CATEGORY Military Justice and Discipline

Text Excerpt from JAG Reporter Post: 23 Sept 2021 https://www.jagreporter.af.mil

Decrypting Bitcoin and Blockchain

For Military Lawyers

BY LIEUTENANT COLONEL DEAN KORSAK AND MAJOR ERIK FUQUA

This article should serve as a cryptocurrency primer for lawyers practicing in the Federal government. It will provide a basic overview of the history of Bitcoin and blockchain technology then discuss blockchain use cases for military interests and criminal law hurdles created by cryptocurrency.

INTRODUCTION

New technologies create new challenges and opportunities. Bitcoin and its underlying **blockchain technology** increasingly impact all facets of society. Bitcoin's status as digital gold is merely the tip of this technology. Military organizations feel impacts from this technology that span from personnel security risk management to longer term prospects of streamlining nearly every aspect of operations. Blockchain technology alone is fast becoming an integral part of human existence, just like credit cards, the Internet, and cell phones. Bitcoin and blockchain are ushering in new norms affecting nearly every aspect of life. Military lawyers must familiarize themselves with the challenges created by this new technology and be ready to address them in situations ranging from the courtroom to legal assistance to the operational environment. This article provides an overview of these issues to accelerate familiarization.

What Is Cryptocurrency in Simple Words?

Cryptocurrencies are systems that allow for secure payments online which are denominated in terms of virtual "tokens."

~Investopedia

Close-up photo of several gold plated bitcoins
(Photo © iStock.com/skodonnell)

MONEY LEADS THE WAY

A variety of industries are evaluating adoption of blockchain technology, but the leading use-case for blockchain adoption is financial use in the form of **cryptocurrency**.[1] Money exists to facilitate transactions among strangers who specialize in different skills, enabling complex economies.[2] As humanity developed, groups developed mediums of exchange to facilitate commerce.[3] The barter system was one early medium.[4] Money then displaced the barter system and developed further into a ledger-based medium of exchange, eliminating the need to carry items of value and enabling credit-based economies.[5] These developments produced today's complex ledger system. Consistent with centuries-old monetary theory, Bitcoin and other cryptocurrencies seem to be a natural development to account for an increase in exchanges between transacting parties, which "requires larger or more efficient medium of exchange, but not necessarily more money."[6]

> Military lawyers must familiarize themselves with the challenges created by this new technology.

A basic understanding of money and ledgers is necessary to understand the revolutionary impact of Bitcoin and blockchain technology.[7] The U.S. dollar primarily exists in ledger form in computer systems — only approximately eight percent exists as physical coin or cash.[8] The deposit ledger system is nearly exclusively used for all major transactions today. It involves a buyer's bank subtracting an amount from the buyer's account ledger and a seller's bank adding that amount to the seller's ledger. Yet it is not that simple. In reality, the system is highly complex, relies heavily on trust, and it can sometimes take days to complete a transaction. It requires many middlemen, from banks to credit card processors, and other costly components such as vaults and armored trucks, as well as the human capital requirements of large organizations simply to manage the spreadsheets and computer systems.

Cryptocurrency cuts out all the middlemen and removes the need for trust. Put another way, cryptocurrencies like Bitcoin are decentralized. Decentralization allows cryptocurrencies to be exchanged or converted at any time and almost anywhere in the world in, at most, a matter of minutes. However, these features of decentralization also create tension with fiat currencies.

EXPAND YOUR KNOWLEDGE

External Links to Additional Resources

- Afghans turn to crypto market for stability during Taliban takeover (CNBC After Hours)
- What is Money? And Could Bitcoin Be the Best One? (TedX)
- Bitcoin hodlers are about to spark a run (Cointelegraph)
- Today's Cryptocurrency Prices (Coin Market Cap)
- How Does Bitcoin Actually Work? (YouTube)

Fiat currencies

Fiat currencies are backed by an issuing government. Since fiat currency depends on convertibility and trust,[9] national economic progress depends on the extent to which a country's fiat currency is globally accepted. Fiat currencies can become so-called "bad money" when a nation's economic policies, excessive debt, and other negative industrial and societal trends lead to a decline in world economic power.[10] However, by removing a central authority and the need for trust, Bitcoin and related cryptocurrencies create a form of permanent and universal value that is mostly insulated from regional economic and political instability. For example, no government or organization controls Bitcoin. It has a fixed supply cap of 21 million Bitcoin, so Bitcoin's value cannot be diluted in the way that governments dilute fiat currency by creating more money. Despite these stability characteristics, the growing popularity of Bitcoin and other cryptocurrencies results in price volatility while the market determines a defined range of value. Beyond the monetary aspects of Bitcoin, its underlying blockchain technology alone is just as revolutionary. A closer look at this technology reveals many opportunities, solutions, and challenges for the military and other large organizations.

