United States Government Accountability Office

Report to the Select Committee on Intelligence, U.S. Senate

December 2023

ECONOMIC SANCTIONS

Agency Efforts Help Mitigate Some of the Risks Posed by Digital Assets

Accessible Version

GAO-24-106178

GAO Highlights

Highlights of GAO-24-106178, a report to the Select Committee on Intelligence, U.S. Senate

December 2023

ECONOMIC SANCTIONS

Agency Efforts Help Mitigate Some of the Risks Posed by Digital Assets

Why GAO Did This Study

The increasing use of digital assets may pose challenges for the implementation and enforcement of U.S. sanctions. As of October 2023, the total market capitalization of all cryptocurrencies was about $1.1 trillion, according to one index. The U.S. maintains dozens of economic sanctions programs to serve a range of foreign policy goals. Sanctions may place economic restrictions on entire countries, sectors of countries' economies, individuals, or entities. Such restrictions can include, for example, denying a designated entity access to the U.S. financial system or freezing an entity's assets under U.S. jurisdiction.

GAO was asked to review matters relating to the national security implications of certain types of digital assets. This report describes (1) the risks that digital assets pose to U.S. agencies' ability to implement and enforce U.S. sanctions and factors that may mitigate those risks, and (2) actions U.S. agencies have taken to address the risks that digital assets present with regard to implementing and enforcing U.S. sanctions.

GAO interviewed agency officials and reviewed government reports, guidance, and press releases related to sanctions actions and digital assets. GAO also interviewed 15 stakeholders who GAO selected based on their experiences related to digital assets and sanctions. These stakeholders, many of whom had prior government experience, included researchers, representatives of the digital assets industry, and individuals who provide legal or advisory services on sanctions and digital assets issues.

View GAO-24-106178. For more information, contact Kimberly Gianopoulos at (202) 512-8612 or gianopoulosk@gao.gov.

What GAO Found

Digital assets like Bitcoin and other virtual currencies pose risks to implementing and enforcing U.S. sanctions, but several factors partially mitigate these risks (see table). A key feature of digital assets is that they enable users to rapidly transfer value across countries' borders. Yet many digital assets are recorded on a public ledger, which may enable U.S. agencies and analytics firms to trace transactions and potentially identify illicit actors. However, digital asset owners also may use the anonymizing features of some digital assets or other techniques that obscure their identities in an attempt to evade sanctions.

Selected Risks Digital Assets Pose to Sanctions Implementation and Enforcement and Factors that Help Mitigate Risks

Examples of Risks Digital Assets Pose to Sanctions Implementation and Enforcement	Examples of Factors that Help Mitigate Risks Posed by Digital Assets
• Digital assets provide users some anonymity, and actors may use techniques that obscure their financial transactions. • Actors may take advantage of discrepancies between legal systems and financial reporting requirements in different jurisdictions to avoid consequences of illicit financial activity. • Sanctioned actors may use cybercrime to generate revenue, for example by stealing digital assets.	• Agencies may be able to trace transactions on public blockchains and identify illicit actors. • Use of digital assets as a means of payment is limited and the value of digital assets is highly volatile. • The implementation of global standards may lead to increased compliance with Anti-Money Laundering requirements.

Source: GAO. | GAO-24-106178

Because digital assets currently have relatively limited use as a payment mechanism, sanctioned entities and other illicit actors may seek to convert digital assets to a more traditional currency in jurisdictions with weak regulations and limited sanctions programs. Efforts to increase compliance with global standards may help to mitigate this risk, but uneven implementation from country to country remains a vulnerability that sanctioned actors may exploit.

The risks digital assets pose to sanctions implementation will likely continue to evolve. An increase in the use and acceptance of digital assets could erode the potency of U.S. sanctions and lead to greater sanctions evasion. On the other hand, advancements in capabilities to trace transactions and identify illicit actors could mitigate some sanctions evasion risks.

GAO found that agencies have taken various actions to address the risks posed by digital assets to U.S. sanctions implementation. For example, the Department of the Treasury (Treasury) has sanctioned, and the Department of Justice (DOJ) and other agencies have taken enforcement actions against, entities and individuals for facilitating sanctions evasion with digital assets. Treasury, the Department of State, DOJ, and other agencies also work with international organizations and foreign partners to build investigative capacity and implement anti-money laundering standards to protect the global financial system from digital assets being used for illicit purposes, including sanctions evasion.

Contents

Abbreviations:

AML	Anti-Money Laundering
BSA	Bank Secrecy Act
CBDC	Central Bank Digital Currency
CRS	Congressional Research Service
DeFi	Decentralized Finance
DHS	Department of Homeland Security
DOJ	Department of Justice
EO	Executive Order
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
IMF	International Monetary Fund
IRS-CI	Internal Revenue Service - Criminal Investigation
NFT	Non-Fungible Token
North Korea	Democratic People's Republic of Korea
OFAC	Office of Foreign Assets Control
RUSI	Royal United Services Institute
State	Department of State
TFI	Office of Terrorism and Financial Intelligence
Treasury	Department of the Treasury
VASP	Virtual Asset Service Provider
VPN	Virtual Private Network

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 13, 2023

The Honorable Mark R. Warner
Chairman
The Honorable Marco Rubio
Vice Chairman
Select Committee on Intelligence
United States Senate

To evade U.S. economic sanctions, sanctioned actors—including those from Iran and the Democratic People's Republic of Korea (North Korea)—have used the nearly instantaneous and borderless transactions of digital assets.[1] For example, in April 2023, Treasury's Office of Foreign Assets Control (OFAC) designated two individuals located in China for laundering stolen virtual currency, a type of digital asset, in support of North Korea's weapons programs.[2] Sanctions may place economic restrictions on entire countries, sectors of countries' economies, individuals, or entities. Such restrictions can include denying a designated entity access to the U.S. financial system or freezing an entity's assets under U.S. jurisdiction.

Both individuals and entities may seek to evade U.S. sanctions by using digital assets. Digital assets are representations of value; financial assets and instruments; or claims used to make payments or investments, or to transmit or exchange funds or their equivalents issued or represented in

[1]For purposes of this report, a U.S. economic sanction is any restriction or condition on economic activity with respect to a foreign country or foreign entity that the U.S. government imposes for reasons of foreign policy or national security. Other types of sanctions could include military or diplomatic sanctions. In this report, we generally refer to U.S. economic sanctions as "sanctions." In this report, the term entity may also include individuals.

[2]See 88 Fed. Reg. 25736. The Department of the Treasury's Office of Foreign Assets Control publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs" and the list is known as the Specially Designated Nationals and Blocked Persons List (SDN List). SDN assets are blocked, which means that U.S. persons are generally prohibited from dealing with them. In addition to the SDN List, OFAC maintains other sanctions lists such as the Foreign Sanctions Evaders (FSE) list, which includes foreign persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. sanctions.

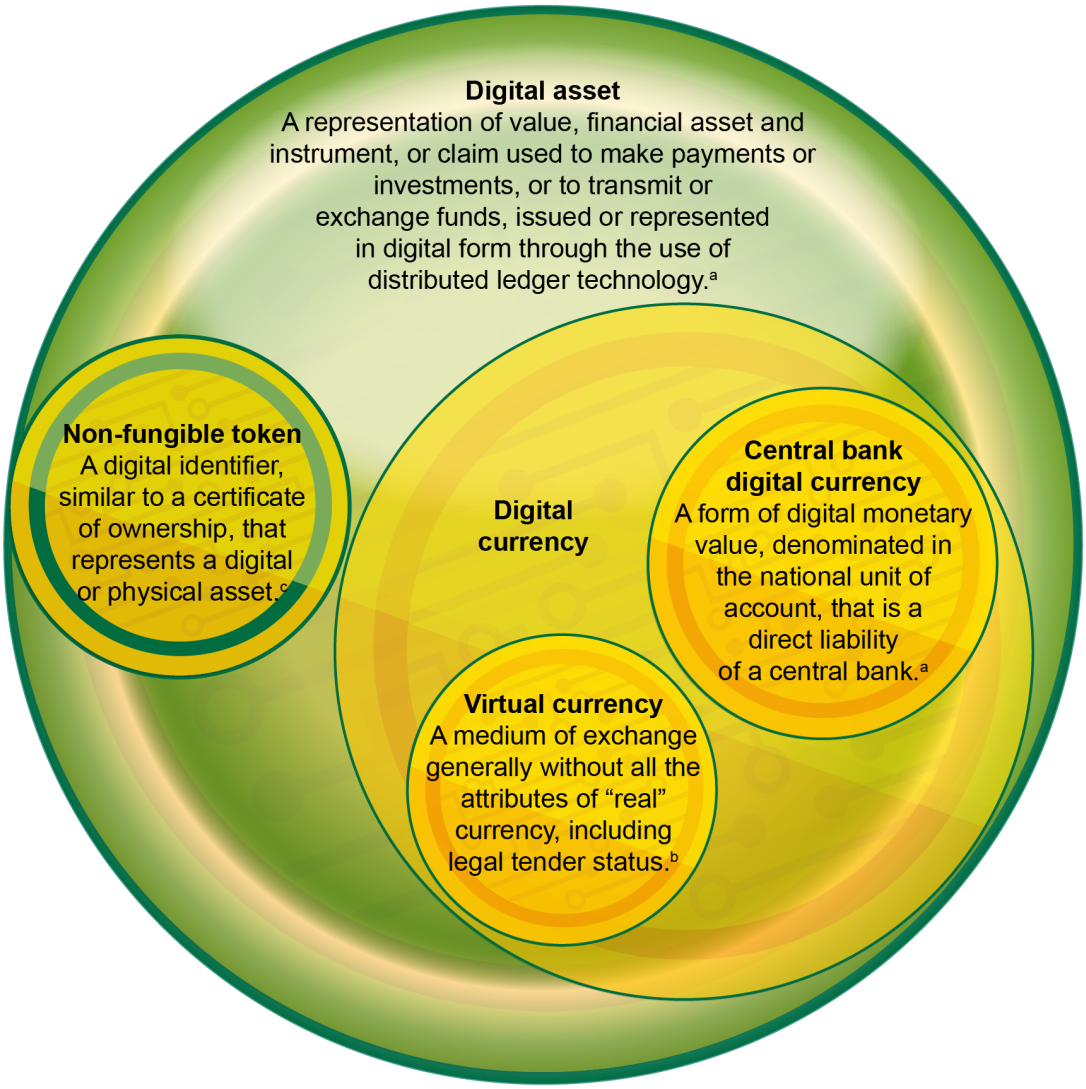
digital form through distributed ledger technology. Distributed ledger technology provides a secure way of conducting and recording transfers without the need for a central authority. Digital assets encompass various assets, including virtual currencies (see fig. 1).[3] A virtual currency is a medium of exchange that can operate like currency in some environments, but generally does not have all the attributes of "real" currency, including legal tender status.[4] Virtual currencies include cryptocurrencies, such as Bitcoin. As of October 2023, the total market capitalization of all cryptocurrencies was about $1.1 trillion, according to one index.[5]

[3]In this report, we will generally refer to digital assets and virtual currencies unless otherwise specified. See Appendix II for additional details and other terms related to digital assets.

[4]The purpose and function of legal tender is for courts to determine whether it is a satisfactory payment for monetary debt. A jurisdiction can define its specific limits of what is legal tender, see e.g. 31 U.S.C. § 5103, but generally it is anything when offered (tendered) and accepted in order to pay off the debt.

[5]According to CoinMarketCap, total market capitalization is the sum of individual crypto assets' market capitalizations. CoinMarketCap determines market capitalization by multiplying the circulating supply of that crypto asset by the reference price of the crypto asset, which uses the distribution of prices reported by an exchange. Data from CoinMarketCap show the total market capitalization of all cryptocurrencies, including stablecoins and tokens. While market capitalization for non-digital assets reflects the total dollar market value of all a firm's outstanding shares, the market capitalization for digital assets may be less tangible. We reviewed data-related documentation but did not assess the accuracy of the underlying data.

Figure 1: Relationship across Some Digital Assets



Source: GAO review of various sources (data); GAO (icons). | GAO-24-106178

Notes: The terms presented in the figure are general definitions adapted from multiple sources. See GAO-24-106178, Appendix II for additional details on these and other terms related to digital assets.

[a]Definitions adapted from Ensuring the Responsible Development of Digital Assets, Exec. Order No. 14067, 87 Fed. Reg. 14,143 (Mar. 9, 2022). Distributed ledger technologies share data across a network that creates a digital ledger of verified transactions or information among network participants, and the data are typically linked using cryptography to maintain the integrity of the ledger and execute other functions, including transfer of ownership or value.

[b]Definition adapted from Financial Crimes Enforcement Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013). The purpose and function of legal tender is for courts to determine whether it is a satisfactory payment for monetary debt. A jurisdiction can define its specific limits of what is legal tender, see e.g.

31 U.S.C. § 5103, but generally it is anything when offered (tendered) and accepted in order to pay off the debt.

[c]Definition adapted from GAO, *Science & Tech Spotlight: Non-Fungible Tokens (NFTs)*, GAO-22-105990 (Washington, D.C.: June 14, 2022).

Digital assets may include anonymizing features and capabilities. As we have previously reported, digital assets also have the potential to reduce the cost of international transfers and increase the speed of transactions.[6] A Department of the Treasury report from April 2023 characterized virtual asset transfers as nearly instantaneous and borderless.[7]

Because of these features and benefits, individuals and entities may attempt to use digital assets to engage in illicit activities and circumvent the U.S. financial system. For example, in March 2022, the President issued an Executive Order that stated that digital assets such as virtual currencies may be used as a tool to circumvent U.S. and foreign economic sanctions regimes and other tools and authorities. The Executive Order directed agencies to address illicit financing risks associated with digital assets.[8] Moreover, members of Congress and others have expressed concerns about Russia using digital assets to evade U.S. imposed sanctions in response to Russia's invasion of Ukraine in 2022.[9]

You asked us to review matters relating to the national security implications of certain types of digital assets. This report examines (1) the risks that digital assets pose to U.S. agencies' ability to implement and enforce U.S. sanctions and factors that may mitigate those risks, and (2) actions that U.S. agencies have taken to address the risks that digital

[6]For a more detailed discussion of the potential benefits and risks of blockchain-related products and services in financial services see GAO, *Blockchain in Finance: Legislative and Regulatory Actions Are Needed to Ensure Comprehensive Oversight of Crypto Assets*, GAO-23-105346 (Washington, D.C.: June 22, 2023).

[7]Department of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance*, (Washington, D.C.: Apr. 2023).

[8]Ensuring the Responsible Development of Digital Assets, Exec. Order No. 14067, 87 Fed. Reg. 14,143 (Mar. 9, 2022).

[9]For example, see *Tightening the Screws on Russia: Smart Sanctions, Economic Statecraft and Next Steps, Hearing before the United States Senate Committee on Banking, Housing, and Urban Affairs*, 117th Cong. (2022) (statement of Senator Elizabeth Warren, Member of the United States Senate Committee on Banking, Housing, and Urban Affairs.)

assets present with regard to implementing and enforcing U.S. sanctions.[10]

To examine the risks that digital assets pose to U.S. agencies' ability to implement and enforce U.S. economic sanctions and factors that may mitigate those risks, we conducted interviews with officials from the Departments of Homeland Security (DHS), Justice (DOJ), State (State), and the Treasury (Treasury), as well as Internal Revenue Service-Criminal Investigation (IRS-CI). We also interviewed 15 stakeholders who were knowledgeable of sanctions implementation and enforcement as well as digital assets.[11] These stakeholders included researchers from academia and think tanks, representatives of the digital assets industry, and individuals who provide legal or advisory services on sanctions and digital assets issues. We identified potential stakeholders by reviewing the results of a literature search of relevant articles and congressional hearings and obtaining recommendations for stakeholders during initial interviews we conducted.

To select the stakeholders, we considered several factors, including whether the potential stakeholder had professional or technical experience that would allow them to comment knowledgeably on issues related to sanctions implementation and enforcement and digital assets and whether the stakeholder had prior government experience. While the views of the 15 stakeholders we interviewed are not generalizable to all stakeholders, they provide illustrative examples on the risks that digital assets pose to U.S. agencies' abilities to implement and enforce sanctions and factors that may mitigate those risks.

