Criminal acts alleging crypto-related crime expected to rise in 2021

Prepared by:

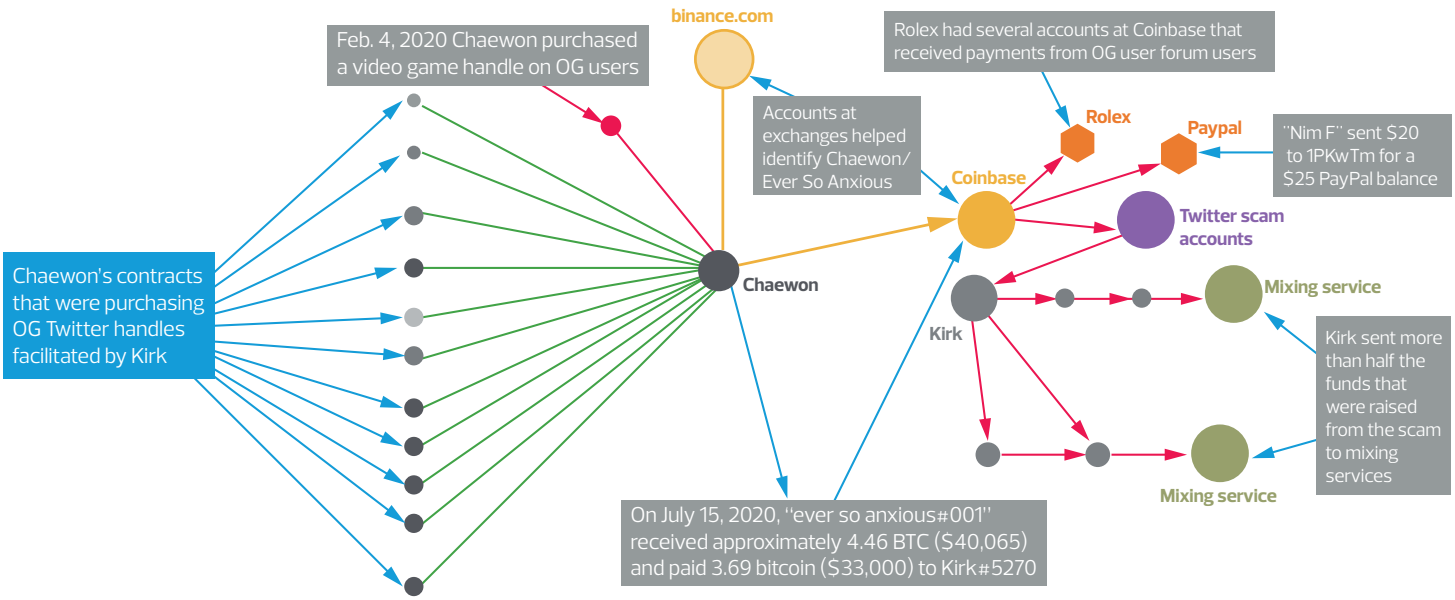
- **RSM authors**: Christopher Ekimoff, Chuck Torrisi, Nichole Devries, Kevin Handt
- **BakerHostetler authors**: Teresa Goody Guillén, Michelle N. Tanney, Audrey van Duyn

February 2021

Introduction

In July 2020, social media giant Twitter was hacked, compromising the accounts of high-profile individuals such as President Barack Obama, President Joe Biden, Jeff Bezos, Elon Musk and Kanye West.[1] The breach led to accounts tweeting a scam to millions of users, resulting in the hackers swindling $140,000 in Bitcoin.[2]

Alarmingly, the hackers were only teenagers, who bypassed Twitter's account security by accessing the platform's internal administration tools.[3] Law enforcement investigated and ultimately caught the hackers using Chainalysis, a blockchain analysis company, to follow a series of transfers between the hackers' digital wallets, as seen in Exhibit 1.[4]



1 Nathaniel Popper, *Twitter Hack May Have Had Another Mastermind: A 16-Year-Old*, NEW YORK TIMES (Sept. 1, 2020), https://www.nytimes.com/2020/09/01/technology/twitter-hack.html.

2 *Id.*

3 *Id.*

4 Chainalysis In Action: How Law Enforcement Used Blockchain Analysis to Follow Funds and Identify the Twitter Hackers (July 31, 2020), https://blog.chainalysis.com/reports/chainalysis-doj-twitter-hack-2020.

