# Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists

In the past decade, illicit actors, including criminals and violent extremists, have slowly but steadily diversified their funding sources by incorporating virtual assets known as cryptocurrencies.[a] Cryptocurrency appeals to users due to 1) the ability to make transfers without an intermediary or geographic limitation 2) finality of settlement 3) lower transaction costs compared to other forms of payment and 4) the ability to publicly verify transactions. While cryptocurrency is used for legitimate, legal transactions, it appeals to violent extremists because of its pseudonymity, varying oversight and regulatory requirements by country, convenience, and quick transfer speeds. First responder situational awareness and recognition of illicit use of cryptocurrencies can potentially prevent terrorist-related fundraising.

**SCOPE:** This product serves to assist first responders by providing basic information on cryptocurrency and its potential use by terrorists.

**NOTE:** See attached chart for details on key terminology and basics of cryptocurrency as a guide for this toolbox.

**CONSIDERATIONS:** The following are recommendations to better equip first responders and their organizations.

**Collaboration:** Partnerships with subject matter experts can aid with the technical requirements related to investigations dealing with virtual currencies. *NOTE: If a cryptocurrency expert is not present in your jurisdiction, contact the FBI for subject matter experts and diagnostic tools to help with investigations.*

- Engage and build partnerships with federal partners (HSI, ICE, and IRS) to leverage their established programs and resources related to tracking illicit actors' use of cryptocurrency.
- Engage and build partnerships with private sector partners to gain insight into cryptocurrency transactions (through blockchain-based forensics, data analysis, and information sharing).
  - These partners may include crypto advocacy groups; financial services sector (banks); non-bank financial institutions such as MSBs,[c] financial technology, and online retailers; and think tanks.
- Engage and build partnerships with financial institutions to leverage their reporting of suspicious activity to identify and target transactions that may be associated with illicit terrorist activity.

[a] Cryptocurrency as defined by the US Federal Trade Commission is a type of digital currency that generally only exists electronically. There is no physical coin or bill unless using a service that allows one to cash in cryptocurrency for a physical token. One usually exchanges cryptocurrency with someone online, with a phone or computer, without using an intermediary like a bank. Bitcoin and Ether are well-known cryptocurrencies, but there are many different cryptocurrency brands, and new ones are continuously being created.

[b] Privacy coins, such as Monero, Dash, and Zcash, have features to allow complete anonymity through private ledgers.

[c] The term "money services business" includes any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities: 1) Currency dealer or exchanger, 2) Check casher, 3) Issuer of traveler's checks, money orders or stored value, 4) Seller or redeemer of traveler's, checks, money orders or stored value, 5) Money transmitter, or 6) U.S. Postal Service.





0010211-NCTC

23 SEPTEMBER 2021
AUTHORED BY NCTC, DHS, FBI

## Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists *(continued)*

**Training:** Knowledge of how cryptocurrency transactions are facilitated and emerging cryptocurrency uses may enhance detection, deterrence, collection, and mitigation of the illicit use of cryptocurrencies by terrorists.

- Request cyber or cryptocurrency-related training through subject matter experts located at a local FBI or ICE HSI Field Office, Joint Terrorism Task Force (JTTF), or fusion center.
- Learn how to recognize cryptocurrency addresses and Quick Response Codes (QRCs) used to represent the sending and receiving of assets.
- Build awareness around public block explorers, such as Blockchain.com and Blockchair.com, and other reliable public sources for cryptocurrency and token market information like Coinmarketcap.com.

**Relevant Information:** The following can help guide the investigative process,[d] including examples of the types of information that may indicate potential illicit use of virtual currency.[e]

**Violent Extremists Promote Cryptocurrency:** In early 2021, a prominent Telegram[USBUS] channel that promotes violent extremist related material posted a graphic, with corresponding text, promoting the use of Monero cryptocurrency. The same channel previously published a 34-page guide, titled "Cryptocurrency - A Privacy & Security Goys [non-Jew] Practical Guide."


Snapshot of the graphic posted to promote Monero cryptocurrency.

