Information & Security

Sean Costigan & Greg Gleason
vol. 43, no. 1 (2019): 13-20
https://doi.org/10.11610/isij.4301

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

What If Blockchain Cannot Be Blocked? Cryptocurrency and International Security

Sean Costigan (✉), *Greg Gleason*

George C. Marshall European Center for Security Studies,
https://www.marshallcenter.org/

ABSTRACT:

Pariah states and criminal gangs are often early adopters of disruptive technologies. With blockchain, the possibilities for circumventing controls and systems—or creating new ways of business—are rich grounds for such early adopters. What has gone widely ignored in the buzz around cryptocurrencies is the role that states play and their changing perspectives on the matter. This article analyzes the geo-strategic implications of a suite of technologies that has the possibility of altering core economic tenets about money and, along the way, attracting the attention of those who would skirt the law.

ARTICLE INFO:

RECEIVED: 21 MAY 2019
REVISED: 5 SEP 2019
ONLINE: 14 SEP 2019

KEYWORDS:

cybersecurity, cryptocurrency, blockchain, international security, counterterrorism

A key challenge of law enforcement has always been to make sure that crime never pays, at least well. When law enforcement could not succeed at monitoring and preventing crime and even if there were no smoking gun tipping off who committed a particular crime, the high card was always their ability to track down criminals. Usually the best way to do that was to heed the admonition of skilled investigators everywhere – follow the money. Fast forward to today as new forms of digital money – known as cryptocurrency – are now making the money harder and potentially in near future impossible to follow. The counter-crime implications of

✉ Corresponding Author: sean.costigan@marshallcenter.org

these developments are already apparent and significant national security implications are becoming apparent. What is just starting to come into focus are the vast implications for international security.

Unlike bank issued currencies, cryptocurrencies such as Bitcoin are not the product of a single fiscal authority. Cryptocurrencies also share the unique characteristic that they can be transferred between parties without oversight or even a third party having any evidence that a transfer occurred. When combined with cryptocurrencies, new ways of disguising e-commerce transactions through encrypted and anonymizing applications, make it possible for parties who cannot even identify one another to conduct business beyond the ken of law enforcement and regulatory authorities.

Change itself is not new. The great Austro-American economist Joseph Schumpeter nearly a century ago spoke of the evolutionary development of economies as being driven by the capacity to achieve new efficiencies through change, which may at times include almost convulsive change.[1] Schumpeter argued that one of the great advantages of capitalism was the dynamism it gained from the "creative destruction"[2] of new, efficient practices by replacing less efficient practices. More recently, Clayton Christensen and others have shown how breakthrough technological innovations can supplant less adept and less agile technological processes by unleashing "disruptive innovation."[3] Disruptive technology can swiftly upend even seemingly stable commercial relationships by rapidly shifting market shares.

But change in the way money functions is new and the risks associated with this change are an order of magnitude more important than products, companies, monopolies or even whole sectors being replaced by competitors. In less than a decade since Bitcoin was created, the emergence of cryptocurrencies has already challenged traditional ways of tracking criminals. It is just over five years since the first large criminal marketplace, the Silk Road, sprang into action in late 2011 until it was shuttered in November 2013.[4] Silk Road was the first large illegal internet market place conducting transactions out of open view and concealed through the use of a cryptocurrency, but it was most certainly not the last.

In July 2017, U.S. Attorney General Jeff Sessions announced that the U.S. FBI in league with other law enforcement agencies in seized and closed down AlphaBay,[5] a successor criminal enterprise to the Silk Road. AlphaBay was similar to the Silk Road with one important difference—the volume of activity was ten times the size of Silk Road's operations. It is true that law enforcement has quickly gotten much better at the sleuthing work of identifying cyber criminals, but it is also true that criminals are often the first to adopt technologies, innovate and share expertise and so are increasingly more adept at what they do. Risks of cryptocurrencies to law enforcement are now apparent. What is less apparent is that just around the corner is a new phase of cyber security that will be even more disruptive on an international basis. This new aspect of crypto innovation is going beyond national security to the area of international security.

Bitcoin is only one of a growing number of cryptocurrencies,[6] all of which work essentially along the same essential lines but through different platforms and processes. The underlying logic of Bitcoin is based on blockchain, a distributed public

ledger technology that puts the movement of value—"money" if you will—to work in a way that simulates a conventional currency. Every 10 minutes or so the current, encrypted ledger is distributed to all the holders in such a way as to prohibit double spending and maintain provenance without permitting ready identification. If cryptocurrency is not money, it does not matter because it can be exchanged for money, fungibles and objects.