To corroborate information from stakeholder interviews and provide additional context, we reviewed reports from government agencies, firms in the digital assets industry, an international organization, and think tanks as well as scholarly papers related to the risks that digital assets pose to U.S. agencies' abilities to implement and enforce sanctions and factors that may mitigate those risks. While our focus was on sanctions evasion risks, we also considered some broader illicit finance risks, if such risks also apply to sanctions evasion.

[10]We also have ongoing work examining the intelligence community's efforts to address challenges and opportunities associated with cryptocurrency.

[11]See Appendix III for the names and affiliations of the stakeholders we interviewed.

To examine the actions U.S. agencies have taken to address the risks that digital assets present with regard to implementing and enforcing U.S. sanctions, we reviewed government press releases, reports, and other documents. We also conducted interviews with officials from Treasury, DOJ, State, DHS, and IRS-CI. See Appendix I for additional information on our scope and methodology.

We conducted this performance audit from July 2022 to December 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Economic Sanctions Overview

Economic sanctions provide a range of tools that the U.S. may use to seek to alter or deter the behavior of a foreign government, individual, or entity to advance U.S. national security or foreign policy objectives. For example, sanctions may be used in response to human rights abuses, narcotics trafficking, terrorism, weapons proliferation, or occupation of a foreign country. Economic sanctions may include:

- blocking property and interests in property subject to U.S. jurisdiction;
- limiting access to the U.S. financial system, including limiting or prohibiting transactions involving U.S. individuals and businesses;
- restricting private and government loans, investments, insurance, and underwriting;
- denying foreign assistance and government procurement contracts; and
- limiting trade, such as a comprehensive embargo or restrictions on particular exports or imports.

The U.S. may implement sanctions unilaterally or may work with other partners—for example, in the United Nations Security Council or with the European Union—to sanction a target multilaterally.

Individuals and entities may attempt to limit the impact of sanctions by engaging in sanctions evasion. Sanctions evasion can take many forms and may involve digital assets.[12]

Agency Roles in Sanctions Implementation and Enforcement

Treasury implements economic sanctions by taking actions that include designating individuals, companies, and entities for the application of sanctions. Such actions may include blocking U.S.-based assets, prohibiting financial transactions, and restricting access to U.S. financial services.

- Treasury's primary office for sanctions implementation and enforcement is the **Office of Foreign Assets Control (OFAC).** OFAC administers and enforces economic sanctions based on U.S. foreign policy and national security objectives. OFAC acts under presidential national emergency powers as well as authority granted by specific legislation to restrict U.S. persons from engaging with specified persons and jurisdictions.[13] Restrictions can require rejecting transactions and blocking assets. OFAC enforces sanctions by conducting civil investigations of potential sanctions violators and working with law enforcement agencies.
- Treasury's **Financial Crimes Enforcement Network (FinCEN)** administers the Bank Secrecy Act (BSA) and implementing anti-money laundering (AML) regulations and enforces compliance with the BSA.[14] In addition, FinCEN monitors and analyzes financial information on threats, producing intelligence reports that may identify

[12]According to a global sanctions evasion advisory issued by Treasury, ministries from other countries, and the European Commission, types of sanctions evasion include the use of real estate to hold value and adoption of complex ownership structures to avoid identification.

[13]The President may use authorities granted in the National Emergencies Act, Pub. L. No. 94-412, 90 Stat. 1255 (Sept. 14, 1976) (codified as amended at 50 U.S.C. ch. 34) and the International Emergency Economic Powers Act, Pub. L. No. 95-223, title II, 91 Stat. 1626 (Dec. 28, 1977) (codified as amended at 50 U.S.C. §§ 1701 *et seq*.), among other authorities, to issue executive orders authorizing sanctions.

[14]The Currency and Foreign Transactions Reporting Act, its amendments, and other statutes relating to the subject matter of the act have come to be referred to as the Bank Secrecy Act. These statutes are codified as amended in scattered sections of Titles 12 and 31 of the U.S. Code. Regulations implementing the Bank Secrecy Act primarily appear in 31 C.F.R. Ch. X.

targets for designation and sanctions violators and issuing guidance to help U.S. financial actors stay compliant with applicable regulations.

- Treasury's **Office of Terrorist Financing and Financial Crimes** formulates and coordinates comprehensive anti-money laundering policies and strategies, among others. That office also leads the U.S. delegation to the Financial Action Task Force (FATF), an independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and financing weapons of mass destruction.

State develops and implements certain foreign-policy related sanctions and coordinates with Treasury on the implementation of other sanctions authorities to ensure sanctions, including those related to digital assets, are used in a manner that advances broader U.S. foreign policy objectives, according to State officials. Specifically, State takes various actions, including restricting visas and foreign aid, implementing rewards programs as well as downgrading or suspending diplomatic relationships, among others. In addition, State collaborates with Treasury to take actions to improve global AML regulations and enforcement, according to agency officials.

DOJ investigates and prosecutes violations of sanctions and export laws and provides legal reviews of sanctions' designations. Within DOJ, the Federal Bureau of Investigation (FBI) examines digital assets across its investigative programs. FBI has a Virtual Assets Unit, a specialized team that provides its expertise across the FBI in support of investigations in which virtual assets are illicitly used, according to agency officials.

Other DOJ components' work also involves digital assets. For example, DOJ's Criminal Division's Money Laundering and Asset Recovery Section and Computer Crime and Intellectual Property Section house the Digital Currency Initiative and the National Cryptocurrency Enforcement Team. DOJ also established the Virtual Currency Initiative to focus on strengthening international law enforcement efforts to combat the illicit use of digital assets, according to agency officials.

DHS and the IRS-CI have played significant roles in digital assets-related investigations, according to a DOJ report.[15] In addition, IRS-CI has units that may be involved in the enforcement of sanctions.

Other U.S. agencies are involved in digital asset regulations but have limited roles related to sanctions implementation. We therefore excluded these agencies from the scope of this review. These agencies include Consumer Financial Protection Bureau, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, the Board of Governors of the Federal Reserve, Commodity Futures Trading Commission, National Credit Union Administration, and Securities and Exchange Commission.[16]

Sanctions and Illicit Finance Regulating Authorities

The National Emergencies Act[17] and **the International Emergency Economic Powers Act**[18] grant the President authority to issue executive orders (EO) authorizing sanctions.[19] For instance, pursuant to the National Emergencies Act and the International Emergency Economic Powers Act, the President has imposed measures upon the declaration of a national emergency. These measures have ranged from comprehensive jurisdiction-based embargoes to targeted restrictions on persons engaged in specified activities.

OFAC publishes a list of individuals and entities, known as the Specially Designated Nationals and Blocked Persons List, whose assets subject to

[15]Department of Justice, Report of the Attorney General, *The Role Of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related To Digital Assets*, (Washington, D.C.: Sept. 6, 2022). DHS offices contributing to digital assets-related investigations include Homeland Security Investigations (HSI) and United States Secret Service.

[16]We previously recommended each of these financial regulators establish a (or adapt an existing) coordination mechanism to identify and address blockchain-related risks. One regulator agreed with the recommendation and the others neither agreed nor disagreed. We also previously recommended that Congress consider legislation for federal oversight of some digital assets and related spot markets. See GAO-23-105346. As of October 20, 2023, these recommendations have not been implemented.

[17]Pub. L. No. 94-412, 90 Stat. 1255 (Sept. 14, 1976) (codified as amended at 50 U.S.C. ch. 34).

[18]Pub. L. No. 95-223, title II, 91 Stat. 1626 (Dec. 28, 1977) (codified as amended at 50 U.S.C. §§ 1701 *et seq.*).

[19]Sanctions may also be specifically authorized by statute.

U.S. jurisdiction are blocked and with which U.S. persons are generally prohibited from dealing. The addition of an individual, group, or entity to this list is referred to as a sanctions designation.

In October 2021, OFAC issued guidance to the virtual currency industry. OFAC's guidance stated that sanctions compliance obligations apply equally to transactions involving virtual currency and those involving traditional fiat currencies (also known as government-issued legal tender).[20]

The BSA and its implementing regulations generally require covered financial institutions and other businesses to help detect and prevent money laundering and terrorist financing through various reporting, recordkeeping, and other obligations. For instance, among other obligations, regulations implementing the BSA require that banks and other covered financial institutions identify and report suspicious activity[21] and have customer identification programs[22] and AML programs.[23]

Section 311 of the USA PATRIOT Act authorizes the Secretary of the Treasury to find that reasonable grounds exist for concluding that one or more foreign jurisdictions, financial institutions, classes of transactions, or types of accounts is of primary money laundering concern.[24] Upon making the finding of primary money laundering concern, Section 311 further grants the Secretary of the Treasury the authority to take certain special

[20]Department of the Treasury, Office of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry* (October 2021).

[21]See e.g., 31 CFR 1020.320.

[22]A customer identification program must include, among other requirements, risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. See e.g., 31 C.F.R. § 1020.220 (for banks).

[23]For instance, an AML program for banks must include: i) A system of internal controls to assure ongoing compliance, ii) Independent testing for compliance to be conducted by bank personnel or by an outside party, iii) Designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance, iv) Training for appropriate personnel, and v) Appropriate risk-based procedures for conducting ongoing customer due diligence to include, but not be limited to: a) Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and b) Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information. 31 C.F.R. § 1020.210.

[24]Pub. L. No. 107-56, §311, 115 Stat. 298 (Oct. 26, 2001) codified as amended at 31 U.S.C. § 5318A *note*. This authority has been delegated to the Director of FinCEN.

measures to protect the U.S. financial system from specific money laundering and terrorist financing risks.[25]

Section 9714(a) of the Combatting Russian Money Laundering Act authorizes the Secretary of the Treasury to determine that reasonable grounds exist for concluding that one or more financial institutions operating outside the U.S., classes of transactions within or involving a jurisdiction outside the U.S., or types of accounts within or involving a jurisdiction outside the U.S. is of primary money laundering concern in connection with Russian illicit finance.[26] Section 9714 authorizes Treasury to use the same special measures as with section 311 of the USA PATRIOT Act as well as a special measure that imposes restrictions on the transmittal of funds by any domestic financial institution.

Digital Asset Transactions on Blockchains

Distributed ledger technologies are a relatively secure way of conducting and recording transfers of digital assets without the need for a central authority.[27] Distributed ledger technologies are “distributed” because multiple participants in a computer network (individuals, businesses, etc.), share and synchronize copies of the ledger. New transactions are generally added in a manner that is cryptographically secured, permanent, and visible to all participants in near real time.

Blockchain refers to a type of distributed ledger technology where data are shared across a network that creates a digital ledger of verified transactions or information among network participants, and the data are typically linked using cryptography to maintain the integrity of the ledger and execute other functions, including transfer of ownership or value.

[25]Such special measures imposed on domestic financial institutions or domestic financial agencies include the prohibition or conditions on the opening or maintaining of correspondent or payable-through accounts as well as recordkeeping and information collection requirements.

[26]Pub. L. No. 116-283, Div. H, Title XCVII, Subtitle B, § 9714, 134 Stat. 4838 (Jan. 1, 2021) codified as amended as a note to 31 U.S.C. § 5318A.

[27]In practice many service providers claiming to be decentralized do in fact have a central authority.

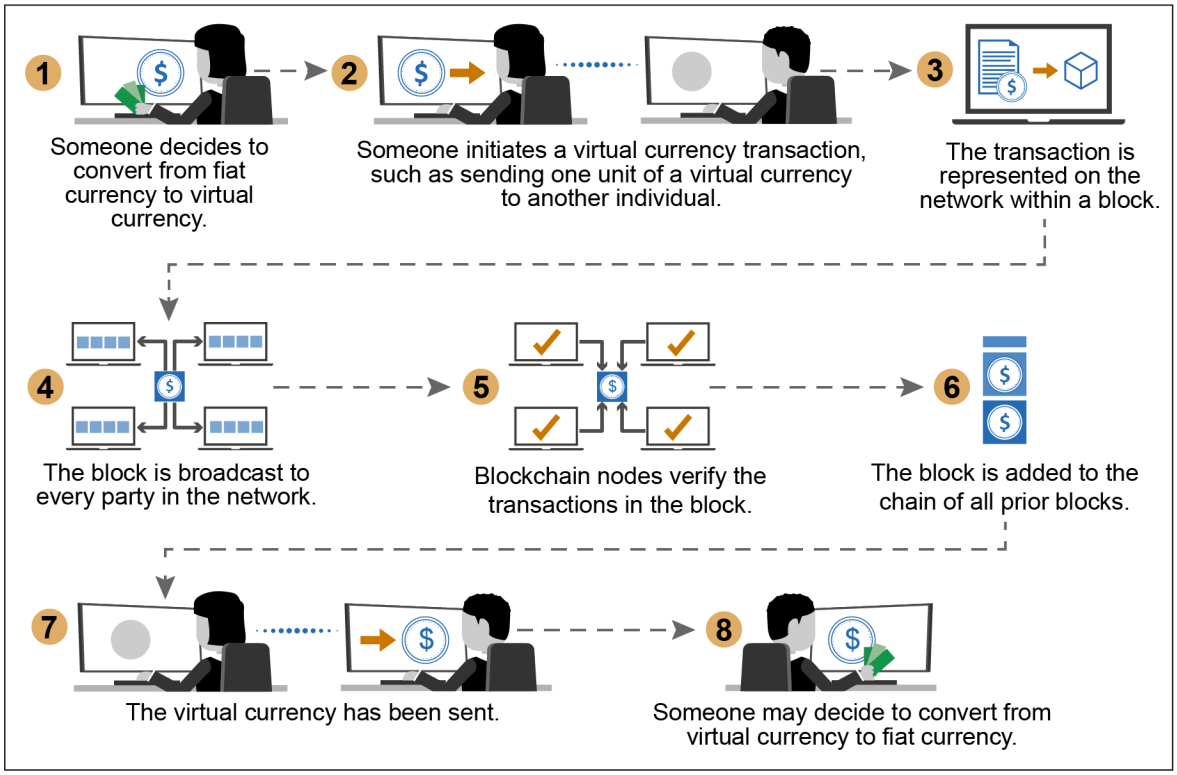
A blockchain functions through a series of computational steps.[28] Transactions are added to a blockchain's ledger in the form of blocks. First, a transaction is sent to a blockchain network. The members of the network (known as nodes) then validate and queue the transaction with other valid transactions. For example, one node will group valid transactions onto a block and broadcast the block to the network. Other nodes will check the validity and authenticity of transactions and will only add the block if its values are valid.

Virtual currencies such as Bitcoin and Ether are examples of digital assets used as a medium of exchange on blockchains. Figure 2 provides a simplified visualization of a virtual currency transaction on a public blockchain, including the conversion between fiat currencies and virtual currencies.[29]

[28]For additional information on blockchain see GAO, *Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges*, GAO-22-104625 (Washington, D.C.: Mar. 23, 2022) and GAO, *Science & Tech Spotlight: Blockchain & Distributed Ledger Technologies*, GAO-19-704SP (Washington, D.C.: Sept. 16, 2019).

[29]In permissionless (public) blockchains, any user, authority, or other observer can view raw transaction data, records, and history associated with a transaction. While popular virtual currencies such as Bitcoin record transactions on public blockchain ledgers, some blockchains have embedded privacy technology that limits what can be viewed on the ledger.

Figure 2: Simplification of a Virtual Currency Transaction



Source: GAO (data), GAO (icons). | GAO-24-106178

Notes: We define fiat currencies as government-issued legal tender. See GAO-24-106178, Appendix II for terms related to digital assets.

Firms That Trace Digital Asset Transactions

Some firms in the digital assets industry—referred to as blockchain analytics companies—provide the ability to potentially identify, trace, and attribute digital asset transactions on certain blockchains. According to a DOJ report, these firms' tools use methods that enable linking and attributing a wide range of transactions to real-world individuals and entities.[30] These tools enhance governments' understanding of complex

[30]Department of Justice, *The Role Of Law Enforcement*.

blockchain relationships as well as their investigations and enforcement capabilities, according to the report.[31]

Digital Assets Pose Sanctions Risks That Can Be Mitigated by Several Factors

Sanctions evasions risks exist as a result of digital assets' features, but several factors can mitigate this threat. Specifically, sanctions evasions risks stem from: the level of anonymity digital assets provide, the use of techniques and services to obscure digital assets transactions, jurisdictional arbitrage, the use of assets with additional anonymity-enhanced features, and the ability to generate funds from cybercrime and digital asset mining activities.