- Handwritten wallet passwords, application (app) personal identification numbers (PINs), and seed phrases, since cryptocurrency wallets are often encrypted.
- Electronic storage devices, such as universal serial bus (USB) sticks and external hard drives, in locations that are not near computers. Electronic storage devices that contain keypads or other access controls.
- Pieces of paper appearing to have seemingly random strings of alpha-numeric characters.
- Wallet apps on cellphones and online search histories that reference words like "coin," "wallet," or "crypto."
- QR codes representing wallet addresses (both public and private keys) used as a social media public profile, stored on paper, or contained within mobile or desktop apps.
- Browser plugins that serve as cryptocurrency wallets for receiving or mining cryptocurrency.

[d] Since a great deal of this is highly technical, working with individuals familiar with digital forensics is suggested to assist with the investigative process.

[e] Each indicator listed may be lawful by itself or may constitute the exercise of rights guaranteed by the US Constitution. A single indicator may not be the sole basis for action.

## Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists *(continued)*

The following are examples of the types of information that may assist in any investigation; many more databases and file types exist that are app-specific.

- Private keys may be stored in .dat, .keys, .wallet, or .json file formats on a computer hard drive or mobile device. Users may store seed phrases in other apps or text-based note programs as well as on paper.
- Cached images from mobile apps may capture private keys, seed phrases, and other collectible data and will be stored in the cache.db.
- Databases to further explore on mobile devices include: knowledgeC.db and indexedDB. sqlite3 (iOS) and localappstate.db (Android). Apps will have app-specific databases, like public keys stored in zcashsdk_mainnet_data.db (Zcash app called Nighthawk on Android)
- On iPhones, keychaindump/backup_keychain.plist may contain possible stored wallet passwords.

**INDICATORS:**[f] Possible observable indicators that may signify terrorist use of illicit virtual currency include:[g]

- Multiple high-value transactions in short succession, such as within a 24-hour period, or in a staggered or regular pattern. An example is no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases, or to a newly created or previously inactive account.
- Funds deposited or withdrawn from a cryptocurrency address with direct and indirect links to known suspicious sources, including darknet marketplaces, mixing or tumbling services, questionable gambling websites, ransomware, or theft reports.
- Crypto-related language in an app or email-based communications indicative of illicit activity or in the purchase of illicit goods (drugs or stolen credit card information).
- Customer transactions involving more than one type of cryptocurrency or "chain-hopping" (trading one cryptocurrency for another), particularly to privacy coins (Monero, Dash, or Zcash).
- Portfolios that only consist of privacy coins or have a high value in privacy coins.
- Use of money mules at cryptocurrency automated teller machines making small to large deposits at different times and locations into the same address(es).
- Transfers of cryptocurrencies in micro-payments or large volumes in exchange for privacy coins.
- Frequent use of international exchanges with lax or nonexistent "Know Your Customer" and anti–money laundering requirements.
- Virtual currency funds or privacy coins (Monero, Dash or Zcash) originating from an over-the-counter trade broker that advertises its services as privacy-oriented or anonymous.

[f] Each indicator listed may be lawful by itself or may constitute the exercise of rights guaranteed by the US Constitution. A single indicator may not be the sole basis for action.
[g] Cryptocurrency brokers are subject to Title 31 Bank Secrecy Act regulations and illicit cryptocurrency transactions used for terrorist financing may also constitute money laundering, fraud, or other Title 18 Criminal Code violations.

## Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists *(continued)*

- Use of obfuscation techniques, such as sending or receiving directly from third-party mixing or gambling services, layering transactions (moving funds to a series of wallets to obscure the origin), and transfers less than reporting thresholds (similar to structured cash transactions).
- Public addresses flagged on recognized law enforcement bolos, such as the list of the Office of Foreign Assets Control or law enforcement publications.
- Individual registrations with an exchange within a short period using a shared address, mobile device, phone number, or Internet portal addresses.
- An address linked to fraudulent activity in media reports or open-source intelligence (known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites).
- Individuals who set up offices or move offices with no clear business rationale to do so.

The following are common market examples of cryptocurrency with corresponding emblems or symbols recognizable online, on social media, or on electronic devices (applications).


