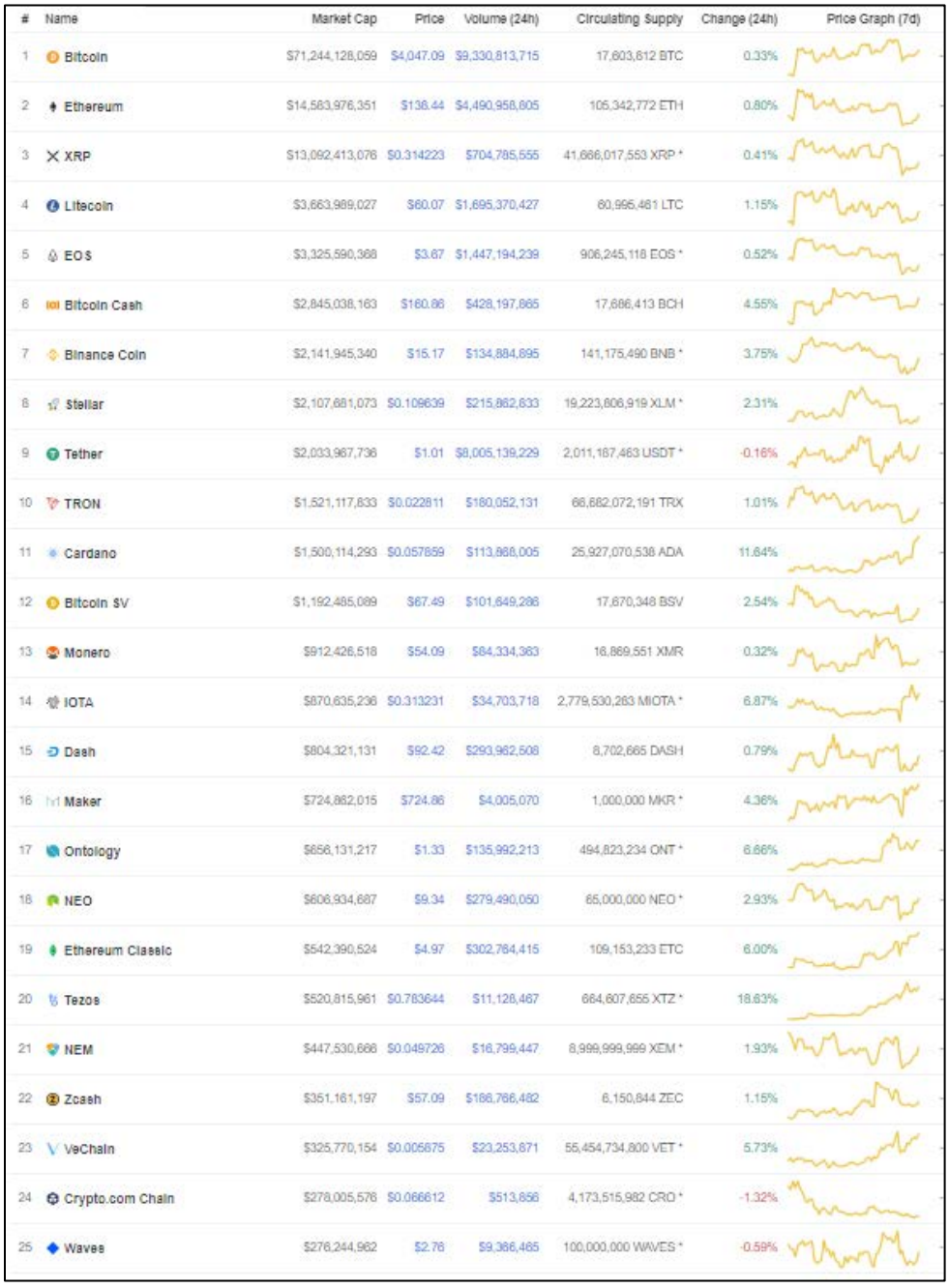
Importantly, although no cryptocurrency has approached the adoption rates or market capitalization of Bitcoin, each of the top 12 cryptocurrencies has a market capitalization in excess of $1 billion (Figure 2), suggesting that altcoins are an attractive alternative for users disillusioned with Bitcoin. That said, fluctuation is significant, so it is impossible to assess whether or not this growth will continue. In January 2018, the market capitalization of all cryptocurrencies reached a peak in excess of $830 billion, but by November 2018 it had dropped 80 percent to just over $135 billion.[18]

[16] Ibid.

[17] Ibid.; and Anne Sraders, "What Is Litecoin? What to Know in 2019," Dec. 18, 2018, https://www.thestreet.com/investing/what-is-litecoin-14813041.

[18] Ryan Browne, "Cryptocurrencies have shed almost $700 billion since January peak," CNBC, Nov. 23, 2018, https://www.cnbc.com/2018/11/23/cryptocurrencies-have-shed-almost-700-billion-since-january-peak.html.

Figure 2. Top 25 cryptocurrencies by market capitalization



#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$71,244,128,059	$4,047.09	$9,330,813,715	17,603,612 BTC	0.33%	
2	Ethereum	$14,563,976,351	$138.44	$4,490,958,605	105,342,772 ETH	0.80%	
3	XRP	$13,092,413,076	$0.314223	$704,785,555	41,666,017,553 XRP *	0.41%	
4	Litecoin	$3,663,989,027	$60.07	$1,695,370,427	60,996,461 LTC	1.15%	
5	EOS	$3,325,590,368	$3.67	$1,447,194,239	906,245,118 EOS *	0.52%	
6	Bitcoin Cash	$2,845,038,163	$160.86	$428,197,885	17,686,413 BCH	4.55%	
7	Binance Coin	$2,141,945,340	$15.17	$134,884,895	141,175,490 BNB *	3.75%	
8	Stellar	$2,107,681,073	$0.109639	$215,862,633	19,223,606,919 XLM *	2.31%	
9	Tether	$2,033,967,736	$1.01	$8,005,139,229	2,011,167,483 USDT *	-0.16%	
10	TRON	$1,521,117,833	$0.022811	$180,052,131	66,682,072,191 TRX	1.01%	
11	Cardano	$1,500,114,293	$0.057859	$113,868,005	25,927,070,538 ADA	11.64%	
12	Bitcoin SV	$1,192,485,089	$67.49	$101,649,286	17,670,348 BSV	2.54%	
13	Monero	$912,426,518	$54.09	$84,334,363	16,869,551 XMR	0.32%	
14	IOTA	$870,635,236	$0.313231	$34,703,718	2,779,530,283 MIOTA *	6.87%	
15	Dash	$804,321,131	$92.42	$293,962,508	8,702,665 DASH	0.79%	
16	Maker	$724,862,015	$724.86	$4,005,070	1,000,000 MKR *	4.36%	
17	Ontology	$656,131,217	$1.33	$135,992,213	494,823,234 ONT *	6.66%	
18	NEO	$606,934,687	$9.34	$279,490,050	65,000,000 NEO *	2.93%	
19	Ethereum Classic	$542,390,524	$4.97	$302,784,415	109,153,233 ETC	6.00%	
20	Tezos	$520,815,961	$0.783644	$11,128,467	664,607,655 XTZ *	18.63%	
21	NEM	$447,530,666	$0.049726	$16,799,447	8,999,999,999 XEM *	1.93%	
22	Zcash	$351,161,197	$57.09	$186,766,482	6,150,844 ZEC	1.15%	
23	VeChain	$325,770,154	$0.005875	$23,253,871	55,454,734,800 VET *	5.73%	
24	Crypto.com Chain	$278,005,576	$0.066612	$513,856	4,173,515,982 CRO *	-1.32%	
25	Waves	$276,244,962	$2.76	$9,366,465	100,000,000 WAVES *	-0.59%	

Source: "Top 100 Cryptocurrencies by Market Capitalization," CoinMarketCap, last accessed Mar. 22, 2019, https://coinmarketcap.com/.

Cryptocurrency market penetration

Determining how many people are using cryptocurrencies is complicated because individual users can have multiple wallets. As a result, the number of active wallets cannot be used as a proxy to determine how many people are using cryptocurrencies (similarly, the number of active bank accounts cannot be used to determine how many people are using the banking system). That said, the number of users is significant. By the beginning of 2019, almost 26 million wallets had made transactions on the Bitcoin blockchain since its creation 10 years earlier.[19]

Some analysts have attempted to gauge cryptocurrency use through surveys. This method is imperfect, but its results affirm that cryptocurrency use is significant. In the United States, for example, 8 percent of respondents told Statista that they own cryptocurrency, while data firm Dalia reported 9 percent.[20] Another survey by Finder.com similarly found that 8 percent of respondents in the United States owned cryptocurrency. It also provided more granular respondent data suggesting that more than 5 percent owned Bitcoin, 1.8 percent owned Ethereum, and less than 1 percent owned Bitcoin Cash and Ripple.[21]

Other countries—perhaps those where the advantages of cryptocurrency are more compelling than the disadvantages—report much higher cryptocurrency use. Turkey had the highest reported usage at 18 percent, Romania had 12 percent, Japan had 11 percent, Poland had 11 percent, and Spain had 10 percent.[22] Despite popular reporting on the cryptocurrency craze in

[19] ICO Manager, "How Many People Own Cryptocurrency," ICO Making, Jan. 14, 2019, https://icomaking.com/how-many-people-own-cryptocurrency/.

[20] Rytis Jakubauskas, "How Many People Actually Own Cryptocurrency?" Dalia, May 11, 2018, https://daliaresearch.com/blog-cryptocurrency-ownership/; and Raynor de Best, "How Many Consumers Own Cryptocurrency?," Statista, Aug. 20, 2018, https://www.statista.com/chart/15137/how-many-consumers-own-cryptocurrency/.

[21] Dieter Holger, "Over 16 Million Americans Now Own Cryptocurrency, Survey Finds," Bitcoinist.com, Mar. 19, 2018, https://bitcoinist.com/16-million-americans-cryptocurrency/. Importantly, some respondents reported owning multiple cryptocurrencies.

[22] Rytis Jakubauskas, "How Many People Actually Own Cryptocurrency?" Dalia, May 11, 2018, https://daliaresearch.com/blog-cryptocurrency-ownership/; and Raynor de Best, "How Many Consumers Own Cryptocurrency?," Statista, Aug. 20, 2018, https://www.statista.com/chart/15137/how-many-consumers-own-cryptocurrency/.

South Korea,[23] Dalia found that only 6 percent of respondents in that country reported owning any.[24]

Ownership rates do not, however, tell the entire story. Another way to look at market penetration in a given location is to examine BTM (an ATM for cryptocurrencies) locations. Over 4,000 BTMs are estimated to be in operation worldwide. Although most of these machines are in the US, global distribution is considerable (Figure 3).

Putting these figures in context, however, significantly changes the picture of cryptocurrency ownership. A 2017 report estimated there are between 2.9 million and 5.8 million active users of cryptocurrency, which suggests significant use.[25] However, some 640 million people worldwide carry MasterCard, and over a billion are active Visa users.[26] Paypal and its Venmo service counted 235 million active users in early 2018.[27] Similarly, there are an estimated 3.5 million conventional currency ATMs throughout the world.[28]

Moreover, none of these numbers differentiate between investors and consumers. As a result, these statistics do not reflect what percentage of owners are purchasing cryptocurrency as part of a long-term investment strategy, and what percentage of are using cryptocurrencies as currencies (in either legal or illegal activities).

[23] Su-Hyun Lee and Nathaniel Popper, "In South Korea, the Virtual Currency Boom Hits Home," *New York Times*, Dec. 3, 2017, https://www.nytimes.com/2017/12/03/technology/virtual-currency-south-korea.html.

[24] Rytis Jakubauskas, "How Many People Actually Own Cryptocurrency?" Dalia, May 11, 2018, https://daliaresearch.com/blog-cryptocurrency-ownership/.

[25] Garrick Hileman and Michael Rauchs, "Global Cryptocurrency Benchmarking Study," University of Cambridge Judge Business School Centre for Alternative Finance, 2017, https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency/.

[26] Alex Lielacher, "How Many People Use Bitcoin in 2019?" Bitcoin Market Journal, Feb. 11, 2018, https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/.

[27] "PayPal Adds 8M Active Users, Grows Mobile Volume 52 Percent," PYMNTS.com, Apr. 26, 2018, https://www.pymnts.com/earnings/2018/paypal-earnings-mobile-volume-user-growth-barclays/.

[28] "What Is a Cryptocurrency ATM?" CoinCodex, June 2018, https://coincodex.com/article/1965/what-is-a-cryptocurrency-atm/.

Figure 3. Bitcoin ATMs by country

Source: "Bitcoin ATMs by Country," Coin ATM Radar, https://coinatmradar.com/countries/.

Weaknesses of cryptocurrencies

Beyond the one-off theft and hacking of individual wallets, cryptocurrencies are vulnerable to threats including, but not limited to, the 51 percent problem, exchange hacking and technical vulnerabilities, and human error or avarice.

The 51 percent problem is a long-known concern that has become more pressing in recent years, since multiple such attacks have occurred. A 51 percent attack takes advantage of the fact that anyone can participate in the work of mining. In this type of an attack, a single individual or group gains control of 51 percent of the network's computing power (i.e., a single individual or group controls 51 percent of the nodes that maintain the blockchain).[29] This group then effectively controls the decentralized ledger and consequently can (a) engage in double-spending by interfering with the validation of transactions, or (b) block other nodes from mining the cryptocurrency.[30] Critically, one analyst noted that the threat was actually more significant than the name suggests and that (for technical reasons) a 51 percent attack could be orchestrated successfully with control of merely 30 percent of the network's nodes.[31]

Some research suggests that Bitcoin itself is relatively safe from a 51 percent attack, given the size of its mining network, but other cryptocurrencies (including Ethereum Classic, MonaCoin, Bitcoin Gold, ZenCash, Verge, and Litecoin Cash) have been attacked in this way over the last year.[32] Moving forward, it seems likely that such attacks will continue to occur—particularly given that this vulnerability is an inherent part of the system for most cryptocurrencies. As Litecoin founder Charlie Lee noted, "By definition, a decentralized cryptocurrency must be susceptible to 51 percent attacks."[33]

---

[29] As noted above, mining is an energy-intensive process that is effectively cost-prohibitive to the individual user. The energy necessary to control 51 percent of a network's computing power is thus likely to be high, and so attacks are likely to occur only when the potential benefit from the attack outweighs the costs associated with launching the attack. This will be less of an obstacle as the cost of computing power decreases, and in the meantime recent research suggests that nefarious actors might *rent* the resources to launch the attack. This approach would presumably make such attacks easier to execute and more likely to happen. Source: Alyssa Hertig, "Blockchain Feared 51% Attack Now Becoming Regular," *Coindesk*, June 8, 2018, https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular.

[30] Jake Frankenfield, ed., "51% Attack," Investopedia, Feb. 7, 2019, https://www.investopedia.com/terms/1/51-attack.asp.

[31] Megan McBride, conversation with industry expert, Feb. 28, 2019.

[32] Osato Avan-Nomayo, "Bitcoin 51% Attack Is Unrealistic, New Study Concludes," *Bitcoinist*, Nov. 26, 2018, https://bitcoinist.com/bitcoin-51-percent-attack-study/; and Hertig, "Blockchain 51% Attack."

[33] Gareth Jenkinson, "Ethereum Classic 51% Attack — The Reality of Proof-of-Work," *Cointelegraph*, Jan. 10, 2019, https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work.

Exchange hacking and technical vulnerabilities are also serious concerns for most cryptocurrency users. In the past few years, hackers have exploited vulnerabilities in exchange platforms to steal vast numbers of private keys—in effect, stealing control of the cryptocurrencies in those wallets. Most infamously, the popular exchange Mt. Gox filed for bankruptcy in February 2014 after losing 850,000 Bitcoins (valued around $500 million at the time) in such an attack.[34]

Peer-to-peer software also is incredibly vulnerable to certain types of malware. The speed with which these malicious programs can spread across the network makes cryptocurrencies prime targets for hackers.[35] Further, malware on one cryptocurrency network can steal other types of cryptocurrencies that it encounters on a user's computer.[36] For example, a thief could deploy malware through the Bitcoin network, but steal the Ethereum or Litecoin that are also held by those Bitcoin users.

Similarly troublesome in this category are coding errors that introduce vulnerabilities into the system. One notable example comes in the form of a bug in code written by Gavin Wood, a cryptocurrency expert and one of Ethereum's founders. The bug disabled access to a large number of Ethereum wallets, irreversibly freezing $150 million worth of the cryptocurrency.[37]

Human error or avarice is a universal vulnerability that is impossible to ignore. Cryptocurrencies can be permanently lost if an individual loses the ability to access the wallet in which the cryptocurrencies are stored, but this vulnerability is compounded at the exchange level. As one example, in December 2018 the CEO of QuadrigaCX died unexpectedly and did not leave the executor of his estate (his wife) the information necessary to access his cryptocurrency wallets. As a result, the nearly $250 million in cryptocurrencies that the CEO was holding for clients became (perhaps permanently) inaccessible.[38] A still open question in the case is whether or not the CEO simply failed to ensure that this information would be passed along (i.e., human error) or faked his own death in order to steal the funds (i.e., human

[34] Charlie Osborne, "The Mt. Gox Bitcoin Debacle: Bankruptcy Filed, Customer Bitcoin Lost," *ZDNet*, Feb. 25, 2014, https://www.zdnet.com/article/the-mt-gox-bitcoin-debacle-bankruptcy-filed-customer-bitcoin-lost/.

[35] Weaver, "Inside Risks of Cryptocurrencies," 4.