Pseudonymous transactions such as these—in which Bitcoin is sent and received using a pseudonym—can ultimately be deciphered through blockchain analysis, revealing the identities of those who misuse the technology for personal gain. However, the ease with which the Twitter scam was perpetrated illustrates how criminal use of cryptocurrency can pose significant threats to public safety and national security. With the increased usage of cryptocurrency, also referred to as digital assets or virtual currency, depending on the regulatory agency, law enforcement and cybersecurity specialists expect a rise in cryptocurrency-related crime in 2021.[5] Accordingly, businesses should implement and maintain robust compliance programs to detect suspicious activity and ensure regulatory compliance.

Background

Cryptocurrency is a digital or virtual medium of exchange that uses cryptography to conduct financial transactions. Most cryptocurrencies are decentralized, meaning there is no central institution that moderates transactions, issues currency or maintains payment ledgers.[6] Instead, each cryptocurrency relies on its own blockchain, a digital payment ledger composed of complex algorithms maintained by a network of peer-to-peer users.[7] Every cryptocurrency transaction is cryptographically recorded on the blockchain, which ensures immutable and accurate tracking of payments and prevents double-spending and counterfeiting.[8]

Generally, cryptocurrency can be exchanged directly between users or through other intermediaries (such as cryptocurrency exchanges).[9] Users have unique public addresses (similar to bank account numbers) and private keys (similar to passwords) through which they can send and receive cryptocurrency.[10] When a cryptocurrency transaction is initiated, it is shared with users on the network associated with the cryptocurrency.[11] "Miners" then validate and aggregate blocks of transactions, which are then added to the blockchain at set intervals.[12] In exchange for their transaction validation services, miners receive payment in the form of transaction fees and a mining reward, a predetermined amount of the cryptocurrency being "mined."[13]

Cryptocurrencies vary in the degree of anonymity and privacy provided to their users. For example, Bitcoin is public, allowing users to view the transactions associated with any Bitcoin address.[14] Other cryptocurrencies, however, make it more difficult to trace their transactions, and may reroute transactions through a randomly generated address for use in that specific transaction.[15]

How cryptocurrency is used

Legitimate uses

Cryptocurrency holds great promise for legitimate use; the technology facilitates transactions by enabling users to transfer cryptocurrency around the world in exchange for goods, services and other sources of value.[16] It minimizes transaction costs, which, in turn, may facilitate "micro-payments" enabling users to sell low-cost goods and services that may not otherwise be profitable due to higher costs associated with traditional credit and debit transactions.[17]

Cryptocurrency also has potential to provide a new entree to markets, including to individuals living in emerging countries without access to banks or other traditional financial institutions.[18] Moreover, individuals living in countries experiencing hyperinflation without access to other foreign currency exchanges may use cryptocurrency to avoid the effects of inflation.[19]

Illegitimate uses

As noted earlier, public safety and national security face numerous threats from criminal activity involving cryptocurrency. Bureau of Investigation Director Christopher Wray recently explained that criminals use cryptocurrency in an attempt to prevent the FBI from tracing money. He noted, for example, that "cybercriminals behind ransomware attacks often use cryptocurrency to try to hide their true identities when acquiring malware and infrastructure, and receiving ransom payments."[20]

---

5 *Cyberthreats to financial organizations in 2021*, KASPERSKY (Nov. 31, 2020), https://securelist.com/cyberthreats-to-financial-organizations-in-2021/99591/.

6 U.S. Dept. of Justice, *Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework 3 (Oct. 8, 2020), available at* https://www.justice.gov/archives/ag/page/file/1326061/download [hereinafter *Cryptocurrency Enforcement Framework*].

7 *Id.* at 3.

8 *Id.* at 4.

9 *Id.* at 3.

10 *Id.*

11 *Id.* at 4.

12 *Id.*

13 *Id.*

14 *Id.*

15 https://www.investopedia.com/terms/m/monero.asp

16 *Cryptocurrency Enforcement Framework*, *supra* note 6, at 5.