Some factors may partially mitigate these risks. For example, transactions on public blockchains may be traced, implementation of global standards may increase compliance with Anti-Money Laundering (AML) requirements, and use of anonymity-enhanced digital assets may be more challenging than use of other assets. As digital assets are rapidly evolving, future changes could have a significant impact on both the risks they pose to sanctions implementation and enforcement and the factors that help to mitigate these risks.

Digital Assets Afford Some Anonymity, but Transactions May Be Traced

Digital assets have been used to evade sanctions, in part, because they enable some anonymity.[32] Blockchain analytics firm Chainalysis reported that 43 percent of the illicit transaction volume that it estimated in 2022 came from activity associated with sanctioned entities. Chainalysis contextualizes the estimate of volume associated with sanctioned entities by explaining that 2022 was the year in which, according to Chainalysis,

[31]According to IRS-CI officials, blockchain analytics tools may not be effective when identifying real-time movement of funds as compared to when used historically to investigate cases. In addition, not all transactions occur on the blockchain. Blockchain analytics firms' tools would not be able to access such "off-chain" transactions, according to the officials.

[32]Government agency and industry officials sometimes refer to the level of anonymity afforded by digital assets as pseudo anonymity.

OFAC launched some of its most ambitious and difficult-to-enforce crypto sanctions.[33]

When an actor acquires a digital asset such as Bitcoin, it is sent to their public address, and although other actors can see the address and the balance of the address on the blockchain, they cannot see the identity of the asset's owner. Often, the identity of the actor transacting in digital assets is not identified until the actor seeks to convert the digital asset back into fiat currency, according to one stakeholder. Stakeholders we interviewed cited blockchain analytics firms' reports indicating that illicit actors have used the level of anonymity afforded by digital assets to evade sanctions. Stakeholders also told us that U.S. government enforcement actions served as evidence of sanctions evasion through digital assets.[34]

While digital assets can provide actors a level of anonymity in their financial transactions, many are not completely anonymous because their transactions are recorded on a blockchain. As a result, these transactions can be connected to real world identities. Stakeholders and a DOJ report have highlighted how the public, immutable nature of blockchain ledgers facilitates tracking and tracing and can enhance law enforcement's efforts. In contrast, tracking and tracing are not always available for transactions using fiat currency, according to a DOJ report.[35] Blockchain analytics firm TRM Labs' Illicit Crypto Ecosystem Report also highlighted the tracing capabilities blockchains afford and indicated that the transparent and traceable nature of digital asset transactions facilitates

[33]Chainalysis' estimates of the illicit transaction volume associated with cryptocurrency depends on their identification of addresses associated with illicit activity and changes over time as they identify new addresses associated with illicit activity. In addition to considering whether the illicit activity was related to sanctions, Chainalysis identifies illicit activity as being related to child abuse material, ransomware, stolen funds, terrorism financing, scam, cybercriminal administrator, fraud shop, or darknet market. For more information, see Kim Grauer, Eric Jardine, Erin Leosz, and Henry Updegrave, *The 2023 Crypto Crime Report*, Chainalysis (February 2023).

[34]The term stakeholders refers to the group of 15 stakeholders whom we identified as being knowledgeable in digital assets and sanctions and with whom we met. The stakeholders included six researchers from academia and think tanks, five individuals working in the legal or advisory space, and four individuals working in the digital assets industry. For more information on how we selected the stakeholders, see Appendix I.

[35]Department of Justice, *How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets*, (Washington, D.C.: June 6, 2022).

the systematic measurement of illicit activity. Therefore, public blockchains could provide insights into criminal networks and typologies.[36]

The nature of public blockchains also assists U.S. government officials in investigating potential sanctions evasion. Regulators and law enforcement can in some cases take user and transaction information that is viewable to them but with a level of anonymity from a public blockchain and pair it with other pieces of information. This enables them to identify participants in a transaction, notes Treasury's Digital Asset Action Plan.[37] According to stakeholders and agency officials, the U.S. government contracts with blockchain analytics firms to track the data to help identify instances of sanctions evasion and other illicit activity.

According to OFAC, FinCEN, and FBI officials, public ledger records also allow agencies monitoring sanctions compliance or investigating illicit financial activity to conduct "look backs." Look backs are reviews of historical transactions appearing on open source blockchains that potentially allow agencies to discover past illicit activity on blockchains, take action against illicit actors, or generate new investigative leads. Look backs enable agencies to trace related transactions on blockchains to identify a network of other potential illicit actors to consider investigating and imposing additional enforcement actions. According to FinCEN officials, look backs are possible because new information about wallets and transactions is gathered over time. FinCEN officials noted that look backs are not only helpful for agency review, but also important for financial institutions to meet their compliance obligations to detect and report potentially suspicious activity.

Techniques to Obscure Transactions Increase Risk of Sanctions Evasion, but Some Transactions Are Still Traceable

Sanctioned actors and others who facilitate sanctions evasion may use a variety of techniques and technical services to further obscure digital asset transactions and their identities, including the use of Virtual Private

[36]TRM, *Illicit Crypto Ecosystem Report: A Comprehensive Guide to Illicit Finance Risks in Crypto,* (June 2023).

[37]Department of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets*, (Washington, D.C.: Sept. 16, 2022).

Networks (VPN), false identities, mixers and tumblers, chain hopping, peel chains, and proxies:

Virtual Private Networks (VPN). Use of a VPN can allow an actor to mask the true location of an entity executing a digital asset transaction in order to make a transaction appear as if it does not involve an entity in a sanctioned jurisdiction.[38] For example, an actor in a country under comprehensive sanctions, such as Cuba or Iran, could use a VPN to make it appear as if they are operating in a country that is not under sanctions.[39] A 2019 FinCEN advisory identified the use of a VPN to access a virtual currency exchange account as a red flag for illicit activity, including sanctions evasion, of which Virtual Asset Service Providers (VASPs) should be aware.[40]

False identities. Use of false identities involves adopting aliases or stolen identities to mask the true identity of a party to a digital asset transaction. Further, this could mean that even if investigators are able to determine the identity of the digital asset owner, the identity may be false. According to OFAC officials, the use of stolen identities and aliases can complicate investigations into illicit financial activities, including efforts to evade sanctions. Several recent OFAC press releases on digital asset-related sanctions designations include multiple aliases associated with the designated actor.

Mixers and tumblers. Mixers and tumblers are services that mix the virtual currency of several users during transfers to increase anonymity and break the trail of linked transactions (see fig. 3). A DOJ report highlighted that the use of mixing or tumbling services could facilitate sanctions evasion.[41] Similarly, International Monetary Fund's (IMF) 2022 Global Financial Stability Report noted that users could circumvent

[38]Publications by GeoComply, a firm that provides users geolocation information on digital asset transactions, state that there are also other ways that actors can mask the location of transactions, including downloading software to manipulate location and device tampering.

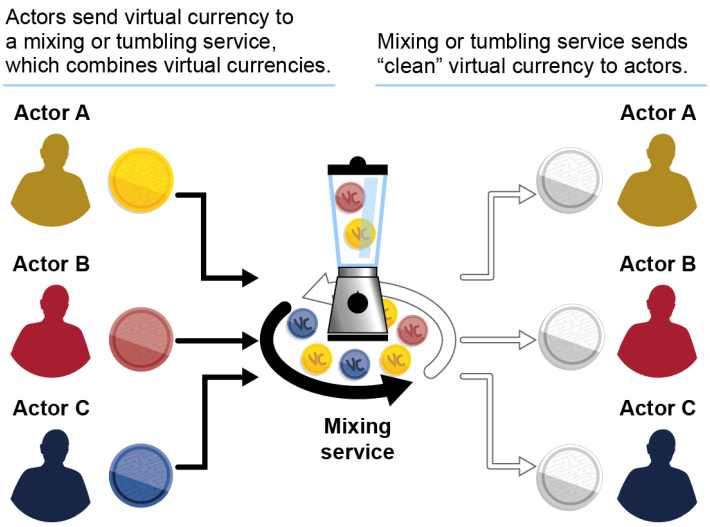
[39]Generally, comprehensive sanctions include broad-based trade restrictions and prohibit commercial activity with an entire country. Comprehensive sanctions can contain exceptions for humanitarian assistance.

[40]The Financial Action Task Force generally identifies a VASP as a person or business that conducts virtual asset operations for, or on behalf of, another person. This includes exchanging virtual currency to fiat currency or exchanging between one or more forms of virtual assets.

[41]Department of Justice, *How To Strengthen International Law Enforcement Cooperation.*

sanctions implementation and other requirements designed to verify identities of the transacting parties through the use of mixers.[42] OFAC made sanctions designations targeting two virtual currency mixers, Tornado Cash and Blender.io, in 2022 for processing millions in virtual currency stolen by North Korean actors, according to Treasury. In October 2023, FinCEN issued a notice of proposed rulemaking in which it found that transactions involving convertible virtual currency mixing are of primary money laundering concern and proposed requiring domestic financial institutions and domestic financial agencies to implement certain recordkeeping and reporting requirements relating to these transactions.[43]

Figure 3: Virtual Currencies Can Be Moved Through Services Designed to Make Transactions Difficult to Trace



Source: GAO analysis of documentation from federal and third-party entities, such as blockchain analytic firms (data), GAO (icons). | GAO-24-106178

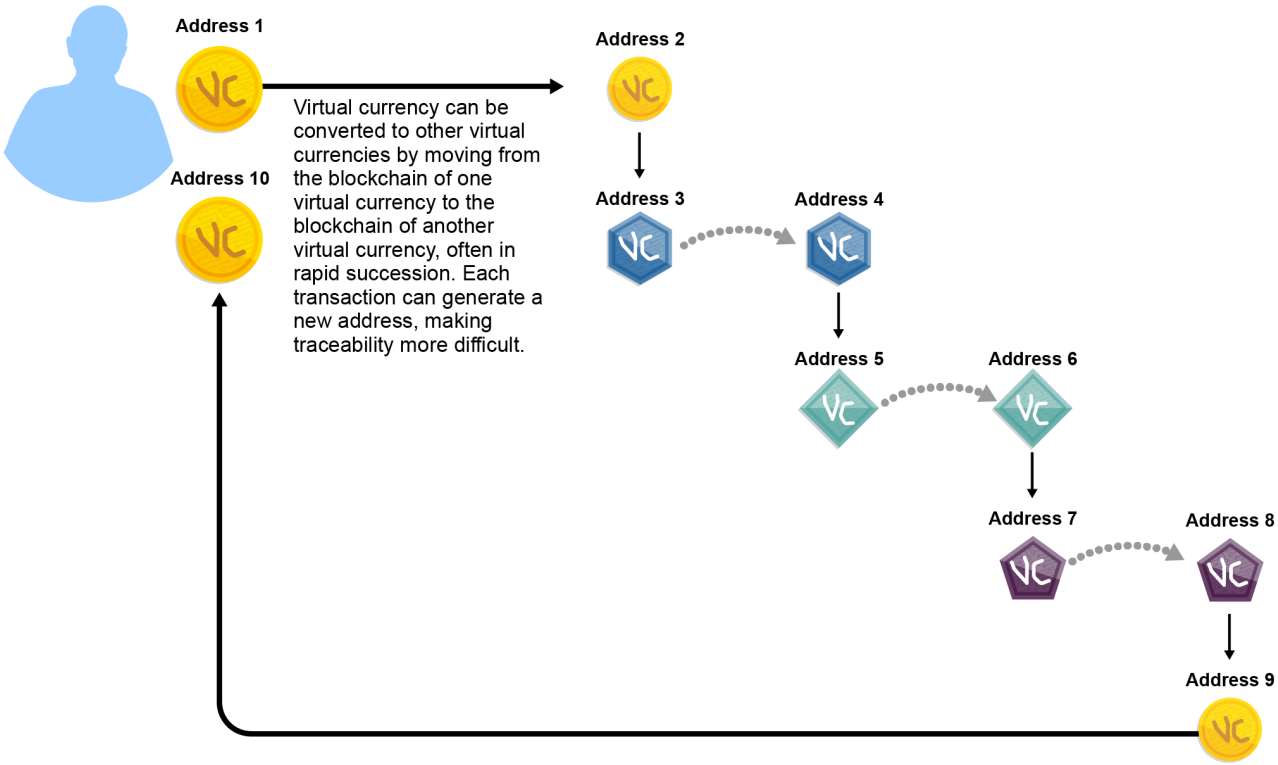
Chain hopping. Chain hopping involves transferring the value of one virtual currency to another virtual currency on a different blockchain, often in rapid succession (see fig. 4). Chain hopping is a method used to obscure transactions, according to a DOJ report and stakeholders. Criminals have reportedly increased chain-hopping to obscure the source and destination of illicit assets as part of their money laundering

[42]International Monetary Fund, *Global Financial Stability Report: Shockwaves from the War in Ukraine Test the Financial System's Resilience*, (Washington, D.C.: April 2022). The IMF report cited analysis by blockchain analytics firm, Chainalysis, in the context of this conclusion.

[43]88 Fed. Reg. 72701.

strategies.[44] For example, in 2020 DOJ announced criminal enforcement actions against two Chinese nationals because they attempted to use chain-hopping to launder stolen virtual currency and evade sanctions.

Figure 4: Moving Virtual Currency from One Address to Another through "Chain Hopping" May Make Transactions Difficult to Trace



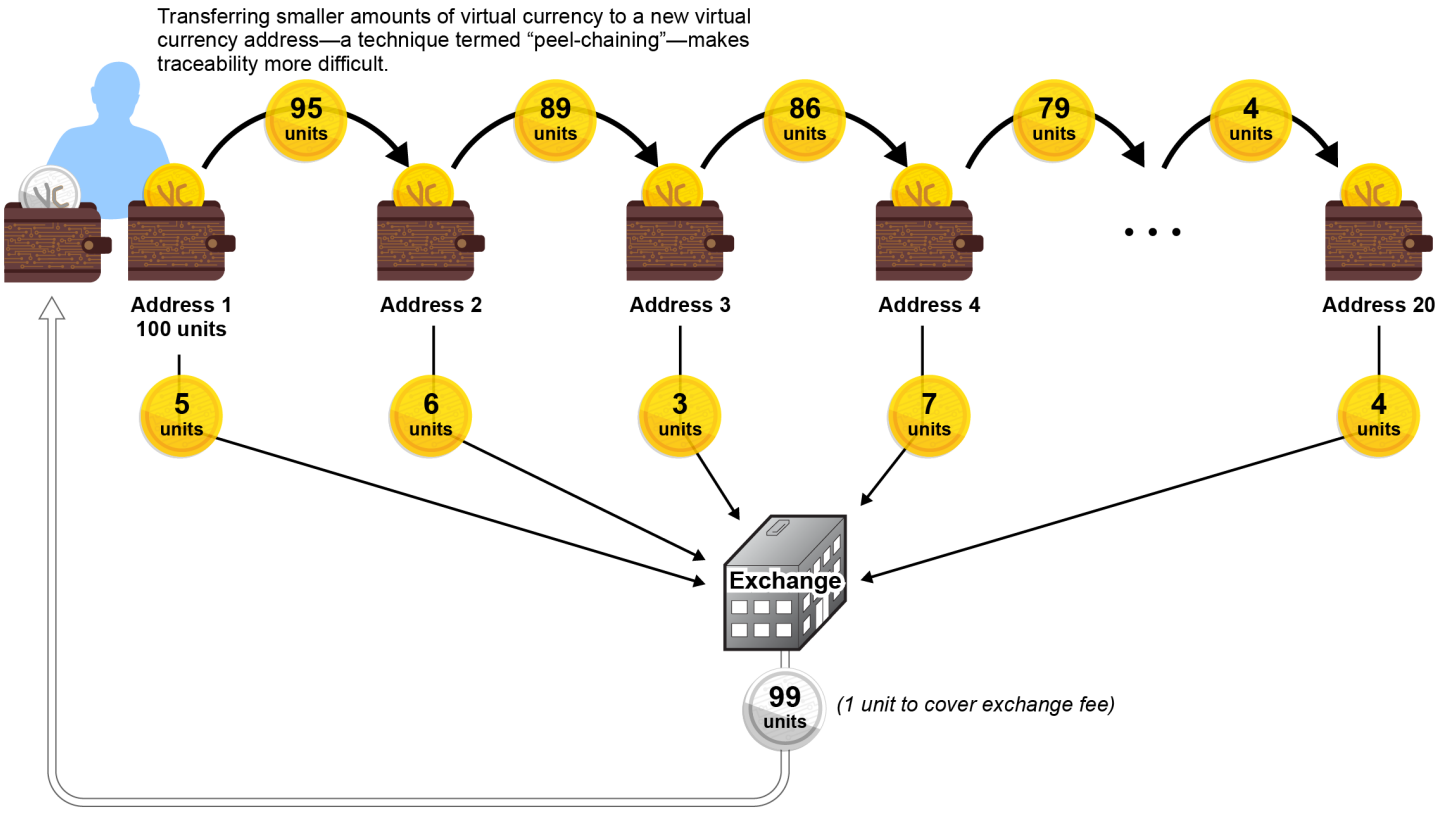
Source: GAO analysis of Attorney General's Cyber Digital Task Force, Cryptocurrency Enforcement Framework (data), GAO (icons). | GAO-24-106178

Peel chains. A peel chain is a technique in which an asset owner moves a large amount of virtual currency located at one virtual currency address through a series of transactions, transferring smaller amounts of virtual currency to a new address each time to conceal the source of the funds (see fig. 5). For example, OFAC made sanctions designations targeting Chinese nationals Tian Yinyin and Li Jiadong in March 2020 after they assisted North Korea in laundering stolen virtual currency from a 2018 cyber hack. Tian and Li attempted to obscure the origins of the funds by transferring the virtual currency among addresses they held. They then sent the obscured funds to four different exchanges through hundreds of

[44]TRM, *Illicit Crypto Ecosystem Report.*

automated transactions. They again moved the stolen virtual currency from the four exchanges through multiple peel chains until they were reconstituted at two new exchanges. This allowed the North Korean co-conspirators to convert stolen virtual currencies to Bitcoin and further conceal their trail. The North Korean actors ultimately converted the Bitcoin to Chinese yuan and prepaid gift cards.

