**Regional Organized Crime Information Center**

Special Research Report

# Bitcoin and Cryptocurrencies

## Law Enforcement Investigative Guide

**Regional Organized Crime Information Center**

Special Research Report

# Bitcoin and Cryptocurrencies

## Law Enforcement Investigative Guide



Everybody's heard about Bitcoin by now. How the value of this new virtual currency wildly swings with the latest industry news or even rumors. Criminals use Bitcoin for money laundering and other nefarious activities because they think it can't be traced and can be used with anonymity. How speculators are making millions dealing in this trend or fad that seems more like fanciful digital technology than real paper money or currency. Some critics call Bitcoin a scam in and of itself, a new high-tech vehicle for bilking the masses.

But what are the facts? What exactly is Bitcoin and how is it regulated? How can criminal investigators track its usage and use transactions as evidence of money laundering or other financial crimes? Is Bitcoin itself fraudulent?

Bitcoin Basics

REGIONAL ORGANIZED CRIME INFORMATION CENTER SPECIAL RESEARCH REPORT

# Law Enforcement Needs to Know About Cryptocurrencies

Law enforcement will need to gain at least a basic understanding of cyptocurrencies because criminals are using cryptocurrencies to launder money and make transactions contrary to law, many of them believing that cryptocurrencies cannot be tracked or traced. Fortunately, however, this belief is not true. Bitcoin and other cryptocurrencies can be traced, detected, and tracked.

Also, civilians concerned about the stability of the dollar are converting them to cryptocurrencies, which hackers can then steal and/or destroy.

Criminals are also using cryptocurrencies to transact ransomware or extortions against innocent victims. Criminals are using cryptocurrencies on the DarkNet (the other Internet) to transact criminal activities.

Next month's ROCIC Special Research Report will concentrate on ransomware and the DarkNet. You may also find two previous ROCIC reports helpful — "Penetrating the Darknet: Silk Road, Bitcoins, and the Onion Router" and "Hack Attack! Protecting Data Networks From Cyber Criminals." They are available online on the ROCIC Website under Publications.

Bitcoin (BTC) is a cryptocurrency, defined as a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. You have to download software (usually free) in order to use it.

Although Bitcoin was the first real cryptocurrency, launched in 2008, there are now dozens of alternative cryptocurrencies, most of them based on the concept of Bitcoin.

Bitcoin is a virtual currency because it can be used to purchase goods and services but it exists only on computer networks. Bitcoin is a cryptocurrency because it uses encryption.

Bitcoin is just a brand name. There are no physical coins; there is nothing physical at all, only computer codes and computer formulas (algorithms).

Bitcoin has no intrinsic value; it is not redeemable for another commodity, e.g., gold.

The supply of Bitcoins is not determined by a centralized entity, such as a bank, and its computer network is completely decentralized. The supply of Bitcoins was determined by its creator (a person or entity known only as Satoshi Nakamoto) and is controlled by its inherent formula or algorithm. The total possible number of Bitcoins is 21 million, estimated to be reached in the year 2140. There are now about 16.8 million Bitcoins in existence. However, one Bitcoin (whose value in dollars varies significantly with time based on buyers vs. sellers) can be divided almost infinitely (100 million times).

Nakamoto announced Bitcoin as "a new electronic cash system that uses a peer-to-peer network to prevent double-spending. It's completely decentralized with no server or central authority."

Bitcoin is legal but is not a currency approved by the U.S. government. Bitcoin is considered property and not currency by the Internal Revenue Service.

Bitcoin can be bought and sold with dollars. Bitcoin can be used to purchase goods and services online provided the merchant is willing and able to process Bitcoin. Bitcoin can also be used as a store of value (i.e., buy low, sell high).

In simple terms, here's how a typical Bitcoin transaction works:

- A computer user who owns Bitcoin wants to buy a gift card (or any other item) online.
- The transaction is broadcast to a network of computers known as nodes.
- The network of nodes validates the transaction and the user's status using known algorithms.
- The computer node that validates the transaction the fastest is awarded newly created Bitcoins. This validation requires quite a bit of computer power and the electricity to run it. The people who do this are called "miners." They perform "proof-of-work," using the SHA 256 Hash algorithm.
- Once verified, the transaction is combined with other transactions to create a new block of data for the blockchain ledger.
- The new block is added to the existing blockchain in a way that is permanent and unalterable.
- The computer user is awarded the gift card. This process may take several minutes.

# Bitcoin's transactional properties

**Irreversible:**

After confirmation, a transaction can not be reversed. By nobody. And nobody means nobody. Not you, not your bank, not the president of the United States, not Satoshi, not your miner. Nobody. If you send money, you send it. Period. No one can help you, if you sent your funds to a scammer or if a hacker stole them from your computer. There is no safety net.

**Pseudonymous:**

Neither transactions nor accounts are connected to real-world identities. You receive Bitcoins on so-called addresses, which are seemingly random chains of around 30 characters. While it is usually possible to analyze the transaction flow, it is not necessarily possible to connect the real world identity of users with those addresses.

**Fast and global:**

Transactions are propagated nearly instantly in the network and are confirmed in a couple of minutes. Since they happen in a global network of computers they are completely indifferent to your physical location. It doesn't matter if I send Bitcoin to my neighbor or to someone on the other side of the world.

**Secure:**

Cryptocurrency funds are locked in a public key cryptography system. Only the owner of the private key can send cryptocurrency. Strong cryptography and the magic of big numbers makes it impossible to break this scheme. A Bitcoin address is more secure than Fort Knox.

**Permissionless:**

You don't have to ask anybody to use cryptocurrency. It is software that everybody can download for free. After you installed it, you can receive and send Bitcoins or other cryptocurrencies. No one can prevent you. There is no gatekeeper.

The stages of a typical BItcoin transaction are depicted on the chart on the following page. Some basic knowledge of computer science is necessary to understand the process. The technology used by Bitcoin and the blockchain cannot be sufficiantly covered in this publication. There are many technical manuals and online resources that delve into the underlying technology.

# How a Bitcoin Transaction Works

Bob, an online merchant, decides to begin accepting Bitcoins as payment. Alice, a buyer, has Bitcoins and wants to purchase merchandise from Bob.

