Version 1.09

Last Update: 03/02/2017

A guide for bitcoin investigators

European Cyber Crime Centre (EC3)
Europol, The Hague, Netherlands
o3@europol.europa.eu

The objective of this guide

The guide should serve as a source of practical information covering aspects of the technology that are relevant for the investigators. The first part will cover wallets, addresses, network and transactions, addressing these from the law enforcement (LE) point of view, while the second part will mainly focus on online investigation, addressing issues of tracing and attribution.

The information provided in this guide was often collected through experiments and observation and therefore it may contain claims you would like to challenge. If this is the case, please direct your questions/comments/suggestions to the author of the guide.

What is covered:

- ✓ Anatomy of a bitcoin transaction
- ✓ Bitcoin wallets and addresses
- ✓ Tracking of bitcoin payments
- ✓ Identification of bitcoin users
- ✓ Bitcoin seizure
- ✓ Cooperation with the private sector
- ✓ Examples of criminal abuse of bitcoin

What is not covered:

- × Centralised virtual currencies
- × Altcoins
- × Legitimate use of bitcoin
- × Decryption of messages in bitcoin blockchain
- × Non-monetary use of blockchain technology
- × Bitcoin price considerations
- × Bitcoin legislation issues

Highlights of the guide

Most readers will not read the guide in its entirety and will instead focus on what is most important for them. The following chapters are likely to be of highest relevance for the investigators:

Contents

Introduction

Bitcoin was not the first virtual currency. Centralised digital currencies have been coming and going since the 1990s. Yet, its popularity over the last few years has been so great that many people have started using the terms 'virtual currency' and 'bitcoin' interchangeably. The logical questions are: why is it so and why are we still primarily talking about bitcoin and not another virtual currency?

While other virtual currencies such as E-gold or Liberty Reserve were in existence before the advent of bitcoin, they suffered from the fact that they were run by centralised entities. This made them relatively easy to take down once it was established that they facilitated criminal activity.

Back in 2009, bitcoin emerged as the first decentralised digital currency. This meant that for the first time in history, one person could send a secure payment directly to another without using a third party as an intermediary.

Instead of trusting companies and institutions, bitcoin users put their faith into a system built on an elegant and very well thought-through mix of online technologies and cryptography. Practically all decentralised currencies we know nowadays are more or less derived from bitcoin and due to their dependence on cryptography they are often referred to as cryptocurrencies.

To date, bitcoin remains the most important cryptocurrency that boasts over €10 billion in market value. Its increasing adoption allows for a practical legitimate use including investment, trade, person-to-person transactions or payment for goods or services online. However, a global digital currency that allows for reliable, fast and irreversible online transactions, has no central control or built-in KYC mechanism and is relatively difficult to trace is practically guaranteed to be abused by criminals. And indeed, the abuse is occurring with an increasing frequency as the criminals have gradually accepted it as a currency of choice for trade in the darknet and various extortion or fraudulent schemes.

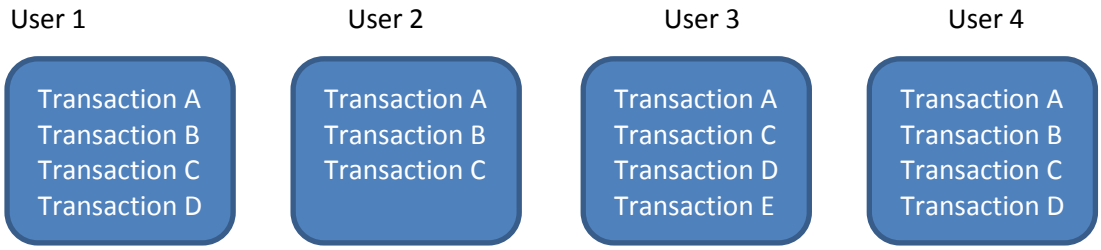
Yet, bitcoin is far from completely anonymous. Yes, it is true that bitcoin blockchain itself does not reveal any information that could lead to identification of a payer and a recipient. On the other hand, a combination of open source research, commercial tools and information provided by private sector can lead to identification of suspects and their financial activities — and this is exactly what this guide is about.

How bitcoin works in a nutshell

Bitcoin 101

Bitcoin is a digital currency that is stored on bitcoin addresses sitting in bitcoin wallets. All transactions moving bitcoins from one address to another have to be electronically signed and then are propagated to the bitcoin network. The peer-to-peer nature of the network does not mean that the knowledge about the transaction is limited to two parties — sender and the receiver. On the contrary, all transactions are propagated across the whole bitcoin network to make sure every single participant hears about them.

Each of the participants keeps a log of all incoming and outgoing transactions. However, due to network latency and other reasons, different users may keep track of different sets of transactions at any moment:



Nevertheless, digital currency must be an exact science that cannot allow the existence of multiple different logs. Therefore, one of these logs must be the chosen one that gets accepted by the rest of the network.

The 'right' log is decided by a brute-forcing competition called mining. Every couple of minutes, one of the computers participating in the mining competition wins a privilege to append their log of recent transactions to the blockchain, which contains all the previously validated bitcoin transactions ever made. The primary task of the miner is to collect and validate transactions of other participants. To avoid abuse of the system, miners cannot create transactions on behalf of anyone else.

Mining costs resources — mining hardware and electricity. In order to motivate miners to spend resources on validating the transactions, the winning miner receives a reward in form of newly generated bitcoins generated out of nowhere and landing into their bitcoin address.

This elegant reward scheme not only motivates miners to validate transactions, it also makes sure bitcoins are created at a transparent, predictable and limited rate. Indeed, bitcoin mining is the only way new bitcoins are introduced into circulation; all 15.87 million bitcoins in existence as of 15 September 2016 were initially received by the miner.

Having understood the basic and very simplistic explanation of how bitcoin works we can have a closer look at individual components of bitcoin technology, particularly focusing at those that may be of relevance to investigators.

Public and private keys and bitcoin addresses

Before looking at how transactions work and can be traced, we will inspect what private and public keys are and how they work. The topic will be looked at from the LE viewpoint, particularly regarding their different formats, safe manipulation and seizure.

A bit of theory first

Bitcoin is based on a combination of several technologies, one of which is a public key cryptography dictating that two different keys are required to send and receive transactions. A public key can be distributed to anyone in order to receive a payment while the private key that should only be known to its owner is used to create a signature for a transaction that cannot be forged.

Public key cryptography solves two fundamental problems all digital currencies face:

- It allows users to uniquely identify their addresses in the system.
- It prevents users to spend coins they do not own.

Key addresses v. wallets

Both the private and public keys are stored in a bitcoin wallet. One person can possess any number of bitcoin wallets and each wallet can store any number of private keys. These private keys are used to generate public keys. A public key, when hashed, turns into a bitcoin address, which will be demonstrated later in the chapter.

Bitcoin addresses can be — with a bit of simplification — thought of as bank accounts or email addresses as they can be publicly shown to anyone to receive payments. However, unlike bank accounts or email addresses, which keep their content private, knowledge of the bitcoin address reveals bitcoin balance and transactions sent to and from this address.

A private key acts as a lock for the bitcoin addresses. The owner of a private key has access to the funds stored on the corresponding bitcoin address. This means that the owner can move funds from his address to any other address of his choice. It is not possible to derive a private key from a bitcoin address and therefore it is absolutely safe to share the bitcoin address.

The owner of a private key has unrestricted access to the funds in the corresponding bitcoin address. A very telling proof of this fact was given by a Bloomberg TV reporter, whose bitcoins were stolen after he exposed his private key on television. All that was necessary was to take a photo of the screen, take a note of the private key, import it into a wallet and send bitcoins to new owner's address. This shows that a private key should, as its name suggests, be kept private[1].

Private keys and bitcoin addresses are commonly stored in a wallet within a wallet.dat file. Both file and private keys are perfectly portable. The file can be copied from one drive or USB key to another and the private key can be exported to another bitcoin wallet. All of the above fundamentals apply not only to bitcoin but to other cryptocurrencies as well.

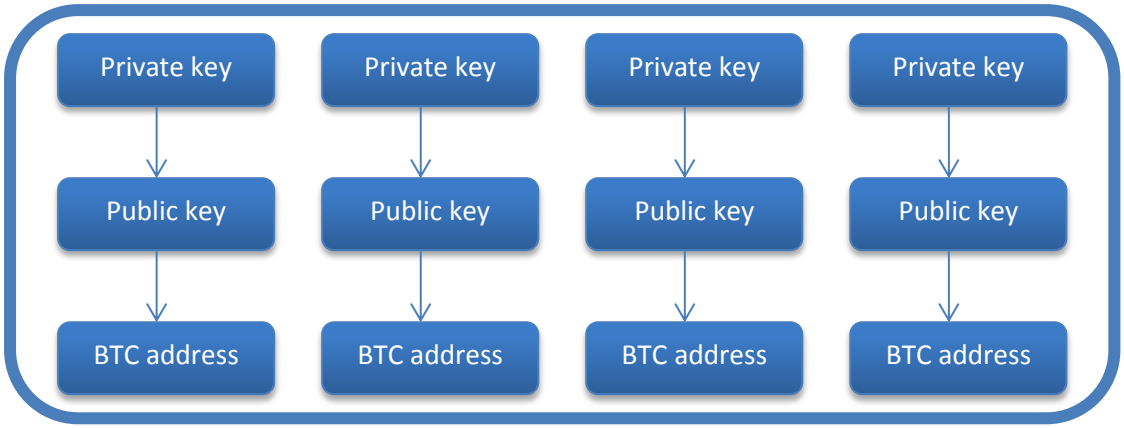
Relationship between private key, public key and bitcoin address

Practically every active bitcoin user ends up with a wallet that contains multiple private keys and corresponding public keys and bitcoin addresses. Each bitcoin address has a balance that can have either zero or a positive non-zero value. The sum of the balances for all addresses in the wallet is the total balance that the wallet holds and that can be spent.

Each transaction results in one or more bitcoin address spending the entire previously received payment. For example, if there are three bitcoins received by a bitcoin address and the user decides to use this address to pay 2.5 bitcoins, the final balance of the address will not be 0.5 bitcoins as one could intuitively expect. Instead, all bitcoins on the address will be spent. This will be practically demonstrated in the bitcoin tracing section.

There is a 1:1:1 relationship between the private key, the public key and the bitcoin address. The bitcoin address is mathematically derived from the public key and the public key is derived from the private key.

Bitcoin wallet



[1] EC3 Cyberbit on bitcoin transactions, May 2016.

While the bitcoin address can be derived from the private key almost instantly, doing it the other way around is computationally impractical. A sequence of different hashing algorithms would have to be deciphered, making the reverse engineering of the private key practically impossible.

Multi-signature transactions

The vast majority of bitcoin addresses are between 30 and 35 characters long and start with a number 1. However, those who have already spent some time looking at the blockchain may also have noticed bitcoin addresses starting with number 3. These addresses are called pay-to-script (P2SH) hash addresses. These addresses are not managed by the owner of the private key; instead, a script determines what happens with the transaction. This topic can be quite technical and there are some excellent sources online for those interested in finding out more about P2SH transactions.

For an investigator, it is enough to know that by far the most popular example of a pay-to-script hash address is a multi-signature transaction, where multiple keys have to sign a transaction to release funds — for example, *3KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM*

Multisignature transaction: M out of N private keys are required to sign a transaction.

While multisignature transactions have a legitimate purpose, they are often employed by darknet marketplaces, where two out of three actors including buyer, seller and administrator of the marketplace must sign the transaction for the seller to receive it. This feature, when used properly, protects buyers and prevents so-called exit scams where a darknet administrator decides to close the shop and to pocket all bitcoins on the escrow account.

Strings to watch for at the crime scene/in the suspect's computer

There are three most common representations of the **private key**:

1. Hex: *1E79423A4ED27608A15A2616A2B0E5E52CED330AC530EDCC32C8FFC6A520AED1*
2. Private key is longer than the bitcoin address and starts with number 5: *5J3hzQ41KoJX64H5YRTqS9YB9LVGacU2qusL37Ys1eVpJTgnr4u*
3. Compressed private key may look similar but starts with either K or L: *KyoPrwwmvSZymMrJLRhePV6jTFFpGU6uMVLv5nQhkMM4dpDKaMgG*

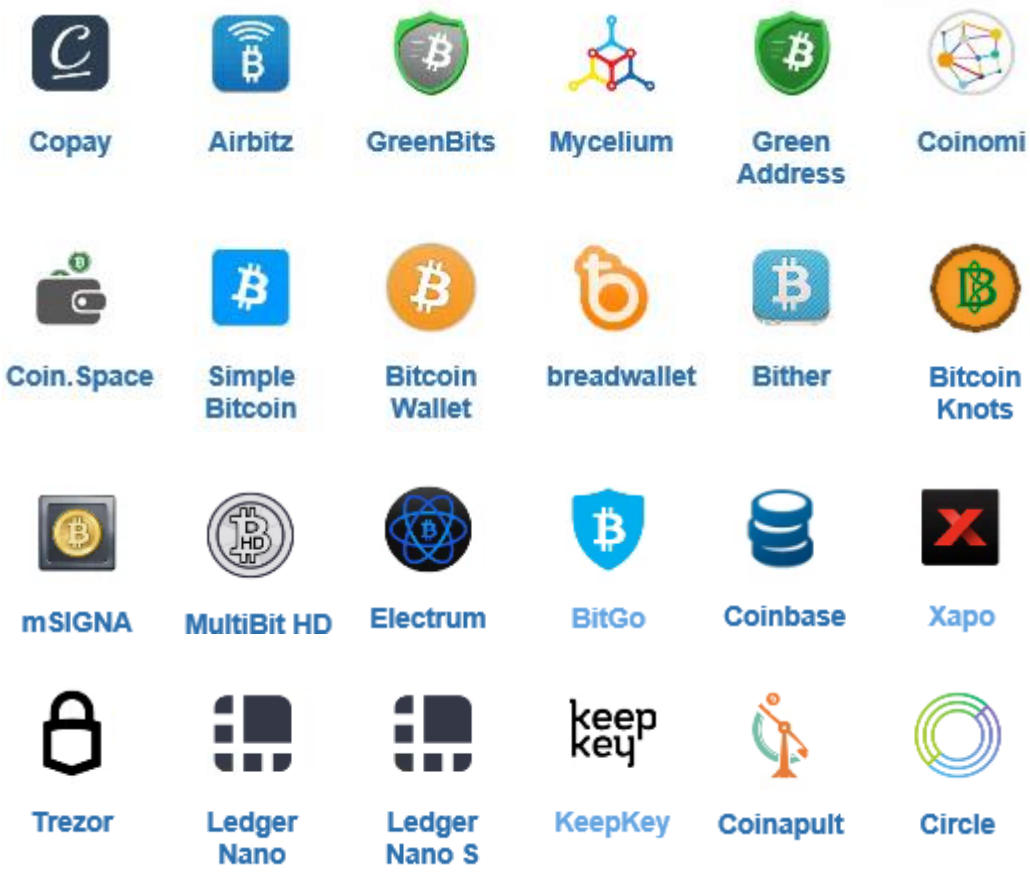
In addition, there are three most common representations of the **public key or a bitcoin address**. A public key is rarely found; what is usually discovered on paper or in electronic form is a bitcoin address:

1. Public key: *04e2ff72520d37d88c61d0bac1caa6fccec4ffefd372d22247686affa1ebdeea52d0dd21354ed98d2173abee0977ce4c62648290fb34fe172f0153b98bf132fc66*
2. Normal bitcoin address: *13mE8VYvGym8Rj9ddHoagcNxmDs1SaxbNJ*
3. Pay-to-script hash bitcoin address: *3KgtbGgaX2ngstNpvyv7LwpHSweVeqGbpM*

For more details on format and creation of keys and addresses please refer to *Appendix 2: Format of keys and addresses*

What should also be watched for is the presence of use of typical bitcoin services including wallets or exchangers. The evidence may be found in form of notes and other printed documents or electronic evidence such as running applications, processes, icons, browsing history etc. The following names and logos of wallets and online exchangers may all suggest that the suspect is an active bitcoin user:

Most Popular Bitcoin Wallets:



Most Popular Bitcoin Exchangers and Payment Processors:

Practical Bitcoin Forensics

When it comes to bitcoin forensics, some investigators only scan the storage media using keyword "bitcoin". While certainly worth trying, this check is not sufficient as storage media may contain bitcoin artefacts without using the actual keyword.

Those searching for bitcoin addresses may have come up with a basic regexp string, starting with 1 or 3, followed by another 25-34 characters), which can be expressed as:

^[13][a-zA-Z0-9]{26,35}$

The more knowledgeable ones may even factor in the Base58 encoding[2], that excludes characters that may appear as visually ambiguous: 0,O, I (uppercase i) and l (lowercase L). This excludes many irrelevant strings from the results.

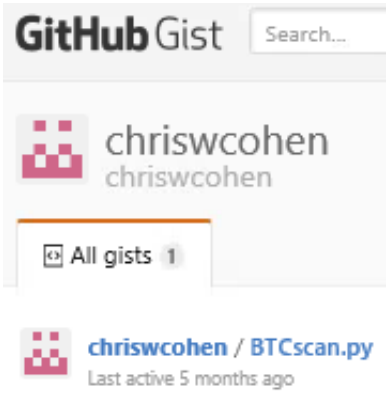
^[13][a-km-zA-HJ-NP-Z1-9]{26,35}$

or

^1[1-9A-Za-z][^OIl]{26,35}$

However, even these searches can collect a lot of irrelevant strings. Fortunately, the search process can be further improved by validation of the last four bytes of the bitcoin address string. These four bytes should correspond to a double SHA256 hash of the preceding string[3]. Implementation of this base58check validates the bitcoin address and practically eliminates any false positives.

Unlike regular expressions, the validity check is much harder to implement. For this reason, Chris Cohen, Computer Forensic Investigator at South West Forensics (UK LE), developed a very practical script that can be used to search storage media for bitcoin addresses.



To this day there does not seem to be any other forensic tool, free or commercial, able to search for base58check strings. Additionally, the tool also searches for other valuable artefacts including different formats of private keys.

BTCscan is an open-source tool developed in python that does not require any setup[4]. The latest version of BTCscan can be downloaded from https://gist.github.com/chriswcohen/7e28c95ba7354a986c34. The tool has a command line interface but that should not make it prohibitive to novice investigators.

[2] Further explored in Appendix 2
[3] Also detailed in Appendix 2
[4] Assuming Python is already installed. If this is not the case, Python can be downloaded from https://www.python.org/downloads/. Make sure to download version 3.0 or higher.

The only mandatory argument is -i/--input which is used to specify drive, directory or file that will be searched through so the command can by as simple as:

python BTCscan.py -i suspect_usb1.dd

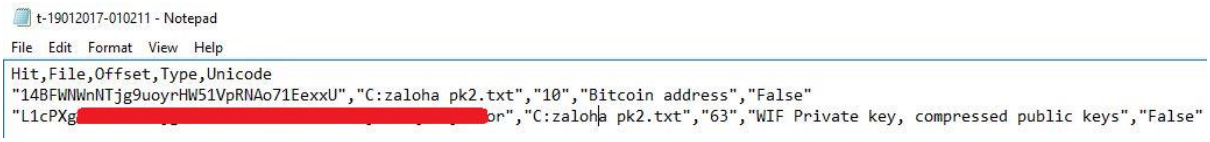
or

python BTCscan.py --input =”C:\”

After the command is executed, investigator is asked to provide a case name that will form a part of an output file. Though described by the author as “not a fully-fledged forensic tool” it actually is very effective. In the example below the tool recovered 2 files which it then recorded in a .csv file:

```
C:\Users\Dr\Desktop\Python>python BTCscan.py --input="C:\"

BTCscan 0.9 by Chris COHEN (chris.w.cohen@gmail.com)

Website: https://gist.github.com/chriswcohen/7e28c95ba7354a986c34
Donations: 1BnvsBZcyVxF8L8HboUcDc2mAUu9K2qsTe

If you find BTCscan to be of use to yourself, organisation or company then I
politely ask that you write me a very short email letting me know how it
worked out for you. This information will never be published - it is solely
for my own personal interest.


Case name: test

Scanning: C:BTCscan.py (13981 bytes)
Scanning: C:cmd.exe (232960 bytes)
Scanning: C:test-18012017-234804.csv (0 bytes)

2 files examined
2 Base58Check matches found
246941 bytes examined
0.03 seconds processing time

Output file: test-18012017-234804.csv
```

The content of the CSV file reveals extracted bitcoin address as well as the private key:



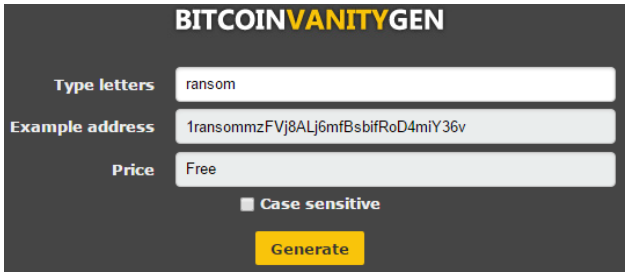
Beware, the tool only works with Python 3.0 and higher. Version 2.7 which is still used by many investigators is not supported and the script will stop after *Case name* is entered.

BTCscan searches through all folders and subfolders. Note that the tool does not search for encrypted or compressed items so a suspiciously looking compressed files may have to be manually unpacked before running the BTCscan. Also, the tool will not look into forensic areas (unallocated clusters or alternate data streams). On the other hand, it may recover items from files associated with bitcoin software and cache files from bitcoin related websites, as long as these are in ANSI and Unicode format.

Bitcoin vanity addresses

Some users or services own a personalised bitcoin address. These addresses have a non-random looking text at the beginning or at the end such as 1Peter. These addresses are often referred to as vanity addresses. Probably the most well-known example is **1snow**qQP5VmZgU47i5Awwz9fsgHQg94Fa created by Wikileaks to fund Edward Snowden's legal defence. This address received almost 200 bitcoins in individual contributions as of 1 May 2016.

It is relatively easy to obtain such address. Several tools such as bitcoinvanitygen can generate vanity address for free or in exchange for a small fee.



A word of warning before generating your very own '1TopCop' address: one should be careful when using unverified third party services such wallets or address generators, as these services may keep a copy of the private key and steal bitcoins once a payment arrives at the address. Bitcoin fora are filled with claims of those who had their funds taken from vanity addresses: *1*, *2* and *3*.

To mitigate such scams, it is important to avoid using sites and applications that have not developed a strong reputation among the bitcoin community. One should stick to the common types of wallets and avoid using vanity generators altogether. If there is a genuine need, only verified tools that have earned the trust of the community, such as the Vanitygen command line tool, should be considered. Vanitygen runs on a local computer that is effectively brute forcing bitcoin addresses until it generates a bitcoin address containing the desired text string. Those who do not possess decent hardware can use cloud solutions such as AWS or Vultr and run Vanitygen remotely.

The tool is straightforward to use; the command *vanitygen* is followed by a desired string starting with number 1. For illustration, the private key with a bitcoin address starting with 5 case-sensitive characters took about 3 minutes to generate on a computer with i7 processor:

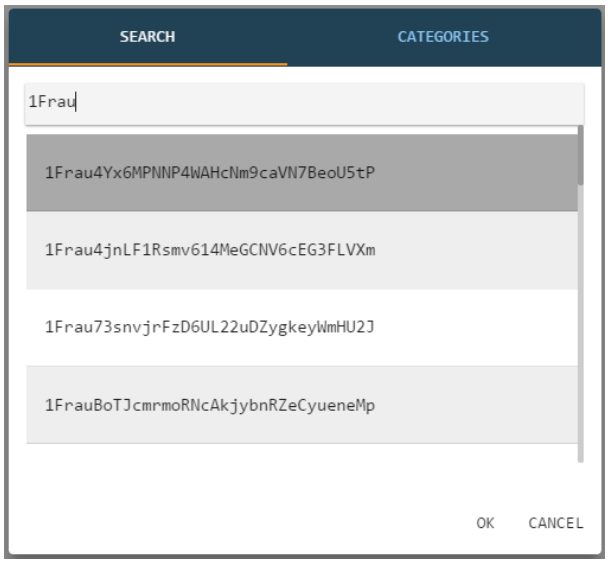
```
C:\Users\Drobek\Desktop\bitfixer\willitblend\Vanity>vanitygen 1Jarek
Difficulty: 259627881
Pattern: 1Jarek
Address: 1Jarekr84LN18Rqc1Vrqmpfb4ezuLoLPdj
Privkey: 5JYnZtPvQfeJQxR1SaH8BHuEYEXgFaY5AAo5koiGNvw9vfhqHZG
```

However, those who have a decent graphic card can instead use command *oclvanitygen* that takes advantage of GPU instead of CPU and can perform the above calculation in a few seconds.

```
C:\Users\Drobek\Desktop\bitfixer\willitblend\Vanity>oclvanitygen 1Jarek
Difficulty: 259627881
Pattern: 1Jarek
Address: 1Jareko295176f2JMreqdopGyi8KSVCpCf
Privkey: 5JnZZ6n9tnYkfG1FrrSuETLKkA3stE9PMrvBZYEbuMJcwB6GkrA
```

Handling partial bitcoin addresses

Sometimes an investigator may come across hardly legible bitcoin addresses either in the form of handwritten notes or printed notes, where part of the address is missing or is illegible. This may constitute a problem, because the free online blockchain explorers do not typically search for a part of bitcoin address. This is where the commercial tool Chainalysis with built-in autocomplete functionality comes in useful [5].



It only takes a first few characters to get a complete bitcoin address filled in. This functionality may also be useful with perfectly legible bitcoin addresses that are only available on paper, in which case it is again possible to enter the first few letters of an address before the autocomplete kicks in. Such a feature not only increases convenience but also prevents human error, which is quite likely to happen when transcribing long random strings.

[5] UPDATE: Other commercial tools such as Elliptic also added such functionality in late autumn 2016.

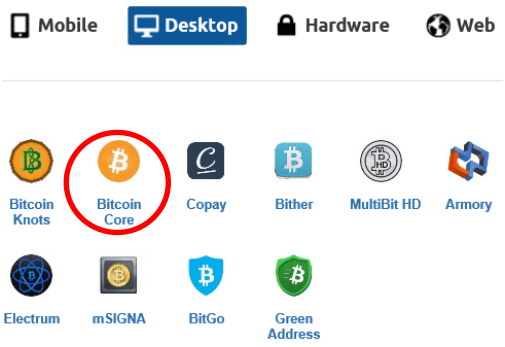
Bitcoin network: what it is and how it operates

In order to have the ability to send and receive bitcoins, one has to download a bitcoin client or a bitcoin wallet (these terms can be used interchangeably). There are many different types of bitcoin wallet to choose from. The original bitcoin client called Bitcoin Core, which is still very popular, requires the user to download the full blockchain in order to work properly.

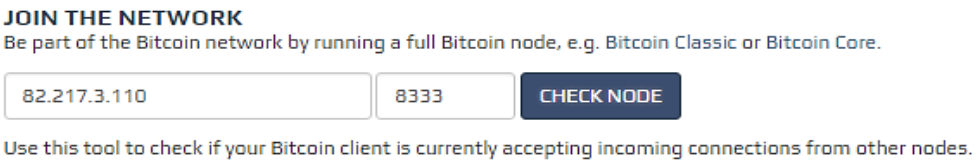
Nowadays it may take several days for the client to download the bulky blockchain and bring it up to date. Once the blockchain has been downloaded and is fully in sync with the rest of the bitcoin network, the wallet displays a correct balance, which is a total amount of bitcoins available on all bitcoin addresses stored within the wallet. It also displays a list of recent transactions where bitcoins were received or spent.

Bitcoin clients connect to other clients and form a bitcoin network. The main purpose of the network is to verify and propagate all transactions across the network so that all participants across the network become aware of all transactions. Active wallets that contain blockchain and can verify the transactions and disseminate these further are commonly referred to as nodes.

Anyone can run a node. All that is required is a computer and a decent connection to the internet. All the user has to do to run it is to download and install a bitcoin wallet, for example Bitcoin Core from the bitcoin.org website:



There are no registration forms to fill in or KYC requirements to comply with. Additionally, if bitcoin port 8333 is not blocked by a firewall, the wallet starts functioning as yet another full node in the bitcoin blockchain. When in doubt, users may check whether the IP address of their node features on bitnodes.21.co: if it is not, the firewall settings are usually to blame.



All nodes in the network are created equal — there is no central or privileged authority. All network communication between nodes is made over TCP, one of the core internet protocols. Users can decide to join and leave the network at any time and inactive or non-responsive nodes are by default forgotten after 3 hours.

Essentially, the more full nodes there are out there, the more resilient and robust the network. Despite the decreasing trend, the current number remains more than sufficient to keep the network secure and decentralised. Out of the 6 000, about one-third is hosted in United States, followed by Germany, France, the Netherlands and the United Kingdom. It is not surprising to see these

countries leading the list as they offer good value for money when it comes to hosting and cloud services.