Figure 5: Transferring Progressively Smaller Transaction Amounts from One Virtual Currency Address to Another May Make Transactions Difficult to Trace



Source: GAO analysis of documentation from federal and third-party entities, such as blockchain analytic firms; GAO (icons). | GAO-24-106178

Risks posed by techniques to obscure transactions are mitigated to some extent by the evolving blockchain analytics and other industry tools, according to stakeholders. Blockchain analytics and other tools may enable law enforcement to follow the trail of some illicit transactions. It then may be possible to connect the transaction to a real identity when the actor attempts to convert the digital asset into fiat currency.

Differences in Jurisdictions' Implementation of Legal Systems Raise Risk of Sanctions Evasion, but Efforts to Increase Compliance with Global Standards May Help

Actors may take advantage of discrepancies between legal and regulatory systems in different jurisdictions to avoid consequences of illicit financial activity, also called "jurisdictional arbitrage." Jurisdictional arbitrage provides an opportunity for these actors to evade sanctions, according to a number of U.S. government and international organization reports, as well as other stakeholders and agency officials. Some stakeholders told us that they consider jurisdictional arbitrage to be the most significant risk that digital assets pose to sanctions implementation and enforcement. This is because tracing illicit financial activities and seizing the proceeds from the activities is nearly impossible if actors use VASPs, such as exchanges, in jurisdictions where sanctions and digital asset regulatory programs do not exist, do not meet international standards, or are not effectively implemented. According to OFAC and FinCEN officials, the speed and borderless nature of digital transactions make this an especially significant issue.

Treasury's Digital Asset Action Plan and the 2023 Economic Report of the President list gaps in implementing AML standards across countries, the absence of entities with AML controls in some digital asset transactions, and VASPs that fail to comply with AML and sanctions requirements as key illicit finance risks, including sanctions evasion risks.[45] According to Treasury officials, strong AML protections are the backbone of appropriate controls to identify and prevent illicit activity, including sanctions evasion. TRM Labs reported that over the course of 2022, they tracked over 500 active exchanges they considered high-risk, which include exchanges operating from sanctioned jurisdictions that together transferred tens of billions of dollars in value.[46]

Stakeholders and U.S. agency officials provided potential reasons why some jurisdictions lack adequate regulation and become potential locations for illicit transactions, including the following:

[45]Department of the Treasury, *Action Plan;* The White House, *Economic Report of the President,* (March 2023).

[46]TRM, *Illicit Crypto Ecosystem Report.*

- Some jurisdictions, especially small countries and territories, do not have the capacity or technical expertise to develop regulatory structures that include AML requirements for VASPs in line with international standards, including the requirement that VASPs collect customer information and monitor digital asset transactions. Limited understanding of digital asset-related technology also makes those jurisdictions a potential target for illicit transactions.
- Some jurisdictions may have regulations in place but lack the political will or resources to implement them effectively. Others are in the process of developing or passing legislation or implementing regulations, which takes considerable time, according to Treasury officials.
- Some jurisdictions are uncooperative and refuse to provide U.S. law enforcement with information on illicit transactions passing through VASPs in their jurisdiction even if they may have standards and monitoring mechanisms in place.

The Financial Action Task Force (FATF) has established international standards and works to generate the political will to bring about national legislative and regulatory reforms in jurisdictions around the world.[47] FATF "Recommendations" set out a framework of measures that jurisdictions should implement in order to combat money laundering, terrorist financing, and more.[48] FATF acknowledges that countries have diverse legal, administrative, and operational frameworks as well as different financial systems. Therefore, countries cannot take identical measures to counter these threats. According to FATF, the Recommendations set an international standard that countries should implement through measures adapted to their particular circumstances.[49]

According to FATF, more than 200 jurisdictions have committed to the 40 FATF Recommendations and submit to periodic assessments of their

[47]FATF uses the term "jurisdictions" to include countries, territories (such as the Cayman Islands), and other entities (such as the European Commission).

[48]In October 2023, FATF reported that twelve out of 40 countries, whose questionnaires FATF assessed, noted that they are seeing use of virtual assets for crowdfunding to support terrorism financing, with detection of this activity increasing since 2020. For more information see Financial Action Task Force, *Crowdfunding for Terrorism Financing*, (Paris, France: October 2023).

[49]According to Treasury officials, the FATF Recommendations call for countries to implement targeted financial sanctions regimes to comply with United Nations Security Council resolutions. However, the FATF Recommendations do not call for countries to comply with the sanctions regimes of other countries, including U.S. sanctions.

implementation of the Recommendations. FATF also produces lists referred to as the Black and Grey Lists which identify jurisdictions subject to increased monitoring for insufficiently implemented AML standards.

Increased implementation of FATF standards has helped to strengthen AML compliance in many jurisdictions, which may reduce sanctions evasion through jurisdictional arbitrage, said Treasury and DOJ officials as well as other stakeholders. However, Treasury officials also said that it remains a risk as long as there are jurisdictions unable or unwilling to implement AML policies and procedures that detect and disrupt actors' efforts to use their financial institutions to engage in illicit financial activities.

In 2018, FATF amended its Recommendation 15 to clarify how the FATF standards apply to activities or operations involving virtual assets.[50] According to FATF, cases provided by member countries showed, among other things, criminals using virtual assets to evade financial sanctions. Recommendation 15 specifies that to manage and mitigate the risks emerging from virtual assets, countries should ensure that VASPs are regulated for AML purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures in the FATF Recommendations.

Additionally, FATF's Travel Rule (FATF Recommendation 16), which FATF clarified applied to virtual asset transactions in 2019, calls for countries to require VASPs and other financial institutions to share relevant originator and beneficiary information alongside virtual asset transactions.[51] This information can be useful for financial institutions in conducting sanctions screening and complying with other preventive measures to mitigate criminal and terrorist misuse of the financial system, according to Treasury officials.

As of June 2023, FATF reported that just over one-quarter (25 of 98) of the jurisdictions reviewed for compliance with Recommendation 15 were

[50]FATF uses "virtual assets" to refer to a digital representation of value that can be digitally traded, transferred, or used for payment. It does not include digital representation of fiat currencies.

[51]In the U.S., a BSA rule, which FinCEN often calls the funds "Travel Rule," requires a financial institution and intermediary financial institution to pass on certain information to the next financial institution, in certain funds transmittals involving more than one financial institution. See 31 C.F.R. § 1010.410(f).

deemed to be largely or fully compliant with FATF requirements.[52] FATF characterized jurisdictions' implementation of the FATF standards for virtual assets and VASPs as "relatively poor" and noted that VASP compliance remained behind most other financial sectors. FATF also reported in June 2023 that more than half (73 of 135) of the respondents to a survey of participating jurisdictions indicated they had not taken any steps towards Travel Rule implementation. FATF underscored that it is vital that countries act rapidly to implement the FATF recommendations for VASPs.

Anonymity-Enhanced Assets Increase Risks but Are More Challenging to Use

While popular virtual currencies such as Bitcoin record transactions on public blockchain ledgers, some anonymity-enhanced cryptocurrencies have embedded privacy technology that limits the traceability of their activity. For example, anonymity-enhanced cryptocurrencies, such as Monero and Zcash, can use encryption features that make it more difficult to trace or attribute transactions and can increase the risk of sanctions evasion.

Various reports have indicated these assets increase sanctions evasion risks, and stakeholders said that these assets may be harder to trace. Treasury's Digital Asset Action Plan and the 2023 Economic Report of the President list the use of these assets and other anonymity-enhancing technologies as a key illicit finance risk.[53] Likewise, IMF's 2022 Global Financial Stability Report states that users could circumvent sanctions implementation and other requirements designed to identify transacting parties by using anonymity-enhanced assets.[54]

While anonymity-enhanced assets may increase the risk of sanctions evasion, the challenges in transacting with such assets partially mitigates this risk. Stakeholders said that there is less demand for anonymity-enhanced assets than Bitcoin and that anonymity-enhanced assets can

[52]Financial Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers*, (Paris, France: June 2023).

[53]Department of the Treasury, *Action Plan*; The White House, *Economic Report of the President.*

[54]International Monetary Fund, *Global Financial Stability Report*. The IMF report cited analysis by blockchain analytics firm, Chainalysis, in the context of this conclusion.

be harder to convert into more usable fiat currency. One stakeholder said that some anonymity-enhanced assets can effectively obscure the movement of small amounts of currency, but they lack the liquidity to move large sums.

Digital Assets May Enable Sanctioned Entities to Generate Funds via Cybercrime and Digital Asset Mining Activities

U.S. agency, think tank, and blockchain analytics firms' reports have concluded that cybercrime using digital assets has been used to offset the economic consequences of U.S. sanctions and fund illicit activities. For example, Treasury's Digital Asset Action Plan states that the U.S. government has seen instances of virtual assets being used to fund the activities of rogue regimes, such as the recent thefts by North Korean-affiliated Lazarus Group.[55]

Lazarus Group is tied to the U.S. and UN-designated Reconnaissance General Bureau, North Korea's primary intelligence service, and carries out malicious cyber activities against government, financial, and other institutions as well as critical infrastructure targets. In March 2022, Lazarus Group carried out a virtual asset heist of approximately $620 million from a blockchain project linked to the online game Axie Infinity, according to Treasury. North Korean actors then used mixing services, among other methods, to launder the illicit proceeds to fund the North Korean regime's activities. Theft of virtual currency by nation-state actors such as North Korea may be a means to find alternative funding streams that reduce the impact of sanctions regimes, states a DOJ report.

Stakeholders, reports by an international organization and blockchain analytics firm, and academic papers have also stated that the process cryptocurrencies use to generate new coins and verify new transactions, otherwise known as mining of digital assets, is emerging as a source of revenue generation. Such revenue could assist actors to mitigate the impact of sanctions, although the magnitude is not substantial.[56] Since 2017, Russian virtual currency mining company Bitriver AG and its

[55]Department of the Treasury, *Action Plan*.

[56]Crypto exchange Coinbase has said mining involves vast, decentralized networks of computers around the world that verify and secure blockchains – the virtual ledgers that document cryptocurrency transactions. In return for contributing their processing power, computers on the network and the miners operating them are rewarded with new coins.

subsidiaries, all of which OFAC sanctioned in 2022, have operated a number of servers that mine virtual currency. These sanctioned entities mine virtual currency to generate revenue that Russian entities can attempt to use to mitigate the impact of sanctions.

Stakeholders told us that the sanctioned countries Iran, North Korea, and Russia have been using mining as a way to mitigate the impact of sanctions by generating revenue.[57] Similarly, academic papers have discussed the mining of digital assets to evade sanctions in Iran and Venezuela.[58]

According to an IMF Report, "over time, sanctioned countries could also allocate more resources toward evading sanctions through mining. Mining for energy-intensive blockchains like Bitcoin can allow countries to monetize energy resources, some of which cannot be exported due to sanctions."[59] However, the IMF report notes that the magnitude of mining is not substantial. In particular, the IMF report noted that, as of August 2021, the monthly average of all Bitcoin mining revenues in the prior year

[57]In addition to data mining, sanctioned countries could also engage in staking, according to IRS-CI officials. According to one exchange, staking is a process by which users lock their cryptocurrency to support the operation of a blockchain network, essentially helping to secure and validate transactions on the blockchain in exchange for cryptocurrency or transaction fees. The IRS officials said staking activities could be more challenging to identify than mining because they require less hardware and electricity.

[58]Benedicte Bull and Antulio Rosales, "Into the Shadows: Sanctions, Rentierism, and Economic Informalization in Venezuela." *European Review of Latin American and Caribbean Studies*, no. 109 (2020): pp. 107-133; Christoph Wronka, "Digital Currencies and Economic Sanctions: the Increasing Risk of Sanction Evasion." *Journal of Financial Crime*, vol. 29, no. 4 (2022): pp. 1269-1282.

[59]International Monetary Fund, *Global Financial Stability Report.*

was about $1.4 billion. Of this amount, Russian miners could have captured close to 11 percent, and Iranian miners, 3 percent.[60]

Other Factors Mitigate the Risk of Digital Assets Being Used to Evade Sanctions

According to U.S. agency officials and reports, certain features of digital assets limit their current potential as a sanctions evasion tool. Specifically, digital assets have limited uses as a means of payment, liquidity in digital asset markets is limited, and the value of digital assets is highly volatile.

Limited use as a means of payment. Digital assets' limited acceptance as a form of payment forces illicit actors to convert the digital assets into fiat currency. The limited use as a means of payment may mitigate sanctions evasion risk as it may discourage illicit actors from using digital assets. Should illicit actors need to convert funds, law enforcement may be able to identify those attempting to evade sanctions. According to reports from the Center for a New American Security and Royal United Services Institute (RUSI), criminal actors generally must "cash out" their illicit proceeds. In other words, they must convert virtual currencies into fiat currencies because virtual currencies are not widely accepted as payment for day-to-day goods and services.

As noted in Treasury's Digital Asset Action Plan, the exchange or withdrawal of virtual currency for fiat currency commonly necessary to spend the funds is typically conducted at a VASP. U.S.-based VASPs are required to maintain AML programs and follow sanctions. This may limit

[60]The IMF report cited August 2021 data from the Cambridge Bitcoin Electricity Consumption index. The Cambridge Bitcoin Electricity Index tracks, over time, the geographic distribution of Bitcoin's aggregate computing power of all mining hardware attempting to solve the puzzle at a given point in time. The index performs various data validation techniques. For example, it contrasts reported data to publicly observed data from third-party services. The index uses a sample of geolocational mining facility data, which is collected from several Bitcoin mining collectives. However, it assumes that data provided by participating mining pools constitutes a representative sample and they caveat that the sample may not be sufficiently representative. Furthermore, it assumes that the Internet Protocol addresses of mining facility operators are an accurate indicator of the data's location. However, the index acknowledges that those in the industry in certain locations may use virtual private networks or proxy services to hide their Internet Protocol addresses in order to obfuscate their location.

the ability of actors who seek to evade sanctions to use exchanges that comply with U.S. regulations.

Limited liquidity in digital asset markets. According to U.S. officials and stakeholders, liquidity of digital asset markets is not sufficient to substantially fund government operations, especially for large governments. For example, it is unlikely for a government the size of Russia's to be able to evade sanctions by illicit use of digital assets on a scale that would allow them to bypass western financial systems, according to these sources.

