



# Audit of the United States Marshals Service's Management of Seized Cryptocurrency



AUDIT DIVISION

22-082

---

**JUNE 2022**

---



# EXECUTIVE SUMMARY

## Audit of the United States Marshals Service's Management of Seized Cryptocurrency

### Objective

Our audit objective was to evaluate the United States Marshals Service's (USMS) management of seized cryptocurrency. This audit covers seized cryptocurrency in USMS custody from fiscal year (FY) 2017 through FY 2021.

### Results in Brief

We found that the USMS has implemented adequate safeguards over the storage of and access to seized cryptocurrency in its custody. However, the USMS faces challenges in managing and tracking cryptocurrency in the U.S. Department of Justice's (DOJ) official seized asset tracking system. As a result, the USMS is using supplemental spreadsheets that lack documented operating procedures and other important inventory management controls. These deficiencies risk an inaccurate accounting of cryptocurrency in USMS custody and the potential for a loss of assets. Additionally, current USMS seized cryptocurrency management policies related to asset storage, quantification, valuation, and disposal are inadequate or absent, and in some instances provide conflicting guidance. The USMS is actively seeking to outsource the management of seized cryptocurrency. However, without properly documented policies and procedures, the USMS lacks an adequate foundation for building performance requirements for a cryptocurrency services contract.

### Recommendations

Our report contains seven recommendations to improve the USMS's management and tracking of seized cryptocurrency. We requested a response to our draft audit report from the USMS, which can be found in Appendix 2. Our analysis of their response is included in Appendix 3.

### Audit Results

Cryptocurrency is a type of virtual currency that can be traded and used for investment purposes or to pay for goods and services. Although cryptocurrency is not recognized as legal tender by the U.S. Government or in most countries, and is not backed by an intrinsically valuable object such as gold, its unique attributes, including its virtual nature and often a high degree of anonymity, have made it increasingly attractive to criminals conducting illegal business transactions. To combat this, the DOJ uses its statutory authority to seize cryptocurrency used in, or obtained through, illicit activity. The USMS serves as the primary custodian for the DOJ's seized assets and, as of June 2021, managed nearly 200 DOJ cryptocurrency seizures. In September 2021, we valued these assets at about \$466 million.

### Inventory Management

The USMS uses several spreadsheets to track and manage its seized cryptocurrency inventory because the DOJ's official seized asset tracking system, the Consolidated Asset Tracking System (CATS), does not have the necessary functionality to enable daily management of cryptocurrency assets. While we believe that the USMS and the DOJ need a seized property management system that provides appropriate functionality for managing cryptocurrency assets, we nevertheless assessed the adequacy of the current, spreadsheet-based inventory records and found two areas of needed improvement. Specifically, we found that the USMS does not have documented policies or procedures related to the use of these inventory spreadsheets. We also found that the cryptocurrency spreadsheets lack necessary inventory management controls to prevent and detect fraudulent or erroneous alteration of the inventory records, such as the ability to track edit history. Finally, we found that the inventory spreadsheets the USMS uses to track and manage seized cryptocurrency were not accurate. Based on our analysis, we identified 28 seized cryptocurrency

assets in the USMS's inventory spreadsheets that did not appear in CATS and determined that the differences were due to tracking errors in the USMS's spreadsheets. In our judgment, these errors occurred because the USMS does not conduct periodic inventory reconciliations between its supplemental spreadsheets and CATS to ensure that the inventories are complete and accurate. Without periodic reconciliations, seized assets could be mismanaged and inventory records could be fraudulently altered without detection.

### **Policy Revisions**

We found that the USMS should strengthen its existing policies and procedures related to quantifying cryptocurrency, handling cryptocurrency “forks” (whereby a single cryptocurrency splits into two separate currencies), and storing cryptocurrency. For example, we found that USMS policy does not require exact quantities of seized cryptocurrency to be recorded in CATS and does not have an established process for recording in CATS new cryptocurrency assets created after a fork. Additionally, we identified an instance of conflicting policy requirements related to CATS custody record creation, as well as areas where the USMS is not fully complying with current policy in documenting the value of seized cryptocurrency in CATS. Addressing these issues will help the USMS ensure that seized asset records include information that is critical to managing cryptocurrency, such as the asset type and quantity. Additionally, better documenting its required practices with respect to the management of seized cryptocurrency will help USMS ensure that its employees, especially new employees, know and understand what is expected of them when handling seized cryptocurrency.

### **Cryptocurrency Services Contract**

The USMS is in the process of awarding a contract to outsource its seized cryptocurrency management and disposal responsibilities. At the time of our audit, the USMS was addressing contract award protests and had not yet awarded its cryptocurrency services contract. We take no issue with the USMS's contract requirements documentation and oversight plan. However, the USMS should establish seized cryptocurrency policies and procedures related to inventory management, asset storage, quantification, valuation, and disposal prior to handing over its seized cryptocurrency responsibilities to a contractor. We believe this will best prepare the USMS to ensure the future contractor's services meet USMS's needs and expectations.

# Table of Contents

|   |           |
|---|-----------|
| <b>Introduction</b> .....   | <b>1</b>  |
| Virtual Currency and Cryptocurrency.....  | 1         |
| Cryptocurrency Wallets .....  | 1         |
| Cryptocurrency Transactions.....  | 2         |
| DOJ Asset Forfeiture Program .....  | 2         |
| OIG Audit Approach.....   | 3         |
| <b>Audit Results</b> .....  | <b>4</b>  |
| The USMS Faces Challenges Managing Cryptocurrency Using CATS .....  | 4         |
| CATS Inventory Records .....  | 4         |
| Accounting for Cryptocurrency Transaction Fees.....   | 5         |
| Tracking Forked Cryptocurrencies .....  | 5         |
| The USMS Should Implement Additional Controls Over Its Cryptocurrency Inventory Records .....                                     | 6         |
| Inventory Records May Be Altered Without Detection.....   | 6         |
| The USMS Has Not Established Guidelines for Its Inventory Records .....   | 6         |
| Asset Disposal Procedures Specific to Cryptocurrency Would Improve the USMS’s Liquidation or Other Handling of These Assets ..... | 7         |
| Anonymity Enhanced Cryptocurrency.....  | 7         |
| Non-Exchange and De Minimis Value Assets .....  | 8         |
| The USMS Should Strengthen Its Existing Cryptocurrency Policies .....   | 8         |
| Improvements to Current Cryptocurrency Policies .....   | 8         |
| Conflicting Policy and Instances of Non-Compliance .....  | 10        |
| The USMS’s Plans to Award a Cryptocurrency Contract Require Oversight .....   | 10        |
| <b>Conclusion and Recommendations</b> .....   | <b>11</b> |
| <b>APPENDIX 1: Objective, Scope, and Methodology</b> .....  | <b>12</b> |
| Objective.....  | 12        |
| Scope and Methodology.....  | 12        |
| Statement on Compliance with Generally Accepted Government Auditing Standards .....   | 12        |
| Internal Controls.....  | 12        |
| Sample-Based Testing.....   | 12        |
| Computer-Processed Data .....   | 13        |
| <b>APPENDIX 2: The USMS Response to the Draft Audit Report</b> .....  | <b>14</b> |