Top 30 countries hosting accessible bitcoin nodes

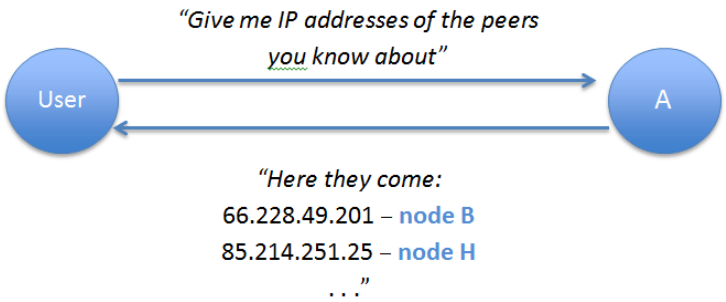
1. United States (1736)	2. Germany (757)	3. France (389)
4. Netherlands (335)	5. Canada (297)	6. United Kingdom (269)
7. n/a (233)	8. Russian Federation (156)	9. China (141)
10. Australia (91)	11. Sweden (85)	12. Switzerland (80)
13. Japan (73)	14. Singapore (62)	15. Ukraine (56)
16. Hong Kong (51)	17. Ireland (49)	18. Italy (47)
19. Spain (45)	20. Poland (43)	21. Korea, Republic of (41)
22. Bulgaria (40)	23. Brazil (38)	24. Norway (38)
25. Czech Republic (36)	26. Finland (33)	27. Lithuania (31)
28. Austria (28)	29. Taiwan (28)	30. Romania (24)

Source: bitnodes.21.co

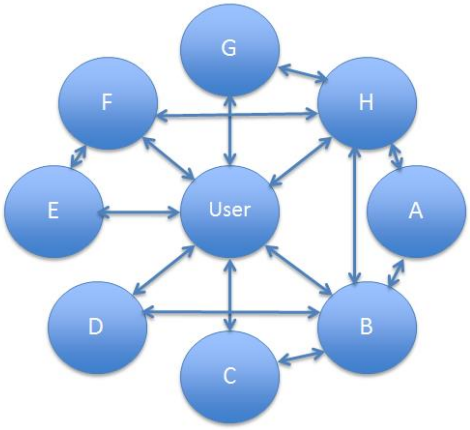
There are no financial incentives for running a full node and promoting the transaction throughout the bitcoin network, which, combined with a rapidly increasing size of the blockchain resulting in correspondingly increasing storage requirements, has led to a decrease from about 10 000 nodes in the beginning of 2014 to less than 6 000 accessible nodes in September 2016. By default, each node can provide up to 125 connections to the network. Assuming the average user is connected to five or six nodes at the same time, the current network could, without any impact on the quality of service, support at least 150 000 wallets running concurrently.

Network communication

When a node is started, it tries to establish a connection to other nodes in the network. First, the node either tries to connect to IP addresses of so-called seed nodes that are hardcoded into the client. Users can also manually connect to a node of their choice when they start their node with *bitcoind –addnode=<IP address>.* After the connection is established, the node requests the IP addresses of other nodes to which it subsequently connects.



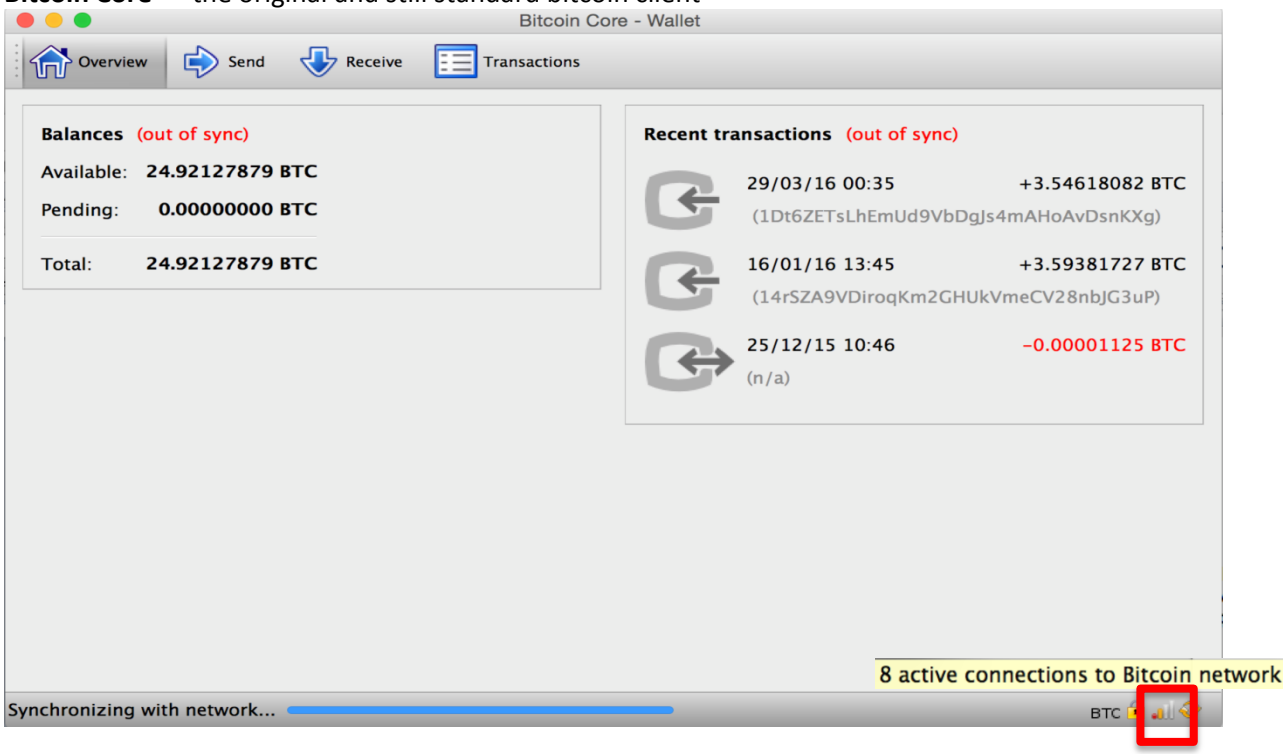
The discovery procedure then repeats with the user contacting nodes B and H, which will share a different set of nodes they are connected to, and this process iterates for as long as it is required. At the end, the client might be connected to a default number of eight nodes.



In practice, the majority of the network activity is not visible to the end user. In most cases the software takes care of the node discovery, connectivity and download of the blockchain from the identified peers, which is indicated on the lower right corner of the bitcoin client.

The network activity changes from '*No Source discovered*' to '*Synchronising with network …*'. At the same time, users can easily see how many nodes they are connected to when they move the mouse over the icon that looks like a wi-fi strength indicator.

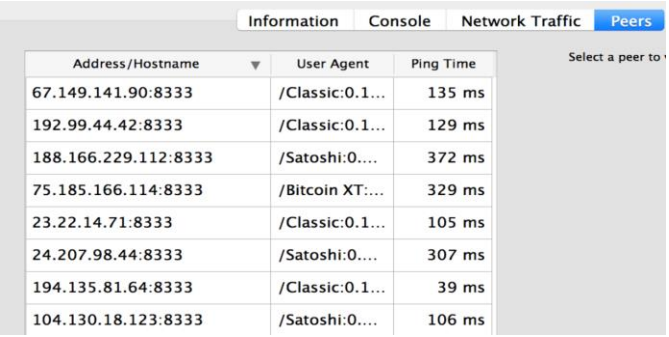
Bitcoin Core — the original and still standard bitcoin client



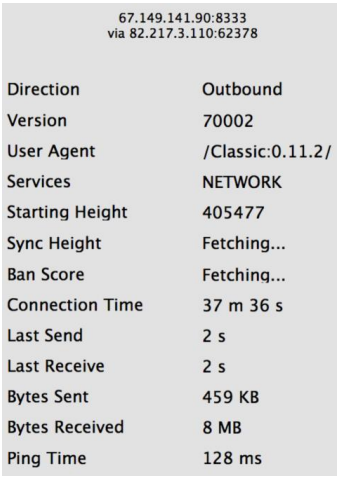
Inspecting a suspect's wallet

The most obvious findings the investigator will discover include balance and lists of incoming and outgoing transactions and bitcoin addresses controlled by the wallet. However, there is more to be discovered on closer inspection.

The IP addresses of the nodes the client is connecting to can be found in the standard Bitcoin Core client (*Help -> Debug Window -> Peers* on both PC and Mac wallet):



The same information can be received by typing '*getpeerinfo*' into the bitcoin console. When any of the peers is selected, metadata about connection is displayed. Note the two IP addresses at the top — the first one is the IP address and port number on the remote node and the second one is the local wallet's external IP address.



When inspecting the suspect's wallet, the remote node with the earliest connection time may give the investigator an idea of how long the suspect's wallet was open. Judging by the image on the right, the suspect's client has been running for at least 37 minutes.

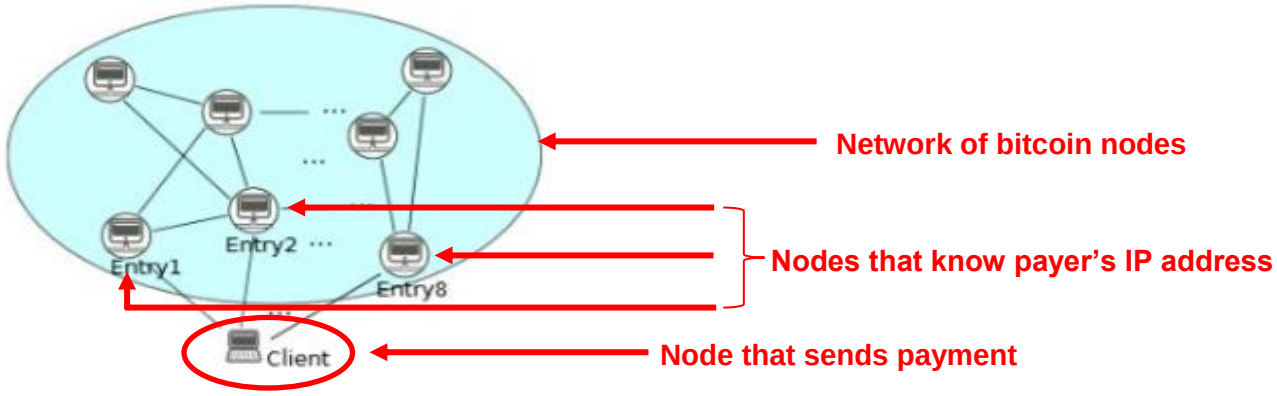
Live data forensics should be deployed in all investigations involving virtual currencies, yet the resource constraints may force investigators to prioritise. Deployment of live data forensics depends on the nature of the case, amount of bitcoins stored in the wallet, availability of skilled staff and resources and probability of a positive result.

Particular attention should be paid to outgoing transactions and their timestamps. If there is a sign of a recent outgoing transaction, the RAM should be preserved as a priority. The majority of wallets are encrypted and the password is consequently required to unlock the private key to make the transaction. Therefore, if the suspect has made a recent transaction, it is likely that the password is still stored in the RAM. Since there is currently no way of circumventing the password protection, extraction of the password from RAM significantly increases probability of bitcoin seizure.

Those who use Wireshark may attempt to extract bitcoin communications from the network transfers. Data transfers going through port 8333 used by bitcoin can be captured with any packet sniffer and Wireshark will even identify the bitcoin traffic under the '*Protocol*' tab.

Tracing based on network analysis of bitcoin traffic

As early as 2011, a famous hacker/researcher, Dan Kaminsky, suggested that it is possible to discover the IP addresses of a payer by an analysis of internet traffic. To conduct deanonymisation, it would be necessary to open a connection to all bitcoin nodes active in the network and for each transaction to find the IP address of the client that first broadcast the transaction to the network.



Based on how bitcoin works, the first person who sends a transaction over to the rest of the bitcoin network should be the payer. Therefore, discovering the first node that broadcast the transaction should reveal the IP address of the owner of the input bitcoin addresses. This logic should lead to identification of the payer unless he or she uses an obfuscation technology such as a proxy server, VPN or Tor, is behind NAT or uses a web-based bitcoin wallet.

While this may sound like a great resource for investigators, it is not — or at least was not in the middle of 2016. However, deanonymisation of bitcoin users through network traffic analysis is a subject of ongoing research conducted by both academia and the private sector.

In short: it is recommended that LE does not spend investigation resources on trying to monitor the bitcoin network in order to discover the payer's IP address. Instead, LE should keep in touch with partners in the specialised private sector and academia who may invest in running their own nodes in the bitcoin network.

Propagation and confirmation of transactions

Once submitted, the payment is propagated throughout the network.

Due to the peer-to-peer nature of the network it is not possible to exclude the presence of malicious actors relaying malicious transactions. Therefore the nodes have a capability to check the transactions themselves instead of relying on the third parties.

The main activity of nodes in the network includes propagation of valid transactions using the following logic:

1. Once the client connects to the network it engages in communication with the other nodes.
2. Whenever the client hears of a transaction, it makes several checks such as whether the transaction is new, whether it is valid or whether the transferred bitcoins were not already spent.
3. If all checks are passed, the transaction gets propagated to all nodes connected to the client. The nodes validate and rebroadcast the transaction and the process repeats itself until the transaction reaches everyone on the network. If there is any issue with validation, the transaction gets discarded so the network is not spammed with already known or invalid transactions.
4. Once the transaction is confirmed by a miner (wait for it — the explanation is coming on the next page), it is included in a block. Once confirmed, the block is then again propagated across the network so that all nodes can append it to the locally stored blockchain.

Bitcoin mining

Every single participant may see a slightly different list of transactions. This is due to many factors including the distributed nature of the network, network latency, different implementation of bitcoin clients and malicious actors trying to spend the same input twice or otherwise abuse the network. Therefore it is common that some nodes in the network know about a particular transaction while some others do not. And so there is a need to establish which set of transaction is the 'correct' one.

It is the miner that decides which transaction will go into the next block and which transaction will have to wait. Every couple of minutes, one of the nodes earns a privilege to validate the recent transactions, to confirm them and append them to the blockchain. The term *mining* that refers to the process may sound confusing; the actual activity is much closer to rubber-stamping.

A miner is a computing device running a full node that engages in an optional competition with the other nodes. Essentially, the miners have to solve a mathematical riddle in order to win the privilege of making an entry to the blockchain. The logic behind the mining is that the miners have to prove their commitment to the network by sacrificing computing power and electricity to solve the riddle, which is essentially brute-forcing of SHA256 hash of the block and a random number called nonce until the hash reaches an acceptable value set by the system. This is also referred to as a proof-of-work concept, the primary purpose of which is to deter malicious actors who have nothing to lose by abusing the system.

Many confuse network propagation with an entry to the bitcoin blockchain. The truth is that when the transaction gets propagated across the network, it is not simultaneously inserted into the blockchain. Only the miner solving the puzzle has the right to append to it. The word append is important here as the miners cannot change the content of the previous blocks in the blockchain — they can merely build on top of it. While propagation including the basic checks only takes seconds, the confirmation of the transactions takes on average 10 minutes[6].

The technical description of mining procedure is not something the investigator must necessarily know and there are some excellent articles covering the topic available online.

[6] To be more technical, the average confirmation time is closer to 9 minutes and 20 seconds, which is 7.2 % faster than the officially indicated confirmation time. What is the reason for this discrepancy? The difficulty of the brute-forcing automatically adjusts every 2016 blocks — which is roughly 2 weeks. If the blocks are mined 20 % faster than they should be, the difficulty will be increased by 20 %. The total mining power in the bitcoin network tends to grow, which means that the blocks are generated faster by the end of the 2016 block long period. For this reason, it takes on average 10 minutes to mine a block right after the difficulty is adjusted but it can take less after a few days due to gradual increase of the computational power of the network.

Bitcoin generation

The mining is a process that serves two main purposes:

- It confirms the latest transactions, which become a part of the blockchain.
- It is the only way to generate new bitcoins, which are given to the miner and thus serve as a motivation for the miners to dedicate their computing power to support the network.

The bitcoin supply is growing at a predetermined rate. The generation started on 3 January 2009 with 50 bitcoins per block of transactions and it halves approximately every 4 years[7]. In total, 21 000 000 bitcoins will be gradually released to the network by 2140, when the emission will stop. Due to the higher number of bitcoins released in the first few years the majority of bitcoins has already been distributed to the miners. As of August 2, 2016 the total amount of bitcoins in circulation reached 15.8 million, which represents over 74 % of the total projected amount.

There are a number of neat tables and graphs illustrating the emission schedule and bitcoin supply that can be found at the official bitcoin wiki website. The current number of generated bitcoins can be checked at many websites including coinmarketcap.com.

#	Name	Market Cap	Price	Available Supply
1	Bitcoin	$ 7,067,471,685	$ 453.40	15,587,650 BTC

Note that this number includes coins that were lost through hardware failures, locked by forgotten passwords or sent to an unspendable address so the term 'Available Supply' should not be taken literally.

Criminal abuse of bitcoin mining

Since bitcoin mining is a process that is very demanding on IT infrastructure and electricity, it is not surprising that mining applications attracted the attention of botnet owners, who pushed bitcoin mining malware to their infected victims. Botnet bitcoin mining reached its peak in spring 2013, when several huge networks of infected computers were effectively competing against the legitimate miners. The most well-known botnet was ZeroAccess, which at the beginning of 2013 generated several thousands of euros a day by mining bitcoin — while burning victims' electricity worth a much higher amount. The botnet was taken down in December 2013 as a result of law enforcement operations driven by EC3, EU LEAs and partners from the internet security industry. Over the last 6 months of its activity, the botnet ceased any bitcoin mining efforts because its opportunity cost was too high as greater income could have been realised from other criminal activities.

[7] Again, in reality it is a few weeks less than 4 years. This is due to the same reason the blocks, on average, take less than 10 minutes to mine.

Another downside for botnet operators was that the infected machines were easily exposed to the victims who detected the resource-consuming applications running on their machines. Other parties that fell victim to bitcoin mining were educational and research institutions, whose students abused access to free IT resources, and landlords who opted to pay for their tenants' excessive energy consumption.

In late 2013, botnet mining of bitcoin was practically dead due to application specific-integrated circuits (ASICs) that arrived on the market. These were single-purpose devices custom-built for bitcoin mining and nothing else than bitcoin mining. The arrival of ASICs opened a new chapter in the evolution of mining technologies and essentially exterminated increasingly inefficient abuse of bitcoin mining by botnets. Since the ASICs were optimised for brute-forcing SHA256 algorithm used by bitcoin, they were dozens of thousands times faster compared to processors or graphic cards.

All of a sudden, criminals could literally do anything else with their botnets — sending spam, distributing malware, performing DDoS attacks or clickjacking. All these activities were much more profitable than mining bitcoin — even when assuming zero costs for hardware and electricity, as these were born by the victims.

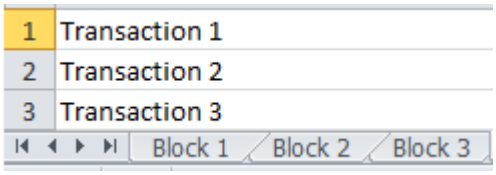
However mining of virtual currencies may reappear, albeit in a slightly different way or form. Many other cryptocurrencies use a different hashing algorithm than SHA256. These include Litecoin and Dogecoin using Scrypt or Dash using X11. ASICs are costly to develop and have not been produced for some of the more recent algorithms. Therefore some of the altcoins may still be mined by CPUs and graphic cards and continue to be open to abuse by botnet mining. As the value of altcoins is more volatile than the value of penny stocks, the usual practice would be to immediately convert freshly mined altcoins to bitcoins. This also happens to be a reason why the price of most altcoins gradually decreases over time as they are mined and instantly sold for bitcoins.

A little known fact about bitcoin mining is that it can assist in investigations as explored in the chapter dedicated to tracing bitcoin transactions.

Bitcoin blockchain

A snappy answer to 'What is blockchain' could be: a chain of blocks.

To understand the concept of blockchain, we have to understand what transactions and blocks are. Transactions are all transfers of bitcoins among bitcoin addresses. There is no exception — every movement of bitcoins is a transaction. Blocks are containers that hold transactions together. Transactions are periodically picked up and stuffed into the blocks. To imagine the blockchain, one may think of the blocks as worksheets in a Microsoft Excel workbook, where each transaction is recorded on a separate row.

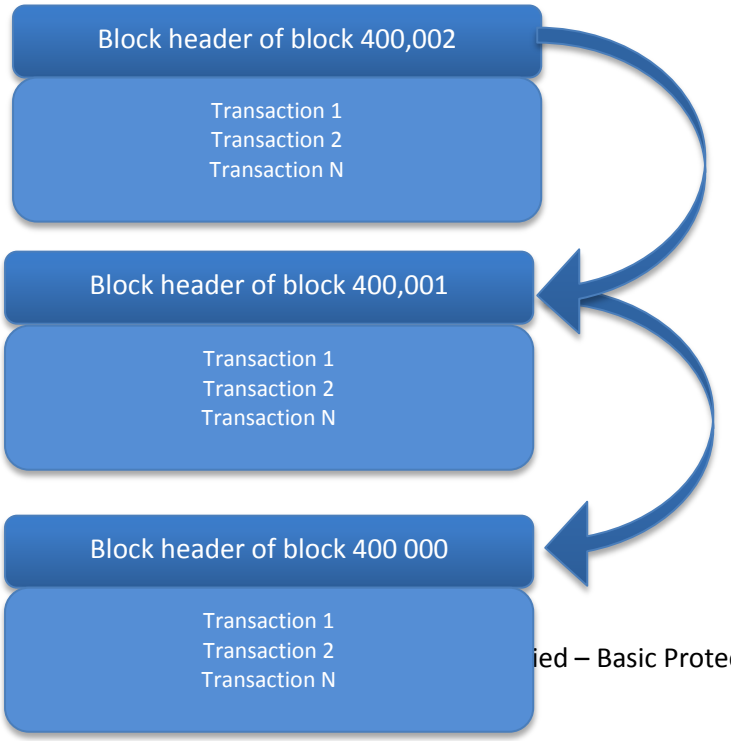


Blockchain is a data structure stored in a flat file and contains chronologically ordered blocks and these blocks hold all transactions that were ever transferred in the bitcoin network. Unlike the worksheets in the Excel workbook, transactions are stored in blocks and the blocks are mathematically linked (or chained) together.

Each block has a block header. The header contains metadata about the block, including:

- a **previous block hash** — a unique SHA256 hash that refers to the previous block;
- a **block height** that started with the first block back on 3 January 2009 with block height 0 and increases incrementally with each block; the block height reached 420 000 in July 2016;
- a **timestamp** using the format YYYY-MM-DD HH:MM:SS in the UTC time zone;
- a **Merkle root**, which is a hash of all transactions in the block;
- a **nonce** (a random variable) and a **difficulty** that are only relevant to bitcoin miners.

The blocks are linking backwards: each block refers to the previous block in the chain (technically speaking it refers to the hash stored in the block header of the previous block).



This cascading effect ensures that once a block has many other blocks following it, it cannot be changed without a recalculation of all subsequent blocks. Such recalculation would require an impractically large amount of computation. Therefore, the existence of a long chain of blocks makes the blockchain's deep history immutable. This immutability is a key feature of bitcoin's security; if one block is maliciously altered, this makes that part of the blockchain invalid.

From the perspective of the LE investigator, the only partially practical information to derive from the headers includes:

(1) the timestamp containing both the date and time of when the block was mined in UTC format;
(2) the block height that is unique for each block.

In addition to the block header, each block contains a list of transactions. The order of transactions within a block depends almost entirely on the miner. However, there are some rules even the miner must adhere to; for example, the first transaction of the block must be miner's reward. Also, transactions have to appear after any transactions upon which they depend. For example, if address A sends bitcoins to address B and address B to address C then the transaction sent by A has to be validated first.

Investigators do not need to parse the blockchain flat files themselves, as both header and transaction information is available through all major blockchain explorers, such as blockchain.info.

Location of the blockchain

It should be kept in mind that the users can install bitcoin software to any location. Nevertheless, many opt for the default location, which differs according to operating system:

1. Windows
   (a) On Windows XP the path is:

   C:\Documents and Settings\<username>\Application data\Bitcoin

   (b) while on later Windows (Vista 7, 8, 10) it was changed to:

   C:\Users\<username>\Appdata\Roaming\Bitcoin

   A shortcut to open the folder would be to go to Start -> Run and run the following command: *explorer %APPDATA %\Bitcoin*

2. Mac
   On all versions of Mac OS X the path is:
   ~/Library/Application Support/Bitcoin/

3. Linux

   In the mainstream versions of Linux the file will be located in:

   ~/.bitcoin/

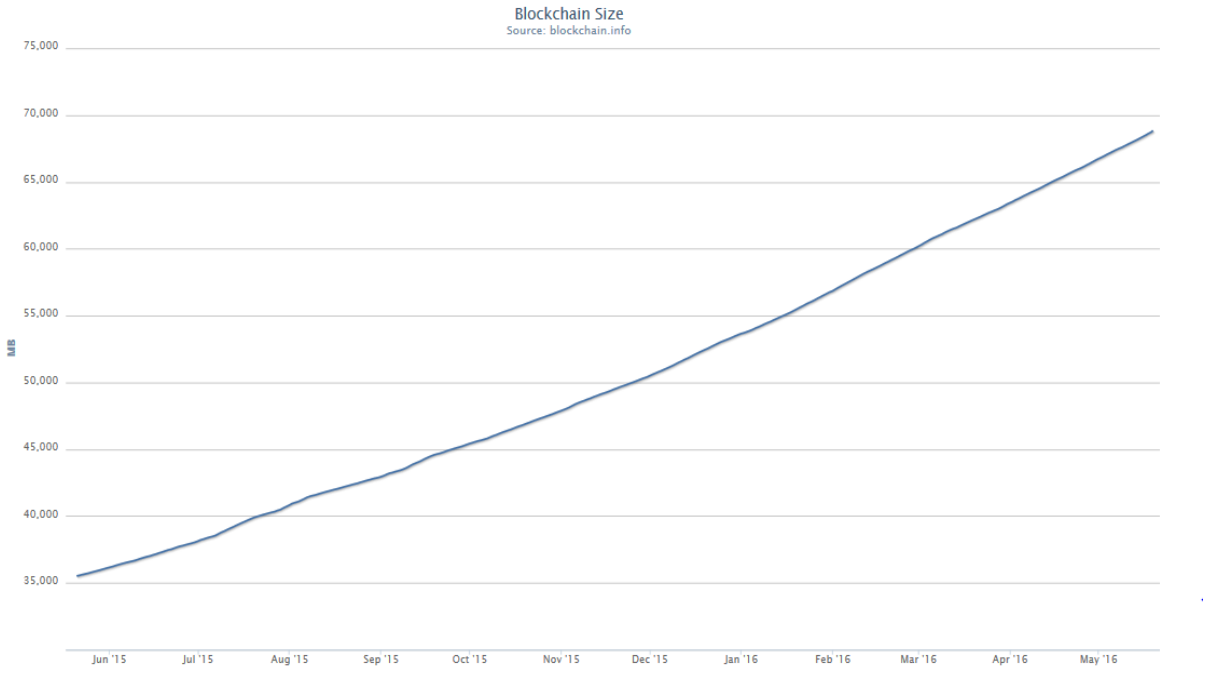
Bitcoin blockchain is split into many files, each about 134 Mb in size:

Name	Date Modified	Size	Kind
Bitcoin	Today 9:33 pm	--	Folder
bitcoind.pid	13 Aug 2015 10:15 pm	4 bytes	Document
blocks	Today 8:15 am	--	Folder
blk00000.dat	16 Dec 2014 12:23 pm	134.2 MB	Document
blk00001.dat	16 Dec 2014 12:27 pm	134.2 MB	Document
blk00002.dat	16 Dec 2014 12:32 pm	134.2 MB	Document
blk00003.dat	16 Dec 2014 12:36 pm	134.2 MB	Document
blk00004.dat	16 Dec 2014 12:40 pm	134.2 MB	Document
blk00005.dat	16 Dec 2014 12:52 pm	134.2 MB	Document
blk00006.dat	16 Dec 2014 12:56 pm	134.2 MB	Document

The folder **blocks** containing bitcoin blockchain are stored in the same folder as the wallet file **wallet.dat** containing public and private keys. As mentioned, the default location of the folder can be changed — fortunately for those who use a limited capacity SSD drive as drive *C:* can opt to store the blockchain on another drive where the capacity may be much larger. If the default path is changed, bitcoin could be run with a **datadir** parameter pointing to the directory, such as:

bitcoin-qt.exe –datadir=<D:\Bitcoin>

There are as many files as required to store the blockchain, which means that their number is gradually increasing along with the size of the blockchain. As of June 2016, its size reached 70 Gb.



A constantly updated chart can be seen at https://blockchain.info/charts/blocks-size. While we can see the increase is not exponential it is not completely flat either. While the new blocks are being appended in regular intervals, the average size of the individual blocks has increased from a few kilobytes to almost 1 Mb in May 2016.

Webbtc.com/stats contains a simple yet useful high-level and constantly updated summary of the blockchain. The total number of addresses reached almost 160 million in June 2016. These addresses sent or received coins in course of more than 140 million transactions.

Blocks	419,826 (1,004 side, 10,098 orphan, 430,928 total)
Transactions	141,148,680 (368,210,852 inputs, 408,889,339 outputs)
Addresses	159,831,189
Blockchain Size	70.6 GB
Total Coins	15,745,675.00000000

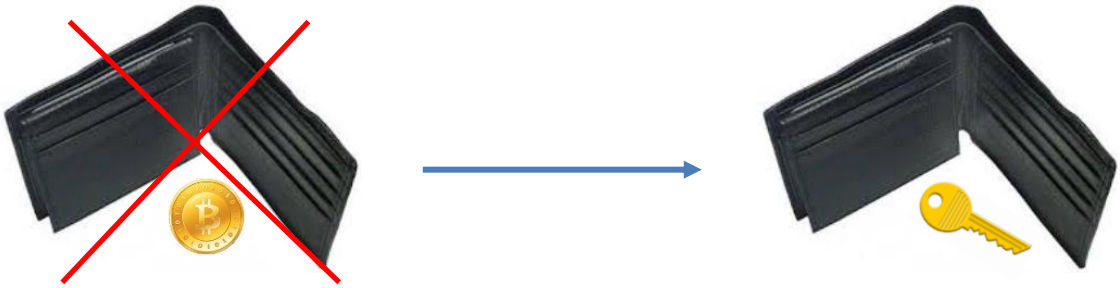
It is also interesting that the vast majority of transactions were simple payment transactions sent to bitcoin address or directly to public keys, with multi-signature addresses contributing to about 5 % of the total. Only 0.02 % of addresses used the so-called OP_RETURN script that is used to store non-financial data, such as messages senders decided to store permanently. However, the real number of non-financial transactions is likely to be considerably higher as many data storage transactions were not explicitly flagged as OP_RETURN.