## WALLETS AND ADDRESSES

Bob and Alice both have Bitcoin "wallets" on their computers.

Wallets are files that provide access to multiple Bitcoin addresses.

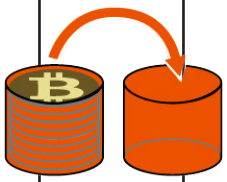
An address is a string of letters and numbers, such as 1HULMwZEPkjEPeCh43BeKJL1ybLCWrfDpN.

## CREATING A NEW ADDRESS

Bob creates a new Bitcoin address for Alice to send her payment to.

Each address has its own balance of Bitcoins.

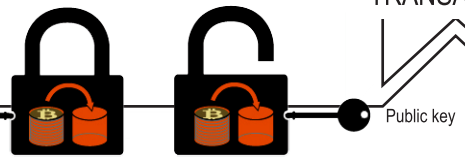
## SUBMITTING A PAYMENT



Alice tells her Bitcoin client she'd like to transfer the purchase amount to Bob's address.

### Public Key Cryptography

When Bob creates a new address, what he's really doing is generating a "cryptographic key pair," composed of a private key and a public key. If you sign a message with a private key (which only you know), it can be verified by using the matching public key (which is known to anyone). Bob's new Bitcoin address represents a unique public key, and the corresponding private key is stored in his wallet. The public key allows anyone to verify that a message signed with the private key is valid.

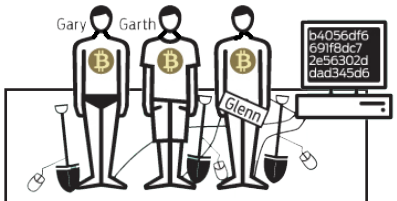



Alice's wallet holds the private key for each of her addresses. The Bitcoin client signs her transaction request with the private key of the address she's transferring Bitcoins from.

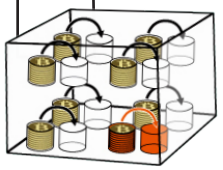
Anyone on the network can now use the public key to verify that the transaction request is actually coming from the legitimate account owner.

## VERIFYING THE TRANSACTION

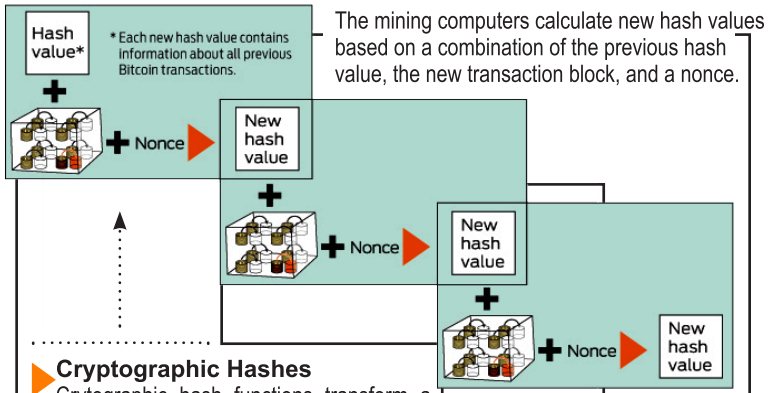
Gary, Garth, and Glenn are Bitcoin miners.




Their computers bundle the transactions of the past 10 minutes into a new "transaction block."



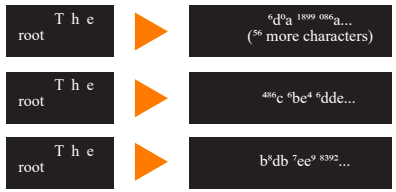
The miners' computers are set up to calculate cryptographic hash functions.




The mining computers calculate new hash values based on a combination of the previous hash value, the new transaction block, and a nonce.

### Cryptographic Hashes

Crytographic hash functions transform a collection of data into an alphanumeric string with a fixed length, called a hash value. Even tiny changes in the original data drastically change the resulting hash value. And it's essentially impossible to predict which initial data set will create a specific hash value.



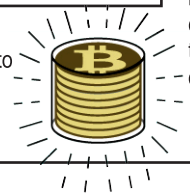

### Nonces

To create different hash values from the same data, Bitcoin uses "nonces." A nonce is just a random number that's added to data prior to hashing. Changing the nonce results in a wildly different hash value.

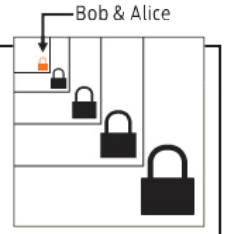

Creating hashes is computationally trivial, but the Bitcoin system requires that the new hash value have a particular form–specifically, it must start with a certain number of zeros.

The miners have no way to predict which nonce will produce a hash value with the required number of leading zeros. So they're forced to generate many hashes with different nonces until they happen upon one that works.

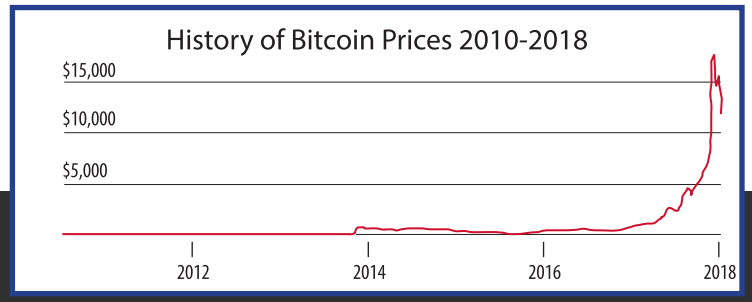
Each block includes a "coinbase" transaction that pays out 50 Bitcoins to the winning miner–in this case, Gary. A new address is created in Gary's wallet with a balance of newly minted Bitcoins.



## TRANSACTION VERIFIED




As time goes on, Alice's transfer to Bob gets buried beneath other, more recent transactions. For anyone to modify the details, he would have to redo the work that Gary did–because any changes require a completely different winning nonce–and then redo the work of all the subsequent miners. Such a feat is nearly impossible.




