



President Nicolás Maduro of Venezuela and President Vladimir Putin discussed bilateral relations and measures to stabilize oil market, Beijing, September 3, 2015 (President of Russia Web site)

# Evasive Maneuvers

## How Malign Actors Leverage Cryptocurrency

By Sara Dudley, Travis Pond, Ryan Roseberry, and Shawn Carden

*All the perplexities, confusion and distress in America arise, not from defects in their Constitution or Confederation, not from want of honor or virtue, so much as from the downright ignorance of the nature of coin, credit and circulation.*

—JOHN ADAMS, LETTER TO THOMAS JEFFERSON, AUGUST 25, 1787

---

Colonel Sara Dudley, USA, is assigned to Joint Special Operations Command. Lieutenant Colonel Travis Pond, USAF, is the Program Acquisition Evaluator at the Department of Defense Office of the Inspector General. Colonel Ryan Roseberry, USA, is an Intelligence Officer assigned to George C. Marshall Center. Colonel Shawn Carden, USA, is the Director of Future Operations at U.S. Army Cyber Command G35.

**T**he U.S. National Defense Strategy outlines a fundamental competition between free and open societies and revisionist powers and rogue regimes. These powers and regimes frequently act below the threshold of war, enabled by recent technological advances. Effective responses to these advances demand

creative solutions. The emergence of cryptocurrencies represents a novel frontier that diminishes U.S. comparative advantage in mapping funding to threat networks worldwide. By disrupting the visibility and control present within the traditional centralized international banking system, the use of cryptocurrencies negates the ability

for U.S. personnel to monitor and restrict funding sources. The ability to follow the money is at risk based on peer-to-peer exchange of encrypted currencies. To probe this vulnerability, explanations of blockchain technologies and cryptocurrencies show how adversaries use the technology to circumvent financial market control and sanction protocols. The U.S. Government will need to act to mitigate the current risk in poorly governed cryptocurrency market places.

## Explaining Cryptocurrency

The global economic system has benefited substantially from the establishment of the free market system since the end of World War II. In 1944, the Bretton Woods Agreement established the U.S. dollar (USD) as the world's reserve currency, providing stability and liquidity that enabled significant growth in international trade. At that time, the USD was backed by U.S. gold reserves, which were the largest in the world.<sup>1</sup> In 1971, President Richard Nixon eliminated the exchangeability of USD for gold, but the strength of the U.S. economy and the norms of international trade created over the previous 20-plus years allowed the USD to retain its status as the world's reserve currency. The market confidence in the U.S. economy, along with centralized governmental monetary policy, continue to support the valuation of the USD internationally. Decentralized cryptocurrencies threaten to undermine the dominance of the USD due to the ways in which they can subvert the global financial system.

A digital or virtual currency maintains three basic pieces: an encryption used to secure each coin, a mathematical proof-of-work used to validate each coin's legitimacy, and a blockchain (database) that records transactions. The blockchain records a transaction history and posts it to a distributed ledger that creates data integrity and visibility to all participants. The desire to use this technology to support a completely free market system, not tethered to any state managed currency, drove the establishment of the segment

leader, Bitcoin, in 2009.<sup>2</sup> All other available cryptocurrency outside of Bitcoin bears the generic label of "altcoin," that is, an alternative to Bitcoin, but operates on similar open-source code. Crucially, these currencies disrupt standard banking systems by introducing a means to establish peer-to-peer transactions without centralized ledger controls.