Script Types	220,937 unknown, 40,381,243 pubkey, 342,502,086 pubkey_hash, 569,641 multisig, 24,095,624 script_hash, 1,168,137 op_return
P2SH Types	106,783 unknown, 85 pubkey, 97 pubkey_hash, 19,128,958 multisig, 77 script_hash

Bitcoin wallets and seizure

Usually there are two key objectives in bitcoin investigations: identify the suspect and seize bitcoins that were stolen or used to facilitate criminal activities. This chapter will cover different types of storage methods that can be encountered by law enforcement.

Note that bitcoins are not actually stored 'on' a device; instead, the device stores a wallet that contains the private key that allows the bitcoins to be spent. This is illustrated by the figure below. Therefore, gaining access to someone's private key means gaining access to someone's bitcoins.



Gaining access to a suspect's private key

The private key will be controlled:

1. by a wallet installed on the suspect's computer, phone or external storage device including a HW wallet or USB disk;
2. by a paper wallet or being written on a piece of paper;
3. by the third party who manages bitcoins for someone else — usually — or the virtual currency exchanger or online wallet provider. In these cases, the third party may be in control of the private key.

- **Software wallets**

There are a variety of desktop bitcoin wallets available for the common operating systems (Windows/Linux/Mac)[8]. These wallets provide a graphic user interface (GUI) that allows the users to conveniently check the balance on their bitcoin addresses and the list of recent transactions and to send/receive bitcoins. Some of the most popular software wallets are Bitcoin Core and Electrum.

A key difference between the original client Bitcoin Core (previously also known as Bitcoin-QT) and many other software wallets is that the former requires download of the full blockchain. The balance is not properly updated until the full blockchain is downloaded, which may take a few days to accomplish. Most of the other wallets are so-called lightweight wallets that only download the portion of the blockchain that is relevant for the user rather than the full blockchain.

Software wallets store *wallet.dat* file on a local drive. The wallet file containing the private keys can either be stored unencrypted or encrypted. In the former case, access to the suspect's computer is all that is required to access the bitcoins and transfer them to an LE-controlled wallet. However, in practice, a vast majority of users — regardless of whether they use bitcoins for legitimate or illegal purposes — do encrypt their wallets. For guidelines on what to do with an encrypted wallet please refer to the next chapter.

[8] For a full list of wallets per platform see https://bitcoin.org/en/choose-your-wallet

So far we have discussed the standard implementation that requires download and interaction with the full blockchain to function. However, due to the large and constantly growing size of the blockchain, so called lightweight (also light) clients are becoming increasingly popular.

These 'light' clients do not download the blockchain and therefore do not have the ability to validate transactions for the network. This saves users dozens of gigabytes on their hard drives and ample amounts of processing resources. For this reason, the light wallets are particularly popular on mobile devices and smartphones that are short on disk space, computing resources and battery. As the blockchain gradually increases in size, we can expect increasing number of users to move from full to lightweight clients or online or mobile wallets such as Coinbase, Blockchain.info, Xapo or Circle.

Probably the most fitting analogy compares a full node to a tourist in an unknown location, equipped with a detailed map of the area. By comparison, the light wallet resembles a tourist without a map who is reliant on advice from random strangers for turn-by-turn directions[9].

Some popular light wallets such as MultiBit employ so called simplified payment verification (SPV). Since these wallets do not store blockchain locally, they are dependent on third party online services to parse the blockchain and return relevant results to the user's wallet. When a wallet requests specific data[10], it reveals the bitcoin addresses it stores, which creates a privacy risk and provides an interesting opportunity for a bitcoin investigator.

Security researchers have already discovered a possibility to link bitcoin addresses to a specific wallet based on which addresses are requested by the light client[11]. The only available tracing tool that is currently taking advantage of this information is Chainalysis, which also records IP addresses, which can be used for identification of a suspect.

The following table summarises key differences among the different types of bitcoin clients.

Functions	Miners	Full nodes	Light clients
Checking balance	X	X	X
Receiving or sending payments	X	X	X
Storage of full blockchain	X	X	
Validation of transactions	X	X	
Propagation of transactions	X	X	
Confirmation of transactions	X		

[9] Andreas M. Antonopoulos, 'Mastering Bitcoin', December 2014.

[10] SPV clients have to connect to full nodes and use bloom filters to only download transactions that are relevant. This might reveal bitcoin addresses stored by SPV clients.

[11] Jonas David Nick, 'Data-driven de-anonymization in bitcoin', MSc Thesis, 2015 (http://jonasnick.github.io/papers/thesis.pdf).

- **Mobile devices**

A list of the most popular wallets on iOS

Mobile wallets are available for all major mobile operating systems (Android/iOS/Windows Phone). These wallets store the user's private keys locally on the phone within the application.

Access to the private keys for mobile wallets requires:

(a) unlocking the phone;
(b) opening the wallet application, which may be locked by a PIN/fingerprint verification.

As with desktop wallets, access requires either the suspect's cooperation or a bypass of the phone's security followed by examination using Cellebrite, XRY, Paraben or a similar product.

Generally, users who own large amount of bitcoins store the majority of bitcoins in paper, hardware or a software wallet and would only use the mobile wallet to store smaller amounts of bitcoin for day-to-day transactions. Therefore if a mobile wallet is discovered this suggests a high likelihood the offender stores most of his or her bitcoins elsewhere.

- **Web wallets**

Access to web wallets requires knowledge of the username or wallet ID, password and possibly two-factor authentication codes. The best-known web wallet is the one operated by the most popular blockchain explorer blockchain.info. Most of the web wallets allow users to download their wallet or export their private key so that users may store these locally.

- **Paper wallets**

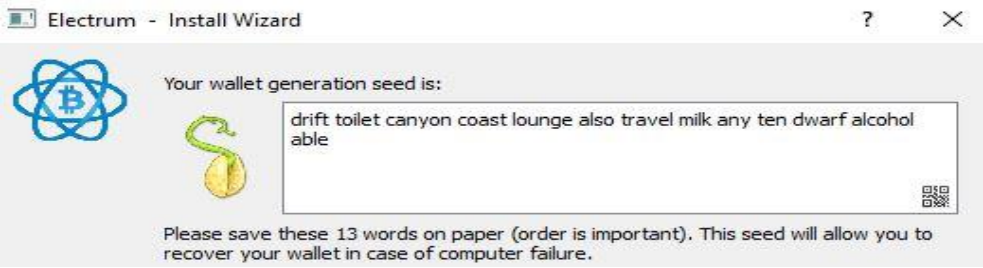
Paper wallets store private keys completely offline. All that is required for access to bitcoins is the private key that can be printed and stored exclusively on paper. The private key is often accompanied by a public key and corresponding QR codes.

Since paper wallet generators may generate bitcoin public and private keys offline, an air-gapped computer is often used to create the keys. Afterwards, the keys are saved to a piece of paper and any files created on the computer can be deleted. As one would expect, a paper wallet is resistant to hacking and malware attempts, but the owner needs to keep it safe from thefts or elemental damage.

The paper wallet is relatively inconvenient for a regular use and those who decide to create it usually store a significant portion of their bitcoin wealth on this type of wallet. If a paper wallet is encountered on site during an investigation, it will allow for immediate access to the funds associated with that private key by importing the private key into any existing wallet software. Most wallets allow import of private keys and this option can be commonly seen in File -> Import menu.

- **Deterministic wallets**

So-called deterministic wallets, which can be either software, online wallets or paper or hardware wallets, drive private keys from a seed, quite commonly in form of 10 to 15 words that may or may not form a sentence.



The key advantage of the deterministic wallet for a typical user is the ease of backup and recovery. If the user remembers or writes down the seed to a deterministic wallet, he or she no longer has to worry about unrecoverable wallet files or corrupted hard drive. Instead, he or she may recreate a new wallet from the seed. This would reliably recover all private and public keys from the wallet so the seed can essentially be thought of as the master password. That also means that if an attacker or investigator discovers the seed he or she will gain an immediate access to all bitcoin addresses in the deterministic wallet.

Sometimes the deterministic wallets are referred to as 'brain wallets'. As long as the seed is not saved, written down or printed, the bitcoins essentially only exist in the memory of the owner. However, as the users are unlikely to memorize multiple words in a correct order, they often store the seed electronically or on a paper which can therefore be collected during house searches.

Risk of attacks on deterministic wallets

The seed must be long, unique, and practically impossible to guess as the user essentially exposes his or her wallet to the whole world for it to brute-force the password.

What an attacker can do is to download a copy of the blockchain and parse it to retrieve all unique bitcoin addresses — which could generate over 100 million bitcoin (BTC) addresses. Addresses with non-zero balances could be identified and extracted and then cross-matched against addresses that can be generated by using weak passwords ('passw0rd', 'Ford Perfect', wordlists of popular songs, quotes, etc.). Once the match is found, the attacker can use the password to recreate the private key and steal the victim's bitcoins[12].

[12] For more details on the subject please refer to a fascinating presentation by Ryan Castellucci on cracking of Brainwallets who discovered hundreds of bitcoins on the blockchain sitting on addresses created by brain wallets using guessable passphrases. The method is not limited to the bitcoin; it could be used for all altcoin brainwallets as well.

- **Hardware wallets**

A hardware wallet is a special type of bitcoin wallet which stores the user's private keys in a secure hardware device. This wallet securely stores the private keys so that it cannot be transferred out of the device in plaintext.

How hardware wallets sign transactions

1. Hardware wallets often receive a transaction from a computer typically via USB.
2. The hardware wallet signs the transaction.
3. The signed transaction is then transferred back to the computer and broadcast to the network.

This process does not reveal a private key. Therefore, this process does not expose the private keys to an accessible internet connection. Access to the private keys stored on a hardware wallet requires physical access to the device. In addition, devices can be secured by a pin code and optionally by another form of authentication. This device is safe from malware, keylogger or seizure by law enforcement. Brute-forcing these will cause the device to time out for exponentially increasing periods of time and hence the suspect's cooperation will be required to access funds stored on a hardware wallet.


ACT RESPONSIBLY AND DO NOT DISCLOSE THE SEED TO ANYBODY. KEEP YOUR RECOVERY SEED IN A SAFE PLACE. ALSO, NEVER MAKE A DIGITAL COPY OF YOUR RECOVERY SEED AND NEVER UPLOAD IT TO ONLINE SERVICES. BE AWARE, THAT HAVING A DIGITAL COPY OF THE SEED IN A COMPUTER, MOBILE PHONE OR AN ONLINE SERVICE SIGNIFICANTLY DECREASES THE SECURITY OF BITCOIN WALLETS. TREZOR CANNOT BE HELD RESPONSIBLE FOR FINANCIAL LOSSES RESULTING FROM NOT FOLLOWING THESE SECURITY INSTRUCTIONS.

TREZOR
The Bitcoin Safe

Recovery Seed

Device Label

The most popular hardware wallet is Trezor. The manufacturer delivers it along with a *Recovery Seed* booklet that initially contains 12-24 empty boxes, where the user is supposed to write down recovery seed words to have a safe backup of the wallet. As mentioned previously, anyone who gets access to these words controls can recreate the wallet and seize the bitcoins, which makes the booklet primary target during house searches.

Probably the most interesting hardware wallet for those interested in privacy/anonymity is a special credit card-sized wallet BitLox. As the device is sold for between USD 200 and USD 400 — depending on the features offered — it is likely to be used to store a large quantity of bitcoins.

BitLox allows its owner to create up to 50 invisible wallets that are not shown until the owner enters the number of wallet and its pin into the device. Thus the investigator will never be sure if all the suspect's wallets have been seized. Additionally, the device works well with the Tor and Tails operating system (after connecting to PC with a USB cable) and has several other features attractive for criminals. In March 2016 the device featured on Deepdotweb, the most popular online resource on underground marketplaces.

Bitcoin seizure

If the investigator identifies a suspect's bitcoin addresses on the blockchain, a fundamental thing to keep in mind is that it is not possible to seize bitcoins remotely (unless suspect keeps his funds on an online exchange). To seize the bitcoins at the suspect's premises, investigators have to locate:

1. the bitcoin wallet on the suspect's hard drive — in which case a password is needed to manipulate the bitcoins as the vast majority of wallets nowadays are encrypted;
2. the suspect's private key — in which case there is a need to import it into a wallet;
3. the suspect's recovery seed (usually 12-24 random words).

To seize bitcoins it is not sufficient to simply copy the wallet.dat file, import the private key or enter the recovery seed into the LE-controlled software. Doing so would merely allow the investigator to discover relevant public keys along with the amount of unspent bitcoins. At this point, bitcoins cannot be thought of as 'seized' as the suspect himself or herself, or another person controlling the private key, can move the move the funds to another address. In order to seize bitcoins, an additional step is required to complete the transfer of funds. The investigator has to transfer these into a bitcoin address controlled by law enforcement.

The secure wallet would ideally have its own blockchain and be well audited by the community, so the Bitcoin Core wallet is a very good candidate. It stands to reason that the official bitcoin address should be in place before the seizure and the personnel conducting the search/seizure should have it on paper or a USB key so that they can transfer bitcoins without any delay. Therefore, if this is not the case or if there is a requirement to seize bitcoins at the scene and the LE bitcoin address is not known, the investigator should use the next best available solution — creating a bitcoin address on the fly.

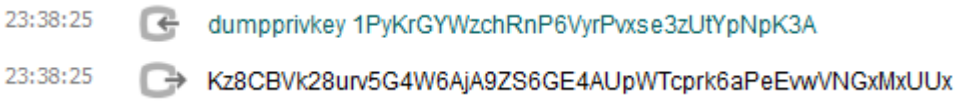
Probably the fastest and a relatively secure way to do so is to use bitaddress.org, a pure JavaScript site that generates the private key and corresponding bitcoin address based on the user's mouse movement, thereby introducing a very good source of randomness. Ideally, the website would be accessed by a trusted computer using a secure connection and the website would be saved offline and only afterwards used to create private key and corresponding addresses. The seizure would be completed by moving the bitcoins to a newly generated bitcoin address.

Alternatively, the bitcoin address can also be provided to LE by a bitcoin exchanger. This is particularly useful if LE seek to immediately convert seized bitcoins to fiat currency (a traditional currency such as € or $). Such approach may eliminate the need to set up and maintain a dedicated LE wallet.

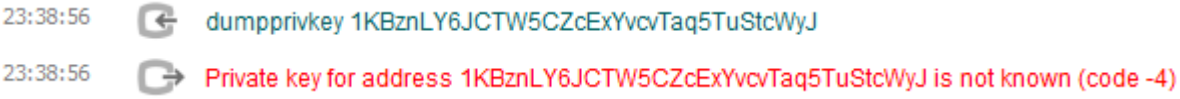
Export and import of private keys

The private key may be printed on paper or stored in a wallet.dat file on the suspect's computer, phone or USB key. If the last of these is the case, the key can be extracted using the *dumpprivkey* command followed by a specific bitcoin address. This command reveals the corresponding private key in the wallet import format (WIP). Note that on encrypted wallets the suspect's password must be provided in order to reveal the private key. Also note that the command *dumpprivkey* does not remove the private key from the wallet — it merely exposes it in cleartext.

The following example demonstrates the use of the command followed by a public key and a corresponding response revealing the private key.



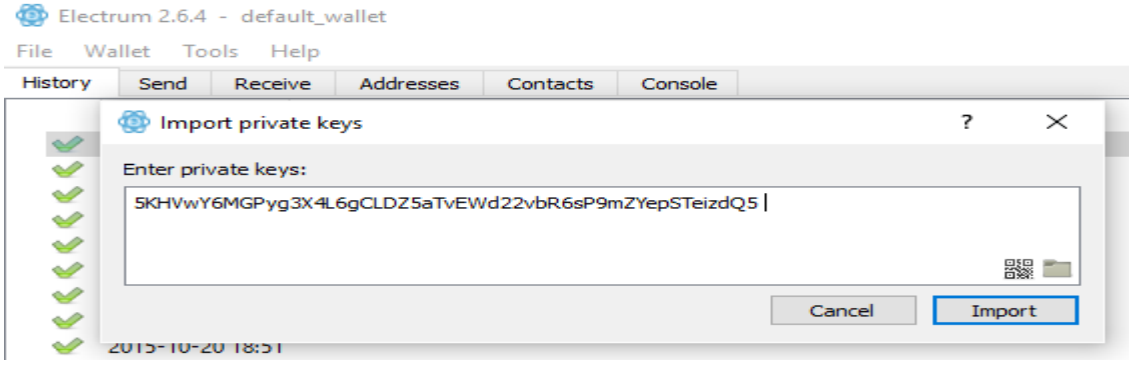
Naturally, in order to export the private key the wallet must actually contain the private key for the queried bitcoin address; otherwise the command will return the following error.



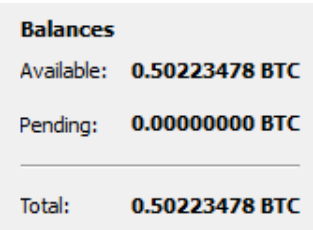
When the suspect's private key is retrieved, it must be imported into a wallet so that bitcoins can be transferred to an address that is in the sole possession of law enforcement. The import procedure is different for each wallet. For the standard Bitcoin Core wallet one has to select *Help -> Debug Window* and enter *importprivkey* followed by the private key.

In Electrum, another popular wallet, the import can be found under:

Wallet -> Private keys -> Import and all that needs to be done is to insert one or more private keys into dialogue window.



Once the private key is imported, it may take a while for the wallet to synchronise all the transactions linked to the corresponding bitcoin address. At the end of the procedure the wallet will show all



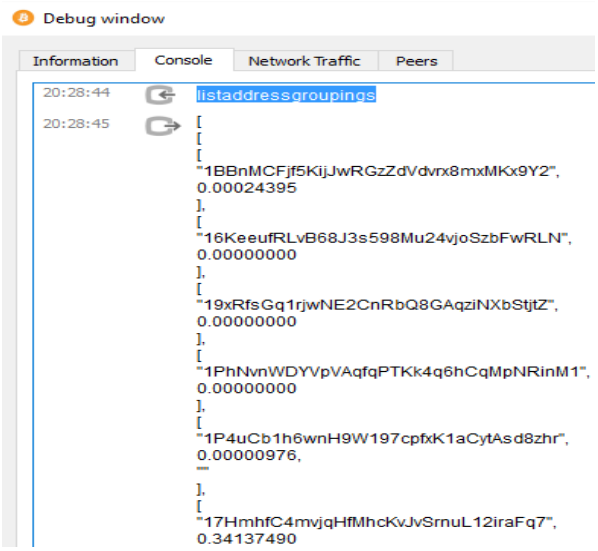
spendable funds — which on the example on the left is about 0.5 bitcoins.

After the private key has been imported into a wallet and the balance is known, all bitcoins should be transferred in one transaction into the LE-controlled bitcoin address. Alternatively, if the investigator manages to gain access to the suspect's wallet and password, he or she may transfer the bitcoins even without extracting the private key.

There is one other possibility for seizing bitcoins — if the investigator identifies that suspect has an account at a virtual currency exchange, the exchanger may be approached and asked to freeze the criminal's assets. These may include bitcoins, alternative cryptocurrencies such as Litecoins, Ethereum or Dash or even a fiat currency, which keep sitting in the online exchange accounts.

Note that even though some suspects may opt to store a portion of their cryptocurrencies on the exchange, they are still likely to store further bitcoins in their software wallet.

Retrieval of all bitcoin addresses stored in the wallet

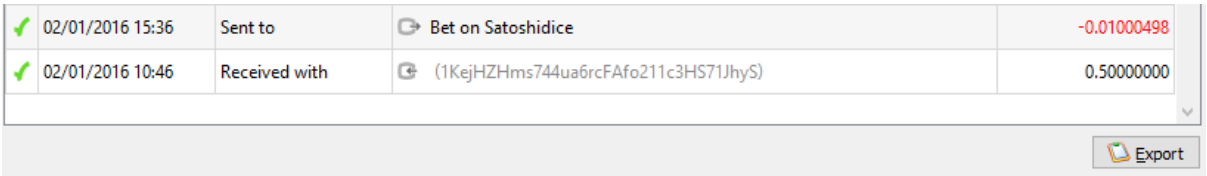


Regardless of whether the seizure was successful or not, the investigator should extract a list of all bitcoin addresses that were stored within the suspect's wallet.

The *listaddressgroupings* command can be used to list all bitcoin addresses along with their spent or unspent balances. It is important to get this list so that all bitcoin addresses can be traced later on using free or commercial transaction-tracing tools.

Note that this command does not require knowledge of the user's password and can therefore be executed even on an encrypted wallet.

The list of transactions can also be retrieved without knowing the password. This can be done using the GUI of the Bitcoin Core wallet in the transaction tab that exports all transactions along with dates, amounts, labels and transaction IDs into a neat.csv file.



Dealing with encrypted wallets

An encrypted wallet can still be opened and checked for balance, list of transactions and present bitcoin addresses. However, the extraction of a private key or transfer of funds to another address requires a password. This chapter focuses on how to find it.

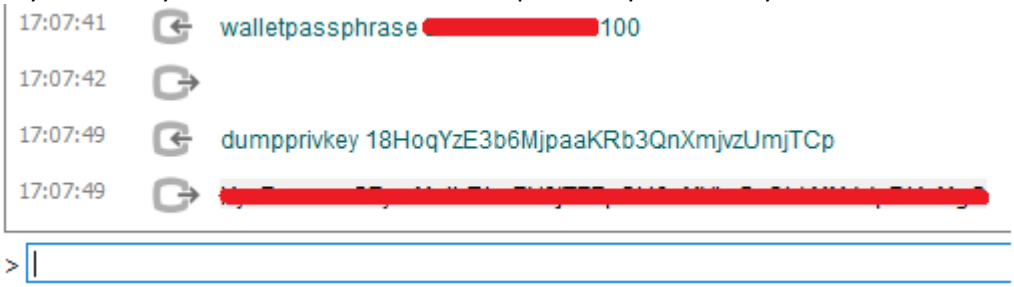
1. **Cooperating with the suspect**

   Before investing any effort into password retrieval, it makes sense to ask the suspect to provide it voluntarily or through a mandatory disclosure if the national legislation allows such an approach.

   Note that investigators may essentially have an unlimited number of guesses as to the password — the wallet will not become irreversibly locked or deleted after a certain number of unsuccessful attempts so the suspect may not ruin the investigation by providing a sequence of incorrect passwords.

2. **Using live data forensics**

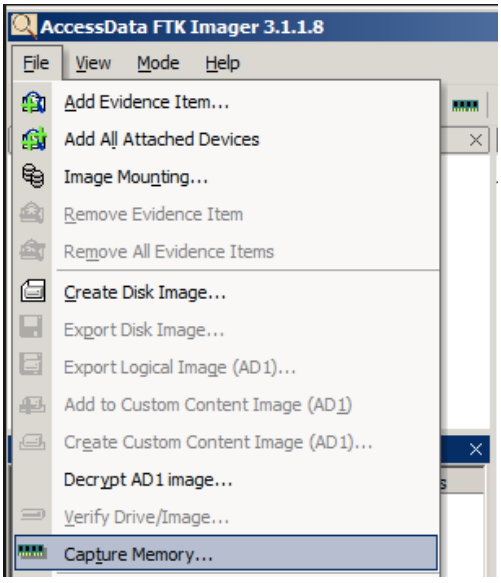
   (a) When opening the bitcoin console (in the Bitcoin Core wallet it is hidden in *Help -> Debug Window* section), the console command line will reveal recently executed commands. Pressing the '*up cursor key*' is all that is needed to browse the history. Each keystroke may reveal a command that was previously entered by the user.



   (b) On linux systems a '*history*' command, when typed without any options, lists the last executed commands entered by the user. Even if the password to the wallet is not present, the chances are that some other password was entered recently. Since people tend to reuse variations of their passwords, these could be saved for later use for vocabulary attack.

```
147  wc -l /root/scan/02032014
148  top c
149  history
```

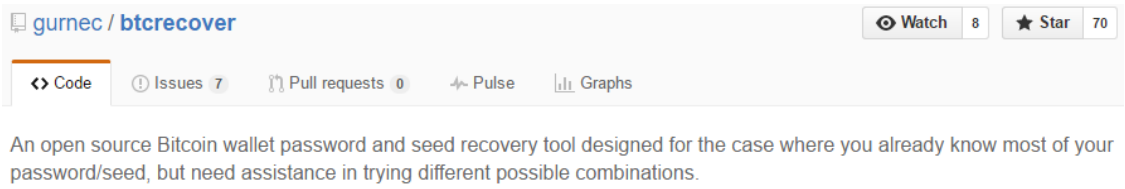
   (c) Whenever possible, it is advisable to make a memory dump before the machine is shut down. There are several tools available to capture the operating memory; one of the most popular and straightforward to use is *FTK Imager*, which can take images of both RAM and hard drive. *FTK Imager* is available both as a GUI and as a command line tool.



The memory dump can then be analysed later using the *Volatility* tool that may succeed in extracting the relevant bitcoin wallet password. An alternative would be to use a *strings* command searching for all text strings in the memory. All relevant strings may be saved into a file that will serve as a vocabulary for a brute-forcing attack. Note that the passwords are stored in RAM in unencrypted format.

3. Brute-forcing the key

LE can try to brute-force the wallet password using John the Ripper or another password-cracking tool. There are scripts such as https://github.com/gurnec/btcrecover that can be downloaded and used to try to brute-force the password oneself. However, since the encryption algorithm is strong such scripts running on a single PC can only check a few dozen passwords a second and so are useless for most practical purposes. As the description of the program suggests, one should know or guess at least something about the password before trying to brute-force it.



Success here naturally depends on password complexity. Nowadays, the majority of bitcoin users are well versed in elementary IT security and are fully aware of the importance of having a complex password that is generally 10 or more characters long. If such a password is truly unique, not repeated in any other application or service, stored in RAM or a disc or written down on a note then there is practically no hope of cracking it.

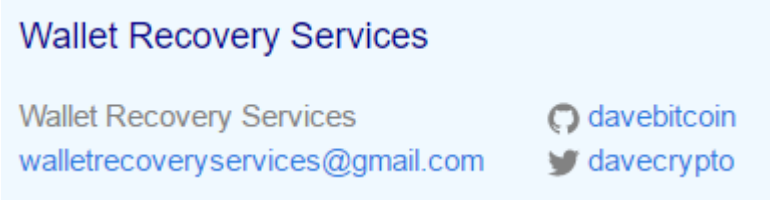
4. Using the EC3 decryption platform

The EC3 Digital Forensics Lab may be used to support investigations of Member States and third parties. Not only does it offer solutions for the recovery and analysis of data extracted from digital media, it also hosts a decryption platform. This platform can be used to decrypt passwords for common applications including bitcoin wallets.

So far the forensics team have had a limited exposure to wallet password cracking, but they are willing to attack the passwords, provided that at least some facts about the password are known or assumed.

5. Outsourcing

If all the other options fail, it is possible to turn to the private sector, most likely to walletrecoveryservices.com, which is recommended by several major online wallet providers. This service has a very good reputation in the bitcoin community.



This is a paid service but the decryption fee of 20 % of the content of the wallet is only payable if the wallet is successfully decrypted.

The risk that the full contents of the wallet may be stolen is mitigated by the fact that it is not necessary to submit a full wallet.dat file. Instead, walletrecoveryservices.com provides a set of instructions on how to extract and submit information necessary for the decryption of the password without the full wallet.dat file or private key actually being handed over. That allows the data necessary for the decryption of the password to be handed over, without exposure to a risk of theft.

Use and criminal abuse of bitcoin signing and verification

Some bitcoin wallets have a convenient interface for signing and verifying messages. Bitcoin Core offers these functions right under *File* in the main menu.

Despite the prominent placement, these functions are often not understood or actively used by the majority of bitcoin users. This chapter first demonstrates how signing and verification may be used for legitimate purposes in practice and then highlights possible abuse by criminals.

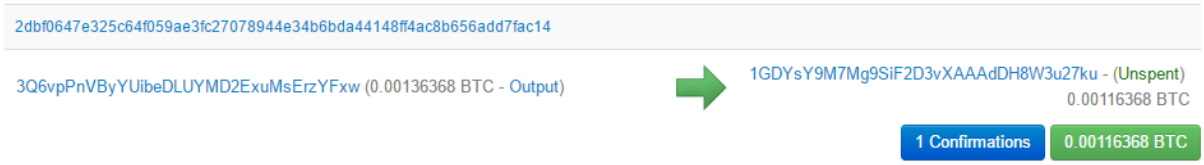
Legitimate use of the signed message

Imagine a situation where a payer sends bitcoins but a recipient says he did not receive anything. One thing that can be done with ease is to check the blockchain to demonstrate the record of the transaction, for example using blockchain.info.

However, a link to a transaction may be far from conclusive as the recipient can try to dispute the relationship between the sender and bitcoin address from which funds were transferred. This can be practically demonstrated by the following simple example, where A expects a payment from B.