[36] Ibid.

[37] Ibid.

[38] Yvette Brend, "Sudden Death of Cryptocurrency Leader Sends Quadriga into Tailspin, Panicking Clients," *CBC News*, Feb. 4, 2019, https://www.cbc.ca/news/canada/british-columbia/quadriga-cryptocurrency-bitcoin-exchange-gerald-cotten-death-india-1.5002955.

avarice). Although the QuadrigaCX case has a number of curious details and is still being investigated, it clearly brings attention to such vulnerabilities.[39]

Common myths about cryptocurrencies

Perhaps surprisingly, some of the alleged strengths of cryptocurrencies are in fact misperceptions about how they operate. Below we discuss the two most prominent myths about cryptocurrencies.

The myth of anonymity

One of the major appeals of cryptocurrency is that it allegedly allows for the anonymous transfer and movement of funds. Obviously, the in-person exchange of cash *can* also be anonymous, but it is widely believed that *all* cryptocurrency transactions are anonymous.

Cryptocurrency transactions appear to be anonymous insofar as no personally identifying information is included in a transaction record. That said, cryptocurrencies are actually "pseudonymous" (not anonymous). By *pseudonymous* we mean that holders of cryptocurrencies are known by their public keys (much like an author might publish under a pseudonym). Cryptocurrency transactions offer the illusion of anonymity because real names and true identification are not required. However, every transaction made by every user is permanently maintained—identified by their public keys—on the blockchain. Thus, if a user's true identity is ever linked to his public key, it would be possible to trace the entirety of his engagement with the cryptocurrency (just as if an author's pen name is ever linked to her real name, all of the books she wrote under the pseudonym would be linked to her true identity).[40]

Users have deployed a number of techniques to increase their anonymity (e.g., obscuring their IP addresses or using a new public key for each transaction). Even in these cases, the public and transparent nature of the blockchain means that an incredible amount of information is permanently available. As one example, a user might generate a new public key for each transaction, much as a conventional criminal might receive funds via a dozen different post office boxes. Unlike P.O. boxes, though, the contents and records of Bitcoin accounts are public.

[39] An investigation by Ernst & Young found that the cryptocurrencies alleged to be held by QuadrigaCX were not in the company's known wallets. See: Elizabeth Pillon and Lee Nicholson, "First Report of the Monitor," *Supreme Court of Nova Scotia Hfx, No. 484742*, Feb. 12, 2019, https://www.scribd.com/document/399507173/EY-QuadrigaCX-Report.

[40] "Bitcoin Anonymity – Is Bitcoin Anonymous?" Buy Bitcoin Worldwide, accessed May 2, 2019, https://www.buybitcoinworldwide.com/anonymity/; and "Is Bitcoin Anonymous?" *Bitcoin Magazine*, accessed May 2, 2019, https://bitcoinmagazine.com/guides/bitcoin-anonymous/.

If the user then sends these funds to someone else in a single transaction, all of the "addresses" would be publicly linked (Figure 4).

Figure 4. Example of cryptocurrency transactions and social network analysis

Tracking Bitcoin transactions *– Lucy is planning to receive 10 Bitcoins from a dozen colleagues, and she has each colleague send the money to a different wallet (i.e., a different public key).*

In aggregate, Lucy now has 120 Bitcoins that she needs to send to Eli. In submitting this transfer to Eli, though, she effectively links the transactions together. An analyst tracking Lucy's online activity would become aware not only of an additional 12 public keys that she was using, but also of the 12 colleagues who sent funds to her in the first place.

Lucy's real-world identity might still be obscured at this point, but a robust understanding of her social network and activity would be emerging.

Source: CNA.

In fact, recent analysis clearly demonstrates the ways in which Bitcoin transactions can be de-anonymized. In 2018, researchers in Qatar published a paper describing how they exploited information on Bitcoin's blockchain to unmask the identities of users of hidden services such as Silk Road, The Pirate Bay, and WikiLeaks—in some cases the researchers were able to uncover personally identifying information.[41] The researchers concluded: "Bitcoin addresses should always be considered exploitable."[42]

One response to the desire for increased anonymity is the creation of so-called "privacy coins" (i.e., cryptocurrencies that prioritize privacy), which have become popular with users who want more anonymity in their cryptocurrency transactions. In a cryptocurrency such as

[41] Husam Al Jawaheri, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad, "When a Small Leak Sinks a Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis," Cornell University's arXiv.org archive, Apr. 11, 2018, https://arxiv.org/pdf/1801.07501.pdf, 1-2.

[42] Ibid., 1.

Bitcoin, the user's personal information is not shared, but her wallet and all her transactions are publicly displayed on the cryptocurrency blockchain.[43] Privacy coins—including Zcash and Monero—mask individual transactions, which blocks a public accounting of transaction amounts and the wallets involved (though the blockchain maintains many of its core features, and thus still protects against double-spending without introducing a third-party authority).[44]

The myth of immutability

Cryptocurrency entrepreneurs and advocates often highlight the immutability of the blockchain as both a defining feature and one of its most valuable qualities. However, just as a nefarious 51 (or perhaps just 30) percent of a network's nodes can collaborate to hijack the blockchain and steal cryptocurrency, a well-intentioned controlling percentage can manipulate the allegedly "immutable" ledger. As one example, in 2016, a majority of Ethereum miners agreed to reverse a hack of their system—fixing the vulnerability a hacker exploited and "editing" the blockchain to return to its pre-hack state.[45] In short, the blockchain is only notionally immutable. In reality, it can be edited under a number of circumstances—both nefarious and benevolent.

[43] Lucas Nuzzi, "ZEC: Unmatched Privacy in a Public Blockchain," *Medium*, Sept. 17, 2018, https://medium.com/digitalassetresearch/zec-best-in-class-privacy-in-a-public-blockchain-1df2a3728739. See "Cryptocurrency: A Primer for Policy-Makers" for a discussion of double-spending and third party authority.

[44] Ibid.; and Steve Fiorillo, "What Is Cryptocurrency? Everything You Need to Know," *The Street*, Aug. 14, 2018, https://www.thestreet.com/investing/bitcoin/what-is-cryptocurrency-14679467.

[45] Nicholas Weaver, "Inside Risks of Cryptocurrencies," *Viewpoints: Communications of the ACM* 61, no. 6 (June 2018), https://www1.icsi.berkeley.edu/~nweaver/papers/cryptorisks.pdf, 5.

Cryptocurrency Activity of Concern

State-sponsored activity

The global response to cryptocurrencies has been varied. Some nations have banned their use, others have implemented restrictions on exchanges, and others have created regulations to facilitate widespread and transparent operation.[46] The least common response is the creation of a government-backed cryptocurrency, and to date only Venezuela is confirmed to have taken this path. That said, other nations of strategic significance to the US —Russia, Iran, and North Korea—are also active in this space.

Venezuela

In February 2018, the Venezuelan government officially launched a cryptocurrency called the Petro. In a white paper posted on a new website for the Petro, the government outlined how the cryptocurrency would work.[47] Venezuela claimed that it would back the Petro with 5 billion barrels of petroleum reserves.[48] The government planned to fix the number of Petros at 100 million and hold 17.6 percent of them; 82.4 million would be available during a pre-sale and a public sale.[49] Once the initial distribution was complete, consumers would be able to purchase Petros through cryptocurrency exchanges.[50] The Venezuelan government called the Petro "The first crypto-asset issued and guaranteed by a sovereign state."[51] In this regard, the Petro would be fundamentally different from most existing cryptocurrencies. As noted in *Bloomberg*:

[46] For a regularly updated list of the status of cryptocurrencies globally, including information on where cryptocurrencies are banned, see "Digital Currencies: International Actions and Regulations," maintained by the international law firm Perkins Coie.

"Digital Currencies: International Actions and Regulations," Perkins Coie, updated May 2019, accessed May 1, 2019, https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html.

[47] "El Petro," Gobiemo Bolivariana de Venezuela, 2018, https://petro.gob.ve/index.html.

[48] Brian Ellsworth, "Special Report: In Venezuela, New Cryptocurrency Is Nowhere to Be Found," Reuters, Aug. 30, 2018, https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U.

[49] Eric Lam, "Here's What Maduro Has Said of Venezuela's Petro Cryptocurrency," *Bloomberg*, Aug. 20, 2018, https://www.bloomberg.com/news/articles/2018-08-20/here-s-what-maduro-has-said-of-venezuela-s-petro-cryptocurrency.

[50] Ibid.

[51] "El Petro," Gobiemo Bolivariana de Venezuela, 2018, https://petro.gob.ve/index.html.

"Cryptocurrencies were originally designed to be decentralized and free from third-party and governmental control, the Petro is neither."[52]

One month after the announcement, Venezuelan President Nicolas Maduro claimed his government had received $5 billion worth of "offers" for Petros from international buyers.[53] However, subsequent reports on the Petro have been contradictory. After the initial pre-sale phase, Maduro claimed that Venezuela had raised $3.3 billion but a few months later, Reuters reported that a cabinet minister involved in the effort had stated that the technology was still in development and that "nobody has been able to make use of the Petro…nor have any resources been received."[54]

Maduro made another public announcement—and Venezuela released another white paper—in October 2018. The framework outlined in the new white paper changed the technological structure of the network (it would no longer run on the Ethereum network), the economic backing of the cryptocurrency (it would now be backed by oil, gold, diamond, and iron reserves), and the release plans of the Petros themselves (shifting it from a non-minable to a minable coin).[55] Maduro also announced a plan to sell its oil in Petros—to "free us from a currency that the elite of Washington uses" —beginning in 2019.[56] Perhaps more interesting, Venezuela began to sell Petros via a government website and require citizens to use Petros to purchase passports around this time.[57]

Despite these developments, the situation today is unclear. Recent reporting indicates that the Petro was a live cryptocurrency as of early 2019, but evidence of activity on the global market is limited.[58] Meanwhile, a February 2019 report (published by a South American cryptocurrency exchange) questioned the legitimacy of the Petro, concluding that the cryptocurrency is fraudulent and that "there are also signs of money laundering in the public

[52] Eric Lam, "Here's What Maduro Has Said of Venezuela's Petro Cryptocurrency," *Bloomberg*, Aug. 20, 2018, https://www.bloomberg.com/news/articles/2018-08-20/here-s-what-maduro-has-said-of-venezuela-s-petro-cryptocurrency.

[53] Ibid.

[54] Ibid.; and Brian Ellsworth, "Special Report: In Venezuela, New Cryptocurrency Is Nowhere to Be Found," Reuters, Aug. 30, 2018, https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U.

[55] Kevin Helms, "Venezuela Makes Petro Crypto a National Currency, Publishes New Whitepaper," News: Bitcoin.com, Oct. 4, 2018, https://news.bitcoin.com/venezuela-petro-new-whitepaper/.

[56] Yogita Khatri, "Venezuela to Sell Oil for Petro Cryptocurrency, Says Maduro," Coindesk, Dec. 7, 2018, https://www.coindesk.com/venezuela-to-sell-oil-for-petro-cryptocurrency-in-2019-says-maduro.

[57] Ibid.

[58] Francisco Memoria, "Turns Out Venezuela's Oil-Backed Petro Cryptocurrency Is Real After All," CCN, Jan. 28, 2019, https://www.ccn.com/turns-out-venezuelas-oil-backed-petro-cryptocurrency-is-real-after-all.

offer of Petro."[59] This analysis was not wholly unexpected, since others had previously speculated that the Petro would be a vehicle for Venezuela to access foreign currencies, obtain goods and services globally, sidestep financial sanctions imposed by the US, and conduct covert transactions that would otherwise be seen by the US or regulators in a traditional payment system.[60]

Russia

Long-standing rumors regarding Russia's creation of a cryptocurrency continue to circulate, but some evidence shows that the country may be moving in this direction.[61] In February 2019, a Kremlin website post outlined an order for the State Duma to adopt "federal laws aimed at the development of the digital economy."[62] Around the same time, it was reported that a member of the State Duma's Committee on Economic Policy had claimed that, unlike the crypto-averse Russian Central Bank, the state was pursuing a regulatory framework that would be hospitable to the integration of cryptocurrency.[63] Some reporting indicated that the legislation currently being debated would lay the foundation for the launch of an oil-backed Russian cryptocurrency.[64] Former Energy Minister Igor Yusufov allegedly claimed that such a cryptocurrency would permit Russia to "avoid costs associated with the unpredictability in the exchange rate of the US dollar, trade restrictions, [and] currency exchange commissions."[65]

[59] Chayanika Deka, "Venezuela's Petro: Fresh Trouble Surfaced as Report Suggests 'Conclusive Evidence' of Money Laundering," AMBCRYPTO, Feb. 27, 2019, https://ambcrypto.com/venezuelas-petro-fresh-trouble-surfaces-as-report-suggests-conclusive-evidence-of-money-laundering/.

[60] "Russia and Venezuela Plan Cryptocurrencies," *Weekend Edition Saturday* and National Public Radio, Jan. 6, 2018, https://www.npr.org/2018/01/06/576197773/russia-and-venezuela-plan-cryptocurrencies; Eric Lam, "Here's What Maduro Has Said of Venezuela's Petro Cryptocurrency," *Bloomberg*, Aug. 20, 2018, https://www.bloomberg.com/news/articles/2018-08-20/here-s-what-maduro-has-said-of-venezuela-s-petro-cryptocurrency.

[61] Kenneth Rapoza, "Will Russia Make Any Waves In Crypto This Year?," *Forbes*, Jan. 2, 2019, https://www.forbes.com/sites/kenrapoza/2019/01/02/will-russia-make-any-waves-in-crypto-this-year/#29f203684271.

[62] Kevin Helms, "Putin's Order: Russia to Adopt Crypto Regulation by July," Bitcoin.com, Feb. 28, 2019, https://news.bitcoin.com/putins-order-russia-cryptocurrency-regulation/.

[63] Yashu Gola, "Russia to Regulate Crypto While Launching its Own Oil-Backed Cryptocurrency," CCN, Feb. 24, 2019, https://www.ccn.com/russia-regulate-cryptop-with-a-keen-eye-on-oil-backed-digital-currency.

[64] Georgi Georgiev, "Russia: Oil-Backed Cryptocurrency in 'Final Stage of Development'," Bitcoinist, Feb. 22, 2019, https://bitcoinist.com/russia-oil-cryptocurrency-law/.

[65] Ibid.

That said, Putin issued a similar order in 2017 and three bills on cryptocurrency were filed with the State Duma in 2018.[66] Thus, these early 2019 activities do not necessarily indicate a major change in policy (or the imminent launch of a Russian cryptocurrency).

Importantly, though, Russia could exploit the cryptocurrency ecosystem without launching its own coin. A brief discussion of this possibility can be found below, in the section "Cybercrimes."

Iran

The appeal of locating mining operations in countries with inexpensive electricity is driven by a desire to increase profitability. Miners profit when the cost of producing the coins (including fees) is lower than the value of the coins mined.[67] The cost of electricity is a critical component in this calculus. One study found that the cost of mining a single Bitcoin in South Korea (the most expensive country) would be $26,170, while the cost of mining a single Bitcoin in Venezuela (the least expensive country) would be $531.[68] In other words, the profit margins on mining are significantly impacted by electricity costs. As a result, states with inexpensive electricity are particularly appealing to miners hoping to increase profit. And Iran's electricity is relatively inexpensive (partly because of US sanctions devaluing the rial), with its cost per Bitcoin estimated to fall in the bottom 20 percent globally.[69]

That said, moving operations into Iran is not seamless for Bitcoin miners. Individuals and small businesses are working to recruit foreign investors, and reporting suggests that miners from China, Spain, Ukraine, Armenia, and France have expressed interest.[70] But even though an Iranian operation has some appeal for small mining operations, mining giants appear to be staying away.[71] Iran's complicated border security—making individual transit and the shipping of equipment challenging—and US economic sanctions are deterring these larger-scale enterprises from investing in the region.[72]

---

[66] Kevin Helms, "Putin's Order: Russia to Adopt Crypto Regulation by July," Bitcoin.com, Feb. 28, 2019, https://news.bitcoin.com/putins-order-russia-cryptocurrency-regulation/.

[67] Wolfe Zhao, "Cheap Power Is Luring Battered Bitcoin Miners to Iran," Coindesk, Dec. 12, 2018, https://www.coindesk.com/cheap-power-lures-crypto-miners-to-iran-but-its-not-as-easy-as-it-sounds.

[68] "Bitcoin Mining Costs Throughout the World," *Elite Fixtures* (blog), Feb. 26, 2018, https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/.

[69] Zhao, "Cheap Power Is Luring Battered Bitcoin Miners to Iran" and "Bitcoin Mining Costs Throughout the World."

[70] Zhao, "Cheap Power Is Luring Battered Bitcoin Miners to Iran."

[71] Ibid.

[72] Ibid.

Perhaps more intriguing is the Iranian government's foray into cryptocurrency. In 2018, it was reported that the Iranian government was exploring the possibility of issuing its own cryptocurrency as a means to circumvent US sanctions. In response, bills calling for investigation into—and sanctioning of those providing aid to—Iranian cryptocurrency efforts were introduced in both the US House and Senate.[73]

In early 2019, the Central Bank of Iran released an early draft of a new regulatory framework that would replace the existing blanket ban on cryptocurrencies with a slightly more permissive model.[74] A week later, an Iranian cryptocurrency called PayMon (or Crypto-Rial) —backed by gold and supported by four major Iranian banks—was announced.[75] Additional reporting indicated that Iran was actively negotiating with Switzerland, South Africa, France, the UK, Russia, Austria, Germany, and Bosnia about the possibility of shifting transactions to cryptocurrency.[76] Though no coins have been issued to date (and some analysts are skeptical about its viability), Iran is poised to move in this direction in the relatively near future.