# BITCOIN'S WILD RIDE IN 2017

**Through November. Bitcoin prices soared to $19,086 in mid-December and then slid back down to $11,000 as of January 19, 2018.**

**MARKET CAP MILESTONES**

- **$25B** — May 4
- **$50B** — August 5
- **$100B** — October 20

**JANUARY**
China cracks down on Bitcoin, partly to help control capital outflows

**MARCH**
Number of GitHub projects related to Bitcoin passes 10,000

**AUGUST 1**
Bitcoin forks into two digital currencies, Bitcoin (BTC) and Bitcoin Cash (BCH)

**SEPTEMBER 4**
People's Bank of China announces freeze on ICO funding

**SEPTEMBER 12**
JP Morgan's Jamie Dimon calls Bitcoin a fraud

**SEPTEMBER 28**
South Korea bans raising money through ICOs

**OCTOBER 24**
Bitcoin Gold fork

**OCTOBER 30**
Vietnam bans Bitcoin and other crypto payments

- 138 days $1K-$2K
- 23 days $2K-$3K
- 63 days $3K-$4K
- 61 days $4K-$5K
- 10 days $5K-$6K
- 13 days $6K-$7K
- 17 days $7K-$8K
- 7 days $8K-$9K

**BITCOIN (BTC) PRICES**

$10,000 $9,000 $8,000 $7,000 $6,000 $5,000 $4,000 $3,000 $2,000 $1,000

| JAN | FEB | MAR | APR | MAY | JUN | JUL | AUG | SEP | OCT | NOV |
|---|---|---|---|---|---|---|---|---|---|---|
| $2.3 | $17.0 | $19.4 | $103.7 | $232.0 | $462.0 | $574.5 | $145.9 | $662.9 | $516.4 | $743.2 |

**ICO FUNDING ($millions)**

# Alternative Cryptocurrencies

Bitcoin is not the only cryptocurrency out there, although it has the largest market capitalization, user base, and the lion's share of news headlines. Inspired by Bitcoin are what's called alt-coins or alternative cryptocurrencies. Although some are easier to mine or create, there is greater risk. Criminals who have used Bitcoin because they believed it could not be traced and found out otherwise have been changing over to other newer cryptocurrencies that may be tougher for law enforcement to crack.

Many cryptocurrencies benefitted the past year from a combination of greater recognition in countries such as Japan and South Korea, rising interest from institutional investors and Wall Street firms, and a boom in a new fundraising method called the initial coin offering, which attracted more than $4 billion in new capital in 2017. Jimmy Song, a Bitcoin developer in Austin, Texas, said, "Retail investors in Korea are driving a lot of the price. They will buy anything that looks reasonably cheap."

All cryptocurrencies have a total market value of about $600 billion. Bitcoin, at $323 billion, comprises most of that, but there are several notable alternatives, such as Ethereum ($71 billion), Ripple ($29 billion), Bitcoin Cash ($32 billion) and Litecoin ($17.6 billion). Reportedly, there are more than 1,300 different types of altcoins, with only 26 having market values above $1 billion. Before 2017, only Bitcoin and Ethereum were at that level. Many of the more obscure alt-coins such as PinkDog, MagicCoin and BitSoar are marginal, while many others are obviously pump-and-dump schemes.

Overall, 165 firms have raised more than $4 billion in 2017 through coin offerings, which resemble crowdfunding campaigns more than traditional fundraising tactics like selling equity or attracting venture capital.

Coinbase has emerged as the biggest Bitcoin exchange, and it has become a company that is closest to the mainstream. Its app has become one of the most downloaded, and it has one of the largest user bases in the industry. So what it does carries weight.

Does Coinbase support any other altcoins?
Coinbase allows trading of Bitcoin, Bitcoin Cash, Litecoin, Ethereum and Ethereum Classic.

### 1) Litecoin (LTC)

Litecoin, launched in 2011, was among the initial cryptocurrencies following Bitcoin and was often referred to as "silver to Bitcoin's gold." It was created by Charlie Lee, a MIT graduate and former Google engineer. Litecoin is based on an open-source global payment network that is not controlled by any central authority and uses "scrypt" as a proof of work, which can be decoded with the help of CPUs of consumer grade. Although Litecoin is like Bitcoin in many ways, it has a faster block generation rate and hence offers a faster transaction confirmation. Other than developers, there are a growing number of merchants who accept Litecoin.
Litecoin began December 2017 at just $88 and the year (2017) at $4.33. Litecoin was up about 7,000 percent, even after settling a bit to trade around $323, according to coinmarketcap.com.
Coinbase's online exchange GDAX supports trading of the currency. Since Coinbase has emerged as the first service many newcomers are trying out, they are also being exposed to Litecoin for the first time. Litecoin has been around long enough, and has enough developers working on it, that it appears more stable than some of the newer currencies. That development team also has a reputation for testing and implementing upgrades that later show up in Bitcoin. Still, it has not been able to attract as many developers and businesses as Bitcoin has, and that has limited its appeal somewhat compared with its larger peers.

### 2) Ethereum (ETH)

Launched in 2015, Ethereum is a decentralized software platform that enables Smart Contracts and Distributed Applications (ĐApps) to be built and run without any downtime, fraud, control or interference from a third party. During 2014, Ethereum had launched a pre-sale for ether which had received an overwhelming response. The

# Alternative Cryptocurrencies

applications on Ethereum are run on its platform-specific cryptographic token, ether. Ether is like a vehicle for moving around on the Ethereum platform, and is sought by mostly developers looking to develop and run applications inside Ethereum. According to Ethereum, it can be used to "codify, decentralize, secure and trade just about anything." Following the attack on the DAO in 2016, Ethereum was split into Ethereum (ETH) and Ethereum Classic (ETC). Ethereum (ETH) has a market capitalization of $41.4 billion, second after Bitcoin among all cryptocurrencies.

**3) Zcash (ZEC)**

Zcash, a decentralized and open-source cryptocurrency launched in the latter part of 2016, looks promising. "If Bitcoin is like http for money, Zcash is https," is how Zcash defines itself. Zcash offers privacy and selective transparency of transactions. Zcash claims to provide extra security or privacy where all transactions are recorded and published on a blockchain, but details such as the sender, recipient, and amount remain private. Zcash offers its users the choice of shielded transactions, which allow for content to be encrypted using advanced cryptographic technique or zero-knowledge proof construction called a zk-SNARK developed by its team.