Nevertheless, stakeholders said that sanctions evasion using digital assets might be more feasible for smaller economies similar to North Korea or for designated individuals, such as Russian oligarchs. Treasury's Digital Asset Action Plan and 2022 National Money Laundering Risk Assessment noted that the use of virtual assets for money laundering remains far below that of fiat currency and more traditional methods.[61] However, Treasury officials said that some of that money laundering in virtual assets has been connected to efforts to evade sanctions.

Digital assets are highly volatile. According to organizations focused on illicit financial activity, digital assets may be too volatile to be an attractive store of value.[62] A survey by ACAMS, an international association dedicated to fighting financial crime, and RUSI, a UK think tank, found that respondents generally agreed that the value of cryptocurrencies is

[61]Department of the Treasury, *Action Plan*; Department of the Treasury, *National Money Laundering Risk Assessment*, (Washington, D.C.: Feb. 2022).

[62]Some digital assets are designed to try to maintain a stable value and reduce volatility. If the use of such assets increases, the extent to which the volatility of digital assets mitigates risk of sanctions evasion may decrease. However, our examination of data from CoinMarketCap, suggests that as of October 2023, such assets do not represent a substantial share of the market capitalization of all crypto assets.

too volatile to serve as an effective alternative to fiat currencies.[63] Figure 6 presents data from CoinMarketCap on the market capitalization of all crypto assets from March 2013 through October 2023.[64] Between November 2021 and mid-October 2023, the market capitalization ranged from $788 billion to nearly $3 trillion, reflecting volatility in the market capitalization of crypto assets. In addition, we have previously found and reported that recent turmoil in crypto asset markets resulted in heavy losses to crypto asset holders, and several prominent crypto asset platforms filed for bankruptcy protection.[65]

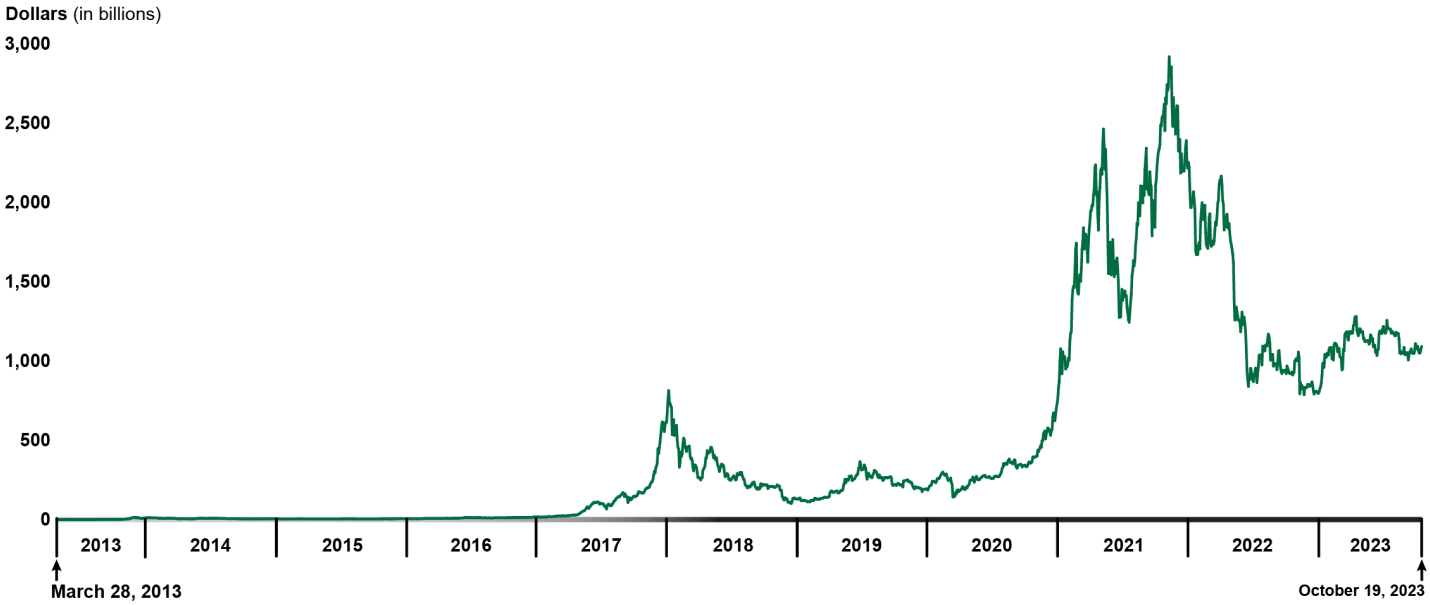
However, the lack of a stable long-term store of value may not deter some illicit actors from digital assets transactions. For example, stakeholders said that some North Korean actors have been willing to accept some losses in order to be able to quickly convert digital assets to fiat currency. This was, in part because they stole the assets and had a limited number of actors willing to accept the risk of entering into transactions with them.

[63]The RUSI-ACAMS Cryptocurrency Risk & Compliance Survey was conducted in collaboration with YouGov, an independent research agency, with the goal of shaping and informing the policy dialogue on cryptocurrency. The survey was distributed to ACAMS members, members of RUSI's Centre for Financial Crime and Security Studies' mailing list, as well as to individual government and cryptocurrency stakeholders between June 3 to July 22, 2020 and resulted in 566 individual responses. ACAMS global membership consists of over 81,000 members in 175 countries and most of the responses came from respondents from North America (32 percent), Europe (23 percent) and Asia (22 percent). Respondents represented a range of organization types, including financial institutions (49 percent), government institutions (24 percent) cryptocurrency industries (10 percent) and other private sector businesses (18 percent). No attempt was made by RUSI or ACAMS to validate the accuracy, completeness or reliability of the survey responses. Due to the reliance on a convenience sample, the results of this survey are not generalizable to the views of all ACAMS members and cryptocurrency stakeholders. However, the results do provide valuable insights about how stakeholders from different sectors who responded to the survey view the use of cryptocurrency and the inherent risks and related compliance controls in the cryptocurrency sector.

[64]CoinMarketCap has data on over 9,000 assets.

[65]For more information see GAO-23-105346.

Figure 6: Total Cryptocurrency Market Capitalization Reflecting Volatility, March 2013–October 2023



Source: GAO analysis of CoinMarketCap.com data. | GAO-24-106178

Notes: According to CoinMarketCap, total market capitalization is the sum of individual crypto assets' market capitalizations. CoinMarketCap determines the capitalizations by multiplying the circulating supply of that crypto asset by the reference price of the crypto asset, which uses the distribution of prices reported by an exchange. Data from CoinMarketCap show the total market capitalization of all cryptocurrencies, including stablecoins and tokens. While market capitalization for non-digital assets reflects the total dollar market value of all of a firm's outstanding shares, the market capitalization for digital assets may be less tangible. We reviewed data-related documentation but did not assess the accuracy of the underlying data.

Risks May Evolve as the Use of Digital Assets Changes

Digital assets are an emerging and rapidly evolving technology. Future changes to digital asset technologies and markets could have a significant impact on the type and magnitude of risks posed by digital assets to sanctions implementation and enforcement. Future changes may also affect the factors that help to mitigate these risks. The risks we cite in this report reflect our observations as of December 2023. Treasury officials stressed the importance of looking ahead and considering possible risks and market changes that could increase the use of digital assets to evade sanctions and limit the reach of sanctions by eroding the global economic power of the U.S. dollar.

Increased Use of Digital Assets and Decentralized Finance Services Could Lead to Greater Risk of Evasion

An increase in the use of digital assets could lead to greater sanctions evasion because illicit actors would not need to risk being caught converting digital assets into fiat currency by a financial institution that has a well-established sanctions compliance program. For example, if acceptance of digital assets as a means of payment increases, people may be able to use digital assets to buy products such as oil or weapons from sanctioned individuals or entities without needing to covert to fiat currency. In addition, greater use of digital assets could also increase liquidity in the digital assets market. The increased liquidity could enhance opportunities for obscuring transactions, including making it more feasible for bigger entities to use digital assets to evade sanctions.

Risk of sanctions evasion could also increase if the use of decentralized finance (DeFi) becomes more widespread. According to Treasury's April 2023 Illicit Finance Risk Assessment of Decentralized Finance, the term DeFi broadly refers to virtual asset protocols and services that purport to allow for some form of automated peer-to-peer transactions, often through the use of self-executing code known as "smart contracts" based on blockchain technology.[66] The assessment noted that DeFi services that have AML and sanctions obligations in the U.S. often do not implement them or other processes to identify customers. The assessment concludes, when DeFi services fail to establish and maintain sufficient AML controls or other processes that could be in line with sanctions compliance measures, criminals are more likely to exploit their services successfully, including to circumvent sanctions.[67]

Moreover, while bank transfers and some digital asset transactions involve financial institutions as intermediaries, it is possible for digital assets to operate like cash without intermediaries by transacting peer-to-peer through unhosted wallets, whereby wallet users can transact without involving any financial services provider. As a result, many of the important obligations of AML regimes that are carried out by financial institutions may not apply, according to a Treasury report. This can limit

[66]This term is frequently used loosely in the virtual asset industry, and often refers to services that are not functionally decentralized.

[67]Department of the Treasury, *Illicit Finance Risk Assessment*.

authorities' collection of and access to information and reduce the effectiveness of preventive measures by financial institutions.[68]

If the use of digital assets increases, the risk of digital asset use to evade sanctions could also increase as a matter of scale—a function of the number and total value of transactions increasing in relation to fiat currency transactions. Treasury officials said that while the majority of commercial transactions are still conducted with fiat currency, the increased adoption of digital assets by the general public could increase opportunities for sanctions evasion to occur. A Congressional Research Service (CRS) report and an academic paper discussed a potential increase in the risk of sanctions evasion if digital assets become more widely issued, adopted, and used—and if they represent a higher share of financial transactions.[69]

An Increase in Digital Asset Use Could Erode the Strength of U.S. Sanctions

Increased use and acceptance of digital assets in the future could contribute to the reduced dominance of the U.S. dollar in international financial markets, potentially eroding the strength of U.S. sanctions and limit their effectiveness in supporting U.S. policy goals. Treasury's Future of Money and Payments report acknowledges that the effectiveness of sanctions tools rests in part on the strength and centrality of the U.S. financial system and currency.[70] The report explains that digital assets could provide new avenues for bad actors to evade U.S. sanctions because the payment systems could be designed to avoid U.S. jurisdiction by not dealing in U.S. dollars, with U.S. persons, or with persons otherwise subject to U.S. jurisdiction. Similarly, an academic paper stated that if digital assets were adopted on a large scale and replaced the U.S. dollar as the medium of exchange for international payments, opportunities for sanctions evasion could increase.[71]

[68]Department of the Treasury, *Action Plan*.

[69]Congressional Research Service, *Digital Currencies: Sanctions Evasion Risks* and Christoph Wronka, "Digital Currencies and Economic Sanctions."

[70]Department of the Treasury, *The Future of Money and Payments*, (Washington, D.C.: Sept. 16, 2022).

[71]Christoph Wronka, "Digital Currencies and Economic Sanctions."

However, Treasury's report and several stakeholders noted that efforts to develop central bank digital currencies (CBDCs) or other digital assets that would challenge the primacy of the U.S. dollar in the international financial system are not sufficiently advanced to pose a risk in the near term. Stakeholders we interviewed noted a hesitancy of other central banks to use a digital currency for cross-border trade in particular. In addition, U.S. agencies have reported there is a long-standing international reliance on the U.S. dollar in particular sectors such as for oil and gas. Furthermore, Treasury's Future of Money and Payments report discusses how the prominence of the dollar reflects factors beyond payment system efficiency that foreign CBDCs may provide.[72]

Nevertheless, countries such as China, Russia, and Venezuela in which sanctioned individuals or entities reside have expressed interest in developing a currency that does not rely on western financial systems, said stakeholders. Such a development could lead to "de-dollarization" and could therefore diminish the effect of U.S. sanctions. See the text box for examples of governments that are exploring development of CBDCs.

[72]These factors include the U.S.' strong economic performance; sound macroeconomic policies and institutions; open, deep, and liquid financial markets; institutional transparency; commitment to a free-floating currency; and strong and predictable legal systems, according to the Treasury report. For more information see Department of the Treasury, *The Future of Money and Payments*, (Washington, D.C.: Sept. 16, 2022).

Chinese, Russian, and Venezuelan Governments Are Exploring Central Bank Digital Currencies to Evade U.S. Sanctions

Governments are exploring the possibility of issuing central bank digital currency (CBDC) to evade sanctions. According to Executive Order 14067, CBDC refers to a form of digital money or monetary value, denominated in the national unit of account that is a direct liability of the central bank.[a] According to the Atlantic Council's CBDC tracker, as of July 2023, 130 countries are exploring a CBDC, and 11 countries have fully launched a digital currency.[b] For example:

- **China's** pilot, which as of July 2023 reached 260 million people, is being tested in over 200 scenarios, some of which include public transit, stimulus payments and e-commerce, according to the Atlantic Council. The Congressional Research Service (CRS) reported that over time a Chinese central bank digital currency and accompanying global payments network could offer China alternatives to the U.S. dollar and workarounds to U.S. sanctions, at least in certain instances.
- **Russian** President Vladimir Putin called for de-dollarization to insulate the Russian economy from existing and potential future U.S. sanctions, according to a CRS report.[c] Russia's central bank is exploring the creation of a CBDC, which could further reduce Russia's reliance on western (and dollar-centered) payments infrastructure.
- **Venezuelan** President Nicol?s Maduro announced in December 2017 plans to launch a new digital currency, the "Petro", allegedly backed by oil reserves and other commodities, according to a CRS report.[d] A Department of the Treasury report cited Venezuela's Petro as an example of a CBDC backed by the state to aid in sanctions evasion.[e]

Source: GAO analysis of various sources. | GAO-24-106178.

[a]Ensuring the Responsible Development of Digital Assets, Exec. Order No.14067, § 9(b), 87 Fed. Reg. 14,143 (Mar. 9, 2022).

[b]Atlantic Council's CBDC Tracker available at https://www.atlanticcouncil.org/cbdctracker/

[c]Congressional Research Service, *De-Dollarization Efforts in China and Russia*, (July 23, 2021)

[d]Congressional Research Service, *Digital Currencies: Sanctions Evasion Risks*, (Feb. 8, 2018)

[e]Department of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets*, (Washington, D.C.: Sept. 16, 2022).

Advancements in Tools and Technologies Could Mitigate Some Sanctions Evasion Risks

Future developments may also help to mitigate the risks posed by digital assets to U.S. sanctions. For example, firms in the digital assets industry are developing tools that would simultaneously confirm individuals' identities while maintaining their privacy. If such tools continue to be developed and are widely adopted by the digital assets industry, some sanction evasion risks could be mitigated. Specifically, stakeholders told us that some new anonymity-enhanced assets contain technologies such as zero knowledge encryption that allow lawful access by law

enforcement or regulators and enable a DeFi service user to confirm that identity has in fact been verified without revealing personal information.

Treasury's Under Secretary for Terrorism and Financial Intelligence said in July 2023 that important developments surrounding tools and technology can help manage AML risk in the DeFi space. In particular, he mentioned zero knowledge proofs and tools that screen user identity information against sanctions lists. At the same time, he noted that many such tools require further technical development and adjustments to meet AML and sanctions implementation requirements. Stakeholders underscored that many users of digital assets value the privacy they can offer and noted that tools such as zero knowledge proofs could allow for privacy without sacrificing the ability to monitor transactions to ensure compliance with AML and sanctions implementation requirements.

Rapidly-evolving blockchain analytics tools could also mitigate the risk of digital asset use to evade sanctions, according to U.S. agency officials and stakeholders. Treasury officials said they rely heavily on their contracts with private sector blockchain analytics firms to help them identify the actors who use digital assets for illicit activities, including sanctions evasion. They said that improvements to data analytics tools and an increasing number of those tools have strengthened their ability to gather evidence for investigations of actors seeking to evade or facilitate the evasion of sanctions, including the ability to consider designating additional actors identified by the tools as parties to transactions with previously-designated actors.