17 *Id.*

18 *Id.*

19 *Id.*

20 Press Release, U.S. Dept. of Justice, *Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework (Oct. 8, 2020), available at* https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-publication-cryptocurrency-enforcement-framework [hereinafter Barr Announcement].

On Oct. 8, 2020, the Department of Justice's Cyber-Digital Task Force issued guidance titled "Cryptocurrency Enforcement Framework" to help the industry understand the challenges that cryptocurrencies present and the federal enforcement priorities in this growing space.[21] The framework notes that "cryptocurrency technology plays a role in many of the most significant criminal and national security threats that the United States faces."[22] The DOJ identified three broad categories, explaining that criminals may use cryptocurrency to:[23]

1. **Engage in financial transactions associated with the commission of crimes**: Criminals use cryptocurrency to commit crimes because it can be more difficult to detect and trace than noncryptocurrency. They can therefore freely transfer value across international borders, enabling the commission of a variety of crimes, such as buying and selling illegal drugs or weapons, leasing servers to commit cybercrimes, soliciting funds to support terrorism or facilitating extortion schemes.[24]
2. **Engage in money laundering or conceal otherwise legitimate activity from tax, reporting or other legal requirements**: Criminals can use cryptocurrency to launder their illicit proceeds because value can be transferred across international borders online and pseudonymously.[25] Criminals also use cryptocurrency to avoid paying taxes or economic sanctions.[26]
3. **Commit crimes that directly implicate the cryptocurrency marketplace**: Cryptocurrency can be stolen from exchanges through hacking or the exploitation of security vulnerabilities.[27]

The regulatory regime

Generally, the DOJ has federal jurisdiction over criminal conduct that may involve cryptocurrency and other virtual assets. A number of other U.S. regulatory agencies also have authority to enforce statutes and regulations that apply to virtual asset-related activities.[28] The DOJ has worked and continues to work closely with these agencies to identify and initiate proceedings against individuals who use cryptocurrency for illicit purposes.[29] These agencies include the Securities and Exchange Commission, the Commodity Futures Trading Commission, the Department of the Treasury and its Financial Crimes Enforcement Network, the Office of Foreign Assets Control and the Internal Revenue Service.

FinCEN

Cryptocurrency exchanges are regulated businesses subject to the federal Bank Secrecy Act, which is administered by FinCEN. FinCEN serves as the Financial Intelligence Unit, which is responsible for receiving and analyzing suspicious activity reports, currency transaction reports, and other information regarding money laundering, financing of terrorism and related offenses.[30]

FinCEN has its own civil enforcement authority through which it can impose monetary penalties to supplement, or act as an alternative to, criminal prosecution. This includes regulatory action to address money laundering and terror financing concerns in the cryptocurrency space.[31] Its relationship with the DOJ and other law enforcement agencies generally involves crime prevention and investigatory assistance, but FinCEN also has the ability to share and receive financial intelligence information among foreign counterparts, creating an important international network.[32]

SEC

One of the SEC's main thrusts is to protect investors by maintaining fair, orderly and efficient markets. As part of this mission, the SEC has taken particular interest in the rapid growth of initial coin offerings as a means for new investment opportunities. Unfortunately, this has resulted in certain fraudulent activity by bad actors seeking to take advantage of investors. In response, the SEC issued a report in 2017 cautioning that offers and sales of digital assets by virtual organizations, including through ICOs, may be subject to the requirements of the federal securities laws, including disclosure and registration requirements.[33] The SEC later released a framework to guide the analysis of whether a digital asset is a security as defined under the federal securities laws. This analysis involves application of the *Howey* test to determine if the offer or sale of a digital asset constitutes an investment

---

21 *Cryptocurrency Enforcement Framework*, *supra* note 6, at 1; see also *Barr Announcement*, *supra* note 20.

22 *Cryptocurrency Enforcement Framework*, *supra* note 6, at 1.

23 *Id.* at 5–6.

24 *Id.* at 6–7.

25 *Id.* at 13.

26 *Id.* at 14–15.

27 *Id.* at 15.

28 *Id.* at 22.

29 *Id.*

30 *Id.* at 23.

31 *Id.* at 25.

32 *Id.* at 29.