BLOCKCHAIN TECHNOLOGY PRIMER

Blockchain technology enabled the creation of Bitcoin. In the groundbreaking Bitcoin white paper, Satoshi Nakamoto described the "chain of blocks" that serves as a record of all Bitcoin transactions.[11] Blockchain technology addressed the limitations of earlier attempts at digital currency, and many other cryptocurrency projects have adopted it as well.[12] In explanation, its applications transcend cryptocurrency and extend to smart contracts,[13] financial services, health care, voting, and more. But what is it?

> The blockchain is a decentralized digital ledger distributed across multiple computers ("nodes").

The blockchain is a decentralized digital ledger distributed across multiple computers (**"nodes"**). It is also publicly viewable. Any person in the world with Internet access can view the entire history of Bitcoin transactions at any time. This distributed digital ledger aspect removes the requirement of trust from transactions and solves the **Byzantine General's Problem**.[14] The Problem describes the need in computer science for individual parties to agree on a specific strategy to avoid a system failure. It manifests in virtual transactions as double-spending. Double-spending can occur if the entities verifying transactions do not agree, resulting in multiple users spending the same piece of currency. Banks and other financial institutions provide the trust that fiat currency does not fall victim to double-spending. The distributed digital ledger provides this confidence for Bitcoin. As processors (**"miners"**) enter transactions on the ledger, the blockchain grows. In exchange for Bitcoin, miners devote computing power to confirm groups of transactions at regular intervals, which creates timestamped blocks in the process, and those blocks become part of the Bitcoin blockchain.[15] Through facilitating these transactions a new Bitcoin block is created approximately every 10 minutes.

EXPAND YOUR KNOWLEDGE

External Links to Additional Resources

- Blockchain Explained (Investopedia)
- Byzantine Generals Problem - Intro to Blockchain (YouTube)
- How the Blockchain is Chaning Money and Business (TedTalk)
- Inside One of The Nation's Largest Cryptocurrency Mines (NBC)
- Can Central Bankers Kill Bitcoin? (Forbes)

Pseudonymous Not Anonymous

Although the Bitcoin blockchain is always viewable (you can even download it and have your computer serve as a node on the Bitcoin network), transactions maintain some degree of privacy. Bitcoin transactions are **pseudonymous**, but not anonymous. As discussed later, this distinction has important implications for law enforcement and limits the ability for bad actors to use Bitcoin to engage in illegal activity. Bitcoin's pseudonymity is due to its use of public-key cryptography. This system involves two keys, one private and one public. The private key allows a person to access the Bitcoin and transact with it.[16]

> At any time, anyone can access the Bitcoin blockchain and view every Bitcoin transaction associated with any given public key.

The public key corresponds mathematically to the private key and can be converted into an address ("hashed") to which anyone can send Bitcoin. At any time, anyone can access the Bitcoin blockchain and view every Bitcoin transaction associated with any given public key. However, the public key is not linked to the owner's personal information. This structure provides a high degree of privacy. However, if an individual is ever linked to the pseudonymous public key, then the world can know the person's entire transaction history and Bitcoin holdings. Definitive connections can be made between wallet addresses and corporate or human identities. For example,

researchers have long since identified the public keys associated with Satoshi Nakamoto, who never spent the roughly 1 million Bitcoin he mined during the first seven months of Bitcoin when it basically had no value.[17] Lastly, while a private key holder will always have the associated public key, it is mathematically impossible to use the public key to identify the private key.[18] This means that cracking the encryption is not feasible to associate public and private key wallet addresses. Bitcoin's use of public key cryptography forces interested parties to attempt to identify Bitcoin users in other ways, such as companies disclosing Bitcoin transactions or linking transactions to particular individuals through timing, amount, and associates. Although financial transactions presently dominate blockchain adoption, use cases extend far beyond personal financial transactions.

CRIMINAL LAW CHALLENGES AND OPPORTUNITIES

The Department of Justice (DOJ) recently acknowledged that the technology "raises breathtaking possibilities for human flourishing."[19] Yet it further noted that "despite its relatively brief existence, cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces."[20] This is no different than criminal enterprises taking full advantage of the Internet.