**4) Dash (DASH)**

Dash (originally known as Darkcoin) is a more secretive version of Bitcoin. Dash offers more anonymity as it works on a decentralized mastercode network that makes transactions almost untraceable. Launched in January 2014, Dash experienced an increasing fan following in a short span of time. This cryptocurrency was created and developed by Evan Duffield and can be mined using a CPU or GPU. In March 2015, Darkcoin was rebranded to Dash, which stands for Digital Cash and operates under the ticker – DASH. The rebranding didn't change any of its technological features such as Darksend, InstantX.

**5) Ripple (XRP)**

Ripple is a real-time global settlement network that offers instant, certain and low-cost international payments. Ripple "enables banks to settle cross-border payments in real time, with end-to-end transparency, and at lower costs." Released in 2012, Ripple currency has a market capitalization of $1.26 billion. Ripple's consensus ledger — its method of conformation — doesn't need mining, a feature that deviates from Bitcoin and altcoins. Since Ripple's structure doesn't require mining, it reduces the usage of computing power, and minimizes network latency. Ripple believes that "distributing value is a powerful way to incentivize certain behaviors" and thus currently plans to distribute XRP primarily "through business development deals, incentives to liquidity providers who offer tighter spreads for payments, and selling XRP to institutional buyers interested in investing in XRP."

**6) Monero (XMR)**

Monero is a secure, private and untraceable currency. This open-source cryptocurrency was launched in April 2014 and soon spiked great interest among the cryptography community and enthusiasts. The development of this cryptocurrency is completely donation-based and community-driven. Monero has been launched with a strong focus on decentralization and scalability, and enables complete privacy by using a special technique called ring signatures. With this technique, there appears a group of cryptographic signatures including at least one real participant — but since they all appear valid, the real one cannot be isolated.

**7) Bitcoin Cash (BCH)**

Bitcoin Cash has the exact same transaction history as the original Bitcoin, up to Aug. 1, 2017. Its primary difference is that it is designed to allow more transactions to pass through, on a per-second basis, than Bitcoin, which leads to lower user fees. It was developed by a group of developers and businesses who weren't satisfied with the existing configuration of Bitcoin.

# Blockchain Technology Could Change the World Much Like the Internet Did

Many technologists are ambivalent about Bitcoin being used as currency but they are much more excited about one piece of Bitcoin's software formula called the blockchain. The blockchain is seen by many as a much better way to carry out transactions and contracts that affect every aspect of life. Some see future applications of the blockchain as changing everyday life just as powerful as the Internet changed things during the past few decades. Some believe the blockchain will be widely adopted within ten years; others claim it may take 20 to 30 years to be assimilated.

Finally, another technology which could have fantastic consequences is the development of quantum computing, which would be like computers on steroids. Breakthroughs in quantum computing could affect cryptocurrencies and blockchain development and affect national security.

The implications of blockchain technology are immense, according to Marco Iansiti and Karim Lakhani, authors of a recent article in *Harvard Business Review:*

"With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared. Intermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction. This is the immense potential of blockchain."

"But while the impact will be enormous, it will take decades for blockchain to seep into our economic and social infrastructure. The process of adoption will be gradual and steady, not sudden, as waves of technological and institutional change gain momentum."

## Five basic blockchain principles:

**1. Distributed Database**
Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

**2. Peer-to-Peer Transmission**
Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.

**3. Transparency with Pseudonymity**
Every transaction and its associated value are visible to anyone with access to the system. Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.

**4. Irreversibility of Records**
Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they're linked to every transaction record that came before them (hence the term "chain"). Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.

**5. Computational Logic**
The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. So users can set up algorithms and rules that automatically trigger transactions between nodes.

*Source: Harvard Business Review*

"I have great respect for Karim and his co-author, but I disagree," wrote Bernard Golden, a tech innovator. "I think blockchain is going to arrive faster and with more bite than they expect; indeed, I think it will occur faster than most people expect." Golden is predicting acceptance of blockchain in five to ten years, not 30 to 40.

Blockchain—a peer-to-peer network that sits on top of the Internet—was introduced in October 2008 as part of a proposal for Bitcoin, a virtual currency system that eschewed a central authority for issuing currency, transferring ownership, and confirming transactions. Bitcoin is the first application of blockchain technology.

The infamous hacks that have hit Bitcoin exchanges exposed weaknesses not in the blockchain itself but in separate systems linked to parties using the blockchain.

Much of the initial private blockchain-based development is taking place in the financial services sector, often within small networks of firms, so the coordination requirements are relatively modest. Financial services companies, for example, are finding that the private blockchain networks they've set up with a limited number of trusted counterparties can significantly reduce transaction costs.

Nasdaq is working with Chain.com, one of many blockchain infrastructure providers, to offer technology for processing and validating financial transactions. Bank of America, JPMorgan, the New York Stock Exchange, Fidelity Investments, and Standard Chartered are testing blockchain technology as a replacement for paper-based and manual transaction processing in such areas as trade finance, foreign exchange, cross-border settlement, and securities settlement.

The Bank of Canada is testing a digital currency called CAD-coin for interbank transfers.

### Current Uses for Blockchain Technology:

- Proof of ownership of modules in app development
- Proof of ownership for digital content storage and delivery
- Proof of ownership for sales and purchase of digital assets
- Digital security trading: ownership and transfer
- Digitization of documents and contracts
- Decentralized storage using network of computers
- Digital identities to protect consumer privacy
- Escrow/ custodian service for gaming industry
- Smart contract IT portal executing order fulfillment
- Decentralized patient records management
- Proof of ownership for digital content
- Digitizing company incorporations, transfer of equity
- Decentralized IT resources for home and business
- Authenticity for employee peer reviews
- Point-based value transfer for ride sharing
- Decentralized prediction platform for share markets
- Anti-counterfeit digitization of assets

# Bitcoin Investigative Field Guide


Many departments develop a policy for handling digital evidence; some practices also apply to handling digital currency.

