

**U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
HOMELAND SECURITY INVESTIGATIONS**

HSI Directive 18-04: Seizure and Forfeiture of Cryptocurrency

Issue Date: August 16, 2018

Effective Date: August 16, 2018

Superseded: None.

Federal Enterprise Architecture Number: 306-112-002b

- 1. Purpose/Background.** Cryptocurrency seizures and forfeitures have become increasingly common in U.S. Immigration and Customs Enforcement, Homeland Security Investigations (HSI). Cryptocurrency is an encrypted, decentralized digital currency or asset that can be bought, sold, and traded for U.S. dollars or other currencies, and used as a medium of exchange to purchase goods and services. This Directive provides HSI field offices with guidance regarding the seizure, handling, tracking, and final disposition of all forms of cryptocurrency.
- 2. Policy.** It is the policy of HSI to ensure that all cryptocurrency seizures are handled in a consistent and secure manner that mitigates the Government's liability and protects all parties' interest in the asset. This Directive establishes the roles and responsibilities related to the seizure, custody, storage, and disposition of cryptocurrency. HSI field offices are required to follow the guidance provided in this Directive in investigations that involve the seizure and forfeiture of cryptocurrency.
- 3. Definitions.** The following definitions apply for the purposes of this Directive only:

 - 3.1. Address.** A string of alphanumeric characters that is transmitted, unencrypted, to a destination or storage location for digital currency (also known as a public key).
 - 3.2. Altcoin.** All cryptocurrencies other than Bitcoin.
 - 3.3. Anonymity Enhanced Cryptocurrencies (AECs).** Cryptocurrencies that use integrated technology, such as mixers and tumblers, to enhance anonymity and obscure virtual currency addresses and transactional history. This type of cryptocurrency can be utilized for the specific purpose of eluding law enforcement.
 - 3.4. Bitcoin.** A type of decentralized cryptocurrency that can be bought, sold, and traded for U.S. dollars or other currencies, and used as a medium of exchange to purchase goods and services. Bitcoin was launched in 2009 to provide a method for processing financial transactions securely without the use of a central authority or traditional banking system. Bitcoins can be identified by the abbreviations BTC and XBT.
 - 3.5. Blockchain.** A public ledger of all transactions for a digital currency.

- 3.6. Centralized Exchanges.** Digital currency transactions performed under the authority of a single figure, group, or platform.
- 3.7. Cold Storage.** A data storage method that is not directly connected to a computer or alternate processing unit (also known as “offline wallet” or hardware wallet).
- 3.8. Cryptocurrency.** A type of decentralized digital currency or asset that can be bought, sold, and traded for U.S. dollars or other currencies, and used as a medium of exchange to purchase goods and services.
- 3.9. Cryptocurrency Exchange Platform.** A business that allows customers to buy, sell, and trade digital currencies. Exchange platforms have also been identified as Money Services Businesses and are required to be registered by the Financial Crimes Enforcement Network (FinCEN), unless a limitation to or exemption from the definition of “money transmitter” applies.¹
- 3.10. Decentralized Exchanges.** Digital currency transactions performed absent the authority of a single figure, group, or platform.
- 3.11. Digital Currency.** A centralized or decentralized digital representation of value that is issued by neither a central bank nor a public authority but is accepted by persons as a means of payment or is exchanged based on its value and can be transferred, stored, and traded electronically. Virtual currency and cryptocurrency are types of digital currency. For the purpose of seizure and forfeiture, HSI treats digital currency as high-risk tangible property.
- 3.12. Fiat Currency.** Refers to currency authorized or adopted by a government as a part of its currency (also known as legal tender or money).
- 3.13. Liquidation.** The process of converting digital currency into fiat currency.
- 3.14. Mixers.** Cryptocurrency mixers are special services used to obfuscate transaction trails, maintain privacy, and/or mask illicit activity (also known as “tumblers”).
- 3.15. Offline Wallet.** A wallet used to securely store unused digital currency offline from a connected network (also known as cold storage).
- 3.16. Online Wallet.** A digital wallet used to store unused cryptocurrency on a connected network, whose private keys are controlled by a third party (also known as a “hot wallet”).

