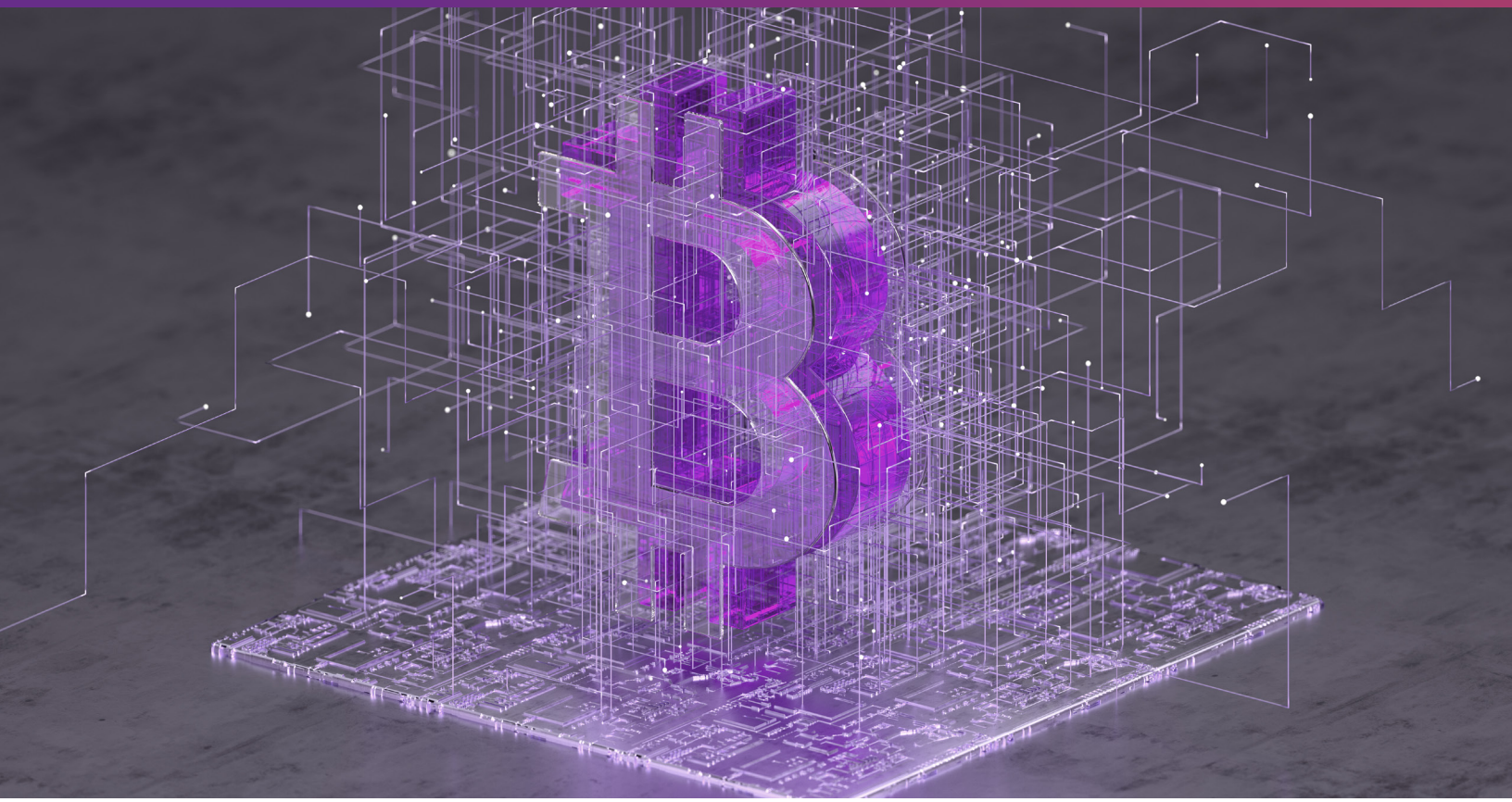
AICPA & CIMA
Worldwide leaders in public and management accounting

FVS Eye on Fraud

The AICPA Forensic and Valuation Services quarterly report on fraud trends and topics



Cryptocurrencies: Forensic techniques to meet the challenge of new fraud and corruption risks

Issued by the AICPA FLS Fraud Task Force
Lead Authors:
Robert A. Musiala, Jr, Esq., CFCS, Teresa M. Goody, Esq., CFE, Veronica Reynolds, Luke Tenery, Mark McGrath, Chris Rowland, and Sunil Sekhri

An Emerging Asset Class and Payment System

It has been approximately 11 years since the Bitcoin Network was launched and the very first cryptocurrency was released into the world following a white paper published by an unidentified developer using the name (or pseudonym) Satoshi Nakamoto.[1] Although bitcoin was the first and is still the most widely known cryptocurrency, there are now thousands of cryptocurrencies, each based on the fundamental technical concepts introduced in Nakamoto's paper and implemented via the Bitcoin Network's open-source code.

Winter 2020, Issue 1

Inside this issue

Overview 1–2

What Makes a Cryptocurrency Investigation Different? 8–11

Cryptocurrency Considerations and Practice Tips for Forensic Accountants . . 12–15

Conclusion 15

[1] Bitcoin.org/Bitcoin.pdf, accessed November 18, 2019.

Over the past 10 years, bitcoin has slowly but steadily become integrated with the mainstream financial system. A few examples: In the United States, you can now exchange U.S. dollars for bitcoin — and vice versa — on a variety of online exchanges or at one of more than 4,000 physical ATMs (which can be searched online on sites like Coin ATM Radar); you can use bitcoin to purchase retail products on Overstock.com; and you can even use bitcoin to purchase a computer at the Microsoft store. According to ***Bloomberg***, E*Trade will soon launch bitcoin trading products, just behind Fidelity, which rolled out its digital-assets services to qualified investors in October of 2019. By all indications, cryptocurrencies are here to stay.

Like any new technology, cryptocurrencies usher in advantages as well as risks. And as with any new technology, criminals and threat actors are often among the earliest adopters as they attempt to exploit those advantages and risks. For this reason, at a minimum, forensic accountants should understand what cryptocurrencies are, how they might turn up in an investigation, and how to respond in these circumstances.

How Have Cryptocurrencies Emerged in Fraud Schemes?

Cryptocurrencies are being used in fraud schemes in much the same way traditional currencies have historically been used. However, these alternative means of value exchange offer some unique challenges for forensic accountants; blockchain and cryptocurrencies present a new twist in traditional accounting schemes. According to blockchain threat intelligence firm CipherTrace, in 2019 alone, approximately $4.26 billion in cryptocurrency funds were lost as a result of criminal activities including cyberthefts, scams, misappropriation, and insider fraud.[2] This amount greatly exceeded that reported in 2018, according to Cointelegraph, a provider of cryptocurrency and blockchain news. Because the details of private investigations are rarely made public, how pervasive cryptocurrency fraud is can be difficult to determine. However, in the public sector, U.S. and international government agencies have been actively prosecuting fraud and corruption involving cryptocurrencies.

The following case descriptions provide a helpful overview of some of the issues that may arise (or have already arisen) in the private sector.