APPENDIX 3: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Report..... 17

# Introduction

Over 2,000 cryptocurrencies exist today that enable users to transfer virtual currency around the globe in exchange for goods, services, and other sources of value. Many of cryptocurrency's central features—including its decentralized operation and, in some cases, a high degree of anonymity—have become increasingly attractive to criminals engaging in and attempting to conceal illegal activity. Specifically, the U.S. Department of Justice (DOJ) has found that bad actors may use cryptocurrency to: (1) engage in financial transactions associated with the commission of crimes, such as buying and selling illicit drugs or weapons on the dark web, leasing computer equipment to commit cybercrimes, or soliciting funds to support terrorist activity; (2) engage in money laundering or shield otherwise legitimate activity from tax, reporting, or other legal requirements; or (3) commit crimes directly involving the cryptocurrency marketplace itself, such as stealing cryptocurrency from exchanges through hacking or using the promise of cryptocurrency to defraud unwitting investors.

## Virtual Currency and Cryptocurrency

Virtual currency is a digital representation of value that, like traditional currency, can be digitally traded and used for payment or investment purposes. Virtual currency is a type of virtual asset that is separate and distinct from digital representations of traditional currencies, financial securities, and other traditional financial assets. Unlike traditional currency, the value of virtual currencies is not based on their recognition as legal tender by a country (no virtual currency is recognized as legal tender by the U.S. Government), or on the currency being backed by an intrinsically valuable object such as gold. Instead, the monetary value of each virtual currency generally is primarily based on agreement or trust among its community of users. The most well-known and widely-circulated form of virtual currency is cryptocurrency, examples of which include Bitcoin and Ethereum.

## Cryptocurrency Wallets

The storage of cryptocurrency is typically associated with an individual “wallet,” which is similar to a virtual account. Wallets contain cryptographic codes known as public and private keys. Public keys are roughly akin to a bank account number and are what wallet owners provide to others in order to send and receive cryptocurrency. Private keys function like a PIN or password that are used to sign transactions and restrict access to spending cryptocurrency. As the name suggests, these keys should be kept private and secured appropriately as they allow the holder to spend cryptocurrency and transfer cryptocurrency to another person. Cryptocurrency wallets can be housed in a variety of forms:

- Hardware Wallet – A tangible, external device
- Software Wallet – Downloaded as software to a computing device
  - Desktop Wallet – Software on either a personal computer or server
  - Mobile Wallet – An application on a smartphone
- Paper Wallet – Public and private keys printed on paper

- An online account associated with a cryptocurrency exchange

The United States Marshals Service (USMS) maintains its wallet keys and seized cryptocurrency in hardware wallets: encrypted thumb drives held in secure offline storage.

## Cryptocurrency Transactions

Cryptocurrency uses a form of cryptography known as encryption to secure financial transactions. Most cryptocurrencies operate with no central administrating authority, such as a bank, to issue currency and maintain payment ledgers. Instead, cryptocurrencies rely on complex algorithms, a distributed ledger often referred to as the “blockchain,” and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

The blockchain enables a particular cryptocurrency’s decentralized system to accurately track payments and to prevent double-spending and counterfeiting by cryptographically recording every transaction. When a transaction is initiated, it is shared with participants on the network associated with the particular cryptocurrency, where special users, often called “miners,” verify that the units have not already been spent and validate the transaction. Once the transaction is validated, the transaction is then added to the blockchain, with each block consisting of a group of reported transactions in chronological order.

## DOJ Asset Forfeiture Program

The Asset Forfeiture Program was created in 1984 when Congress passed the Comprehensive Crime Control Act, which provided federal prosecutors and agents the legal means to seize and forfeit the economic benefit of criminal activity. Asset forfeiture plays a critical role in disrupting and dismantling illegal enterprises, depriving criminals of the proceeds of illegal activities, deterring crime, and restoring property to victims. The effective use of asset forfeiture is an essential component of the DOJ’s efforts to combat the most sophisticated criminal actors and organizations – including terrorist financiers, cyber criminals, fraudsters, human traffickers, and transnational drug cartels.

The USMS is responsible for managing and disposing of most of the property that is seized and forfeited under the authority of [18 U.S.C. § 982](#) and [21 U.S.C. § 853](#) including cryptocurrency derived from, or involved in, criminal activity. The USMS manages the distribution of forfeited property and payments to victims of crime connected to those assets, and to state, local, and tribal law enforcement agencies that directly participate in the law enforcement efforts leading to the seizure and forfeiture of assets. Proceeds generated from asset sales are used to operate the program, compensate victims, and support various law enforcement efforts. The USMS Asset Forfeiture Division’s Complex Assets Unit (CAU) is currently the primary custodian for all cryptocurrency seized under the Department’s [Asset Forfeiture Program](#).<sup>1</sup>

As of June 2021, the USMS had nearly 200 DOJ cryptocurrency seizures comprised of 22 different types of seized cryptocurrency in its custody. In September 2021, we valued these assets at about \$466 million. The largest seizure of cryptocurrency by the DOJ occurred in November 2020, after the successful prosecution of

---

<sup>1</sup> U.S. Department of Justice Office of the Inspector General, [Review of the Department’s Oversight of Cash Seizure and Forfeiture Activities](#), Evaluation and Inspections Report 17-02 (March 2017), [www.oig.justice.gov/reports/review-departments-oversight-cash-seizure-and-forfeiture-activities](http://www.oig.justice.gov/reports/review-departments-oversight-cash-seizure-and-forfeiture-activities)

the founder of the notorious online criminal marketplace known as Silk Road, when the DOJ took custody of thousands of Bitcoins that were the proceeds of illegal activity.<sup>2</sup> The seized cryptocurrency, which had been stolen from Silk Road by an unidentified hacker, were valued at the time of the seizure at over \$1 billion. More recently, in June 2021 the DOJ seized 63.7 Bitcoins that allegedly represented a large portion of the proceeds of a highly publicized ransomware attack of the Colonial Pipeline. At the time of the seizure, these Bitcoins were valued at over \$2.3 million.