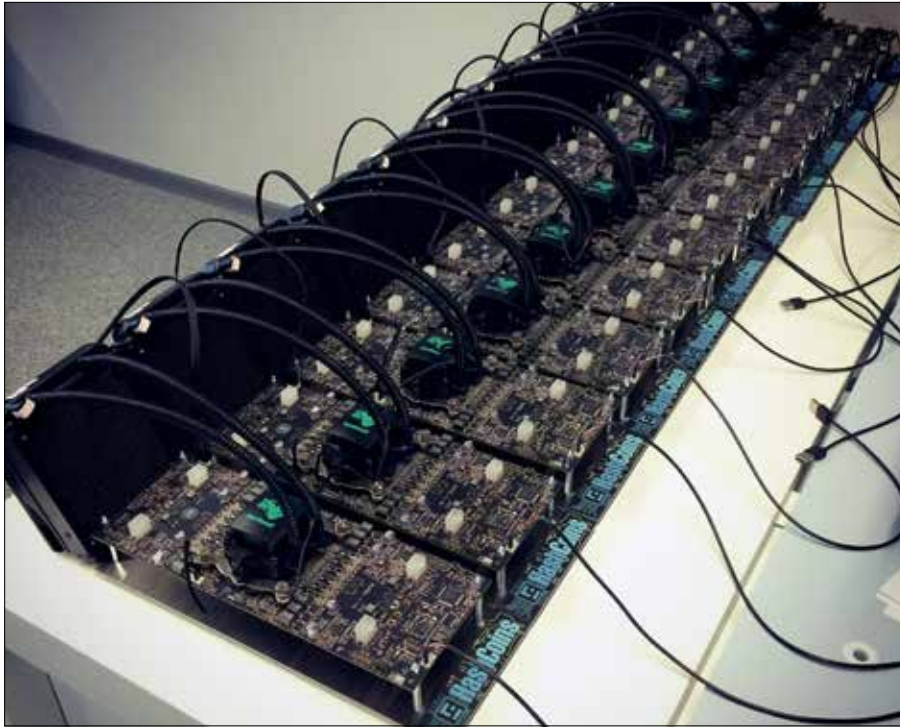
Traditionally, a ledger system that resided in one location stored the total of debits or credits transferred between individuals exchanging currency. While handwritten log books have given way to digital recordkeeping, middlemen (financial institutions) maintain these databases in central locations for easy tracking. However, this traditional method of currency exchange is vulnerable to cyber hacking as well as software and hardware malfunctions. The blockchain application addresses this vulnerability by generating a ledger of transactions verified, validated, and stored by a widely distributed network of autonomous peer computer systems (called mining computers). Various mining computers participate in these blockchains by confirming the transaction records between participant ledgers, and in doing so generate their own profit. A computing source compiles and produces the next block of transactions and mines (or gains) a digital currency token as reward for the effort of solving algorithms. Following the addition of a verified block (combined individual transactions), all computers across the network store the updated database on the distributed blockchain ledger.

The open (public) blockchain ledger effectively resides on thousands of computers participating in the minute-by-minute validation of the blockchain itself. In effect, the distributed blockchain stores and verifies the ledger and, in doing so, eliminates excess transaction fees and other negative externalities associated with single-ledger repositories, for example, the middleman, hacking, and corruption. Championed by a recent World Economic Forum report, blockchain technology allows for broader transparency and integrity in society, including the fight against bribery and

corruption pertaining to monetary transactions because the ledger is public and exists in multiple duplicate copies.<sup>3</sup> The secure, encrypted, transparent, and distributed copies of the blockchain underlying cryptocurrency offer a dramatically new model for financial transactions.

While the international financial community certainly has shown both intrigue and aversion to the potential disruptions in world monetary markets, distributed ledger technology also introduces challenges pertaining to national security. The presence of various middlemen, such as financial institutions, afforded governments the ability to track and trace malign activity through the traditional financial system ledgers. With cryptocurrencies, reputable banks no longer validate an individual's credentials and record his information with each transaction. Rather, anonymity in cryptocurrencies protects point-to-point transactions captured between digitized wallets and encryption keys. This change in the traditional process for managing financial transactions undermines regulatory anti-money laundering efforts performed by financial institutions, which are intended to thwart players attempting to skirt sanctions and finance terror groups. While perhaps not immediately obvious to the casual observer, nonstate actor use and increasing state actor pursuit of cryptocurrencies extend the competitive space into the international financial domain and spotlight cryptocurrency as a national security issue that should concern the Department of Defense (DOD) and Intelligence Community.<sup>4</sup>

The rapid growth of weakly regulated financial and technology markets creates vulnerabilities for safeguarding the international financial system from malign actors. Hence, the nexus of crime, corruption, and terrorism finds refuge in these emergent financial systems.<sup>5</sup> Aside from the benefits of cryptocurrencies, which include providing an attractive means for malign actors to conceal illicit funding and business, and to earn currency by mining, the technology attributes alone attract malfeasance. While the distributed blockchain ledger remains



Mining kit based on golden nonce chip, May 20, 2015 (Alexandr Gromov)

resistant to cyber criminals, the storage of the digital coins (that is, private key encryptions) remains a system weakness.