The novelty of cryptocurrency and blockchain technology poses the primary hurdle for law enforcement and prosecutors, though law enforcement can also use this same technology for investigative advantage. For example, Silk Road was an "eBay for drugs" located on the Darknet.[21] Business on Silk Road was conducted in Bitcoin in an attempt to maintain anonymity.[22] Ultimately, the FBI was able to shut down Silk Road, and it used blockchain analysis to overcome the pseudonymity.[23] More recently, the FBI was able to seize $2.3 million worth of Bitcoin representing a ransom paid by Colonial Pipeline to the hacking group Darkside after the hackers installed ransomware on Colonial's computer systems.[24] Interestingly, the Silk Road and Colonial Pipeline cases also dispel the myth that cryptocurrency is merely a tool for nefarious activity. Instead, they demonstrate how Bitcoin's public blockchain makes it a poor tool for bad actors who wish to maintain anonymity.[25]

The evolving nature of cryptocurrency continues to pose challenges as developers create newer privacy-focused coins and mechanisms for enhancing anonymity.

Despite law enforcement's success, the evolving nature of cryptocurrency continues to pose challenges as developers create newer privacy-focused coins and mechanisms for enhancing anonymity. **Monero's XMR** currency is perhaps the most well-known coin with added technology to increase privacy. In fact, in September 2020, the IRS offered $625,000 for anyone who could crack Monero's privacy features.[26] Other privacy enhancing tools such as **"mixers"** pose similar challenges for law enforcement.[27] Investigative techniques must keep pace with these technology advancements in order to identify indicators of nefarious activity.

Regulatory tools have also targeted the ability to use cryptocurrency for illicit purposes. For example, cryptocurrency exchanges operating in the United States are required to employ Know Your Customer, Anti-Money Laundering, and Combating the Financing of Terrorism measures that apply to other financial services businesses.[28] However, some exchanges are now decentralized, with no requirements or capabilities to maintain user or transaction history.[29] These **decentralized exchanges (DEXs)** lack a trusted intermediary and merely facilitate peer-to-peer cryptocurrency trading.[30] They function more like a building owner of a flea market, helping to facilitate transactions, while not actively participating in transactions. In effect, DEXs stack another level of decentralization on top of the already decentralized cryptocurrency. This structure limits the ability of law enforcement and regulators to track

or audit transactions on DEXs and would likely make any attempt to subpoena information from a DEX fruitless. After all, DEXs have no central entity to audit or subpoena. DEX transactions require users to transfer cryptocurrencies using physical or virtual digital wallets which contain a person's full transaction history for that wallet. This aspect of cryptocurrency also presents concerns for organizations when it comes to security of personnel and the related concerns blockchain technology can generate.

PERSONAL FINANCIAL RISKS

All employees are subject to financial stress. Personal financial health is a performance and security concern. Stock market crashes, identity theft, foreclosure, and related events can impact job performance. Service departments offer a wide variety of assistance to help personnel stay focused on the mission, including legal assistance, financial literacy training, and even tax services. Cryptocurrency will increasingly impact financial stress and factor into these services.

Fraud Schemes

Cryptocurrency is subject to common fraud schemes. For example, the private keys associated with cryptocurrency are akin to passwords and are thus targets of phishing. The Federal Trade Commission has compiled helpful information to assist those inquiring about cryptocurrency fraud.[31]

Tax Implications

Cryptocurrency also has federal tax implications. The IRS treats cryptocurrency as property for tax purposes.[32] This designation imposes tax consequences for something as simple as buying a cup of coffee with Bitcoin, such as the need for the buyer to calculate the basis and gain in the Bitcoin used for the purchase.

Family Law Issues

Cryptocurrency will increasingly become a factor in family law issues as well. Lawyers apply relevant state property laws to divorce agreements and will have to determine how the state at issue treats cryptocurrency. Due to the highly volatile market prices for cryptocurrencies, court orders may be necessary to prevent parties from converting fiat currency to virtual currency. This temporary restraint will safeguard assets until the proceedings are final. Practitioners advising clients on family law matters involving cryptocurrency must be generally aware of the relevant financial and tax implications or be prepared to direct the clients to someone more qualified.

Estate Planning

Finally, cryptocurrency factors into estate planning. Lawyers should understand how to incorporate digital assets into estate plans and should be prepared to discuss the unique aspects of cryptocurrency with their clients. The American Bar Association has published some guidance,[33] and the Air Force JAG Corps has internal guidance for its legal assistance personnel.[34]

> Decentralized transactions do not benefit from a financial institution spreadsheet for transactions, making itemized disclosure and valuation a bit more challenging than traditional transactions.