Person A: *Have you sent me the payment? I do not see it …*

Person B: *Check the blockchain —you have it here:*



Person A: *I get a lot of payments these days … How do I know it was you who made this payment?*

Person B: *I can send you a screenshot of my wallet …*

Person A: *How do I know it would not be a Photoshop job?*

Person B: *Here you have my cryptographic signature.*

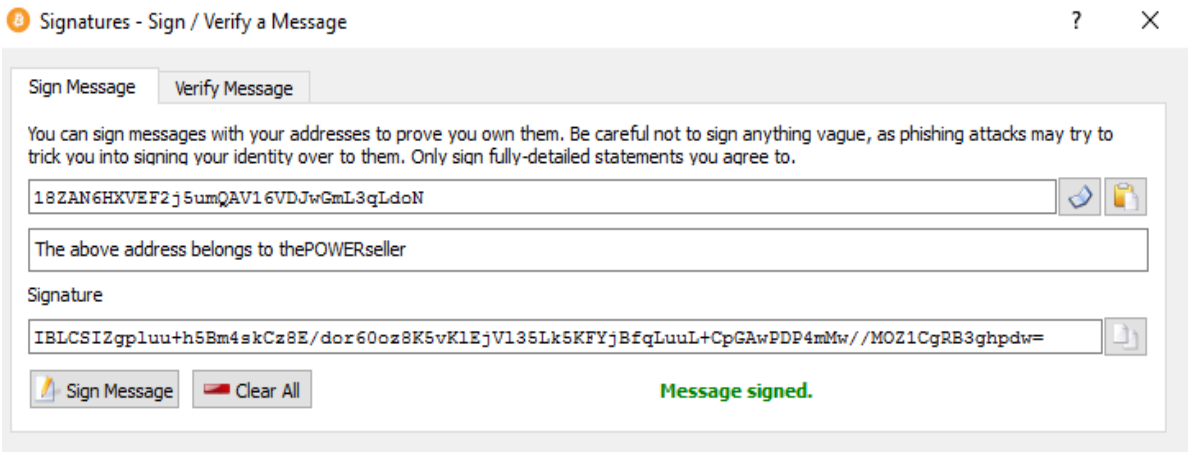
Person A: *Verified! Dandy! Lovely doing transactions with you!*

So — now A is 100 % sure that the bitcoin address 3Q6vPnVBy … made the payment and B owns private key(s) controlling the bitcoin address.

As we have seen, by signing a message a person can prove an ownership of a particular bitcoin address.

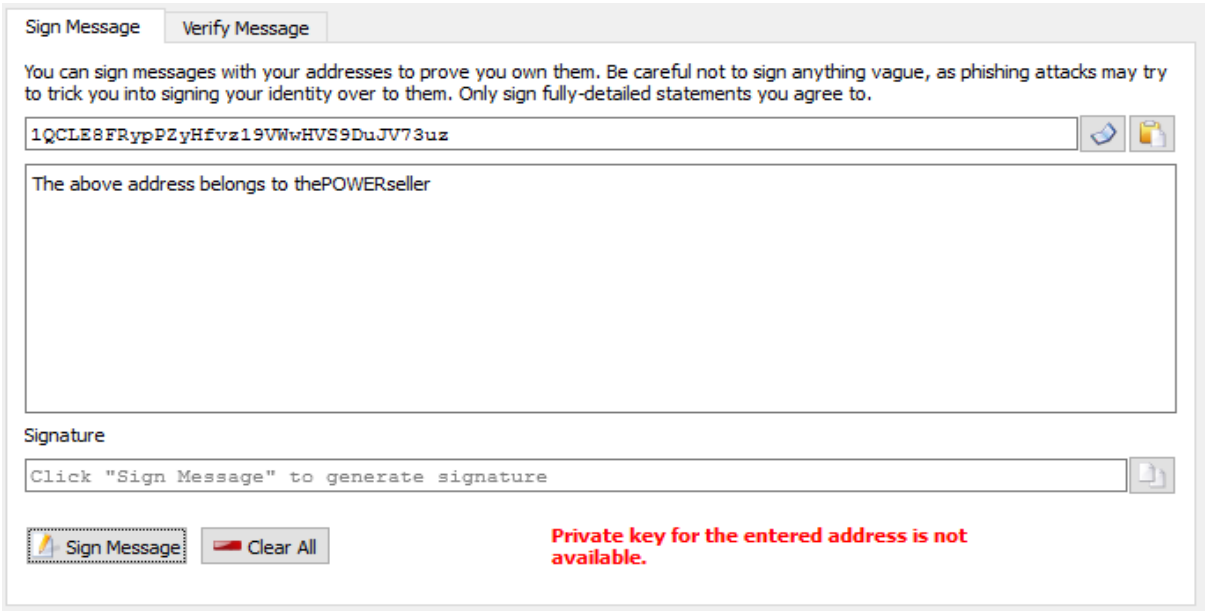
How does message signature and verification work in practice?

In order to sign the message, the user has to provide the bitcoin address they own and store in their wallet and then type an arbitrary message. After the button 'Sign Message' has been clicked, a signature will be generated by the wallet and a green message saying 'Message Signed' will appear below the signature.

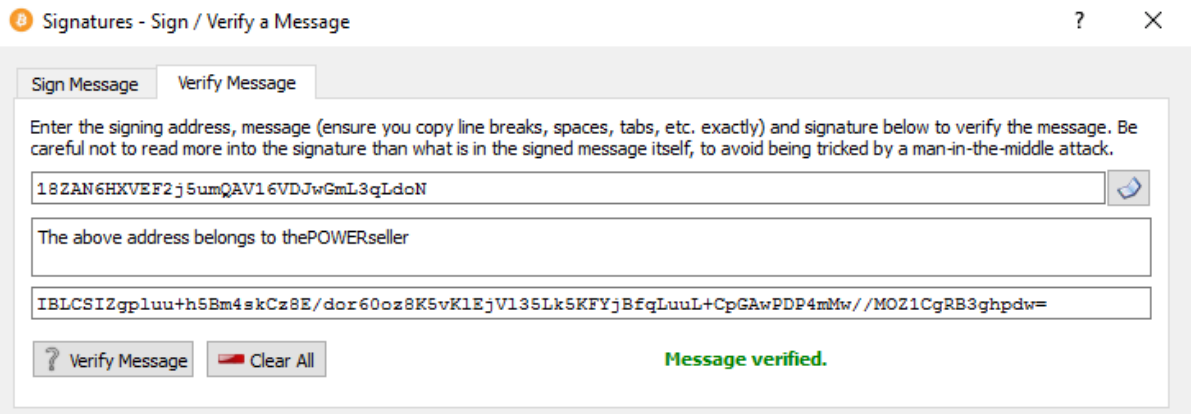


The message is only signed if the bitcoin address corresponds to a private key stored by the wallet.

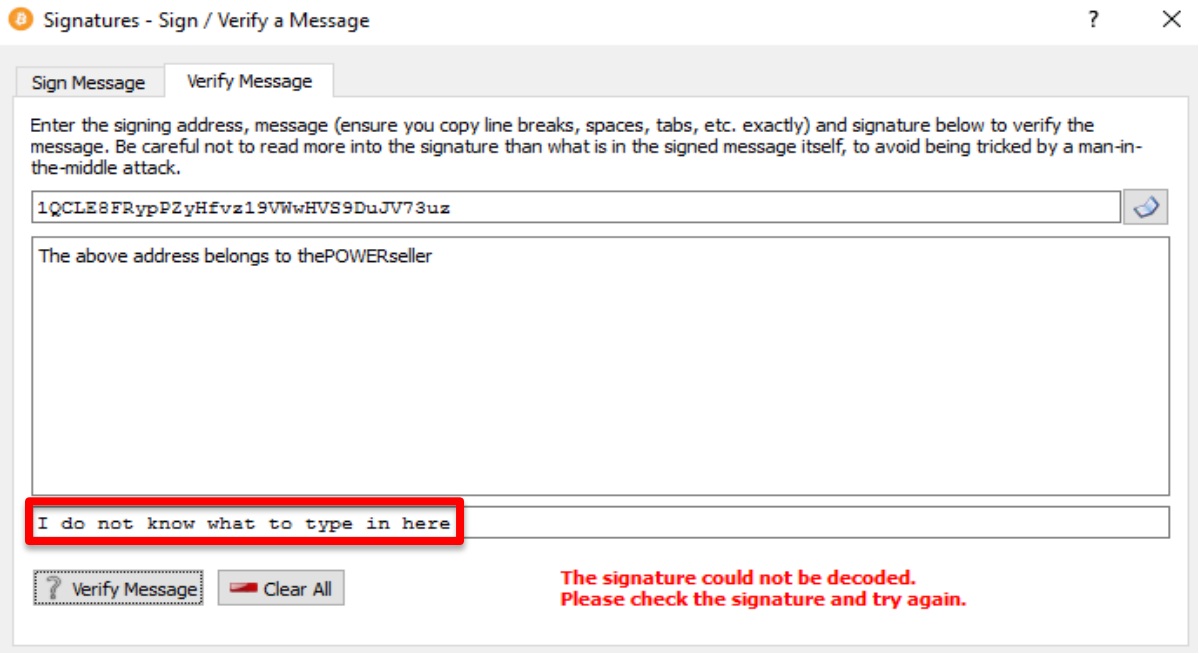
If a person wants to sign someone else's bitcoin address the signing will fail as the wallet will not be able to find the relevant private key for the bitcoin address provided by the user.



Verification of the signed message is also relatively straightforward. The recipient can verify any message to prove the link between a bitcoin address and a person who claims ownership of the address:

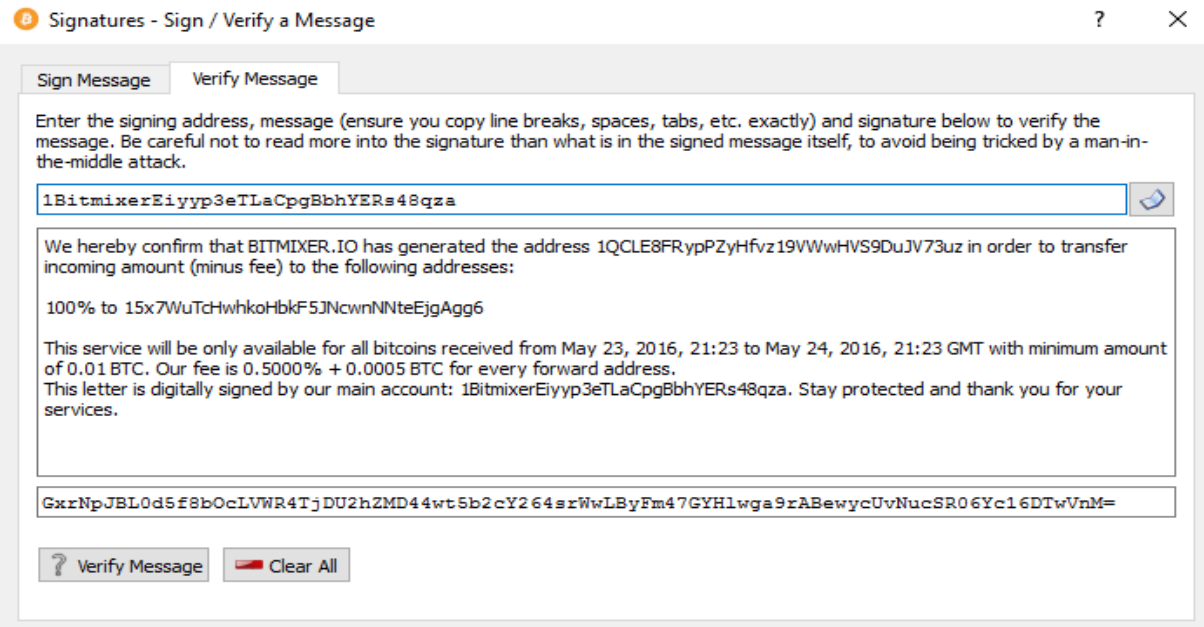


This is a foolproof solution, as those who do not own the private key cannot sign the message and are unable to put together a signature that would be verified.



Proof of identity is certainly a useful feature and it is something criminals have found useful as well. For example, sellers in the darknet use PGP and bitcoin signatures to prove their identity and ownership of bitcoin addresses. An experienced seller with a good reputation on one darknet website may create a brand new profile on another website yet can become a trusted seller, simply because he or she can offer an undeniable proof of identity.

Similarly, some mixing service providers such as bitmixer.io sign transactions to build trust with their customers. Customers then know that the deposit address indeed belongs to bitmixer.io and has a guarantee that the message was indeed generated by this entity. Also, in case of fraud, they can produce this proof in an attempt to discredit the mixing website if the transaction is not carried out:



A list of crimes facilitated by bitcoin

Over the last few years, bitcoin has experienced growth in terms of adoption and market value but the technology is far from achieving mainstream adoption. With a bit of simplification, there are four broad types of habitual bitcoin users profiled as technology enthusiasts, libertarians, speculators and criminals[13]. This chapter exclusively focuses on the activity of the last group, briefly listing bitcoin-facilitated types of crime as observed by both LE and private industry.

1. **Darknet**

Bitcoin is well established within the darknet and has gradually become a currency of choice for all sorts of criminal-to-criminal payments. While other cryptocurrencies such as Litecoin, Dash or Monero have been accepted by some of the marketplaces, the overwhelming majority of trade is still facilitated by bitcoin. Commonly traded items include drugs, fake IDs, counterfeit currency, compromised data including payment cards or accounts at online services, malware kits, weapons, explosives, chemical substances, 3D templates and 'how-to' guides for aspiring criminals.

[MS] [Bulk] [Sticky] Turkish Dragon Heroin +++NEW VENDOR SPECIAL PRICES+++

Item # 192094 - Opioids / Heroin - Drug-Monkey (325)

Views: 12081 / Bids: Fixed price

Buy price
USD 79.00
(0.1127 BTC)

There are indications that weapons sold in the darknet have been used to commit terrorist attacks in the EU whereas many websites claiming to collect contributions for terrorist groups or assassinations were most likely created by fraudsters.

Apart from trading illegal goods and services, typical crimes in the darknet include goods-not-delivered after the buyer decides to pay upfront, exit scams of marketplaces and business-as-usual scams performed by bitcoin mixers. Many mixers tend to work in a binary mode — if the deposit is relatively small the funds are laundered but once it reaches a certain threshold it is pocketed by the mixer operator.

Although most offenders do not exchange child abuse material for monetary gain, commercial exploitation has been observed by LE. This may be in the form of a payment for access to static material as well as more interactive live streaming of child abuse. More inventive approaches include crowdfunding websites, where offenders ask for financial contribution to facilitate their access to victims, such as through covering travel expenses to the third world countries, in exchange for privileged access to a newly generated child abuse material.

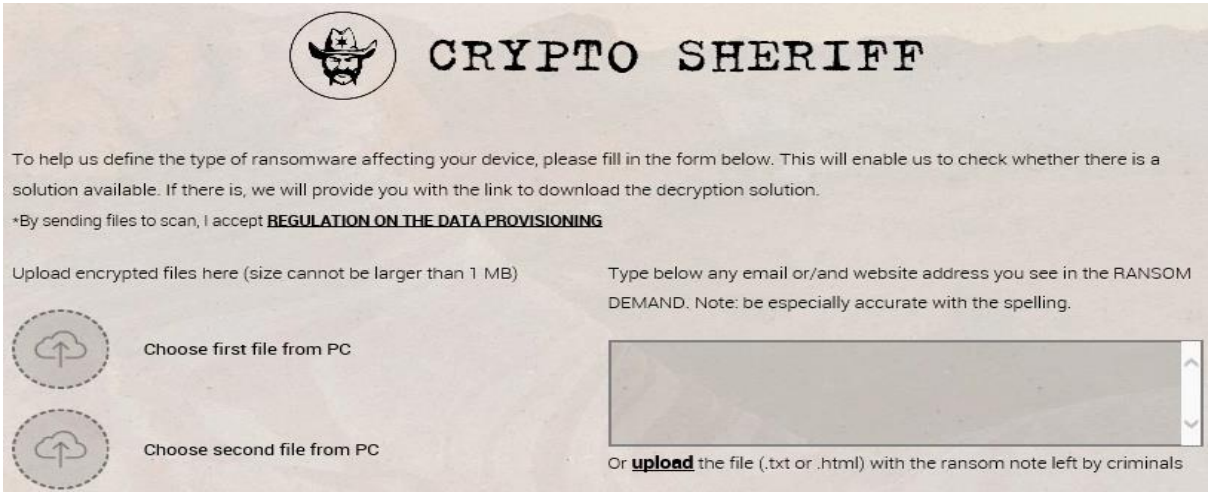
[13] Taylor and Francis Online, 'Characteristics of bitcoin users: an analysis of Google search data', 2015 (http://www.tandfonline.com/doi/full/10.1080/13504851.2014.995359).

2. Malware

(a) Ransomware

While ransomware had existed long before bitcoin came to existence, its explosive growth in 2013 coincided with the rise of bitcoin. Ransomware won a popularity contest over alternatives such as fake antiviruses and has become the key bitcoin-facilitated threat for the general population. By 2016, almost all forms of ransomware demand ransom in bitcoins, often as the only available payment option. While individual victims can be asked to pay anywhere between 0.2 to 10 bitcoins, targeted infections of companies providing critical services result in much higher demands[14].

While Europol advises against payment of the ransom to avoid funding criminal activity, many affected parties make an economic decision on whether the cost of ransom is lower than the loss of the data. The role of law enforcement is not limited to investigation; a significant emphasis is given to awareness and prevention efforts. At the end of July 2016, the Dutch police, Europol, Intel Security and Kaspersky Lab launched nomoreransom.org which, in addition to crime prevention advice, also helps victims to identify the malware and in some cases offers a decryption key for the encrypted files[15]:



[14] *International Business Times*, 'Hackers demand $3m bitcoin ransom from hospital to unlock vital files', 2016 (http://www.ibtimes.co.uk/los-angeles-hackers-demand-3m-ransom-hospital-unlock-vital-files-1543962).

[15] Europol Press Release, 'No more ransom', 2016 (https://www.europol.europa.eu/content/no-more-ransom-law-enforcement-and-it-security-companies-join-forces-fight-ransomware).

Since 2015, ransomware has been offered 'as a service' (RaaS). The price of RaaS kits is generally very low and can even drop to zero, as the malware developer/distributor receives a 20-50 % commission from all proceeds earned by the attacker deploying the malware.

Ransomware infections of traditional computing devices including servers/desktops/laptops continue to generate the vast majority of the income for criminals but ransomware also targets mobile phones, smart TVs or literally any device running one of the mainstream operating systems.

(b) Bitcoin-stealing Trojans

Bitcoin users are commonly targeted by remotely controlled Trojans going after their bitcoin wallets, private keys or logins to online bitcoin services. The wallets are attractive targets; if the wallet file is not encrypted or if the passwords are keylogged, there is nothing preventing the attacker from emptying the victim's wallet. The same effect can be achieved by stealing the victim's private key. Many of those who have lost funds had downloaded a compromised bitcoin or altcoin wallet.

(c) Clipboard malware

Clipboard poisoning attacks are a fairly well-established abuse vector, typically used to replace a URL stored in the clipboard with a link to malicious websites. When targeting bitcoin users, the malware is able to detect a bitcoin address copied to the clipboard and replace it with a hardcoded bitcoin address owned by an attacker. This is an elegant approach, as the malware does not necessitate keylogging the password or a network communication back to the attacker.

More advanced versions of the malware include of thousands of bitcoin addresses and will automatically select one that is closest to the intended recipient of the payment.

(d) Mining botnets

It did not take criminals long to realise that there is money to be made by mining bitcoin. Indeed, cryptocurrency that is distributed among those who sacrifice their hardware and electricity was appealing to botnet owners having an unobstructed access to plenty of both. Several botnets including the previously mentioned ZeroAccess were actively mining bitcoin until about mid 2013, when specialised bitcoin mining machines (ASICs) hit the market and made the traditional mining through processors and graphic cards obsolete.

Nowadays, bitcoin mining is no longer profitable — unless one invests in ASICs and has access to free electricity, as demonstrated by a few incidents across the EU, when suspects running bitcoin mining rig using stolen electricity were arrested.

3. Extortion schemes

Bitcoin has also become a favourite payment method for a number of non-malware-related victim-to-criminal payments commonly triggered by extortion. Based on anecdotal evidence provided by virtual currency (VC) exchangers, one of the fastest-growing crimes they witnessed in 2016 was sextortion. In addition to the usual luring and doxing of needy victims across adult chatrooms, unsophisticated criminals were quick to capitalise on the AdultFriendFinder and Ashley Madison breaches:

[MS] AdultFriendFinder Dump
Item # 54855 - Dumps / Dumps - ultimatum2016 (472)

Views: 557 / Bids: Fixed price

Buy price
USD 10.00
(0.0143 BTC)

Millions of users of these adult dating services were subject to identification and subsequent blackmail by scammers typically asking for 1 to 20 bitcoins in return for not disseminating the information to the victims' personal and professional contacts. While email remains the favourite communication channel with victims, some suspects prefer to make it clear that they know where the victim resides and send a blackmail letter via regular post.

If you do not wish me to destroy your life then send $2000 in **BITCOIN** to the ***Receiving Bitcoin Address*** listed below. **Payment MUST be received within 10 days of the post marked date on this letter's envelope**. If you are not familiar with bitcoin, read the attached "How-To"

Another form of exploitation widely popularised by a group called DD4BC (DDoS for Bitcoin) benefits from a combination of DDoS-capable botnets and bitcoin. Ransom demands were disseminated by both the group and impostors with no means to perform an actual DDoS attack. Several groups emerged in the aftermath of the arrest of the main target running DD4BC at the end of 2015.

The increased adoption of bitcoin may facilitate traditional crimes such as hijacks or kidnaps, where a human life may be at stake. Several of these crimes have already reported outside Europe. Completely anonymous, fast and irreversible digital payment may gradually render the bags filled with cash left at a remote location obsolete.

Virtually any threat could be combined with a demand of bitcoins, as evidenced by an increasing number of hoaxes reported through email or fake/compromised VoIP accounts. False reports of bombs being planted at airports, bus and train stations, schools and kindergartens that can be distributed in bulk are scalable to a much larger degree than LE resources.

4. Hacking of bitcoin companies

Bitcoin has proven to be highly resilient against counterfeiting attempts and attacks on its infrastructure. However, the same cannot be said about centralised entities providing services in the

VC ecosystem. VC exchangers transacting large volumes of digital assets and traders at these platforms are particularly attractive targets for hacking attacks.

Cryptsy, Shapeshift, Gatecoin and Bitfinex all suffered large-scale hacks in 2016. The Bitfinex breach in particular, resulting in the loss of almost 120 000 bitcoins[16] represents the largest loss of funds since the notorious Mt Gox incident in early 2014 when over 744 000 bitcoins disappeared. Unlike most attacks in the early bitcoin years, many companies affected by recent criminal activity have reported the incidents to LE and have actively supported investigation efforts.

5. Payment for criminal infrastructure

Criminals who do not wish to hide their presence in the darknet but still seek a high level of privacy may opt to purchase domain or infrastructure services at one of the providers offering payment in bitcoins or other cryptocurrencies.

6. Bitcoin double spend

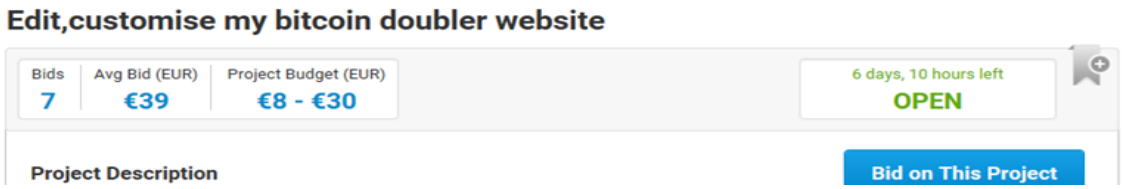
The majority of bitcoin users are aware that they should wait a few minutes for at least one confirmation to consider a transaction finalised. However, bitcoin is used in many scenarios where a fast payment is necessary, such as payments in shops or restaurant or at vending machines. In each of these scenarios, a scammer could perform a double-spend attack by sending a legitimate payment followed by a malicious payment from the same bitcoin address into another address under his control, this time with a higher transaction fee. Later on, when both transactions are picked up by the miner, there is a high chance that the malicious transaction will be given priority and the legitimate transaction will not make it into the blockchain. Due to bitcoin's specific nature and the generally low damage per incident these crimes are unlikely to be reported.

7. Bitcoin high-yield investment programs

While many incorrectly label bitcoin as a Ponzi scheme there are actual Ponzi schemes benefiting from surfing the bitcoin wave. Probably the largest scheme at the moment is MMM[17] run by a prolific Russian scammer Sergei Mavrodi. Most of the victims of the scheme are based in China or third world countries.

A plethora of websites ask for deposits in exchange for unrealistic returns on investment; some of these are referred to as bitcoin doubling websites[18]. Scammers with no web development skills outsource the work at very low cost to India or Pakistan.

[16] *Financial Times*, 2016, 'Bitcoin Bitfinex exchange hacked: the unanswered questions' (http://www.ft.com/cms/s/0/1ea8baf8-5a11-11e6-8d05-4eaa66292c32.html).
[17] MMM official website: http://mmmglobal.org/
[18] Lion Invest official website: http://www.lioninvest.org/



Altcoins are plagued with very different types of scams. Many altcoins just replicate bitcoin source code and are promoted using false claims. Even genuine altcoins can become subject to pump and dump schemes. Due to the extremely low liquidity of some of the coins, they are inexpensive to buy in bulk and notably increase in price in the process of doing so. The initial price increase is further fuelled as the other investors are attracted to join in, tempted by promotional spam campaigns in social media and the VC fora. The manipulators then sell all coins when a desired price is reached, leaving others with plummeting prices.

8. Social engineering

Bitcoin is not yet widespread when it comes to so-called Nigerian scams, probably due to the profile of a bitcoin user being quite different to the profile of a typical victim falling for an unsophisticated advanced fee fraud. Bitcoin would require a significant increase in adoption in order to be massively exploited for this type of fraudulent activity.

Therefore, attackers have to resort to more advanced techniques, including the development of sites that appear to be relevant for bitcoin investors such as bitcoin price prediction websites, and wait for reckless individuals to sign up for these sites reusing credentials they use at one of the VC exchanges.

Scammers commonly take advantage of the negative events affecting bitcoin users. In the aftermath of the Bitfinex hack, phishing emails, Facebook profiles and phony websites were created in an effort to steal users' credentials by asking them to fill out an 'application for refund'.

9. Money laundering

A number of services including exchangers, wallet providers, mixers and alternative currencies provide a higher degree of privacy in the placement, layering or integration phases of money laundering in exchange for a fee. Several exchangers have been found to have absent or insufficient AML and KYC policies in place, resulting in their takedown, fine[19] or arrest of the administrators[20]. Occasionally OCG may opt to invest illegitimate proceeds in bitcoin mining equipment in order to generate new bitcoins or to justify the origin of their funds[21].

[19] NewsBTC, 'Bitcoin exchange OKCoin fined in money laundering case', 2016 (http://www.newsbtc.com/2016/08/15/china-okcoin-exchange-fined/).
[20] CNN Money, 'Bitcoin exchange CEO arrested for money laundering', 2014 (http://money.cnn.com/2014/01/27/technology/security/bitcoin-arrest/).
[21] Europol, 'Spanish network behind the illegal distribution of pay-TV channels dismantled', 2016 (https://www.europol.europa.eu/content/spanish-network-behind-illegal-distribution-pay-tv-channels-dismantled).

How to investigate bitcoin transactions in a nutshell

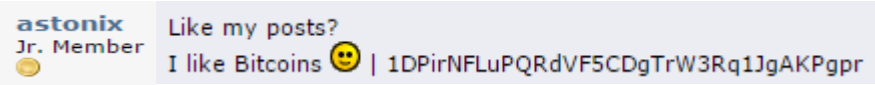
Bitcoin was not created with the objective of being completely anonymous.

Instead, it combines an interesting mix of transparency and privacy for its users, which is referred to as pseudonymity. This concept is best explained by its to-this-day-unknown creator Satoshi Nakamoto: 'The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.' As mentioned earlier in this guide, all bitcoin transactions can be viewed and inspected without a need to send subpoenas or MLATs and dealing with all the bureaucracy that inevitably comes with cross-border investigations.

Many investigations involving VCs start with something that is often known to the victim — the bitcoin address of the offender. The essential question for the investigator therefore is: What can the investigator do with the bitcoin address?

1. Google is your friend

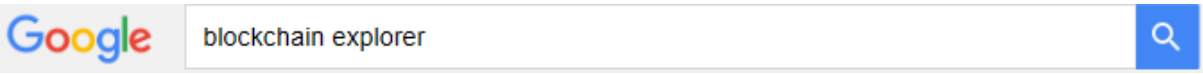
Before trying anything else, one should simply run the BTC address through the search engine. The successful hits often lead to online forums such as bitcointalk.org, where the bitcoin addresses feature in the messages, signatures or profiles of the discussants.



Many forums display public information on the person who created the post including nickname, contact details and lists of all posts along with associated timestamps. Furthermore, IP logs, activity summaries, personal/private messages and additional contact details may be provided by the administrators on request.

2. Use a blockchain explorer

All bitcoin transactions dating back to the very beginning of 2009 are recorded in bitcoin blockchain, a large public database storing all data in an unencrypted state. The blockchain is not stored centrally — it is stored by thousands of individuals and companies around the world running bitcoin clients. Anyone can download the blockchain files and try to dissect the data, import it to a database and query it. However, since that would be a cumbersome task most investigators rely on publicly available and free-to-use blockchain explorers.