**Bitcoin/BITCOIN**


**Monero/XMR**


**Ethereum/ETH**


**ZCash/ZE**


**Litecoin/LTC**


**Dashcoin/DSH**

**PIVX**


**Ripple/XRP**


**Dash/DASH**


**Peercoin/PPC**

## Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists *(continued)*

### RESOURCES

**DHS**

**Anonymous Networks and Currencies** https://www.dhs.gov/science-and-technology/anc

**State and Major Urban Fusion Centers** empower frontline law enforcement, public safety, fire service, emergency response, public health, and private-sector security personnel to lawfully gather and share threat-related information. https://www.dhs.gov/fusion-center-locations-and-contact-information

**US SECRET SERVICE - NATIONAL COMPUTER FORENSICS INSTITUTE** offers training in cryptocurrency investigations. www.NCFI.usss.gov

**2018 Public-Private Analytic Exchange Program – Blockchain and Suitability for Government Applications** https://www.dhs.gov/publication/2018-aep

**FBI**

- **JTTFs** are cells of highly trained and locally based investigators, analysts, linguists, SWAT experts, and other specialists from dozens of US law enforcement and intelligence agencies. www.fbi.gov/contact-us/field-offices
- **Money Laundering Unit:** 1-800-CALL-FBI or https://www.fbi.gov/contact-us
- **Virtual Currency Evolving Threats Team and Virtual Currency Emerging Evolving Threats Working Group:** 1-800-CALL-FBI or https://www.fbi.gov/contact-us

**FEDERAL TRADE COMMISSION** https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams

**FINANCIAL CRIMES ENFORCEMENT NETWORK** www.fincen.gov

**INTERPOL** (Darknet and Cryptocurrencies) https://www.interpol.int/How-we-work/Innovation/Darknet-and-Cryptocurrencies

**NATIONAL WHITE COLLAR CRIME CENTER (NW3C) - BITCOIN INVESTIGATIVE FIELD GUIDE** www.nw3c.org/resources/Bitcoin-investigative-field-guide/Bitcoin-IFG.pdf

**US DEPARTMENT OF JUSTICE - CRYPTOCURRENCY ENFORCEMENT FRAMEWORK** https://www.justice.gov/archives/ag/page/file/1326061/download

**US IMMIGRATION AND CUSTOMS ENFORCEMENT, HOMELAND SECURITY INVESTIGATIONS**

- **National Bulk Cash Smuggling Center – Crypto Intelligence Program:** BCSC@ice.dhs.gov
- **Tipline:** 866-DHS-2-ICE or https://www.ice.gov/webform/ice-tip-form

# Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists *(continued)*

## APPENDIX: CRYPTOCURRENCY BASICS

Cryptocurrency is defined by the US Federal Trade Commission as a type of digital currency that generally only exists electronically. There is no physical coin or bill unless one is using a service that allows cashing in cryptocurrency for a physical token. One usually exchanges cryptocurrency with someone online, with a phone or computer, without using an intermediary like a bank. Bitcoin and Ether are well-known cryptocurrencies, but there are many different cryptocurrency brands, and new ones are continuously being created. Virtual currency is a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency.

Two primary types of virtual currencies:

- Convertible
- Non-Convertible

Three types of entities:

- Administrator
- Exchanger
- User

Cryptocurrency can:

- Be stored online and in software (computers, mobile devices, and tablets) as well as offline (external hard drives and removable storage devices).
- Be exchanged internationally, potentially facilitating faster cross-border transactions versus traditional MSBs.
- Be known sometimes as "privacy coins" (Monero, etc.) that obfuscate transactions on their specific blockchain, potentially complicating tracking those transactions.
- Offer user pseudonymity as each transaction is recorded on the blockchain's public ledger by the transaction identification (ID)—a hash value composed of a complex series of numbers and letters (unique to each transaction)—that is maintained and updated by mining nodes on each block of the ledger.

**Blockchain** is a decentralized public ledger organized into a series of chronological, interlinked data blocks. Cryptocurrencies rely on these blockchains to facilitate transactions, and in some cases, blockchains can perform other functions not related to currency transactions.

**Private Key** is a cryptographic private key used by an individual to encrypt and sign a transaction and verifies their right to spend cryptocurrency from a specific address. Private keys are stored either offsite on an online service's servers or onsite in a file on the user's device that may be in various file formats (.dat, .keys, .wallet, or .json). The file can also be stored on USB drives. Private keys generate public keys and public addresses.

**Public Addresses** are used when sending and receiving cryptocurrency, and each cryptocurrency has a unique and identifiable series of numbers and letters. Addresses show up on the blockchain once the address has been used, but they are not inherently associated with any personally identifiable information. The amount of cryptocurrency stored at an address is viewable on the blockchain and each transaction using the address generates a unique transaction ID. Depending on the type of cryptocurrency, addresses will look differently and can be represented by a Quick Response Code (QRC) code.

