The JSOU Quick Look is intended to provide a brief overview of a complex topic.
For more in-depth JSOU Press products, visit
https://jsou.libguides.com/jsoupublications

JSOU Quick Look

Cryptocurrency

WHAT IS BLOCKCHAIN?

It is impossible to understand cryptocurrency without first discussing blockchain technology, the underlying cryptocurrency technology with a wide application outside of cryptocurrency—from securing property deeds to safeguarding voting tallies. When a transaction is made, an algorithm generates an original hash that is added to the blockchain since it corresponds to the previous blockchain entry. The blockchain is usually publicly available to all participants that have loaded the software and therefore it is theoretically inalterable, meaning that the cryptocurrency cannot be double-spent. Without a central arbiter to enforce the rules of the system, the validation process of the blockchain community keeps the system honest.[1] However, due to the time needed to confirm transactions, lag time remains one of cryptocurrencies limiting factors as it takes more time to process than traditional digital transactions.

What Is Cryptocurrency?

Cryptocurrency is a medium of exchange—or to some, an investment—originally conceived of in the cyber, cryptographic, and Libertarian communities. Roughly speaking, cryptocurrencies are created by those that hold a particular cryptocurrency software on their computers. Most cryptocurrencies need mining—using these computers' computational power to solve increasingly complex mathematical equations.

Cryptocurrency wallets, which typically take the form of a smartphone app, hold individual cryptocurrency. If one owns cryptocurrency, they must have an accompanying wallet, which serves as central depository for an individual's cryptocurrency. Once containing cryptocurrency, the wallet is used to buy and sell products or to simply store the cryptocurrency while it gains value. These wallets are accessible after keying in a randomly generated password, created at the time of setting up the wallet, which consists of 11 words or more. Therefore, if a user loses their password, they are unable to access whatever cryptocurrency they held within their wallet.

Once mined, the cryptocurrency generates a particular hash—an encrypted algorithm that details the transaction history of the currency. With the most common and lucrative cryptocurrencies (namely Bitcoin and Ethereum), the transaction histories are posted to a public ledger which is accessible by anyone. Through energy intensive processes, this encryption can be broken, making cryptocurrencies not necessarily anonymous. Outside of mining, cryptocurrency can be acquired through market exchanges.

Given that financial markets are created by humans rather than a natural ordering of markets, policymakers often interfere in financial markets when it suits their political objectives, creating unnatural distortions and inefficiencies. White papers have circulated since the 1990s on how to digitally free economics from politics and develop a currency free from state oversight.[2]

Crypto wallets can be hacked through hardware on smart phones, conducting transactions on public Wi-Fi that is unsecured, and exploiting software bugs in crypto add-ons (i.e. apps tracking the value of cryptocurrencies).[3] This list does not even take into account the possibility that in the future, quantum computing may be able to conduct a huge number of calculations to break blockchain cryptography.[4] The concept of Know Your Customer (KYC) protocols have been put in place to deter money laundering and other malign economic activities.

Many cryptocurrencies have a cap on the amount of coins they create. This controls for inflation and does not allow for human intervention into crypto economies. Most cryptocurrencies are priced through strict supply and demand market signals.

In these cases, there is no human intervention into the system to stabilize the price of a cryptocurrency—hence, the wild volatility that has plagued many cryptocurrencies since their inception.

What Are Some Cryptocurrencies That Are Used By Malign Actors?

Terrorist groups and criminals have increasingly flocked to cryptocurrencies as a way to obfuscate their financial gains. Additionally, they use cryptocurrency to fundraise, sell illegal drug/arms traffic, send remittances/transfer funding, provide attack funding, and deliver operational funding.[5] Malign actors have moved towards using this new technology after previous ways of sending and receiving money were closed by law enforcement. In what follows, two cryptocurrencies (out of the 6,955 in existence[6]) are described. The first—Bitcoin—remains the most popular, while the other—Monero—has been associated with malign actors due to its obfuscated blockchain ledger.

Bitcoin: Bitcoin, which has a cap of 21 million Bitcoins, operates on a decentralized system using a peer-to-peer network. When 51 percent of users confirm a transaction as valid, they compete against each other to solve increasingly complex equations to verify the new block, then it is added to the blockchain. Anyone can see all the Bitcoin transactions—though not necessarily what was purchased—provided they have the software installed.