Blockchain explorers are used to conveniently query the blockchain and display the results in a human-friendly way. While there are differing opinions on which explorer is the best, the popularity contest has been won by Blockchain.info. While many other blockchain explorers exist, these

generally provide users with identical information served in a different visual package. One notable exception is blocktrail.com, which parses bitcoin.org for metadata[22], a feature only to be seen in commercial tools. As the investigators become increasingly familiar with blockchain.info, it is recommended to stick to this trusted explorer to facilitate the exchange of information. For consistency reasons, we will also use this explorer in the practical part of this guide.

3. Try to identify addresses on Walletexplorer.com

Tracing bitcoin flow from one bitcoin address to another would make little sense without attribution — linking at least one of these addresses to a real subject.

Please note that what is generally identified by Walletexplorer and its commercial alternatives is not the full name of the suspect who owns the bitcoin address. Instead, what is revealed is a name of the managing entity, such as exchanger, wallet provider, payment processor, merchant or a gaming site. Then it is up to LE to send a request to the identified company in an attempt to get the client details.

Walletexplorer.com remains the best publicly available free resource that links several millions of bitcoin addresses to wallets managed by hundreds of the largest entities.

4. Use commercial bitcoin tracing tools CHAINALYSIS ELLIPTIC

There are several excellent commercial tools that can be used to track bitcoin transactions and identify owners of bitcoin addresses. These include Chainalysis, Elliptic, Blockseer, Ciphertrace, Skry or Bitanalysis. While subject to a licence fee, usually in form of a monthly subscription payment, these tools offer additional information and convenience open source tools lack.

Compared to Walletexplorer, these tools can offer: improved wallet detection resulting in a lower number of false positives or false negatives, more wallets linked to entities and graphic visualisation of links between wallets. Some tools also offer additional information to the bitcoin addresses gathered through the scraping of web or darknet sites. Feel free to contact EC3 for contact on the above companies.

5. Involve EC3

EC3 may cross-match the bitcoin addresses provided against addresses that are stored in-house including data extracted from online marketplaces taken down as part of operation Onymous and several other marketplaces and other sources harvested online or received from other LE agencies. Please note that in order to request operational assistance from EC3 it is mandatory to use the

[22] Observed by Andrew Rowbotham from Kriminalpolizeidirektion Offenburg

official communication channel — SIENA (Secure Information Exchange Network Application). If you need any assistance contact your national unit which should help you with putting together the request and sending it over to the Europol liaison bureau, which will pass it to the relevant section at Europol.

Questions regarding virtual currencies and relevant investigations may be submitted to the Virtual Currency Taskforce on SPACE (if you require access please contact jaroslav.jakubcek@europol.europa.eu). Please avoid sending operational data through this channel.

6. Contact identified entities

Similar to other cybercrime investigations, the majority of investigations would lead nowhere without assistance from the private sector. The role of bitcoin exchangers in particular cannot be overestimated as these companies enable the conversion of fiat money to virtual currencies and vice versa and hence are commonly used by bitcoin users.

Bitcoin exchangers are goldmines of information on individual clients, typically storing name, verified contact details, IP logs, activity logs, all bitcoin and other cryptocurrency addresses used by the user on the exchange, personal messages, payment information, a proof of ID and proof of home address. Proof of ID is usually a passport, national identity card or driver's licence.

Since fake IDs can be freely downloaded from the internet or purchased in the darknet, some exchangers have another form of verification in place including a Skype verification or asking the customer to produce a selfie holding the ID or a paper with a random text written on it.

Contact details for the exchangers and other notable participants in the VC ecosystem can be found in the annex to this guide.

7. Seize bitcoins

There are two key objectives in bitcoin investigations — to detect the suspects and to recover bitcoins that have been stolen or used to facilitate criminal activities. The investigators should be aware of two main ways to seize bitcoins:

1. gaining access to the suspect's wallet.dat file combined with a password or discovering a private key or a wallet seed, typically in the text file or printed on a paper;
2. cooperation with third parties managing the suspect's bitcoins. Once it has been discovered that a suspect is storing bitcoins at one of the online exchanges or wallets, it may be possible to request a temporary freeze of these assets.

This is, in a nutshell, how the investigator may follow the money within the bitcoin blockchain. The next section inspects tracing and attribution in greater detail.

How to investigate bitcoin transactions in detail

1. Google is your friend

The majority of investigations following the movement of virtual currency start with an identified bitcoin address belonging to the suspect. Often the address is known to victims who were instructed to send bitcoins over to the suspect as a result of extortion or other criminal activity.

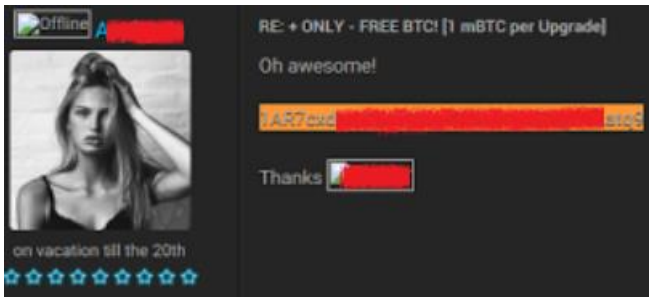
When a bitcoin address is entered into a search engine, it quite often generates a number of search results. It is likely that many of these will be just links to blockchain explorers, which will not provide details leading to an immediate identification of the suspect. Nevertheless, many investigations have succeeded because of the suspect's negligence, when they published their bitcoin address online.


CASE

An example of how simple open source research can identify the perpetrator was provided by a US-based exchanger.

A suspect gathered 70 000 usernames and passwords from one of the recent data breaches and developed an automated script that was testing each of these credentials against the exchanger's website. He managed to compromise about 20 accounts and consequently withdrew 1.85 bitcoins to his personal bitcoin address before the exchanger blocked his account. While the damage in this case was relatively low, the offender could easily replicate the crime with new sets of credentials. Also, he very likely targeted other exchangers as well.

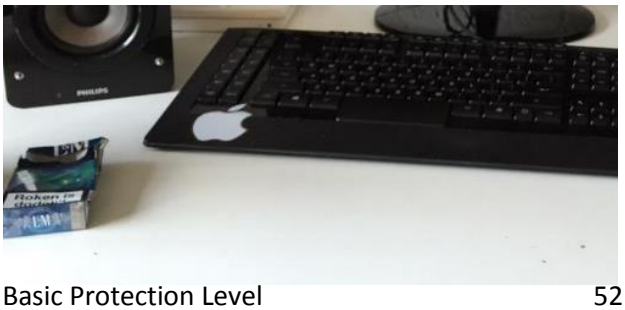
All the funds were sent to a single bitcoin address. The exchanger decided to follow the money and entered the bitcoin address into a search engine. The address was shown to be linked to a user account on a forum website.



This account was then linked to Twitter, Steam accounts and YouTube. The YouTube account provided the real name of the offender, which also featured on Facebook. To further confirm the identity of the suspect, one of the photos on Facebook showed the same sound speakers as a photo that featured on leakforums.net.

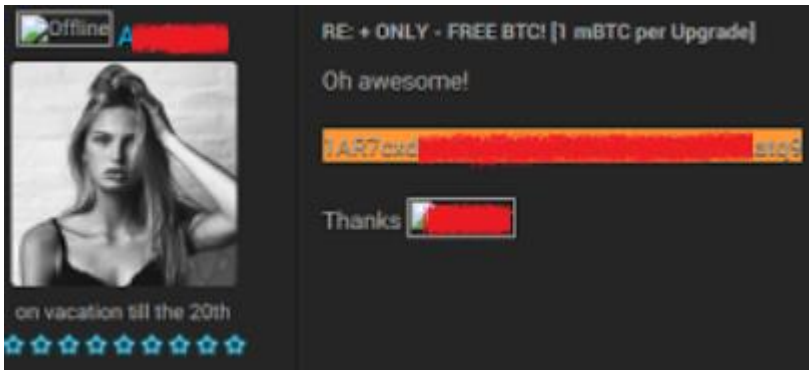
Photo on Facebook:

Photo on leakforums.net

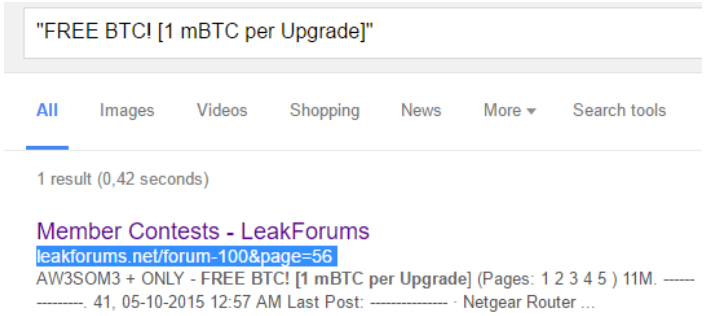


The moral of the story is that with a bit of luck and persistence, the individuals behind suspicious transactions may be detected using basic OSINT techniques.

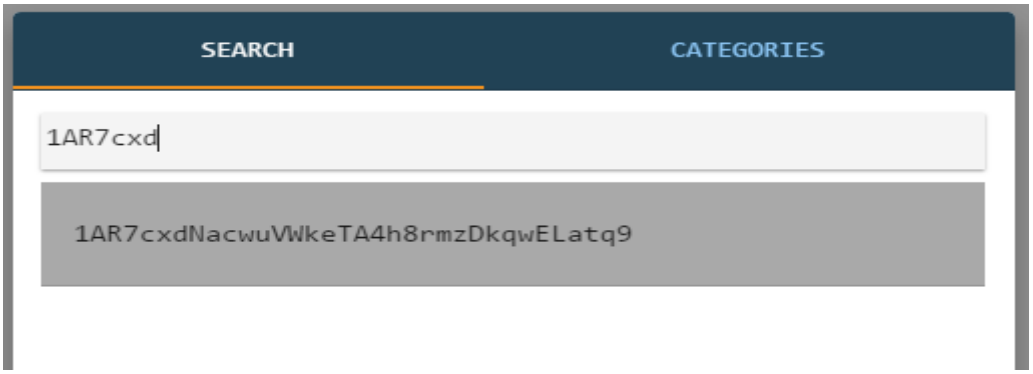
Speaking about investigation techniques, there are at least two ways to identify the full BTC address based on the image below. Before proceeding to the solution, try taking a good look at the image and think about the answer.



The first approach would be use of a search engine, followed by registration on discovered forum and search for strings of text visible at the image.



The second approach would be to use the commercial tool shown in the chapter on Handling partial bitcoin addresses



Out of dozens of millions of existing bitcoin addresses, the string '*1AR7cxd*' brings up exactly one result: *1AR7cxdNacwuVWkeTA4h8rmzDkqwELatq9*

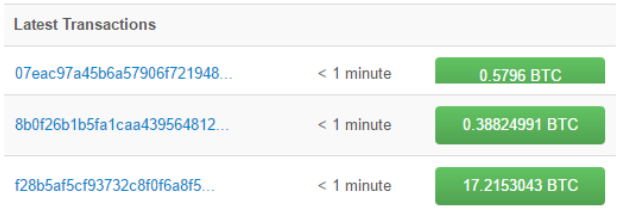
2. Use a Blockchain Explorer

The term 'Blockchain Explorer' offers a good hint about what these tools are used for — making sense of the dozens of gigabytes of data stored in the bitcoin blockchain. They are typically used by bitcoin users to check or verify whether their transaction went through. For investigators, the main motivation is to follow the flow of bitcoin in an effort to trace the movement of funds from one bitcoin address to another.

The upper part of blockchain.info shows the recent blocks added to the blockchain. The fact that the transactions are in the blocks means that these were not only propagated through the network but were also confirmed by the miner and therefore are not practically reversible.

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
412407	26 minutes	1777	13,129.34 BTC	BTCC Pool	989.07
412406	30 minutes	1730	16,228.55 BTC	AntPool	998.13
412405	36 minutes	1972	14,389.46 BTC	AntPool	998.07
412404	39 minutes	1772	13,933.80 BTC	F2Pool	999.88
412403	42 minutes	2101	11,332.07 BTC	F2Pool	999.65
412402	43 minutes	1860	34,379.73 BTC	BitFury	998.16

Source: Blockchain.info, 19 May 2016.

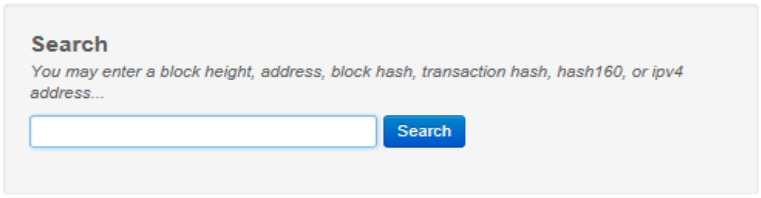


The left side of the website shows real-time incoming unconfirmed transactions as they get propagated through the bitcoin network and picked up by blockchain.info nodes. The following section of the website provides a more detailed look at the unconfirmed transactions.

The block 'Height' shows the age of the block, starting with the very first block #0 back in 2009 all the way to the current block height of over 440 000 as of November 2016 and still counting. The second column — 'Age' — is a practical demonstration of bitcoin confirmation times, where the new blocks are created on average once per 10 minutes — with considerable swings both ways as can be seen on the example above. Also shown are aggregated values per block, such as the number of transactions per block, their value in bitcoins or US dollars (representing aggregated outputs that include payment, change and a fee, which will be discussed later) and the total size of the block in kilobytes.

Unlike many other block explorers, blockchain.info can automatically recognise various types on input. Based on the length and pattern of the input, it distinguishes whether the user entered a bitcoin address, IP address, number of a block or something completely different. When it comes to IP addresses, only Ipv4 is recognised while entering Ipv6 only generates an error message.

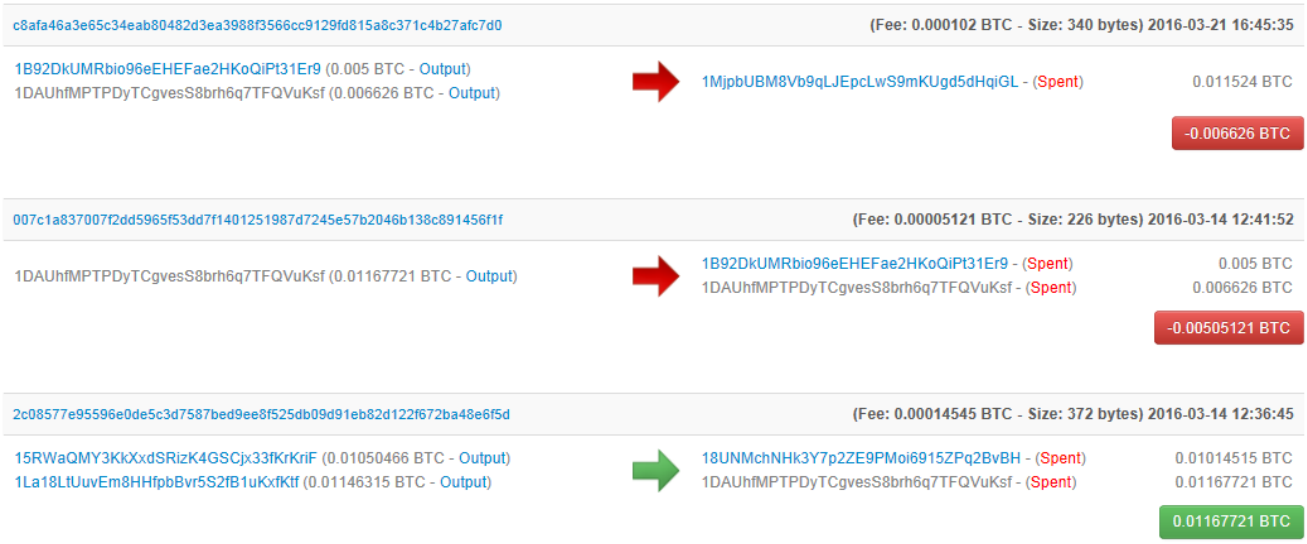
Nevertheless, vast majority of the users search for either a bitcoin address or a transaction hash.



The summary for the bitcoin address is at the top of the site. It shows a great deal of information about each transaction; the most important ones feature the bitcoin address, total number of both incoming and outgoing transactions, total amount of bitcoins ever received and current balance. The following is a summary for bitcoin address *1DAUhfMPTPDyTCgvesS8brh6q7TFQVuKsf*.

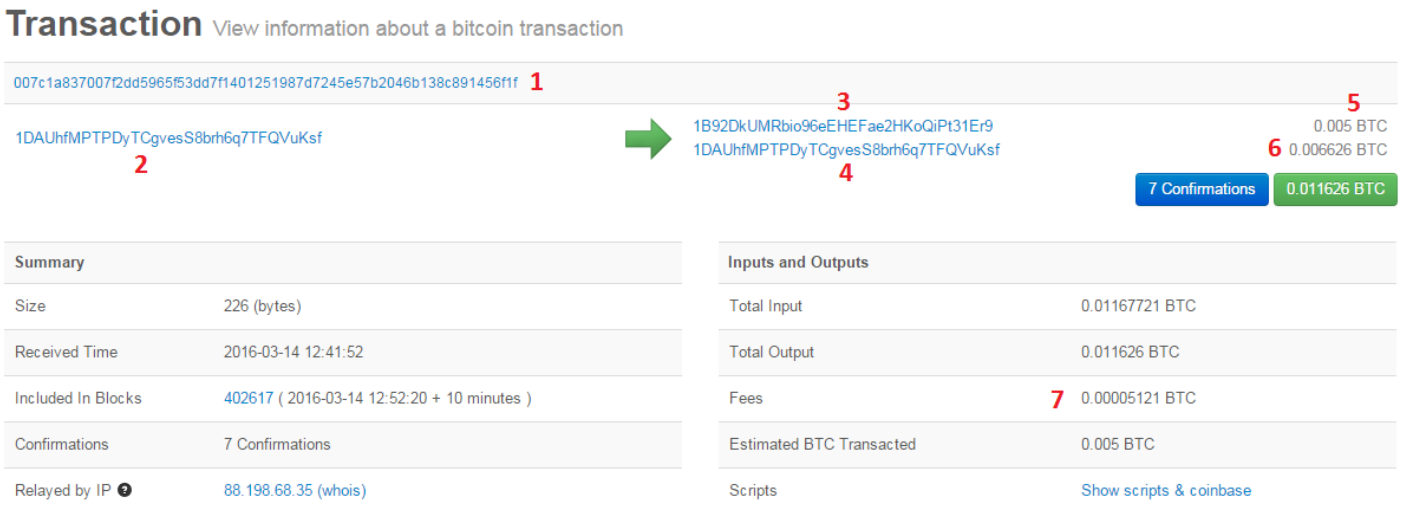
Summary		Transactions	
Address	1DAUhfMPTPDyTCgvesS8brh6q7TFQVuKsf	No. Transactions	3
Tools	Taint Analysis - Related Tags - Unspent Outputs	Total Received	0.01167721 BTC
		Final Balance	0 BTC

The summary is followed by the list of incoming and outgoing transactions to the bitcoin address sorted chronologically starting with the latest transaction. Note that in our case the abovementioned address first received a small amount of bitcoins on 14 March 2016 at 12:36 before spending everything in two transactions on the same day at 12:41 and 16:45 respectively.



Each transaction includes an *input* and an *output*. One transaction's output is input for the next transaction — in this way bitcoin transactions can be traced all the way to the point when bitcoins were generated by the miner.

The following is an example of a transaction[23]. There are several elements of information in a bitcoin transaction are highlighted in red.



Transaction View information about a bitcoin transaction

007c1a837007f2dd5965f53dd7f1401251987d7245e57b2046b138c891456f1f 1

1DAUhfMPTPDyTCgvesS8brh6q7TFQVuKsf
2

3
1B92DkUMRbio96eEHEFae2HKoQiPt31Er9
1DAUhfMPTPDyTCgvesS8brh6q7TFQVuKsf
4

5
0.005 BTC
6 0.006626 BTC

7 Confirmations | 0.011626 BTC

Summary	
Size	226 (bytes)
Received Time	2016-03-14 12:41:52
Included In Blocks	402617 (2016-03-14 12:52:20 + 10 minutes)
Confirmations	7 Confirmations
Relayed by IP	88.198.68.35 (whois)

Inputs and Outputs	
Total Input	0.01167721 BTC
Total Output	0.011626 BTC
Fees 7	0.00005121 BTC
Estimated BTC Transacted	0.005 BTC
Scripts	Show scripts & coinbase

1. This is the transaction ID (also known as TxID). This is used to refer to a transaction, and can be entered in any bitcoin blockchain explorer to find a transaction. The transaction ID is a (SHA-256) hash of all information in a bitcoin transaction. It can be recognised as a 64-character-long hexadecimal string. Hence, it is longer than bitcoin addresses.
2. This is the input bitcoin address from which bitcoins were sent to another address. The total amount of bitcoins spent in this transaction can be seen in the green box.
3. This is one of the new outputs. This is the bitcoin address the bitcoins were sent to. The amount that was sent to this address is numbered 5.
4. This is the change address, the other new output. In this particular example it is returned back to an input address (2).
5. This is an amount that was sent to another Bitcoin address.
6. This is a change amount. Change will be returned to the same wallet that contains the input bitcoin address.
7. This is a transaction fee. Note that the fee amount is lower (0.00005121) than the standard minimum amount (around 0.001 per Kb), as the fee in this transaction was dynamically set to match the network's current load.

[23] EC3 Cyberbit on bitcoin transactions.

Tracing bitcoin transactions

The purpose of this chapter is to demonstrate how to follow the money in the bitcoin blockchain. It explains how to interpret the blockchain and demonstrates different types of bitcoin transfers on a number of easy-to-digest examples.

It is necessary to understand the following basic rules for the transactions:

1. One person can have multiple wallets and one wallet can hold multiple bitcoin addresses.
2. A non-zero number of bitcoins must be transferred from one address to another.
3. Each transaction has an input and output side. Input shows where bitcoins are coming from and output shows where the bitcoins are going to.
4. The addresses on the input side must have a sufficient amount of bitcoins available for the transaction. It is not possible to send more bitcoins than one already has in one's possession.
5. All addresses on the input side[24] will be fully spent.
6. The majority of transactions in the blockchain and practically all recent transactions have to include a fee; otherwise miners may not put the transaction into the blockchain.
7. The amount of all inputs must be equal to amount of all outputs plus the fee for the transaction (Sum of inputs = sum of outputs + fee). Bitcoin transactions follow the zero sum logic so what goes in must come out.

A transfer from one bitcoin address to another does not necessarily represent a movement of funds from one person to another and it may not even represent a movement between two different wallets. One address may send bitcoins to another address and but these two addresses may still reside in the same wallet. What is 100 % certain is that the flow of bitcoins from one bitcoin address to another and everything else is a mere hypothesis.

On the next few pages, several common types of transactions will be discussed. These will be followed by a more detailed inspection of input transactions, transaction fees and mixers.

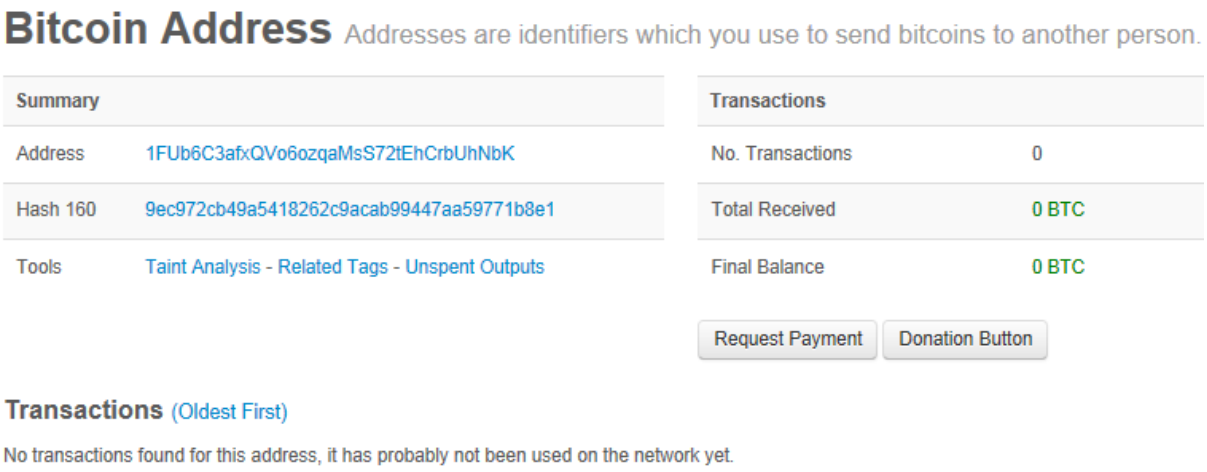
[24] More technically correct would be to say that all unspent outputs from the previous transactions were selected to serve as inputs for the current transaction have to be fully spent. We will later see that there may be several unspent outputs sitting on the same address and each of these can be spent separately.

Type 1: Non-existent transactions

To follow the money in a bitcoin blockchain, there has to be a transaction to start with.

While this may sound obvious to some, Europol has received quite a few requests for tracing of transactions when no transaction exists and thus the bitcoin address in question has never received or sent any bitcoins. Such requests often come as a result of a ransomware infection or other form of extortion where the victim does not pay the ransom and instead reports the crime to law enforcement.

An example of one such address:
https://blockchain.info/address/1FUb6C3afxQVo6ozqaMsS72tEhCrbUhNbK



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1FUb6C3afxQVo6ozqaMsS72tEhCrbUhNbK	No. Transactions	0
Hash 160	9ec972cb49a5418262c9acab99447aa59771b8e1	Total Received	0 BTC
Tools	Taint Analysis - Related Tags - Unspent Outputs	Final Balance	0 BTC

Request Payment Donation Button

Transactions (Oldest First)

No transactions found for this address, it has probably not been used on the network yet.

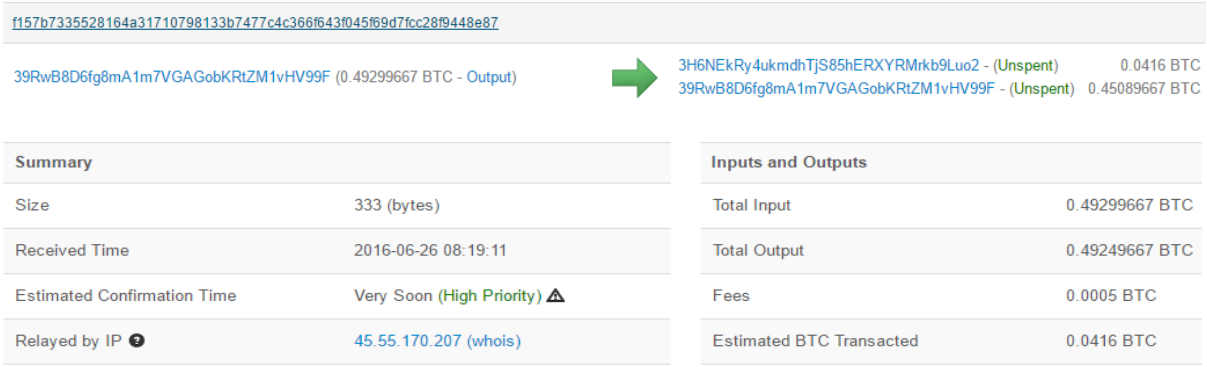
Unfortunately, there is not much that can be done with such request as there is nothing to trace and the only thing that can be done is to cross-match the address against several millions of other addresses stored by Europol. However, bitcoin addresses used by different exploitation schemes are often newly generated addresses that are unique for each victim so the probability of a hit in such cases is very low.

Type 2: 1 input and 2 output transactions (where input address features in the output)

This is one of the most often seen transactions in a bitcoin blockchain. It features one input feeding into two outputs. This means that the address on the left is fully spent and all bitcoins present on it are moved over to the output addresses.

What is happening here? Address A is spending bitcoins, which are transferred to Address B. However, since the balance on A is higher than the amount transferred to B, change has to be returned to a payer. In the above example, the change returns to address A.

An example of such a transaction is:
f157b7335528164a31710798133b7477c4c366f643f045f69d7fcc28f9448e87



f157b7335528164a31710798133b7477c4c366f643f045f69d7fcc28f9448e87

39RwB8D6fg8mA1m7VGAGobKRtZM1vHV99F (0.49299667 BTC - Output)

3H6NEkRy4ukmdhTjS85hERXYRMrkb9Luo2 - (Unspent) 0.0416 BTC
39RwB8D6fg8mA1m7VGAGobKRtZM1vHV99F - (Unspent) 0.45089667 BTC

Summary	
Size	333 (bytes)
Received Time	2016-06-26 08:19:11
Estimated Confirmation Time	Very Soon (High Priority)
Relayed by IP	45.55.170.207 (whois)

Inputs and Outputs	
Total Input	0.49299667 BTC
Total Output	0.49249667 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.0416 BTC

What can we find out about the above transaction?

At the beginning of the transaction, there are approximately 0.49 bitcoins sitting on address A (39RwB8D6fg8mA1m7VGAGobKRtZM1vHV99F). A then sends 0.0416 Bitcoins to B (3H6NekRy4ukmdhTjS85hERXYRMrkb9Luo2). Assuming A had previously only received one transaction, it has to spend all bitcoins that are sitting on the address, so it transfers all 0.49 bitcoins. Since only 0.0416 bitcoins are actually sent to B, the remainder has to return to the sender as change. In the example above, the second output is the change that is returned input address A. Hence, address A owns approximately 0.45 bitcoins at the end of the transaction.

The above example marks an obvious distinction between traditional banking transactions that would typically only include one input and one output. In the traditional environment, only the exact amount is paid so there is no need to create additional change output. Unfortunately for investigators that is not how bitcoin transactions work.