North Korea

North Korea is confirmed to have been active in the cryptocurrency space—largely motivated by a desire to avoid crippling international sanctions and to fund its weapons of mass destruction (WMD) program—since at least early 2017. The scope of their activities, however, has been somewhat less clear.[77] An early move into this space was the WannaCry 2.0 ransomware attack, which directed hundreds of victims to send funds to a Bitcoin address in order to regain access to their computers.[78] Though the gains from these attacks were modest

[73] Zack Seward, "US Lawmakers Seek Sanctions Against Iran's Cryptocurrency Efforts," Coindesk, December 21, 2018, https://www.coindesk.com/us-lawmakers-seek-sanctions-against-irans-cryptocurrency-efforts.

[74] Maziar Motamedi, "Iran's central bank issues draft rules on cryptocurrency," Aljazeera, January 29, 2019, https://www.aljazeera.com/news/2019/01/iran-central-bank-issues-draft-rules-cryptocurrency-190129051653656.html.

[75] Yogita Khatri, "Gold-Backed Cryptocurrencies Launched by Iranian Banks: Report," Coindesk, February 5, 2019, https://www.coindesk.com/gold-backed-cryptocurrency-launched-by-iranian-banks-report.

[76] Adrian Zmudzinski, "Four Iranian Banks Support Gold-Backed Cryptocurrency," Cointelegraph, February 5, 2019, https://cointelegraph.com/news/four-iranian-banks-support-gold-backed-cryptocurrency.

[77] David Carlisle and Kayla Izenman, "Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia," Royal United Services Institute, Apr. 2019, https://rusi.org/sites/default/files/20190412_closing_the_crypto_gap_web.pdf, accessed Apr. 26, 2019; and William Suburg, "North Korea Launched Cryptocurrency Attacks in Response to Sanctions, FBI Says," Cointelegraph, May 30, 2019, https://cointelegraph.com/news/north-korea-launched-cryptocurrency-attacks-in-response-to-sanctions-says-fbi.

[78] Ibid.

(an estimated $144,000), this move was merely the beginning.[79] In the past two years, the country seems to have simultaneously engaged in large-scale hacking to steal cryptocurrency and a robust mining operation to earn it.

In the first category, North Korea has been "accused of employing more than 7,000 hackers around the world focused on stealing cryptocurrencies, which has yielded tens of millions of dollars."[80] Since 2017, the country has been linked to a half dozen hacks yielding approximately $545 to $735 million in funds (the precise number is difficult to determine given fluctuations in value over time; it also is not clear how successfully North Korea has converted these yields into conventional currencies).[81]

In the second category, analysis suggests that the country has made $15 to $200 million through cryptocurrency mining operations.[82] Moreover, it has engaged in crypto-jacking on at least two confirmed occasions to amplify its mining activities (see the section "Cybercrimes" for a more detailed explanation).[83]

Illegitimate applications

Beyond their legitimate uses, cryptocurrencies have become (and arguably were first) popular among criminals and criminal organizations engaged in illegitimate activities. As one expert noted, the criminal community is an adopting community and is often at the forefront when a new technology such as cryptocurrencies becomes available.[84]

Importantly, though, using cryptocurrencies is not in itself illegal, except in countries where it is banned. However, cryptocurrencies are particularly well suited to some types of nefarious activity and can facilitate otherwise criminal enterprises.

---

[79] Ibid.

[80] Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden, "Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency," *Joint Forces Quarterly* 92, no. 1 (2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_58-64_Dudley-et-al.pdf.

[81] David Carlisle and Kayla Izenman, "Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia," Royal United Services Institute, Apr. 2019, accessed Apr. 26, 2019, https://rusi.org/sites/default/files/20190412_closing_the_crypto_gap_web.pdf.

[82] Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden, "Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency," *Joint Forces Quarterly* 92, no. 1 (2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_58-64_Dudley-et-al.pdf.

[83] Ascertaining the precise amount that North Korea has earned via these activities is complicated both by the difficulty of assessing its activities, and because cryptocurrency values fluctuate so significantly.

[84] Megan McBride and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

At present, the federal government does not offer an official system for categorizing crimes involving cryptocurrencies. One expert, though, noted that "the universe of prosecutions" could be broken loosely into three categories: regulatory crimes "against market participants who are not compliant with…related laws or regulations," conventional crimes using cryptocurrency (e.g., dark web activity), and cybercrimes using cryptocurrency (e.g., hacking, ransomware).[85] We discuss each category below.

Regulatory crimes

Crimes in this category largely exploit the fact that cryptocurrencies represent an innovation and that regulatory and law enforcement entities have not yet fully caught up (see Figure 5 for an example). In the US, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the Internal Revenue Service (IRS) monitor cryptocurrency exchangers, transmitters, and administrators, as well as individuals who profit from cryptocurrencies (both as miners and as investors). The global regulatory environment, however, remains fractured with different countries approaching cryptocurrencies from different (and even incompatible) frameworks. As US officials have noted, in the absence of consistent international regulation—tracking individual transactions, sharing information, etc.—illicit actors can exploit both domestic and international markets.[86]

To date, prosecutions in this sphere have addressed issues including unlicensed money transmission, noncompliance with anti-money laundering or related laws and regulations, and failure to file suspicious activity reports (SARs).[87] These types of violations can be prosecuted either criminally or through civil actions. For example, Ripple settled a class-action lawsuit for $800,000 for not complying with such regulations.[88]

Although illicit activity still primarily occurs with conventional currencies, in June 2018 FinCEN's Thomas Ott testified to Congress: "FinCEN believes virtual currency presents specific illicit finance risks and that without vigilance and action, the scale of this activity could grow."[89] FinCEN has started to see evidence of improved regulatory compliance, however, as SAR filings "increase[ed] 90 percent from 2016 to 2017."[90]

---

[85] Ibid.

[86] Megan McBride and Lauren Frey, conversation with US officials, Mar. 1, 2019.

[87] Megan McBride and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

[88] Ibid.

[89] Thomas P. Ott, Testimony for the Record Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.

[90] Ibid.

Figure 5. Case highlight: "Bitcoin Maven"

In July 2018, US District Judge Manuel L. Real sentenced Theresa Lynn Tetley to a year and a day in prison "for conducting an illegal business and engaging in unlawful monetary transactions involving Bitcoins." Tetley, known as the "Bitcoin Maven," operated a person-to-person exchange of Bitcoins for US dollars without registering with FinCEN or reporting transactions to FinCEN or the IRS. Tetley pleaded guilty to the unlicensed exchange operation as well as to money laundering. The Drug Enforcement Administration (DEA) charged that Tetley "fueled a black-market financial system," including laundering Bitcoin obtained through the sale of illicit narcotics. The DEA and IRS contend that Tetley's illegal business "exchanged between $6 and $9.5 million for customers across the country."

Source: United States Drug Enforcement Agency, "'Bitcoin Maven Sentenced to Federal Prison in Virtual Currency Money Laundering Case," Jul. 9, 2018, accessed May 30, 2019, https://www.dea.gov/press-releases/2018/07/09/bitcoin-maven-sentenced-federal-prison-virtual-currency-money-laundering.

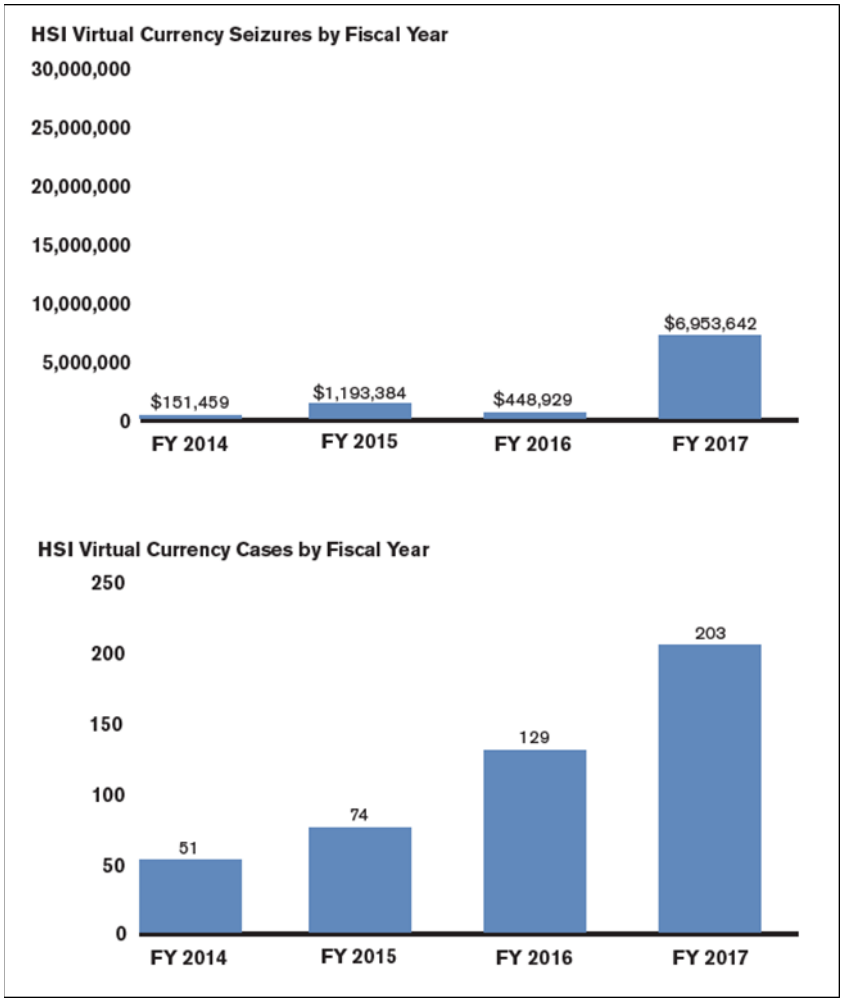
Traditional criminal activity

Crimes in this category use cryptocurrencies in the commission of more traditional criminal activities. Importantly, the use of cryptocurrencies is not what makes these actions illegal. Rather, cryptocurrencies simply facilitate otherwise criminal activity.

Cryptocurrencies have become popular among criminal organizations because of the widespread perception that they offer (1) anonymity (and even pseudonymity is more appealing than the oversight of conventional banking), (2) largely unregulated global reach, (3) improved transaction times (cryptocurrency transactions are processed 24/7 and do not stop on weekends or holidays), and (4) inaccessibility to law enforcement authorities (although this is beginning to change).

However, criminals do encounter risks when using cryptocurrencies because their values are unstable and wallets are subject to theft. Additionally, government regulators and law enforcement actors are growing their investigative capabilities, which has resulted in more frequent seizures. The US Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), for example, has seen a significant increase in both the number of cases it has pursued and the amount of funds it has seized (Figure 6).

Figure 6. Homeland Security Investigations virtual currency seizures and cases



Source: Office of Terrorism and Financial Intelligence, National Strategy for Combating Terrorist and Other Illicit Financing, Department of the Treasury, 2018, 37.

Though there is evidence that cryptocurrencies are being used by criminal and terrorist actors, the cryptocurrencies still play an essentially secondary role. Buyers and sellers, including drug dealers and arms traffickers, continue to assess transactions in terms of conventional currencies even when the transaction occurs in Bitcoin. These individuals are still *thinking* about the transaction in conventional currencies (and using the cryptocurrency merely to facilitate the exchange).[91] One consequence of this fact is that law enforcement agencies have

[91] Annie Lowrey, "Bitcoin Is Falling Out of Favor on the Dark Web," *Atlantic*, Mar. 1, 2018, https://www.theatlantic.com/business/archive/2018/03/bitcoin-crash-dark-web/553190/.

been able to exploit the financial transactions that occur when criminals convert cryptocurrencies into conventional currencies. Criminals typically exchange cryptocurrency for conventional cash following a transaction because they are cryptocurrency *users* but not cryptocurrency *investors* (i.e., they are not interested in holding these volatile coins indefinitely). During this exchange, these actors are the "most vulnerable" to traditional investigatory practices.[92] As a result, law enforcement is best able to penetrate the system at the exchanges.

Similarly, although some terrorist organizations use cryptocurrencies, there is little evidence that terrorist organizations are using cryptocurrencies as their primary currency. The Treasury Department's 2018 National Terrorist Financing Risk Assessment argues that cryptocurrencies "do not currently pose a significant terrorist financing risk" in part because there is no evidence that any terrorist organization is solely operating with cryptocurrencies.[93] The Center for a New American Security (CNAS) estimates that terrorists are "slow to adopt" cryptocurrencies because of their inability to easily access the "technological and telecommunications infrastructure" necessary to buy, mine, or exchange with regularity.[94]

Despite these limitations, a range of criminal activities have involved cryptocurrencies in recent years, which can be grouped into three loose categories: purchasing goods, advancing terrorist activity, and laundering money.

Cryptocurrency to purchase goods

Criminals have been repeatedly observed using cryptocurrencies to purchase illegal or legal goods to use in the commission of a crime (see Figure 7 for an example).

[92] Gregory C. Nevano, Testimony Before the US House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, *Illicit Use of Virtual Currency and the Law Enforcement Response,* June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NevanoG-

[93] "National Terrorist Financing Risk Assessment," US Department of the Treasury, 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf.

[94] Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "Terrorist Use of Virtual Currencies," Center for a New American Security, May 2017, http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

Figure 7. Case highlight: "Dread Pirate Roberts" and Silk Road

The most infamous instance of the use of cryptocurrencies on the dark web was the creation, and eventual shut down, of the Silk Road. In 2011, Ross William Ulbricht, also known as "Dread Pirate Roberts," created the website Silk Road to facilitate the sale and purchase of drugs on the dark web. Ulbricht launched the Silk Road website, and began by selling homegrown psychedelic mushrooms. Eventually the site took off (largely in the wake of a Gawker report about it) becoming a "virtually anonymous and thriving marketplace" that functioned akin to an escrow service (facilitating payments between buyers and sellers). In 2012, an interagency task force targeting the Silk Road was created and a series of arrests (of both buyers and sellers) began. Eventually, an account controlled by the Federal Bureau of Investigation (FBI) contacted Ulbricht to alert him to a series of "flagged posts" that required him to log into the highly encrypted site from his laptop. Once it had been confirmed that Ulbricht had logged into the site, he was arrested and his laptop was commandeered, allowing the US government to shut down the site. Ulbricht was charged with narcotics trafficking, solicitation of murder for hire, and money laundering and was sentenced to life in prison.

Source: David Adler, "Silk Road: The Dark Side of Cryptocurrency," Fordham Journal of Corporate & Financial Law (blog), Feb. 1, 2018, https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/.

Historically, much of this activity has occurred on the dark web, with the Treasury Department estimating that $4 billion in cryptocurrency traversed the dark web between 2011 and 2018.[95] The story of this activity, however, is more complicated than one simple statistic suggests:

- The *amount* of illegal cryptocurrency activity remains high. A 2018 study found that "the absolute value [of Bitcoin transactions] has increased, with $660 million of Bitcoin being sent to Darknet markets in 2017."[96] In other words, the monetary value of these illicit transactions has increased over the past five years.
- The *percentage* of illegal cryptocurrency activity (in relation to legal cryptocurrency activity) is lower, though. The same study noted that "the share of Bitcoin transactions sent to Darknet markets has declined from 30 percent in 2012 to less than 1 percent

[95] Thomas P. Ott, Testimony for the Record Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.

[96] Chainalysis Team, "The Changing Nature of Cryptocrime," *Insights* (blog), Jan. 18, 2018, https://blog.chainalysis.com/reports/report-the-changing-nature-of-cryptocrime.

> in 2017."[97] Thus, although the raw value of illegal activity conducted in cryptocurrencies has increased, the percentage of illicit activity has declined. Analysts have speculated that this trend can be linked to the mainstream adoption of Bitcoin (which has increased the overall number of legal users), an increase in legal Bitcoin investors (which has also increased the overall number of legal users), and the emergence of new cryptocurrencies that offer more anonymity than Bitcoin (and are appealing to actors who do not want to be found by law enforcement entities).[98]

Importantly, according to the 2015 Internet Organized Crime Threat Assessment conducted by Europol—an annual report examining the cybercrime threat landscape—"Bitcoin is no longer used preferentially within Darknet marketplaces."[99] Further, the *Atlantic* argues that Bitcoin is becoming less popular among criminals due to increases in Bitcoin's transaction fees, the lack of anonymity due to increased law enforcement capabilities, and volatility in the value of Bitcoin.[100] It is unclear, however, whether similar shifts in the ratio of licit to illicit use is also true for other cryptocurrencies.

Another, high-visibility example of this type of criminal use of cryptocurrency is described in Figure 8.

[97] Ibid.

[98] Jay B. Sykes and Nicole Vanatko, "Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals, " Congressional Research Service, Apr. 3, 2019, https://www.everycrsreport.com/files/20190403_R45664_5523da9e96a50aa8d5d3c085f6fd777b8a8112a4.pdf, 2, 9; and Sean Foley, Jonathan R. Karlsen, and Talis J. Putnins, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?," Review of Financial Studies, Dec. 14, 2018, https://ssrn.com/abstract=3102645.

[99] "The Internet Organised Crime Threat Assessment (IOCTA)," EUROPOL, 2015, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

[100] Annie Lowrey, "Bitcoin Is Falling Out of Favor on the Dark Web," *Atlantic*, Mar. 1, 2018, https://www.theatlantic.com/business/archive/2018/03/bitcoin-crash-dark-web/553190/.