## **OIG Audit Approach**

Our objective was to evaluate the USMS's management of seized cryptocurrency. The scope of our audit generally covers the USMS's custody, management, storage, tracking, appraisal, and disposal of seized cryptocurrency from fiscal year (FY) 2017 through FY 2021.

To accomplish our objective, we observed the physical controls and safeguards over seized cryptocurrency at the CAU office. Additionally, we interviewed USMS personnel, including officials from the CAU and Asset Forfeiture Division's Real Property Unit. We analyzed the effectiveness of current controls over seized cryptocurrency. We also evaluated DOJ and USMS policies and procedures related to virtual currency seizures and reviewed seized cryptocurrency inventory records to ensure they adhered to policy requirements. Finally, we assessed the performance work statement for the USMS's planned cryptocurrency services contract to ensure it aligned with current USMS controls over seized cryptocurrency. Appendix 1 contains further details on our audit objective, scope, and methodology.

---

<sup>2</sup> Seizing cryptocurrency entails transferring cryptocurrency assets to a DOJ-controlled cryptocurrency wallet.

## Audit Results

The USMS has implemented adequate safeguards over the storage and access to seized cryptocurrency in its custody. It uses several spreadsheets to track and manage its seized cryptocurrency inventory because the DOJ's Consolidated Asset Tracking System (CATS) does not have the necessary functionality to enable daily management of cryptocurrency assets. However, the USMS needs to improve its policies and practices related to seized cryptocurrency management. Specifically, we found that the USMS does not have documented policies or procedures related to the use of inventory spreadsheets. Additionally, current USMS seized cryptocurrency management policies are inadequate, absent, or in some instances provide conflicting guidance related to asset storage, quantification, valuation, and disposal. The USMS is actively seeking to outsource the management of seized cryptocurrency, making it even more critical that it establish expected practices through documented policies and procedures to ensure the future contractor's services meet USMS expectations for the proper management of all facets of the seized cryptocurrency life cycle.

### The USMS Faces Challenges Managing Cryptocurrency Using CATS

The USMS faces challenges in managing and tracking cryptocurrency in CATS, the DOJ's official system of records for seized and forfeited assets, because CATS does not have the necessary functionality for tracking and recording important attributes of cryptocurrency. As a result, CAU employees have supplemented its use with spreadsheets maintained outside of CATS to track pertinent information such as cryptocurrency quantities, variants, asset valuation, blockchain forks, and transaction fees.

First established in 1993, CATS is a consolidated asset forfeiture database used by the entire Asset Forfeiture Program to track information and support operations of asset forfeiture functions such as seizure, custody, forfeiture, equitable sharing, and disposal. During our audit, employees from USMS's Asset Forfeiture Division raised concerns with the use of CATS for tracking cryptocurrency, describing it as antiquated and lacking the requirements necessary for the purpose. Consistent with this view, we found, CATS does not adequately document: (1) variations in cryptocurrency types; (2) valuation fluctuations as a result of market movements; (3) transaction and transfer fees that reduce the quantity of cryptocurrency in custody as it changes hands; or (4) tracking new cryptocurrency assets that are created as a result of blockchain forks. Each of these concerns are discussed in further detail below.

#### CATS Inventory Records

We found that CATS does not have designated fields to document the type or quantity of seized cryptocurrency in USMS custody. When seized cryptocurrency is added to CATS, each type of currency is assigned a unique identification number and categorized under the Asset Type "Financial Instrument." The asset is further categorized under the Asset Subtype "Virtual Currency." Beyond these two asset designations, CATS users must use text fields such as the "Asset Description" field to document the type (e.g., Bitcoin, Ethereum, etc.) and quantity of cryptocurrency seized, which are two of the most critical components for managing cryptocurrency inventories because they are needed to properly value the asset and determine how the USMS will handle and eventually dispose of the asset.

We further found that the contents of the text fields in CATS vary widely depending on the amount of detail provided by the seizing investigative agency that first enters the asset into CATS—including information

pertaining to the type and quantity of seized cryptocurrency. For instance, our analysis of CATS data for all seized cryptocurrency currently in USMS custody showed that some asset descriptions did not specify the quantity in custody, or used approximated amounts rather than the actual quantity. Additionally, because CATS does not provide designated fields for these attributes, historically CAU would manually sort and filter all seized assets under the “Virtual Currency” subtype in order to ascertain its complete inventory of seized cryptocurrency.

After the initiation of this audit, the USMS manually updated the CATS file for each cryptocurrency asset in its custody by adding a text data entry including the type and quantity of each asset into an unused text box within CATS. This manual update allows CAU to run a CATS report that displays each cryptocurrency type and the quantity in custody. As this new practice requires data entry, it is prone to human transcription error. The new practice also allows for only one type of cryptocurrency and a single asset quantity for each CATS file. Additionally, we found instances of seized assets in CATS being miscategorized as virtual currency, such as cryptocurrency that was converted to cash prior to the USMS taking custody of the asset.

Since the CATS data for all seized cryptocurrency is inconsistent and the process for manually determining each asset’s cryptocurrency type and current quantity is burdensome and prone to human error, there is a risk of an inaccurate count or valuation when the USMS is working within its active inventory. While CATS provides the function necessary to track the chain of custody of seized cryptocurrency, it does not provide the functionality needed to track the actual inventory and current value of seized cryptocurrency assets.

### **Accounting for Cryptocurrency Transaction Fees**

When seized cryptocurrency changes hands, the transaction incurs a fee that reduces the quantity being transferred by a small amount. This fee is used to create incentives for miners to verify and record transactions in the blockchain. In most cases, seized cryptocurrency is transferred from the seizing agency to the USMS’s wallet, and then transferred from the USMS wallet to the platform used to dispose of the asset, resulting in two transfer fees. The fee amount fluctuates constantly as it is based on variable conditions such as current network demand and transaction size. As previously stated, the quantities of seized cryptocurrency are documented in text fields for each cryptocurrency asset in CATS. However, the quantity recorded is often the initial seized quantity and is not updated to account for subsequent transaction fees incurred after the asset is transferred into USMS custody. As a result, the quantity of seized cryptocurrency in the DOJ’s official system of record may not accurately reflect the quantity in USMS custody.