While pointed out earlier that traditional ledger systems are vulnerable, theft of cryptocurrencies requires less hacking skill than penetrating the centralized ledger systems, which banks have hardened. Secure digital storage of the private and public key information associated with cryptocurrency exists outside the blockchain within individual computers, exchange markets, and businesses established to provide offline, or cold-storage. Similar to a brokerage house converting shares of a company into cash for a seller, cryptocurrency exchanges support the transition of the digital currency back into a fiat currency like the USD. Theft of the encryption keys for a coin gives a criminal carte blanche to spend it without the need for identification. Due to the need to secure the encryption keys from theft by hackers, some exchanges and separate businesses now exist to safeguard the encryption keys offline in the equivalent of digital safe deposit boxes. The introduction of these cryptocurrency technologies disrupts not only financial markets but also efforts to monitor and maintain the

integrity of financial exchange. The anonymity of use, low barriers to entry, and weak regulation and limited legal jurisdiction in the cryptocurrency marketplace represent an opportune platform for illicit actors. The initial forays of criminal, corrupt, and terror networks into the cryptocurrency markets foreshadow the future challenges of starving large-scale, bad actors of funding.

### Expanding the Competitive Space

Cryptocurrency transactions expand the international financial competitive space by creating an alternative to a fiat-based monetary system that skirts international financial mechanisms set to detect and intercept suspicious activities. Digital currencies also thwart U.S. Government sanctions policies, which rely on their effectiveness for tracking sales and trade conducted in USD. Outside of digital banking tools designed to disrupt rogue parties from receiving money, cryptocurrencies also negate military capabilities that are able to destroy physical cash stockpiles or target enemy financiers. The two effects of cryptocurrencies create a synergis-

tic effect that allows rogue actors to cooperate in a secondary value transfer market impervious to the established world economic order. In doing so, cryptocurrencies present a viable means to unseat the USD as the recognized global reserve currency.

*Upsetting the World Financial System and Unseating the USD as World Currency.* While the USD has remained the dominant reserve currency following Bretton Woods, two nations have challenged the USD's dominance. In 2009, China and Russia called for the International Monetary Fund (IMF) to develop a new global currency, arguing that inflation and deficit spending in the United States would devalue reserves held in USD.<sup>6</sup> Today, the USD is still the most widely held reserve currency, and nearly two-thirds of all international trade is done in USD. Conducting trade in USD requires the use of the U.S. banking system to support the transactions, and all those transactions are subject to U.S. laws intended to protect international financial markets from bad actors. National security legislation that impacts the financial system includes anti-money laundering, countering the financing of terror, sanctions, the Foreign Corrupt Practices Act, and the USAPATRIOT Act.

The United States gains economic and diplomatic advantages through the strength of the U.S. financial markets in conjunction with the heavy use of the USD in world market trade. As a result, the United States can sustain large budget deficits, enforce sanctions, and dictate terms in international trade. From a strategic standpoint, competitors benefit by reducing U.S. dominance in world currency markets and international trade. Andrei Kostin, the head of Russia's second largest bank, VTB, indicated that Russia intends to find alternatives to the USD, suggesting, "This whip that the Americans use in the form of the dollar would then, to a great extent, not have such a serious impact on the global financial system."<sup>7</sup> Many rogue nations that desire to move money for malign intent echo Kostin.

Cryptocurrencies offer such an option for rogue actors: a new option for those

desiring alternatives to the USD and the affiliated banking and trade regulations. Referred to as a “money-laundering revolution” by a hacker and suspected terrorist’s defense lawyer in New York City, nonstate actors reveal the benefits of functioning within the weakly regulated space of digital currency markets not tied to the USD.<sup>8</sup> Cryptocurrencies fueled illegal trade by criminal organizations on the “Silk Road,” the online equivalent of a black market Amazon.<sup>9</sup> While not widely adopted, jihadist networks have raised funds through cryptocurrencies on Internet-based, crowdsourcing platforms. These platforms empower them to evade the international banking system stopgaps, which were instituted to hinder money laundering and prevent terror funding.<sup>10</sup>

With the technology and expertise at hand, a future digital economy is becoming a potential threat to the USD. The use of cryptocurrencies to evade traditional bad-actor countermeasures in the world financial system, and avoid the regulatory requirements of using the USD entirely, exposes burgeoning weakness in U.S. dominance of funding. The simultaneous migration from the USD, and the loss of the ability to control sanctions, would dilute a primary economic tool that the United States uses to curb confrontational behaviors, promote regime change, and limit access to products affiliated with national security.

**Avoiding Sanctions.** Rogue regimes and revisionist powers are also aggressively seeking digital currency to erode the power of U.S. sanctions. Russia, Venezuela, Iran, and North Korea are actively exploring ways to implement national cryptocurrencies to circumvent the dollar and evade global oversight of financial transactions. The common theory is that the anonymity of cryptocurrencies will undermine U.S. hegemony by degrading its ability to control the flow of financial transactions in and out of sanctioned countries.<sup>11</sup> Direct cryptocurrency payments allow sanctioned countries to bypass financial controls established to enforce sanctions.