Figure 8. Case highlight: Russian influence in the 2016 presidential election

A similarly interesting case—in which cryptocurrency was used to purchased legal goods pseudonymously—is now one of the most notorious hacking incidents in US history. In July 2018, the U.S. Department of Justice indicted 12 Russian spies with "conspiracy to commit an offense against the United States" because of their involvement in influencing the 2016 presidential campaign.[a] They used methods such as spearphishing and hacking to engage in this criminal activity, but they also used Bitcoin to further their efforts.[b] The indictment indicated the Russians acquired Bitcoin both by mining and by purchasing them on person-to-person exchanges. The Bitcoin were then used to acquire the "computer infrastructure that was employed in the hacking attacks" against the Democratic National Committee, as well as the dcleaks.com domain that was used to post emails from Hillary Clinton's hacked account.[c]

Sources:
[a] United States of America v. Viktor Borisovich Netyksho et al., Jul. 13, 2018, https://int.nyt.com/data/documenthelper/80-netyksho-et-al-indictment/ba0521c1eef869deecbe/optimized/full.pdf.
[b] Nathaniel Popper and Matthew Rosenberg, "How Russian Spies Hid Behind Bitcoin in Hacking Campaign," *New York Times*, Jul. 13, 2018, https://www.nytimes.com/2018/07/13/technology/bitcoin-russian-hacking.html.
[c] Ibid.

Cryptocurrency to further terrorist activity

Although much has been written about the ways in which cryptocurrencies might facilitate terrorist financing, at the public level there is "no more than anecdotal evidence" that such activity is actually taking place.[101] The public evidence that does exist, however, suggests that terrorists—or terrorist sympathizers—have attempted to harness cryptocurrencies to finance operations, transfer funds, and obtain goods, though the numbers linked to these activities are relatively modest. The 2018 National Terrorist Financing Risk Assessment noted that since 2015 terrorist groups have in a "limited number of instances" sought donations via cryptocurrency, and there were a few "isolated examples" of terrorists moving funds via cryptocurrency.[102]

[101] Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "Terrorist Use of Virtual Currencies," Center for a New American Security, May 2017, http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf, 2.

[102] "National Terrorist Financing Risk Assessment," US Department of the Treasury, 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf, 26.

In the terrorist ecosystem, fundraising seems to be the most common cryptocurrency-related activity. A 2014 article titled "Bitcoin and the Charity of Violent Physical Struggle," written under the nom de guerre Amreeki Witness, argued that Bitcoin was an excellent means of fundraising. According to the author, by using Bitcoin "one can prevent his 'brothers' who live outside the borders of the Caliphate from having to pay taxes to the infidels while simultaneously financing the mujahideen without exposing them to any legal risk."[103]

Since then, a number of cases have been made public. In most instances, a terrorist group or member uses social media to request that supporters send money to the organization through cryptocurrencies. Affiliates of the Islamic State (IS), al-Qaeda (AQ), Al-Sadaqah (a group known to have connections to AQ), and Hamas are all known to use cryptocurrencies in this way.[104] To cite just three examples of such activity:

- In January 2015, law enforcement shut down an ISIS-linked dark web account connected to Abu Mustafa (a known ISIS fundraiser) that was being used to fundraise through Bitcoin.[105] Abu Mustafa's message stated: "One cannot send a bank transfer to a mujahid [engaged in Jihad] or suspected mujahid without the kafir [infidel] governments ruling today immediately being aware….A proposed solution to this is something known as Bitcoin….To set up a totally anonymous donation system that could send millions of dollars' worth of Bitcoin instantly…right to the pockets of the mujahideen, very little would be done [against it]."[106] The call for funds was only modestly successful, and he allegedly raised a mere five Bitcoins (equivalent to $1,000 at the time of his post) before the FBI closed his account.[107]
- In 2016, the Mujahideen Shura Council, an Islamic terrorist organization with connections to ISIS, attempted to raise funds through a Bitcoin campaign. The group

[103] Gabriel Weimann, "Going Darker? The Challenge of Dark Net Terrorism," Wilson Center, 2016, https://www.wilsoncenter.org/sites/default/files/going_darker_challenge_of_dark_net_terrorism.pdf.

[104] Nikita Malik, "How Criminals and Terrorists Use Cryptocurrency: And How to Stop It," *Forbes*, Aug. 31, 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#68fb07f83990; and Yaya Fanusie, "Hamas Military Wing Crowdfunding Bitcoin," *Forbes*, Feb. 4, 2019, https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#1588fe884d7f.

[105] Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "Terrorist Use of Virtual Currencies," Center for a New American Security, May 2017, http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

[106] Gabriel Weimann, "Going Darker? The Challenge of Dark Net Terrorism," Wilson Center, 2016, https://www.wilsoncenter.org/sites/default/files/going_darker_challenge_of_dark_net_terrorism.pdf.

[107] Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "Terrorist Use of Virtual Currencies," Center for a New American Security, May 2017, http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

did so by "posting infographics on Twitter with QR codes linking to a bitcoin address."[108] Though the campaign was ambitious, analysis two months after the tweets indicated that it had yielded only two donations (worth approximately $500).[109]

- In 2019, al-Qassam Brigades (the military wing of Hamas) reached out to supporters on social media to solicit funds. The group posted infographics explaining how Bitcoin worked, a video titled "How to Buy Bitcoins," and a Bitcoin address to which donations could be sent.[110] Analysis indicates that the group raised approximately $900 in the first day.[111] A few days later, Hamas shared a different Bitcoin address that received over $2,500 in donations over the next week.[112]

In a few instances, terrorist groups have used cryptocurrencies to transfer funds and obtain goods. ISIS fighters in Syria have allegedly used cryptocurrencies to facilitate both international transactions and domestic purchases.[113] In more than one case, US citizens allegedly aspiring to "conduct a terrorist attack or travel abroad to join ISIS accessed Bitcoin accounts to help pay for expenses associated with their activity."[114] Terrorists have also been observed using cryptocurrencies to purchase legal and illegal goods. Reports indicate that ISIS purchased the weapons used in the 2015 Munich attacks on the dark web, and the owner of a website containing ISIS propaganda allegedly paid the site's service provider in cryptocurrency.[115]

Though terrorists have clearly been using cryptocurrencies, the reality is that cryptocurrencies will pose a "strategic threat in the counterterrorism context only when they can compete with

[108] Yaya Fanusie, "The New Frontier in Terror Fundraising: Bitcoin," Cipher Brief, Aug. 24, 2016, https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin.

[109] Ibid.

[110] Yaya Fanusie, "Hamas Military Wing Crowdfunding Bitcoin," *Forbes*, Feb. 4, 2019, https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#1588fe884d7f.

[111] Ibid.

[112] Ibid.

[113] Nikita Malik, "How Criminals and Terrorists Use Cryptocurrency: And How To Stop It," *Forbes*, Aug. 31, 2018, https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#68fb07f83990.

[114] "National Terrorist Financing Risk Assessment," US Department of the Treasury, 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf, 27.

[115] Antonia Ward, "Bitcoin and the Dark Web: The New Terrorist Threat?" *The RAND Blog*, Jan. 22, 2018, https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html; and "National Terrorist Financing Risk Assessment," US Department of the Treasury, 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf, 27.

cash and other readily available means of financing."[116] Thus, the 2018 National Terrorist Financing Risk Assessment concluded that "virtual currencies do not currently pose a significant [terrorist financing] threat."[117] The issue is partly one of match. As a recent RAND study concluded: "Current cryptocurrencies are generally not well matched with the totality of features [e.g., anonymity, usability, security, etc.] that would be needed and desirable" to terrorist actors.[118]

Several factors, however, may cause this to change. First, terrorist groups may be forced to invest more heavily in cryptocurrencies as their access to existing financial systems decreases. As regulatory enforcement improves, and military and law enforcement entities systematically erode the systems on which they rely, terrorists may shift to cryptocurrency.[119] Second, newer cryptocurrencies may provide greater anonymity. Concerns about anonymity are significant for those involved in terrorism financing, so the success of privacy coins such as Zcash and Monero, which can "reduce traceability of transactions," will be particularly appealing to actors in this space.[120] Third, terrorist organizations may be more comfortable with cryptocurrencies as they become more popular in areas that have poor regulatory practices. Increasingly robust regulatory frameworks in certain markets may make cryptocurrency transactions unappealing in these spaces, but ongoing regulatory laxity in other markets may increase their appeal.[121] Fourth, cryptocurrencies may have increased appeal for terrorist actors if they gain traction globally. If terrorists can conduct standard financial transactions with cryptocurrencies—purchasing goods in local markets, etc. —they may be more likely to adopt them.[122]

[116] Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "Terrorist Use of Virtual Currencies," Center for a New American Security, May 2017, http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf, 4.

[117] "National Terrorist Financing Risk Assessment," US Department of the Treasury, 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf, 27.

[118] Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats," RAND, 2019, https://www.rand.org/pubs/research_reports/RR3026.html, 35.

[119] David Manheim, Patrick B. Johnston, Joshua Baron, Cynthia Dion-Schwarz, "Are Terrorists Using Cryptocurrencies?," The RAND Blog, Apr. 21, 2017, https://www.rand.org/blog/2017/04/are-terrorists-using-cryptocurrencies.html.

[120] Ibid.

[121] Ibid.

[122] "National Terrorist Financing Risk Assessment," US Department of the Treasury, 2018, https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf, pg 27.

Cryptocurrency to launder money

Criminals can use cryptocurrencies to launder money in a variety of ways (see Figure 9 for one example), but the most common approach is through cryptocurrency exchanges. One analytic group assessed that approximately $2.5 billion in Bitcoin had been laundered through cryptocurrency exchanges between 2009 and 2018; and US prosecutors allege that Liberty Reserve (a now defunct service that dealt in a cryptocurrency called "LR") facilitated over $6 billion in money laundering between 2006 and 2013.[123] Critically, these figures represent just a small percentage of likely money laundering via cryptocurrencies because they consider only two coins (Bitcoin and LR). Moreover, these figures also represent only a small percentage of global money laundering activities. That said, government officials believe that money laundering via cryptocurrencies is a "growth industry" and that the volume and percentage will increase in the coming years.[124]

Not all cryptocurrency-related money laundering occurs through exchanges. Perhaps most secure, but least convenient, is laundering money through person-to-person exchanges in which a criminal can exchange cryptocurrencies directly with another individual.[125] In this type of exchange an individual can anonymously exchange dirty money for clean cryptocurrency. Unfortunately, the marketplaces that facilitate these person-to-person exchanges are challenging for law enforcement to investigate because the transactions themselves do not take place through a centralized website or server that can be targeted.[126]

Another form of money laundering using cryptocurrencies takes place through BTMs. These BTMs operate just like traditional ATMs, except they exchange conventional currency for Bitcoin (or vice versa). For a fee, one can purchase Bitcoin and instantaneously deposit it into a digital wallet. A representative from Coinsource, the largest BTM operator in the world, commented during a recent interview that criminals are trying to launder money through Coinsource's BTMs and are doing so in small amounts to go undetected.[127] To date, US regulators have not focused on investigating BTMs, instead forcing BTM companies to self-

[123] Jay B. Sykes and Nicole Vanatko, "Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals," Congressional Research Service, Apr. 3, 2019, https://www.everycrsreport.com/files/20190403_R45664_5523da9e96a50aa8d5d3c085f6fd777b8a8112a4.pdf, 2, 9.

[124] Ibid.

[125] "The Internet Organised Crime Threat Assessment (IOCTA)," EUROPOL, 2015, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

[126] Ibid.

[127] Tom Schoenberg and Matt Robinson, "Bitcoin ATMs May Be Used to Launder Money," *Bloomberg Businessweek*, Dec. 14, 2018, https://www.bloomberg.com/features/2018-bitcoin-atm-money-laundering/.

regulate in an attempt to decrease criminal activities.[128] As one example, BTM company Cottonwood is working to obtain a BitLicense (a permit awarded by New York banking regulators). If Cottonwood is awarded a BitLicense, it would signify that regulators believe Cottonwood has adequate protections in place to ensure its BTMs are not being used for criminal activities.[129] Unfortunately, although some BTM companies are attempting to weed out potential money launderers on their own, a handful of BTM companies are not verifying identification or imposing limits on transactions, which is creating a haven for money launderers.

Figure 9. Case highlight: Liberty Reserve

In 2013, federal and international law enforcement agencies identified Liberty Reserve as a currency service that was facilitating criminal activity by processing billions of dollars related to hacking activities, money laundering operations, and extortion schemes.[a] In January 2016, the founder, Arthur Budovsky, plead guilty to committing money laundering. According to the US Department of Justice, Budovsky "specifically designed" Liberty Reserve to "to help users conduct anonymous and untraceable illegal transactions and launder the proceeds of their crimes."[b] Over time, the service "became one of the principal money-transmitting services used by cybercriminals around the world to amass, distribute, store, and launder the proceeds of their illegal activity."[c] Before it was closed, the service had more than 5 million users worldwide (600,000 of whom were operating in the US).[d]

Sources:
[a] Thomas P. Ott, Testimony for the Record Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.
[b] "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million Through His Digital Currency Business," U.S. Department of Justice, PRN 16-113, Jan. 29, 2016, https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.
[c] Ibid.
[d] Ibid.

Cybercrimes

Crimes in this final category are those that involve the illegal use or exploitation of the cryptocurrencies themselves. These crimes—typically cybercrimes—are lucrative

[128] Ibid.

[129] Ibid.

undertakings that exploit technological loopholes and vulnerabilities inherent in what is still a new technology.

One example is *crypto-jacking*, which involves hijacking others' computing power to mine cryptocurrencies.[130] This can be accomplished by infecting the victim's computer with malware, or by commandeering the user's system though an application, game, service, or website without the user's knowledge or permission. In all cases, the victim's computer is used to mine cryptocurrencies as a background operation.[131] Through this mining, cybercriminals are able to make money while parlaying the costs of the activity (e.g., electricity) to unsuspecting individuals.[132]

Another example is *ransomware* which is malware that locks down a computer's operations and/or data and demands payment (i.e., ransom) in exchange for returning the user's computer to its normal operation.[133] Both individuals and corporations have been victims of ransomware attacks, and the US Treasury Department estimates that from June 2016 to June 2018 over $1 billion in cryptocurrency was exchanged as part of ransomware extortion efforts.[134] Ransomware attacks are, unfortunately, becoming more popular because of their ease-of-use and almost guaranteed payout.[135] Nefarious actors do not need to be coding experts: they can purchase ransomware online or even contract out to more experienced hackers.[136]

As a final example, cybercriminals have hacked individual wallets, virtual currency exchanges, and dark web sites to outright steal cryptocurrencies. The US Treasury Department concluded that cryptocurrency exchanges lost more than $1.5 billion worth of cryptocurrency to hackers

[130] Robert Novy, Prepared Testimony Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NovyR-20180620.pdf.

[131] Michael Nadeau, "What Is Cryptojacking? How to Prevent, Detect, and Recover from It," CSO, Dec. 13, 2018, https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html.

[132] Michael Baker, "How Cryptocurrencies Are Fueling Ransomware Attacks and Other Cybercrimes," *Forbes*, Aug. 3, 2017, https://www.forbes.com/sites/forbestechcouncil/2017/08/03/how-cryptocurrencies-are-fueling-ransomware-attacks-and-other-cybercrimes/#284696fe3c15.

[133] "Ransomware," Dictionary.com, https://www.dictionary.com/browse/ransomware.

[134] Thomas P. Ott, Testimony for the Record Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.

[135] Michael Baker, "How Cryptocurrencies Are Fueling Ransomware Attacks and Other Cybercrimes," *Forbes*, Aug. 3, 2017, https://www.forbes.com/sites/forbestechcouncil/2017/08/03/how-cryptocurrencies-are-fueling-ransomware-attacks-and-other-cybercrimes/#284696fe3c15.

[136]Ibid.

between 2016 and 2018.[137] In 2013, HSI arrested two criminals for electronically stealing cryptocurrency from an illicit dark web site. The criminals stole the cryptocurrencies by compromising the website, and HSI ultimately seized $4.5 million in cryptocurrency and conventional currencies that the two had amassed.[138]

In good news, however, law enforcement has had some success in this area. In 2017, US Secret Service efforts led to the arrest of a Russian national who allegedly operated BTC-e, a cryptocurrency exchange platform suspected of "facilitating over $4 billion worth of Bitcoin transactions worldwide for cyber criminals engaging in computer hacking, identity theft, ransomware, public corruption, and narcotics distribution."[139] Moreover, "researchers estimate approximately 95 percent of ransomware payments were laundered through BTC-e" from 2011 to 2017.[140] Additionally, in March 2018, the Treasury Department clarified that sanctioning individuals and organizations includes sanctioning their cryptocurrency holdings, and that—when and where possible—cryptocurrency wallets would be added to its Specially Designated Nationals List.[141]

As cyberattacks become easier to execute, and continue to yield profits, the number of such attacks is likely to increase, which may also result in an increase in cryptocurrency-related cybercrimes. There are, moreover, already multiple examples of successful attacks:

- **NotPetya attack:** In 2017, massive ransomware attacks in Ukraine impacted multinational corporations such as Maersk and Merck. The cybercriminals used a variant of the Petya malware to shut down a victim's system until the target paid a specified ransom. Many of the victims that did pay the ransom never regained access to their files, and analysts eventually concluded that the ransomware attack was a red herring to disguise the fact that the malware was "really designed to exact maximum destruction and disruption, with Ukraine the clear target."[142] Moreover, the

[137] Thomas P. Ott, Testimony for the Record Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.