### **Tracking Forked Cryptocurrencies**

A blockchain fork occurs when there is a radical change to the rules of a blockchain network that results in the blockchain splitting into two branches, one that follows the previous rules and the other following the new rules. For example, a Bitcoin fork in August of 2017 resulted in the creation of Bitcoin Cash, a separate currency with its own blockchain that trades independently of Bitcoin, and in November 2018 Bitcoin Cash experienced its own fork that resulted in the creation of yet another currency, Bitcoin SV. When a fork occurs, holders of the cryptocurrency in the original blockchain will be given units of the new forked cryptocurrency as well. If a fork occurs in the blockchain of a cryptocurrency asset in USMS custody, the USMS may end up with two separate and distinct cryptocurrency assets stemming from the originally seized asset, and both of these assets would need to be recorded and tracked independently of the other. However, the USMS does not currently have an established process for recording forked cryptocurrency in

CATS. As a result, the USMS may fail to identify and track forked assets for disposal, thereby losing income from the disposal of forfeited assets.

## **The USMS Should Implement Additional Controls Over Its Cryptocurrency Inventory Records**

Due to the limitations of tracking seized cryptocurrency in CATS documented above, the USMS has had to resort to supplemental records – spreadsheets – to manage its inventory of seized cryptocurrency. We determined that CAU actively uses these spreadsheets to conduct day-to-day management of its seized cryptocurrency assets, and even the USMS’s own policy recognizes the use of these spreadsheets for each type of cryptocurrency in its custody. Although we believe that the USMS and the DOJ require an upgraded seized asset tracking system that provides appropriate functionality for managing cryptocurrency assets, this audit nevertheless assessed the adequacy of the current, spreadsheet-based inventory records. In this section of our report, we describe two areas of risk that the USMS should address to improve controls over the inventory data managed in its spreadsheets: the spreadsheets do not track edit histories, and the USMS has not developed specific policies guiding proper use of the spreadsheets.

### **Inventory Records May Be Altered Without Detection**

The USMS’s supplemental spreadsheets do not have the capability to track edits made to the cryptocurrency entries in the USMS’s inventory records. As a result, these inventory records could be edited or deleted without a record of such a change being made and without the knowledge of individuals responsible for maintaining the spreadsheets. According to a CAU official, these spreadsheets are stored in a secure shared drive that cannot be accessed remotely. Additionally, access to the spreadsheets must be granted by the Assistant Chief of the CAU and is limited to USMS staff who work with seized cryptocurrency. While we believe these controls, if properly implemented, should effectively prevent unauthorized access to the spreadsheets, the USMS should take further action to maintain the integrity of the data stored in its inventory records. Therefore, we recommend the USMS manage its cryptocurrency inventory records in a property management system designed with the features that are necessary to maintain appropriate controls over these types of assets — particularly a system that logs edit history to prevent fraudulent alteration of the inventory records.

### **The USMS Has Not Established Guidelines for Its Inventory Records**

While USMS policy recognizes the use of spreadsheets for managing each type of seized cryptocurrency, we found that the USMS has not established more detailed guidelines on their proper use as official inventory records. In particular, the USMS does not have a requirement to periodically reconcile its cryptocurrency inventory spreadsheets with the CATS inventory records to ensure that the inventories are complete and accurate. We compared the USMS’s cryptocurrency inventory spreadsheets to the cryptocurrency inventory in CATS and identified 28 seized cryptocurrency assets in the USMS’s inventory spreadsheets that did not appear in CATS. Eleven of the 28 are non-DOJ cryptocurrency seized assets, which do not have CATS IDs, that were being tracked on the DOJ inventory spreadsheets in error. We determined that the differences between CATS and the USMS’s cryptocurrency inventory were due to tracking errors in the USMS’s spreadsheets. In our judgment, these discrepancies could have been identified and corrected earlier if the USMS periodically reconciled its cryptocurrency inventory spreadsheets to the CATS inventory. Conducting periodic reconciliations of its inventory spreadsheets and the CATS inventories could also allow the USMS to detect whether its cryptocurrency inventory records have been mistakenly or fraudulently altered.

Therefore, we recommend that the USMS, pending implementation of recommendation 1, establish policy requirements for the proper use, security, and handling of its cryptocurrency inventory spreadsheets, including a requirement to periodically reconcile its inventory spreadsheets to the CATS inventory to ensure all assets are properly accounted for in the system and that the inventory records are complete and accurate.

## **Asset Disposal Procedures Specific to Cryptocurrency Would Improve the USMS's Liquidation or Other Handling of These Assets**

We identified several issues related to the USMS's disposal of forfeited cryptocurrency, particularly the disposal of Anonymity Enhanced Cryptocurrency (AEC), cryptocurrency with minimal market value, and cryptocurrency that is not traded on the exchange used by the USMS. Prior to disposal, the USMS must receive a Declaration or Order of Forfeiture allowing the USMS to legally dispose of, or liquidate, an asset. Until 2020, the USMS disposed of seized cryptocurrency by holding sealed bid auctions for large quantities of forfeited Bitcoin. In January of 2021 CAU opened an exchange account, which is an online exchange platform for buying, selling, transferring, and storing digital currency, in order to expand their liquidation methods of forfeited cryptocurrency. This change allowed the USMS to dispose of additional types of cryptocurrency outside of Bitcoin. Of the 361 cryptocurrency assets in USMS custody during our review, we identified 15 cryptocurrency assets that cannot be disposed. Specifically, 7 of the 15 assets are AECs, 4 are not traded on the exchange, and the remaining 4 are each worth less than 10 cents, also referred to as de minimis value assets.

### **Anonymity Enhanced Cryptocurrency**

An AEC is a cryptocurrency that is transferred among users through anonymous blockchain transactions that hide their origin and destination. According to USMS, these types of currencies are known to facilitate money laundering and fund terrorism and have no legitimate business use. As a result, the DOJ Criminal Division's Money Laundering and Asset Recovery Section (MLARS) has instructed the USMS not to sell forfeited AECs, as doing so would place them back into circulation. MLARS determines whether a specific cryptocurrency is considered an AEC. However, we found that there currently are no documented processes in place guiding the USMS's: (1) communication with MLARS in identifying seized assets as AECs; (2) handling of AECs while in USMS custody; or (3) disposal of AECs once a Declaration or Order of Forfeiture is obtained. The USMS's current practice is simply to maintain custody of seized AECs in perpetuity, even after a Declaration or Order of Forfeiture is obtained, since the USMS cannot sell the asset.<sup>3</sup> This practice requires the USMS to carry the cost and administrative burden of managing these seized assets indefinitely, with little or no likelihood that these costs will later be offset by a future disposal of the AEC assets. Therefore, we recommend the USMS develop and implement formal processes and procedures to identify, handle, document, and dispose of AECs.