The size of the transaction is 333 bytes and the fee for the transaction is 0.0005 BTC. This corresponds to a fee of about 0.0015 BTC per Kb, which is slightly higher than usual and as a result it may be treated by the miner as the priority — it may be confirmed it as quickly as possible and may be inserted into the next block.

Note that the fee is very important, as a suspect may opt to use the same amount of the fee per transaction or fee per Kb for many other transactions. On the other hand, the IP address of the node that passed the information about the transaction to blockchain.info is usually of little practical value for the investigator.

The transaction was received by one of the blockchain.info nodes on 26 June 2016 at 08:19:11. So this is merely a propagation time, not the time of confirmation. The time format is UTC so it is 2 hours behind European Summer Time. Hence the time would correspond to 09:19:11 in the United Kingdom or 10:19:11 in the Netherlands.

After about 1 hour, the same transaction had been confirmed seven times. This means it was put into the blockchain by the miner and six other blocks were mined on top of it. The block number where the transaction is located is 418033.

Summary	
Size	333 (bytes)
Received Time	2016-06-26 08:19:11
Included In Blocks	418033 (2016-06-26 08:32:09 + 13 minutes)
Confirmations	7 Confirmations

Inputs and Outputs	
Total Input	0.49299667 BTC
Total Output	0.49249667 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.0416 BTC

Type 3: 1 input and 2 output transactions (where input address does not feature in the output)

This is the most common transaction nowadays. Like the previous type of transaction, it features one input feeding into two outputs. The input address is fully spent and all bitcoins are moved to two different output addresses.

What is happening here? Address A is spending bitcoins, which are transferred to address B. This time the change goes back to the same wallet that contains A, but the change is returned to a newly generated bitcoin address C, as can be demonstrated by the following transaction: 08ecd5354a0aa3acb5e94f53ebbe2bbbbcc7403899207f27d8572a83b70b0e7f.

Summary	
Size	225 (bytes)
Received Time	2016-01-02 14:36:22
Included In Blocks	391442 (2016-01-02 20:52:59 + 377 minutes)
Confirmations	140 Confirmations
Relayed by IP	192.146.137.1 (whois)

Inputs and Outputs	
Total Input	0.5 BTC
Total Output	0.49999502 BTC
Fees	0.00000498 BTC
Estimated BTC Transacted	0.01 BTC
Scripts	Show scripts & coinbase

This type of a transaction is a bit trickier, because it is not possible to distinguish which one of the two addresses in the output represents a payment and which is the change. Both addresses are different from the one in the input and sometimes only the payer and recipient know the real story.

There are several ways to **determine the change address**:

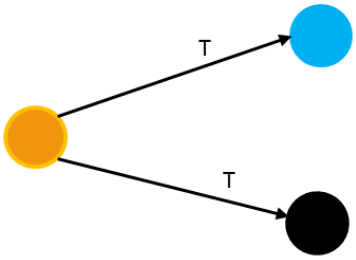
1. Check whether output address features among inputs as seen on the previous type of transaction (transaction type 2)

2. If this does not work, check the output addresses to see if these have any historical transactions. If they do, they cannot be change addresses as the change address has to be either the reused input address or the newly generated address.

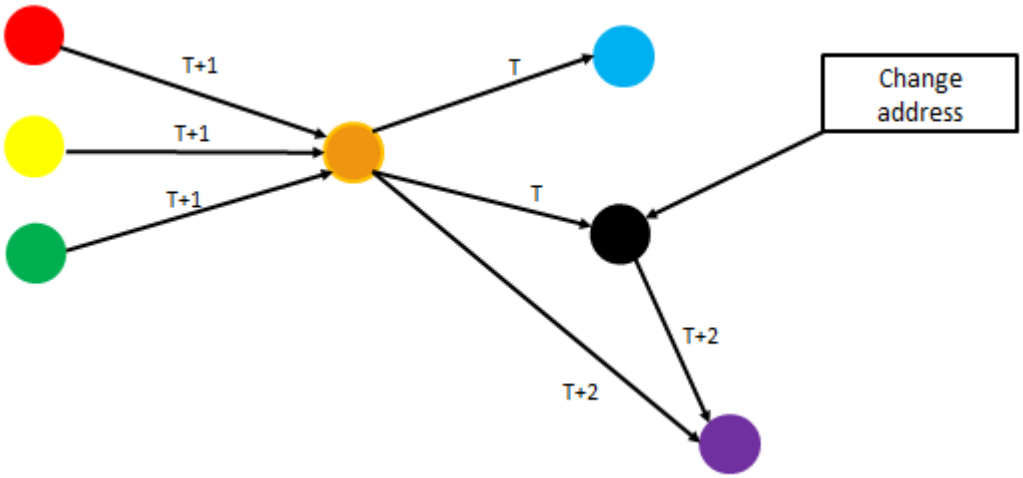
   This approach did not help as both 1KfrRC4WN9wJJxvCn3Z9vQbpR8xQCFrqYR and 122PeFgD4MdoCYN9ZEB4z6DxcnzaG8BpWS never featured on the blockchain before the transaction.

3. Another, rather time-consuming, approach involves checking the past and the future. This will be demonstrated using a rather colourful example.

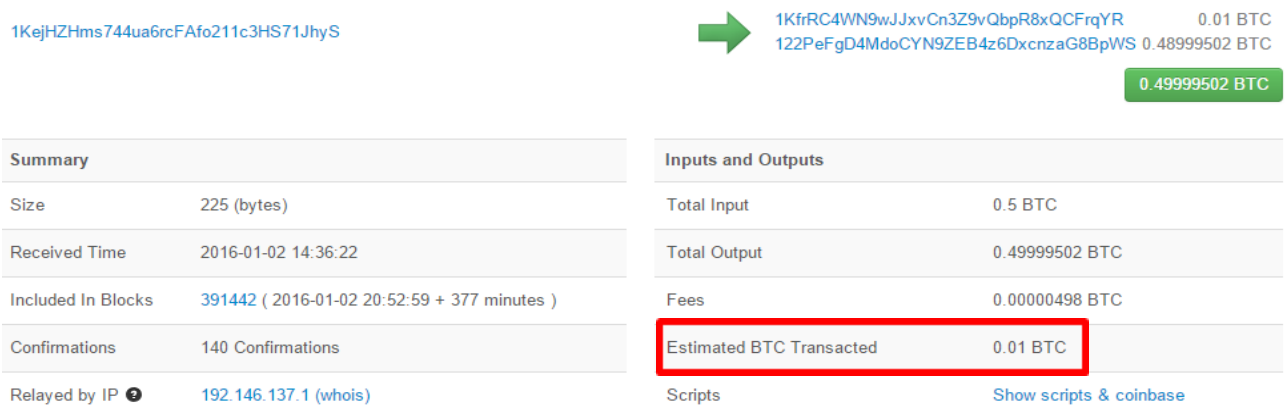
   The following transaction resulted in a payment to either the blue or the black address. Looking at this transaction in isolation we may be unable to say which addresses is a payment and which is a change.



   If we check future transactions to and from the orange address, we may discover one where a payment arrived from three different input addresses (T+1). This still does not help much. However, checking other future transactions we can see that the payment received in transaction (T+1) was sent from the orange to the black and purple addresses (T+2). Since the orange and black addresses were spent during one transaction, they had to be present in the same wallet and that is why the black address must have been the change. Consequently this also means that the blue address was the one that received the payment.



4. A similar algorithm is implemented by blockchain.info that attempts to establish which of the outputs is a payment. And indeed, also blockchain.info identified that the payment was 0.01 BTC and therefore 122PeFgD4MdoCYN9ZEB4z6DxcnzaG8BpWS must have been the change address.



5. There used to be a bug in the official bitcoin client that caused all change to be sent to the first output of a transaction. Essentially, the random number generator was broken and always returned *0*, making the change always appear as the first output. This bug was fixed on 30 January 2013. However, we have to keep in mind that other implementations of wallets did not suffer from this error and therefore we can still see 6.8 % of transactions in the second place of the two-output transactions[25] even before that date.

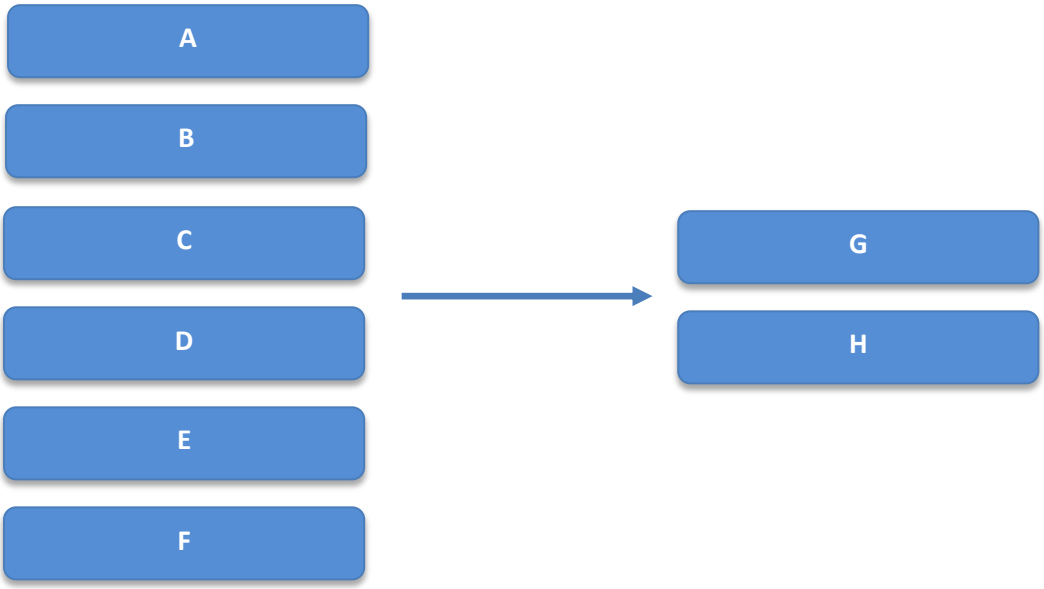
6. We can also try to apply a behavioural approach to determine the payment address. For example, humans like round numbers, so in theory it is more likely that someone paid 0.01 bitcoins rather than 4.8999502 bitcoins and therefore the latter is likely to be change and more often than not this also may be a correct assumption. Naturally this approach may backfire if the suspect deliberately intends to frustrate the investigator.

   We can also take a look at the previous transactions linked to suspects in order to extrapolate their transaction behaviour taking into account date/time of transaction, frequency of bitcoin transfers, fee amount, tendency to send rounded amounts, etc.

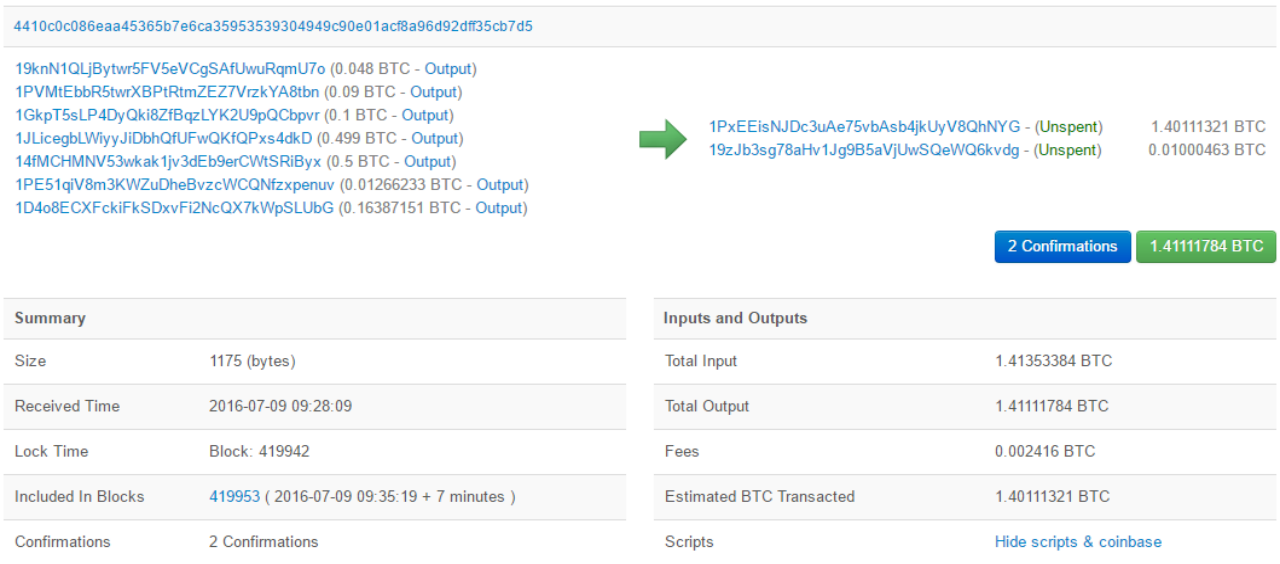
[25] Michele Spagnuolo, 'BitIodine: extracting intelligence from the bitcoin network', Politecnico di Milano, Milan, Italy, 2014.

Type 4: Multiple input transactions

The next type of transaction is a multi-input transaction that can include anywhere between two and several hundred[26] input addresses. To an untrained person, this may look like a confusing transaction, probably involving some kind of mixing that will make investigation difficult.



An example of such a 'complicated' transaction with multiple input addresses is: 4410c0c086eaa45365b7e6ca35953539304949c90e01acf8a96d92dff35cb7d5.



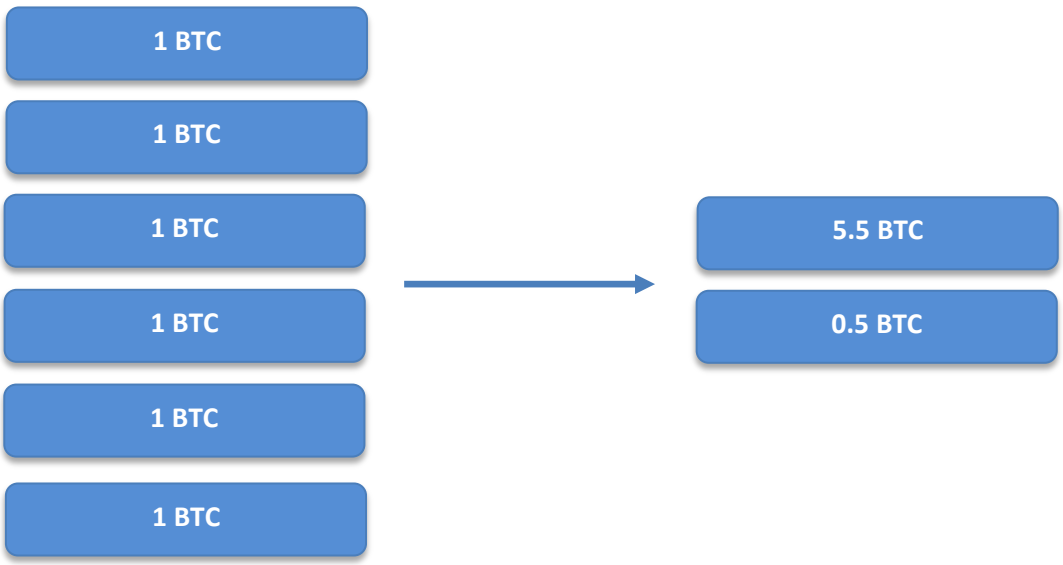
[26] While the number of inputs/outputs is not subject to a hard limit, the total size of the transaction must be lower than 100 Kb to be included in a block so the maximal number of inputs/outputs is by no means infinite.

The reality could not be more different. The vast majority of transactions in the bitcoin blockchain that have multiple inputs are signed and propagated by the same wallet. In the example above we can reasonably assume that the seven input addresses all belong to the same entity. Therefore having multiple input addresses is not confusing; it actually helps the investigator to link different addresses together and to tie these to a single wallet.

This linking of inputs is the most fundamental clustering technique as it links the addresses to the same cluster that may either be an independent user or a known entity.

So far we have discussed the input side of the transaction and how this can be beneficial for the investigator. However, there is still a need to distinguish between a payment and change on the output side. Essentially, the six approaches listed in the previous section can help us to tell these two apart.

However, there is one more factor to take into account — the number of bitcoin addresses spent by each of the addresses on the input side. Here we can correctly assume that bitcoin wallets try to be reasonable when handling inputs and usually they do not try to spend more inputs than necessary. This can be demonstrated by the following example.



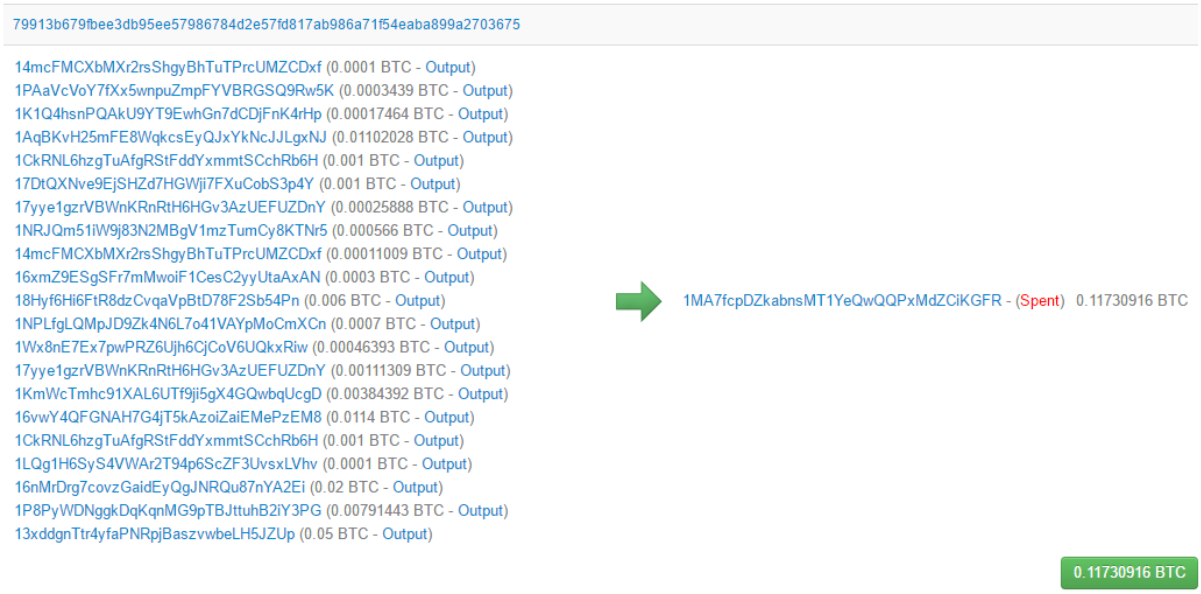
This transaction combines six inputs of exactly one BTC that were previously received by the paying wallet. In total, six bitcoins are spent in the transaction. Based on the two transactions on the output side, we can decide whether the payment was 5.5 BTC or 0.5 BTC. Since we know that wallets generally do not spend more inputs than necessary the payment has to be 5.5 BTC because the payment of 0.5 BTC would not justify the use of six different input addresses. Consequently, the remaining 0.5 BTC must be the change.

19knN1QLjBytwr5FV5eVCgSAfUwuRqmU7o (0.048 BTC - Output)
1PVMtEbbR5twrXBPtRtmZEZ7VrzkYA8tbn (0.09 BTC - Output)
1GkpT5sLP4DyQki8ZfBqzLYK2U9pQCbpvr (0.1 BTC - Output)
1JLicegbLWiyyJiDbhQfUFwQKfQPxs4dkD (0.499 BTC - Output)
14fMCHMNV53wkak1jv3dEb9erCWtSRiByx (0.5 BTC - Output)
1PE51qiV8m3KWZuDheBvzcWCQNfzxpenuv (0.01266233 BTC - Output)
1D4o8ECXFckiFkSDxvFi2NcQX7kWpSLUbG (0.16387151 BTC - Output)

Coming back to the example on the previous page, we see that 7 different inputs were spent to pay either 1.4 BTC or 0.01 BTC. Applying the same logic we can see that it would not make sense to combine seven inputs, each between 0.012 and 0.5 BTC just to send 0.01 BTC and

therefore 1.4 BTC has to be the payment and therefore 0.01 BTC is the change.

The multi-input transaction may as well only have one output. Since all bitcoins sitting on the input side were transferred, there is no need for change and therefore we only have one address on the output side.



This is a so-called consolidation transaction, where the purpose is often to empty the wallet — to move all the available funds to another wallet, controlled either by the same or a different entity.

Type 5: Single input and single output transactions

This is a straightforward one. Bitcoins move from one address to the other one. Unfortunately this is not how the majority of transactions look. In order to create such a transaction, one has to send exactly all the bitcoins from one address to another so there is no need to either spend multiple input addresses or to create a change address.

Transaction 281b0e73b30f2bbb4f1859ed432cceb9e1431418794b27247f72ea834da73268 shows how the transfer looks in the real world.

281b0e73b30f2bbb4f1859ed432cceb9e1431418794b27247f72ea834da73268 (Fee: 0.00000691 BTC - Size: 223 bytes) 2016-05-15 20:16:39

16Nj2vwbcidN1miG5qFvY2iUSmeZ1cKTzy (0.01098 BTC - Output) → 1KejHZHms744ua6rcFAfo211c3HS71JhyS - (Spent) 0.01097309 BTC

0.01097309 BTC

Summary		Inputs and Outputs	
Size	223 (bytes)	Total Input	0.01098 BTC
Received Time	2016-05-15 20:16:39	Total Output	0.01097309 BTC
Included In Blocks	412153 (2016-05-17 11:38:29 + 2,362 minutes)	Fees	0.00000691 BTC
Confirmations	5944 Confirmations	Estimated BTC Transacted	0.01097309 BTC
Relayed by IP	46.101.15.184 (whois)	Scripts	Hide scripts & coinbase

The amount B receives is slightly smaller than what A sends as the remainder (0.00000691 BTC) is a fee that will be discussed later on in the chapter. Although many transactions were confirmed for free in the past the fee is required for all recent transactions.

The transaction can be interpreted as a transfer from one bitcoin address to another. Again, we do not know whether these bitcoin addresses belong to two different parties or even two different wallets. In reality, the above transaction was a transfer between addresses sitting within the same wallet but there is no way to figure that out just by looking at the transaction alone.

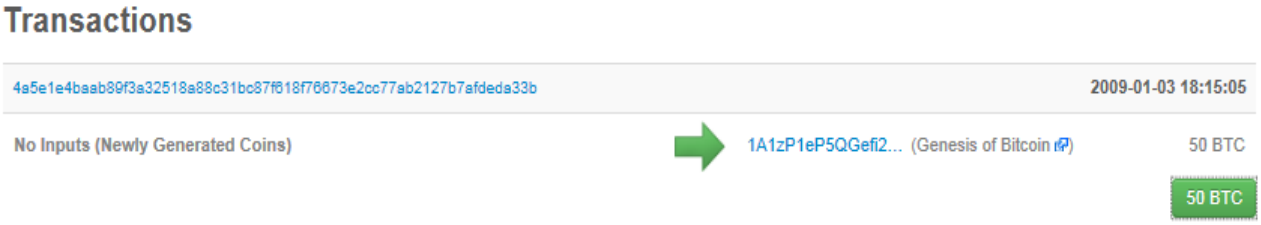
Type 6: 0 input, 1 output — coinbase transaction

There are a relatively small percentage of transactions in the blockchain that have zero inputs and one output. However this small percentage still corresponds to 420 000 transactions as of 9 July 2016, which is the same number as the number of blocks in the blockchain. The equation is not a coincidence; every single block contains exactly one of these transactions.

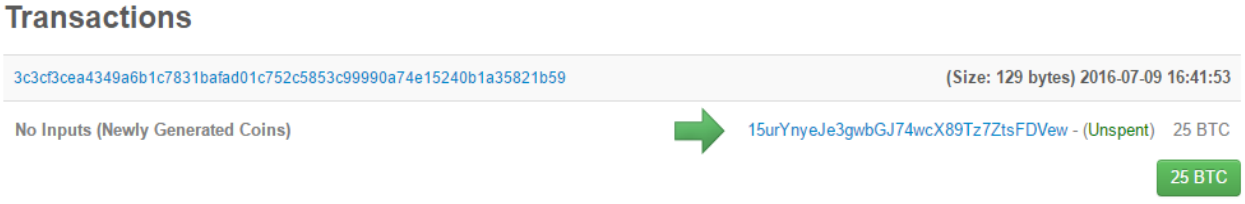
Such a transaction, also called a coinbase transaction, is a reward to the miner. This is always the first transaction of a block and consists of two parts. One is the fixed block reward fee, which used to be 50 BTCs per block but after two halvings it decreased first to 25 bitcoins in November 2012 and then to 12.5 bitcoins in July 2016. The other part is the transaction and it is a sum of the transaction fees collected from all transactions included in the block.

In the future, the fixed reward will decrease and the decrease in income is expected to be compensated for by an increase in the variable income coming from processing an increasing number of transactions and possibly also by the appreciation of bitcoins.

The best example of such a transaction is in the very first block ever mined back in January 2009 by Satoshi Nakamoto: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.



In some blocks, like 419,999, the last block that preceded the latest halving had no other transactions in the block. This means that the miner was able to mine the block in just a few seconds and no other transactions were inserted into the block.

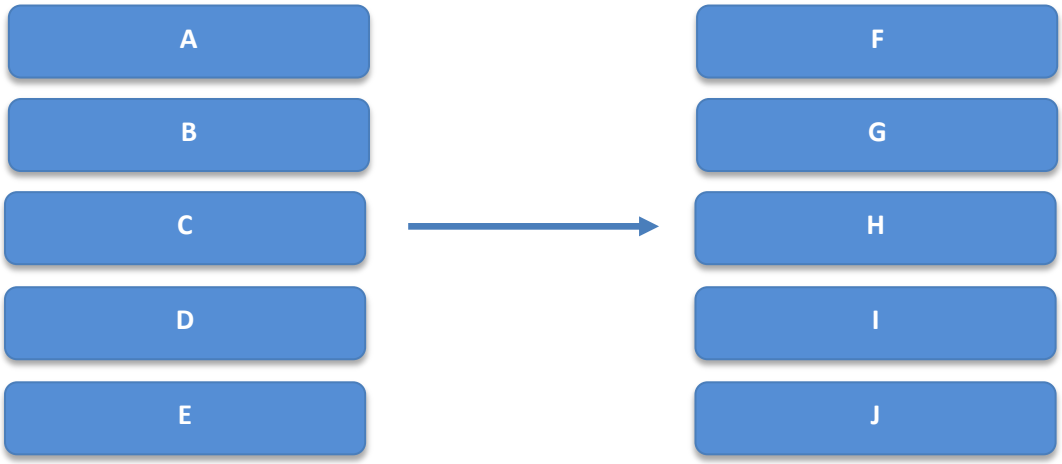


The following block, 420,000, was the first block that had the block reward halved to 12.5 bitcoins. The remaining income of 0.57569681 bitcoins was generated from transaction fees collected from the remaining 1 256 transactions in the block.

The chapter on *Tracing bitcoin transactions using a miner* will explore identification of the miners as well as the possibility to trace transactions that did not travel too far after they were mined.

Type 7: Multiple output transactions

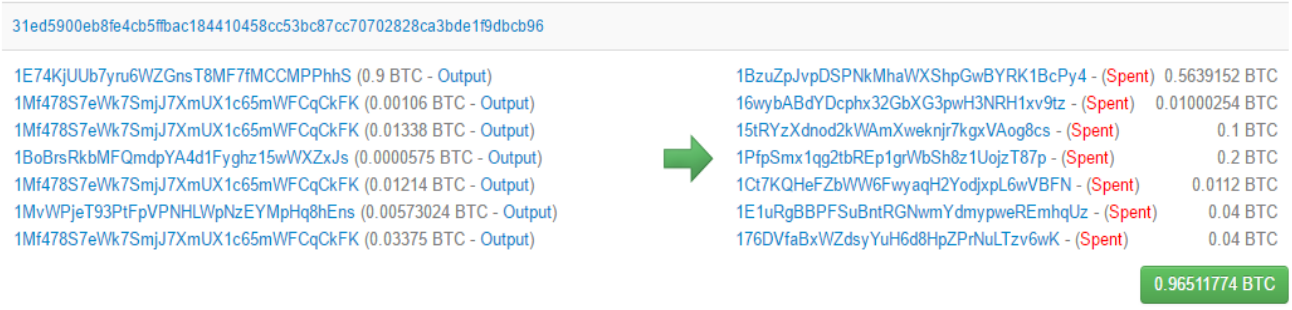
These transactions are typically not carried out by users; instead, they are linked to services processing large amounts of transactions, such as VC exchangers, gaming sites or even marketplaces. A common scenario in such cases is that the inputs collected from multiple users are transferred to those seeking withdrawals.



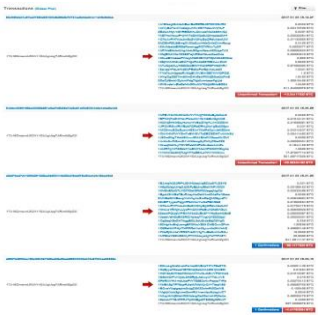
The main reason to perform many of these transactions is to save on transaction fees. As will be discussed in a separate chapter, the transaction fee depends on the size of the transaction in kilobytes. As there is a considerable overhead generated by every single transaction, grouping these together saves space and consequently the costs as well. This makes particular sense for business users who execute large numbers of transactions every day.