Investment Schemes

Cryptocurrencies provide new opportunities for those interested in perpetrating multilevel marketing and Ponzi schemes. Among the most common are those in which the fraudster solicits money from investors by promising high returns on bitcoin or other cryptocurrency investments. Although the scheme is the same as traditional Ponzi schemes, the fraud involves cryptocurrency rather than fiat currency.[3] One early example of a bitcoin Ponzi scheme is illustrated by an SEC action in which the Commission charged bitcoin mining companies":[4]

> According to the SEC's complaint filed in federal court in Connecticut, "mining" for Bitcoin or other virtual currencies means applying computer power to try to solve complex equations that verify a group of transactions in that virtual currency. The first computer or collection of computers to solve an equation is awarded new units of that virtual currency. The SEC alleges that Homero Joshua Garza perpetrated the fraud through his Connecticut-based companies GAW Miners and ZenMiner by purporting to offer shares of a digital Bitcoin mining operation. In reality, GAW Miners and ZenMiner did not own enough computing power for the mining it promised to conduct, so most investors paid for a share of computing power that never existed. Returns paid to some investors came from proceeds generated from sales to other investors.

In another pivotal case, SEC v. Shavers,[5] which prosecutors called the first U.S. criminal securities fraud case related to bitcoin, the organizer of an alleged Ponzi scheme, Trendon T. Shavers, created an online entity, Bitcoin Savings and Trust, to operate his Ponzi scheme and defrauded investors out of more

[2] ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/; see also https://venturebeat.com/2019/08/12/ciphertrace-cryptocurrency-thefts-scams-and-fraud-could-hit-4-3-billion-in-2019/, accessed November 18, 2019.

[3] Fiat currency is legal tender issued and backed by a central government.

[4] www.sec.gov/news/pressrelease/2015-271.html, accessed November 18, 2019.

[5] www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf, accessed November 18, 2019.

than 700,000 bitcoins. Instead of providing promised returns to investors (of up to 7% interest per week), Shavers allegedly used investor funds to pay other existing investors and exchanged bitcoin into U.S. dollars to pay his own personal expenses.

The following are just a few examples of recent schemes that have been subject to U.S. enforcement actions:

- On May 21, 2019, the SEC obtained a court order to shut down a $30 million Ponzi scheme operating out of Florida through Argyle Coin LLC, a purported cryptocurrency business. According to the SEC complaint, hundreds of investors were tricked into investing in Argyle Coin under the false claim that its tokens were backed by diamonds. Instead, new investor money was used to pay fake returns to prior investors and to pay the exorbitant personal expenses of the individuals associated with Argyle Coin.[6]
- On May 23, 2019, the SEC announced federal court action against a California man claiming to sell instructional packages that included "points" that could be converted into digital assets known as PRO Currency. The agency alleged that the multilevel marketing companies offering the packages and digital tokens were involved in a fraudulent pyramid scheme that raised over $26 million between January 2017 and March 2018 in an unregistered securities offering.[7]
- On June 19, 2019, the U.S. Department of Justice (DOJ) unsealed a criminal complaint alleging money laundering and fraud against a Swedish citizen and his company. According to the complaint, the Swedish man used websites to trick potential investors into sending him cryptocurrency payments that totaled approximately $11 million. The individuals thought they were purchasing shares in investment companies; instead, the cryptocurrency funds were converted to fiat, transferred to the Swedish man's bank account, and later used to buy real estate in Thailand.[8]
- On August 13, 2019, the SEC announced fraud charges and filed an emergency action in federal court and an application for a temporary restraining order against blockchain firms Veritaseum Inc. and Veritaseum LLC, seeking to freeze approximately $8 million of proceeds raised in what the SEC alleged was a fraudulent initial coin offering (ICO) scheme and unregistered securities offering that took place in 2017 and 2018.[9]
- On August 29, 2019, the SEC announced that it settled charges with Bitqyck Inc. and its founders, alleging that they had defrauded investors in securities offerings of two cryptocurrency tokens and had operated an unregistered exchange. According to the SEC, the defendants lied to investors and fraudulently raised $13 million through unregistered token sales.[10]
- On September 30, 2019, the DOJ announced an indictment against the principal of cryptocurrency escrow company Volantis Escrow Platform LLC after he allegedly received a total of $7 million from two separate victim companies after making false statements in connection with bitcoin transactions.[11]

Investment schemes involving cryptocurrencies are a global phenomenon that extends beyond the United States. In one case, a group in Taiwan defrauded more than 1,000 people of approximately $51 million by promising investors annual returns of up to 355% on cryptocurrency investments.[12]

Embezzlement

Insider theft also has emerged as a threat. In perhaps the most publicized example, Gerald Cotton, the late founder of Canadian cryptocurrency exchange QuadrigaCX, was alleged to have embezzled around $200 million worth of cryptocurrency from customer accounts.[13] He allegedly perpetrated the fraud by creating fake accounts on the exchange, falsely crediting them with nonexistent fiat amounts, and then purchasing real cryptocurrency from customers on the exchange.[14] Upon his apparent death, others were unable to access his cryptocurrency accounts as he was the only one in possession of the passwords.

[6] www.sec.gov/news/press-release/2019-72, accessed November 18, 2019.

[7] www.sec.gov/news/press-release/2019-74, accessed November 18, 2019.

[8] www.justice.gov/usao-ndca/pr/alleged-cryptocurrency-fraudster-arrested-thailand-charged-multi-million-dollar, accessed November 18, 2019.

[9] www.sec.gov/news/press-release/2019-150 , accessed November 18, 2019.

[10] www.sec.gov/litigation/litreleases/2019/lr24582.htm, accessed November 18, 2019.

[11] www.justice.gov/usao-sdny/pr/principal-cryptocurrency-escrow-company-indicted-7-million-fraudulent-scheme, accessed November 18, 2019.

[12] http://focustaiwan.tw/news/asoc/201901180015.aspx, accessed November 18, 2019

[13] www.coindesk.com/quadrigacx-ceo-set-up-fake-crypto-exchange-accounts-with-customer-funds, accessed November 18, 2019

[14] See footnote 23.

In November 2018, the U.S. Commodity Futures Trading Commission (CFTC) ordered a man charged with embezzlement and fraud to pay more than $1.1 million in restitution to his former employer, a Chicago-based proprietary trading firm, as well as to select customers of the firm. The defendant allegedly stole more than $600,000 in cryptocurrencies from his former employer and fraudulently solicited approximately $545,000 from customers in a cryptocurrency investment scheme.[15]

In another example, South Korea's largest cryptocurrency exchange, Bithumb, lost tens of millions in cryptocurrencies in March 2019, due to what investigators believe were "legitimate" withdrawals by an insider. Another South Korean exchange, Coinbin, was forced into bankruptcy in 2019 when it suffered losses of approximately $26 million after embezzlement by an executive left it insolvent.[16]

Phishing

Phishing has spread to include exploiting cryptocurrency, with attackers seeking to lure victims into sending cryptocurrency payments that settle almost instantly — and are irreversible once made. In the summer of 2019, several phishing schemes sought to take advantage of the hype associated with Libra, Facebook's newly announced cryptocurrency. Although Libra has not yet been issued into circulation, one scammer falsely offered pre-sale Libra currency ahead of its official launch.[17] Other scammers launched fake social media accounts promoting fraudulent offerings of the cryptocurrency at a discounted rate through third-party sites.[18] According to a July 2019 ***Forbes*** story, another criminal syndicate promoted Libra investment services on social media that required submission of a phone number to enroll.[19] The victim would then receive a boiler-room call from a fraudulent Libra representative offering to sell Libra. In these and other phishing schemes, the fraudsters typically request payment in bitcoin or other cryptocurrencies.