33 U.S. Securities and Exchange Commission, Release No. 81207: Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO 10 (July 25, 2017), *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf

contract.[34] The SEC framework noted that with respect to a digital asset, the analysis to determine its classification as a security depends on "the circumstances surrounding the digital asset and the manner in which it is offered, sold or resold.[35]"

In October 2019, using its civil enforcement power, the SEC obtained a temporary restraining order against Telegram Group Inc. and its wholly owned subsidiary, TON Issuer Inc., which were alleged to have engaged in an unregistered digital token offering that raised more than $1.7 billion of investor funds.[36] A settlement was entered in June 2020 whereby defendants were ordered to disgorge $1,224 billion in ill-gotten gains and to pay a civil penalty of $18.5 billion.[37] Similarly, the SEC obtained a judgment against Kik Interactive Inc. in October 2020,[38] and filed an action against Ripple Labs Inc. in December 2020,[39] alleging unregistered offerings of digital securities.

The SEC also works in tandem with other agencies, such as the DOJ, to prosecute certain instances of these crimes. For example, in December 2020, the SEC charged Amir Bruno Elmaani (aka Bruno Block) for conducting an illegal securities offering of digital tokens to turn a profit by minting millions of unauthorized tokens for himself at no cost and selling them on the secondary market, causing the value of others' tokens to plummet.[40] A parallel proceeding was brought by the DOJ, charging Mr. Elmaani with tax evasion for evading reporting requirements, filing a false tax return, operating his business and owning assets through pseudonyms and shell companies, obtaining income through nominees, and dealing in gold and cash.[41]

CFTC

The CFTC is vested with statutory authority regarding various aspects and uses of virtual assets. The CFTC retains jurisdiction in cases where a cryptocurrency is the underlying asset in a derivatives contract, or if fraud or manipulation exists involving cryptocurrency traded through the means of interstate commerce.[42]

Generally, the CFTC has taken enforcement action in cases involving:

- Unregistered Bitcoin futures exchanges and fictitious trades on derivatives platforms
- Entities that are legally required to implement anti-money laundering procedures
- Cryptocurrency Ponzi schemes[43]

The CFTC has also issued interpretive guidance on whether "delivery" has occurred in the context of commodity transactions in virtual currencies and warnings about the volatility in spot cryptocurrency markets.

Compliance programs

As cryptocurrency becomes more popular, cryptocurrency-related crime is also expected to increase in 2021, especially as a result of the COVID-19 pandemic. According to the FBI, fraudsters are leveraging increased fear and uncertainty to steal money and launder it through certain offshore or foreign cryptocurrency exchanges.[44] Indeed, in its forecast for 2021, cybersecurity specialist Kaspersky projects that the pandemic will cause "a massive wave of poverty," with "certain economies crashing and local currencies plummeting.[45]" This would likely motivate crime, including cybercrime. A decrease in local currencies would make cryptocurrency theft "a lot more attractive.[46]"

---

34 U.S. SEC, Framework for 'Investment Contract' Analysis of Digital Assets, *available at* https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets. An investment contract is a type of security.

35 *Id.*

36 U.S. SEC, Press Release, "SEC Halts Alleged $1.7 Billion Unregistered Digital Token Offering," U.S. SEC (Oct. 11, 2019), *available at* https://www.sec.gov/news/press-release/2019-212.

37 U.S. SEC, Press Release, "Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges" (June 26, 2019), *available at* https://www.sec.gov/news/press-release/2020-146.

38 U.S. SEC, Press Release, "SEC Obtains Final Judgment Against Kik Interactive For Unregistered Offering" (Oct. 21, 2020), *available at* https://www.sec.gov/news/press-release/2020-262.

39 U.S. SEC, Press Release, "SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering" (Dec. 22, 2020), *available at* https://www.sec.gov/news/press-release/2020-338.

40 U.S. SEC, Litigation Release, No. 24980, "SEC Charges Individual for Self-Minting Scam and Unregistered ICO," U.S. SEC (Dec. 9, 2020), *available at* https://www.sec.gov/litigation/litreleases/2020/lr24980.htm.

41 U.S. Dept. of Justice, Press Release, No. 20-284, "Cryptocurrency Founder "Bruno Block" Charged With Multimillion-Dollar Tax Evasion Scheme" (Dec. 9, 2020), *available at* https://www.justice.gov/usao-sdny/pr/cryptocurrency-founder-bruno-block-charged-multimillion-dollar-tax-evasion-scheme.