CONFLICTS OF INTEREST

Cryptocurrency, such as Bitcoin, complicates the financial disclosure process. Each year, approximately 400,000 United States employees must disclose their financial connections to different companies and financial institutions, to include investments, close personal relationships, and business interests.[35] The government uses these disclosures to identify conflicts of interest and ensure employees make decisions in the government's best interest. The two commonly used forms are the United States Office of Government Ethics **(OGE) Form 278e** for senior personnel with public disclosure requirements and **OGE Form 450** for non-senior personnel with confidential disclosure requirements.[36] Given the novel and unique nature of cryptocurrency, many filers may not be aware of the disclosure requirements applicable to cryptocurrency. Current OGE guidance defines cryptocurrency as property held for investment.[37] Financial disclosure filers must report a cryptocurrency holding if

the value of the holding exceeds $1,000 at the end of the reporting period or if the holding produced more than $200 in income during the reporting period. Filers have additional reporting requirements for cryptocurrencies that are also securities.[38] Decentralized transactions do not benefit from a financial institution spreadsheet for transactions, making itemized disclosure and valuation a bit more challenging than traditional transactions.

Whether a cryptocurrency is a security is currently one of the most complicated and controversial legal questions related to cryptocurrency and corporate finance.

Whether a cryptocurrency is a security is currently one of the most complicated and controversial legal questions related to cryptocurrency and corporate finance.[39] In December 2020, the Securities and Exchange Commission (SEC) sued the largest U.S.-based cryptocurrency firm, Ripple, alleging Ripple's XRP cryptocurrency was an unregistered security.[40] SEC officials have previously opined that Bitcoin and another popular cryptocurrency, Ethereum, are not securities.[41] Federal ethics and financial disclosure guidance will likely require updating upon finalization of the Ripple lawsuit or issuance of comprehensive cryptocurrency regulations on this topic.

As with any new technology, regulations and litigation will impact value, compliance, and reporting requirements. Additionally, federal agencies may define and classify digital assets differently for different reporting purposes. Admittedly, most of the federal workforce is not required to file financial disclosures, but employees still may face personal financial issues due to cryptocurrency's confusing regulatory environment.

FEDERAL PERSONNEL SECURITY CONCERNS

All large organizations maintain personnel risk management policies. United States Government personnel security management policies include a plethora of programs designed to protect and advance organizational objectives. These programs include preventing opportunities for espionage, insider threats, fraud, and financial conflicts of interest. Beyond prevention efforts, the services offer programs such as legal assistance for taxes, estate planning, and consumer protection to minimize personal distractions and increase focus on assigned missions. The following paragraphs provide an overview of how cryptocurrency technology implicates these programs.

Current DoD guidance prohibits personnel with a security clearance from owning foreign state-backed, hosted, or managed cryptocurrency or wallets hosted by foreign exchanges, excluding diversified investments.

Over four million United States employees and contractors are cleared for access to classified information, with the DoD accounting for the large majority of these cleared personnel.[42] Security Clearance suitability determinations screen for foreign contacts, business relationships, influence, and preference.[43] Current DoD guidance prohibits personnel with a security clearance from owning foreign state-backed, hosted, or managed cryptocurrency or wallets hosted by foreign exchanges, excluding diversified investments.[44] The guidance aims to avoid cleared personnel having assets held hostage on a foreign exchange, but does not apply to DEXs.[45] This lack of focus is especially important since DEX use may pose a greater clearance risk than foreign exchanges.

Use of foreign exchanges has been significantly mitigated by the largest ones creating separate, U.S. regulatory complaint services for U.S. customers, and by blocking U.S.-based IP addresses from accessing foreign exchange services.[46] For example, in November 2020, Binance forced U.S.-based users to leave its original exchange, pointing them instead to its reduced service "BinanceUS" exchange.[47] Further risk mitigation comes from how cryptocurrency trading commonly occurs — it involves automated transactions based on technical indicators, functioning like a diversified investment portfolio, not large individual transactions that could be held hostage.

Since DEXs do not hold or track assets, there simply is no easy way to track, audit, or otherwise catch illicit decentralized financial activities.

So long as assets are not held on foreign-controlled wallets, DEX use does not pose the same risk of assets being held hostage, but it does increase the risk of personnel hiding illicit transactions. Since DEXs do not hold or track assets, there simply is no easy way to track, audit, or otherwise catch illicit decentralized financial activities. This limitation places greater importance on the use of current screening and investigative techniques to prevent, identify, and respond to **insider threats** to government programs. This new era will require employees to pay greater attention to coworkers who exhibit indicators of unexplained financial gain.