According to the Blockchain Council, an industry advocacy group, a new type of phishing scheme unique to cryptocurrency involves what has become known as dusting. Fraudsters send very small amounts (as in "dust") of cryptocurrency to a large number of addresses. The fraudster then monitors the transactions to see where the dust is accruing to identify which addresses correlate to a single wallet. In some cases, this allows the scammers to identify wallet owners. Attackers then use this information for phishing or blackmail attempts designed to extort cryptocurrency payments.

SIM Swapping

The rise of cryptocurrencies has been accompanied by an epidemic of SIM swapping (also known as SIM jacking), which involves a criminal impersonating a mobile-carrier customer in order to switch the victim's phone number to a fraudulent subscriber identity module (SIM) card. In doing so, the criminal often gains access to the victims' cryptocurrency accounts. In late 2018, authorities arrested a SIM swapper named Joseph Harris. Harris allegedly stole $14 million from cryptocurrency startup Crowd Machine by unlawfully obtaining the CEO's cryptocurrency wallet credentials.[20] In early 2019, prosecutors in California secured the first conviction for SIM swapping when a 20-year-old college student was sentenced to 10 years in prison after defrauding around 40 victims of more than $5 million.[21] Between 2018 and 2019, more than $50 million in cryptocurrency was stolen through SIM-swapping techniques.[22] The hackers are often under 25 years old, as in several recent cases,[23] and leave a trail of evidence after bragging about their conquests on social media. The hackers frequently work together in groups.

[15] www.cftc.gov/PressRoom/PressReleases/7839-18, accessed November 18, 2019.

[16] https://www.coindesk.com/crypto-exchange-bithumb-hacked-for-13-million-in-suspected-insider-job , accessed November 18, 2019

[17] www.coindesk.com/libra-scams-on-the-rise-as-newbies-learn-about-facebooks-crypto, accessed November 18, 2019.

[18] www.theverge.com/2019/7/23/20706772/facebook-libra-scams-pages-groups-accounts-pre-sale-cryptocurency-fraud, accessed November 18, 2019.

[19] www.forbes.com/sites/investor/2019/07/26/facebooks-libra-scammers-attack/#6ae8c3bf355b, accessed November 18, 2019.

[20] www.vice.com/en_us/article/7x3may/cops-arrest-sim-swapper-14-million-cryptocurrency, accessed November 18, 2019.

[21] www.vice.com/en_us/article/gyaqnb/hacker-joel-ortiz-sim-swapping-10-years-in-prison, accessed November 18, 2019.

[22] breakermag.com/hackers-steal-more-than-50-million-in-cryptocurrency-in-15-months/, accessed November 18, 2019.

[23] www.vice.com/en_us/article/gyaqnb/hacker-joel-ortiz-sim-swapping-10-years-in-prison; breakermag.com/hackers-steal-more-than-50-million-in-cryptocurrency-in-15-months/; www.vice.com/en_us/article/7x3may/cops-arrest-sim-swapper-14-million-cryptocurrency; all accessed November 18, 2019.

Cryptomining Malware

Cryptomining malware (also known as crypto-jacking) occurs when cybercriminals install malicious code on the devices of individuals or organizations through techniques similar to phishing attacks. However, instead of stealing personal information, the malicious code harnesses processing power to generate cryptocurrencies through mining. The cybercriminals then transfer the newly mined cryptocurrencies to wallets they control. These types of attacks have increased significantly over the past two years. Examples of recent attacks include the following:

- In June 2018, Japanese authorities arrested 16 suspects for their alleged involvement in a cryptomining malware scheme. The suspects were allegedly mining monero, a cryptocurrency with certain privacy features, in their victims' machines.[24] Also in the summer of 2018, security researchers uncovered cryptomining malware attacks that targeted a specific type of router, spreading monero-mining malware to every web page that a user visited using the vulnerable router.[25] In January 2019, security researchers published findings on a new variant of monero-mining malware that had the built-in ability to block rival mining software and disable cloud security agents, including those of a number of leading cloud service providers.[26]
- In April of 2019, two Romanian cybercriminals were convicted in Ohio on 21 felony counts related to the infection of 40,000 computers with malware in order to steal credit card and other information to sell on the dark web. The schemes included taking control of the victim's computers, which allowed the defendants to use the processing power of the computers to engage in cryptocurrency mining. The victim's incurred losses of millions of dollars.[27]
- In March 2019, hackers reportedly exploited a vulnerability in a major enterprise application server for the purpose of installing cryptomining malware.[28] A few months later, in June 2019, a China-based malware campaign was discovered that reportedly breached more than 50,000 servers across the world and infected more than 700 new victims a day. According to reports, most of the affected firms were in the healthcare, telecom, media, and IT sectors. The malware packages were written using sophisticated Chinese language tools and placed on Chinese language servers.[29] Another attack reported in June 2019 involved a fraudulent website impersonating a cryptocurrency trading platform. When visited, the malicious website reportedly executed an attack that installed cryptomining malware."[30]
- In August of 2019, cryptomining malware was found hidden in popular Ruby code libraries. Half of the infected libraries were blockchain-related and had been downloaded hundreds of times.[31]
- In perhaps the most noteworthy example, a former software engineer at a major U.S. bank was indicted for unauthorized intrusion into stored data of the defendant's former employer and more than 30 other companies. According to the U.S. DOJ, the defendant gained unlawful access to data on cloud servers and "used this access not only to steal data but also used stolen computer power to 'mine' cryptocurrency for her own benefit."[32] According to the indictment filed by the FBI, the access resulted in a breach of the information of 100 million bank customers.
- A similar scheme was uncovered by U.S. authorities in October 2019, when prosecutors in the United States indicted Ho Jun Jia, who stands accused of wire fraud, access device fraud, and identity theft for allegedly stealing the identities of multiple parties to gain unauthorized access to cloud computing services, which the defendant then used to run a large-scale cryptocurrency mining operation. At one point, one of the fraudulent accounts constituted a cloud provider's "largest consumer of data usage by volume."[33]

[24] cointelegraph.com/news/japan-16-arrested-in-monero-cryptojacking-case-local-media-report, accessed November 18, 2019. .

[25] thehackernews.com/2018/08/mikrotik-router-hacking.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&m=1, accessed November 18, 2019.

[26] unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/, accessed November 18, 2019.

[27] www.justice.gov/opa/pr/two-romanian-cybercriminals-convicted-all-21-counts-relating-infecting-over-400000-victim, accessed November 18, 2019.

