WELL-KNOWN EXCHANGERS

Bitcoin exchangers are the conduit to convert cryptocurrency into fiat currency. Similar to traditional financial institutions, in many jurisdictions exchangers collect identifying information on their customers at the time of account opening. The following exchangers are commonly used within the bitcoin community:

- Bitfinex
- Bitstamp
- BTC-E
- Circle
- Coinbase
- Kraken
- Local Bitcoins
- Poloniex
- Xapo

WHAT TO DO WITH A PARTIAL BITCOIN ADDRESS

Whenever you come across a bitcoin address, ensure that you copy the address legibly and accurately, including the proper capitalization. Addresses are case-sensitive and even one mischaracterization may make it impossible to identify the address. However, if you only have a partial bitcoin address, several tracing tools have an auto-complete option that can identify the full address. The best option for this type of analysis is BlockSeer.com. WalletExplorer.com will also identify addresses based on the first several characters, known as "firstbits."

OTHER CRYPTOCURRENCIES

Currency Type	How to Identify the Currency
Bitcoin	25-36 characters beginning with a 1 (one) or a 3
Dash	34 characters beginning with an X
Dogecoin	34 characters beginning with the letter D
Ethereum	42 characters beginning with 0x
Litecoin	33 characters beginning with the letter L
Monero	Raw address has 95 characters starting with a 4
Ripple	34 characters beginning with the leter R

FOR FURTHER INFORMATION...

Join the NCIJTF Virtual Currency Team's Special Interest Group (SIG) on the Law Enforcement Enterprise Portal (LEEP) which is available to law enforcement agencies, intelligence partners, and criminal justice entities.

https://portal.cjis.gov

To request training or tracing assistance, email the NCIJTF Virtual Currency Team:

NCIJTF_OTP_VCT@ic.fbi.gov

Identifying Cryptocurrencies: An Investigator's Guide

NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE

OFFICE OF THREAT PURSUIT
VIRTUAL CURRENCY TEAM

NCIJTF_OTP_VCT@IC.FBI.GOV

What Is Bitcoin?

Bitcoin is an alternative to fiat currency—that is, real money. It is a type of digital currency which uses encryption techniques to regulate both the transfer of funds and the generation of new bitcoins. Bitcoin acts independently from any central banking authorities and has no regulating or governing body. The integrity of the system is maintained by individuals or groups known as "miners," who are tasked with verifying the existence of funds through complex math problems. Transactions are conducted in a peer-to-peer network without any intermediary, such as a financial institution.

A **bitcoin address**, also known as a public address, consists of 25-36 alphanumeric and case-sensitive characters starting with a one or a three. These addresses send and receive bitcoins. Each transaction is captured in the **blockchain,** which is a freely-available public ledger that captures the history of all verified transactions. Bitcoin transactions are **irreversible.** Once funds are sent, there is no mechanism in place to recover funds. **Exchangers** act as the on and off-ramps to the formal financial system by exchanging fiat currency for virtual currencies, and vice versa.

To send bitcoins, an individual must sign with a **private key,** which is a cryptographic signature proving the individual with the key has the right to send the bitcoins. Private keys are either stored on a computer when using a software wallet or on a remote server if using a web wallet. They can also be stored on thumb drives, encrypted hardware, mobile phone applications, or even written down by hand and stored in a safe place.

Bitcoin is used as currency globally in both legitimate and criminal financial transactions. It is the primary currency used in illicit transactions on **Dark Web** marketplaces, although other cryptocurrencies are used on these sites as well. Bitcoin can be used to purchase merchandise on Overstock.com, Expedia, MGM Resorts, and at thousands of other merchants worldwide.
Finally, bitcoin can be acquired through transactions at specialized bitcoin ATMs in which cash is exchanged for bitcoin in the form of QR codes.

What Does A Bitcoin address Look like?

The image below shows an actual bitcoin address connected to the takedown of the Silk Road dark market, which was responsible for selling narcotics and other illegal paraphernalia. The QR code identified on the bottom right of the next panel is the code associated with this same address.

Bitcoin addresses will always be 25-36 case-sensitive alphanumeric characters.

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX

Indicators That A Suspect Is Using Virtual Currency

There are several signs to look for to identify if a suspect is using bitcoin, such as:

- The presence of a .wallet file, wallet.dat file, or software wallets on the suspect's computer
- Browser history:
  - Visiting exchangers (See "Well Known Exchangers" for more detail)
  - Visiting sites associated with virtual currency usage (CoinDesk, CryptoCoin News, CoinTelegraph, etc.)
  - Visiting vendors that accept virtual currency (especially online dark markets)
  - Visiting forums discussing bitcoin or other virtual currencies
- Mobile applications, such as wallet providers, games (Bitcoin Flapper, Bitcoin Billionaire), or exchange services (ShapeShift, Coinbase, zTrader, etc.)
- Social media posts related to virtual currency use or other criminal activity
- Bank statements identifying payments to or from exchangers (activity with the formal banking system may trigger Suspicious Activity Reports)

What To Look For During A Search

Wallet software — this software is used to manage bitcoin on a device. If wallet software is identified, it is likely that a suspect has been involved in bitcoin transactions. Common wallet software includes Armory, Breadwallet, Electrum, GreenAddress, Multibit, and Mycelium (see icons below). Wallet software can be found on computers as well as on mobile devices.

Use of a Tor Browser — Tor browsers conceal users' identities by encrypting and bouncing communication traffic through global relay networks, purposely disguising IP addresses. Cookies and browsing histories are not stored when using Tor browsers. Many people will use the Linux-based service TAILS or a VPN service to connect to Tor to further layer their connection activity.

Visiting Dark Web Marketplaces—These are hidden websites which allow users to anonymously purchase goods and services—especially illegal goods, including drugs, weapons, or stolen credit card information. Websites on the Dark Web end in ".onion" (instead of the commonly used ".com" on the open web). Common Dark Web markets are: AlphaBay, Dream Market, Outlaw Market, and Hansa Market, though there are many more.

Printed or Electronic QR Codes — QR codes can contain copies of public and private keys required to access bitcoin and are associated with a specific address. QR codes are used in paper wallets that are generally not stored electronically.