BLOCKCHAIN TECHNOLOGY USE CASES AND MILITARY APPLICATIONS

Although blockchain technology will for all time be associated with Bitcoin due to their common genesis, it has broader applications.[48] Any type of data or information can be **"tokenized"** and placed upon a blockchain. For assets, the asset is associated with a digital token, and whoever has the private keys to that token owns the asset. In March 2021, a tokenized digital image sold online at Christie's for $69.3 million.[49] In 2018, the owners of the St. Regis Aspen resort hotel in Aspen, Colorado tokenized and sold nearly 20 percent of the hotel through $18 million in digital tokens.[50] Blockchain technology can also be used to secure data and process transactions in almost any industry. Estonia now uses it to handle all the country's healthcare billing.[51] A Russian airline company recently developed a blockchain-based system for digital aviation fuel payments, cutting processing times from 4 to 5 days to 15 seconds.[52] There are many other indicators that society is on the cusp of blockchain mass adoption.

There are many other indicators that society is on the cusp of blockchain mass adoption.

The DoD has been interested in blockchain technology for a few years now. In 2018, the Defense Logistics Agency acknowledged the potential for blockchain to enhance supply chain management.[53] The Defense Advanced Research Projects Agency (DARPA) began experimenting with blockchain in 2019, and the DoD Digital Modernization Strategy noted its cybersecurity benefits.[54] Over the past year-and-a-half, Simba Chain has been awarded multiple contracts to develop blockchain projects for the Air Force, the Navy, and the DoD.[55] The Space Force also recently chose a blockchain company to develop data security systems.[56] So far in 2021, the Air Force has vetted 22 proposals for innovative blockchain research.[57] While the details remain proprietary, the proposed use cases were very promising, especially for military uses and commercialization. Military involvement in blockchain development could have a more pronounced impact on society than the military's role in the Global Positioning System. Yet as with any new technology, the use cases are not limited to those who wish to benefit society. Criminals are discovering their own use cases, posing new challenges for law enforcement and prosecutors.

Military lawyers should stay current on the broad applications of blockchain technology in the defense community, especially as other global powers advance their capabilities.

For example, at times the United States struggles to keep up with near-peer advancements in cyber hacking.[58] China recently created its own cryptocurrency, in part to circumvent United States sanctions.[59] Blockchain technology presents a new chapter of capabilities for cyber, operations, and even acquisitions. Military lawyers with a basic understanding of this technology will be better equipped to advise senior ranking officials as they increasingly encounter it in these various spheres.

With increasing use and corporate adoption, cryptocurrency and blockchain technology are already changing how society operates.

CONCLUSION

This overview will likely be the first of many resources devoted to this new technology. With increasing use and corporate adoption, cryptocurrency and blockchain technology are already changing how society operates. Familiarity with cryptocurrency is becoming a competency requirement for lawyers, regardless of practice area. Blockchain technology itself is also quickly finding broader uses in expanding global economic power, military cyber strategy, and fundamental human rights. Military lawyers must begin paying more attention to these new and quickly involving issues in order to accelerate change, or lose.

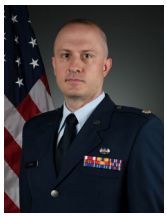
Edited by Captain Jordan F. Davis and Captain Olivia B. Hoff

Layout by Thomasa Huffstutler

ABOUT THE AUTHORS

Lieutenant Colonel Dean W. Korsak, USAF

(LL.M., Columbia Law School; J.D., Mississippi College School of Law; B.S., Liberty University) is the Staff Judge Advocate for the Air Force Research Laboratory, Information Directorate, Rome, New York. Lt Col Korsak began his military career as an electronics technician. As an attorney, he has provided counsel to installation and headquarters level program teams spearheading the development and maturing of advanced technologies. He is a member of the Mississippi bar.



Major Erik T. Fuqua, USAF

(LL.M. Candidate, George Washington University Law School; J.D., Baylor Law School; B.A., The University of Tennessee at Martin) is an LL.M. student at George Washington University Law School and is assigned to the Air Force Institute of Technology. Major Fuqua has served as a trial counsel, medical law attorney, Chief of Military Justice, and Special Assistant United States Attorney. He is a member of the Tennessee bar.

ENDNOTES

[1] For clarity, the remainder of this article will use the term cryptocurrency. Other sources may use terms such as virtual currency or digital currency.

[2] *See generally* Yuval Noah Harari, Sapiens: A Brief History of Humankind 173-187 (2015) (explaining the development of money over spans of human history).

[3] David Kinley, Money: A Study of the Theory of the Medium of Exchange 39-52 (1909).

[4] *Id*. at 16 (internal citations and quotations marks omitted).

