Investigative Assistance

Federal, state, local, tribal and territorial law enforcement and regulatory agencies around the country recognize the challenges crypto-currencies pose. Companies around the world understand the need for criminal investigations and provide services that analyze Bitcoin transactions.

Chainalysis and BlockSeer are two companies that conduct Blockchain forensics to analyze Bitcoin transactions and identify Bitcoin users.

If you have questions or need investigative assistance please contact us on the web at training@nw3c.org.

Access the Bitcoin Investigative Field Guide online at NW3C.org

NW3C offers a mobile-friendly investigative guide for use in the office or the field. This guide provides answers to common questions law enforcement may have when dealing with Bitcoin. The intuitive interface allows users to quickly locate information addressing a number of concerns such as:

- Am I authorized to handle Bitcoin?
- What do I need to obtain and use Bitcoin?
- How do I identify Bitcoin transactions?
- How do I gain access to and seize suspect's Bitcoin?
- What are the best practices for preserving Bitcoin as digital evidence?

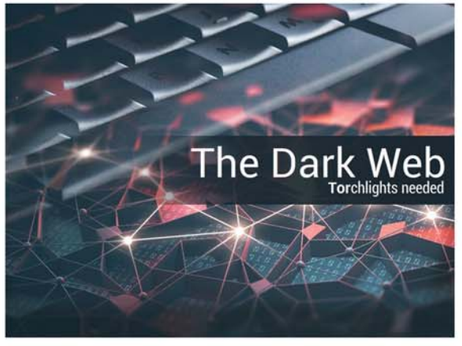
And more

Online Training

All of NW3C's online courses are free to law enforcement.

Below are some recommended courses for handling digital evidence, understanding cryptocurrency and the dark web:

First Responders and Digital Evidence
Identifying and Seizing Electronic Evidence
Encryption
Virtual Currency
The Dark Web: **Tor**chlights needed



Visit NW3C.org for more information.

This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

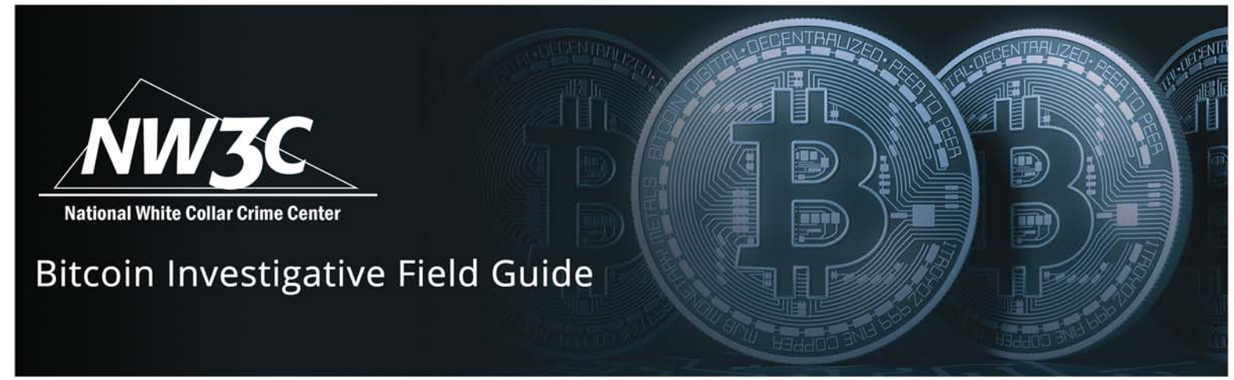
©2017. NW3C, Inc. d/b/a the National White Collar Crime Center. All rights reserved.

Image credits: 181300621 3D Sculptor, 200159044 IurilMotov, 191918041 Phive, 196360357 alekseyvanin, 200939332 SergeVo, 198321577 Aha-Soft used under license from BigStockPhoto.com

Smartphone Google Pixel Mock-up - Creative Commons - credit Daniel Bolyhos

NW3C
National White Collar Crime Center

Bitcoin Investigative Field Guide



What is Bitcoin?

Bitcoin is an open-source, peer-to-peer cryptocurrency that allows transactions to be processed directly from one party to another without the need of a third party or financial institution. Unlike currency such as the dollar or euro, Bitcoin is not tied to any country or subject to regulation.

The foundation of Bitcoin stems from the idea of creating an electronic payment system based on cryptographic proof instead of trust. Every Bitcoin transaction is recorded on a general ledger, known as the "blockchain."

What is the value of Bitcoin?

Bitcoin is given value due to supply and demand. Secure and pseudo-anonymous Bitcoin transfers occur through online exchanges and can be exchanged into fiat or virtual currencies.

In 2017, the value of Bitcoin in US dollars spiked between the months of March (1 BTC = $1,267) and August (1 BTC = $4,195). Like other popular cryptocurrencies, Bitcoin is subject to extreme swings of volatility, so large purchases or sales of Bitcoin can shift prices 30% or more in a single day. However, the overall value of Bitcoin largely relies on its growing base of users, merchants and startups who accept it as a form of payment.

Current exchange rates and trend charts can be found on third-party sites.

What can be purchased using Bitcoin?