[28] www.imperva.com/blog/hundreds-of-vulnerable-docker-hosts-exploited-by-cryptocurrency-miners/, accessed November 18, 2019.

[29] www.guardicore.com/2019/05/nansh0u-campaign-hackers-arsenal-grows-stronger/, accessed November 18, 2019.

[30] www.bleepingcomputer.com/news/security/fake-cryptocurrency-trading-site-pushes-crypto-stealing-malware/, accessed November 18, 2019.

[31] decrypt.co/8602/malicious-cryptjacking-code-found-in-11-ruby-libraries, accessed November 18, 2019.

[32] www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-indicted-federal-charges-wire-fraud-and-computer-data-theft, accessed November 18, 2019.

[33] www.justice.gov/usao-wdwa/press-release/file/1207986/download, accessed November 18, 2019.

Recent notable statistics on cryptomining malware include the following:

- New cryptomining malware samples increased 629% to more than 2.9 million in the first quarter of 2018 and then by another 2.5 million new samples in the second quarter of 2018.[34]
- According to cybersecurity nonprofit Cyber Threat Alliance, from 2017 to 2018, cryptomining malware detections increased by 459%.[35]

Ransomware

Cybercriminals are taking full advantage of newer technologies, such as cryptocurrencies, to perpetrate fraud, and one such notable trend in recent years is ransomware. Ransomware is a form of malicious software that takes control of a victim's digital device and holds it hostage until the victim pays the hackers to regain access. Hackers almost exclusively demand that ransomware payments be made in bitcoin. In 2019, intelligence firm Chainalysis noted that 64% of the money stolen through ransomware attacks was laundered through cryptocurrency exchanges,[36] while McAfee Labs reported that during the first quarter of 2019 ransomware attacks increased by 118%.[37] By all accounts, ransomware attacks are an increasing cause for concern.

The ransomware business model works by effectively creating a hostage situation using the victim's data. As stated, ransomware is a form of malware that renders the victim's data and systems useless by encrypting the data and crippling system operations. Once the attackers are paid the ransom, they usually provide a means to decrypt the data and allow the entity to "get back to business." In paying the ransomware using cryptocurrency, such as bitcoin, one is creating a blockchain trail that can, in theory, be used to track transactions. Because attackers use methods to obfuscate their identity, tracing such payments can be very difficult. As noted in a prior ***FVS Eye on Fraud*** article (Fall 2018, Issue 4)[38] "cryptocurrencies make it easier for attacks to happen on a global scale, and the anonymity of cryptocurrencies makes it harder to track down, along with the perpetrators, who are often located outside of the United States and in countries that are out of reach of the DOJ, such as some Eastern European nations and North Korea."

The ransomware trend has helped shape the insurance industry as well, leading to a vicious cycle of increased ransom payments and emboldened cybercriminals. According to a ProPublica story on the "extortion economy,"[39]

> [r]ansomware is proliferating across America, disabling computer systems of corporations, city governments, schools and police departments. [In August 2019], attackers seeking millions of dollars encrypted the files of 22 Texas municipalities. Overlooked in the ransomware spree is the role of an industry that is both fueling and benefiting from it: insurance. In recent years, cyber insurance sold by domestic and foreign companies has grown into an estimated $7 billion to $8 billion-a-year market in the U.S. alone. … Ransomware is one of the most common cybercrimes in the world. Although it is often cast as a foreign problem, because hacks tend to originate from countries such as Russia and Iran, ProPublica has found that American industries have fostered its proliferation. … On June 10, [2019] Lake City [Florida] government officials noticed they couldn't make calls or send emails. … The city soon learned it was struck by Ryuk ransomware. Over the past year, unknown attackers using the Ryuk strain have besieged small municipalities and technology and logistics companies, demanding ransoms up to $5 million, according to the FBI.

[34] www.businesswire.com/news/home/20180924006048/en/McAfee-Labs-Sees-Cryptocurrency-Mining-Surge-Continue, accessed November 18, 2019.

[35] www.cyberthreatalliance.org/joint-analysis-on-illicit-cryptocurrency-mining/, accessed November 18, 2019.

[36] cointelegraph.com/news/chainalysis-64-of-ransomware-attackers-launder-proceeds-via-crypto-exchanges, accessed November 18, 2019.

[37] www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html, accessed November 18, 2019.

[38] www.aicpa.org/content/dam/aicpa/interestareas/forensicandvaluation/newsandpublications/downloadabledocuments/fvs-eye-on-fraud-newsletter.pdf, accessed November 18, 2019.

[39] www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks#166952, accessed November 18, 2019.

What happens after you pay a ransomware attacker? Cryptocurrency ransom payments (typically in bitcoin) are deposited into the attacker's digital wallet, identified by the wallet address (much like a traditional bank account). Once the attacker receives the cryptocurrency payment, a decryption key is typically provided (through a cryptocurrency broker) to the victim. The decryption tool is normally tested prior to use and then applied to the affected systems to decrypt the data.

Examples of recent ransomware attacks include the following:

- In November 2018, the U.S. Treasury Department's Office of Foreign Assets Control added Bitcoin Network public key addresses to the U.S. sanctions lists. These public keys were related to the SamSam ransomware, which has hit more than 200 victims over the past few years, including corporations, hospitals, ports, universities, and government agencies. From 2015–2018, damages from SamSam ransomware are estimated at more than $30 million.[40]
- In June 2019, the city of Riviera Beach, Florida, was targeted by ransomware, with hackers demanding a ransom of $600,000. The city council agreed to have its insurance carrier pay the 65-bitcoin ransom. The attack was reportedly triggered when a police department employee opened an email attachment containing malware, which rapidly spread through the city's computer systems, crippled its email system and, crucially, the city's 911 dispatch operations.[41]
- In August 2019, gamers found themselves under threat from ransomware that targeted players of Fortnite, a popular online game. Affected players downloaded what they thought was a helpful in-game add-on that turned out to be ransomware.[42]
- In August 2019, French enforcement agencies broke up a botnet ring estimated to have made millions from ransomware from 2016–2019 by infecting over 850,000 computers in more than 100 countries, primarily in Central and South America.[43]
- In October 2019, ransomware attackers encrypted file systems at three Alabama hospitals. Medical staff at the hospitals were reportedly "forced to switch to a manual paper system to track patient data while their systems were down."[44]
- According to a report by anti-malware company EmsiSoft published in October 2019, "[i]n the first nine months of 2019, at least 621 government entities, healthcare service providers and school districts, colleges and universities were affected by ransomware." The report estimates total losses from these attacks at $5 billion.[45]

Exchange Hacks

Of all financial crimes involving cryptocurrencies, by far the greatest losses have resulted from hacks of cryptocurrency exchanges. In May 2019, The Wall Street Journal reported that more than $1.7 billion in cryptocurrency had been stolen from exchanges around the world.[46] After absconding with funds, criminals often attempt to hide the unlawfully acquired cryptocurrencies across other exchanges, where the cryptocurrency can later be converted to fiat currency. According to a 2018 WSJ report, almost $90 million has been laundered through exchanges since 2016.[47]

Notable hacks from 2019 include the following:

- In January, Australian cryptocurrency exchange Cryptopia lost approximately $16 million in cryptocurrencies in a hack.[48] Fifteen days later, the exchange was hacked again for an additional $180,000 in cryptocurrencies, indicating that the hackers continued to control some of the exchange's cryptocurrency wallets.[49]

[40] www.coindesk.com/us-regulators-tie-two-Bitcoin-addresses-to-iranian-ransomware-plot; and slate.com/technology/2018/12/iranian-indictment-samsam-ransomware-Bitcoin-wallet-addresses.html, accessed November 18, 2019

[41] www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html, accessed November 18, 2019.