An effective cryptocurrency policy will address the following:

- Identify who is authorized to conduct Bitcoin seizures and transactions
- List internal and external notifications when a case involves Bitcoins
- Standard operating procedures for handling and preserving digital evidence
- Chain-of-custody instructions for devices containing digital evidence

It is highly recommended that your department set up an all-encompassing crypto-currency policy. Set up a department-controlled wallet on a secure machine and establish rules surrounding the process of seizing and storing Bitcoin. The address of the wallet should be easily accessible to allow the swift seizing of Bitcoin if it is encountered during the course of an investigation, due to its fungible and unique nature. Seizing a suspect and their computer does not mean seizing the Bitcoin; anyone in the world that the suspect trusted with their Bitcoin could move it in seconds. It is imperative to move the funds to an address that you control the private key to.
Refer to your local prosecutor or legal counsel for any details or steps taken after the funds have been seized.

A "wallet" is the Bitcoin equivalent of a bank account. Wallets provide an easy-to-use interface for an individual to receive, store, and send Bitcoin to other people. A wallet massively simplifies the complicated process of signing a transaction, broadcasting it to the blockchain, and verifying incoming transactions. In nearly all cases, it is as simple as typing in an address, a transaction amount, and hitting Send.

A wallet simply manages your collection of public/private key pairs. Wallets continuously check the global blockchain for transactions that are broadcast with one of your addresses as the receiver. When your wallet sees that you "own" Bitcoin according to the ledger, it updates your balance. When you want to send or forward your balance to someone else, you use their public key as the address, and release the funds of one of your public keys by signing the transaction with the corresponding private key.

Since anyone with the private key of an address has complete control over funds in that address, this gives Bitcoin a certain level of flexibility and control not otherwise found in fiat ("cash") currency. There could be multiple copies of the private key stored in multiple locations, or different people could have it. There is no central bank or system to freeze funds.

When seizing Bitcoin, it is essential to move the Bitcoin to a wallet you control, or they could be sent anywhere in the world in minutes, even if you have the suspect in custody and their device secured.

Since a wallet is simply a way of storing, managing, and securing your private keys that allow you to sign a transaction, different types of wallets offer different levels of ease-of-use and security. Wallets can exist in many different forms. The most commonly used is a

Source: *Bitcoin Investigative Field Guide,* by the National White Collar Crime Center, accessible online at https://www.nw3c.org/Resources/Bitcoin-investigative-field-guide/content/index.html#/?_k=kjt5dz

# Bitcoin Investigative Field Guide

software wallet, which is a program that runs on your computer or mobile device. There are also web-based wallets that you log into with an email or username and password.

The Cyber Crime Unit at the National White Collar Crime Center recommends the use of the Coinbase online wallet. Coinbase operates as a US-based exchange and is the only large Bitcoin service to have never suffered a security breach compromising customer or user information or funds. They are law enforcement-friendly and are willing to work with law enforcement to track funds, freeze user accounts, and otherwise assist in investigations however they can. They are an industry leader and are the largest US-based exchange.

Creating an account for their service involves identity verification, due to Know Your Customer laws. After successfully completing registration, you can log in and view your Bitcoin wallet with the Accounts tab at the top of the screen. Click "Receive" next to the Bitcoin wallet, and you will be prompted with a QR code to scan, if you have seized a mobile device storing Bitcoin, and a text string if it is a software or online wallet. Simply copy and paste the string into the input field in whatever wallet you're seizing funds from and dump the balance to secure the funds. You then have the choice of converting the seized Bitcoin to USD through your Coinbase wallet, to preserve the monetary value, or leaving it as-is to preserve the property and potential chain-of-custody.

The most common way of storing and securing Bitcoin is the computer wallet, which runs as an application on your computer. They are generally very easy to use, with clear indicators on-screen of how to transfer funds out. The most common computer wallets are Electrum, Armory, Bitcoin Core, and MultiBit-HD. These will typically be identified as an icon on the user's desktop. You can also use the Search function on the computer to look for any file with the word "wallet" in the file name, or a .dat file extension.

Almost every type of wallet uses a file with this naming convention, and a file like that existing on a computer is indicative of Bitcoin being in play.

A relatively new type of wallet, online wallets exist on a user's Android or iOS smartphone. This type of wallet is generally very simple and features a basic and intuitive interface designed for the average end-user who is just getting into Bitcoin. They can be identified by a logo or icon on the home screen of a smartphone. They are occasionally secured by an additional PIN or password with a lock-out feature if failed too many times. The most common wallets for mobile devices are Mycelium, Greenbits, breadwallet, and Airbitz.

Online wallets typically function as an extension of the exchange on which they were purchased. They are accessed through a website and require log-in information, and typically require a form of two-factor authentication as additional security.

The most popular exchanges and online wallet services are Coinbase, GDAX, Gemini, and Kraken. Many of these also serve as trading platforms, similar to a stock exchange. The 4 listed above all require proof of identity, due to Know Your Customer laws, and operate out of the United States. Coinbase and GDAX have been known to cooperate with law enforcement investigations in the past, surrendering customer information and purchase patterns.

Cold storage wallets can be more difficult to identify, as they are simply a website that was visited and used. The best way to identify these are through the suspect's browser history. Searching for "bit", "coin", or any of the four exchanges above will cover almost every commonly used exchange. If any of the other three types of wallets are found during the course of an investigation, it is almost guaranteed that the suspect used an online wallet at some point to either buy or sell their Bitcoin for US dollars, and it is worth looking into which exchange they used and attempting to obtain additional information about them from the exchange.

# Bitcoin Investigative Field Guide

*Investigative Note: Contact the online wallet service for assistance in freezing an account to prevent additional transactions.

Cold storage is an alternative way of storing Bitcoin, and by far the most secure. Since you need the private key to send Bitcoin, cold storage revolves around the idea of never exposing the private key to the Internet. This may mean writing it down on a piece of paper, storing it on a USB stick, or memorizing it. This type of wallet is much harder to identify, as it could be anything. If there is evidence of Bitcoin being in play, such as recently used Bitcoin exchanges, empty Bitcoin wallets, or recently visited websites explaining Bitcoin, it is possible that a cold storage wallet is being used.

Look for labeled USB drives, pieces of paper with 12 to 24 random English words (a recovery seed), or a long string of what appears to be gibberish or encrypted information. The information on the USB drive, the recovery seed, or the string of gibberish can all be imported into Coinbase to directly seize the funds without any technical knowledge needed.