¹ FinCEN’s regulations provide that whether a person is a money transmitter is a matter of facts and circumstances. The regulations identify six circumstances under which a person is not a money transmitter, despite accepting and transmitting currency, funds, or value that substitutes for currency. Title 31, Code of Federal Regulations (C.F.R.) Section 1010.100(ff)(5)(ii)(A)–(F).

- 3.17. Private Key.** A digital code (key) which is encrypted and only known by the intended recipient or owner. The private key is used to “sign” an outgoing transaction.
- 3.18. Public Key.** Half of an asymmetric key pair represented as an address. Each public key has a corresponding private key.
- 3.19. Screenshot.** A digital image copy of the screen of a computer monitor, telephone, or other visual output device (also known as a screen capture or screen grab).
- 3.20. Recovery Seed.** A list of words which store the information needed to recover a cryptocurrency wallet (also known as a mnemonic phrase).
- 3.21. Virtual Currency.** A type of centralized or decentralized digital currency having a medium of exchange that operates like currency.
- 3.22. Wallet.** A software application or other mechanism used to manage addresses and conduct transactions with a digital currency. A wallet is also used for holding, storing, and transferring a digital currency.
- 4. Responsibilities.**
- 4.1.** The **Executive Associate Director of HSI** is responsible for the oversight of the policy and procedures in this Directive.
- 4.2.** The **Deputy Assistant Director, Investigative Services Division**, is responsible for ensuring the implementation of the provisions of this Directive within HSI.
- 4.3.** The **Unit Chief, Asset Forfeiture Unit (AFU)**, is responsible for implementing the provisions of this Directive within HSI.
- 4.4.** The **Special Agents in Charge** are responsible for implementing the provisions of the Directive within their respective areas of responsibility.
- 4.5.** **Special Agents (SAs)** are responsible for complying with the provisions of this Directive.
- 4.6.** The **United States Marshals Service (USMS)** provides “cold” storage for Bitcoins.
- 4.7.** The **Fines, Penalties and Forfeitures Office (FPFO)** is responsible for processing seized and forfeitable cryptocurrency and “cold” storage of altcoins.
- 4.8.** **Seized Property Specialists (SPSs)** are responsible for the temporary storage of seized and forfeitable cryptocurrency.

5. Procedures/Requirements.

5.1. **Seizure/Storage of Bitcoins.** Upon seizure of Bitcoins, the SA (b) (7)(E) (b) (7)(E) Subsequent to notification, the SA must request, through AFU, a Bitcoin wallet for cold storage of the seized Bitcoin(s). (b) (7)(E) new Bitcoin wallet for each seizure. The following information is required when requesting a wallet (b) (7)(E) for transfer of Bitcoin seizures:

- 1) Applicable seizure documents;
- 2) Date of seizure;
- 3) (b) (7)(E)) incident number, or seizure/incident number from another agency if adopting a seizure;
- 4) Public Key of the wallet from which Bitcoins are to be transferred;
- 5) Exact quantity of Bitcoins seized; and
- 6) Field office POC.

USMS will create and provide a unique wallet in accordance with each request and provide the public key (b) (7)(E). One wallet will be created per Search, Arrest, and Seizure (b) (7)(E) report. Bitcoins documented on separate (b) (7)(E) reports must not be combined when making transfers to a USMS wallet. Wallets provided by USMS will be the only long-term storage used for Bitcoins. USMS is responsible for the maintenance and disposition of all Bitcoins seized by HSI SAs that are subsequently forfeited or remitted. Once (b) (7)(E) the public key to the SA, the SA will initiate the transfer of the Bitcoins to USMS and (b) (7)(E) with the following information:

- 1) The date of transfer;
- 2) The exact number of Bitcoins transferred; and
- 3) Screenshots documenting the transfer of the Bitcoins (all screenshots must clearly capture the transactional hash).