Russia, due to economic pressures applied to punish it for its actions in

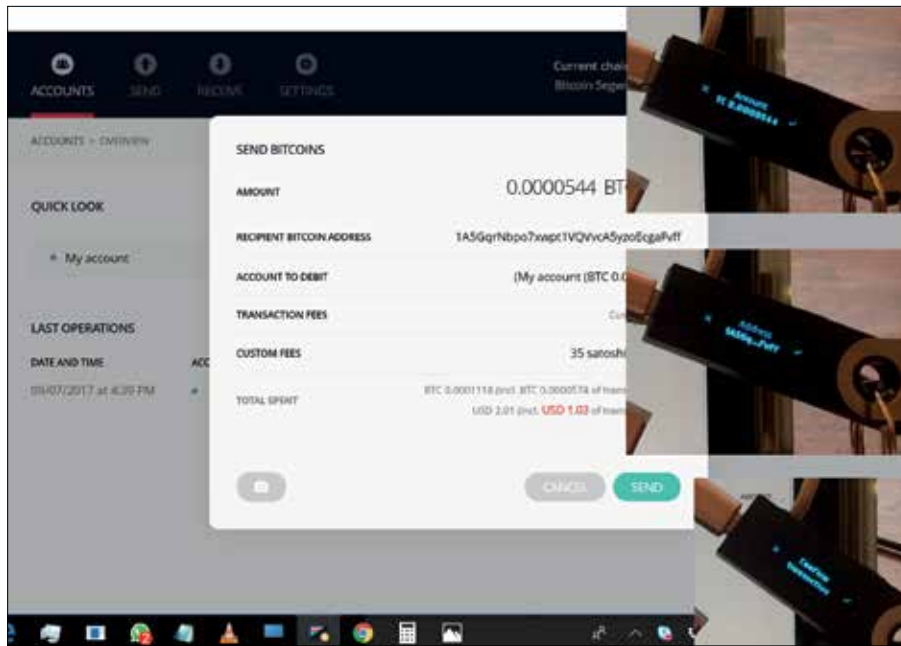
Crimea and chemical agent use, continues to adjust and develop means to evade sanctions. At the 2017 St. Petersburg International Economic Forum, President Vladimir Putin “announced that Russia was considering launching its own ‘digital ruble’ and praised the possibilities of virtual currencies.”<sup>12</sup> Russian officials further suggested extending a supranational cryptocurrency for the BRIC nations (that is, Brazil, Russia, India, and China) as an alternative to the current U.S.-dominated economic system.<sup>13</sup> A BRIC digital trading block would offer not only an alternative currency but also the anonymity of financial transactions among the member nations—a model that rogue nations might establish to circumvent Western sanctions. Although Russia has yet to develop its own digital ruble, Moscow is reportedly behind Venezuela’s new cryptocurrency with the purpose of helping an ally while using the experience as an experiment for future cryptocurrencies.<sup>14</sup>

Venezuela’s new national cryptocurrency, the *petro* (*petromoneda*), is pegged to the value of oil. On the first day of its presale it raised over \$735 million, with hopes of achieving \$6 billion.<sup>15</sup> As noted by the Brookings Institution, “Foreign investors exclusively funded the presale; this rapid influx of capital could not have occurred by conventional means as Venezuela is subject to international sanctions.”<sup>16</sup> Through the use of cryptocurrency, Venezuela effectively circumvented sanctions and accumulated foreign currency without meeting Western demands or addressing the underlying weakness of its national economy to attract traditional foreign direct investment. Furthermore, Venezuela may have brought short-term economic liquidity to a country suffering from hyperinflation and a contracting economy producing 40 percent less than it did 5 years ago.<sup>17</sup> If the *petro* succeeds, its digital model may serve as the example for other nations to follow.