Money has always been an abstract commodity, but digital money is dramatically different. When Claude Shannon in the late 1930s as a young researcher on signal theory at MIT realized that physical signals such as telegraph transmissions could be represented as numerical code he initiated the digital revolution.[7] Advances in cryptography and computing in World War II opened the information age. The subsequent creation of semiconductors and integrated circuits made possible vast increases in computational power. From there, linking individual computers into networks made facilitated the creation of the Internet and web. The invention of asymmetric public key encryption made it possible to conduct ecommerce online with the assurance that transactions could take place with a high degree of confidentiality.[8]

Because of their extreme volatility, cryptocurrencies carry a high investment risk that is compounded by the absence of transparency.[9] The private sector financial industry has not embraced cryptocurrencies as such [10] but have tinkered and adopted some Blockchain technology.[11] That said, the private sector is clearly not prepared to ignore cryptocurrencies' future implications. For instance, the fast growing "fintech" sector is represented in every major commercial and investment bank and has been working to monetize and absorb the opportunities presented by the blockchain and crypto. In contrast, the public sector financial management and oversight community has been slow to respond to the implications raised by the emergence of cryptocurrencies. Many central banks, including the U.S. Federal Reserve [12] as well as other international financial organizations,[13] are more wary of cryptocurrencies but nevertheless see the blockchain technology as playing a role in the future. There is a consensus throughout the entire financial community that distributed ledger technology, DLT, is as an inevitable stage in the future evolution of money. Aided by Russia, Venezuela has launched their own cryptocurrency, the petromoneda to help supplement their meager cash reserves. Russia's Federal Security Service (FSB) recently also acknowledged that it is directly involved in the International Standards Organization (ISO) efforts to create a global standards for new "blockchain" technology for Bitcoin and other cryptographic currencies winning international attention.[14]

National central banks in most countries play the key role of serving as the gatekeepers in their role as overseers of monetary policy through managing capital flows in the form of setting currency exchange rates for the purposes of export and import management. There is a wide variety in the differences of central banks among countries. Some central banks stipulate and enforce currency exchange rates directly. In other countries central banks function in parallel with secondary currency markets in which supply and demand autonomously play a role in establishing exchange rates. Despite the variety of monetary arrangements, in all cases

national financial authorities need to have visibility with respect to financial transfers in order to properly do their job. The same is true for the public international financial institutions with which they work, such as the International Monetary Fund.[15] Cryptocurrencies may deprive these institutions with a level of visibility that is necessary.

The settlement of accounts among central banks, commercial banks, and retail banks continues to exist in the context of national central bank authorities. Dynamic changes in legal and observable payment processing technologies and mechanisms are increasingly relying on private firms such as Apple, Google, PayPal, Square, Stripe, Vantiv, and WorldPay and others in adopting recently developed peer-to-peer services such as Venmo, all of which continue to be observable exchanges. Cryptological transfers such as those through blockchain can be conducted within the legitimate and observable processes but, technologically, can also be conducted outside this circle in a way in which they are not necessarily visible. The present scale of these illegal transfers currently appears to be small. That is a conjectural rather than empirical conclusion because, obviously, if they are not visible they cannot be counted. However, there are no technical constraints which ensure that the scale of unmanaged financial transfers will remain small. If blockchain transfers are not visible, it follows that some at least will not be blocked. The question is how big the scale? Already, we see that pariah states have amassed considerable sums of Bitcoin, among other currencies. For instance, according to a panel of experts reporting to the UN Security Council, North Korea has collected upwards of $670 million worth of bitcoin, much of which through financial crime.[16]

World practice in controlling capital mobility is varied but is increasingly diverging between the more democratic, market-driven processes of the western world in which the use of cryptocurrencies are only officially endorsed with reservations as opposed to some of the more authoritarian and state-driven processes of the eastern world in which electronic transfers not under the control of the state are widely viewed as categorically unacceptable. The creation of a “Great Firewall” to use state control over the telecommunication infrastructure to establish filters and blocks to eliminate ostensible risks to national security is an example of how a state can employ its administrative capacity to control the cyber revolution.[17] Rumors recently circulated in the press and were then explicitly denied by Chinese authorities that there was a plan to eliminate the use of VPNs, virtual personal network services, located outside of the physical territory of China.[18] However, measures have been taken in China to block such applications as WhatsApp and chat services.[19]

These steps fall short of addressing the emerging and growing role of peer-to-peer (P2P) communications through wireless electromagnetic space that does not rely upon servers, optical fiber or copper wires, or relay transmissions systems. Such P2P transmissions, including the transmission of monetary value through cryptocurrencies is outside of the view and thus the control of government authorities.