Seized Bitcoins must be turned over to USMS (b) (7)(E) from the date of seizure, pending forfeiture. This policy creates a limited exception to the guidance set forth in Section 12.3, "Storage of High Risk Evidence," of the *Evidence Handbook* (HSI Handbook (HB) 15-05), dated November 19, 2015, or as updated, as well as guidance set forth in Section 2.8.20, "Timeframes for Property Transfer," of the *Seized Asset Management and Enforcement Procedures Handbook* (SAMEPH) (U.S. Customs and Border Protection (CBP) HB 4400-01B), dated July 2011, or as updated. HSI will not

store seized Bitcoins, (b) (7)(E)

This policy allows for exceptions where investigative activities preclude SAs from complying with the (b) (7)(E) requirement; however, it is the responsibility of the Group Supervisor to obtain a written temporary storage waiver (b) (7)(E) before the expiration of the (b) (7)(E) requirement. The request must include justification for the delay, as well as the expected date the property will be transferred to USMS.

Recovery seeds, hardware wallets, and electronic devices (related to Bitcoin seizures) held by HSI offices, pursuant to a temporary storage waiver, must be placed in an agency approved evidence bag, sealed with Department of Homeland Security (DHS) Form 366A, *Evidence*, and transferred to the SPS. Documents containing private keys and recovery seeds must be placed in an opaque envelope, prior to being placed in an agency approved evidence bag. These assets will be maintained in accordance with the guidance set forth in Sections 8.5, "Identification of Evidence," and 8.6, "Packaging and Sealing Evidence," of the *Evidence Handbook* (HSI HB 15-05), dated November 19, 2015, or as updated, as well as guidance set forth in Sections 2.8.15, "Property Verification and Handling," and 2.8.16, "Packaging Requirements," of the SAMEPH (CBP HB 4400-01B), dated July 2011, or as updated. Recovery seeds, hardware wallets, and electronics devices must be held in a secured property storage area, within a safe, and segregated from other evidence.

(Note: HSI SAs seeking pre-seizure wallets should contact (b) (7)(E) information regarding approved temporary storage options for anticipated cryptocurrency seizures.)

5.2. Forfeiture/Disposition of Bitcoins. All seized Bitcoins must undergo respective administrative, civil, or criminal forfeiture proceedings prior to liquidation.

Bitcoins seized pursuant to a finding of probable cause or via a warrant should be documented on an (b) (7)(E) report in (b) (7)(E). The seizing SA will determine whether the case should undergo administrative, civil, or criminal forfeiture and utilize the appropriate (b) (7)(E) Legal Status (b) (7)(E) Bitcoins obtained through abandonment must be documented on an (b) (7)(E) in (b) (7)(E) and use the (b) (7)(E) status code.

SAs must contact their local CBP FPFO to initiate the Administrative Forfeiture process within (b) (7)(E) of the date of seizure. Bitcoins obtained through abandonment using DHS Form 4607, *Notice of Abandonment and Assent to Forfeiture of Prohibited or Seized Merchandise*, must also undergo the Administrative Forfeiture process administered by CBP FPFO. SAs are responsible for coordinating cases among the Assistant United States Attorney (AUSA), the local FPFO, and the Office of the Principal Legal Advisor (OPLA).

Upon forfeiture of Bitcoins, SAs must (b) (7)(E) with a forfeiture order and any other supporting documentation deemed applicable. (b) (7)(E) coordinate the liquidation of forfeited Bitcoins with USMS. USMS will conduct periodic auctions to sell Bitcoins. Proceeds from the sale of Bitcoins will be deposited into the Treasury Forfeiture Fund (TFF) and credit applied to HSI.

5.3. Returning Bitcoins to a Defendant or a Claimant. In the event that Bitcoins are to be returned to a defendant or a claimant, the SA must provide (b) (7)(E) the following information:

- 1) (b) (7)(E) Incident number;
- 2) Authorizing document;
- 3) Associated USMS public key;
- 4) Exact number of the Bitcoins to be returned;
- 5) Public Key of the agency wallet where Bitcoins are to be transferred; and
- 6) The date of return.

USMS will transfer the specified Bitcoins back to HSI. The SAs must then transfer the Bitcoins to the defendant's and/or the claimant's wallet.