---

<sup>3</sup> Once the USMS awards its cryptocurrency services contract, the contractor will be responsible for the administration, management, and compliance with MLARS determination of AECs, meaning that the contractor would also be unable to sell them and would need to seek alternative means to dispose of forfeited AECs. The pending contract is discussed in [The USMS's Plans to Award a Cryptocurrency Contract Require Oversight](#) section of the report.

## Non-Exchange and De Minimis Value Assets

As previously stated, the USMS is currently in custody of eight seized cryptocurrency assets, other than AEC assets, that it cannot dispose of despite obtaining forfeiture orders for them between 2018 and 2020. Four assets are cryptocurrency types not traded on the exchange and the remaining four assets are of a de minimis value. Similar to AECs, the USMS's current practice is to maintain custody of de minimis value and non-exchange cryptocurrency in perpetuity even after a forfeiture order is obtained; the USMS stated that it is waiting to award its cryptocurrency services contract to dispose of these assets, as the contractor will be required to have the capability to dispose of all seized cryptocurrency in USMS custody. While this practice requires the USMS to carry the cost and administrative burden of holding assets indefinitely, we recognize that the USMS's inability to dispose of non-exchange and de minimis value assets will be resolved when the cryptocurrency services contract is awarded and the contractor assumes responsibility for disposal, and we therefore make no recommendation on this issue.

## The USMS Should Strengthen Its Existing Cryptocurrency Policies

While we found that the USMS generally has policies and procedures in place guiding the custody, management, and disposal of seized cryptocurrency, we identified several areas where strengthening existing policies and procedures would be beneficial to the USMS's handling of cryptocurrency. Specifically, the USMS should establish policies related to: (1) documenting quantities of cryptocurrency in both CATS and its inventory records; (2) managing new cryptocurrency inventories resulting from a blockchain fork; and (3) physical storage and safeguarding of cryptocurrency assets and wallet keys. We also identified a conflicting policy requirement and areas where the USMS is not fully complying with current policy in documenting the value of seized cryptocurrency in CATS.

## Improvements to Current Cryptocurrency Policies

We discovered that USMS policy does not require exact quantities of cryptocurrency seized to be recorded in CATS. As a result, some recorded quantities of seized cryptocurrency were approximated and may have been rounded to the nearest whole number. As the value of seized cryptocurrency in USMS custody is directly impacted by the quantities on hand, it is imperative that the USMS require exact quantities of cryptocurrency seized to be recorded in CATS. This is an issue because even a fraction of a unit of cryptocurrency can represent significant value: for example, if one Bitcoin is valued at \$50,000, then rounding off even .001 of a Bitcoin risks losing approximately \$50 of the asset's value.<sup>4</sup> Therefore, we recommend the USMS require the quantity of seized cryptocurrency be recorded in CATS, and in the USMS's inventory record down to a sufficient number of decimal places to ensure that fractional cryptocurrency units are not lost or overlooked due to rounding or approximation.

As previously mentioned, the USMS does not have an established process for recording forked cryptocurrency assets in CATS. Current USMS policy requires that when an agency seizes multiple types of cryptocurrencies, each type must be assigned its own identification number in CATS. However, during our inventory analysis, we found 10 seized assets in USMS custody tied to 5 unique identification numbers in CATS. All of these resulted from an additional cryptocurrency asset being added to the inventory due to a fork in the initially seized cryptocurrency. In our judgment, the current process of managing forked cryptocurrency under a single identification number in CATS not only violates current USMS policy, but also

---

<sup>4</sup> Bitcoin's close price value low was \$29,374.15 on 1/1/21, and its high was \$67,566.83 on 11/8/21.

presents a risk to adequate and accurate inventory control. Therefore, we recommend the USMS develop and implement policies and procedures to handle cryptocurrency forks that occur for an asset in custody, to include assigning a unique CATS identification number to the new asset.

Cryptocurrency wallets in USMS custody are required to be stored offline on encrypted thumb drives, which are held in a locked safe located in a room with controlled access, on a secure floor of a federal building that is monitored by video surveillance. Additionally, the USMS requires at least two CAU employees, one of which must be a government employee, to be present whenever the thumb drives are accessed. We witnessed CAU officials retrieving the cryptocurrency thumb drives from the safe and accessing the wallets contained on those thumb drives. In addition, we reviewed the physical security of the USMS space utilized to store the encrypted thumb drives. We also found that the USMS conducts an annual physical inventory of the cryptocurrency wallets in its custody and an annual physical inventory of the cryptocurrency wallets is conducted by third party auditors as a part of yearly financial statement audit requirements. While we determined that the USMS exercised adequate and appropriate physical controls over seized cryptocurrency, the USMS has not formally established these practices through documented policy. As a result, CAU employees may not be fully aware of expected practices in the proper handling and safeguarding of seized cryptocurrency. Therefore, we recommend the USMS establish documented policies related to the storage of, and physical controls over, seized cryptocurrency once it is transferred into USMS custody, including pertinent USMS wallet keys.

According to the DOJ Asset Forfeiture Policy Manual, once an asset is forfeited, the USMS is required to promptly sell the asset and deposit the proceeds into the Assets Forfeiture Fund. Historically, the USMS's cryptocurrency disposal process was to auction Bitcoin, which required the USMS to obtain approval to hold an auction and then advertise the auction to ensure they would attract potential buyers capable of acquiring sufficient quantities of Bitcoin. Completing these requirements and amassing large enough quantities of Bitcoin to justify an auction often dictated how long cryptocurrency assets stayed in USMS custody once they were forfeited. CAU's more recent use of its exchange account to liquidate forfeited cryptocurrency has significantly expedited the cryptocurrency disposal process. Using its exchange account, CAU is capable of liquidating cryptocurrencies in its custody immediately after forfeiture, without any of the delays that were inherent to holding an auction. Despite this, a CAU official told us that, while CAU tries to liquidate cryptocurrency as quickly as possible, the sale typically occurs between 30 and 60 days after it has been forfeited. This timeline largely is due to two factors: (1) CAU found that batching assets together is more efficient and lowers the fees it pays to the exchange; and (2) certain USMS financial reporting processes that restrict withdrawals from the exchange account near the end of each month, and because according to a USMS official CAU must not store cryptocurrency or the proceeds from sales in its exchange account for extended periods of time, those monthly restrictions on withdrawals also limit the time periods during which USMS can liquidate forfeited cryptocurrency. As a result, CAU currently must coordinate its liquidation efforts to accommodate these limiting factors, which has the effect of extending the time between forfeiture and liquidation, thereby exposing the assets to unpredictable market value fluctuations and delaying the deposit of funds into the Assets Forfeiture Fund. The USMS intends to resolve this issue using its planned cryptocurrency services contract, which will require the contractor to liquidate cryptocurrency within 5 business days of the asset being forfeited.