42 *Cryptocurrency Enforcement Framework, supra* note 6, at 32.

43 *Id.*

44 Press Release, U.S. Fed. Bureau of Investigation, *FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic* (April 13, 2020), *available at* https://www.fbi.gov/news/pressrel/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic.

45 *Cyberthreats to financial organizations in 2021, supra* note 5.

46 *Id.*

With cybercrime on the rise, implementing and evaluating compliance programs is more important than ever. Recently, several regulatory agencies have published guidance to help financial institutions develop programs to stop cryptocurrency compliance problems before they start:

1. **FinCEN**: In May 2019, FinCEN published new guidance on the application of BSA regulations to money services businesses that engage in transactions involving cryptocurrencies.[47] The FinCEN guidance summarizes these businesses' obligations under the BSA, including a culture of compliance, an adequate AML program, a designated BSA compliance officer, ongoing training and periodic independent review of the AML program.[48]
2. **DOJ**: In June 2020, the Criminal Division of the DOJ issued revised guidance about how it will evaluate corporate compliance programs.[49] The DOJ guidance explains the factors that prosecutors will consider when determining "whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution.[50]"
3. **CFTC**: In September 2020, the CFTC issued new guidance that outlines factors to be considered when evaluating compliance programs in connection with enforcement matters.[51] The CFTC guidance follows the May 2020 update to the CFTC civil monetary penalty guidance.[52]

The BSA's requirements and the threat of monetary penalties give financial institutions strong incentives to implement and maintain robust compliance programs. Businesses may also implement cryptocurrency compliance software, similar to what was used to catch the Twitter hackers.[53] It is important for businesses to review the recent regulatory guidance and implement internal controls that will help them analyze their procedures and detect suspicious activity.

Conclusion

Cryptocurrency presents a new avenue for criminal activity outside traditional financial environments with which companies and regulators are familiar. Research suggests money laundering activities involving cryptocurrency account for a small fraction of all identified cases.[54] However, as bad actors seek to add a layer of obscurity to their illicit activities, money laundering involving cryptocurrency is likely to rise. The unique mechanisms of cryptocurrency—as well as the developing regulatory and enforcement environment—should be monitored going forward to ensure pressing cryptocurrency issues can be considered appropriately.

47 U.S. Dept. of the Treasury, Financial Crimes Enforcement Network, *FinCEN Guidance FIN-2019-G001: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019), *available at* https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20CVC%20Guidance%20FINAL.pdf; see also BakerHostetler, *New FinCEN Guidance for Cryptocurrency and Blockchain Businesses (2019), available at* https://bakerlaw.com/webfiles/IP/2019/Articles/06-06-2019-Jehl-Musiala-Forman-Wasick-FinCENGuidance.pdf.

48 *Id.*

49 U.S. Dept. of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs (June 2020), available at* https://www.justice.gov/criminal-fraud/page/file/937501/download; see also BakerHostetler, *DOJ Makes Important Changes to Its Guidance on Evaluating Compliance Programs (June 9, 2020), available at* https://www.bakerlaw.com/alerts/doj-makes-important-changes-to-its-guidance-on-evaluating-compliance-programs.

50 *Id.*

51 U.S. Commodity Futures Trading Commission, Rel No. 8235-20, *CFTC Issues Guidance on Factors Used in Evaluating Corporate Compliance Programs in Connection with Enforcement Matters* (Sept. 10, 2020), *available at* https://www.cftc.gov/PressRoom/PressReleases/8235-20; see also BakerHostetler, *CFTC Joins Other Federal Agencies in Issuing Guidance to Make Transparent Certain Guideposts When Contemplating an Enforcement Action* (Sept. 24, 2020), *available at* https://www.bakerlaw.com/alerts/cftc-joins-other-federal-agencies-in-issuing-guidance-to-make-transparent-certain-guideposts-when-contemplating-an-enforcement-action#1.

52 *Id.*

53 *Chainalysis In Action, supra* note 4.

54 SWIFT/BAE Systems, *Follow the Money: Understanding the Money Laundering Techniques that Support Large-Scale Cyber Heists (2020), p. 19.*

+1 800 274 3978
rsmus.com

WP-NT-FAS-ALL-0121