A practical example of such transaction that demonstrates a movement of funds from the Bitstamp exchange over to seven addresses, four of which belong to other exchanges:

Transaction 31ed5900eb8fe4cb5ffbac184410458cc53bc87cc70702828ca3bde1f9dbcb96



Nevertheless, one should be a bit more careful when grouping inputs of these transactions as these may be a product of mixing. If that is the case, several different wallets may have signed the inputs in which case it would be an unpleasant mistake to cluster these addresses together. Bitcoin mixing is discussed in greater detail in a separate chapter.



Here is another example of multi-output transactions. The same input address containing a large number of bitcoins keeps sending payment to multiple bitcoin addresses once every few minutes. Note that the input address 17A16QmavnUfCW11DAApiJxp7ArnxN5pGX also features on the output side, so the majority of transactions see greater part of bitcoins coming back to the same addres. Any idea who may be behind these transactions?

Summary		Transactions	
Address	17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	No. Transactions	6496
Hash 160	43849383122ebb8a28268a89700c9f723663b5b8	Total Received	65,601.13861611 BTC
Tools	Taint Analysis - Related Tags - Unspent Outputs	Final Balance	611.34303675 BTC

84ddc42080166be22255b861e5cd7d6b38d12d3e81e92d30344c2e1efca6a4d3 2017-01-03 15:39:56

17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	1NFBVHLK2JXKcGvYvTWq7Xfk3eBytbXcL5	0.0038 BTC
	1BPMXj7e5HrHevPUexNV19r4tbBrrQgM4S	0.01313121 BTC
	1KCWj6H4X5syHz4xnYnBoZMqYLVrK2QDim	0.01688581 BTC
	1JPCNR5wJRWEyb7GReDRrLjXo1gSe228pw	0.021 BTC
	1NiG9muSCaSuowH58AnTNoPzGswJdK82xm	0.04214327 BTC
	1CU1iHMFWYZm7nBK16VTx5BGSDHTwM4h3U	0.08411462 BTC
	1J32m5NpTHxU6XvwJ5MAS4dYX3cxzXLiQW	0.0999 BTC
	1ArHn5wFtZmvD1VKHbmg9yFhYyF5ra2Z8	0.09990001 BTC
	1HnszjftUkLy7QY8FzbKNPU3rJbok4JACL	0.1644139 BTC
	1At4R7q14T25UaY1eShtYMaWPGQKY9kg4o	1.8399 BTC
	111khWGs3Mj7UgKT7aS6hLsYK11ii4Gmw	17.87807712 BTC
	17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	621.68717308 BTC

Unconfirmed Transaction! -20.26394162 BTC

e8d37bed7d4139fb38f1206ec0b8f2414b052c4f3ab578e50cc4efb150aef3e8 2017-01-03 15:34:58

17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	1BAmqih33JRP4J5XHUcojVqB2Aa9TLD3Y5	0.001 BTC
	1H6y6UzjyUHp2JjZ3FyEjUnyEfcWhPVDCX	0.00186432 BTC
	1KH6irB3kQ7LYDfTDbii9RtP9XoqejNqCU	0.00332466 BTC
	1EpzU3K4Ec7EuRAayNxQoMAmDAdFz15boc	0.0053 BTC
	3MVEeQiWEaupYrAWqALSmRetjjM28qvcPV	0.00648694 BTC
	38nBP1ypsxFcjg4ffPbitVknYuGcRShf3b5	0.01609334 BTC
	1C7bJwPH7hJsJtnSsZW2KySqGRdvAbxtUW	0.01700175 BTC
	1Khzvz1RMjjKJJyaPmGM4RsBwX2fo6W9Uv	0.03628505 BTC
	33esktFQUqWPSWM4qGLEkS7YHip8omCSxE	0.05003967 BTC
	12eobVdH9xBK3RiCYptzqT7AgXjY3D29gU	0.08000001 BTC
	1Gq5oqX8zDh7ikqgEQL3xU5rJsSbjC8YqQ	0.235 BTC
	162HpHwBnjLemqEF2fNuXS51GHSGwvZPnh	1.29836 BTC
	1C5RaNtYFHjJTKPPRoYm43yuvrKx9M1kNZ	3.39652148 BTC
	1FKzRjGvHeYPR3FvbZ1YfgTvrEb5wWLRGu	19.9999 BTC
	1MFErcY5ZMZ5WyF7WMkuyc4gTsT7Pri8Tr	29.9999 BTC
	17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	641.9511147 BTC

1 Confirmations -55.1477529 BTC

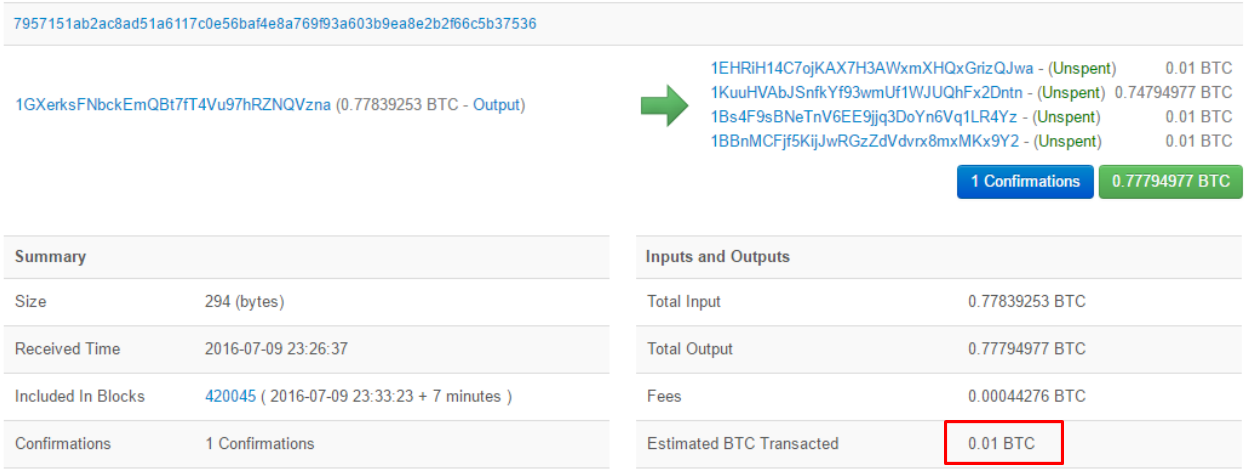
In this particular case, it is Poloniex, one of the exchanges and the largest exchange where one can convert bitcoins to dozens of altcoins. For a busy exchange like Poloniex it makes sense to “bundle” individual transactions into one and save on transaction fees.

POLONIEX

While the above type of transaction is common for companies it is not exclusively limited to them. Users can either use scripts to the same effect or even use several GUI wallets including Bitcoin Core that allow a payment to be sent to multiple addresses as part of one transaction. This is possible simply through '*Add Recipient*', after which the payer selects the address of the recipient, label and amount.

Essentially, there is no limit on the number of outputs and there are many transactions with hundreds of outputs.

This is an example of a user transaction where a payment of 0.01 BTC was sent to three different addresses and 0.7479 BTC was returned as change.



Note that in this particular case blockchain.info did not get the estimated BTC transacted correctly as it only picked up one out of three 0.01 transfers.

Treatment of input addresses

So far we have looked mainly at the output side. However, there is also a bit of science ehind selecting the input. Inputs will be chosen from the addresses that have received bitcoins in the past. If the payer only received payment to a single address and has not spent it yet, then this will be the input address. However, what happens if there are multiple addresses with non-zero balances? Which ones will be used for the transaction?

Treatment of the input address depends very much on the type of wallet used. All wallets have built-in functions that determine how inputs will be dealt with. This commonly starts by checking whether the payer actually has enough funds for the transaction.

```
// Choose coins to use
set<pair<const CWalletTx*,unsigned int> > setCoins;
CAmount nValueIn = 0;
if (!SelectCoins(vAvailableCoins, nValueToSelect, setCoins, nValueIn, coinControl))
{
    strFailReason = _("Insufficient funds");
    return false;
```

Every implementation of a bitcoin client can have a different approach to inputs. The following example explains the input behaviour of the Bitcoin Core wallet.

There are five input addresses available with a total balance of approximately 1.13 bitcoins. If we wanted to spend all bitcoins in a single transaction, we would pay this amount and all five addresses would be spent in the transaction.

What would happen if we wanted to spend 0.005 bitcoins? Three addresses out of five have a high enough balance to cover the payment on their own so which one will be selected? Human behaviour would dictate going for the lowest possible amount that satisfies the need, which in our case is 0.01069209 bitcoins.

	Amount	Received with label	Received with address	Date	Confirmations	Priority
☐	0.78757477	(no label)	1GuWTK3zNCwkKxeTKX4EGYE7aeUELJmDPr	03/06/2016 08:04	3589	medium
☐	0.33137490	(change)	1EHRiH14C7ojKAX7H3AWxmXHQxGrizQJwa	27/06/2016 00:02	0	lower
☐	0.01069209	(change)	1Bs4F9sBNeTnV6EE9jjq3DoYn6Vq1LR4Yz	25/06/2016 18:20	0	lowest
☐	0.00024395	(change)	1BBnMCFjf5KijJwRGzZdVdvrx8mxMKx9Y2	15/05/2016 22:34	5614	low
☐	0.00000976	(no label)	1P4uCb1h6wnH9W197cpfxK1aCytAsd8zhr	20/03/2016 15:28	14601	lower

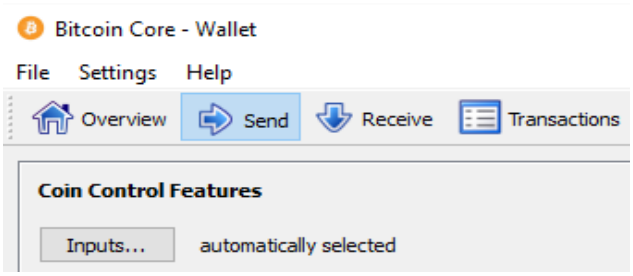
However, this is not the way most bitcoin wallets behave. The key factor in determining which input will be used is the '*Priority*' column. Generally, wallets also tend to minimise the number of inputs and change — like people would do. However, the priority is given to the input that has a high number of confirmations.

Hence based on priority 1GuWTK3zNCwkKxeTKX4EGYE7aeUELJmDPr was chosen as an input.

After the payment the prioritisation of the input readjusts. The amount sitting on 1GuWTK3zNCwkKxeTKX4EGYE7aeUELJmDPr was fully spent and was therefore replaced by a newly created bitcoin address 1BnKkNgNXuEEsCaEnZjSmVKnooYgwA37H5 and its priority has been set as lower.

	Amount	Received with label	Received with address	Date	Confirmations	Priority
☐	0.78245048	(change)	1BnKkNgNXuEEsCaEnZjSmVKnooYgwA37H5	27/06/2016 07:06	1	lower
☐	0.33137490	(change)	1EHRiH14C7ojKAX7H3AWxmXHQxGrizQJwa	27/06/2016 00:02	0	lower
☐	0.01069209	(change)	1Bs4F9sBNeTnV6EE9jjq3DoYn6Vq1LR4Yz	25/06/2016 18:20	0	lowest
☐	0.00024395	(change)	1BBnMCFjf5KijJwRGzZdVdvrx8mxMKx9Y2	15/05/2016 22:34	5622	lower
☐	0.00000976	(no label)	1P4uCb1h6wnH9W197cpfxK1aCytAsd8zhr	20/03/2016 15:28	14609	lowest

If possible, Bitcoin Core tries to use only coins with at least one confirmation before it moves to other inputs. However, if there are only unconfirmed inputs to choose from or the user manually selects an input that is unconfirmed the transaction will still go through. This may come as a surprise to many — a user may opt to spend an input received in a transaction that is not yet confirmed and therefore not part of a block in the blockchain.



The previous paragraph mentioned a possibility of manual input selection. The user can choose an input by accessing *Send -> Inputs…* in Bitcoin Core. Note that many other wallets offer such a feature.

Understanding the selection of inputs is important for the investigator as it provides a justification for why certain input or inputs were chosen for a transaction. This has a practical impact on the investigation, particularly if it comes to multi-input transactions (see transaction type 3).

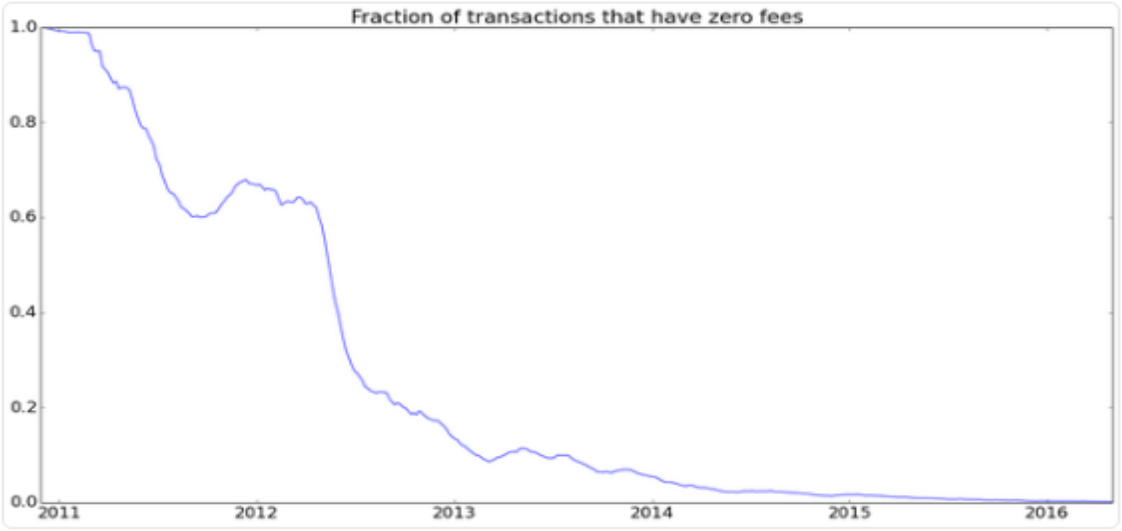
Transaction fees

Bitcoin transactions are not free of charge. There is a good reason for that. If the transactions were free, anyone could create a loop script sending the same bitcoins back and forth or split a small amount of bitcoins, such as one BTC, in order to create 100 000 transactions of 0.00001 BTC, effectively filling the blocks, causing bloating of the blockchain and clogging the network through intentional or unintentional denial of service attack. The transaction fee to a large degree prevents such malicious behaviour.

In the past, some claimed that bitcoin will support free payments. While this was theoretically true, payers gladly opted to pay a very small fee, often a fraction of a cent, to make sure their transaction is either prioritised or at least not refused by the miner. This fee has recently increased to a few dozens of cents mainly due to two reasons:

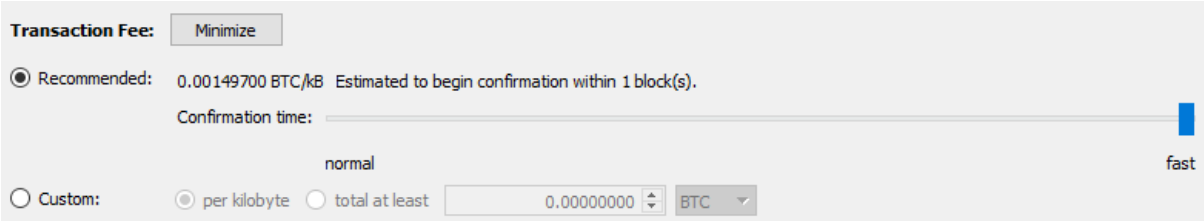
1. Bitcoin has substantially increased in price and therefore the same fraction of a bitcoin is worth much more than years ago.
2. Due to scalability issues, the number of transactions is often higher than can be accommodated by the fixed limited size of one block. It is up to the miner to decide which transaction to prioritise. Not surprisingly, a price that is paid by the transaction is the most important criterion for many miners.

The proportion of the transactions that were sent using a zero fee is shown below, where 1.0 = 100 %. The chart was produced Blockspy (a non-public tool).



Most wallets allow users to decide the size of the fee they want to pay for the transaction. The fees per transaction may differ considerably. The following figure shows a payer setting a 0.00005022 BTC/Kb fee that corresponds to €0.03. However, being a penny-pincher has a drawback, which is the long time it takes to confirm the transaction. As the following test conducted on 25 June 2016 demonstrates, the expected waiting time for the first confirmation would reach 24 blocks, which is about 4 hours.

However, the price could reach 0.001497 BTC/Kb or a whopping €0.92 as of 25 June 2016. This would be acceptable for most transfers but it is prohibitively expensive for micro transactions.

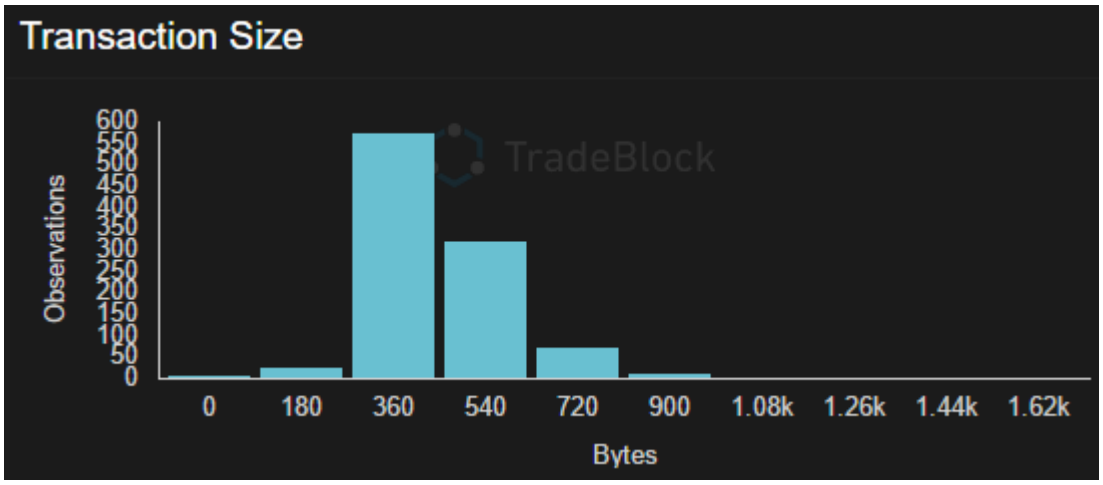


The size of the fee could be very relevant to the investigator. When seizing virtual currencies, one has to add a sufficient fee to the transaction to make sure:

1. the transaction goes through; and
2. the transaction goes through as quickly as possible so that no other owner of the private key can spend bitcoins from another device.

Generally, a transaction fee of around 0.001/Kb is suitable for smaller seizures whereas a slightly higher fee is recommended for transactions of over 100 BTCs.

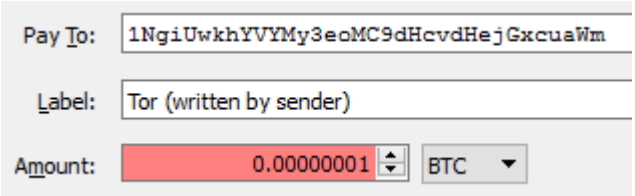
The confirmation time is not an exact science. The estimated time to begin confirmation indicated by the wallet is what it says it is — an estimate. Another thing to keep in mind is that the above estimate of the fee was based on 1 kb. The overwhelming majority of transactions, particularly those that have a small number of inputs and outputs, are smaller than 1 kb and normal transactions typically range between 200 to 500 bytes, as can be demonstrated on the following chart.



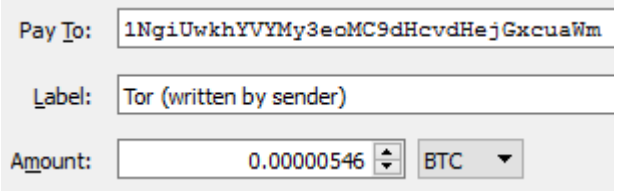
Source: Tradeblock

Many bitcoin sources say that it is possible to send as little as 1 satoshi or 0.00000001 bitcoins, which is the smallest amount of bitcoins that can theoretically sit on one bitcoin address. This is however not possible in the majority of GUI wallets as the software prohibits tiny transfers.

Let's demonstrate this by sending as small an amount of bitcoins as possible using the lowest possible fee. We will try to send a tiny donation to privacy/anonymity service Tor, using Tor's donation address (1NgiUwkhYVYMy3eoMC9dHcvdHejGxcuaWm).



Bitcoin Core wallet, for example, sets the minimum amount that can be sent as 546 satoshi.

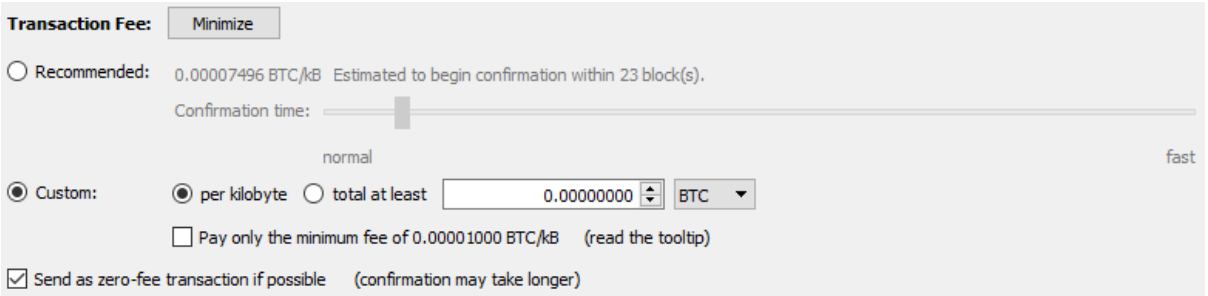


The amount is defined in the bitcoin source code along with the explanation of how developers came up with such a random-looking number:

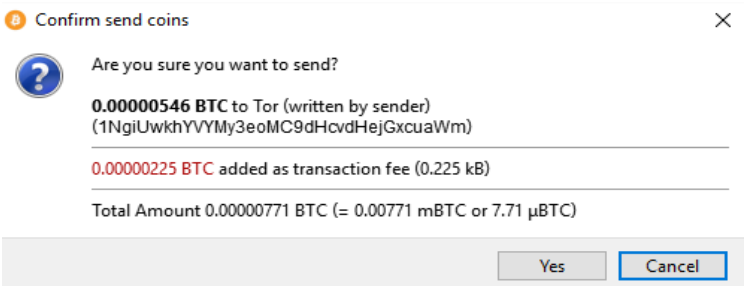
```
// "Dust" is defined in terms of CTransaction::minRelayTxFee,
// which has units satoshis-per-kilobyte.
// If you'd pay more than 1/3 in fees
// to spend something, then we consider it dust.
// A typical txout is 34 bytes big, and will
// need a CTxIn of at least 148 bytes to spend:
// so dust is a txout less than 546 satoshis
// with default minRelayTxFee.
size_t nSize = GetSerializeSize(SER_DISK,0)+148u;
return (nValue < 3*minRelayTxFee.GetFee(nSize));
```

Most miners would however have even stricter criteria and would automatically ignore anything below 5 460 satoshi.

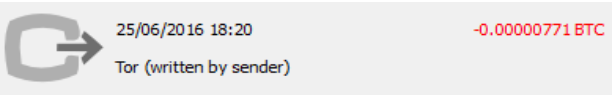
The following settings ensure that the smallest possible fee is paid, but this is very likely not going to be enough for the miner to confirm the transaction.



As of 25 June 2016 the minimum transaction fee allowed to be sent by a Bitcoin Core wallet is 225 satoshi (or 0.00000225 BTC), which corresponds to about €0.003.

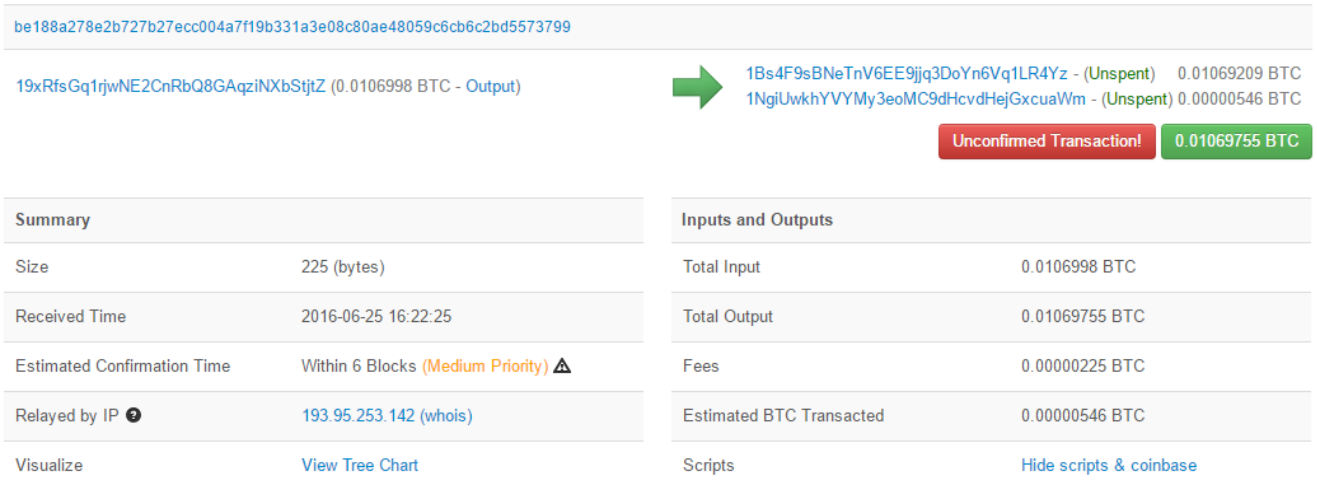


After the transaction has been confirmed by the user, it appears on the list of recent transactions.



The bitcoins were subtracted from the wallet (or more correctly one or more addresses in the wallets were fully spent) and the bitcoins will be hanging around in limbo until they are confirmed by the miner. This means that the recipient will not be able to spend bitcoins until the transaction is confirmed.

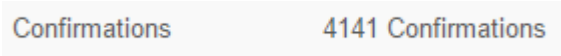
The transaction was picked up by one of the nodes owned by blockchain.info but it has still not been appended to the blockchain. How do we know that? A hard-to-overlook red label saying '*Unconfirmed Transaction!*' tells us that while the transaction was successfully propagated by the network it still has not been picked up by a miner and appended into a block so it could not yet become part of the blockchain.



In our particular case, the estimated confirmation time of up to six blocks that is shown below the transaction turned out to be completely off. While the estimating algorithm of Bitcoin Core is reasonably precise, the estimate provided by blockchain.info cannot be trusted, especially when it comes to low fee transactions.

Once the 

label disappears the transaction will be recorded on the blockchain and confirmed, and the estimated confirmation time will be replaced by the number of confirmations, for example.:



Even with a single confirmation, the risk of any change is very small and every subsequent confirmation makes the risk only a theoretical possibility.

However, our transaction sent to Tor was — as one could expect — never added into the blockchain. No miner decided to put it into a block because of the extremely small transaction amount and almost non-existent transaction fee. After hanging around for a few days in limbo (more technically in mempool or memory pool), the transaction was dropped.

When the transaction is in the memory pool it appears to the payer that it has left the wallet but it is not a part of the permanent blockchain yet. The memory pool by default keeps the unconfirmed transaction for 72 hours before it is dropped. If the volume of unconfirmed transactions temporarily increases to over 300 Mb the transactions may be dropped even sooner.

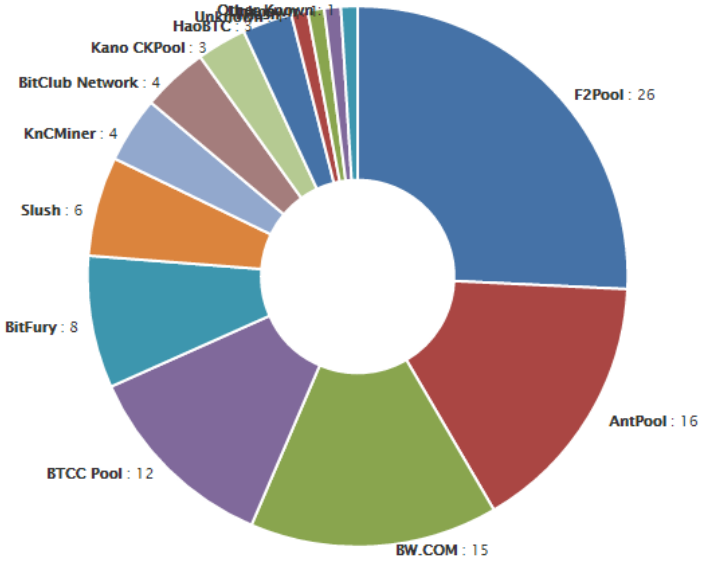
In such cases, the payers have to rebuild their transaction history[27] to get the sent bitcoins back. By rebuilding the transaction history, the payers would see their bitcoins back in their wallet and would be able to spend them again.