Monero: This cryptocurrency is lesser known than Bitcoin but more in line with the original cryptocurrency philosophy since it holds the right to economic privacy, even for a malign actor, because individuals cannot see that a transaction was made by a user. Unsurprisingly, Monero is most active in dark market communities, and was used as payment in the WannaCry ransomware attack.[7] Just like with Bitcoin, Monero also relies upon miners to verify transactions as valid before being added to the blockchain. There is not a fixed amount of Monero coins in the system, which makes it predisposed to inflation.[8]

How Is Cryptocurrency Utilized By Competitors?

China: China has recently rolled out its own cryptocurrency, dubbed the Digital Currency Electronic Payment (DCEP), which is essentially a digital version of its own currency—the Yuan. Its advantages include decentralized banking wherein those residing in the countryside—and who are usually not tied into the banking system—can participate in banking. However, unlike traditional cryptocurrency, the DCEP will remain under state control, which means, like traditional currencies, it can be manipulated by the state.[9] The Chinese hope to eventually replace the dollar as the global reserve currency, and to the Chinese Communist Party, this starts through spreading the DCEP into countries involved in the One Belt, One Road initiative. All told, the DCEP may allow those in rural communities to increasingly experience economic gains, which have been distributed unevenly throughout the country and allow the CCP to track financial crimes, yet the digital currency also opens up users to being surveilled by the state and having their transaction data unknowingly used by the state.

Iran: Iran does not currently have its own state-backed cryptocurrency. However, it would be a mistake to think the Iranian state is disinterested in exploiting the use of this non-fiat currency. The Iranians have closely followed cryptocurrency development and in fact, have been exposed as using cryptocurrency to evade sanctions. Moreover, the Iranians have been avid miners of cryptocurrency. Despite utilizing cryptocurrency, the insular Iranian government also remains suspicious of a competing currency that could undermine the state-backed Rial.[10] Recently, the Iranian president has encouraged cryptocurrency mining within the government. Further, the Iranian parliament has called for tightening regulations on cryptocurrency exchanges operating within Iran.

Russia: While the state views blockchain technologies as potentially advantageous, it views cryptocurrency as being associated with crime. As such, the Russian parliament has proposed bringing cryptocurrency under state control and defining it as an asset versus a currency.[11] Moreover, the Ministry of Finance has forbid Russians from earning coins through cryptocurrency mining.[12] Despite these bans, Russia's prospering cybercrime community still prefers to deal in cryptocurrency to remain (partially) anonymous.[13]

North Korea (DPRK): Like the Iranians, the North Koreans do not have their own state-backed cryptocurrency. Rather, the DPRK relies on cryptocurrency as a source of state revenue by way of theft. The DPRK has been responsible for cryptocurrency heists from some of the largest exchanges, including Mt. Gox (formerly the largest exchange in the world) and through ransomware attacks (e.g. WannaCry).

How Might SOF Anomalously Employ Cryptocurrency?

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

- using cryptocurrencies to make "anonymous" purchases
- using cryptocurrencies to make black market purchases
- using captured wallets to engage in masked cryptocurrency activity
- targeting nefarious actors using cryptocurrencies (via hacking, ransomware, etc.)
- using cryptocurrencies to facilitate payments
- use cryptocurrencies to pay ransoms—In this scenario, post a reward for the safe return of a U.S. citizen that anyone could claim using a wallet on their phone.
- using cryptocurrency smart contracts to coordinate payment parameters and the transfer of funds without face-to-face meetings—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.[14]

Additional anomalous uses would be to outfit operators with the necessary equipment and training to exploit enemy use of crypto on devices they acquire as part of the collected exploitable material and exploitation process.[15] ■

Endnotes

1. Paul Vigna and Michael Casey, *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic Order* (New York: Macmillan, 2016).
2. Vigna and Casey, *The Age of Cryptocurrency*.
3. Julia Magas, "Six Tools Used by Hackers to Steal Cryptocurrency: How to Protect Wallets," *Cointelegraph*, 29 July 2018, https://cointelegraph.com/news/six-tools-used-by-hackers-to-steal-cryptocurrency-how-to-protect-wallets.
4. Cointelegraph Japan, "How the Crypto World Is Preparing for Quantum Computing, Explained," *Cointelegraph*, 20 January 2020, https://cointelegraph.com/explained/how-the-crypto-world-is-preparing-for-quantum-computing-explained.
5. Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Monica: RAND Corporation, 2019), https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf.
6. John Wanguba, "How Many Cryptocurrencies Are There In 2020?" *E-Crypto News*, 8 September 2020, https://e-cryptonews.com/how-many-cryptocurrencies-are-there-in-2020/#:~:text=According%20to%20CoinMarketCap%2C%20the%20total,a%20total%20of%204%2C621%20cryptocurrencies.
7. Sean Gallagher, "Researchers Say WannaCry Operator Moved Bitcoins to 'Untraceable' Monero," *ARS Technica*, 24