Much like Venezuela, crypto technology may provide Iran a lifeline to counter existing sanctions in the short term. After the United States pulled out of the Joint Comprehensive Plan of Action, better

known as the Iranian nuclear deal, and threatened additional sanctions, the value of the Iranian *rial* plunged to record lows against the USD, crippling Iran’s economy.<sup>18</sup> Mohammad Reza Pourebrahimi, head of the economic committee in Iran’s parliament, stated that he has already “obliged the Central Bank of Iran to start developing proposals for the use of cryptocurrency.”<sup>19</sup> He added that Iran has been in talks with Russia to establish a cryptocurrency system to exchange goods between the two countries.<sup>20</sup> Short of a national cryptocurrency, major Iranian hotels recently announced they would begin to accept cryptocurrencies such as Bitcoin, Ethereum, and Bitcoin Cash, to encourage tourism and avoid U.S. sanctions.<sup>21</sup> The general discussion on the effects on the Iranian economy should not distract from the U.S. resolution to aggressively seek sanctions enforcement. As outlined by General Joseph Votel, the commander of U.S. Central Command, in a threat statement delivered to the House Armed Services Committee in February of this year, “Iran remains the major threat to U.S. interests and partnerships in the Central Region through support for numerous proxies, including Lebanese Hizballah operating in multiple countries, hardline Iranian-backed Shia Militia Groups in Iraq and Syria, and Iranian support-enabled Houthis in Yemen.”<sup>22</sup>

North Korea began using cryptocurrencies to skirt U.S. sanctions in May 2017.<sup>23</sup> While not pursuing its own cryptocurrency, North Korea benefits by earning or stealing cryptocurrencies, which it then uses to purchase items required to support the regime. According to Recorded Future, a digital intelligence firm, North Korea has earned \$15 to \$200 million in USD-equivalent value (value range dependent on fluctuating prices) through legal cryptocurrency mining operations.<sup>24</sup> Steven Kim, a visiting research fellow at the Jeju Peace Institute in South Korea, acknowledged that “cryptocurrency is the ideal form of money for North Korea because it can be moved quickly and anonymously across borders and can be used to buy goods and services online or converted to hard currency.”<sup>25</sup>



Bitcoin transaction with screenshots verifying amount and destination address, and physically confirming transaction, December 16, 2017 (FlippyFlink)

North Korea’s illegal hacking activities are also of concern. 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.<sup>26</sup> Given the extensive “maximum pressure” campaign undertaken by the Trump administration to limit North Korea’s continued pursuit of weapons of mass destruction, its legal and illegal use of the unregulated cryptocurrency markets undermines these international efforts. Suggested by a former U.S. National Security Agency agent, “these coins are being turned into something—currency or physical goods—supporting North Korea’s nuclear and ballistic missile program.”<sup>27</sup> Like Venezuela and Iran, North Korea has demonstrated another method by which cryptocurrencies can undermine sanctions.

Although not under economic sanctions, Chinese participation in the realm of cryptocurrency should signal another competitive space that China views strategically. Maintaining control over its own currency, eroding the prevalence of the USD, and diminishing the strength of Western financial institutions all support the Chinese Grand Strategy released by the 19<sup>th</sup> Party Congress.<sup>28</sup> In recent years,

China’s leadership has routinely stated its desire to unseat the USD as the world’s global currency.<sup>29</sup> Michael Collins, the deputy assistant director of the Central Intelligence Agency’s East Asia Mission Center, warned that “Beijing does not want to go to war with the United States but is attempting to undermine Washington’s global position by using all avenues available.”<sup>30</sup> One of China’s primary avenues is the domination of global trade through its “One Belt, One Road” economic initiative, which includes the cyber realm.<sup>31</sup> Thus far, China has indicated that it may develop its own state-backed form of digital currency but has been less supportive of decentralized initiatives, such as Bitcoin.<sup>32</sup>

China’s intent to create a new world order by becoming a socialist superpower by 2050 includes an interest in cryptocurrencies. Previously observed is China’s reluctance to pursue IMF approval of the *renminbi* as a world reserve currency; Chinese banks fear that decentralized digital exchanges would directly conflict with China’s financial stability and control.<sup>33</sup> Regardless, China understands the power of the blockchain and, as of January 2018, has invested over 100 million dollars in research toward its application.<sup>34</sup> A globally accepted China-backed

cryptocurrency could potentially weaken U.S. dominance in the global market, and significantly buttress Chinese Grand Strategy.