[138] Gregory C. Nevano, Testimony Before the US House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, *Illicit Use of Virtual Currency and the Law Enforcement Response,* June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NevanoG-20180620.pdf

[139] "Fact Sheet: DHS Cybersecurity Policy," US Department of Homeland Security, Aug. 22, 2018, https://www.dhs.gov/news/2018/05/15/fact-sheet-dhs-cybersecurity-policy.

[140] Ibid.

[141] "OFAC FAQs: Sanctions Compliance," US Department of the Treasury, last updated Feb. 6, 2019, accessed May 22, 2019, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs.

[142] Robert Hackett, "Why You Shouldn't Pay the Petya Ransom," *Fortune*, June 28, 2017, http://fortune.com/2017/06/28/ransom-bitcoin-petya/; and Ralph Bajak and Raphael Satter, "Companies still

Washington Post reported in early 2018 that the Central Intelligence Agency (CIA) had allegedly concluded that Russia's Main Intelligence Directorate (GRU) had created NotPetya.[143]

- **SamSam attack:** In November 2018, the Justice Department indicted two Iranian men for a ransomware operation that targeted over 200 hospitals, city governments, universities, and healthcare providers across the United States and Canada between 2015 and 2018.[144] The SamSam ransomware encrypted files on affected systems and offered to decrypt the files only if victims paid ransom in Bitcoin.[145] At the time of their indictment, the two men had earned more than $6 million from the attacks, while the impact of business operations had cost their victims over $30 million.[146] The men also targeted the government of Atlanta, Georgia in what one publication called "one of the most sustained and consequential cyberattacks ever launched against a major American city."[147] This attack was not, however, the last: in the first half of 2019 alone, more than 20 municipalities experienced cyberattacks.[148]
- **DD4BC attacks:** The cybercriminal group Distributed Denial of Service for Bitcoin (DD4BC) is, according to analysis, responsible for victimizing nearly 300 companies (including private companies, financial services, and the online gambling and entertainment industries) and causing over $1 million in damages.[149] The response to

hobbled from fearsome cyberattack," AP News, June 30, 2019, https://www.apnews.com/ce7a8aca506742ab8e8873e7f9f229c2.

[143] Ellen Nakashima, "Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, Jan. 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[144] US Department of Justice, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," Department of Justice Office of Public Affairs, PRN: 18-1559, Nov. 28, 2018, https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

[145] Ibid.

[146] Nicole Perlroth and Katie Benner, "Iranians Accused in Cyberattacks, Including One That Hobbled Atlanta," *New York Times*, Nov. 28, 2018, https://www.nytimes.com/2018/11/28/us/politics/atlanta-cyberattack-iran.html?module=inline.

[147] Ibid.

[148] Emily Sullivan, "Ransomware Cyberattacks Knock Baltimore's City Services Offline," NPR, May 21, 2019, https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline.

[149] Laura Eimiller, "Electronic Crimes Task Force Collaborates with Europol to Target Bitcoin Distributed Denial of Service Attacks," FBI, Jan. 13, 2016, https://www.fbi.gov/contact-us/field-offices/losangeles/news/press-releases/electronic-crimes-task-force-collaborates-with-europol-to-target-bitcoin-distributed-denial-of-service-

this challenge was Operation Pleiades, a global collaboration involving the FBI's Electronic Crimes Task Force, US Secret Service, INTERPOL, and police authorities from Australia, France, Japan, and Romania.[150] The operation led to the arrest of "a main target," the detention of an additional suspect, and the seizure of relevant evidence.[151]

Importantly, not all crimes involving the illegal use or exploitation of the cryptocurrencies are undertaken by non-state actors. Discussions of money laundering typically focus on criminal actors, but state actors may also engage in this activity. North Korea, for example, has been observed participating in all three of the cybercrimes above: crypto-jacking, ransomware, and hacking.[152]

Analysts have also speculated about why a state actor might engage in this activity. One article suggested, for example, that states might use cryptocurrencies to "[launder] state money into the hands of threat actors and terror groups."[153] Another article speculated that "[influencing] the cryptocurrency ecosystem can be a decisive option for national competition below the threshold of war."[154] As Chris Telley noted in an article in *Small Wars Journal*, Russia might harness its "vast and underutilized power industry" to dominate the mining industry.[155] Kremlin official Dmitry Marinichev has apparently suggested that Russia could control approximately 30 percent of mining efforts globally, but more concerning is the possibility that Russia might launch a 51 percent attack (which would permit it to control all transactions in the targeted currency).[156] And critically, Russia has other potential pathways to exploit the cryptocurrency ecosystem. It might, for example, "funnel money into populist political parties or diaspora guerilla movements without trace and without domestic effect" or destabilize

attacks; and "International Action Against DD4BC Cybercriminal Group," EUROPOL, Jan. 12, 2016, https://www.europol.europa.eu/newsroom/news/international-action-against-dd4bc-cybercriminal-group.

150 "International Action Against DD4BC Cybercriminal Group."

151 Ibid.

152 David Carlisle and Kayla Izenman, "Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia," Royal United Services Institute, Apr. 2019, accessed Apr. 26, 2019, https://rusi.org/sites/default/files/20190412_closing_the_crypto_gap_web.pdf.

153 William Allen, "Cryptocurrency in Threat Finance: The Manipulation of Non-Fiat Digital Currencies to Finance Nefarious Actors," *Small Wars Journal*, accessed June 3, 2019, https://smallwarsjournal.com/jrnl/art/cryptocurrency-threat-finance-manipulation-non-fiat-digital-currencies-finance-nefarious.

154 Chris Telley, "A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency," *Small Wars Journal*, https://smallwarsjournal.com/jrnl/art/coin-tsar-two-disruptive-sides-cryptocurrency.

155 Ibid.

156 Ibid.

markets in which the fiat currency has a smaller supply than the cryptocurrency that Russia controls.[157]

Though much has been written about the use of cryptocurrencies by terrorist movements, this type of activity represents a modest percentage of illicit cryptocurrency activity in general. And the scope of nefarious applications available to, and being pursued by, well-resourced and under-resourced state and non-state actors is not only wide-ranging, but also constantly evolving.

[157] Ibid.

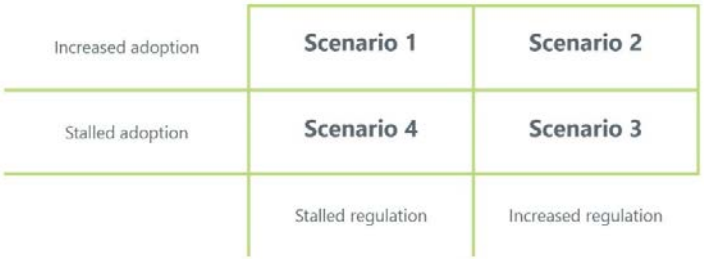
The (Likely) Futures of Cryptocurrency

Making predictions about the future of cryptocurrency is precarious at best. Focusing on the very near future, one can easily speculate that cryptocurrencies will continue to be created and that cryptocurrency values will remain volatile. Predictions that look father into the future are more interesting and compelling, but when looking farther ahead consensus disappears. Instead, experts have suggested a variety of futures that have implications for the global economy, ranging from the insignificant (e.g., the complete disappearance of cryptocurrencies within 10 years) to the catastrophic (e.g., the collapse of Bretton Woods and upending of the global economic framework).[158]

We assess that two major variables will shape the future of cryptocurrencies: regulation and adoption. Each of these variables may either increase or stall, and our analysis of the (likely) futures of cryptocurrency explores the four possible permutations this would produce (Figure 10):

1. Scenario 1: Increased adoption and stalled regulation
2. Scenario 2: Increased adoption and increased regulation
3. Scenario 3: Stalled adoption and increased regulation
4. Scenario 4: Stalled adoption and stalled regulation (i.e., the status quo)

Figure 10. The (likely) futures of cryptocurrency



Source: CNA.

In exploring these possible future scenarios, we did not assess the activities of cryptocurrency *investors*. Though we understand that investment activity is critical to the long-term health of cryptocurrencies, the question of whether or not cryptocurrencies form an investment bubble is unresolved. We assumed that they do not form a bubble (i.e., that the entire market would

[158] Megan McBride, conversation with industry expert, Feb. 5, 2019; and Jonathan Schroden, conversation with US Army finance officer, Feb. 22, 2019.

not implode in the short-term) so that we could explore mid-term potential futures with national security implications.

Scenario 1: Increased adoption and stalled regulation

In this scenario, the future of cryptocurrency is characterized by an increase in adoption rates, but no measurable increase in domestic or global efforts at regulation.

One possibility is that this change will begin in developed and economically stable countries as the technological challenges to adoption are resolved (e.g., user friendly wallets, more BTMs). That said, cryptocurrencies—in the absence of greater regulation (and the stability and security that this would ensure)—are not particularly appealing to populations with viable alternatives. As one analyst noted, most people "just want a payment system that is safe and easy to use. And given cryptocurrencies' shortcomings—the lack of consumer protection, dizzying price fluctuations, fiddly software, slow throughput and a voracious appetite for electricity—at the moment they fail that test."[159] Some of these issues are technological challenges that might be resolved (e.g., fiddly software), but some would require a degree of oversight and regulation not present in this scenario (e.g., consumer protection).

It may, as a result, be more likely that increased adoption will begin in less economically developed countries. Although the current regulatory framework is fractured and inadequate—permitting widespread criminal activity and fraud—the benefits may outweigh the risks for some populations. In some cases the "downsides [to cryptocurrency use] are things that people in the West care about, but when you look at foreign currencies many already suffer from those issues and so cryptocurrency can be an attractive competitor."[160]

Importantly, this scenario has the potential to fork in two directions based on the degree to which the cryptocurrency community maintains—in the face of widespread adoption and the absence of increased regulation—a culture of privacy.

If privacy does remain an important feature, and the regulatory framework stalls at the status quo (i.e., a place of relative global inconsistency), then the future might include an increased proliferation of privacy coins and options for ensuring anonymity.

[159] "Dividing the cryptocurrency sheep from the blockchain goats," *Economist Technology Quarterly*, Aug. 30, 2018, https://www.economist.com/technology-quarterly/2018/09/01/dividing-the-cryptocurrency-sheep-from-the-blockchain-goats.

[160] Jonathan Schroden, conversation with US Army finance officer, Feb. 22, 2019.

If privacy is deprioritized (perhaps as a result of an industry-led effort to demonstrate mainstream potential), and the regulatory framework stalls at the status quo, then the future might be characterized by increased industry-led efforts to collaborate with existing regulatory and law enforcement officials to decrease the amount of criminal activity on these networks.

Scenario 2: Increased adoption and increased regulation

In this scenario, the future of cryptocurrency is characterized by an increase in adoption rates and an increase in domestic and global efforts at regulation.

It is possible, of course, to imagine that increased domestic and global regulation will precede increased adoption. In this scenario, a continually improving regulatory framework might increase consumer confidence and interest in cryptocurrencies. It seems more likely, though, that increased user adoption will precede the kind of robust regulatory framework that this scenario envisions. And importantly, this adoption might be precipitated by activity in any of at least four spheres: users, vendors, states, and banks.

User-driven adoption

At present, adoption rates are relatively low because a variety of issues are keeping consumers from embracing cryptocurrencies. The work of obtaining cryptocurrencies (that may lose value overnight) far outweighs the benefit of being able to shop at the approximately half dozen online marketplaces that currently accept cryptocurrencies, so consumers have little incentive to embrace the technology. Consumers know that it is easier to simply use a credit card for online shopping.

It is possible, however, that widespread adoption among users in developing economies might persuade vendors to develop the infrastructure necessary to accept cryptocurrencies. The benefits of cryptocurrencies, as noted earlier, may outweigh the risks for some populations. It is already the case, for example, that cryptocurrencies are "driving innovation" in parts of Africa where applications such as BitPesa and BitFinance are "democratizing the economy and providing a banking service free of hyperinflation."[161] And in Afghanistan, young women have been using Bitcoin to "earn wages through global services and purchase products on worldwide markets, without the bank account forbidden by their local brand of Islam."[162] If these initiatives continue, and these populations begin to demand access to the international

[161] Chris Telley, "A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency," *Small Wars Journal*, https://smallwarsjournal.com/jrnl/art/coin-tsar-two-disruptive-sides-cryptocurrency.

[162] Ibid.

marketplace, it is likely that vendors will develop the necessary infrastructures to accept cryptocurrencies, which may precipitate the development of a more robust regulatory framework.

Vendor-driven adoption

In this scenario, vendors identify some financial benefit (e.g., tapping into otherwise inaccessible markets) to transacting in cryptocurrencies that may ultimately lead to widespread user adoption. If corporations such as Walmart, Target, and Amazon accepted cryptocurrencies—and developed the technologies to make the practice user-friendly—then users would likely assume a degree of security and follow suit (especially if vendors incentivized user-adoption).

Not all developments in this scenario, however, rely on vendor adoption of existing cryptocurrencies. Instead, a vendor might create a cryptocurrency attractive enough to encourage adoption. One potentially interesting move in this direction is the 2019 announcement that Facebook was "leading a consortium" to "create a new digital currency and financial system to transform the way money moves around the world."[163] According to the white paper they released, members of the Libra Association—"formed from the network of validator nodes that operate the Libra Blockchain"—include financial heavyweights such as Visa, Mastercard, and PayPal.[164] The white paper also identifies early 2020 as the "target launch" of the Libra. As the *Wall Street Journal* noted, Facebook's success in this arena would "[threaten] to upend the traditional, lucrative plumbing of e-commerce and would likely be the most mainstream application yet of cryptocurrency."[165]

State-driven adoption

Another potential future in this category is the rise of state-sponsored cryptocurrencies. To date, only Venezuela has taken the leap, but the trend in this direction is clear. Christine Lagarde, Managing Director of the International Monetary Fund (IMF), suggested in late 2018 that governments should consider launching their own cryptocurrencies to prevent criminals

[163] Julia Boorstin, "Facebook Launches a New Cryptocurrency Called Libra," CNBC.com, June 18, 2019, https://www.cnbc.com/2019/06/17/facebook-announces-libra-digital-currency-calibra-digital-wallet.html.

[164] "Libra White Paper," Libra Association, 2019, https://libra.org/en-US/white-paper/.

[165] AnnaMaria Androitis, Liz Hoffman, Peter Rudegeair, and Jeff Horwitz, "Facebook Building Cryptocurrency-Based Payments System," *Wall Street Journal*, May 2, 2019, https://www.wsj.com/articles/facebook-building-cryptocurrency-based-payments-system-11556837547.

from monopolizing the space.[166] Moreover, a number of countries—including, but not limited to, Canada, China, the Eastern Caribbean Islands, Iran, the Marshall Islands, Norway, Russia, Saudi Arabia, Sweden, Thailand, Tunisia, Turkey, United Arab Emirates, Ukraine, the United Kingdom, and Uruguay—are apparently interested in (or actively exploring) state-sponsored activity in the cryptocurrency world. Early 2019 reporting indicated that three countries (Afghanistan, Tunisia, and Uzbekistan) were interested in issuing Bitcoin bonds—at least theoretically supported by IMF director Christine Lagarde—as a means to increase access to international markets.[167]

These state-sponsored efforts fall into two distinct categories. In some cases (e.g., Venezuela or Iran), the objective is to embrace the privacy of cryptocurrencies to avoid international sanctions. In other cases (e.g., Afghanistan), the objective is to embrace the transparency of cryptocurrencies to demonstrate fiscal responsibility. Afghanistan has a terrible reputation in financial markets (the IMF has identified the country as "high risk") and consequently struggles to borrow money from conventional sources. By pursuing a Bitcoin bond, Afghanistan hopes to obtain critically necessary funds via a system that "allows some measure of protection against terrorist financing through its auditable blockchain."[168] If it can "show that its money is completely detached from bad actors that have plagued its past, it may finally be able to demonstrate to the world that it can join the world economy and build to a common future."[169]

Bank-driven adoption

A final potential motivator of widespread adoption is a future in which central bank digital currencies (CBDCs) dominate the market. CBDCs would stand in stark contrast to conventional cryptocurrencies. They would not, for example, embrace public, trustless ledgers like those that define existing cryptocurrencies.[170] Instead, these CBDCs would likely adopt the centralized and private ledgers that banks currently use to process transactions "safely and seamlessly."[171] Should this occur, Nouriel Roubini (a professor at New York University) has

[166] Phillip Inman, "IMF says governments could set up their own cryptocurrencies," *Guardian*, Nov. 13, 2018, https://www.theguardian.com/business/2018/nov/14/imf-says-governments-could-set-up-their-own-cryptocurrencies.

[167] Esther Kim, "3 Countries Tell IMF They Want to Issue Bitcoin Bonds," Bitcoinist, Apr. 17, 2019, https://bitcoinist.com/these-3-countries-tell-imf-they-want-to-issue-bitcoin-bonds/.

[168] Derek Tonin, "Afghanistan Considers Turning to Crypto Bonds to Rebuild," CoinGeek, Apr. 22, 2019, https://coingeek.com/afghanistan-considers-turning-to-crypto-bonds-to-rebuild/.

[169] Ibid.

[170] Nouriel Roubini, "Why Central Bank Digital Currencies Will Destroy Bitcoin," *Guardian*, Nov. 19, 2018, https://www.theguardian.com/business/2018/nov/19/why-central-bank-digital-currencies-will-destroy-bitcoin.