- Bitcoin addresses consist of 24-36 alphanumeric characters and will only ever start with a 1, 3, or bc1 (example: 1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xQX). 1 and 3-type addresses are case sensitive.
- Ether addresses consist of 42 characters and start with a 0x.

**Public Key** is generated and paired with the private key, and this public or private key pairing proves ownership of the corresponding public address. The public address is derived from the public key.

## Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists *(continued)*

### APPENDIX: CRYPTOCURRENCY BASICS

**Seed Phrase**, also known as recovery keys, are a sequence of words acting as a wallet backup that can recover and recreate the wallet and all the derived keys in the same or any compatible wallet app. When a new wallet is created, a pneumonic "seed" phrase is generated. This phrase is a random sequence of 12, 18, or 24 English words that cannot be changed. In some cases, words may be added to the phrase by the user, but in all cases assigned words cannot be deleted or changed. The order of the words matters. This seed phrase can be used to gain access to the account without the private key or password. If first responders recover a seed phrase during an investigation, they can then seize the account. The seed phrase is the starting point for private key generation.

*Trezor hardware wallet with root (seed) key card*

**Wallets** are used when wallet software service providers communicate with cryptocurrency networks to generate and store private keys. Each wallet contains hundreds of public addresses that can be used for transactions. Wallets can be hosted on web apps, offline hardware, or paper-based wallets. Cryptocurrency wallet app icons and web-browsing search history for wallet software or computer files with a ".dat" extension may assist investigators in the identification of an electronic wallet.

#### Types of Wallets and Wallet Services

- **Exchange Services** process millions of customers' transactions. Users can open an account and generate wallets with an exchange service to purchase cryptocurrency with fiat currency (US Dollar) or exchange one type of cryptocurrency for another. These wallets are often custodial (where the exchange holds the private keys), although some exchanges offer non-custodial options. Exchanges in the US are mandatorily responsive to US legal processes and will provide wallet owner information (driver's license information, place of residence, bank account information).
  - Popular exchange service examples include Coinbase[USPER], Binance (overseas-based but some US presence), Kraken[USPER], and Poloniex (overseas-based).

**Growing Diversification of Services Offering Cryptocurrency:** PayPal[USBUS] and other fiat service providers are starting to offer the capability to store, trade, and make purchases with cryptocurrencies. US-headquartered service providers are subject to US laws and regulations.

- **Hardware Wallets** are small (often USB-sized) hardware devices that store a user's private keys for each wallet. It is secured with a PIN and backed up with a seed phrase. Examples include Ledger, Trezor, and KeepKey. One single hardware device can store multiple wallets for many different types of cryptocurrency.
  - Each hardware wallet requires corresponding software.
  - A hardware wallet is known as cold storage—once unplugged, the private key remains in the wallet device and no one can access or move funds around without the personal identification number code.
  - However, cold storage allows access to the funds if an individual has the software password plus hardware PIN code, or seed phrase.

# Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists *(continued)*

## APPENDIX: CRYPTOCURRENCY BASICS

**Types of Wallets and Wallet Services** *(continued)*

- **Paper Wallets** are printed, physical pieces of paper.
- **Software Wallet Apps** are the most popular form of storage. Wallet software programs exist for computer, tablet, and mobile phone operating systems. The private keys are either stored with the software wallet service itself (hosted or custodial wallet) or held on the user's device (non-custodial wallet). Each app may be secured with a password and backed up with a seed phrase. Example wallets include Exodus, Samourai, and Electrum.
  - Wallet software services vary greatly in security. Under-secured wallets may leave digital forensic artifacts related to cached images or recovery of seed phrases and private key files or QRCs on the phone or computer hard drive.

EXAMPLES OF COMMON DESKTOP WALLET APPLICATIONS:

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

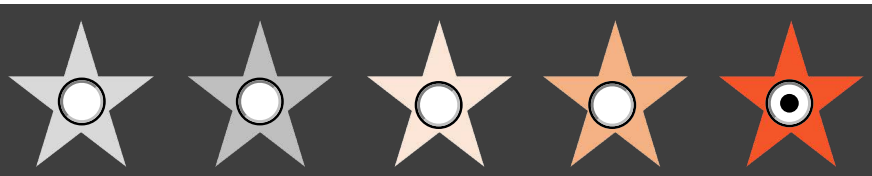
# PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS.

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT

028706 ID 5-16