Bitcoin should be collected as soon as possible once it has been determined that seizure is appropriate. Because there is a risk that a co-conspirator might drain a suspect's Bitcoin, time is of the essence.

**How to seize Bitcoin protected by encryption**

Step 1
As in all cases involving evidence, responding personnel should thoroughly document the scene.
When a Bitcoin wallet is discovered, access to it is often protected by encryption.
In the event the suspect's computer or mobile device is unlocked, follow best practices for maintaining the current state of the device to prevent it from locking from inactivity.

Step 2
Ensure you (or authorized person) have access to your department's Bitcoin wallet. You will need to know the credentials for accessing the department Bitcoin wallet. If there is no existing department Bitcoin wallet, DO NOT use a personal Bitcoin wallet.
Without a Bitcoin wallet, you cannot continue through the collection process. Please proceed to the "Preservation" section on page 14.

Step 3
If you can access the suspect's Bitcoin wallet:
To transfer a suspect's Bitcoin to a department Bitcoin wallet, you must have access to the private keys within his/her Bitcoin wallet.
Getting the suspect to volunteer the encryption code is the easiest method of access. If the suspect will not volunteer the encryption code, simply getting the suspect to admit he knows the encryption code is helpful in obtaining an order to compel the suspect to unlock the wallet.
If you cannot access the suspect's Bitcoin wallet:
The device on which the encrypted wallet exists should be seized in compliance with department procedures for seizing any other encrypted device. Officers should document the scene, keep the device powered, and call the department's IT specialist as soon as possible. Proceed to "Preservation" on page 14.

Step 4
Depending on the type of Bitcoin wallet encountered, follow the below process.

Mobile wallets: If the suspect is using a mobile wallet, the process for making a transfer is relatively simple. In the suspect's wallet, navigate to the transfer or send tab. Enter the department wallet's address or scan its QR code in the space labeled recipient. Enter the full value of the wallet as the amount to be transferred. Then press transfer or send to move the funds to the department wallet.

Software wallets: Generally, funds can be obtained from a software wallet using the same method as a mobile wallet. However, with a software wallet, the suspect's private keys may be available either within the wallet or stored elsewhere on the device. Access

# Bitcoin Investigative Field Guide

to a suspect's private keys gives indefinite access to the accounts associated with those keys. While it is not recommended that the officer attempt to access the private keys, it is important that the device is treated as an encrypted device and seized, even if the officer can transfer the Bitcoin.

Online wallets: If a suspect is using an online wallet, police can use the above method to transfer funds. Because online wallets use a third party to store Bitcoin funds, that third party can freeze accounts and assist in the seizure of funds left online. Police can do so using the same method to freeze traditional bank accounts, but the warrant or subpoena must be directed at the online wallet operator.

Hardware wallets: Because hardware wallets are external memory or paper QR codes containing private keys, they must be loaded into a wallet that allows private keys to be imported. For an officer seizing the property of a suspect, it is sufficient to secure the hardware wallet and get it into the hands of an IT specialist as soon as possible.

Often the private keys in a Bitcoin wallet will be hidden, but as long as the officer has access to the wallet the funds can be transferred.

It is important to remember that a wallet may actually have multiple files that are holding Bitcoin separately. If an officer is transferring funds from an open or unencrypted wallet, they should ensure that there are not multiple files in the wallet. There should be a tab that allows all the wallets within the program to be viewed. It is possible that individual wallets may be separately encrypted within the program. If that is the case, then the device should be seized as an encrypted device.

**How to seize Bitcoin not protected by encryption.**

Step 1
As in all cases involving evidence, responding personnel should thoroughly document the scene.

When a Bitcoin wallet is discovered not protected by encryption, you have complete access to all available Bitcoins.
In the event the suspect's computer or mobile device is unlocked, follow best practices for maintaining the current state of the device to prevent it from locking from inactivity.

Step 2
Ensure you (or authorized person) have access to your department's Bitcoin wallet. You will need to know the credentials for accessing the department Bitcoin wallet. If there is no existing department Bitcoin wallet, DO NOT use a personal Bitcoin wallet.
Without a Bitcoin wallet, you cannot continue through the collection process. Please proceed to the "Preservation" section on page 14.

Step 3
Depending on the type of Bitcoin wallet encountered, follow the below process.

Mobile wallets: If the suspect is using a mobile wallet, the process for making a transfer is relatively simple. In the suspect's wallet, navigate to the transfer or send tab. Enter the department wallet's address or scan its QR code in the space labeled recipient. Enter the full value of the wallet as the amount to be transferred. Then press transfer or send to move the funds to the department wallet.

Software wallets: Generally, funds can be obtained from a software wallet using the same method as a mobile wallet. However, with a software wallet, the suspect's private keys may be available either within the wallet or stored elsewhere on the device. Access to a suspect's private keys gives indefinite access to the accounts associated with those keys. While it is not recommended that the officer attempt to access the private keys, it is important that the device is treated as an encrypted device and seized, even if the officer can transfer the Bitcoins.

Online wallets: If a suspect is using an online wallet,

# Bitcoin Investigative Field Guide

police can use the above method to transfer funds. Because online wallets use a third party to store Bitcoin funds, that third party can freeze accounts and assist in the seizure of funds left online. Police can do so using the same method to freeze traditional bank accounts, but the warrant or subpoena must be directed at the online wallet operator.

Hardware wallets: Because hardware wallets are external memory or paper QR codes containing private keys, they must be loaded into a wallet that allows private keys to be imported. For an officer seizing the property of a suspect, it is sufficient to secure the hardware wallet and get it into the hands of an IT specialist as soon as possible.

Often the private keys in a Bitcoin wallet will be hidden, but as long as the officer has access to the wallet the funds can be transferred.

It is important to remember that a wallet may actually have multiple files that are holding Bitcoins separately. If an officer is transferring funds from an open or unencrypted wallet, they should ensure that there are not multiple files in the wallet. There should be a tab that allows all the wallets within the program to be viewed. It is possible that individual wallets may be separately encrypted within the program. If that is the case, then the device should be seized as an encrypted device.

Step 4
By successfully transferring Bitcoins from the suspect's wallet to the department, he/she (or anyone with access to the suspect's wallet) is no longer in possession of the Bitcoins.