[5] *See* Jane Gleeson-White, Double Entry: How the Merchants of Venice Created Modern Finance 20–21 (2013) (explaining that double-entry accounting first emerged in about 1300 A.D).

[6] *Id*. at 101.

[7] *See* Makato Yano et al., Blockchain and Crypto Currency: Building a High Quality marketplace for Crypto Data 64-65 (2020) (providing a discussion of monetary systems and the function of money).

[8] Jack Weatherford, The History of Money: From Sandstone to Cyberspace 124 (1997).

[9] Harari, *supra* note 2, at 186.

[10] *See generally*, Kevin Phillips, Bad Money: Reckless Finance, Failed Politics, and The Global Crisis of American Capitalism 20-21 (2008) (providing historical examples of indicators of when a nation has passed its zenith of world economic power).

[11] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf (last visited 13 March 2021). "Satoshi Nakamoto" is a pseudonym, and Satoshi's identity has been a mystery since Bitcoin's inception. *See* Zoë Bernard and Grace Kay, *The many alleged identities of Bitcoin's mysterious creator, Satoshi Nakamoto*, Business Insider (26 February 2021), https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12.

[12] All cryptocurrencies created after Bitcoin are referred to as alternative coins, or "alt coins." Also, this article uses the Bitcoin blockchain in its discussion since it is the original blockchain. While other cryptocurrencies and blockchain projects may use blockchain technology, they will have their own separate blockchains.

[13] *See generally*, Yano, *supra* note 7, at 32-34 (explaining the need for smart contracts and the limitations of blockchain, including how smart contracts are computer programs built on blockchain protocols that automatically facilitate preset agreement criteria).

[14] *See* Leslie Lamport et al., *The Byzantine General's Problem*, 4 ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS, Issue 3, 382 (1982), https://doi.org/10.1145/357172.357176, (providing an overview of the Byzantine General's Problem as an allegory first used to describe computing limitations), *see also* Anthony Stevens, *Understanding the Byzantine Generals' Problem (and how it affects you)*, Medium (7 May 2018), https://medium.com/coinmonks/a-note-from-anthony-if-you-havent-already-please-read-the-article-gaining-clarity-on-key-787989107969, (Explaining The Problem in its simplest form asks the question: "How can individual parties find a way to guarantee full consensus?").

[15] *See* Alyssa Hertig, *What is Proof-of-Work?*, Coindesk (16 December 2020), https://www.coindesk.com/what-is-proof-of-work (discussing the proof-of-work concept and providing additional discussion of blockchain mining).

[16] "Not your keys, not your coins" is a well-known saying in the cryptosphere popularized by Bitcoin expert Andreas Antonopoulos. Stakefish, *Not Your Keys, Not Your Coins*, Medium (21 May 2020), https://link.medium.com/LX3kckUHgfb.

[17] Daniel Phillips, *How many Bitcoin does its inventor Satoshi Nakamoto still own?*, Decrypt (3 January 2021), https://decrypt.co/34810/how-many-bitcoin-does-its-inventor-satoshi-nakamoto-still-own (explaining that as of 3 January 2021, Satoshi's wallets were worth over $30 billion).

[18] S*ee Bitcoin Private Keys, Public Keys, and Addresses: The Basics*, Bitcoin Clarity, https://getbitcoinclarity.com/blog/2020/05/16/what-is-a-bitcoin-private-key (last visited 13 March 2021) (providing further information on keys and addresses), *and* Bitcoin Magazine, An Overview of Bitcoin's Cryptography (18 June 2021), https://bitcoinmagazine.com/technical/overview-bitcoins-cryptography (explaining how Public Key Cryptography uses "trapdoor functions" to easily generate public keys from private keys but which are effectively impossible to reverse engineer).

[19] U.S. Dep't of Justice, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework* (8 October 2020), https://www.justice.gov/archives/ag/page/file/1326061/download.

[20] *Id*.

[21] S*ee* Marcell Nimfuehr, *Silk Road: A Cautionary Tale about Online Anonymity*, Medium (18 August 2018), https://medium.com/@marcell74/the-silk-road-a-real-thriller-and-the-truth-about-the-anonymity-of-bitcoin-198b519ca397.

[22] *Id*.

[23] Alex Hern, *US seizes $1bn in bitcoin linked to Silk Road site*, The Guardian (6 November 2020, 11:55 AM), https://www.theguardian.com/technology/2020/nov/06/us-seizes-1bn-in-bitcoin-linked-to-silk-road-site.