**Combining Generates National Security Threats.** A breakdown in international financial market transactions in USD and in the applications of international sanctions combine to generate a noteworthy national security threat. At the moment, malign actors hiding illegal transactions in cryptocurrency markets, or renegade companies skirting sanctions to generate short-term profit, represent a general nuisance to the overall maintenance of the international financial system. However, if rogue state actors cooperate to establish their own secondary market system of cryptocurrency transactions to trade among themselves, the effectiveness of using the global financial system to thwart these regimes would be significantly challenged.<sup>35</sup>

Unless rogue states coordinate to support all import and export transactions inside a single cryptocurrency, they would still need to convert open market cryptocurrencies to fiat currency. Currently, the cryptocurrency space displays wild fluctuations in value and demonstrates the instability of speculative investments and early market normalization. Since the value of each competing cryptocurrency remains purely based on investor confidence, currency prices tend to increase and decrease rapidly. Rogue nations releasing national digital currency tied to underlying assets presents a contemporary equivalent to the gold standard. If developed, trust among rogue actors in other digital marketplaces could allow for the free flow of illicit trade and funding among participant nations. Disconcertingly similar to the Cold War model, one could imagine this type of alternative market system leading to independent states choosing to operate in one or multiple marketplaces. This type of parallel digital market system challenges both nonkinetic (financial markets) and kinetic (DOD) means by which the United States might disrupt illicit actor funding.

As of July 28, 2018, open market cryptocurrencies represent under 1

percent of currency assets internationally, hence they do not represent an immediate financial market threat. However, this growing revolution in the establishment of cryptocurrencies harkens back to concepts introduced by Frederick Hayek in his 1976 essay, “Denationalisation of Money.” Hayek proposed the need to remove the central bank monopoly over issuance of currency, which is the organizing principle of current cryptocurrencies. While the USD emerged as the stable world currency of choice, the functioning of U.S. Federal Reserve monetary policy as the de facto World Bank leaves many countries dissatisfied.

If rogue states coordinated their efforts to counter this actuality with support of a supranational cryptocurrency standard for trade and exchange, this technology could present a significant challenge to one of the primary tools used by the U.S. Government and the international community to counter continuously evolving gray area threats and activities of rogue nations and violent extremist organizations. The current instability in cryptocurrency marketplaces presents a window of opportunity for the United States to prepare for the revolution in international financial payment systems.

## The Way Ahead

Advances in digital technologies and global connectivity benefit more than just bad actors in the financial landscape. Indeed, the United States participates (and thrives) in the cryptocurrency market. Well-established financial networks remain underpinned by a strong USD, which means decline of the USD is not a fait accompli. Despite increasing risk, there exist opportunities to maintain the USD’s comparative advantage if actions are taken in the near term. Possible actions include advancing the U.S. capacity to countermand malign activity in the cyberspace domain of cryptocurrencies. To do so, the United States must reimagine its role in this new competitive financial space. Acknowledging U.S. vulnerabilities exposed by decentralized blockchain technology, the possibility of rogue national cryptocurrencies, and weakness

in current digital currency regulations inform the way ahead.

**Blockchain.** As described in the new Joint Publication 3-12, *Cyberspace Operations*, the attributes of the cryptocurrency blockchain afford a position of marked advantage, representing key terrain in cyberspace.<sup>36</sup> Application of defensive practices involves understanding the ledger systems in cryptocurrency blockchains to detect pathways of bad actors and the establishment of a system to alert other legal actors, replicating the function of the current international banking system. Using offensive measures requires seizing or destroying the cryptocurrency of these actors in cyberspace, such as asset seizure or DOD kinetic strikes. Ultimately, DOD in particular must learn from the ways in which non-state actors use cryptocurrencies in order to properly prepare to counter their inevitable use by other U.S. competitors.

**National Cryptocurrency.** Rogue nations establishing an adaptive parallel digital currency world marketplace directly challenge U.S. national security. The U.S. Government should consider the benefits of first-mover advantage to mitigate this potential. Establishing a stable USD form of cryptocurrency, backed by the fiat USD, would serve to retain U.S. command of world financial markets by allowing the near seamless conversion of this cryptocurrency back to fiat USD. Seizing this initiative would maximize the benefits of distributed ledger technologies and negate benefits of bad actors establishing parallel systems. Doing so would allow the United States to not only mitigate national security risks but also lead the world in countering corruption through financial transparency. Providing a reliable digital currency in the highly volatile cryptocurrency space allows the United States to preserve its positional and systematic financial advantage.

**Regulation.** Regardless of how much cryptocurrency matures and proliferates in the future, it already represents a significantly disruptive technology. The United States must position itself to continue to influence controls in the world financial markets. Leading the way in releasing a USD cryptocurrency affords

the United States the ability to define the rules, regulations, and international oversight required to ensure the integrity of transitioning from a fiat to a cryptocurrency landscape. A crypto-USD, backed by the U.S. central bank, would enable the United States to offer higher levels of security regarding the cryptocurrency, complementing the benefits of openness generated with blockchain technology. The United States must reinvent guidelines in this cyberspace domain that aid the retention of a comparative advantage in the economic and financial elements of national power.