In Russia officials have referred to cryptocurrencies in the past in very hostile terms. Now, however, there are indications that a shift in perspective is now taking place as illustrated by Vladimir Putin's meeting with the creator of Bitcoin's closest competitor, Ethereum.[20] The recent interest of Russian officials in cryptocurrency as means of exchange may be less important than the interest in understanding the potential of cryptocurrencies as instruments of disruptive intervention in international markets, given the Russian government's goal of pairing up with China in an effort to displace the U.S. dollar as the de facto global reference currency.[21] While there have been multiple delays,[22] President Putin has ordered the adoption of cryptocurrencies by July 2019. Here too, if we follow the money, we find that 20 % of the top 50 blockchain startups by funds raised were Russian.[23]

So far, the wide-scale use by criminals of cryptocurrencies has been nominal. This may be primarily because the financial technology is so technically advanced and complicated that it requires substantial technical expertise to master. Empirical instances of the use of cryptocurrencies by terrorists, global criminal groups, illegal economic cartels, traffickers in weapons of mass destruction, and other global syndicates either acting on their own in conjunction with rogue or otherwise disruptive states, is not something that has captured international attention. Such a focus is direly needed if we are going to be smart in addressing these threats.

The risks of emerging cryptocurrencies to international security can only be properly addressed in the context of international diplomacy and cooperation. But in all diplomatic agreements, big and small, in the end there is no right without a remedy. If there is no fall back to hard consequences, any soft power diplomacy is little more than a bromide. All international agreements in a world as dynamic as that of the present must be, to some extent, self-enforcing and based on the self-interests of all participants prepared to defend them. Any confidence that a new global treaty on cyber security will in itself be sufficient to address the risks of the disruptive potential of cryptocurrencies to our national and well as international security interests is surely naive. More research needs to be done on what steps individually and independently we can take to protect national and international security interests. It is time to get smart about these disruptive technologies before the costs become more than we can afford.

References

1 Harvard Library, http://oasis.lib.harvard.edu/oasis/deliver/~hua11007.

2 Joseph Alois Schumpeter, *Can Capitalism Survive?* (New York, Harper & Row,1978), https://archive.org/details/cancapitalismsur00schu.

3 Clayton M. Christensen, Michael E. Raynor, and Rory McDonald, "What Is Disruptive Innovation?" *Harvard Business Review*, December 2015, https://hbr.org/2015/12/what-is-disruptive-innovation.

4 "Ross Ulbricht, A/K/A 'Dread Pirate Roberts,' Sentenced In Manhattan Federal Court to Life in Prison," Department of Justice, U.S. Attorney's Office, May 29, 2015,

https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.

[5] "Attorney General Jeff Sessions Delivers Remarks at Press Conference Announcing AlphaBay," U.S. Department of Justice, Washington, July 20, 2017, https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-delivers-remarks-press-conference-announcing-alphabay.

[6] Jacob Bushmaker, "The Top 50 Cryptocurrencies," *Invest in Blockchain*, November 12, 2018, https://www.investinblockchain.com/top-cryptocurrencies/.

[7] "A Boole/Shannon Celebration," Massachusetts Institute of Technology, 2019, http://booleshannon.mit.edu/.

[8] Peter Bright, "Locking the bad guys out with asymmetric encryption," *Ars Technica*, December 2, 2013, https://arstechnica.com/information-technology/2013/02/lock-robster-keeping-the-bad-guys-out-with-asymmetric-encryption/.

[9] Brian Barrett, "Security News This Week: Two Huge Cryptocurrency Heists Cost Investors Millions," *Wired*, July 22, 2017, https://www.wired.com/story/ether-cryptocurrency-theft/.

[10] Arjun Kharpal, "Intel and major banks, including HSBC and BOAML, pour $107 million into blockchain group," *CNBC*, May 23 2017, http://www.cnbc.com/2017/05/23/r3-funding-blockchain-intel-bank-of-america-hsbc.html.

[11] Olga Kharif , Big Banks Are Stocking Up on Blockchain Patents, *Bloomberg*, December 21, 2016, https://www.bloomberg.com/news/articles/2016-12-21/who-owns-blockchain-goldman-bofa-amass-patents-for-coming-wars.

[12] Jerome H. Powell, "Innovation, Technology, and the Payments System," Speech to the Board of Governors of the Federal Reserve System, March 03, 2017, https://www.federalreserve.gov/newsevents/speech/powell20170303a.htm.