More than 100,000 merchants worldwide accept Bitcoin as a form of payment for goods and services. Due to the popularity of the online marketplace and ease of payments, businesses and individuals benefit from the use of Bitcoin in purchasing:

Firearms • Airline Tickets • Property • Consumable Goods
Lottery Tickets • Automobiles • Computers • Gift Cards • Rentals

Why is Bitcoin important to law enforcement?

Due to the perception of anonymous transactions, Bitcoin is of great interest to individuals and criminal organizations. It has been used in everything from drug deals to human trafficking to assassinations. Using Bitcoin, there is no risk of a financial institution filing a Suspicious Activity Report, nor is there a need to exchange large amounts of cash between parties. Law enforcement may find it challenging to learn how this cryptocurrency works, who is using it and how it is used in criminal activity.

This guide provides basic information and tips on how to identify the presence of Bitcoin and digital wallets, and the collection process.

How is Bitcoin obtained?

Bitcoin can be purchased through online exchanges such as Coinbase, Kraken, GDAX and others at market price.

Bitcoin can also be obtained via “mining.” A miner is an individual or group who solves complex algorithms on powerful software to validate virtual currency transactions made. When miners verify that a block of transactions is accurate and calculate the block’s hash, then they are rewarded with a newly created Bitcoin.

Where is Bitcoin stored?

Bitcoin is stored in Bitcoin wallets that allow users to send, store, and receive Bitcoin from other users. Bitcoin wallets simplify the process of signing a transaction, broadcasting it to the blockchain, and verifying incoming transactions.

There are 4 types of wallets:

Computer wallets run as an application on a computer and are the most common way of storing and securing Bitcoin. In-program instructions tell users how to transfer funds. These wallets are typically identified by an icon on the user’s desktop, but can also be hidden. Use the search function to find the term “wallet” or a .dat file extension.

Mobile wallets exist on a user’s Android or iOS smartphone. This type of wallet is generally simple and features a basic and intuitive interface designed for average end-users new to Bitcoin. They can be identified by a logo or icon on the homescreen or app tray. Occasionally, mobile wallets are secured by an additional PIN, password or biometric security feature.

Online wallets exist on websites and typically function as an extension of the exchange on which they are purchased. Accessed with a log-in, online wallets utilize additional security measures. Online wallets are more difficult to identify. Online wallet service providers can freeze accounts and provide details to law enforcement on users under investigation.

Cold storage is an alternative way of storing Bitcoin, and by far the most secure. A private key is required to send Bitcoin which revolves around the idea of never exposing the key to the internet. These wallets are difficult to identify as the key could exist on USB drives, paper, or memorized by a suspect. Recovery seeds, which are used to back up Bitcoin wallets, often range between 12 and 24 random words.

How is a Bitcoin wallet obtained?

Most computer and mobile wallets are available for free from third-party vendors directly or in the Apple App and Google Play stores. Online and cold storage wallets are available by subscription or at a flat rate. When selecting a wallet, visit the vendor website and consider user reviews and ratings.

Wallets should provide additional information such as current Bitcoin exchange rates and contact information for technical support.

How is Bitcoin seized?

Prior to seizing Bitcoin, it is important to check or establish department policy on handling digital evidence and virtual currency. The next step is to set up a departmental Bitcoin wallet accessible only to personnel designated by department policy.

Bitcoin wallets are often encrypted, so obtaining a password or PIN from a suspect to gain access is important to the seizure process. If it is not possible to proceed, excercise best practices and precautions in preventing further access to the device or online wallet.

Bitcoin should be collected as soon as possible once it has been determined that a seizure is appropriate.

1

Identification

Become familiar with service providers of the different types of Bitcoin wallets for computers, mobile devices, and the web. Once it is discovered that criminal activity may involve Bitcoin, there is often limited time to access the supect’s Bitcoin wallet.

At this point, determine if is possible to obtain the passcode or key to the device and the Bitcoin wallet.

Restrict access to all devices that may contain evidence.

2

Collection

If it is not possible to access the suspect’s Bitcoin wallet, prevent tampering by putting the device into airplane mode or placing it into a Faraday bag.

Once the suspect’s Bitcoin wallet is unencrypted on a mobile device or computer, it is possible to transfer funds to your departmental Bitcoin wallet. Enter the address of the wallet or scan the QR code if possible. Press or click the transfer button to move the funds. A Bitcoin wallet may contain multiple files that store Bitcoin separately. Be sure to check subfolders and tabs within the program or app.

3

Preservation

After transferring Bitcoin to the departmental wallet, they are relatively safe.
At this point, follow chain of custody and digital evidence handling protocols. Check to see if the departmental wallet allows for a Bitcoin vault to be established. This is a security feature which requires multiple parties to complete a transfer.

Many vendors of online wallets provide assistance regarding law enforcement inquiries and investigations.

4

Investigative Use

Bitcoin is often used on the “dark web,” which is a part of the world wide web that requires special software to access. It is possible that seized Bitcoin was part of a transaction that occurred in a dark web market. The blockchain database is very much like a full history of banking transactions: it can provide information that may be important to an investigation.

Following the money can often uncover additional suspects and organizations.