[42] threatpost.com/fortnite-ransomware-masquerades-as-an-aimbot-game-hack/147549/, accessed November 18, 2019.

[43] www.vice.com/en_us/article/wjwd7x/cops-hijack-retadup-botnetwipe-malware-from-850000-computers; thenextweb.com/hardfork/2019/08/29/cybergendarmes-shut-down-monero-mining-botnet/; and www.bbc.com/news/world-europe-49494927, all accessed November 18, 2019.

[44] gizmodo.com/alabama-hospitals-pay-out-in-ransomware-attack-amid-fbi-1838826293, accessed November 18, 2019.

[45] blog.emsisoft.com/en/34193/state-of-ransomware-in-the-u-s-2019-report-for-q1-to-q3/, accessed November 18, 2019.

[46] www.wsj.com/articles/hackers-swipe-more-than-40-million-of-Bitcoin-from-cryptocurrency-exchange-11557296830, accessed November 18, 2019.

[47] https://www.wsj.com/articles/how-dirty-money-disappears-into-the-black-hole-of-cryptocurrency-1538149743?tesla=y&mod=e2li, accessed November 18, 2019

[48] www.coindesk.com/hacked-cryptocurrency-exchange-cryptopia-goes-into-liquidation, accessed November 18, 2019.

[49] elementus.io/blog/cryptopia-hacker-strikes-again-15-days-later/, accessed November 18, 2019.

- In March, DragonX, a Singapore exchange, lost an undisclosed amount of cryptocurrencies in a hack and called on other exchanges to freeze any transactions believed to be associated with the stolen funds.[50]
- According to cryptocurrency capital flow research team Clain.io, in May 2019, 7,074 bitcoins (then worth approximately $40 million) were stolen from global cryptocurrency exchange Binance. After the hack, the stolen Bitcoin was reportedly sent to Chipmixer, a bitcoin "tumbler" that obfuscates the origin of cryptocurrencies on the bitcoin blockchain.[51] According to a company press release, hackers were able to execute the fraud by obtaining a large number of application programming interface (API) keys and two-factor authentication codes.[52]
- In June, cryptocurrency exchange Gatehub reported $9.5 million in losses due to a hack.[53]
- In July, cryptocurrency exchange Bitpoint announced that it had lost $32 million in cryptocurrency in a hack.[54]

What Makes a Cryptocurrency Investigation Different?

As the preceding examples show, forensic accountants are likely to encounter cryptocurrencies in various scenarios and with increased frequency. To prepare for this, accountants need to achieve a basic understanding of the technology that underpins cryptocurrencies, the markets in which they operate, and the regulations that govern these new assets.

Technical Features of Blockchain and Cryptocurrencies

In technical terms, a blockchain is a cryptographically secured transaction network and ledger that is shared among and verified by all computer nodes participating in a distributed system. In plain English, blockchain is a new type of database that brings together four key characteristics in a way that no other database has done before:

- Advanced public-private key cryptography enables enhanced data privacy and security.
- Distributed networks increase network security and trust among parties.
- Data immutability prevents tampering with records.
- Disintermediation allows blockchains to "cut out the middleman" in data transfer, enabling peer-to-peer (P2P) transactions.

It is worth noting that, since 2015, multiple nonfinancial use cases have emerged for blockchain technology. Most of these leverage private blockchains to enhance speed, transparency, and security over management and transfer of data in a variety of areas, including supply chain, digital identity, digital advertising, IoT (Internet of Things) device management, and even energy-grid security. However, for the financial-crime practitioner, the key area of focus is cryptocurrencies and the public blockchain networks on which they operate.

The Bitcoin Network was the world's first implementation of blockchain and bitcoin the first use case for the technology. The Bitcoin Network runs on an open-source codebase supported by a distributed network of computers located all over the world. These computers contribute their processing power to run network nodes. Anyone can download open-source software and volunteer to donate their processing power to the Bitcoin Network — and many have done so, with the Bitcoin Network arguably now wielding more total processing power than even the largest cloud providers. But why would so many voluntarily donate their processing power? After all, processing power can cost quite a bit of money in the form of computer hardware and electricity costs. The answer: They do it because they get paid.

Approximately every 10 minutes, all bitcoin transactions transmitted to the global Bitcoin Network are grouped together in what are termed blocks of transactions. And every 10 minutes, the computer nodes that support the Bitcoin Network (also called miners) race to solve complex mathematical algorithms that effectively serve to process and authenticate each transaction block. Through a process encoded into the Bitcoin Network open-source protocol, the first miner to solve the algorithm needed to process a transaction block is rewarded with newly minted bitcoins. The reward is granted to a different miner every 10 minutes for every block verified.

[50] www.coindesk.com/singapore-based-crypto-exchange-dragonex-has-been-hacked, accessed November 18, 2019.
[51] blog.clain.io/binance-hack-2019-deep-dive-into-the-money-laundering/, accessed November 18, 2019.
[52] www.binance.com/en/support/articles/360028031711, accessed November 18, 2019.
[53] cointelegraph.com/news/report-nearly-10-million-in-xrp-stolen-in-gatehub-hack, accessed November 18, 2019.
[54] cointelegraph.com/news/japanese-crypto-exchange-bitpoint-suffers-32-million-hack, accessed November 18, 2019.

After the winning miner has verified the transaction block, all other miners around the world race to double-check the winning miner's work. Once 51% of all computer nodes supporting the network have arrived at the same answer as the winning miner, the block of transactions is time-stamped and linked to the immediately preceding block of transactions through cryptographic hash functions. These hash functions "chain" each block of transactions (hence blockchain) together in a way that makes the dataset effectively immutable.

Once a block has been added to the blockchain, it becomes impossible to alter the data without alerting the entire blockchain. Every node that supports the Bitcoin Network maintains their own independent copy of the full blockchain transaction ledger; the blockchain can be updated only when 51% or more of these nodes agree to accept a new block of transactions. This enables a truly disintermediated network where no single node controls the network and no central authority exists to freeze, alter, or otherwise interfere in bitcoin transactions.

Through this functionality, bitcoins are transferred on the Bitcoin Network directly between senders and recipients in P2P transactions. These P2P transactions are further secured through advanced public-private key cryptography, which secures the virtual bitcoin wallets that store and transfer bitcoin on the network. Every bitcoin wallet has a public key and a private key. The private key is known only to the wallet owner and is needed to access bitcoin held in the wallet. The public key is derived from the private key, the latter of which is used to generate a 34-character string of letters and numbers that serves as the public address of a bitcoin wallet. Every transaction on the Bitcoin Network can be viewed on the publicly available blockchain, which provides a record of every bitcoin transaction that has ever occurred. This record includes (among other things) the public keys of the sender and recipient, a timestamp, and the amount of the transaction.