## Conflicting Policy and Instances of Non-Compliance

We found conflicting guidance in the USMS's cryptocurrency policy for creating the "Custody/Storage Details" record for seized assets entered into CATS. One area of the policy allows 3 days to create the record after taking physical custody of an asset, while another area allows 7 days. The USMS should correct this ambiguity in a manner that ensures custody records are created in a timely manner.

We also discovered that the USMS inconsistently complied with its policy for documenting the appraised value of seized cryptocurrency in its custody. USMS policy requires CAU to enter the USMS-appraised value into the "Comments" section of the CATS appraisal screen using the following language: "Appraisal based on a close market price of \$\_\_\_\_/ (type of cryptocurrency) multiplied by \_\_\_\_ (amount of cryptocurrency) in custody." Of the 361 cryptocurrency assets in USMS custody during our review, we found that 58 did not have any appraised value recorded in the CATS documents provided by CAU, and none of the remaining 303 assets documented the valuation using the prescribed language in USMS policy. In our judgment, it is important that the CATS records include both the quantity and appraised value of cryptocurrency assets transferred into USMS custody. Therefore, we recommend the USMS ensure all CAU employees are familiar with established policies on appraising and recording the value of seized cryptocurrency.

## The USMS's Plans to Award a Cryptocurrency Contract Require Oversight

The USMS intends to award a contract for cryptocurrency services to a small business that will be required to provide a full range of cryptocurrency management and disposal services including, but not limited to, accounting, customer management, audit compliance, managing blockchain forks, wallet creation and management, private encryption key generation and safekeeping, backup and recovery of private encryption key material, as well as future actions associated with the cryptocurrency forfeiture process. Since 2020, the USMS has attempted to award this contract on two separate occasions, but both awards were protested and later rescinded because the awardee was not a small business.

At the time of our audit, the USMS had not yet awarded the cryptocurrency services contract; therefore, we were unable to assess the contractor's performance, or the USMS's oversight of the contractor. We assessed the contract Performance Work Statement, which details the required actions the contract awardee will be obligated to perform, and the USMS's plan for conducting contract oversight, and found that the Performance Work Statement contains adequate requirements that, if properly implemented by the contract awardee, should ensure seized virtual currencies are adequately managed and safeguarded. Additionally, we did not identify concerns with the contract Quality Assurance Surveillance Plan performance standards that the USMS will use to evaluate the contract awardee's performance. However, in our judgment, the USMS needs to establish seized cryptocurrency policies and procedures related to inventory management, asset storage, quantification, valuation, and disposal, as described above, prior to handing over its seized cryptocurrency responsibilities to a contractor.

## Conclusion and Recommendations

The USMS has implemented adequate safeguards over its storage and access to seized cryptocurrency in its custody. However, the USMS should implement a seized property management system with appropriate functionality for managing cryptocurrency assets. Additionally, several improvements would strengthen controls over cryptocurrency assets in USMS custody, particularly regarding establishing guidelines for the proper storage, documenting, tracking, and disposal of seized cryptocurrency. With the USMS's ongoing effort to outsource the management of its seized cryptocurrency, it is imperative that the USMS document its required cryptocurrency management practices in policies. Based on our findings, we make seven recommendations to improve the USMS's management of seized cryptocurrency.

We recommend that the USMS:

1. Manage its cryptocurrency inventory records in a property management system designed with the features that are necessary to maintain appropriate controls over these types of assets — particularly a system that logs edit history to prevent fraudulent alteration of the inventory records.
2. Pending implementation of recommendation 1, establish policy requirements for the proper use, security, and handling of its cryptocurrency inventory spreadsheets, including a requirement to periodically reconcile its inventory spreadsheets to the CATS inventory to ensure all assets are properly accounted for in the system and that the inventory records are complete and accurate.
3. Develop and implement formal processes and procedures to identify, handle, document, and dispose of AECs.
4. Require the quantity of seized cryptocurrency be recorded in CATS, and in the USMS's inventory record down to a sufficient number of decimal places to ensure that fractional cryptocurrency units are not lost or overlooked due to rounding or approximation.
5. Develop and implement policies and procedures to handle cryptocurrency forks that occur for an asset in custody, to include assigning a unique CATS identification number to the new asset.
6. Establish documented policies related to the storage of, and physical controls over, seized cryptocurrency once it is transferred into USMS custody, including pertinent USMS wallet keys.
7. Ensure all CAU employees are familiar with established policies on appraising and recording the value of seized cryptocurrency.

# APPENDIX 1: Objective, Scope, and Methodology

## Objective

The objective of the audit was to evaluate the USMS's management of seized cryptocurrency.

## Scope and Methodology

Our audit covers the USMS's management of seized cryptocurrency from June 2017 to September 2021. To accomplish our objective, we visited the CAU office to observe physical controls and safeguards over seized cryptocurrency. Additionally, we interviewed USMS personnel, including officials from CAU and the Asset Forfeiture Division's Real Property Unit. We analyzed the effectiveness of current controls over seized cryptocurrency. We also evaluated DOJ and USMS policies and procedures related to cryptocurrency seizures and reviewed seized cryptocurrency inventory records to ensure they adhered to policy requirements. Finally, we assessed the performance work statement for the USMS's planned cryptocurrency services contract to ensure it aligned with current USMS controls over seized cryptocurrency.

## Statement on Compliance with Generally Accepted Government Auditing Standards

We conducted this performance audit in compliance 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

## Internal Controls

In this audit, we performed testing of internal controls significant within the context of our audit objective. We did not evaluate the internal controls of USMS to provide assurance on its internal control structure as a whole. USMS management is responsible for the establishment and maintenance of internal controls in accordance with OMB Circular A-123. Because we do not express an opinion on the USMS's internal control structure as a whole, we offer this statement solely for the information and use of the USMS.<sup>5</sup>

In planning and performing our audit, we identified internal control components and underlying internal control principles as significant to the audit objective. Specifically, we assessed the design, implementation, and operating effectiveness of USMS's written policies and process controls pertaining to aspects of seized cryptocurrency management within our scope. The internal control deficiencies we found are discussed in the Audit Results section of this report. However, because our review was limited, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

## Sample-Based Testing

To accomplish our audit objective, we performed sample-based testing to select samples to obtain an understanding of the documentation the USMS used to manage their seized cryptocurrency in CATS. In this

---

<sup>5</sup> This restriction is not intended to limit the distribution of this report, which is a matter of public record.

effort, we employed a judgmental sampling design to obtain broad exposure to numerous facets of the areas we reviewed. This non-statistical sample design did not allow projection of the test results to the universe from which the samples were selected.