As the Department of Defense boldly marches toward innovative solutions to combat revisionist states and rogue regimes, the area of cryptocurrencies demands attention. With national security implications, the way ahead offers the potential integration of DOD cyberspace operations into the whole-of-government response. Significant defensive and offensive cyberspace capabilities exist should the U.S. Government remain ahead of the momentum building within this new financial space. The retention of the U.S. comparative economic and financial advantage should remain paramount to dominate the cryptocurrency space. JFQ

---

## Notes

<sup>1</sup> Richard Best, “How the U.S. Dollar Became the World’s Reserve Currency,” *Investopedia.com*, September 23, 2016, available at <[www.investopedia.com/articles/forex-currencies/092316/how-us-dollar-became-worlds-reserve-currency.asp](http://www.investopedia.com/articles/forex-currencies/092316/how-us-dollar-became-worlds-reserve-currency.asp)>.

<sup>2</sup> “Frequently Asked Questions: Find Answers to Recurring Questions and Myths about Bitcoin,” *Bitcoin.org*, available at <<https://bitcoin.org/en/faq#who-created-bitcoin>>.

<sup>3</sup> Don Tapscott and Alex Tapscott, *Realizing the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies* (Geneva: World Economic Forum, June 2017), 3, available at <[www3.weforum.org/docs/WEF\\_Realizing\\_Potential\\_Blockchain.pdf](http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf)>.

<sup>4</sup> Kevin Coleman and Independent Software, “Cryptocurrencies—A Growing Issue for Military, Intel Agencies and Law Enforcement,” *FifthDomain.com*, June 19, 2017, available at <[www.fifthdomain.com/2017/06/19/cryptocurrencies-a-growing-issue-for-military-](http://www.fifthdomain.com/2017/06/19/cryptocurrencies-a-growing-issue-for-military-)

intel-agencies-and-law-enforcement/>.

<sup>5</sup> Financial Action Task Force (FATF), *Emerging Terrorist Financing Risks* (Paris: FATF, October 2015), available at <www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf>.

<sup>6</sup> Andrew Baston, “China Takes Aim at Dollar,” *Wall Street Journal*, March 24, 2009, available at <www.wsj.com/articles/SB123780272456212885>.

<sup>7</sup> Simon Shuster, “Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions,” *Time*, March 20, 2018, available at <http://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/>.

<sup>8</sup> Brett Forrest and Justin Scheck, “Jihadists See a Funding Boon in Bitcoin,” *Wall Street Journal*, February 20, 2018, available at <www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin-1519131601>.

<sup>9</sup> Kim Zetter, “How the Feds Took Down the Silk Road Drug Wonderland,” *Wired*, November 11, 2013, available at <www.wired.com/2013/11/silk-road/>.

<sup>10</sup> Forrest and Scheck, “Jihadist See a Funding Boon in Bitcoin.”

<sup>11</sup> Shuster, “Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions.”

<sup>12</sup> Owen Mathews, “Bitcoin and Blockchain: A Russian Money Laundering Bonanza?” *Newsweek*, September 18, 2017, available at <www.newsweek.com/russia-finally-embracing-virtual-currencies-666794>.

<sup>13</sup> *Ibid.*

<sup>14</sup> Shuster, “Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions.”

<sup>15</sup> Jack Karsten and Darrell M. West, “Venezuela’s ‘Petro’ Undermines Other Cryptocurrencies—and International Sanctions,” Brookings blog, March 9, 2018, available at <www.brookings.edu/blog/techtank/2018/03/09/venezuelas-petro-undermines-other-cryptocurrencies-and-international-sanctions/>.

<sup>16</sup> *Ibid.*

<sup>17</sup> “Venezuela’s Crypto-Currency: Salvation or Scam?” *The Economist*, March 17, 2018, available at <www.economist.com/the-americas/2018/03/17/venezuelas-crypto-currency-salvation-or-scam>.

<sup>18</sup> “Iran Rial Plunges to New Lows as U.S. Sanctions Loom,” Reuters, June 24, 2018, available at <www.reuters.com/article/us-iran-economy-rial/iran-rial-plunges-to-new-lows-as-us-sanctions-loom-idUSKBN1JK0HZ>.