The department's Bitcoin wallet should have controlled access to maintain accountability and integrity in the preservation of the digital evidence.

## PRESERVATION SECTION

### Prior to Collection

Preservation of a suspect's Bitcoin is especially important when the suspect may have co-conspirators. A third party with access to the suspect's private keys can drain the suspect's wallet of its funds before the officer can access the wallet.

Being proactive when Bitcoin is suspected to be in use is the best course of action. Having a department wallet and proper procedures in place before alerting the suspect to possible seizure of his or her assets will help streamline the process and minimize the risk of loss.

If it is not possible to transfer the Bitcoin to a controlled wallet immediately, treat the device as though it is encrypted. As such, officers should leave the device on. Move the mouse to avoid the device entering sleep mode; on a smart phone or other mobile device, it may be necessary to tap the screen. On a phone or mobile device, it is important not to search the phone without a proper specific warrant. Document the scene and leave as much of it unaltered as possible. As soon as possible, call a digital forensic expert for further instructions.

If the suspect has Bitcoin stored on a web based wallet, then the wallet provider can freeze the account with the proper administrative procedure, such as a warrant or a subpoena. Bitcoin stored on web-based wallets are especially vulnerable, so time is a significant factor.

### After Collection

Once a suspect's Bitcoin are in the department's Bitcoin wallet, they will be fairly safe and secure. If the department is using a web-based wallet, ensuring that the department is on a secure server or transferring the coin to either a software wallet and encrypting the wallet or placing the Bitcoin in cold storage can provide additional security.

Some wallets allow for a Bitcoin vault to be established, which allows the transfer of Bitcoins only if multiple

# Bitcoin Investigative Field Guide

parties approve of the transfer. Using a vault may provide even more security for the Bitcoin. However, once the Bitcoin have been transferred to a wallet controlled by law enforcement, the Bitcoin should be safe and adequately preserved.

Online wallets
Web-based wallet services and Bitcoin exchanges have historically been cooperative with law enforcement investigations. In the event you cannot seize Bitcoin from a suspect's wallet, attempt to obtain any username, ID or wallet number that may help identify the wallet in question.

## Investigative Use

### The challenge of anonymity

A common myth regarding the use of Bitcoin is that the identities of those involved in transactions are completely anonymous. This misconception has lead many criminals to pursue Bitcoin as a means to fund illicit activities such as money laundering, fraud, corruption, and criminal trafficking.

The Dark Web is a part of the world wide web that requires special software to access. Within this web, some sites are effectively hidden, as they have not been indexed by a search engine such as Google or Bing. Special markets, referred to as darknet markets, also exist on the dark web and sell illegal products such as drugs and firearms, or deal with sex and labor trafficking. The use of Bitcoin on the Dark Web has increased the challenges faced by law enforcement conducting criminal investigations.

### About the blockchain

A blockchain is a public ledger of all cryptocurrency transactions that have ever been executed. It constantly grows as completed blocks are added with a new set of recordings. Blocks are added in a linear and chronological order as transactions occur. The blockchain holds complete information regarding addresses and balances since the first transaction to the most recently completed block.

The blockchain is much like a full history of banking transactions, while blocks function as individual bank statements.

Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system. The full copy of the blockchain has records of every Bitcoin transaction ever executed. It can thus provide insight about facts like how much value belonged a particular address at any point in the past.

The blockchain is of particular interest to law enforcement due to its inability to be altered in any way.

### *Follow the money*

Bitcoin can be used to purchase goods, property, and services. The Securities Exchange Commission (SEC) also views Bitcoin as a security. Regardless if Bitcoin is considered money or a security, its value cannot be ignored. Bitcoin are often traded in the Dark Web to further anonymize criminals, but the money can ultimately be traced. Whether through legitimate Bitcoin exchanges or personal and business financial records, all money has a start and endpoint.

Through information sharing, multi-agency task forces, partnerships, training, and the use of cutting edge technology, the law enforcement community is enhancing its capabilities to respond to criminal activity involving cryptocurrencies such as Bitcoin.

Law enforcement can work with private companies to investigative cases involving cryptocurrencies. Three of the most well-known are listed below, with descriptions supplied by the companies. This listing does not in any way constitute an endorsement of these private companies by ROCIC or RISS.

**About Chainalysis (www.chainalysis.com)**
The transfer of value over the internet requires new methods of data analysis, visualization and actionable intelligence to protect the integrity of our financial system.

# Bitcoin Investigative Field Guide

Founded in 2014, Chainalysis is the leading provider of Anti-Money Laundering software for Bitcoin. With offices in New York and Copenhagen, Chainalysis works with global financial institutions, like Barclays and Bitcoin exchanges to enable every stakeholder to assess risk in this new economy. According to Chainalysis, customers have checked over $15 billion worth of transactions using their platform.

Through formal partnerships with Europol and other international law enforcement, Chainalysis' investigative tools have been used globally to successfully track, apprehend, and convict money launderers and cyber criminals.

**About BlockSeer (www.blockseer.com)**
BlockSeer's mission is to build a unified foundation of transparency for the public Bitcoin ecosystem. Bitcoin is a revolutionary new technology that has the potential to enable many valuable new services that are fully trusted. Currently, there is a lack of clarity in Bitcoin payments and transactions. By providing transparency of the Bitcoin blockchain and its participants, BlockSeer aims to reduce the level of disorder and chaos and increase the level of knowledge and analysis of the publicly accessible blockchain network.

**About Elliptic (www.elliptic.com)**
Elliptic has delivered robust evidence for law enforcement agencies worldwide.
We trace Bitcoin transactions across hundreds of entities and help you connect illicit Bitcoin activity to real world actors.
Our proprietary database links millions of Bitcoin addresses to thousands of clear web and dark web entities. We back this up with transparent documentary evidence.
We have delivered actionable evidence in cases involving international arms trafficking, money laundering, theft, and drug offences.
Elliptic allows you to link real-world actors to Bitcoin activity. Our proprietary technology has proven effective in major international investigations.
Elliptic's results are backed by our proprietary database of evidence spanning millions of Bitcoin addresses across thousands of clear and dark web entities.