Stakeholders stated that it is a constant battle for regulators and investigators to keep up with the evolving techniques illicit actors use to obscure their digital asset transactions and identities. However, if private sector blockchain analytics firms' tools continue to evolve as quickly as they have in the last few years, they will further help reduce the ability of actors to use digital assets as a means to evade sanctions. In addition, FATF guidance indicates that blockchain analytics can be part of VASPs' enhanced due diligence measures, which may mitigate some of the risks associated with digital assets.[73]

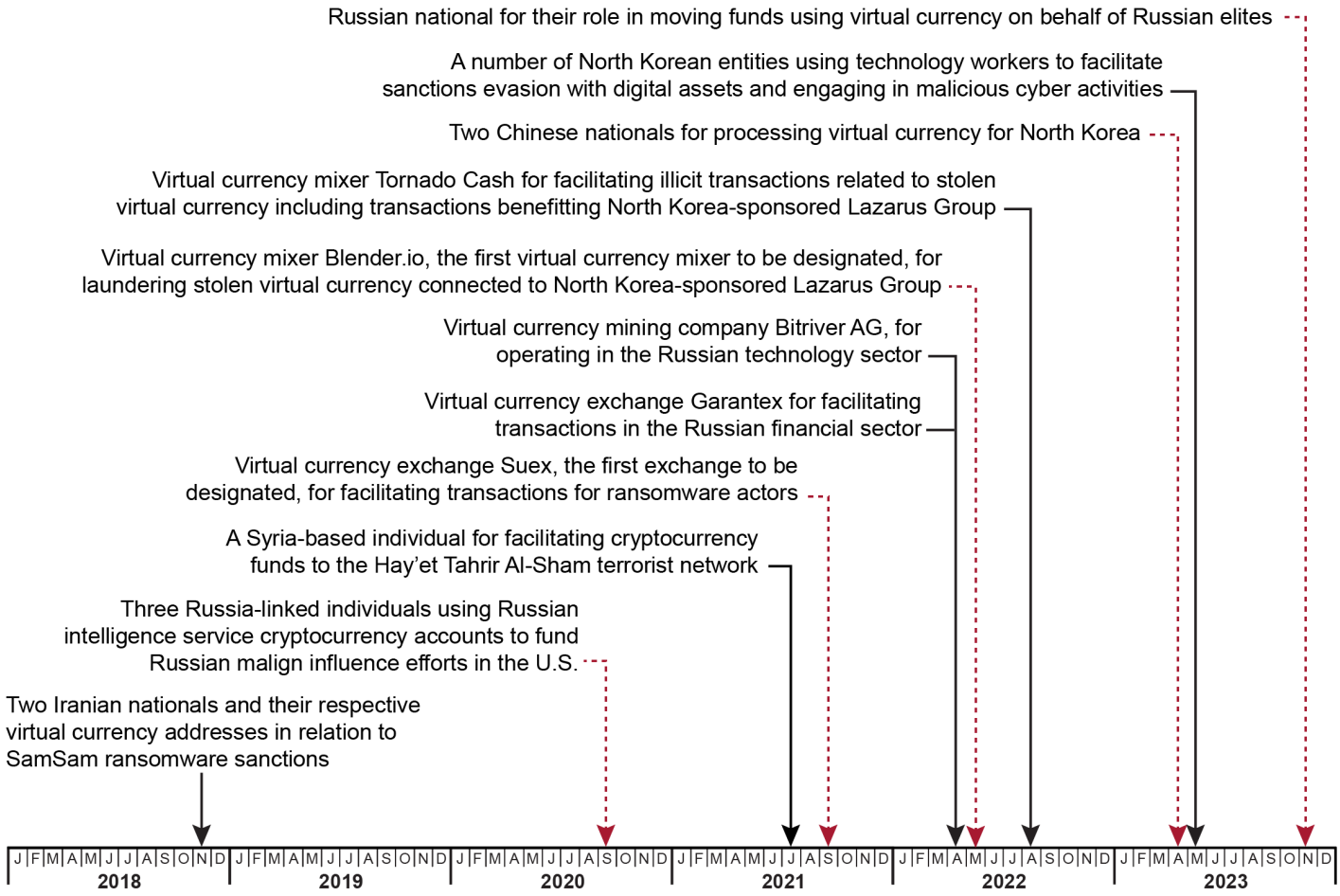
[73]Financial Action Task Force, *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers*, (Paris, France: October 2021).

Agencies Have Taken Actions to Address Certain Risks Digital Assets May Pose to U.S. Sanctions

Agencies have taken actions to address digital asset risks to sanctions implementation and enforcement across five areas: sanctions designations, law enforcement actions, reports and action plans, public messaging, and international efforts.

Sanctions designations and other measures. Treasury's OFAC has designated entities and individuals for facilitating sanctions evasion with digital assets, as shown in figure 7 below.

Figure 7: Examples of Treasury's Office of Foreign Asset Controls' Designations Where Actors Facilitated Sanctions Evasion with Digital Assets



Legend: Democratic People's Republic of Korea = North Korea.

Source: GAO analysis of Department of the Treasury information. | GAO-24-106178

Note: For additional sanctions designations related to digital assets see GAO-24-106178, Appendix IV.

OFAC sanctions designations can minimize sanctions evaders' abilities to access the U.S. financial system and encourage VASPs to comply with U.S. digital asset regulations. When a person or entity, potentially including a VASP, is designated on the Specially Designated Nationals and Blocked Persons List, U.S. persons, including U.S. financial institutions and VASPs, are generally prohibited from engaging in transactions, including virtual currency transactions, with such persons or their property or interests in property. This list entry may include digital

currency addresses known to be associated with the designated person. Stakeholders told us that sanctions designations incentivize entities dealing with digital assets, such as VASPs, to comply with AML requirements and sanctions laws and regulations to avoid being designated themselves.

OFAC has sanctioned various digital asset entities as part of efforts to cut off avenues that actors could use in evading sanctions:

- OFAC designated two virtual currency mixing services, Blender.io and Tornado Cash, in 2022. These two mixing entities were designated for processing millions in stolen virtual currency, which, according to Treasury, were connected to North Korea.
- OFAC designated Russian virtual currency mining company Bitriver AG and 10 of its subsidiaries for operating in the Russian technology sector in April 2022.
- OFAC designated multiple virtual currency exchanges that facilitated illicit transactions including Suex (September 2021), Chatex (November 2021), and Garantex (April 2022). Designations such as Garantex reflect Treasury's efforts to cut off avenues for potential sanctions evasion by Russian actors, according to OFAC.

OFAC has also designated individuals and identified digital asset wallet addresses. As of September 2023, 116 individuals and entities and 542 digital wallet addresses are listed on the Specially Designated Nationals and Blocked Persons List for sanctions evasion reasons related to digital assets, according to OFAC officials. For example:

- The first wallet address identification occurred in November 2018 when OFAC designated two Iranian nationals, and identified their virtual currency wallet addresses, for processing virtual currency connected to ransomware attacks.[74]
- In May 2023, OFAC designated a North Korean individual (along with four North Korean entities) for facilitating the transfer of cryptocurrency generated overseas by North Korean nationals posing as information technology workers to the North Korean government.

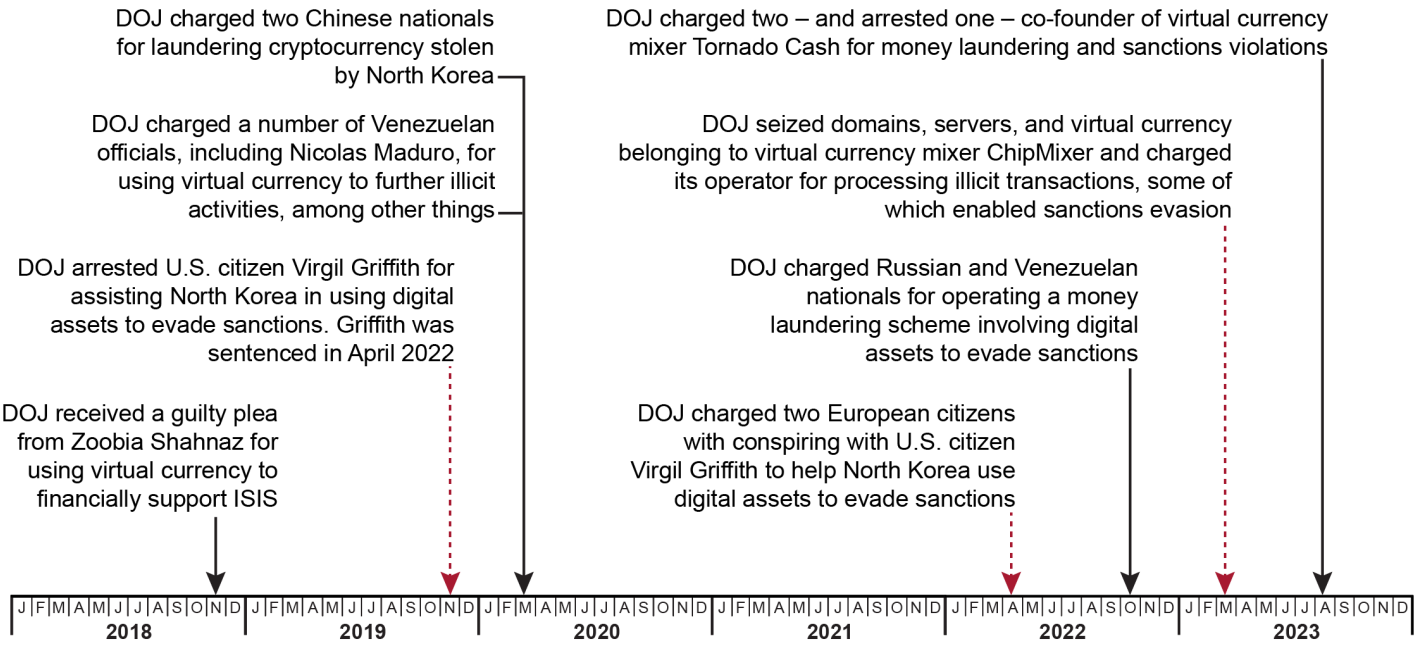
[74]The SamSam ransomware attacks exploited computer network vulnerabilities at corporations, hospitals, universities, and government agencies and demanded ransom paid in the virtual currency Bitcoin for victims to regain access to and control of their computer networks.

- In November 2023, OFAC designated a Russian national for their role in laundering and moving funds using virtual currency on behalf of Russian elites.

Separately from OFAC designations, FinCEN has exercised its authority to combat sanctions evasion involving digital assets. In January 2023, FinCEN issued an order that identified virtual currency exchange Bizlato as a "primary money laundering concern" in connection with Russian illicit finance.[75] This FinCEN order prohibits transmittals of funds involving Bizlato by any U.S.-covered financial institution. The order coincided with DOJ's arrest of Bizlato's founder and efforts to seize Bizlato's cryptocurrency and digital infrastructure.

Enforcement actions. Agencies have taken enforcement actions against entities and individuals for using digital assets to evade sanctions, as shown in figure 8 below.

Figure 8: Examples of Law Enforcement Actions against Those Facilitating Sanctions Evasion with Digital Assets



Legend: Democratic People's Republic of Korea = North Korea; Department of Justice = DOJ.

Source: GAO analysis of Department of Justice information. | GAO-24-106178

[75]This was the first FinCEN order issued under section 9714(a) of the Combatting Russian Money Laundering Act, as amended.

Note: The actions included in this figure do not reflect ongoing cases.

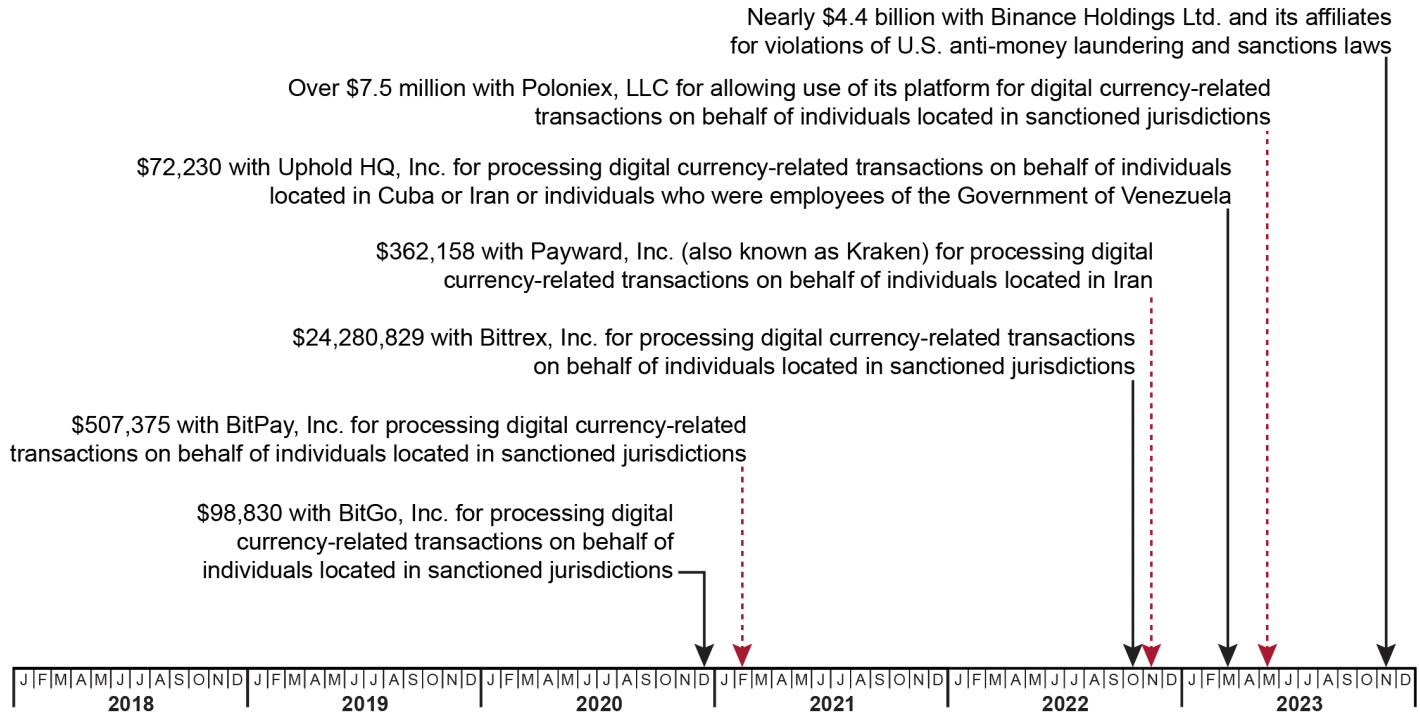
Enforcement actions have targeted individuals who used digital assets to enable sanctions evasion. These actions can take place in the form of prosecutions through the U.S. federal judicial process. Prosecution examples include:

- In April 2022, U.S. citizen Virgil Griffith was sentenced to 63 months in prison and fined $100,000 after pleading guilty to violating U.S. sanctions on North Korea in connection with Griffith's provision of technical information on digital assets to assist North Korea in evading sanctions.
- In October 2022, DOJ charged five Russian and two Venezuelan nationals for using cryptocurrency to evade sanctions related to obtaining Venezuelan oil and U.S. military technology.

Other enforcement actions that targeted digital asset entities involved in sanctions evasion efforts have resulted in digital asset seizures and taking a digital asset entity offline. For example, in March 2023, a DOJ investigation led to the joint U.S. and German seizure of domains, servers, and $46 million in virtual currency from virtual currency mixer ChipMixer and charges against ChipMixer's founder. ChipMixer was responsible for laundering virtual currencies connected to North Korea sanctions evasion efforts, according to DOJ.

Agency enforcement actions have also taken the form of financial settlements with digital asset entities that engaged in apparent violations of U.S. sanctions, as shown in figure 9.

Figure 9: Treasury Announcements of Sanctions-Related Financial Settlements with Entities in the Digital Asset Industry



Source: GAO analysis of Department of the Treasury information. | GAO-24-106178

Note: These financial settlements were with entities that Treasury determined had engaged in apparent violations involving the various actions listed.