[171] Ibid.

argued that CBDCs would "likely replace all private digital payment systems, regardless of whether they are connected to traditional bank accounts or cryptocurrencies."[172] Cryptocurrency purists might find this particular system problematic insofar as it relies on the very third-party authorities that cryptocurrencies were originally designed to eliminate. That said, cryptocurrency purists comprise a small percentage of the population, and CBDCs could restore a degree of anonymity to users as "transactions could be made anonymous, with access to account-holder information available…only to law-enforcement authorities or regulators."[173] The likelihood of this happening is difficult to assess, but it is important to note that such a move would "amount to a financial revolution" and so should not be expected in the near future.[174]

Scenario 3: Stalled adoption and increased regulation

In this scenario the future of cryptocurrency is characterized by an increase in regulation, but no measurable increase in adoption rates. In this future, robust domestic and global regulatory frameworks are developed to disrupt nefarious state-sponsored activities (e.g., hacking, mining, sanction evasion), prevent widespread adoption by terrorist actors, and better investigate and prosecute criminal actors. However, few users are attracted to this increasingly secure means of monetary exchange, and cryptocurrency remains marginal with only modest increases in mainstream use.

Scenario 4: Stalled adoption and stalled regulation

In this scenario the future of cryptocurrency is characterized by a lack of measurable increase in either regulation or adoption.

This path is, in short, the maintenance of the status quo: the global regulatory framework remains fractured as different countries take different approaches to the technology. State-sponsored cryptocurrencies succeed to varying degrees without significantly impacting the global economic framework; widespread user adoption does not occur as the technology does not become more user-friendly, few consumer protections exist, and coin values remain

[172] Ibid.

[173] Ibid.

[174] Ibid.

volatile; and ill-intentioned actors (states, terrorists, and criminals) continue to exploit the technology to further their ends.

The maintenance of the status quo does not, however, mean a complete absence of change. An April 2019 publication by Financial Action Task Force (FATF), an inter-governmental standard-setting body, indicated that the organization had recently agreed on language suggesting that countries should take a range of actions related to the monitoring and regulation of cryptocurrency "service providers."[175] And in June 2019, the organization updated its *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*.[176] In other words, the status quo does involve some movement—relating to both adoption and regulation—but these changes are modest, voluntary, and piecemeal.

Similar to the first scenario, this one has the potential to fork in two directions based on the degree to which the cryptocurrency community maintains a culture of privacy. If privacy does remain an important feature, and the regulatory framework stalls at the status quo (i.e., a place of relative global inconsistency), then the future might include an increased proliferation of privacy coins and options for ensuring anonymity. If privacy is deprioritized (perhaps in an effort to spur user or vendor interest), and the regulatory framework stalls at the status quo, then the future might be characterized by increased industry-led efforts to collaborate with existing regulatory and law enforcement officials to decrease the amount of criminal activity done on these networks.

As these (likely) futures make clear, the cryptocurrency ecosystem is complicated, and accurate mid-term predictions are difficult to make with any confidence. Even within a systematic framework that focuses on two critical variables—regulation and adoption—the potential futures are incredibly diverse. This complexity and diversity, however, creates a host of challenges and opportunities for SOF, which will be explored in the next section.

[175] *FATF Report to G20 Leaders' Summit*, Financial Action Task Force, Apr. 2019, http://www.fatf-gafi.org/media/fatf/documents/G20-April-2019.pdf.

[176] *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Financial Action Task Force, June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

Implications for SOF

As mentioned in the previous section, making predictions about the future of cryptocurrency is precarious given that industry experts have argued for a variety of futures ranging from the total collapse of cryptocurrencies to the total domination of cryptocurrencies. Thus while analysis about cryptocurrencies often focuses on the challenge of understanding the technology, the more pressing challenge may be identifying what direction the technology is taking as the future comes into focus.

CNA initiated this study to explore the cryptocurrency ecosystem and help SOF consider the implications of cryptocurrencies on SOF missions. We assess that while the future is unclear and the technologies are complicated, these implications essentially fall into two categories: challenges and opportunities.

Challenges for SOF

Government and private industry actors face a number of challenges when attempting to counter criminals (and, to a lesser degree, terrorists) from exploiting cryptocurrencies. In the section below, we discuss three challenges that we assess are particularly relevant to SOF: the fractured global regulatory environment; the rapidly evolving cryptocurrency ecosystem; and the lack of adequate knowledge, education, and training.

Fractured regulatory environment

As mentioned above, the regulatory environment for cryptocurrencies is currently fractured and will remain relatively fragmented in two of the four potential futures: Scenario 1 (increased adoption and stalled regulation) and Scenario 4 (stalled adoption and stalled regulation). If criminals, terrorists, and other illicit actors increasingly move to using cryptocurrencies instead of conventional currencies, and if cryptocurrencies and their exchanges are not properly and universally regulated, challenges will grow in tracking and interdicting the financial activities of these threat groups.[177] The lack of a coherent global approach to regulation can result in cryptocurrency safe-havens if terrorist and transnational

[177] Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden, "Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency," *Joint Forces Quarterly* 92, no. 1 (2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_58-64_Dudley-et-al.pdf, 58-59.

criminal organizations can operate freely in countries with limited regulations.[178] These illicit actors can already, in fact, hold and transfer their cryptocurrencies in plain sight, so long as they operate on exchanges outside the jurisdiction of countries with better oversight.[179]

Although the US Treasury Department currently works with foreign regulators and foreign law enforcement entities to provide technical assistance and address vulnerabilities related to regulating cryptocurrency businesses, this challenge is also significant to US Special Operations Command (SOCOM) and the SOF enterprise as DOD's coordinating authority for countering terrorist groups.[180] Our assessment of the relevance of these shifts to SOF's mission stems from several sources: the emphasis placed on isolating terrorists from financial sources of support in the *National Strategy for Counterterrorism*[181]; guidance from the Chairman of the Joint Chiefs of Staff, General Joseph Dunford, for SOF to focus on cutting the "connective tissue" of terrorist group resources[182]; and the establishment of entities such as SOCOM's Operation Gallant Phoenix (OGP), whose charter is to provide SOF-generated information to foreign military and law enforcement partners to enable arrests and prosecutions of foreign fighters and those engaged in support to foreign terrorist groups (including financial support).[183]

As SOF attempt to sever terrorist and transnational criminal groups from their sources of financial support, the lack of a robust and uniform regulatory framework for cryptocurrencies will present challenges. Given this reality, the best possible future for SOF is perhaps Scenario 3 (stalled adoption and increased regulation) because this would facilitate targeting of nefarious activity without a rise in new innovations that would likely accompany increased adoption. A further challenge for SOF is that they are reliant on other US government agencies (e.g., the Treasury Department) to advocate for changes to the regulatory environment overseas. Thus, SOF will have to work closely with other US government agencies to articulate what they are seeing on the ground (e.g., via the activities of entities such as OGP), what

[178] Thomas P. Ott, Testimony for the Record Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.

[179] Megan McBride and Lauren Frey, conversation with US officials, Mar. 1, 2019.

[180] Ibid.

[181] National Strategy for Counterterrorism of the United States of America, White House, Oct. 2018, https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.

[182] Joseph F. Dunford Jr., *Statement Before the Senate Armed Services Committee, Department of Defense Budget Hearing*, Mar. 14, 2019, https://www.armed-services.senate.gov/imo/media/doc/Dunford_03-14-19.pdf, 7.

[183] Miles Hidalgo, "Beyond the Conflict Zone: US HIS Cooperation with Europol," *CTC Sentinel* 11, no. 2 (Feb. 2018), https://ctc.usma.edu/beyond-conflict-zone-u-s-hsi-cooperation-europol/; and Jim Garamone, "Dunford Asks Defense Chiefs to Guard Against Complacency," Joint Chiefs of Staff, https://www.jcs.mil/Media/News/News-Display/Article/1664622/dunford-asks-defense-chiefs-to-guard-against-complacency/.

changes would help them operationally, and what their sense of the second- and third-order effects of such changes would be.

Evolution of technology (and nefarious behaviors)

Although government actors have increased their attention to the nefarious use of cryptocurrencies, the ecosystem is evolving at a faster rate than the techniques and technologies necessary to arrest this type of behavior.[184] Newer cryptocurrencies are developing more advanced encryption methods that complicate efforts to monitor activity, privacy coins are developing more advanced anonymization methods making it harder to track individual users, and hybrid approaches (e.g., those in which digital currencies are exchanged in face-to-face interactions) pose a significant challenge to government actors hoping to track or halt nefarious activity. Moreover, the very number of cryptocurrencies—even if limited to only healthy and viable ones—fluctuates in a way that undermines government efforts to remain ahead of the curve.

These trends present significant challenges for SOF. To begin, foreign terrorist and criminal groups have a plethora of cryptocurrencies to choose from, creating many potential avenues for nefarious financial activity that will need to be monitored. Moreover, in the same way that encrypted chat applications have complicated the ability of SOF and intelligence agencies to intercept terrorist communications,[185] the increase in privacy coins and the potential for further developments to increase privacy and obscure cryptocurrency transactions could pose increased challenges to SOF's ability to monitor and impact financial transactions of interest.

The trends in cryptocurrencies suggest the possibility that they will continue to gain traction in developing economies (where the benefits may outweigh the risks). This possibility will pose challenges, especially for SOF, since these are often the same countries and areas in which terrorist groups are most active.

Increased adoption—regardless of what drives it or where it geographically occurs—is likely to result in increased innovation as new users (with new needs) move into the ecosystem. Moreover, two potential futures are characterized by this trend: Scenario 1 (increased adoption and stalled regulation) and Scenario 2 (increased adoption and increased regulation). The first of these would be particularly challenging for SOF because additional innovations would proceed unchecked by a robust regulatory network.

[184] Megan McBride and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

[185] Bonnie Mitchell et al, "Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation," Office of the Director of National Intelligence, 2017, https://www.odni.gov/files/PE/Documents/10---2017-AEP_Going-Dark.pdf.

Lack of knowledge, training, and education

In the process of researching and writing this paper, we realized that US government expertise on cryptocurrencies is limited to some very small pockets. Indeed, this gap in knowledge of cryptocurrencies among the broader US policy and decision-making community is what prompted us to publish our companion primer.

The US government—including the SOF enterprise—lacks deep institutional knowledge on this topic, and its cyber entities lack sufficient resources to actively invest in such expertise (as they would be expected to do). Furthermore, the cryptocurrency ecosystem is evolving and changing so quickly that it is difficult to stay abreast of new trends. The breadth of cryptocurrency-related nefarious activity—both state and non-state—that has been observed over the past five years reveals a need for robust investment in this arena.[186] Unfortunately, increased attention to this topic does not yet appear to be forthcoming despite the fact that *all* of the future scenarios imagined in the section above require a robust response. Scenarios in which adoption increases—Scenario 1 (increased adoption and stalled regulation) and Scenario 2 (increased adoption and increased regulation)—will likely mean more illicit activity in these networks regardless of whether or not regulation increases. And inaction in scenarios in which adoption stalls—Scenario 3 and Scenario 4—effectively cedes these networks to illicit actors in the hopes that regulatory systems catch up.

As a result, SOF should not assume that some other part of the US government (or even the cyber organizations of DOD) will take care of the cryptocurrency problem for them. This means that SOF will need to deepen their knowledge of these issues, which likely entails developing forms of education and training on cryptocurrencies and likely future trends, as well as actively folding lessons from ongoing operations that encounter cryptocurrencies into training for future missions.

To do this, SOF should partner with organizations that have already developed education and training programs. One example is the "Cryptocurrencies and Dark Web" training that the US Department of Homeland Security's Homeland Security Investigations office has been conducting.[187] Another potential source of information and support is Blockchain Alliance. This organization is explicitly oriented towards helping law enforcement combat nefarious activity

[186] EUROPOL, "The Internet Organised Crime Threat Assessment (IOCTA)," EUROPOL, 2015, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

[187] Gregory C. Nevano, Testimony Before the US House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, *Illicit Use of Virtual Currency and the Law Enforcement Response*, June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NevanoG-20180620.pdf.

in the cryptocurrency ecosystem. As their website notes, their mission is to "provide a forum for open dialogue between industry and law enforcement and regulatory agencies, in order to help combat criminal activity on the blockchain."[188] Unfortunately, most of the resources that Blockchain Alliance provides—in the form of conference calls, information sessions, and technical assistance—are not available to Department of Defense actors because the alliance prefers to preserve its civilian/law enforcement focus.[189] However, given SOF's close partnership with many law enforcement agencies, some transfer of information may still be possible.

Taken individually, the issues enumerated in the sections above present clear challenges for US government (including DOD and SOF) actors operating in this space. Perhaps most significant, though, is that the combination of these challenges (the uncertain future, the constant technological evolution, and the general lack of knowledge, training, and education on cryptocurrencies within DOD) makes the technology appear to be more marginal than it really is and ensures it remains poorly understood. The combination of these factors may continue to make it difficult to persuade DOD entities to dedicate adequate resources to properly address this constantly changing technology.

Opportunities for SOF

Because the cryptocurrency ecosystem is evolving, those with the knowledge and resources to act have many opportunities. In the section below, we focus on opportunities related to national security issues. We chose these scenarios in part because we assessed them to be viable options. They include exploiting the existing technology, collaborating with new partners, shaping the future environment, and taking advantage of cryptocurrencies as users. Other possibilities are also imaginable; for example, it is not impossible to imagine SOF creating a cryptocurrency (likely in collaboration with the intelligence community) as a "honeypot" for nefarious actors. We focused, though, on more modest possibilities.

Exploit vulnerable existing technology

As this report highlights, the existing technology is by no means invulnerable to exploitation. As private industry experts told us, Bitcoin and blockchain provide advantages to investigators over criminals if you learn how to master the software and the tracing capabilities.[190] SOF

[188] Blockchain Alliance Forum, accessed June 3, 2019, https://blockchainalliance.org/.

[189] Megan McBride and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

[190] Ibid.

might mine information about individual users and transactions through at least two vectors: exchanges and identities.

First, cryptocurrency exchanges represent a potentially rich source of information for SOF not only as organizations report suspicious activity, but also as potential weaknesses in the targeted chain of illicit actions are revealed. Because nefarious actors cannot rely exclusively on cryptocurrencies, government actors can target the transaction points where cryptocurrency intersects with traditional financial systems.[191] One industry expert, when asked about structural vulnerabilities, argued that the weakest point is the gateway between cryptocurrency and the rest of the financial system.[192] He made the case that a terrorist movement accepting donations in cryptocurrency would still need to turn that cryptocurrency into "real money" to make it useful.[193] Thus, as long as cryptocurrencies remain marginal and unstable, nefarious actors will need to convert them into conventional currencies when their transactions are complete. These conversions, however, are a clear vulnerability that a variety of US government actors (including SOF) can exploit.

Second, despite a widespread belief that cryptocurrency transactions are anonymous, most coins offer mere pseudonymity. As a result, if an individual's real-world identity is uncovered, the (mostly immutable) public blockchain provides a complete record of all her past actions with that cryptocurrency. This will make it possible to track not only the individual's financial actions, but also the other users with whom those transactions were processed—turning the blockchain into a rich resource for social network analysis. Research suggests, moreover, that widely recognized cryptocurrencies such as Bitcoin are vulnerable to unmasking and can often be linked to personally identifying information.[194] Thus, should SOF collect the relevant information during a raid on a terrorist compound (e.g., information on a cryptocurrency wallet), that information could yield valuable data not only on the movement of funds but also on the terrorist network and its finance operations. Of course, to do this, SOF first need to know what to look for in regards to cryptocurrency usage among such actors.

---

[191] Gregory C. Nevano, Testimony Before the US House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, *Illicit Use of Virtual Currency and the Law Enforcement Response,* June 20, 2018, https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NevanoG-20180620.pdf.

[192] Megan McBride, conversation with industry expert, Feb. 5, 2019.

[193] Ibid.

[194] Husam Al Jawaheri, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad, "When a Small Leak Sinks a Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis," Cornell University's arXiv.org archive, Apr. 11, 2018, https://arxiv.org/pdf/1801.07501.pdf, 1-2.

In addition to the vulnerabilities mentioned above, the unique profiles and signatures of large-scale mining operations make it possible to target these locations via both cyber and tactical operations. For example, mining operations are characterized by the "immense power consumption [that] is needed on a consistent basis" and relatively "low foot traffic."[195] These signatures—in combination with other intelligence—may facilitate the identification and targeting of such locations.

In good news, these vulnerabilities can be meaningfully exploited in at least three of the four futures imagined: Scenario 1 (increased adoption and stalled regulation), Scenario 2 (increased adoption and increased regulation), and Scenario 4 (stalled adoption and stalled regulation). The only future in which these vulnerabilities lose significance is perhaps Scenario 3 (stalled adoption and increased regulation) because in this future, regulatory systems effectively drive nefarious actors away from cryptocurrencies (thus negating the possibility that SOF might exploit these vulnerabilities).

Collaborate with (or lead) new partners

Our research in this area showed that relatively few US government entities are knowledgeable about, or actively working in, the cryptocurrency ecosystem. The novelty and complexity of the technology make acquiring expertise a challenge (exacerbated by the realities of a classification system that does not always facilitate cooperation). This situation is further complicated when the parties involved are the Departments of Justice, Treasury, and Defense, since the three operate under different authorities and sometimes pursue different objectives. Though this lack of widespread expertise presents a challenge (as outlined above), it also presents at least three potential opportunities for SOF.

The first is increased opportunity to collaborate with new partners. Our analysis did identify a few pockets of excellence where there was clear US government expertise in a specific realm of cryptocurrency (e.g., the regulatory environment, the range of illicit uses). Where such expertise exists, there is the potential for SOF to partner both operationally and intellectually. As one example, SOF might aggressively target nefarious actors using cryptocurrencies (e.g., by exploiting the blockchain, by convincing a cryptocurrency user to cooperate), and they could potentially direct illicit actors to specific exchanges that Treasury has visibility into.