The Bitcoin Network is available to anyone in the world. Because of the technical features described, the Bitcoin Network has never been hacked and bitcoins have never been counterfeited. Although individual bitcoin wallets have been susceptible to hacking, the network itself has proven to be incredibly resilient. And bitcoin is only the beginning: there are now more than 1,600 different cryptocurrency products available worldwide. Many of these share fundamental technical similarities with bitcoin and most have their own unique characteristics. Among the more common cryptocurrencies besides bitcoin are ether, litecoin, XRP, monero, tether, z-cash, bitcoin cash, EOS, and lumens.

What does this all mean for a forensic accountant? Key takeaways include the following:

- Once initiated, cryptocurrency transactions cannot be disrupted or prevented.
- Cryptocurrencies reside in wallets that can be accessed only with a unique private key.
- Most cryptocurrency transactions are publicly viewable on a blockchain ledger, which provides the public key addresses, amounts, and timestamp associated with each transaction.
- Cryptocurrencies can be accessed and transacted by anyone with an internet connection and an appropriate hardware device.

The Cryptocurrency Market

Fundamentally, the unique technical features of cryptocurrencies give these new assets value. From a practical standpoint, however, the value of cryptocurrencies is based on the market that has emerged around them. Forensic accountants need to understand the different players in this market and how they interact with one another.

Cryptocurrency miners are, practically speaking, the points at which bitcoin and many other cryptocurrencies enter into existence. As noted earlier, miners are rewarded with newly minted bitcoin in exchange for donating their computer processing power to support the Bitcoin Network. Notably, this newly minted bitcoin will have no prior transactional history on the blockchain. In the Bitcoin Network, mining is now an institutional business; massive data processing centers all over the world devote themselves to winning the reward of newly minted bitcoins that is granted approximately every 10 minutes.

Cryptocurrency administrators replace the role of miners in some instances, where the administrators effectively create new cryptocurrencies of their own making. These are sometimes referred to as "pre-mined" cryptocurrencies. Examples of cryptocurrencies that are created by administrators are Ripple's XRP and ERC20 tokens. Note that ERC20 tokens are created and transferred on the Ethereum Network (not to be confused with ether, the Ethereum Network's "native" cryptocurrency).

Cryptocurrency exchanges are entities that are in the business of engaging with customers to allow them to buy and sell cryptocurrencies in exchange for U.S. dollars and other fiat currencies. Exchanges host customer cryptocurrency accounts, facilitate orders to buy and sell, and profit by charging transaction fees. Exchanges are the primary providers of liquidity in the cryptocurrency markets and they are the primary way that individuals and entities acquire cryptocurrencies and cash out cryptocurrencies for fiat currencies.

Cryptocurrency over-the-counter (OTC) desks have become a growing market in recent years. These are businesses that buy and sell cryptocurrencies for their own account, usually in large volumes. The price volatility of bitcoin appears to have given rise to a number of institutional OTC firms that seek to profit by buying and selling bitcoin at the right times. OTC firms sometimes trade on certain cryptocurrency exchanges but they mostly deal in privately arranged P2P transactions, often with other OTC firms.

Cryptocurrency wallet providers offer services to store cryptocurrencies on behalf of their customers. There are two main types of storage: (i) hot wallets are wallets that are connected to the internet and that often have private keys managed by the wallet provider; (ii) cold wallets store cryptocurrencies offline on external hardware devices. Cold wallets store cryptocurrencies offline on external hardware devices. Although hot wallets are more liquid, cold wallets provide more security from hackers.

Cryptocurrency custody providers provide storage services for cryptocurrencies in large quantities. Their customers typically consist of exchanges, OTC desks, and high-net-worth individuals. Notably, traditional financial institutions, such as Fidelity and Northern Trust, have begun initiatives to provide cryptocurrency custody services.[55]

Cryptocurrency payment processors enable merchants to accept bitcoin and other cryptocurrencies in online and in-person point-of-sale transactions. When a customer wants to pay in cryptocurrency, the payment processor receives the cryptocurrency on the merchant's behalf and then sends the merchant U.S. dollars or fiat currency in an amount that reflects the current exchange rate. The payment processor then either holds the cryptocurrency or trades it for fiat currency through an exchange or OTC desk. In this way, merchants are able to accept cryptocurrency without having to deal with its inherent complexity.

Bitcoin ATMs have been spreading quickly throughout the world, especially in the United States. These are physical kiosks that look like a traditional ATM. The kiosk allows customers to insert cash and receive cryptocurrency. Users also can send their cryptocurrency to the kiosk's public key and receive fiat cash from the machine.

Cryptocurrency mixers or tumblers are anonymizing software tools that take cryptocurrency from one wallet, break up its value into tiny pieces, and send these pieces through thousands of new wallets in "dummy" or "ghost" transactions in an attempt to conceal the owner of the funds. In a related technique, referred to as a coinjoin, multiple parties seek to disguise the source of their cryptocurrency funds by coordinating to send their funds to a single, omnibus wallet and then dispersing the funds to new wallets controlled by the owners. Although these techniques may have some legitimate basis in privacy, in most cases mixers, tumblers, and coinjoins are the cryptocurrency equivalent of the layering transactions criminals use to launder money.

Dark web markets are a critical aspect of the cryptocurrency ecosystem. These are marketplaces accessed on the dark web that sell anything from illegal narcotics, counterfeit products, arms, and even murder for hire. Cryptocurrencies are the payment method of choice on most dark web markets.

[55] www.bloomberg.com/news/articles/2019-01-29/fidelity-is-said-to-plan-march-launch-of-Bitcoin-custody-service, accessed November 18, 2019.

A Brief Introduction to Cryptocurrency Regulation

The legal status of cryptocurrencies is complex and constantly evolving. Although forensic accountants almost always work with outside counsel to navigate legal issues, it is nevertheless helpful for accountants to have a basic understanding of the cryptocurrency regulatory landscape. The U.S. legal environment is complex: four separate U.S. agencies define cryptocurrencies in four different ways. In the eyes of the Financial Crimes Enforcement Network (FinCEN), cryptocurrencies are considered to be "money" for purposes of the Bank Secrecy Act and FinCEN regulations. Meanwhile, the IRS treats cryptocurrencies as "property." On the other hand, the CFTC defines cryptocurrencies as "commodities." Finally, the SEC, while noting that bitcoin and ether are not "securities", has in most cases considered blockchain digital assets to be securities subject to the registration provisions of U.S. securities laws.