### **Computer-Processed Data**

During our audit, we obtained information from the Consolidated Assets Tracking System. We did not test the reliability of the system as a whole; therefore, any findings identified involving information from systems were verified with documentation from other sources.

## APPENDIX 2: The USMS Response to the Draft Audit Report



U.S. Department of Justice  
United States Marshals Service  
*Office of Professional Responsibility*

Washington, DC 20530-0001

May 23, 2022

MEMORANDUM TO: Jason R. Malmstrom  
Assistant Inspector General for Audit  
Office of the Inspector General

FROM: Ronald Carter                      RONALD  
Acting Assistant Director          CARTER                      Digitally signed by  
RONALD CARTER  
Date: 2022.05.23  
11:17:57 -0400

SUBJECT: United States Marshals Service Response to Audit Report: Audit  
of the United States Marshals Service's Management of Seized  
Cryptocurrency

In response to recent correspondence from the Office of the Inspector General regarding the subject report, attached is the United States Marshals Service's response to the Formal Draft Audit Report.

Should you have any questions, please contact Awilda Martinez, External Audit Liaison, at 703-517-3783.

### Attachment

cc: Kimberly Rice  
Regional Audit Manager  
Office of the Inspector General

Victoria E. Miller  
Senior Analyst  
Homeland Security and Justice Team  
Government Accountability Office

Louise Duhamel  
Assistant Director, Audit Liaison Group  
Internal Review and Evaluation Office  
Justice Management Division

Silas V. Darden  
Chief of Staff  
United States Marshals Service

**United States Marshals Service**  
**Review of the Marshals Service's Management of Seized Cryptocurrency**

**Recommendation 1: Manage its cryptocurrency inventory records in a property management system designed with the features that are necessary to maintain appropriate controls over these types of assets- particularly a system that logs edit history to prevent fraudulent alteration of the inventory records.**

**USMS Response:** The United States Marshals Service (USMS) concurs with this recommendation. Beginning in October 2021, the USMS expanded its use of a free text space in the Department of Justice-wide asset tracking system, CATS, for cryptocurrency assets in a way that allowed for enhanced reporting, provided a logging system for alterations of any records, and documented various asset descriptors (i.e., token type, units in USMS custody, and hardware location). The USMS will work with the Justice Management Division's (JMD) Asset Forfeiture Management System (AFMS) to enhance CATS to include dedicated fields for tracking cryptocurrency. In addition, the USMS is in the process of creating a database to house all requests for wallet addresses and issued wallet addresses in a single location. This database will include a tracking log to document any input and alterations to the data. Both systems will provide restrictions that will not allow deletions prior to multi-level approvals. The USMS expects to resolve this recommendation by December 31, 2022.

**Recommendation 2: Pending implementation of recommendation 1, establish policy requirements for the proper use, security, and handling of its cryptocurrency inventory spreadsheets, including a requirement to periodically reconcile its inventory spreadsheets to the CATS inventory to ensure all assets are properly accounted for in the system and that the inventory records are complete and accurate.**

**USMS Response:** The USMS concurs with this recommendation. The use of spreadsheets to track our cryptocurrency inventory was discontinued in October 2021 (see response to Recommendation #1). The USMS has drafted multiple standard operating procedures (SOP) on the custody, management, and disposal of cryptocurrency assets. One of the management SOPs includes requirements to periodically monitor changes to inventory and to perform existence and completeness testing to ensure inventory records are complete and accurate. The USMS expects to resolve this recommendation by September 30, 2022.

**Recommendation 3: Develop and implement formal processes and procedures to identify, handle, document, and dispose of AECs.**

**USMS Response:** The USMS concurs with this recommendation. The USMS published a SOP containing a cryptocurrency classification list on March 25, 2022. Enhanced Coins (AEC) are classified as cryptocurrencies that the USMS no longer accepts for custody or disposal per the DOJ's [Asset Forfeiture Policy Manual](#). For AECs to be liquidated or converted, approval from the Money Laundering and Asset Recovery Section (MLARS) is required per the Asset Forfeiture Policy Manual, Chapter 2: Seizure and Restraint (B.3 Disposition, 2021). MLARS

policy does not specify which cryptocurrencies are AECs because cryptocurrencies can move to a transparent, publicly viewable blockchain which would change the classification of the coin to a non-AEC. The USMS will work to develop and implement a formal process to address AECs, including legacy AECs currently in USMS custody, by December 31, 2022.

**Recommendation 4: Require the quantity of seized cryptocurrency be recorded in CATS, and in the USMS's inventory record down to a sufficient number of decimal places to ensure that fractional cryptocurrency units are not lost or overlooked due to rounding or approximation.**

**USMS Response:** The USMS concurs with this recommendation. The USMS does not round or approximate the cryptocurrency in our custody. The USMS will work with the JMD, AFMS to enhance CATS to track exact quantities seized and quantities transferred to the USMS with the capability to stack records and provide a historical view of the asset through its lifecycle. The USMS expects to resolve this recommendation by December 31, 2022.

**Recommendation 5: Develop and implement policies and procedures to handle cryptocurrency forks that occur for an asset in custody, to include assigning a unique CATS identification number to the new asset.**

**USMS Response:** The USMS concurs with this recommendation. The USMS will work with AFMS, MLARS, and seizing agencies to foster the creation of policies and procedures on forked currency that mirrors the current split forfeiture process that is currently in use with other asset types. The USMS expects to resolve this recommendation by January 31, 2023.

**Recommendation 6: Establish documented policies related to the storage of, and physical controls over, seized cryptocurrency once it is transferred into USMS custody, including pertinent USMS wallet keys.**

**USMS Response:** The USMS concurs with this recommendation. The USMS has drafted, and continues to update, multiple SOPs on the custody, management, and disposal of cryptocurrency assets and the SOPs will address the Office of the Inspector General's specific recommendations related to the storage of and physical controls over seized cryptocurrency. The USMS expects to resolve this recommendation by September 30, 2022.