5.4. Seizure/Storage of Altcoins. Upon seizure of altcoins, the SA will notify the designated (b) (7)(E) POC within (b) (7)(E). Subsequent to notification, (b) (7)(E) (b) (7)(E) if the altcoin is approved for cold storage by USMS. Altcoins accepted by USMS must follow the same procedures established for Bitcoin seizures in Sections 5.1 and 5.2 of this Directive. Altcoins that are not approved for storage by USMS will be placed in cold storage and transferred to the CBP FPFO. For these seizures, (b) (7)(E) (b) (7)(E) SA with instructions regarding generation of a recovery seed to preserve the seized asset and/or electronic/hardware devices. The following information is required when requesting assistance (b) (7)(E) with altcoin seizures:

- 1) Applicable seizure documents;
- 2) The date of seizure;
- 3) (b) (7)(E) incident number, or seizure/incident number from another agency if adopting a seizure;
- 4) Name and symbol of altcoin;
- 5) Public key of the wallet from which altcoins are to be transferred;

- 6) Exact quantity of altcoins seized; and
- 7) Field office POC.

Seized altcoins must be turned over to CBP FPFO for (b) (7)(E) (b) (7)(E) from the date of seizure, pending forfeiture. This policy creates a limited exception to the guidance set forth in Section 12.3, "Storage of High Risk Evidence," of the *Evidence Handbook* (HSI HB 15-05), dated November 19, 2015, or as updated, as well as guidance set forth in Section 2.8.20, "Timeframes for Property Transfer," of the SAMEPH (CBP HB 4400-01B), dated July 2011, or as updated. Altcoins transferred to the CBP FPFO must be accompanied by a completed DHS Form 6051S, *Custody Receipt for Seized Property and Evidence*, and an approved (b) (7)(E) report. HSI will not store seized altcoins, which are classified as high-risk property, in seized property/evidence rooms (b) (7)(E)

This policy allows for exceptions where investigative activities preclude SAs from complying (b) (7)(E) however, it is the responsibility of the Group Supervisor to obtain a written temporary storage waiver from (b) (7)(E) (b) (7)(E). The request must include justification for the delay, as well as the expected date the property will be transferred to USMS or to the CBP FPFO.

Recovery seeds, hardware wallets, and electronics devices (related to altcoin seizures), must be placed in an agency approved evidence bag and sealed with DHS Form 366A, *Evidence*, prior to being transferred to the SPS or CBP FPFO. Documents containing private keys and recovery seeds must be placed in an opaque envelope prior to being placed in an agency approved evidence bag. Altcoins seizures held by HSI Offices, pursuant to a temporary storage waiver, must be maintained in accordance with the guidance set forth in Sections 8.5, "Identification of Evidence," and 8.6, "Packaging and Sealing Evidence," of the *Evidence Handbook* (HSI HB 15-05), dated November 19, 2015, or as updated, as well as guidance set forth in Sections 2.8.15, "Property Verification and Handling," and 2.8.16, "Packaging Requirements," of the SAMEPH (CBP HB 4400-01B), dated July 2011, or as updated. (b) (7)(E)

(b) (7)(E)
(b) (7)(E)

(Note: HSI SAs seeking pre-seizure wallets should (b) (7)(E) for information regarding approved temporary storage options for anticipated cryptocurrency seizures.)

5.5. Forfeiture/Disposition of Altcoins. All seized altcoins must undergo respective administrative, civil, or criminal forfeiture proceedings prior to liquidation.

Altcoins seized pursuant to a finding of probable cause or via a warrant must be documented on an (b) (7)(E) report in (b) (7)(E). The seizing SA will determine whether the case must undergo administrative, civil, or criminal forfeiture and utilize the appropriate

(b) (7)(E) Legal Status **(b) (7)(E)** ”). Altcoins obtained through abandonment should be documented on an **(b) (7)(E)** in **(b) (7)(E)** and use the **(b) (7)(E)** status code.

SAs must contact their local CBP FPFO to initiate the Administrative Forfeiture process **(b) (7)(E)** Altcoins obtained through abandonment using DHS Form 4607, *Notice of Abandonment and Assent to Forfeiture of Prohibited or Seized Merchandise*, must also undergo the Administrative Forfeiture process administered by CBP FPFO. SAs are responsible for coordinating cases among the AUSA, the local FPFO, and OPLA.

Upon forfeiture of altcoins, SAs **(b) (7)(E)** with a forfeiture order and any other supporting documentation deemed applicable.

(b) (7)(E) the liquidation of forfeited altcoins held by USMS in cold storage. USMS will conduct periodic auctions to sell altcoins. Proceeds from the sale of altcoins will be deposited into the TFF and credit applied to HSI.