[24] *See* Press Release, U.S. Dep't of Justice, *Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside* (7 June 2021), https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside. Although Colonial paid the ransom the day after discovering the hack, it was forced to close pipeline operations for nearly a week, creating gas supply shortages for much of the East Coast. Andrew Morse, *Colonial Pipeline CEO tells Senate decision to pay hackers was made quickly*, CNET (8 June 2021), https://www.cnet.com/tech/services-and-software/colonial-pipeline-ceo-tells-senate-decision-to-pay-hackers-was-made-quickly/.

[25] *See, e.g.,* United States v. 280 Virtual Currency Accounts, Civil Action No. 20-2396 (D.D.C. 27 August 2020), https://www.justice.gov/opa/press-release/file/1310421/download (Providing a fascinating example of a DOJ forfeiture action against North Korean hackers who allegedly stole funds from cryptocurrency exchanges. The complaint also contains a discussion of Bitcoin, Ether, blockchain analysis, hacks, and the process by which the DOJ identified the accounts at issue).

[26] Benjamin Pirus, *What are privacy coins and how do they differ from Bitcoin?*, Cointelegraph, (17 February 2021), https://cointelegraph.com/news/what-are-privacy-coins-and-how-do-they-differ-from-bitcoin. Two firms cracked the code within weeks. *Id*.

[27] Osato Avan-Nomayo, *Cryptocurrency Mixers and Why Governments May Want to Shut Them Down*, Cointelegraph (28 May 2019), https://cointelegraph.com/news/cryptocurrency-mixers-and-why-governments-may-want-to-shut-them-down.

[28] Craig Adeyanju, *What Crypto Exchanges Do to Comply With KYC, AML and CFT Regulations*, Cointelegraph, (17 May 2019), https://cointelegraph.com/news/what-crypto-exchanges-do-to-comply-with-kyc-aml-and-cft-regulations.

[29] William Foxley, *ShapeShift Is Going Full DeFi to Lose KYC Rules*, Coindesk (6 January 2021, 9:03 AM), https://www.coindesk.com/shapeshift-going-full-defi-lose-kyc-rules.

[30] Cryptopedia Staff, *What Is a Decentralized Exchange (DEX)?*, Cryptopedia (25 March 2021), https://www.gemini.com/cryptopedia/decentralized-exchange-crypto-dex.

[31] U.S. Federal Trade Commission, *What to Know About Cryptocurrency*, (April 2021), https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency.

[32] *See* I.R.S. Notice 2014-21, https://www.irs.gov/pub/irs-drop/n-14-21.pdf.

[33] Parker F. Taylor, et. al., *Estate Planning with Cryptocurrency*, Am. Bar Association (July-August 2019), https://www.americanbar.org/groups/real_property_trust_estate/publications/probate-property-magazine/2019/july-august/estate-planning-cryptocurrency/ [limited access, must be a member]

[34] U.S. Dep't of Air Force, The Judge Advocate General's Corps, "Wills and Estates Learning Center," (last updated January 2019), https://kmjas.jag.af.mil/moodle/course/view.php?id=477#section-3 [limited access]. These resources include a Digital Assets Bullet Background Paper for Attorneys, dated January 2019, and a link to the National Conference of State Legislatures list of state statutes governing access to digital assets of decedents.

[35] U.S. Office of Gov't Ethics, Results from the 2019 Annual Agency Ethics Program Questionnaire: A Snapshot of the Executive Branch Ethics Program, 5 (2019), https://www.oge.gov/web/oge.nsf/0/44B8C70719A52E3A852586530070037C/$FILE/2019%20AQ%20Summary%20Report%20FINAL.pdf

[36] U.S. Office of Gov't Ethics, Financial Disclosure Guides, https://www.oge.gov/web/OGE.nsf/ethicsofficials_financial-disc; U.S. Office of Gov't Ethics, Legal Advisory: Guidance for Reporting Virtual Currency on Financial Disclosure Reports, LA-18-02 (18 June 2018), https://oge.gov/Web/oge.nsf/Legal Docs/D9038B8D8DE24D88852585BA005BEC34/$FILE/LA-18-06.pdf.

[37] *Id*.

[38] These disclosures would be made using an OGE Form 278-T and the transactions section of the OGE Form 278e.

[39] S*ee, e.g.,* Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (25 July 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf (commonly called "The DAO Report." This report demonstrates the complexity of the securities analysis.).

[40] SEC v. Ripple Labs, Inc., Case No. 1:20-cv-10832 (U.S. Dist. Ct., S.D.N.Y., 22 December 2020).