Second, where such expertise is lacking, SOF have the opportunity to collaborate in ways that might maximize the collective ability to track activity in that arena. This might be done in many ways, including divvying up focus on various regions, actors, or specific cryptocurrencies;

[195] William Allen, "Cryptocurrency in Threat Finance: The Manipulation of Non-Fiat Digital Currencies to Finance Nefarious Actors," *Small Wars Journal*, accessed June 3, 2019, https://smallwarsjournal.com/jrnl/art/cryptocurrency-threat-finance-manipulation-non-fiat-digital-currencies-finance-nefarious.

creating a cryptocurrency community of interest with regular coordination/sync/sharing meetings; or coordinating educational opportunities across the US government.

Third, because the technology is relatively new, many parts of the US government (e.g., FBI, Treasury) are confronting the same challenges as SOF. As such, there is at present no clear leader or center of excellence for cryptocurrency knowledge. Moreover, it may be tempting to frame cryptocurrencies in financial terms that suggest Treasury as the natural leader in this space. Others have argued, though, for a framework that positions DOD at the fore of the challenge. As one article noted:

> It is important to understand that money is trust, an idea, and therefore an information related capability (IRC). [DOD] already [has] skilled professionals who integrate and synchronize IRCs "to influence, disrupt, corrupt, or usurp decision making" in information markets like those that Bitcoin presents; information operations professionals must lead this new fight.[196]

This presents SOF with the opportunity to potentially assume the role of knowledge leader—or cultivate a center of excellence—in this arena. SOF might, for example, develop a robust internal expertise and/or initiate the types of collaborative activities mentioned in the previous paragraph.

The potential benefits available to SOF through cultivating new partnerships can be reaped in all four of the futures imagined. In each instance, SOF has the opportunity—in the short- and mid-term—to forge new relationships (as a partner or as a leader) that might potentially have benefits that far outweigh the challenges provided by the cryptocurrency ecosystem.

Shape the future environment

Another opportunity available to SOF stems from the new and developing nature of the technology. Because so much is currently still evolving, SOF have a chance to think through and advocate for (ideally in collaboration with other US government stakeholders) regulatory actions that might be helpful from an operational standpoint. Alternatively, if the current regulatory environment is beneficial to SOF, they could argue against certain regulatory actions.

As one example, Treasury currently treats cryptocurrencies as an asset and is consequently focused on cryptocurrency exchanges. This creates an opportunity for SOF (and other DOD counter threat finance entities) to complement Treasury's work by exploiting cryptocurrencies the same way they exploit other types of assets seized from nefarious actors. It is entirely possible, however, that Treasury may eventually be inclined (or pressured) to change its

[196] Chris Telley, "A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency," *Small Wars Journal*, https://smallwarsjournal.com/jrnl/art/coin-tsar-two-disruptive-sides-cryptocurrency.

position, at which point SOF may weigh in on the potential advantages and disadvantages of such a shift.

That said, SOF will not be the only US government entity with a vested interest in influencing the future regulatory environment (nor are US actors the only ones with influence given the still nascent nature of the global regulatory environment). As such, they will need to be prepared to adapt their thinking as the future comes into focus and the regulatory environment takes shape.

Moreover, this path is viable only to the extent that the regulatory environment—both domestically and globally—continues to evolve in response to this challenge. In other words, this path will bear significant fruit in only two of the futures imagined: Scenario 2 (increased adoption and increased regulation) and Scenario 3 (stalled adoption and increased regulation). If there is no movement towards increased regulation, then SOF will have nothing to influence (though there will be increased flexibility for SOF to operate in these unregulated spaces).

Exploit the vulnerabilities of cryptocurrencies as users

As this report highlights, nefarious actors are drawn to a variety of cryptocurrency features. The reality, however, is that these same features are available to SOF (until regulatory frameworks and/or more restrictive authorities prevent such activities). SOF thus might benefit from using cryptocurrencies to mask their activities in the same way that illicit actors use cryptocurrencies.

Assuming the appropriate authorities are in place or can be established, potential applications that fit into this category include:

- SOF could use cryptocurrencies to make "anonymous" purchases.
- SOF could use cryptocurrencies to make black market purchases.[197]
- SOF could use captured wallets to engage in masked cryptocurrency activity.
- SOF could target nefarious actors using cryptocurrencies (via hacking, ransomware, etc.).
- SOF could use cryptocurrencies to facilitate payments.
    - SOF might, as private industry experts suggested in an interview, use cryptocurrencies to pay ransoms. In this scenario, they might post a reward for

[197] Blake Miles, "Bloodchits to Bitcoins: Special Operations Uses for Cryptocurrencies," *Havok Journal*, Oct. 27, 2018, https://havokjournal.com/national-security/bloodchits-to-bitcoins-special-operations-uses-for-cryptocurrency/.

the safe return of a US citizen that anyone could claim using a wallet on their phone.[198]

- SOF might use cryptocurrency smart contracts to coordinate payment parameters and the transfer of funds without face-to-face meetings.[199] As one example, a smart contract might require an individual to upload a photograph of a target, after which the contract would execute, and the individual would receive payment.[200]

The reality is that the cryptocurrency ecosystem—including the technology and the regulatory environment—is still evolving and it is not clear what the future holds. Although this ongoing evolution represents a challenge in some registers (e.g., training and education), it unquestionably represents an opportunity in other registers. This anticipated change presents SOF with a constant stream of opportunities via which they might engage creatively and unconventionally with this technology.

That said, this path presents an opportunity for SOF primarily in futures in which the regulatory environment is stalled: Scenario 1 (increased adoption and stalled regulation) and Scenario 4 (stalled adoption and stalled regulation). In these potential futures, SOF will have incredible freedom to operate (authority issues notwithstanding) in this space. If there is a notable increase in regulation, SOF's potential to take advantage of this technology as an end user might be impeded.

[198] Megan McBride and Lauren Frey, conversation with industry experts, Feb. 5, 2019.

[199] A smart contract is "a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract…Smart contracts help you exchange money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman." Ameer Rosic, "Smart Contracts: The Blockchain Technology That Will Replace Lawyers," Blockgeeks, https://blockgeeks.com/guides/smart-contracts/.

[200] Blake Miles, "Bloodchits to Bitcoins: Special Operations Uses for Cryptocurrencies," *Havok Journal*, Oct. 27, 2018, https://havokjournal.com/national-security/bloodchits-to-bitcoins-special-operations-uses-for-cryptocurrency/.

Conclusion

Cryptocurrencies and the technologies related to them are innovations with significant national security implications. In the course of exploring these implications, it became evident that—notwithstanding some pockets of excellence—the US government (including DOD) generally lacked understanding in this area. To help with this challenge, we wrote a companion paper, "Cryptocurrency: A Primer for Policy-Makers," in which we used clear, non-technical language to describe complex concepts and demystify overly technical terms.

In this paper, however, we focused on the implications for the SOF community by assessing the present state of affairs, the range of illicit activities in which cryptocurrencies have played a role, and the potential mid-term futures of the cryptocurrency ecosystem.

In doing this work—consulting with US government, DOD, and private industry experts—we found that cryptocurrencies were not so innovative that they demand fundamentally new systems. Instead, SOF are well-positioned to exploit this technology. As a misunderstood and decentralized technology without a global regulatory system, cryptocurrencies represent opportunities for SOF in at least three registers: (1) a weakness that might be exploited to track illicit activity; (2) a new avenue of exchange that SOF might exploit as a user; and (3) a developing issue via which SOF might establish new relationships as a partner or leader.

As a final note, we recognize that the challenges and opportunities SOF will confront in this space vary considerably across the possible futures we outlined. However, a few clear assertions are possible despite this ambiguity. First, the lack of knowledge, training, and education is problematic regardless of how the future takes shape. As such, SOF should begin by focusing on that challenge, since there is no future in which SOF do not benefit from improvements in this register. Second, SOF have ample opportunities regardless of which possible future is realized. In fact, cryptocurrencies present SOF with more promising paths forward than frustrating dead ends. As Figure 11 illustrates, there is no future in which SOF is unable to exploit this technology.

Figure 11. Likely futures of cryptocurrencies and potential implications for SOF

		Scenario 1: Increased adoption/ Stalled regulation	Scenario 2: Increased adoption/ Increased regulation	Scenario 3: Stalled adoption/ Increased regulation	Scenario 4: Stalled adoption/ Stalled regulation
Challenges	Fractured regulatory environment	↓	↔	↑	↔
	Evolution of technology (and nefarious behaviors)	↓	↔	↑	↔
	Lack of knowledge, training, and education	↓	↓	↓	↓
Opportunities	Exploitable existing technology	↑	↑	↔	↑
	Underdeveloped partnerships	↑	↑	↑	↑
	Malleable future environment	↔	↑	↑	↔
	Underexplored potential applications	↑	↔	↔	↑

Mid-term implications for SOF given its existing posture	
↓	Negative
↔	Neutral
↑	Positive

Source: CNA.

At present, widespread expertise regarding cryptocurrencies is lacking in the US government, and more detailed analysis of the specific issues raised in this paper is needed to fully explore and understand them. But there is also a clear path forward and thus little doubt that SOF should be looking at cryptocurrencies in more detail, to both mitigate the challenges and exploit the opportunities that we identified in our research.

Figures

Abbreviations

AQ	al-Qaeda
ATM	automated teller machine
BCH	Bitcoin Cash
BTC	Bitcoin
BTM	Bitcoin ATM
CIA	Central Intelligence Agency
CNAS	Center for a New American Security
DASH	Dash
DOD	Department of Defense
ETH	Ethereum
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
GRU	Main Intelligence Directorate (Russia)
HSI	Homeland Security Investigations
IRC	information related capability
IRS	Internal Revenue Service
IS	Islamic State
JSOU	Joint Special Operations University
LTC	Litecoin
OGP	Operation Gallant Phoenix
SAR	suspicious activity report
SOF	Special Operations Forces
WMD	weapons of mass destruction
XMR	Monero
XRP	Ripple
ZEC	ZCash

References

Adler, David. "Silk Road: The Dark Side of Cryptocurrency." *Fordham Journal of Corporate & Financial Law* (blog). Feb. 1, 2018. https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/.

Al Jawaheri, Husam, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad. "When a Small Leak Sinks a Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis." Cornell University arXiv.org. Apr. 11, 2018. https://arxiv.org/pdf/1801.07501.pdf.

Allen, William. "Cryptocurrency in Threat Finance: The Manipulation of Non-Fiat Digital Currencies to Finance Nefarious Actors." *Small Wars Journal*. Accessed June 3, 2019. https://smallwarsjournal.com/jrnl/art/cryptocurrency-threat-finance-manipulation-non-fiat-digital-currencies-finance-nefarious.

Androitis, AnnaMaria, Liz Hoffman, Peter Rudegeair, and Jeff Horwitz. "Facebook Building Cryptocurrency-Based Payments System." *Wall Street Journal*. May 2, 2019. https://www.wsj.com/articles/facebook-building-cryptocurrency-based-payments-system-11556837547.

Avan-Nomayo, Osato. "Bitcoin 51% Attack Is Unrealistic, New Study Concludes." Bitcoinist. Nov. 26, 2018. https://bitcoinist.com/bitcoin-51-percent-attack-study/.

Bajak, Ralph, and Raphael Satter. "Companies Still Hobbled from Fearsome Cyberattack." AP News. June 30, 2019. https://www.apnews.com/ce7a8aca506742ab8e8873e7f9f229c2.

Baker, Michael. "How Cryptocurrencies Are Fueling Ransomware Attacks and Other Cybercrimes." *Forbes*. Aug. 3, 2017. https://www.forbes.com/sites/forbestechcouncil/2017/08/03/how-cryptocurrencies-are-fueling-ransomware-attacks-and-other-cybercrimes/#284696fe3c15.

"Bitcoin Anonymity – Is Bitcoin Anonymous?" *Buy Bitcoin Worldwide*. Accessed May 2, 2019. https://www.buybitcoinworldwide.com/anonymity/.

"Bitcoin ATMs by Country." Coin ATM Radar. https://coinatmradar.com/countries/.

"Bitcoin Futures Trading." Forex.com. Accessed May 17, 2019. https://www.forex.com/en-us/education/education-themes/trading-concepts/bitcoin-futures-trading/.

"Bitcoin Mining Costs Throughout the World." *Elite Fixtures* (blog). Feb. 26, 2018. https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/.Blockchain Alliance Forum. Accessed June 3, 2019. https://blockchainalliance.org/.

Boorstin, Julia. “Facebook Launches a New Cryptocurrency Called Libra.” CNBC.com. June 18, 2019. https://www.cnbc.com/2019/06/17/facebook-announces-libra-digital-currency-calibra-digital-wallet.html.

Brend, Yvette. “Sudden Death of Cryptocurrency Leader Sends Quadriga into Tailspin, Panicking Clients.” CBC News. Feb. 4, 2019. https://www.cbc.ca/news/canada/british-columbia/quadriga-cryptocurrency-bitcoin-exchange-gerald-cotten-death-india-1.5002955.

Browne, Ryan. “Cryptocurrencies Have Shed Almost $700 Billion Since January Peak.” CNBC. Nov. 23, 2018. https://www.cnbc.com/2018/11/23/cryptocurrencies-have-shed-almost-700-billion-since-january-peak.html.

Carlisle, David, and Kayla Izenman. "Closing the Crypto Gap: Guidance for Countering North Korean Cryptocurrency Activity in Southeast Asia." Royal United Services Institute. Apr. 2019. Accessed Apr. 26, 2019. https://rusi.org/sites/default/files/20190412_closing_the_crypto_gap_web.pdf.

Chainalysis Team. “The Changing Nature of Cryptocrime.” *Insights* (blog). Jan. 18, 2018. https://blog.chainalysis.com/reports/report-the-changing-nature-of-cryptocrime.

“Cryptocurrency.” Merriam-Webster. https://www.merriam-webster.com/dictionary/cryptocurrency.

De, Nikhilesh. “Survey: Nearly 80% of Americans Have Heard of Bitcoin.” Coindesk. Sept. 6, 2018. https://www.coindesk.com/survey-nearly-80-of-americans-have-heard-of-bitcoin.

De Best, Raynor. “How Many Consumers Own Cryptocurrency?” Statista. Aug. 20, 2018. https://www.statista.com/chart/15137/how-many-consumers-own-cryptocurrency/.

Deka, Chayanika. “Venezuela’s Petro: Fresh Trouble Surfaced as Report Suggests ‘Conclusive Evidence’ of Money Laundering.” AMBCRYPTO. Feb. 27, 2019. https://ambcrypto.com/venezuelas-petro-fresh-trouble-surfaces-as-report-suggests-conclusive-evidence-of-money-laundering/.

“The Dictionary Just Got a Whole Lot Bigger.” Merriam-Webster. Mar. 2018. https://www.merriam-webster.com/words-at-play/new-words-in-the-dictionary-march-2018.

“Digital Currencies: International Actions and Regulations.” Perkins Coie. Updated May 2019. Accessed May 1, 2019. https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html.

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

"Dividing the Cryptocurrency Sheep from the Blockchain Goats." *Economist Technology Quarterly*. Aug. 30, 2018. https://www.economist.com/technology-quarterly/2018/09/01/dividing-the-cryptocurrency-sheep-from-the-blockchain-goats.

Dudley, Sara, Travis Pond, Ryan Roseberry, and Shawn Carden. "Evasive Maneuvers: How Malign Actors Leverage Cryptocurrency." *Joint Forces Quarterly* 92, no. 1 (2019). https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_58-64_Dudley-et-al.pdf.

Dunford, Joseph F. Jr. *Statement Before the Senate Armed Services Committee, Department of Defense Budget Hearing*. Mar. 14, 2019. https://www.armed-services.senate.gov/imo/media/doc/Dunford_03-14-19.pdf.

Eimiller, Laura. "Electronic Crimes Task Force Collaborates with Europol to Target Bitcoin Distributed Denial of Service Attacks." FBI. Jan. 13, 2016. https://www.fbi.gov/contact-us/field-offices/losangeles/news/press-releases/electronic-crimes-task-force-collaborates-with-europol-to-target-bitcoin-distributed-denial-of-service-attacks.

"El Petro." Gobiemo Bolivariana de Venezuela. 2018. https://petro.gob.ve/index.html.

Ellsworth, Brian. "Special Report: In Venezuela, New Cryptocurrency Is Nowhere to Be Found." Reuters, Aug. 30, 2018. https://www.reuters.com/article/us-cryptocurrency-venezuela-specialrepor/special-report-in-venezuela-new-cryptocurrency-is-nowhere-to-be-found-idUSKCN1LF15U.

EUROPOL. "The Internet Organised Crime Threat Assessment (IOCTA)." Official EUROPOL website. 2015. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

"Fact Sheet: DHS Cybersecurity Policy." US Department of Homeland Security. Aug. 22, 2018. https://www.dhs.gov/news/2018/05/15/fact-sheet-dhs-cybersecurity-policy.

Fanusie, Yaya. "Hamas Military Wing Crowdfunding Bitcoin." *Forbes*. Feb. 4, 2019. https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#1588fe884d7f.

---- "The New Frontier in Terror Fundraising: Bitcoin." Cipher Brief. Aug. 24, 2016. https://www.thecipherbrief.com/column/private-sector/the-new-frontier-in-terror-fundraising-bitcoin.