[13] Committee on Payments and Market Infrastructures, "Digital currencies," Bank for International Settlements, November 2015, http://www.bis.org/cpmi/publ/d137.pdf.

[14] Ekaterina Smirnova, Elena Mukhametshina, "FSB participates in the development of the international blockchain standard," *Vedomosti newspaper*, August 18, 2017 (in Russian), https://www.vedomosti.ru/technology/articles/2017/08/18/730045-fsb-blokcheina.

[15] Andreas Adriano and Hunter Monroe, "The Internet of Trust," *Finance & Development* 53, no. 2 (June 2016), http://www.imf.org/external/pubs/ft/fandd/2016/06/adriano.htm.

[16] Anthony Cuthbertson, "North Korea has amassed $670 million in bitcoin and other currencies through hacking," *Independent*, March 12, 2019, https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-bitcoin-cryptocurrency-blockchain-un-report-a8819446.html.

[17] Christopher Balding, "How Badly Is China's Great Firewall Hurting the Country's Economy?" *Foreignpolicy*, July 18, 2017, http://foreignpolicy.com/2017/07/18/how-badly-is-chinas-great-firewall-hurting-the-countrys-economy/.

[18] Xu Jiayuan, "Chinese authorities deny reports of VPN ban," CGTN, July 13, 2017, https://news.cgtn.com/news/3d4d7a4e3063444e/share_p.html.

[19] Paul Mozur, "China Disrupts WhatsApp Service in Online Clampdown," *The New York Times*, July 18, 2017, https://www.nytimes.com/2017/07/18/technology/whatsapp-facebook-china-internet.html.

[20] "Meeting with founder of Ethereum project Vitalik Buterin," *Kremlin.ru*, June 2, 2017, http://en.kremlin.ru/events/president/news/54677.

[21] Nathan Lewis, "China Is Laying The Foundation For The Next World Gold Standard System," Forbes, May 5, 2016, https://www.forbes.com/sites/nathanlewis/2016/05/05/china-is-laying-the-foundation-for-the-next-world-gold-standard-system.

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

[23] Kenneth Rapoza, "Meet The Russians Behind Your Blockchain (And Cryptocurrency, Too)," Forbes, Apr 29, 2018, https://www.forbes.com/sites/kenrapoza/2018/04/29/meet-the-russians-behind-your-blockchain-and-cryptocurrency-too/.

About the Authors

Sean S. **Costigan** is a professor at the George C. Marshall European Center for Security Studies. He is an expert in emerging security challenges and is published widely on matters of national security and foresight. His current research and teaching is on the nexus of cybersecurity, crime and terrorism. He is presently serving as a Senior Adviser to the NATO/GCSP/PfPC Emerging Security Challenges study group, where he leads cybersecurity education efforts; Chair of the Editorial Board, Partnership for Peace Consortium of Defense Academies and Security Studies Institutes; Senior Associate at the Security Governance Group and is an Associate at Vision Foresight Strategy. Prior to joining the Marshall Center faculty, Costigan was an Associate Professor at The New School; Director for Strategic Initiatives, Center for Security Studies ETH Zurich; Visiting Fellow at the University of Calcutta's Institute of Foreign Policy Studies; Executive Editor at Columbia International Affairs Online; Research Associate for Science, Technology and Defense Industrial Policy at the Council on Foreign Relations; and on the staff of the Weatherhead Center for International Affairs, Harvard University.

Gregory **Gleason** is a professor of Eurasian Security Studies at the George C. Marshall European Center for Security Studies. Upon returning in September 2019 from an assignment as U.S. Ministry of Defense Advisor in Uzbekistan, Gleason resumed his post at the George C. Marshall European Center for Security Studies. Since 2007, Gleason's research, teaching and service at the Marshall Center has focused on former communist countries. Before joining the Marshall Center, Gleason taught courses in international relations at the State University of New York and later at the University of Miami before joining the political science faculty of the University of New Mexico. While at the University of New Mexico Gleason taught political science, public administration, and economics, focusing on international relations and comparative foreign policy. Gleason has published numerous articles and books on international relations and political development. He is the author of "Federalism and Nationalism: the Struggle for Republican Rights in the USSR" (1991), "Central Asian States: Discovering Independence" (1997), and "Markets and Politics in Central Asia" (2003), as well as articles in scholarly journals. The National Science Foundation and the National Academy of Sciences as well as other public and private foundations have sponsored Gleason's scholarly research. In addition to academics, Gleason has served in various analytical, advisory and managerial capacities with national and international organizations including Lawrence Livermore National Laboratory, Sandia National Laboratories, the Asian Development Bank, USAID, the U.S. Department of State and other organizations.