[41] Bob Pisani, *Bitcoin and ether are not securities, but some initial coin offerings may be, SEC official says*, CNBC (14 June 2018), https://www.cnbc.com/2018/06/14/bitcoin-and-ethereum-are-not-securities-but-some-cryptocurrencies-may-be-sec-official-says.html.

[42] C. Todd Lopez, *DoD to Take Over Background Checks by Fiscal 2020*, DoD News (25 June 25 2019), https://www.defense.gov/Explore/News/Article/Article/1886923/dod-to-take-over-background-checks-by-fiscal-2020/.

[43] U.S. Office of Personnel Management, Standard Form 86, *Questionnaire for National Security Positions*, Sections 18 - 20C (November 2016), https://www.opm.gov/forms/pdf_fill/sf86.pdf.

[44] U.S. Under Sec. of Def. for Intelligence and Security, *Implementation of Security Executive Agent Directive 3*, (2 November 2020), on file with the authors.

[45] Email from OSD OUSD I&S, "Virtual Currency DEX Guidance," (23 February 2021), on file with the authors.

[46] Benjamin Pirus, *Crypto Exchanges Barring US Citizens Is Heartbreaking and Frustrating*, Forbes (20 September 2020, 8:03 AM), https://www.forbes.com/sites/benjaminpirus/2020/09/30/crypto-exchanges-barring-us-citizens-is-heartbreaking-and-frustrating/ (noting regulatory compliance measures prevent competitive U.S.-based crypto trading).

[47] Colin Harper, *Binance Ramps Up Crackdown on US Users, Giving Them 14 Days to Withdraw Funds*, Coindesk (24 November 2020, 5:39 PM), https://www.coindesk.com/binance-ramps-up-crackdown-on-us-users-giving-them-14-days-to-withdraw-funds.

[48] Jamie Moy, *Forget Bitcoin, It's All About The Blockchain*, Forbes (22 February, 6:33 AM), https://www.forbes.com/sites/jamiemoy/2018/02/22/forget-bitcoin-its-all-about-the-blockchain/.

[49] Kelly Crow & Caitlin Ostroff, *Beeple NFT Fetches Record-Breaking $69 Million in Christie's Sale*, The Wall Street Journal (11 March 2021, 10:48 AM), https://www.wsj.com/articles/beeple-nft-fetches-record-breaking-69-million-in-christies-sale-11615477732.

[50] Rick Carroll, *In $18 million deal, nearly one-fifth of St. Regis Aspen sells through digital tokens*, Aspen Times (9 October 2018), https://www.aspentimes.com/trending/in-18-million-deal-nearly-one-fifth-of-st-regis-aspen-sells-through-digital-tokens/.

[51] Sam Daley, *How Using Blockchain on Healthcare is Reviving the Industry's Capabilities*, Built In (8 May 2021), https://builtin.com/blockchain/blockchain-healthcare-applications-companies.

[52] Press Release, Gazprom Neft, *Aircraft Blockchain Platform Enables Instant Refuelling Payment* (1 March 2021), https://www.gazprom-neft.com/press-center/news/gazprom_neft_aircraft_blockchain_platform_enables_instant_refuelling_payment/.

[53] John Dwyer III, *Troop Support event poses question: How and where can blockchain help?*, DLA Troop Support Public Affairs (21 December 2018), https://www.dla.mil/AboutDLA/News/NewsArticleView/Article/1720207/troop-support-event-poses-question-how-and-where-can-blockchain-help/.

[54] U.S. Dep't. of Def., Dep't of Def. Information Resources Mgmt Strategic Plan FY 19-23, Digital Modernization Strategy 48 (12 July 2019), *available at* https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

[55] Helen Partz, *Simba Chain Wins Another Contract From US Department of Defense*, Cointelegraph (13 May 2020), https://cointelegraph.com/news/simba-chain-wins-another-contract-from-us-department-of-defense.

[56] Emilia David, *US Space Force taps blockchain firm Xage Security for data protection*, Cointelegraph (20 September 2020), https://cointelegraph.com/news/us-space-force-taps-blockchain-firm-xage-security-for-data-protection.

[57] This statement is based on the author's involvement as an Air Force Small Business Innovation Research 21.1A Commercialization Evaluator, and confirmed by AFWERX email on 29 March 2021, on file with the author. More information is available at https://www.afsbirsttr.us/.

[58] *See generally*, Andy Greenberg, Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers (2019) (providing detailed examples of Russian-backed hacks of entire national infrastructure).

[59] *See* James T. Areddy, *China Creates Its Own Digital Currency, a First for Major Economy*, The Wall Street Journal (5 April 2021, 10:48 AM), https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-for-major-economy-11617634118.