<sup>19</sup> Samburaj Das, “Iran and Russia Consider Using Cryptocurrency to Evade U.S. Sanctions: Report,” CNN, May 21, 2018, available at <www.cnn.com/iran-and-russia-consider-using-cryptocurrency-to-evade-us-sanctions-report/>.

<sup>20</sup> *Ibid.*

<sup>21</sup> Joseph Young, “Major Hotels in Iran Accepting Deposits in Cryptocurrency to Avoid U.S. Sanctions,” *Cryptoslate.com*, July 23,

2018, available at <https://cryptoslate.com/major-hotels-in-iran-accepting-deposits-in-cryptocurrency-to-avoid-u-s-sanctions/>.

<sup>22</sup> “Votel: Iran Is Major Threat to U.S. Interests in the Region,” includes video, 2.11.06 (Washington, DC: United States Institute of Peace, March 5, 2018, updated March 14, 2018), available at <http://iranprimer.usip.org/blog/2018/mar/05/votel-iran-major-threat-us-interests-region>.

<sup>23</sup> Ralph Jennings, “North Korea Is Looking at Bitcoin to Escape Its Crippling Economic Sanctions,” *Forbes*, December 19, 2017, available at <www.forbes.com/sites/ralphjennings/2017/12/19/north-korea-seeks-a-pile-of-bitcoin-to-escape-economic-sanctions/#77cf3c4e39ba>.

<sup>24</sup> Alex Ward, “How North Korea Uses Bitcoin to Get Around U.S. sanctions,” *Vox.com*, February 28, 2018, available at <www.vox.com/world/2018/2/28/17055762/north-korea-sanctions-bitcoin-nuclear-weapons>.

<sup>25</sup> Jennings, “North Korea Is Looking at Bitcoin to Escape Its Crippling Economic Sanctions.”

<sup>26</sup> Timothy W. Martin, Eun-Young Jeong, and Steven Russolillo, “North Korea Is Suspected in Bitcoin Heist,” *Wall Street Journal*, December 20, 2017, available at <www.wsj.com/articles/north-korea-is-suspected-in-bitcoin-heist-1522303177>.

<sup>27</sup> Nicola Smith, “North Korea May Have Made as Much as \$200 Million from Bitcoin, According to Expert,” *The Telegraph* (London), March 5, 2018, available at <www.telegraph.co.uk/news/2018/03/05/north-korea-may-have-made-much-200-million-bitcoin-according/>.

<sup>28</sup> Dingding Chen, “China Has a New Grand Strategy and the West Should Be Ready,” *The Diplomat* (Tokyo), October 31, 2017, available at <https://thediplomat.com/2017/10/china-has-a-new-grand-strategy-and-the-west-should-be-ready/>.

<sup>29</sup> Joe McDonald, “China Calls for New Global Currency,” ABC News, March 24, 2009, available at <https://abcnews.go.com/International/story?id=7156932&page=1>.

<sup>30</sup> Saphora Smith, “China Is Waging a ‘Cold War’ Against the U.S., Says CIA Asia Expert,” NBC News, July 21, 2018, available at <www.nbcnews.com/news/world/china-waging-cold-war-against-u-s-says-cia-asia-n893411>.

<sup>31</sup> “Planet China,” *The Economist*, July 28, 2018, 7.

<sup>32</sup> Sara Hsu, “After Cracking Down on Bitcoin, China Contemplates Its Own Digital Currency,” *Forbes*, October 19, 2017, available at <www.forbes.com/sites/sarahsu/2017/10/19/will-china-host-the-worlds-biggest-state-backed-digital-currency/#696ca5221231>.

<sup>33</sup> Sidney Leng and Xie Yu, “China Is Open to Idea of a Digital Currency, as Long as It’s ‘Efficient and Safe,’” *South China Morning Post* (Hong Kong), March 9, 2018, available

at <www.scmp.com/news/china/economy/article/2136551/china-open-idea-digital-currency-long-its-efficient-and-safe>.

<sup>34</sup> Kevin C. Desouza, Chen Ye, and Xiaofeng Wang, “Is China Leading the Blockchain Innovation Race?” Brookings blog, July 19, 2018, available at <www.brookings.edu/blog/techtank/2018/07/19/is-china-leading-the-blockchain-innovation-race/>.

<sup>35</sup> Foundation for the Defense of Democracies, “Cryptocurrencies and Sanctions,” Breakfast Conversation Panel, Center on Sanctions and Illicit Finance, Washington, DC, April 24, 2018.

<sup>36</sup> Joint Publication 3-12, *Cyberspace Operations* (Washington DC: The Joint Staff, June 8, 2018), I-6.