## Technical Assistance

The National White Collar Crime Center provides technical assistance to law enforcement and regulatory agencies in the areas of Cybercrime and Financial Crime. Technical assistance examples includes providing guidance in handling financial investigations and proper handling of electronic evidence (smartphones, computers, etc.).

## RESOURCES FOR LAW ENFORCEMENT

**ROCIC:**
Publications Manager Mark Zimmerman, mzimmerman@rocic.riss.net
Training Manager Ms. Jarret Miller, jamiller@rocic.riss.net
Criminal Intelligence Unit Manager Kendall Neal, kneal@rocic.riss.net
Analytical Unit Manager Cindy Purviance at cpurviance@rocic.riss.net
ROCIC, 1-800-238-7985

"Penetrating the Darknet: Silk Road, Bitcoins, and the Onion Router," ROCIC Special Research Report
http://rocic.riss.net/publications/darknet/Pages/default.aspx

"Hack Attack! Protecting Data Networks From Cyber Criminals," ROCIC Special Research Report
http://rocicuag.riss.net/publications/hack_attack/Pages/default.aspx

**BOOKS:**

*Future Crimes,* by Marc Goodman, Doubleday, 2015

*Digital Gold,* by Nathaniel Popper, HarperCollins, 2015

*Mastering Bitcoin,* by Andreas M. Antonopoulos, O'Reilly Press, 2015

*An Introduction to Systems Science,* by John N. Warfield, World Scientific, 2006

*Good Money, Part I: The New World,* by F. A. Hayek, Ed. By Stephen Kresge, Liberty Fund Press, 1999

*Good Money, Part II: The Standard,* by F. A. Hayek, Ed. By Stephen Kresge, The University of Chicago Press, 1999

*Denationalization of Money: The Argument Refined,* by F. A. Hayek, The Institute of Economic Affairs, 1990

*The Ascent of Money: A Financial History of the World,* by Niall Ferguson, Penguin Press, 2008

*Free to Choose: A Personal Statement,* by Milton Friedman and Rose Friedman, Harvest Book, 1980

*The Psychology of Communication (The Magic Number Seven essay),* by George Miller, Penguin Press, 1969

*The General Theory of Employment, Interest, and Money,* by John Maynard Keynes, Harvest Book, 1964

**BITCOIN INDUSTRY WEBSITES:**

Tennessee Bitcoin Alliance
http://tennesseeBitcoin.org/

LocalBitcoins.com
https://localBitcoins.com/accounts/login/

Bitcoin Foundation
https://Bitcoin.org/en/faq

Coinbase
https://www.coinbase.com/what-is-Bitcoin

## RESOURCES FOR LAW ENFORCEMENT

Bitcoin Charts
https://blockchain.info/charts

Bitcoin Stats
https://blockchain.info/stats

Google Bitcoin, then News

CoinDesk
http://www.coindesk.com/

Bitcoin Price Index
http://www.coindesk.com/price/

The Onion Router Project
https://www.torproject.org/

**GOVERNMENT WEBSITES:**

Financial Crimes Enforcement Network (FinCEN) Support of Law Enforcement
http://www.fincen.gov/law_enforcement/les/

Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies
http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

FBI Cyber Crime
http://www.fbi.gov/about-us/investigate/cyber

National White Collar Crime Center
https://www.nw3c.org/Resources/Bitcoin-investigative-field-guide/content/index.html#/?_k=kjt5dz

**MEDIA WEBSITES:**

BloombergView (currency-Bitcoin)
http://www.bloombergview.com/topics/currency

BitBeat: Wall Street Journal
http://blogs.wsj.com/moneybeat/tag/bitbeat/

Wired magazine
http://www.wired.com/tag/Bitcoin/

**COMMERCIAL WEBSITES:**

Elliptic
https://www.elliptic.co/

Chainalysis
https://www.chainalysis.com/

BlockSeer
https://www.blockseer.com

# ROCIC Can Assist Officers with Investigations

## ROCIC Training and Officer Safety Resources

### ROCIC Criminal Intelligence Unit

The Intel Specialists with ROCIC's Criminal Intelligence Unit (CIU) can access dozens of research tools, specialized databases, public record information, criminal justice information, and data. They are able to search, retrieve, compile, and provide a consolidated reporting of findings to officers. This assistance helps officers in need of quick, accurate, and complete information. Information gained by ROCIC can help develop leads, link criminal activity, gain background information on suspects, and quickly obtain driver's license photos.

### RISSIntel

The RISS Criminal Intelligence Databases (RISSIntel) provides for a real-time, online federated search of RISS and partner intelligence databases, including state systems. Millions of intelligence records are available via RISSIntel. These records include individuals, organizations, groups, and associates suspected of involvement in criminal activity, as well as locations, vehicles, weapons, and telephone numbers.

## Other ROCIC Resources

### ROCIC Publications

Additional training publications can be found on the ROCIC Publications webpage, including topics on fraud, credit card crime, virtual currencies, forged identification, gift card scams, burglaries and thefts, crimes against the elderly, among others. These publications can be accessed by logging into your RISSNET account at https://rocic.riss.net/publications.

### ROCIC Law Enforcement Coordinators

The ROCIC Law Enforcement Coordinators have specialized email lists to get your information out as fast as possible to jurisdictions that might be affected by similar cases.

### ROCIC Analytical Unit

The Analytical Unit converts complex information into easy-to-understand charts and presentations. The Audio and Video Forensic Department can enhance photos and video surveillance footage. The Computer Forensics Department assists in collecting evidence from electronic devices.

### ROCIC Technical Services

The ROCIC Technical Services Unit loans specialized equipment to member agencies at no charge, including surveillance cameras and recording devices.

### ROCIC Training Department

The ROCIC Training Department offers numerous training opportunities for police officers, including operational planning, social media, civil unrest planning and response, risk avoidance, crime scene management, and others. Training courses can be found at www.rocic.com/training.

### ROCIC Officer Safety Website

RISS also offers officer safety resources on their Officer Safety Website, including concealment methods, law enforcement threats, gangs, narcotics, domestic terrorism, sovereign citizens, and armed and dangerous subjects. This information can be accessed by logging into your RISSNET account at https://officersafety.riss.net.

More information on RISS and ROCIC resources can be found at www.riss.net.

This project was supported by Grant #2015-RS-CX-0005 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.