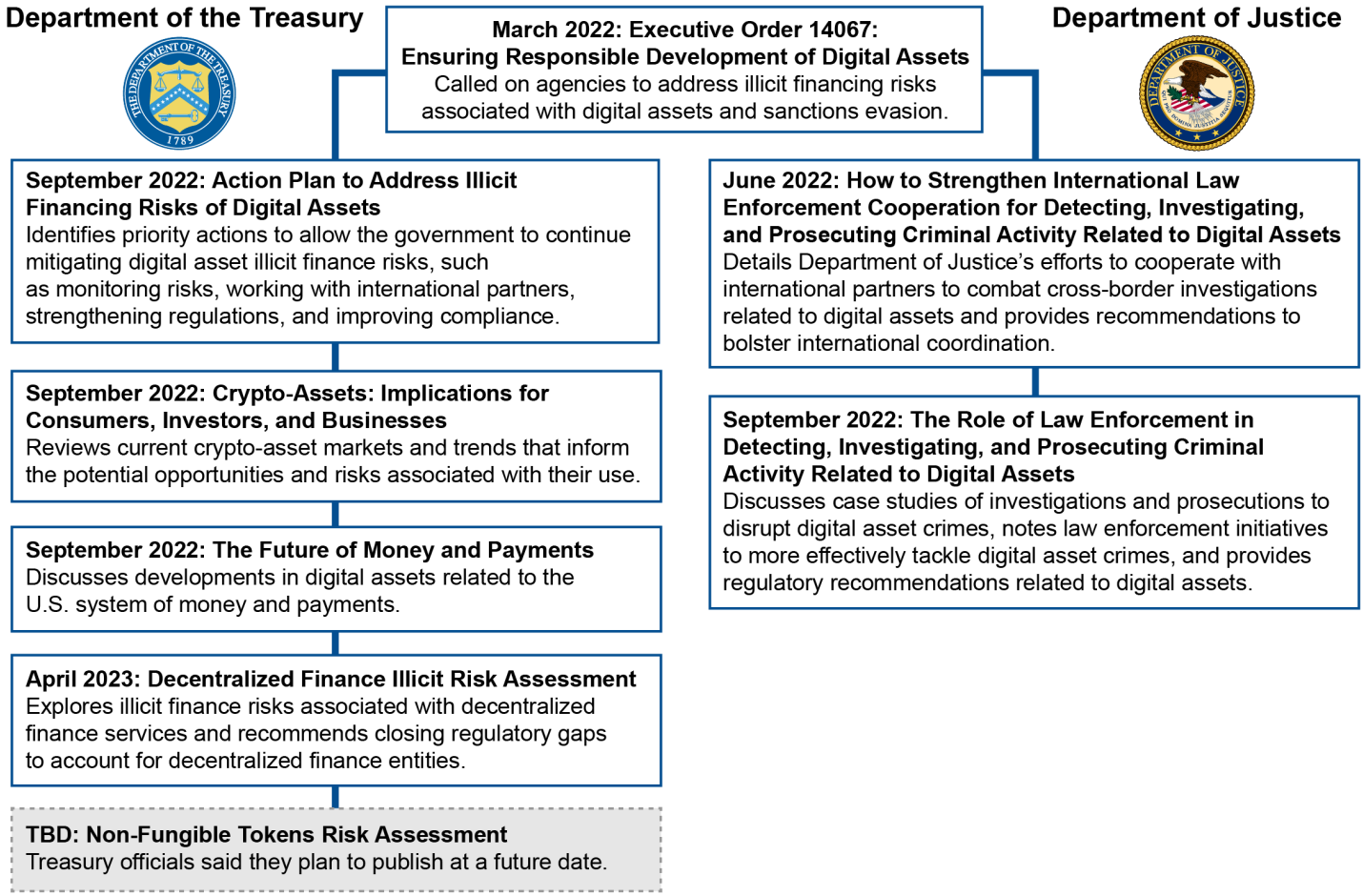
Many agencies contribute to investigations that lead to enforcement actions. For example, Internal Revenue Service – Criminal Investigation (IRS-CI), FBI, and DHS's Homeland Security Investigations office collaborated on an investigation that led to the March 2020 DOJ indictment of two Chinese nationals for laundering stolen virtual currency on behalf of North Korea.

As previously noted in this report, agencies also use private sector tools and expertise to aid in enforcement efforts. Various agencies noted that they have access to private-sector blockchain-tracing technologies from companies such as Chainalysis, TRM Labs, and others that help government officials investigate illicit digital asset activities. These investigations can lead to sanctions designations and enforcement actions. In addition to the technologies themselves, government officials also have access to private sector experts to help them use the tools effectively. For example, a law enforcement agency official said that a Chainalysis employee is co-located at their agency offices. Additionally,

OFAC officials said that they have attended multiple courses offered by blockchain analytics companies to increase their employees' knowledge of digital assets.

Reports and action plans. Agencies have issued an action plan and reports addressing sanctions evasion and other illicit finance risks associated with digital assets. Specifically, Treasury released an action plan and Treasury and DOJ issued multiple additional reports in 2022 and 2023 in response to EO 14067, which called on agencies to address illicit financing risks associated with digital assets. Treasury and DOJ coordinated with other agencies, including State, on these reports, according to officials. These reports are described in figure 10 below.

Figure 10: U.S. Government Agencies' Reports and Action Plans in Response to a 2022 Executive Order Addressing Illicit Finance and Sanctions Evasion Risks



Source: GAO analysis of agency reports and interviews with agency officials; Department of the Treasury, Department of Justice (seals). | GAO-24-106178

Note: The April 2023 Decentralized Finance Illicit Risk Assessment was not mandated by Executive Order 14067 but is associated with Treasury's September 2022 Action Plan to Address Illicit Financing Risks of Digital Assets.

U.S. agencies have released other reports discussing illicit financial activity, including the use of digital assets to evade sanctions, that are not in response to EO 14067. Some of these reports discuss actions taken to mitigate digital asset risks that predate the EO. For example, Treasury's 2022 National Money Laundering Risk Assessment offers an overview of the key money-laundering threats to the U.S, including those posed by

digital assets.[76] Additionally, IRS-CI's 2022 annual report highlighted their contributions to investigations involving digital assets and sanctions.

Public messaging. Multiple Treasury offices have issued guidance, advisories, and other public messages for the digital assets industry to raise awareness of and encourage compliance with AML and sanctions requirements.

Treasury's FinCEN has issued guidance or advisories on a variety of topics related to the use of digital assets to evade sanctions. For example:

- In March 2022, FinCEN published guidance for financial institutions that provided examples of red flags to look for on potential Russian sanctions evasion attempts.
- In May 2019, FinCEN released an advisory on illicit financial activity, including sanctions evasion, involving convertible virtual currency.

Other Treasury offices have released public materials and developed mechanisms to share information with the digital asset industry and encourage compliance with sanctions requirements. For example:

- In October 2021, OFAC published a virtual currency sanctions compliance guidance brochure that includes information outlining how the virtual currency industry can build sanctions compliance programs, protect against misuse of virtual currencies by malicious actors, and understand OFAC's internal processes.
- OFAC published on its website a list of frequently asked questions concerning cyber-related sanctions that includes information about digital assets.
- OFAC officials said that they have a compliance hotline that they encourage the public to use as a resource to contact OFAC with

[76]Treasury's 2022 National Money Laundering Risk Assessment was the third such document published since 2015.

questions regarding sanctions compliance, OFAC guidance, and other general OFAC inquiries.[77]

- FinCEN's Regulatory Support Section responds to inquiries from financial institutions, regulators, law enforcement, and members of the public using FinCEN's regulations, published guidance, and rulings to clarify requirements, according to Treasury officials.
- Treasury officials said that they hold meetings and participate in conferences with the private sector entities to encourage regulations compliance.

Senior agency officials have also made public statements about the use of digital assets to evade sanctions. For example, Treasury Secretary Janet Yellen made public remarks about illicit finance risks, including risks to sanctions evasion, associated with digital assets in a 2022 speech at American University. Additionally, former OFAC and current FinCEN Director Andrea Gacki has spoken at conferences about the use of digital assets to evade sanctions.

International efforts. U.S. agencies work with international organizations and foreign partners to protect the global financial system from illicit use of digital assets. As noted earlier in this report, the U.S. actively participates in FATF to promote the implementation of international AML standards to protect the global financial system against money laundering, terrorist financing, and proliferation financing, including through the use of digital assets. While Treasury leads the U.S. delegation to FATF, other agencies, including State and DOJ, contribute to the delegation as well, according to officials.

Additionally, Treasury officials said that Treasury serves as the co-chair of FATF's virtual assets contact group. The group works to implement FATF Recommendation 15 concerning mitigating illicit finance risks related to new technologies, including virtual assets, and co-led a FATF report on countering ransomware financing. In February 2023, FATF agreed to a roadmap to strengthen implementation of FATF standards on virtual assets and VASPs. This will include a future FATF report on steps that

[77]In 2021, we recommended that OFAC systematically track information on inquiries made to its compliance hotline to identify trends and recurrent issues. As of September 2023, OFAC reported that it had developed and was in the process of testing a new system to track incoming inquiries to its compliance hotline. See *GAO, Venezuela: Additional Tracking Could Aid Treasury's Efforts to Mitigate Any Adverse Impacts U.S. Sanctions Might Have on Humanitarian Assistance,* GAO-21-239 (Washington, D.C.: Feb. 4, 2021).

jurisdictions with materially important virtual asset activity have taken to regulate and supervise VASPs.

U.S. agencies also work with foreign partners in other ways to prevent sanctions evasion with digital assets. For example, State funds training sessions with foreign partners on threats posed by virtual currencies, including sanctions evasion, according to State officials. State also hosts meetings with foreign partners, such as a March 2023 working group meeting with South Korean officials to exchange information about North Korea's malicious cyber activities, including cryptocurrency heists.

According to DHS officials, through State-funded International Law Enforcement Academies, DHS conducts virtual currency investigation trainings for foreign partners through the U.S. Secret Service. Treasury officials said that bilateral engagement is part of their regular efforts to increase AML compliance, such as a roundtable to discuss digital asset-related issues they held with their Estonian counterparts. Finally, in March 2022, State issued guidance instructing embassies to engage foreign counterparts on AML standards regarding Russian sanction evasion efforts, including those involving digital assets.

Agency Comments

We provided a draft of this report to Treasury, DOJ, State, DHS and IRS-CI for review and comment. The agencies provided technical comments, which we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of the Treasury, the Acting Assistant Attorney General for Administration, the Secretary of State, the Secretary of Homeland Security, the Commissioner of the Internal Revenue Service, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8612 or GianopoulosK@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in Appendix V.

Kimberly Gianopoulos
Director, International Affairs and Trade

Appendix I: Objectives, Scope, and Methodology

This report examines (1) the risks that digital assets pose to U.S. agencies' abilities to implement and enforce sanctions and factors that may mitigate those risks and (2) the actions U.S. agencies have taken to address the risks that digital assets present with regard to implementing and enforcing U.S. sanctions.

To examine the risks that digital assets pose to U.S. agencies' ability to implement and enforce U.S. sanctions and factors that may mitigate those risks, we conducted interviews with officials from the Departments of Homeland Security (DHS), Justice (DOJ), State (State), and the Treasury (Treasury), as well as Internal Revenue Service-Criminal Investigation (IRS-CI). Within DOJ, we met with officials from the Federal Bureau of Investigation's (FBI) Virtual Assets Unit as well as DOJ's National Cryptocurrency Enforcement Team, and the Money Laundering and Asset Recovery Section. Within IRS-CI, we met with officials from Global Operations and the Office of Cyber and Forensic Services.

We met with Treasury and State officials as those agencies have units dedicated primarily to sanctions implementation.[1] Treasury officials, who play a primary role in sanctions implementation and administration of anti-money laundering regulations, identified the other agencies as relevant to our objectives.

We also obtained and analyzed the views of 15 stakeholders knowledgeable of sanctions implementation and enforcement as well as digital assets. The stakeholders included six researchers from academia and think tanks,[2] four representatives of the digital assets industry—blockchain analytics firms, a digital asset exchange, and a financial firm—and five individuals who provide legal or advisory services on sanctions

[1]The Department of Commerce also has a unit dedicated primarily to sanctions implementation and also has units with roles in sanctions implementation in addition to other responsibilities. However, their role in sanctions implementation typically involves export controls and as such was not as relevant for digital assets.

[2]We met with individuals from the think tanks the Royal United Services Institute, Center for a New American Security, and Atlantic Council.

and digital assets issues.[3] To identify potential stakeholders, we reviewed the results of a literature search of relevant articles and congressional hearings and obtained recommendations for stakeholders during initial interviews we conducted.[4] We compiled a list of 68 potential stakeholders and collected information on the potential stakeholders' areas of focus, current and prior affiliations, prior government experience, publications, conference or congressional hearing participation, and education.

To select the stakeholders, our considerations encompassed several factors, though not every factor applied to every stakeholder. Specifically, we considered whether:

- the potential stakeholder had professional or technical experience that would allow them to comment knowledgeably on issues related to sanctions implementation and enforcement and digital assets,
- other individuals had recommended the potential stakeholder,
- the potential stakeholder had prior government experience,
- the potential stakeholder had relevant publications or conference or hearing participation, and
- representation came from a variety of organizations.

To narrow down our list of potential stakeholders, we considered the factors across the three groups of stakeholders: researchers; private sector-digital assets industry; and private sector-legal or advisory, aiming to have between three and six stakeholders per group. To represent diverse perspectives, we contacted only one author of any co-authored papers and initially contacted only one person per an organization. For the private sector-industry group, we wanted to ensure that we captured viewpoints from blockchain analytics firms as well as digital asset exchanges or finance-related firms. For non-academic researchers, to ensure a diverse perspective across relevant organizations, we initially chose one representative from the organizations included in our list:

[3]Some stakeholders we interviewed fell into more than one group. For example, some stakeholders had an affiliation with a think tank and also worked in a legal or advisory capacity.

[4]We conducted searches of various databases including Scopus; ProQuest; EBSCO; ProQuest Dialog (which includes EconLit, Investext, ProQuest Dissertations and Theses Professional, and SciSearch®); Harvard Think Tank; Govinfo.gov; and Westlaw Edge. Our search produced 92 articles and 14 hearings. We considered authors of 21 papers or reports we determined would be possibly relevant and which focused on both sanctions and digital assets.

Royal United Services Institute, Center for a New American Security, and the Atlantic Council. See Appendix III for the names, affiliations, and selected government experience of the stakeholders we interviewed.

The stakeholders covered a wide range of areas of expertise and viewpoints, and we sought to capture that range in our findings. While the views of the 15 stakeholders that we interviewed are not generalizable to all stakeholders, they provide illustrative examples on the risks that digital assets pose to U.S. agencies' abilities to implement and enforce sanctions and factors that may mitigate those risks.

We conducted semi-structured interviews with these stakeholders to obtain their views on digital asset risks pertaining to sanctions implementation and enforcement, risk mitigation opportunities, whether risks or risk mitigating factors vary based on asset or actor type, and tools or other collaborative actions that facilitate risk mitigation.

To corroborate information from these interviews and provide additional context, we reviewed agency reports related to the risks that digital assets pose to U.S. agencies' abilities to implement and enforce sanctions and factors that may mitigate those risks. We identified these reports through interviews with agency officials and from researching reports produced as part of the "Executive Order 14067: Ensuring Responsible Development of Digital Assets."[5] These included Treasury's *Action Plan to Address Illicit Financing Risks of Digital Assets* and the DOJ's *The Role Of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related To Digital Assets.*[6]

We also reviewed reports and documents produced by firms in the digital asset industry, an international organization, and think tanks as well as scholarly papers. While our focus was on sanctions evasion risks, we also considered some broader illicit finance risks if such risks also apply to sanctions evasion.

[5]Ensuring the Responsible Development of Digital Assets, Exec. Order No. 14067, 87 Fed. Reg. 14,143 (Mar. 9, 2022).

[6]Department of the Treasury, *Action Plan to Address Illicit Financing Risks of Digital Assets*, (Washington, D.C.: Sept. 16, 2022); Department of Justice, Report of the Attorney General, *The Role Of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related To Digital Assets*, (Washington, D.C.: Sept. 6, 2022).

We also examined the market capitalization of all cryptocurrencies using data from CoinMarketCap.[7] We did not assess the accuracy of the underlying data. However, through a review of data-related documentation, we determined that these data were sufficiently reliable for demonstrating volatility of the cryptocurrency market.