August 2017, https://arstechnica.com/gadgets/2017/08/researchers-say-wannacry-operator-moved-bitcoins-to-untraceable-monero/.
8. "What is Monero (XMR)?" *Monero*, accessed 16 October 2020, https://www.getmonero.org/get-started/what-is-monero/.
9. Hung Tran and Barbara Matthews, "China's Digital Currency Electronic Payment Project Reveals the Good and the Bad of Central Bank Digital Currencies," *Atlantic Council*, 24 August 2020, https://www.atlanticcouncil.org/blogs/new-atlanticist/chinas-digital-currency-electronic-payment-project-reveals-the-good-and-the-bad-of-central-bank-digital-currencies/.
10. Sandali Handagama, "Iran Is Ripe for Bitcoin Adoption, Even as Government Clamps Down on Mining," *Coindesk*, 24 September 2020, https://www.coindesk.com/iran-is-ripe-for-bitcoin-adoption-even-as-government-clamps-down-on-mining.
11. Vasilisa Strizh, Dmitry Dmitriev, and Anastasia Kiseleva, "Russia," in *Blockchain & Cryptocurrency Regulation 2019* (Global Leader Insights, 2019).
12. Anna Baydakova, "Russia's Latest Draft Bill Would Still Largely Ban Crypto, Stifle Miners," *Coindesk*, 3 September 2020, https://www.coindesk.com/russia-ban-crypto-miners.
13. Brian Krebs, "Two Russians Charged in $17M Cryptocurrency Phishing Spree," *Krebs on Security*, 16 September 2020, https://krebsonsecurity.com/2020/09/two-russians-charged-in-17m-cryptocurrency-phishing-spree/#:~:text=U.S.%20authorities%20today%20announced%20criminal,the%20most%20popular%20cryptocurrency%20exchanges.
14. Megan McBride and Zach Gold, *Cryptocurrency: Implications for Special Operations Forces* (Washington, D.C.: Center for Naval Analysis, 2019).
15. Joseph Trevithick, "'Identity Intel Ops' Turn US Special Operators into Combat Detectives," *The Drive*, 30 June 2017, https://www.thedrive.com/the-war-zone/12023/identity-intel-ops-turn-us-special-operators-into-combat-detectives.

Where Can I Learn More About Cryptocurrency?

- *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*, RAND Corporation, https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf
- *Cryptocurrency: A Primer for Policy-Makers*, Center for Naval Analysis, https://www.cna.org/CNA_files/PDF/CRM-2019-U-020185-Final.pdf
- *Cryptocurrency: Implications for Special Operations*, Center for Naval Analysis, https://www.cna.org/CNA_files/PDF/CRM-2019-U-020186-Final.pdf
- *National Security Implications of Virtual Currency: Examining the Potential for Non-state Actor Deployment*, RAND Corporation, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1231/RAND_RR1231.pdf
- *Central Banking in a Digital Age: Stock-taking and Preliminary Thoughts*, Brookings, https://www.brookings.edu/wp-content/uploads/2018/04/es_20180416_digitalcurrencies.pdf
- *Exploring the Use of Zcash Cryptocurrency for Illicit or Criminal Purposes*, RAND Corporation, https://www.rand.org/content/dam/rand/pubs/research_reports/RR4400/RR4418/RAND_RR4418.pdf

FOR MORE INFORMATION, PLEASE CONTACT:
Dr. Mark Grzegorzewski, JSOU Professor, employed as a contractor with Metis in support of the JSOU mission.
813-826-3647 | mark.grzegorzewski.ctr@socom.mil

JOINT SPECIAL OPERATIONS UNIVERSITY
Institute for SOF Strategic Studies
7701 Tampa Point Blvd., Bldg. 5200, MacDill AFB, FL 33621
socom.mil/jsou