With respect to the SEC, it is worthwhile to note that most SEC enforcement actions to date relate to ERC20 tokens that are created, transferred, and stored on the Ethereum Network. The Ethereum Network was modeled in part after the Bitcoin Network and has most of the Bitcoin Network's core functionalities. For example, the native cryptocurrency on the Ethereum Network, ether, is mined in the same way as bitcoin. However, the Ethereum Network has additional functionalities. One of these is the ability for anyone to create their own unique cryptocurrencies, referred to as ERC20 tokens. As indicated, these ERC20 tokens have been the subject of most of the SEC's enforcement actions, as many industry actors created and sold ERC20 tokens in so-called ICOs, which the SEC has, for the most part, viewed as unregistered securities offerings.

The topic of cryptocurrency regulation is ultimately best left for its own separate paper. However, if there is one thing that a forensic accountant should take away about the legal status of cryptocurrencies, it is that these new assets exist in a highly complex legal environment. Further complications arise when a transaction is susceptible to multiple regulatory regimes — for example when the underlying asset of a swap is considered a commodity and regulated by the CFTC, as well as a security and regulated by the SEC. Competent legal counsel should be consulted to understand how the law will treat cryptocurrencies in any given set of circumstances.

Blockchain Analytics Tools

As recently as 2019, the SEC publicly sought a tool that would provide blockchain analysis data of the most widely used cryptocurrencies in order to monitor risk, improve compliance, and inform policy with respect to digital assets. One of the required abilities of the tool is a "capability to derive insights from the available data, including attribution data (i.e. to whom a particular address belongs)." The U.S. government has previously worked with multiple blockchain analysis companies, including Chainalysis, Elliptic, and CipherTrace. Most of the blockchain analysis tools still seem to be limited mainly to analyzing bitcoin's blockchain; the SEC is looking for an analysis of "the most widely used blockchain ledgers."[56] Indeed, there are a number of free tools to conduct blockchain forensic analysis, all of which are publicly available. There are also many pay-for-use tools available, such as Google's suite of blockchain analysis tools and analytics platform, BigQuery, which relies on machine learning to analyze transaction history.[57]

[56] www.theblockcrypto.com/linked/10177/the-sec-is-looking-for-a-blockchain-analysis-tool, accessed November 18, 2019.

[57] bravenewcoin.com/insights/google-adds-6-more-cryptos-to-its-blockchain-analysis-suite, accessed November 18, 2019.

Cryptocurrency Considerations and Practice Tips for Forensic Accountants

As cryptocurrencies continue to become a part of mainstream financial culture, fraud schemes involving cryptocurrencies are likely to become more common. Forensic accountants can prepare for these trends by recognizing the challenges and the broad categories where cryptocurrencies are likely to arise, knowing what tools are available to assist in investigations, and understanding how to approach recovery of cryptocurrency assets.

When Using "Traditional" Investigative Methods to "Follow the Money," What Does a Forensic Accountant Look for?

Forensic accountants are often tasked with tracing illicit transactions and the underlying assets, such as in cases to facilitate the recovery of criminal proceeds or to determine if the defendant can pay a court-ordered sum if a judgment is ordered. Practitioners may also search for evidence to show what has happened to property and assets, identifying the proceeds of property and assets, and identifying those who have handled or received property and assets or their proceeds. Generally, the process for tracing illicit transactions requires the following steps:

Collect information.

- This is an ongoing process to collect information about the parties and transactions involved, in which practitioners compile everything known and search public records, collect nonpublic records (if available), and conduct interviews.
- If the subject is an individual, relevant information may include the subject's place of employment, date and place of birth, names and birthdates of close relatives, Social Security number (or other national identification number), last known address, relevant email addresses, educational background, criminal-record search results, asset search including real estate and other real property, and financial account information.
- If able to conduct interviews when seeking information about illicit transactions, the forensic accountant asks interviewees for records, documents, and other information that might identify, trace, and locate assets. Questions may seek information about the subject's employment and sources of income, real and personal property, financial needs, investments, business dealings, debts, and lifestyle.

Profile the subject.

- Create a personal profile of the subject with the collected information that shows the subject's financial condition. The profile is essentially a financial statement or statement of net worth for the subject.
- Review information for leads and prioritize those leads.
- Review with an eye toward the names of any attorneys, corporate officers, lending officers, and notaries found on any uncovered records. Look for connections between these individuals and the subject.

Trace the illicit transactions.

- Analyze financial records and begin tracing to show what has happened to the property and assets, identifying proceeds, and identifying those who have handled or received property and assets or their proceeds. The objective of this step is to identify and document the movement of assets into and out of accounts.
- Identify connections between people and organizations and the assets at issue and analyze related assets and financial movements.
- Compare and contrast information in the financial profile with known information about suspicious transactions (such as dates, origins, destinations, account holders, banks), group and reconcile the transactions, and identify any gaps in data.
- Look for unexplained changes in the subject's income, expenses, lifestyle, travel patterns, and behavior to assess whether the subject has hidden assets. Such analysis may indicate activities designed to conceal income or income-producing property.
- Consider the following three questions when conducting a tracing analysis:
  - What are the sources of the subject's income, assets, and liabilities?
  - Is there any missing or inconsistent information?
  - Does the subject's lifestyle suggest that there is more than reported income?

There are generally two methods forensic accountants use to trace illicit transactions, direct and indirect, as follows:

With the direct method, the practitioner's efforts include the following:

- Identifies the receipt or disposition of funds or assets by analyzing specific financial transactions.
- Employs direct evidence of the subject's books and records (or financial transactions records belonging to third parties) to analyze the relationship between a subject's receipt and subsequent disposition of funds or assets.
- Traces funds the subject used to purchase assets or make deposits back to the subject's source.
- Examines sources of financial information, which may include tax records, accounting reports, financial statements, bank account records, payroll records, credit reports, court records, mortgage and loan files, and credit card records (substantial additional detail underlies the methods a forensic accountant might use to analyze various banking records).

With the indirect method, the practitioner's efforts include the following:

- Employs circumstantial evidence to analyze the relationship between a subject's receipt and subsequent disposition of funds or assets.
  - Uses the indirect method if direct evidence is unavailable or if the forensic accountant suspects that the subject's books fail to reflect all income.
  - Examines, for example, any evidence that the subject is living beyond his or her means by summarizing the subject's assets compared to reported income over the relevant period.

Challenges for Accountants Dealing with Cryptocurrency

- To understand how value is exchanged in a given transaction, fraud investigations involving cryptocurrency will require specialized product-and risk-related assistance, much like that required when investigating complex financial products involving traditional fiat currency.
- Most financial institutions lack a business strategy or related controls for cryptocurrencies.
- Matters that involve cryptocurrency have the potential to become more complex international issues, as they often involve high-risk locations abroad where financial controls are weak or nonexistent.
- Identifying the source of funds is more difficult and complex in the cryptocurrency ecosystem, as funds are allowed to move in and out of the banking network, making them harder to trace.
- Determining a cryptocurrency wallet provider/payer, transaction identity, and beneficial owner will be difficult; the lack of traditional identifiers for transactions involving cryptocurrency means that other advanced investigative tools and techniques are required to obtain information on senders and recipients.
- Recovering cryptocurrency assets also will be challenging because very few examples of full recovery exist.
- Criminals commonly obfuscate transaction details in an effort to launder cryptocurrency assets. For example, a big issue facing practitioners is the practice of moving between different cryptocurrencies or the use of mixers or tumblers that effectively break apart cryptocurrency wallets and reassemble them with a view to hiding transactions by including them in a group of other transactions of the same value. The idea is that mixing these transactions would confuse anyone trying to "follow the money."