**Recommendation 7: Ensure all CAU employees are familiar with established policies on appraising and recording the value of seized cryptocurrency.**

**USMS Response:** The USMS concurs with this recommendation. The updated SOP for appraising and recording the value of cryptocurrency in USMS custody has been drafted. The SOP establishes valuation sources, timeframes, and data entry requirements. All current Complex Assets Unit (CAU) employees are familiar with established SOPs and are aware of the changes drafted in the updated SOP. CAU employees handling cryptocurrency will be asked to annually acknowledge their adherence to established policies on appraising and recording the value of seized cryptocurrency. The USMS expects to resolve this recommendation by December 1, 2022.

## **APPENDIX 3: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Report**

The OIG provided a draft of this audit report to the USMS. The USMS's response is incorporated as Appendix 2 of this final report. In response to our draft audit report, the USMS concurred with our recommendations and discussed the actions it will implement in response to our findings. As a result, the audit report is resolved. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

### **Recommendation for the USMS:**

- 1. Manage its cryptocurrency inventory records in a property management system designed with the features that are necessary to maintain appropriate controls over these type of assets — particularly a system that logs edit history to prevent fraudulent alteration of the inventory records.**

Resolved. The USMS concurred with our recommendation. The USMS stated in its response that the USMS will work with the Justice Management Division's (JMD) Asset Forfeiture Management System (AFMS) to enhance CATS to include dedicated fields for tracking cryptocurrency. Additionally, the USMS stated that it is in the process of creating a database to house all requests for wallet addresses and issued wallet addresses in a single location. The USMS noted that it expects to resolve this recommendation by December 31, 2022. As a result, this recommendation is resolved.

This recommendation can be closed when we receive evidence that the USMS is managing its cryptocurrency inventory records in a property management system designed with the features that are necessary to maintain appropriate controls over these type of assets — particularly a system that logs edit history to prevent fraudulent alteration of the inventory records.

- 2. Pending implementation of recommendation 1, establish policy requirements for the proper use, security, and handling of its cryptocurrency inventory spreadsheets, including a requirement to periodically reconcile its inventory spreadsheets to the CATS inventory to ensure all assets are properly accounted for in the system and that the inventory records are complete and accurate.**

Resolved. The USMS concurred with our recommendation. The USMS stated in its response that the use of spreadsheets to track their cryptocurrency inventory was discontinued in October 2021. Additionally, the USMS stated that it has drafted multiple standard operating procedures related to cryptocurrency and one of them includes requirements to periodically monitor changes to inventory and to perform existence and completeness testing to ensure inventory records are complete and accurate. The USMS noted that it expects to resolve this recommendation by September 30, 2022. As a result, this recommendation is resolved.

This recommendation can be closed when we receive evidence that the USMS has developed and implemented policy requirements for the proper use, security, and handling of its cryptocurrency inventory, including a requirement to periodically reconcile its inventory to ensure all assets are properly accounted for in the system and that the inventory records are complete and accurate.

3. **Develop and implement formal processes and procedures to identify, handle, document, and dispose of AECs.**

Resolved. The USMS concurred with our recommendation. The USMS stated in its response that the USMS no longer accepts AECs for custody or disposal. The USMS stated that the USMS will work to develop and implement a formal process to address AECs, including legacy AECs currently in USMS custody, by December 31, 2022. As a result, this recommendation is resolved.

This recommendation can be closed when we receive evidence that the USMS has developed and implemented processes and procedures to identify, handle, document, and dispose of AECs.

4. **Require the quantity of seized cryptocurrency be recorded in CATS, and in the USMS's inventory record down to a sufficient number of decimal places to ensure that fractional cryptocurrency units are not lost or overlooked due to round or approximation.**

Resolved. The USMS concurred with our recommendation. The USMS stated in its response that it does not round or approximate the cryptocurrency in their custody. Additionally, the USMS stated that the USMS will work with the JMD AFMS to enhance CATS to track exact quantities seized and quantities transferred to the USMS with the capability to stack records and provide a historical view of the asset through its lifecycle. The USMS noted that it expects to resolve this recommendation by December 31, 2022. As a result, this recommendation is resolved.

This recommendation can be closed when we receive evidence that the USMS has developed and implemented policies requiring the quantity of seized cryptocurrency be recorded in CATS, and in the USMS's inventory record down to a sufficient number of decimal places to ensure that fractional cryptocurrency units are not lost or overlooked due to round or approximation.

5. **Develop and implement policies and procedures to handle cryptocurrency forks that occur for an asset in custody, to include assigning a unique CATS identification number to the new asset.**

Resolved. The USMS concurred with our recommendation. The USMS stated in its response that the USMS will work with AFMS, MLARS, and seizing agencies to foster the creation of policies and procedures on forked currency that mirror the current split forfeiture process that is currently in use with other asset types. The USMS noted that it expects to resolve this recommendation by January 31, 2023. As a result, this recommendation is resolved.

This recommendation can be closed when we receive evidence that the USMS has developed and implemented policies and procedures to handle cryptocurrency forks that occur for an asset in custody, to include assigning a unique CATS identification number to the new asset.

6. **Establish documented policies related to the storage of, and physical controls over, seized cryptocurrency once it is transferred into USMS custody, including pertinent USMS wallet keys.**

Resolved. The USMS concurred with our recommendation. The USMS stated in its response that it has drafted, and continues to update, multiple standard operating procedures (SOPs) on the custody, management, and disposal of cryptocurrency assets. The USMS noted that it expects to resolve this recommendation by September 30, 2022. As a result, this recommendation is resolved.

This recommendation can be closed when we receive evidence that the USMS has developed and implemented policies related to the storage of, and physical controls over, seized cryptocurrency once it is transferred into USMS custody, including pertinent USMS wallet keys.

7. **Ensure all CAU employees are familiar with established policies on appraising and recording the value of seized cryptocurrency.**

Resolved. The USMS concurred with our recommendation. The USMS stated in its response that the USMS has drafted an updated SOP for appraising and recording the value of cryptocurrency in USMS custody. Additionally, the USMS stated that the SOP establishes valuation sources, timeframes, and data entry requirements and all current CAU employees are familiar with established SOPs and are aware of the changes drafted in the updated SOP. The USMS stated that CAU employees handling cryptocurrency will be asked to annually acknowledge their adherence to established policies on appraising and recording the value of seized cryptocurrency. The USMS noted that it expects to resolve this recommendation by December 1, 2022. As a result, this recommendation is resolved.

This recommendation can be closed when we receive evidence that all USMS CAU employees are familiar with established policies on appraising and recording the value of seized cryptocurrency.