5.6. Returning Altcoins to Defendant or Claimant. In the event that altcoins are to be returned to a defendant or a claimant, the SA will transfer the altcoins to the defendant’s or claimant’s wallet. Altcoins held by USMS will be transferred back to HSI. The SA must then transfer the altcoins to the defendant’s and/or the claimant’s wallet. In both instances, the SA must provide **(b) (7)(E)** the following information:

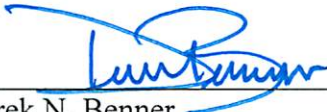
- 1) **(b) (7)(E)** Incident number;
- 2) Authorizing document;
- 3) Associated USMS public key;
- 4) Exact number of altcoins to be returned;
- 5) Public Key of agency wallet where the altcoins are to be transferred; and
- 6) The date of return.

5.7. Local Liquidation of Seized Cryptocurrency. **(b) (7)(E)** local liquidation of altcoins held in cold storage by CBP FPFO (for example, in accordance with a pre-forfeiture court ordered sale or consent to liquidate). Local liquidation, conversion of cryptocurrency and/or use of alternate disposal methods (such as the use of a cryptocurrency exchange platforms) must be approved by the AFU Unit Chief.

Proceeds from the sale of locally liquidated altcoins will be deposited into the TFF and credit applied to HSI.

- 5.8. Anonymity Enhanced Cryptocurrencies.** Seized AECs will be evaluated for liquidation on a case-by-case basis. AECs not approved for liquidation may be requested for Retention as a Special Class of Property to be used in the furtherance of certified undercover investigations. Request for Retention of AECs must be submitted in accordance with the guidance set forth in Chapter 9, “Procedures for Submitting Retention Request,” of the *Retention of Forfeited Property Handbook* (HSI HB 11-04), dated September 12, 2011, or as updated.
- 5.9 (b) (7)(E) Cryptocurrency Entries.** HSI classifies cryptocurrency as high-risk tangible property. Cryptocurrency must be entered into **(b) (7)(E)** Category Code **(b) (7)(E)** and Property Type **(b) (7)(E)** (Note: SAs may contact AFU for additional guidance concerning cryptocurrency **(b) (7)(E)** entries.)
- 5.10. Program Codes.** Project Code^{(b) (7)(E)} must be applied to investigations involving the seizure and forfeiture of Virtual Currency.
- 5.11. (b) (7)(E)**
- 6. Recordkeeping. (b) (7)(E)**
- The SA assigned to each cryptocurrency operation will also be responsible for maintaining a separate physical and electronic copy of the legal and financial documents related to the seizure, custody, storage, transfer, and forfeiture of all digital currency. The SA must also maintain a record of the following:
- 1) Name and symbol of seized Bitcoin or altcoin;
 - 2) Public/private addresses;
 - 3) Transfer dates;
 - 4) Quantity of digital currency transferred;
 - 5) Digital currency exchange fees; and
 - 6) Screenshots of digital currency transactions
- 7. Authorities/References.**
- 7.1. (b) (7)(E)**

- 7.2. HSI HB 15-05, *Evidence Handbook*, dated November 9, 2015, or as updated.
- 7.3. HSI HB 11-04, *Retention of Forfeited Property Handbook*, dated September 12, 2011, or as updated.
- 7.4. CBP HB 4400-01B, *Seized Asset Management and Enforcement Procedures Handbook*, dated July 2011, or as updated.
- 7.5. Treasury Executive Office for Asset Forfeiture Directive 10, *Management of Seized and Forfeited Bitcoin*, dated August 17, 2016, or as updated.
- 8. **Attachments.** None.
- 9. **No Private Right.** This document provides only internal HSI policy guidance, which may be modified, rescinded, or superseded at any time without notice. It is not intended to, does not, and may not be relied upon to create any right or benefit, substantive or procedural, enforceable at law by any party in any administrative, civil, or criminal matter. Likewise, no limitations are placed by this guidance on the otherwise lawful enforcement or litigative prerogatives of ICE.



Derek N. Benner
Deputy Executive Associate Director and
Senior Official Performing Duties of the
Executive Associate Director
Homeland Security Investigations