Additional Scenarios Where Cryptocurrency Is Likely to Arise

In addition to the specific examples mentioned earlier in this article, there are several more general scenarios where forensic accountants are likely to encounter — or risk missing the presence of — cryptocurrency. Some of these scenarios include the following:

- **Probate and divorce proceedings**. Probate and divorce are common situations where individuals often seek to hide assets over which they have custody but not right of ownership. Cryptocurrency is likely to appear more often in these scenarios as an attempted method to sequester assets. Accountants should examine bank records and credit card statements for payments to cryptocurrency exchanges, which may disclose an attempt to convert U.S. dollars into cryptocurrency. Searches of a subject's personal computer or mobile device may provide evidence of installed apps that access cryptocurrency exchanges, wallet services, or market-data resources; these all suggest cryptocurrency use. Notifications from these same market vendors also might appear in personal email accounts.
- **Bribery and corruption**. As cryptocurrencies become more accessible and mainstream, they could very well become a preferred way to make and accept bribes and other corrupt payments. In addition to the methods discussed in the preceding bullet, forensic practitioners should account for the potential presence of cryptocurrency in standard procedures used to investigate violations of the Foreign Corrupt Practices Act, the Anti-Kickback Act, and other common types of institutional investigations. Standard questions about cryptocurrency should be integrated into interviews and questionnaires, employee reporting of cryptocurrency holdings should be required in certain cases, and safeguards related to cryptocurrency should be incorporated into standard anti-corruption policies and procedures.
- **Asset misappropriation, money laundering, and tax evasion.** As forensic accountants know, these three crimes often go hand-in-hand — cryptocurrencies could facilitate all three. Do the subjects have access to cryptocurrency exchanges domiciled in high-risk areas, with weak anti-money-laundering (AML) regimes or substandard know-your-customer (KYC) controls? Are there bitcoin ATMs in the area? Are significant purchases made at merchants that accept bitcoin or other cryptocurrencies? These are the types of questions that forensic practitioners should get into the habit of asking.

Asset Tracing and Recovery

Cryptocurrencies have added a new dimension to asset tracing. Although techniques are still developing, there are now multiple tools accountants can use to assist in tracing cryptocurrencies that reside on public blockchains. A simple internet search for "bitcoin explorer" will retrieve dozens of free tools that will take any given public key and provide information on the amount and time of transactions involving that key as well as information on where the funds came from and where they went. Accountants should familiarize themselves with these resources. Even Google's BigQuery public datasets now include data on Bitcoin and other public blockchains.

More sophisticated tools are available for a fee; these can provide a wealth of additional information, including, in some cases, the entities and persons that control certain public keys. These tools use proprietary heuristic algorithms to take educated mathematical "guesses" of wallets that are owned or controlled by the same person or entity, grouping these wallets into "clusters" of common control. They then integrate data visualization techniques and proprietary intelligence collection procedures to reveal relationships embedded in the blockchain data. Such big-data nodal analysis searches for patterns among hundreds of thousands of transactions; it does this by leveraging all the transaction history in the blockchain ledger to trace activity through each node and to entry and exit points. By doing so, a forensic accountant can seek to identify where currency conversion occurred (as in, through which exchange) and to identify each node's owner. Some of the more sophisticated tools are offered by Chainalysis, Elliptic, Blockchain Intelligence Group, CipherTrace, and Crystal. Forensic practitioners should keep in mind that, in many cases, these tools individually may offer different perspectives into any given cryptocurrency transaction; each unique view is informed by that tool's unique and proprietary algorithms and intelligence gathering and data visualization techniques. For this reason, the use of more than one tool may be warranted.

If cryptocurrency assets can be traced, then there is a chance that they can be recovered. The opportunities to improve actual recovery are real. If a forensic accountant can piece together the right blockchain evidence showing the amounts, times, and public keys of cryptocurrency transactions, the funds may be traceable to a wallet held by a known person or entity. Even better, accountants may demonstrate that cryptocurrency funds were cashed out at a known exchange or other conversion service. This could lead to opportunities to work with law enforcement to attach and seize assets under criminal laws or even to work with legal counsel to recover under theories of civil liability. With such information and data, a forensic examiner may then investigate and legally pursue recovery of assets. This enables forensic accountants to employ industry best practices for search and seizure to recover assets, such as by obtaining forensic images of systems to locate necessary private keys and information related to a transaction.

Attribution, tracking, and asset recovery are inherently more challenging with cryptocurrency. One focus for accountants, however, should be on the point at which currency changes from one form (such as cryptocurrency) to another (such as U.S. dollars). As entities and individuals exchange traditional fiat currency for cryptocurrency and then back again, it must eventually pass through an established financial institution (such as a bank) that is required to have KYC and AML controls. Practitioners can focus on the use of unregulated exchanges, which should be considered red flags, because unregulated exchanges are unlikely to have AML or KYC programs and therefore have a higher risk of illegal activity. In addition to exchanges, other areas where cryptocurrencies intersect with traditional financial transactions can also include payment processors and bitcoin ATMs.

Conclusion

Regardless of the tool a forensic accountant uses, the most effective approach the practitioner can take is to apply traditional forensic methods (such as transaction-pattern analysis and custodian interviews) in combination with more advanced forensic methods to fill in any gaps. For example, a forensic accountant can link blockchain data with public domain information. Such effective use of traditional investigative methods was seen in the Silk Road case. "The Silk Road was created in 2011 by Ross Ulbricht as an online black market for the sale of largely illegal products, mostly drugs, through the exchange of bitcoin". In 2013, the FBI shut down the Silk Road and arrested Ulbricht, thanks largely to an IRS agent's traditional methods. The agent identified Ulbricht via his online alias and connected him to the Silk Road with simple Google searches.[58] The IRS agent used no advanced methods involving blockchain or cryptocurrencies themselves. Even with the availability of sophisticated new investigative tools, the importance of traditional investigative methods should not be overlooked. Cryptocurrencies live online; in many respects, so do their users.

As technologies and fraud schemes change and evolve, so too must the diligent forensic accountant. Although established traditional forensic methodologies will always be relevant, their application to cryptocurrencies and asset tracing will change as more sophisticated analysis tools and analytics platforms are leveraged to support forensic investigations. These methods must be supplemented with new knowledge, tools, and techniques to meet the challenge of new technology. Deep forensic analysis of cryptocurrencies is possible once the challenges of anonymity within the blockchain are addressed; such analysis will likely continue to rely on a potent combination of traditional investigative techniques and new tools rather than a whole new approach. As cryptocurrencies continue to enter the mainstream, forensic accountants will do well to understand them from a holistic perspective that includes the technology, the market and economy, the legal posture, and the practical fraud risks and typologies. By doing so, forensic accountants will play a meaningful role in mitigating the risks and securing the promise of this exciting new chapter in the history of money.

[58] www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html, accessed November 18, 2019.