We report on the risks and any associated mitigating factors that were frequently identified in the interviews we conducted and reports we reviewed. Additional illicit finance risks exist which may also impact the U.S. agencies' ability to implement and enforce U.S. sanctions. The information on foreign law in this report is not the product of GAO's original analysis, but is derived from interviews and secondary sources.

To examine the actions that U.S. agencies have taken to address the risks that digital assets present with regard to implementing and enforcing U.S. sanctions, we reviewed information from various agencies and interviewed agency officials from Treasury, DOJ, State, DHS and IRS-CI. We identified and reviewed agency press releases, government reports, and other documents collected from agency websites relevant to digital assets and sanctions.

We then categorized agency actions into five areas: sanctions designations, law enforcement actions, reports and action plans, public messaging, and international efforts. Lastly, we followed up with agency officials to confirm of the information we found and added any additional documents or information.

Not all agencies we contacted were able to confirm that the information we identified represented a comprehensive list of agency actions taken to address the risks posed by digital assets to sanctions implementation. While Treasury officials were able to confirm a comprehensive list of sanctions designations made for facilitating sanctions evasion with digital assets, DOJ was unable to confirm a complete list of law enforcement actions involving both digital assets and sanctions evasion. We were nonetheless able to provide examples of such enforcement actions. The

[7]According to CoinMarketCap, total market capitalization is the sum of individual crypto assets' market capitalizations. CoinMarketCap determines the capitalizations by multiplying the circulating supply of that crypto asset by the reference price of the crypto asset, which uses the distribution of prices reported by an exchange. Data from CoinMarketCap show the total market capitalization of all cryptocurrencies, including stablecoins and tokens. While market capitalization for non-digital assets reflects the total dollar market value of all of a firm's outstanding shares, the market capitalization for digital assets may be less tangible.

lack of a complete enforcement actions list did not impact our determination that agencies have taken actions to address digital asset risks related to U.S. sanctions.

We conducted this performance audit from July 2022 to December 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Key Terminology Related to Digital Assets

This appendix defines key terminology related to digital assets. In the body of the report, we generally refer to digital assets and virtual currencies unless otherwise specified. As noted below, virtual currencies include cryptocurrencies.

Addresses. Users' crypto asset balances are associated with crypto asset addresses that use principles of cryptography to help safeguard against inappropriate tampering. When a user transfers crypto assets, the recipient provides their crypto asset address to the sender, and the sender authorizes the transaction with their private key (essentially a secret code that proves the sender's control over their crypto asset address).[1]

Blockchain. According to "Executive Order 14067: Ensuring Responsible Development of Digital Assets,"[2] the term ''blockchain'' refers to distributed ledger technologies where data are shared across a network that creates a digital ledger of verified transactions or information among network participants, and the data are typically linked using cryptography to maintain the integrity of the ledger and execute other functions, including transfer of ownership or value.[3]

Central bank digital currency (CBDC). According to Executive Order 14067, CBDC refers to a form of digital money or monetary value, denominated in the national unit of account that is a direct liability of the central bank.

[1]For more information see GAO, *Blockchain in Finance: Legislative and Regulatory Actions Are Needed to Ensure Comprehensive Oversight of Crypto Assets*, GAO-23-105346 (Washington, D.C.: June 22, 2023).

[2]Ensuring the Responsible Development of Digital Assets, Exec. Order No. 14067, 87 Fed. Reg. 14,143 (Mar. 9, 2022).

[3]For additional information on blockchain see GAO, *Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges*, GAO-22-104625 (Washington, D.C.: Mar. 23, 2022) and GAO, *Science & Tech Spotlight: Blockchain & Distributed Ledger Technologies*, GAO-19-704SP (Washington, D.C.: Sept. 16, 2019).

Chain hopping. Chain hopping involves transferring one virtual currency to another virtual currency on a different blockchain, often in rapid succession.

Cryptocurrency. According to Executive Order 14067, the term ‘‘cryptocurrency’’ refers to a digital asset, which may be a medium of exchange, for which generation or ownership records are supported through a distributed ledger technology, such as a blockchain. That is, cryptocurrencies are a type of virtual currency that employs encryption technology and usually operate on a blockchain.

Digital assets. According to Executive Order 14067, the term ‘‘digital assets’’ refers to representations of value; financial assets and instruments; or claims that are used to make payments or investments, or to transmit or exchange funds or the equivalent thereof, issued or represented in digital form through distributed ledger technology. For example, digital assets include virtual currencies, stablecoins, and CBDCs.

Distributed ledger technology. Distributed ledger technologies are a relatively secure way of conducting and recording transfers of digital assets without the need for a central authority. Distributed ledger technologies are “distributed” because multiple participants in a computer network (individuals, businesses, etc.), share and synchronize copies of the ledger. New transactions are generally added in a manner that is cryptographically secured, permanent, and visible to all participants in near real time.

Exchanges. Companies and individuals that offer virtual currency and other virtual asset exchange services are often referred to as “exchanges.”

Mining. According to Coinbase, a cryptocurrency exchange, mining is the process that cryptocurrencies use to generate new coins and verify new transactions. It involves vast, decentralized networks of computers around the world that verify and secure blockchains. In return for contributing their processing power, computers on the network and the miners operating them are rewarded with new coins.

Mixers and tumblers. Mixers and tumblers are services that mix the virtual currency of several users during transfers to increase anonymity.

Non-fungible token. A non-fungible token (NFT) is a digital identifier, similar to a certificate of ownership, that represents a digital or physical asset. In general, a non-fungible asset is unique and not interchangeable with others. An NFT, like an original painting, has its own unique value. By contrast, fungible assets are interchangeable, like dollar bills.[4]

Peel-chain. A peel chain is a technique that criminals use in an attempt to conceal the source of funds. An individual user moves a large amount of virtual currency located at one virtual currency address through a series of transactions, transferring smaller amounts of virtual currency to a new address each time.

Stablecoins. According to Executive Order 14067, the term stablecoins refers to a category of virtual currencies with mechanisms that are aimed at maintaining a stable value. Mechanisms include pegging the value of the coin to a specific currency, asset, or pool of assets or by algorithmically controlling supply in response to changes in demand in order to stabilize value.

Staking. According to one exchange, staking is a process by which users lock their cryptocurrency to support the operation of a blockchain network, essentially helping to secure and validate transactions on the blockchain, in exchange for cryptocurrency or transaction fees.

Virtual asset service provider (VASP). The Financial Action Task Force identifies a VASP as a person or business that conducts one or more of the following activities or operations for, or on behalf of, another person: (1) exchanging virtual currency to fiat currency; (2) exchanging between one or more forms of virtual assets; (3) transferring virtual currencies; (4) safekeeping and/or administering virtual currencies; or (5) participating in and providing financial services related to an issuer's offer and/or sale of a virtual currency.

Virtual currency. FinCEN defines virtual currency as a medium of exchange that can operate like currency in some environments but does not have all the attributes of "real" currency, including legal tender status. FinCEN applies its regulations to "convertible virtual currency," a type of

[4]For additional information on NFTs see GAO, *Science & Tech Spotlight: Non-Fungible Tokens (NFTs)*, GAO-22-105990 (Washington, D.C.: June 14, 2022).

virtual currency that has an equivalent value in real currency or acts as a substitute for real currency. Virtual currencies include cryptocurrencies.

Wallets. Users may store components of crypto asset transactions such as private keys and addresses in a virtual wallet, which allows them to access their crypto assets.[5]

[5]Crypto asset wallets can be custodial or noncustodial. With a custodial wallet, a service provider (such as a crypto asset trading platform or third-party wallet provider) holds the users' private keys. Holding the users' private keys enables the custodial wallet provider to exercise full control over the user's assets, although the custodian generally will have contractual or other legal obligations to take direction from the user regarding the assets, such as sending a remittance or making a payment. A noncustodial wallet is located on the user's computer or other data storage device, and the user retains full control over the private keys and the assets in the wallet. For more information see GAO-23-105346.

Appendix III: List of Stakeholders

Table 1 provides a list of the names, affiliations, and selected government experience of the stakeholders whose views we obtained and analyzed through semi-structured interviews. The stakeholders include six researchers from academia and think tanks, four representatives of the digital assets industry, and five individuals who provide legal or advisory services on sanctions and digital assets issues. See Appendix I for information on our selection of the stakeholders.

Table 1: List of Stakeholders GAO Interviewed

Name	Affiliation	Selected government experience
Researchers		
Aaron Arnold	Senior Associate Fellow in the Centre for Financial Crime and Security Studies at the Royal United Services Institute	Counter-proliferation subject matter expert at the Department of Defense and DOJ
Richard Clark	Assistant Professor of Government at Cornell	N/A
Yaya Fanusie	Adjunct Senior Fellow, Energy, Economics and Security Program at Center for a New American Security	Economic and counterterrorism analyst at the Central Intelligence Agency
Ananya Kumar	Assistant Director of digital currencies at the GeoEconomics Center at the Atlantic Council	N/A
Kevin Werbach	Professor of Legal Studies and & Business Ethics at Wharton School at University of Pennsylvania	Advisor at Federal Communications Commission and Department of Commerce Co-Lead of Federal Communications Commission Agency Review, Obama-Biden Transition Project
Alex Zerden	Adjunct Senior Fellow at Center for a New American Security	Treasury's FinCEN, TFI, and Office of International Affairs White House National Economic Council
Private sector, digital assets industry		
Kayla Izenman	Compliance team member at Coinbase	Department of Commerce Department of State
Jonathan Levin	Co-Founder and Chief Strategy Officer at Chainalysis	N/A
Ari Redbord	Head of Legal & Government Affairs at TRM Labs	Senior Advisor to the Deputy Secretary and the Under Secretary for Treasury's TFI. Assistant United States Attorney for the District of Columbia at DOJ

Name	Affiliation	Selected government experience
Jesse Spiro	Head of Regulatory Relations for the Blockchain, Crypto, and Digital Currencies Business Unit at PayPal	N/A
Private sector, legal or advisory services on sanctions and digital assets issues		
Jamal El-Hindi	Counsel in Americas Litigation & Dispute Resolution practice at Clifford Chance	Deputy Director of Treasury's FinCEN Associate Director for Program Policy and Implementation at Treasury's Office of Foreign Assets Control Inaugural Chief Data Officer at Treasury
Carole House	Executive in Residence at Terranet Ventures, Inc.	Director of Cybersecurity and Secure Digital Innovation at the National Security Council Senior Cyber and Emerging Tech Policy Officer at Treasury's FinCEN
Sigal Mandelker	General Partner at Ribbit Capital	Under Secretary for Treasury's TFI Deputy Assistant Attorney General in the Criminal Division at DOJ
Michael Mosier	Co-founder of Arktouros PLLC and General Counsel at Espresso Systems	Acting Director, Deputy Director, and Digital Innovation Officer of Treasury's FinCEN Cybersecurity & emerging technology counselor to the Deputy Secretary of the Treasury Associate Director at Treasury's Office of Foreign Assets Control Deputy Chief at DOJ's Money Laundering Section
The Honorable Juan Zarate	Global Co-Managing Partner and Chief Strategy Officer at K2 Integrity	Deputy Assistant to the President and Deputy National Security Adviser for Combating Terrorism Inaugural Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes

Legend: Department of the Treasury = Treasury; Department of Justice = DOJ; Financial Crimes Enforcement Network = FinCEN; Office of Terrorism and Financial Intelligence = TFI; not applicable = N/A.

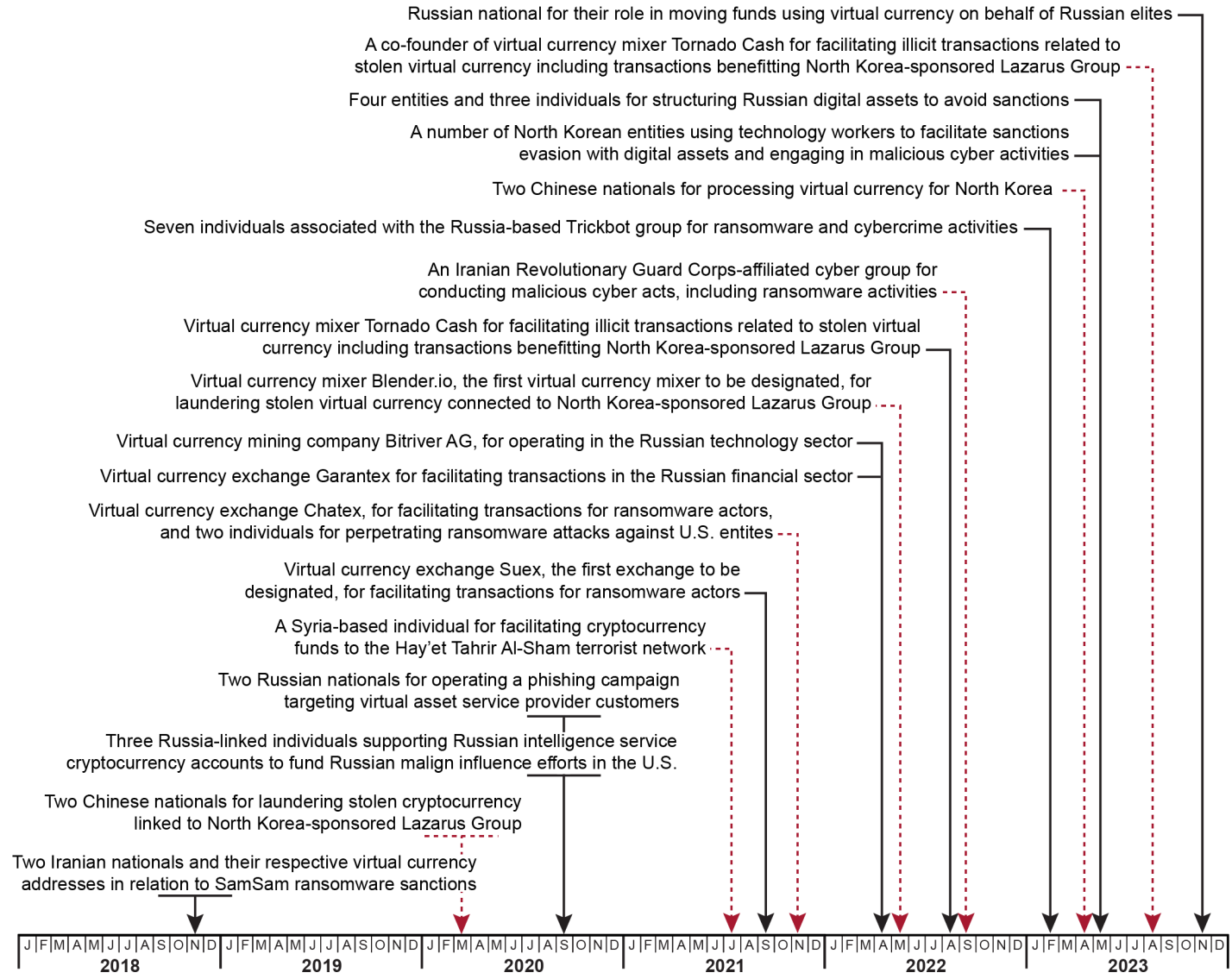
Source: GAO. | GAO-24-106178

Note: Some stakeholders we interviewed fell into more than one affiliation group. For example, some stakeholders had an affiliation with a think tank and also worked in a legal or advisory capacity.

Appendix IV: Department of the Treasury's Digital Assets-Related Sanctions Designations

The Department of the Treasury's (Treasury) Office of Foreign Assets Control has designated entities and individuals for facilitating sanctions evasion with digital assets.

Figure 11: Department of the Treasury's Office of Foreign Asset Controls' Designations for Facilitating Sanctions Evasion with Digital Assets



Legend: Democratic People's Republic of Korea = North Korea.

Source: GAO analysis of Department of the Treasury information. | GAO-24-106178

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Kimberly M. Gianopoulos, (202) 512-8612, or gianopoulosk@gao.gov

Staff Acknowledgments

In addition to the contact named above, Drew Lindsey (Assistant Director), Jeffrey Baldwin-Bott (Analyst in Charge), Nisha Rai, Aaron Rochow, Bobby Treadwell, Donna Morgan, Neil Doherty, Mark Dowling, Pamela Davidson, Pedro Almoguera, Jieun Chang, and Pamela Snedden made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548