FATF Report to G20 Leaders' Summit. Financial Action Task Force. Apr. 2019. http://www.fatf-gafi.org/media/fatf/documents/G20-April-2019.pdf.

Fiorillo, Steve. "What Is Cryptocurrency? Everything You Need to Know." *The Street*. Aug. 14, 2018. https://www.thestreet.com/investing/bitcoin/what-is-cryptocurrency-14679467.

Foley, Sean, Jonathan R. Karlsen, and Talis J. Putnins. "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?" Review of Financial Studies. Dec. 14, 2018. https://ssrn.com/abstract=3102645.

"Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million Through His Digital Currency Business." US Department of Justice. PRN 16-113. Jan. 29, 2016. https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.

Frankenfield, Jake, ed. "51% Attack." Investopedia. Feb. 7, 2019. https://www.investopedia.com/terms/1/51-attack.asp.

Garamone, Jim. "Dunford Asks Defense Chiefs to Guard Against Complacency." Joint Chiefs of Staff. https://www.jcs.mil/Media/News/News-Display/Article/1664622/dunford-asks-defense-chiefs-to-guard-against-complacency/.

Georgiev, Georgi. "Russia: Oil-Backed Cryptocurrency in 'Final Stage of Development.'" Bitcoinist. Feb. 22, 2019. https://bitcoinist.com/russia-oil-cryptocurrency-law/.

Gola, Yashu. "Russia to Regulate Crypto While Launching Its Own Oil-Backed Cryptocurrency." CCN. Feb. 24, 2019. https://www.ccn.com/russia-regulate-cryptop-with-a-keen-eye-on-oil-backed-digital-currency.

Goldman, Zachary K., Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss. "Terrorist Use of Virtual Currencies." Center for a New American Security. May 2017. http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf.

Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Financial Actio Task Force. June 2019. https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf.

Hackett, Robert. "Why You Shouldn't Pay the Petya Ransom." *Fortune*. June 28, 2017, http://fortune.com/2017/06/28/ransom-bitcoin-petya/.

Helms, Kevin. "Putin's Order: Russia to Adopt Crypto Regulation by July." Bitcoin.com. Feb. 28, 2019. https://news.bitcoin.com/putins-order-russia-cryptocurrency-regulation/.

---- "Venezuela Makes Petro Crypto a National Currency, Publishes New Whitepaper." News: Bitcoin.com. Oct. 4, 2018. https://news.bitcoin.com/venezuela-petro-new-whitepaper/.

Herbst, Julia. "A Comprehensive Guide to Crypto References in Pop Culture." *BREAKERMAG*. Oct. 29, 2018. https://breakermag.com/a-comprehensive-list-of-crypto-references-in-pop-culture/.

Hertig, Alyssa. "Blockchain Feared 51% Attack Now Becoming Regular." Coindesk. June 8, 2018. https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular.

Hidalgo, Miles. "Beyond the Conflict Zone: US HIS Cooperation with Europol." *CTC Sentinel* 11, no. 2 (Feb. 2018). https://ctc.usma.edu/beyond-conflict-zone-u-s-hsi-cooperation-europol.

Hileman, Garrick, and Michael Rauchs. "Global Cryptocurrency Benchmarking Study." University of Cambridge Judge Business School Centre for Alternative Finance. 2017. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-cryptocurrency/.

Holger, Dieter. "Over 16 Million Americans Now Own Cryptocurrency, Survey Finds." Bitcoinist.com. Mar. 19, 2018. https://bitcoinist.com/16-million-americans-cryptocurrency/.

ICO Manager, "How Many People Own Cryptocurrency." ICO Making. Jan. 14, 2019. https://icomaking.com/how-many-people-own-cryptocurrency/.

"The In's and Out's of Cryptographic Hash Functions." Blockgeeks. 2018. Accessed May 17, 2019. https://blockgeeks.com/guides/cryptographic-hash-functions/.

Inman, Phillip. "IMF Says Governments Could Set Up Their Own Cryptocurrencies." *Guardian*, Nov. 13, 2018. https://www.theguardian.com/business/2018/nov/14/imf-says-governments-could-set-up-their-own-cryptocurrencies.

"International Action Against DD4BC Cybercriminal Group." EUROPOL. Jan. 12, 2016. https://www.europol.europa.eu/newsroom/news/international-action-against-dd4bc-cybercriminal-group.

"The Internet Organised Crime Threat Assessment (IOCTA)." EUROPOL. 2015. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015.

"Is Bitcoin Anonymous?" *Bitcoin Magazine*. Accessed May 2, 2019. https://bitcoinmagazine.com/guides/bitcoin-anonymous/.

Jakubauskas, Rytis. "How Many People Actually Own Cryptocurrency?" Dalia. May 11, 2018. https://daliaresearch.com/blog-cryptocurrency-ownership/.

Jenkinson, Gareth. "Ethereum Classic 51% Attack—The Reality of Proof-of-Work." Cointelegraph. Jan. 10, 2019. https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work.

Joint Special Operations University, *Special Operations Research Topics 2018 (Revised Edition for Academic Year 2019)*. MacDill AFB, FL: JSOU Press, 2018. https://jsou.libguides.com/ld.php?content_id=41898487.

Kharpal, Arjun. "Over 800 Cryptocurrencies Are Now Dead as Bitcoin Is 70 Percent off Its Record High." CNBC. Jul. 2, 2018. https://www.cnbc.com/2018/07/02/over-800-cryptocurrencies-are-now-dead-as-bitcoin-feels-pressure.html.

Khatri, Yogita. "Gold-Backed Cryptocurrencies Launched by Iranian Banks: Report." Coindesk. Feb. 5, 2019. https://www.coindesk.com/gold-backed-cryptocurrency-launched-by-iranian-banks-report.

---- "Venezuela to Sell Oil for Petro Cryptocurrency, Says Maduro." Coindesk. Dec. 7, 2018. https://www.coindesk.com/venezuela-to-sell-oil-for-petro-cryptocurrency-in-2019-says-maduro.

Kim, Esther. "3 Countries Tell IMF They Want to Issue Bitcoin Bonds." Bitcoinist. Apr. 17, 2019. https://bitcoinist.com/these-3-countries-tell-imf-they-want-to-issue-bitcoin-bonds/.

Lam, Eric. "Here's What Maduro Has Said of Venezuela's Petro Cryptocurrency." *Bloomberg*. Aug. 20, 2018. https://www.bloomberg.com/news/articles/2018-08-20/here-s-what-maduro-has-said-of-venezuela-s-petro-cryptocurrency.

Lee, Su-Hyun, and Nathaniel Popper. "In South Korea, the Virtual Currency Boom Hits Home." *New York Times*. Dec. 3, 2017. https://www.nytimes.com/2017/12/03/technology/virtual-currency-south-korea.html.

"Libra White Paper." Libra Association. 2019. https://libra.org/en-US/white-paper/.

Lielacher, Alex. "How Many People Use Bitcoin in 2019?" Bitcoin Market Journal. Feb. 11, 2018. https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/.

Lowrey, Annie. "Bitcoin Is Falling Out of Favor on the Dark Web." *Atlantic*. Mar. 1, 2018. https://www.theatlantic.com/business/archive/2018/03/bitcoin-crash-dark-web/553190/.

"Making Sense of Bitcoin, Cryptocurrency, and Blockchain." Pwc United States. Accessed Mar. 20, 2019. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html.

Malik, Nikita. "How Criminals and Terrorists Use Cryptocurrency: And How to Stop It." *Forbes*. Aug. 31, 2018. https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#68fb07f83990.

Manheim, David, Patrick B. Johnston, Joshua Baron, and Cynthia Dion-Schwarz. "Are Terrorists Using Cryptocurrencies?" *The RAND Blog.* Apr. 21, 2017. https://www.rand.org/blog/2017/04/are-terrorists-using-cryptocurrencies.html.

McBride, Megan. Conversation with industry expert. Feb. 5, 2019.

McBride, Megan. Conversation with industry expert. Feb. 28, 2019.

McBride, Megan. Conversation with SOCOM personnel. Jan. 25, 2019.

McBride, Megan, and Lauren Frey. Conversation with industry experts. Feb. 5, 2019.

McBride, Megan, and Lauren Frey. Conversation with US officials. Feb. 5, 2019.

McBride, Megan, and Lauren Frey. Conversation with US officials. Mar. 1, 2019.

Memoria, Francisco. "Turns Out Venezuela's Oil-Backed Petro Cryptocurrency Is Real After All." CCN. Jan. 28, 2019. https://www.ccn.com/turns-out-venezuelas-oil-backed-petro-cryptocurrency-is-real-after-all.

Miles, Blake. "Bloodchits to Bitcoins: Special Operations Uses for Cryptocurrencies." *Havok Journal*. Oct. 27, 2018. https://havokjournal.com/national-security/bloodchits-to-bitcoins-special-operations-uses-for-cryptocurrency/.

Mitchell, Bonnie, Krystle Kaul, G.S. McNamara, Michelle Tucker, Jacqueline Hicks, Colin Bliss, Rhonda Ober, Danell Castro, Amber Wells, Catalina Reguerin, Cindy Green-Ortiz, and Ken Stavioha. "Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation." Office of the Director of National Intelligence. 2017. https://www.odni.gov/files/PE/Documents/10---2017-AEP_Going-Dark.pdf.

Motamedi, Maziar. "Iran's Central Bank Issues Draft Rules on Cryptocurrency." Aljazeera. Jan. 29, 2019. https://www.aljazeera.com/news/2019/01/iran-central-bank-issues-draft-rules-cryptocurrency-190129051653656.html.

Nadeau, Michael. "What Is Cryptojacking? How to Prevent, Detect, and Recover from It." CSO. Dec. 13, 2018. https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html.

Nakashima, Ellen. "Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes." *Washington Post*. Jan. 12, 2018. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

National Strategy for Counterterrorism of the United States of America. White House. Oct. 2018, https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.

"National Terrorist Financing Risk Assessment." US Department of the Treasury. 2018. https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf.

Nevano, Gregory C. Testimony Before the US House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, *Illicit Use of Virtual Currency and the Law Enforcement Response*. June 20, 2018. https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NevanoG-20180620.pdf.

Novy, Robert. *Prepared Testimony Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance*. June 20, 2018. https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-NovyR-20180620.pdf.

Nuzzi, Lucas. "ZEC: Unmatched Privacy in a Public Blockchain." *Medium*. Sept. 17, 2018. https://medium.com/digitalassetresearch/zec-best-in-class-privacy-in-a-public-blockchain-1df2a3728739.

"OFAC FAQs: Sanctions Compliance." US Department of the Treasury. Last updated Feb. 6, 2019. Accessed May 22, 2019. https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs.

Office of Terrorism and Financial Intelligence. National Strategy for Combating Terrorist and Other Illicit Financing. US Department of the Treasury. 2018. 37.

Osborne, Charlie. "The Mt. Gox Bitcoin Debacle: Bankruptcy Filed, Customer Bitcoin Lost." ZDNet. Feb. 25, 2014. https://www.zdnet.com/article/the-mt-gox-bitcoin-debacle-bankruptcy-filed-customer-bitcoin-lost/.

Ott, Thomas P. Testimony for the Record Before the House Committee on Financial Services Subcommittee on Terrorism and Illicit Finance. June 20, 2018. https://docs.house.gov/meetings/BA/BA01/20180620/108476/HHRG-115-BA01-Wstate-OttT-20180620.pdf.

"PayPal Adds 8M Active Users, Grows Mobile Volume 52 Percent." PYMNTS.com. Apr. 26, 2018. https://www.pymnts.com/earnings/2018/paypal-earnings-mobile-volume-user-growth-barclays/.

Perlroth, Nicole, and Katie Benner. "Iranians Accused in Cyberattacks, Including One That Hobbled Atlanta." *New York Times*. Nov. 28, 2018. https://www.nytimes.com/2018/11/28/us/politics/atlanta-cyberattack-iran.html?module=inline.

Pillon, Elizabeth, and Lee Nicholson. "First Report of the Monitor." *Supreme Court of Nova Scotia Hfx, No. 484742*. Feb. 12, 2019. https://www.scribd.com/document/399507173/EY-QuadrigaCX-Report.

"Ransomware." Dictionary.com. https://www.dictionary.com/browse/ransomware.

Rapoza, Kenneth. "Will Russia Make Any Waves in Crypto This Year?" *Forbes*. Jan. 2, 2019. https://www.forbes.com/sites/kenrapoza/2019/01/02/will-russia-make-any-waves-in-crypto-this-year/#29f203684271.

Rosic, Ameer. "Smart Contracts: The Blockchain Technology That Will Replace Lawyers." Blockgeeks. https://blockgeeks.com/guides/smart-contracts/.

Roubini, Nouriel. "Why Central Bank Digital Currencies Will Destroy Bitcoin." *Guardian*. Nov. 19, 2018. https://www.theguardian.com/business/2018/nov/19/why-central-bank-digital-currencies-will-destroy-bitcoin.

"Russia and Venezuela Plan Cryptocurrencies." *Weekend Edition Saturday* and National Public Radio. Jan. 6, 2018. https://www.npr.org/2018/01/06/576197773/russia-and-venezuela-plan-cryptocurrencies.

Schoenberg, Tom, and Matt Robinson. "Bitcoin ATMs May Be Used to Launder Money." *Bloomberg Businessweek*. Dec. 14, 2018. https://www.bloomberg.com/features/2018-bitcoin-atm-money-laundering/.

Schroden, Jonathan. Conversation with US Army finance officer. Feb. 22, 2019.

Seward, Zack. "US Lawmakers Seek Sanctions Against Iran's Cryptocurrency Efforts." Coindesk. Dec. 21, 2018. https://www.coindesk.com/us-lawmakers-seek-sanctions-against-irans-cryptocurrency-efforts.

Sraders, Anne. "What Is Litecoin? What to Know in 2019." Dec. 18, 2018. https://www.thestreet.com/investing/what-is-litecoin-14813041.

Suburg, William. "North Korea Launched Cryptocurrency Attacks in Response to Sanctions, FBI Says." Cointelegraph. May 30, 2019. https://cointelegraph.com/news/north-korea-launched-cryptocurrency-attacks-in-response-to-sanctions-says-fbi.

Sullivan, Emily. "Ransomware Cyberattacks Knock Baltimore's City Services Offline." NPR. May 21, 2019. https://www.npr.org/2019/05/21/725118702/ransomware-cyberattacks-on-baltimore-put-city-services-offline.

Sykes, Jay B., and Nicole Vanatko. "Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals." Congressional Research Service. Apr. 3, 2019. https://www.everycrsreport.com/files/20190403_R45664_5523da9e96a50aa8d5d3c085f6fd777b8a8112a4.pdf.

Telley, Chris. "A Coin for the Tsar: The Two Disruptive Sides of Cryptocurrency." *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/coin-tsar-two-disruptive-sides-cryptocurrency.

Tonin, Derek. "Afghanistan Considers Turning to Crypto Bonds to Rebuild." CoinGeek. Apr. 22, 2019. https://coingeek.com/afghanistan-considers-turning-to-crypto-bonds-to-rebuild/.

"Top 100 Cryptocurrencies by Market Capitalization." CoinMarketCap. Last accessed Mar. 22, 2019. https://coinmarketcap.com/.

United States Drug Enforcement Agency. "Bitcoin Maven Sentenced to Federal Prison in Virtual Currency Money Laundering Case." Jul. 9, 2018. Accessed May 30, 2019. https://www.dea.gov/press-releases/2018/07/09/bitcoin-maven-sentenced-federal-prison-virtual-currency-money-laundering.

United States of America v. Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkjn, and Anatoliy Sergeyevich Kovalev. Jul. 13, 2018. https://int.nyt.com/data/documenthelper/80-netyksho-et-al-indictment/ba0521c1eef869deecbe/optimized/full.pdf.

US Department of Justice. "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses." Department of Justice Office of Public Affairs. PRN: 18-1559. Nov. 28, 2018. https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

Ward, Antonia. "Bitcoin and the Dark Web: The New Terrorist Threat?" *The RAND Blog*. Jan. 22, 2018. https://www.rand.org/blog/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-.

Weaver, Nicholas. "Inside Risks of Cryptocurrencies." *Viewpoints: Communications of the ACM* 61, no. 6 (June 2018). https://www1.icsi.berkeley.edu/~nweaver/papers/cryptorisks.pdf.

Weimann, Gabriel. "Going Darker? The Challenge of Dark Net Terrorism." Wilson Center. 2016. https://www.wilsoncenter.org/sites/default/files/going_darker_challenge_of_dark_net_terrorism.pdf.

"What Is a Cryptocurrency ATM?" CoinCodex. June 2018. https://coincodex.com/article/1965/what-is-a-cryptocurrency-atm/.

Zhao, Wolfe. "Cheap Power Is Luring Battered Bitcoin Miners to Iran." Coindesk. Dec. 12, 2018. https://www.coindesk.com/cheap-power-lures-crypto-miners-to-iran-but-its-not-as-easy-as-it-sounds.

Zmudzinski, Adrian. "Four Iranian Banks Support Gold-Backed Cryptocurrency." Cointelegraph. Feb. 5, 2019. https://cointelegraph.com/news/four-iranian-banks-support-gold-backed-cryptocurrency.

This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

3003 Washington Boulevard, Arlington, VA 22201

www.cna.org • 703-824-2000

NOBODY GETS CLOSER
TO THE PEOPLE. TO THE DATA. TO THE PROBLEM.

CNA is a not-for-profit research organization that serves the public interest by providing in-depth analysis and result-oriented solutions to help government leaders choose the best course of action in setting policy and managing operations.