[27] The transaction history can be rebuilt by starting the bitcoin client from the command line using –reindex parameter — *bitcoin-qt.exe —reindex*. Another option would be using *zapwallettxes* to remove all transactions that are not part of the blockchain from the wallet, e.g. *bitcoin-qt.exe -zapwallettxes=1*

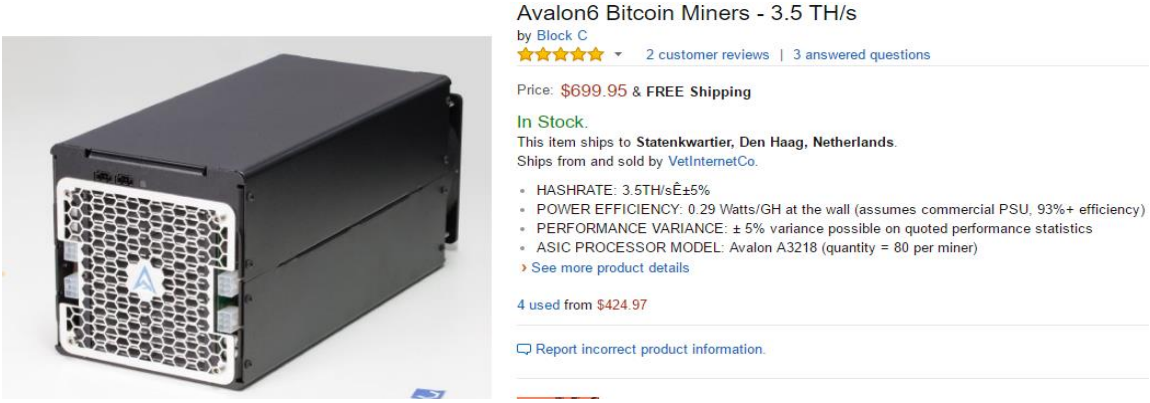
Tracing bitcoin transactions using miners

Some members of the bitcoin community consider mining to be the most anonymous way to get bitcoins. It is possible to see certain logic behind this thinking, as the newly minted bitcoins have no transaction history.

As discussed in the chapter dedicated to mining, gone are the days when bitcoins were mined on personal computer CPUs and GPUs. Increased difficulty resulted in a relatively low number of parties that are realistically capable of mining bitcoins. Instead of dozens of thousands of individuals, the bitcoins are mined by professionals, even if they are companies owning warehouses packed with racks with ASICs or mining pools. For almost every block, we can identify the miner. All of the larger miners are known entities and many websites offer a list of miners that recently managed to mine the most blocks.



Even though bitcoin mining is no longer profitable for individuals it is relatively easy to purchase a 'domestic' bitcoin ASIC. While the combined cost of the device and electricity will not make bitcoin mining a lucrative opportunity, it may provide a small continuous income in bitcoins until it becomes obsolete in a few months' time.



Individuals who decide to buy an ASIC miner tend to participate in bitcoin mining pools. These are businesses that aggregate the processing power of dozens, hundreds or even thousands of miners. The advantage for miners of joining one of the larger pools is that they do not have to wait for ages hoping that one day they may win a block — instead they get paid a smaller amount but with much higher frequency — every time anyone in the mining pool finds a block. This makes an income much less volatile and more predictable. The amount of bitcoins each miner earns corresponds to the computing power the miner contributed to the pool.

Since pool participants receive their part of the block reward from the pool, which can be identified, and which may cooperate with LE, this is hardly a completely anonymous method of acquiring bitcoins. Yet, since the miners are generally not classified as money service businesses (MSBs), they do not have to comply with the same stringent KYC as virtual currency exchangers. For this reason the information received from the pools may not always uniquely identify the suspect.

For majority of transactions it is relatively straightforward to identify the miner. As previously discussed, blockchain.info allows owners of bitcoin addresses to tag them and some of the miners do indeed do so.

Block #300000

Summary	
Number Of Transactions	237
Output Total	2,080.05436605 BTC
Estimated Transaction Volume	804.26061613 BTC
Transaction Fees	0.0402836 BTC
Height	300000 (Main Chain)
Timestamp	2014-05-10 06:32:34
Difficulty	8,000,872,135.97
Bits	419465580
Size	128.81 KB
Version	2
Nonce	222771801
Block Reward	25 BTC

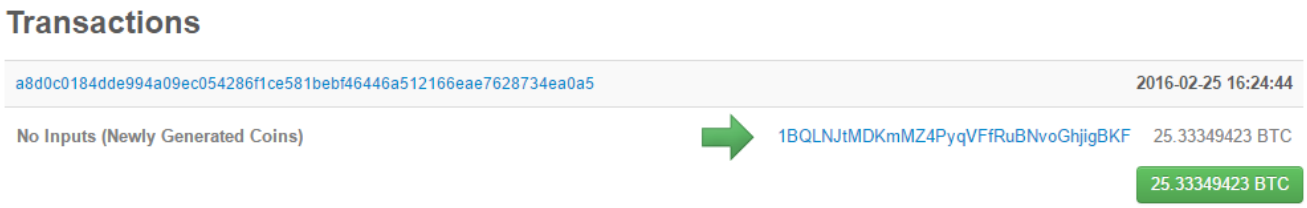
Transactions

b39fa6c39b99683ac8f456721b270786c627ecb2467008883159918770 24b983 2014-05-10 06:32:34

No Inputs (Newly Generated Coins) → 1CjPR7Z5ZSyWk6... (ghash.io) 25.0402836 BTC

25.0402836 BTC

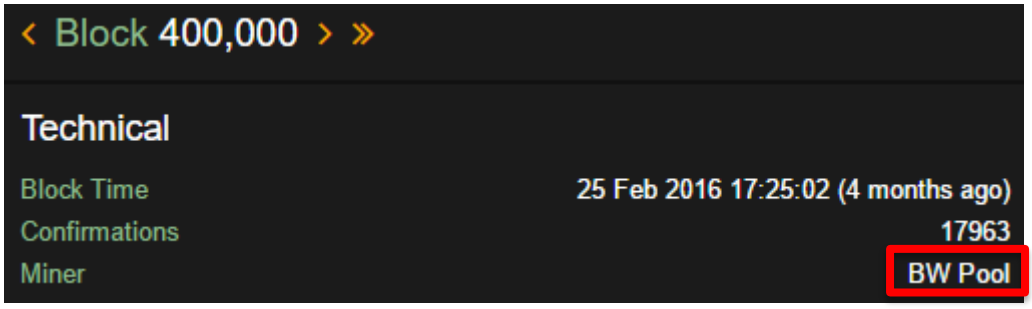
We can see that block 300 000 was mined by Ghash.io, as indicated by the address tag in the first transaction. Unfortunately for the investigators, not all entities feel the urge to label their addresses, and so many blocks on blockchain.info do not provide the name of the miner — as can be seen on block 400 000.



In this particular case blockchain.info does not list the name of the miner for historical blocks, which is rather disappointing since it stores the information, as can be seen on its home site showing the miners that mined and propagated the last six blocks.

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
417960	18 minutes	1033	5,282.95 BTC	F2Pool	544.18
417959	25 minutes	102	248.67 BTC	Slush	41.65
417958	26 minutes	286	1,914.45 BTC	BW.COM	107.98
417957	28 minutes	1143	5,623.81 BTC	BTCC Pool	979.42
417956	36 minutes	541	3,008.36 BTC	BW.COM	180.37
417955	40 minutes	1707	8,418.20 BTC	AntPool	958.91

Luckily there is no need to approach blockckain.info in order to find out the identity of the miner as the information can be found on other websites. A good source in this case is TradeBlock, which provides the name of the miner for all historical blocks; all it takes to find it is to type the number of the block into TradeBlock explorer.



This helps us to verify the miner that may provide information about the member of the pool, which may happen to be subject to an investigation. Alternatively, the miner may provide information on someone it sent bitcoins to, etc.:

Pool Admin -> Individual Miner identified by Admin -> Criminal Transaction

Pool Admin -> Individual Miner identified by Admin -> Recipient of a payment from the individual miner -> Criminal transaction

Therefore, if a miner transfers bitcoins to someone who becomes subject of an LE enquiry, the miner can be questioned regarding the nature of the transactions he or she made and may help to identify the receiver of the payment.

Naturally, the tracking through the miner is only efficient if the criminal transaction occurs a small number of hops away from the miner.

Bitcoin mixers

Coinjoin mixers

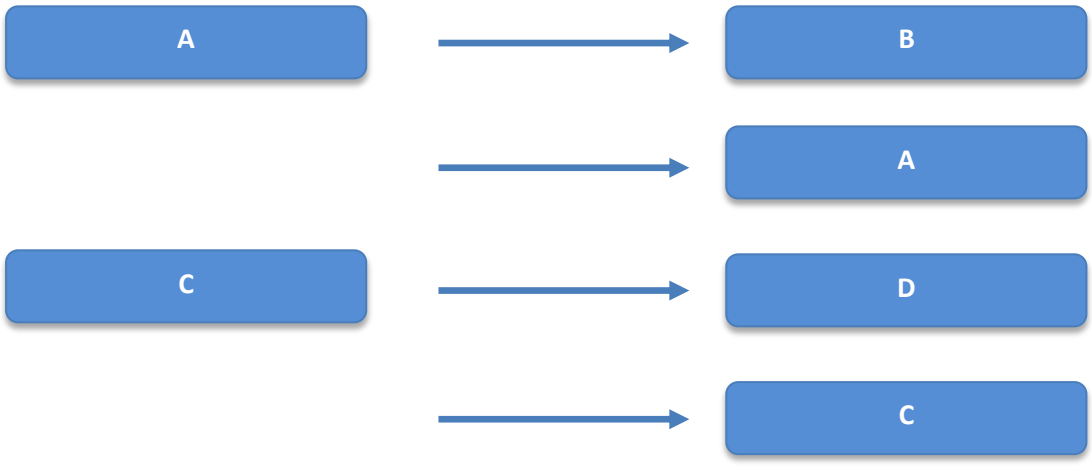
Coinjoin (sometimes also Coin Join) is one of the most popular anonymisation methods, where multiple parties agree to create a bitcoin transaction. Each party provides one or more signatures — one signature per each input. The inputs within a transaction are completely independent of each other. This means that bitcoin users agree separately on an input to spend, and a set of outputs to receive. Then they separately sign the transaction and later merge their signatures.

The process is best demonstrated through a diagram comparing two persons who send a 'normal' payment with a Coinjoin transaction.

Normal transaction 1: Person A sends a payment to Person B and gets change back.

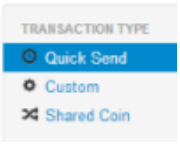
Normal transaction 2: Person C sends a payment to Person D.

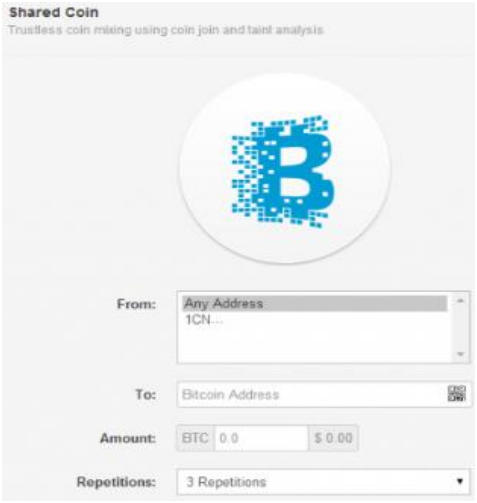
Coinjoin transaction: Two normal transactions get mixed together. This makes it difficult to follow the transaction and creates a challenge for bitcoin-tracing tools that may erroneously cluster the input addresses belonging to different wallets together.



In the above case there are four different possible outputs for each input. The order of the inputs and outputs is mixed and establishing the correct link becomes a guessing game. This is further complicated because Coinjoin is not limited to two wallets or two participants. There can be several participants involved in the transaction, all mixing the coins at the same time.

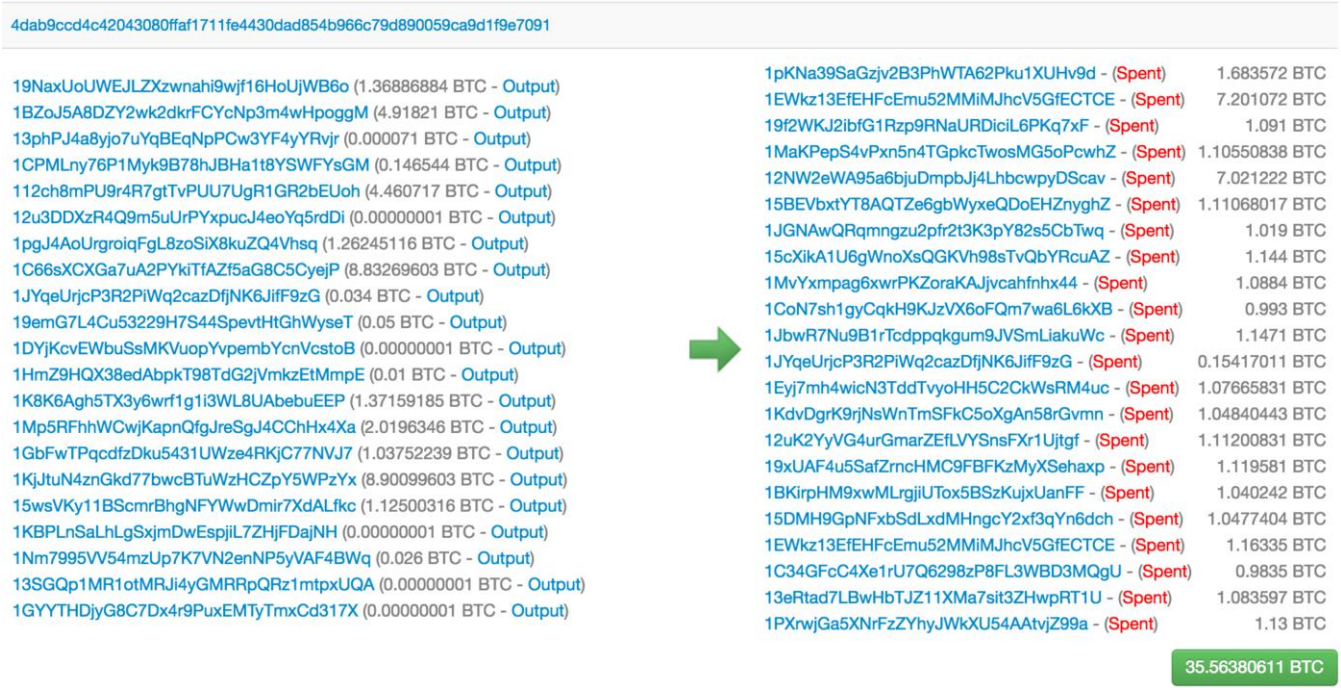
By far the most popular implementation of Coinjoin is called Sharedcoin and it is bundled into the online wallet blockchain.info. This is a highly convenient implementation of Coinjoin that does not require users to bother with a command line and this convenience factor had made Sharedcoin notorious and widely used. When a user of a blockchain.info wallet seeks to send the Sharedcoin transaction, he or she has to explicitly select it as it is off by default. No advanced skills are required to perform the mixing — the users of blockchain.info simply send a payment using Sharedcoin.





Sharedcoin may also be indicated by the amount of the transaction fee. The Sharedcoin wiki indicates that while the service is free of charge, the transaction still requires a network fee of 0.0005 BTC. By observing dozens of Sharedcoin transactions we noticed that the transaction fee typically ranged from 0.0003 to 0.0008 BTC per transaction. Interesting enough, all transaction fees had a 0.000x format with exactly four decimal places as can be seen looking at an example of a typical Sharedcoin transaction.

Transaction 4dab9ccd4c42043080ffaf1711fe4430dad854b966c79d890059ca9d1f9e7091



Summary	
Size	4219 (bytes)
Received Time	2014-10-05 05:28:51
Included In Blocks	323902 (2014-10-05 05:30:53 + 2 minutes)
Confirmations	92871 Confirmations
Relayed by IP	Blockchain.info

Inputs and Outputs	
Total Input	35.56430611 BTC
Total Output	35.56380611 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.9835 BTC
Scripts	Hide scripts & coinbase

While the fee certainly cannot be the primary identifier of a Shared Coin transaction, it might be taken into consideration. There is, however, an even better indicator of a Shared Coin presence. Since this service is provided exclusively by Blockchain.info, we can check for this nametag in the 'Relayed by IP' field that is otherwise of little use for the majority of transactions.

Sharedcoin poses a serious threat for bitcoin investigators not only due to obfuscation of transactions but also due to immense popularity of the mixing service. As of 25 June 2016, Sharedcoin was the entity with the largest number of addresses and the largest number of transactions in the blockchain[28]:

MY GRAPHS NAMED CLUSTERS TOP CLUSTERS

Cluster	TX	Addr.	Bal.
SharedCoin etc.	12460000	10407609	3503
GoCoin.com	1980000	1962759	1
Coinbase.com	5710000	1762412	17785
LocalBitcoins.com	1810000	1045035	20
BTC-e.com	2930000	527688	215
BitPay.com	2140000	500303	4
Agora Market	1170000	498001	119
MtGox.com	1060000	492740	1
38SmEHTCWWwFX5XwStBiQ1gpL12MQzCgBn	495000	490803	0
14DEe98jRB65VTxKTcpJ13xWGVZ8iigohD	482000	475985	0
Evolution Market	461000	420632	58
999Dice.com	707000	405075	6

[28] Screenshot taken from Chainalysis in November 2016

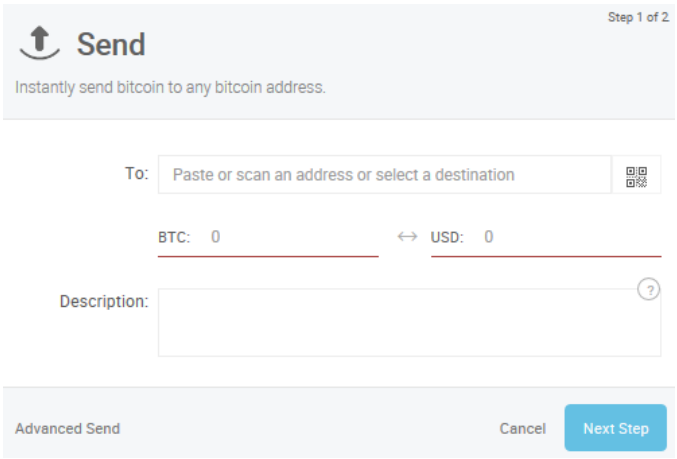
Sharedcoin is a label linked to over 12.5 million transactions and 10 million addresses[29]:

MY GRAPHS | NAMED CLUSTERS | TOP CLUSTERS

Cluster	TX	Addr.	Bal.
SatoshiDice.com	12590000	31291	31
SharedCoin etc.	12460000	10407609	3503
Coinbase.com	5710000	1762412	17785
Discus Fish (F2Pool)	3730000	32647	3843
BTC-e.com	2930000	527688	215
Huobi.com	2720000	103505	507
LuckyB.it	2520000	7	70
Xapo.com	2320000	304628	6926
BitPay.com	2140000	500303	4
MMMGlobal.org	2000000	118979	113
GoCoin.com	1980000	1962759	1
Coins.co.th	1900000	245360	79

Here comes the logical question — what to do about Sharedcoin transactions? It is easier to suggest what not to do: do not cluster the addresses on the input side of the transaction together. Doing so would lead to false positives, i.e. mistakenly grouping several bitcoin addresses that are sitting in different wallets into a single wallet.

A good news for investigators is that the service was temporarily disabled on 10 May 2016 and as of 1 November the Sharedcoin was still disabled. It is up to a court hearing that will decide whether the feature will be enabled for future transactions.



As of the end of October 2016, Blockchain.info has been testing a new type of wallet that does not offer any mixing functionality.

[29] Screenshot taken from Chainalysis in November 2016

Non-coinjoin-based mixers

While Sharedcoin used to be a very popular service, there are other mixing solutions out there and there are plenty of them. Yet none of them is as convenient as Sharedcoin built into blockchain.info. Several other solutions were trying to achieve anonymity through the built-in wallet mixing; these included Darkwallet, which is now discontinued, and a number of services such as TorWallet that has been operated by a known scammer.

The majority of mixers nowadays have chosen a different way of implementation. Instead of mixing provided by a wallet, the transactions are mixed after they leave the wallet. These services usually require the user to:

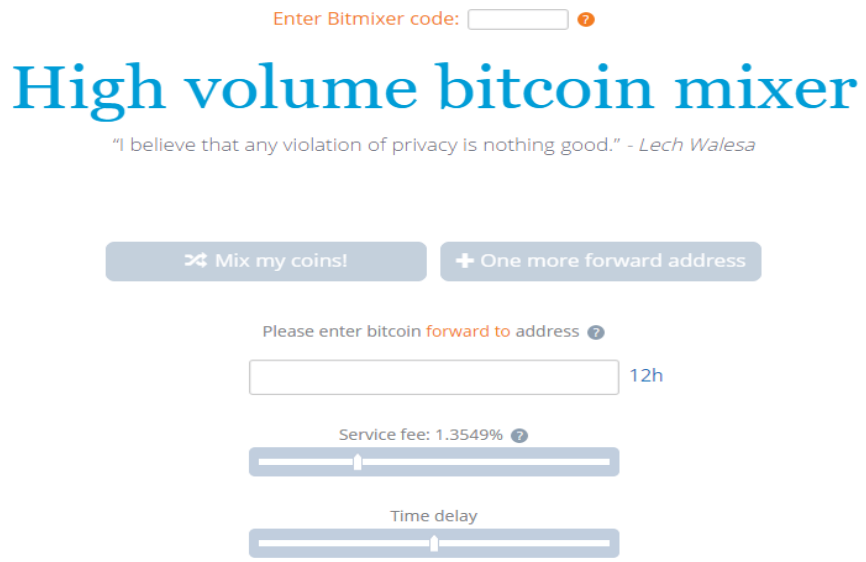
1. send a bitcoin transfer to a bitcoin address controlled by the mixer;
2. specify a destination address, where the 'laundered' bitcoins are supposed to be delivered.

After the funds are received by the mixer, the mixing can be performed using two different approaches:

1. it mixes the bitcoins with bitcoins provided by other participants, creating a large number of transactions, adding as much obfuscation as possible to frustrate the investigator;
2. instead of mixing the coins, bitcoins are sent to a requested destination address from a completely different wallet than the one that received the suspect's tainted bitcoins. This essentially makes any attempts to follow the money useless as there will not be any link between the user's original and destination bitcoin address. This mixing will be demonstrated on the next page.

The mixers can be found in the darknet as well as the open web. Generally, both quality of mixers and the amount of laundered bitcoins seem to be higher in the darknet.

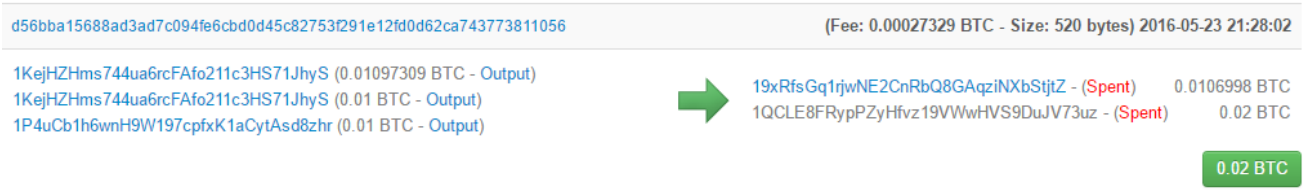
The number of mixers in the open web is limited. Probably the best functioning and most trust evoking mixer/tumbler/laundry at the moment is bitmixer.io, which allows ample amounts of bitcoins to be laundered in one go, suggests a dynamic service fee by default and permits the setting of a time delay between transfer to the mixer and the bitcoins being sent to the destination address.



Additionally, users can specify a code given to them during the previous transaction to make sure that their individual transactions do not get mashed together. The minimum fee for this mixer is relatively reasonable — 0.5 % plus an additional 0.0005 BTC per forwarding address.

The following transactions show the behaviour of the bitmixer on the blockchain.

1. The user decides to launder 0.02 BTC. He sends this amount to the bitcoin address provided generated by the mixer for the transaction — *1QCLE8FrypPZyHfvz19VWwHVS9DuJV73uz*.

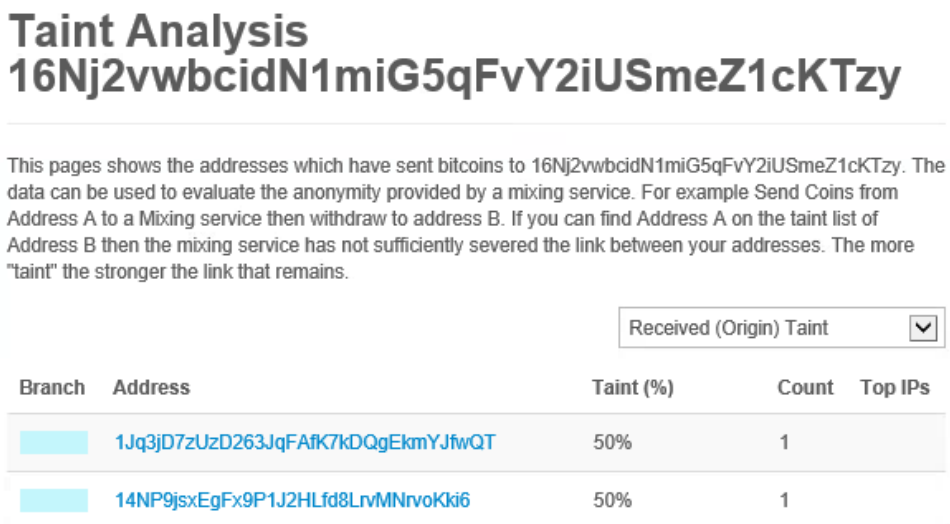


2. The destination address to which the laundered bitcoin should be sent was 15x7WuTcHwhkoHbkF5JncwnNNteEjgAgg6.

The transfer to the destination address came from 1Ba4dqgfKZV16f3LG9mPEeQkbeTJGxMFoL. This address has absolutely no link to the user's original bitcoin addresses, so the bitcoins were successfully and properly laundered.

Note that with no delay set, the transaction was propagated 15 minutes later and 0.0194 BTC was transferred to the destination address, leaving 0.0006 BTC as an expected reward for the mixer. Indeed, looking at the time and amount of the laundered bitcoins may be the best way to track the transaction. Nevertheless, if a user decides to set a delay and a higher random fee, the probability of successfully tracing the transaction would be very low.

Users can easily check whether their funds were laundered correctly. Ideally, there would be a very low taint (strength of link) between the original and destination bitcoin address. One such publicly available tool that allows checking of the taint is blockchain.info/taint/ followed by one of the two bitcoin addresses, for example:
https://blockchain.info/taint/16Nj2vwbcidN1miG5qFvY2iUSmeZ1cKTzy:



Taint Analysis
16Nj2vwbcidN1miG5qFvY2iUSmeZ1cKTzy

This pages shows the addresses which have sent bitcoins to 16Nj2vwbcidN1miG5qFvY2iUSmeZ1cKTzy. The data can be used to evaluate the anonymity provided by a mixing service. For example Send Coins from Address A to a Mixing service then withdraw to address B. If you can find Address A on the taint list of Address B then the mixing service has not sufficiently severed the link between your addresses. The more "taint" the stronger the link that remains.

Received (Origin) Taint

Branch	Address	Taint (%)	Count	Top IPs
	1Jq3jD7zUzD263JqFAfK7kDQgEkmYJfwQT	50%	1	
	14NP9jsxEgFx9P1J2HLfd8LrvMNrvoKki6	50%	1	

There are several popular mixers in the darknet including Helix, Grams or Bitcoin Blender that generally take 2-3 % commission for the mixing. It is very important for these mixers to keep a high level of trust in the community as the users are paranoid and they have very good reason to be, as the mixers are centralised entities that could decide to steal from their users whenever they intend to do so.

Relatively high commissions for laundering and possible exit scams made some of the bigger marketplaces such as Alphabay develop their own low-cost high-security Coin Tumbler as an additional service for their users.

Deobfuscating bitcoin mixing

Essentially, there are two ways to deal with bitcoin mixers.

1. Technical approach

The technical approach usually follows the ‘what goes in must go out logic’. Therefore, if there is a bitcoin address with 100 BTCs to be laundered, we can hope that the laundered proceeds minus the commission, for example 98.5 BTCs to the mixer, will appear on a ‘clean’, laundered address a few minutes later.

As mentioned, mixers may fight this logical approach by adopting a randomised fee, time delay between receiving the bitcoins from a dirty address and passing it to a clean address or splitting the

input into several output addresses. All these measures seem threatening to the investigator but they are often not properly utilised by the offenders.

EC3 had a short discussion with the owner of the mixer, who claimed that in 90 % of cases, the users use the minimal fee and the laundered transaction appears one or two blocks after the payment into the mixer. If true, this would make the transactions relatively easy to track as for example a 5 BTC transfer would soon come out at the other side as 4.9745 BTC (= 5 BTC minus 0.5 % minus 0.0005).

The owner of the mixer promised his cooperation with LE requests by providing the link between the original and destination bitcoin address. The major drawback however is that it is claimed that the logs are kept for 24 hours. Still, if LE is trying to trace a real-time transaction sent to bitmixer.io to launder ransomware payments, bitmixer admin could be asked to provide urgent assistance.

Notwithstanding with the above, a German investigator who developed the Coindog tracing tool managed to find an exploit that neutralizes Bitmixer.io mixing process in majority of cases (the success depends on quality of the transaction data available). He is willing to assist other investigators trying to deobfuscate transactions processed by this mixer. Contact details for the investigator may be received through EC3.

2. Non-technical approach

The major mixers on the open web could be taken down and it seems that the individuals running these services are somewhat willing to respond to LE queries. While investigators might be hesitant to ask about a specific transaction to avoid the possibility of these services colluding with criminals, one has to assume that the owners of the services usually have no way of contacting their clients and notifying them about active investigations.

Bitmixer.io

Keeps originating and destination bitcoin address for 24 hours, which only makes it practical in a very limited number of cases.

- Contact details: bitmixer@tutanota.com

Fogify.net

Keeps originating and destination bitcoin address for an undetermined period of time.

- Contact details: Tomislav Mucic, tomislav.mucic@netis.si

DarkLaunder.com, **BitLaunder.com**, **CoinMixer.net, CoinChimp.com, TorWallet.com,**

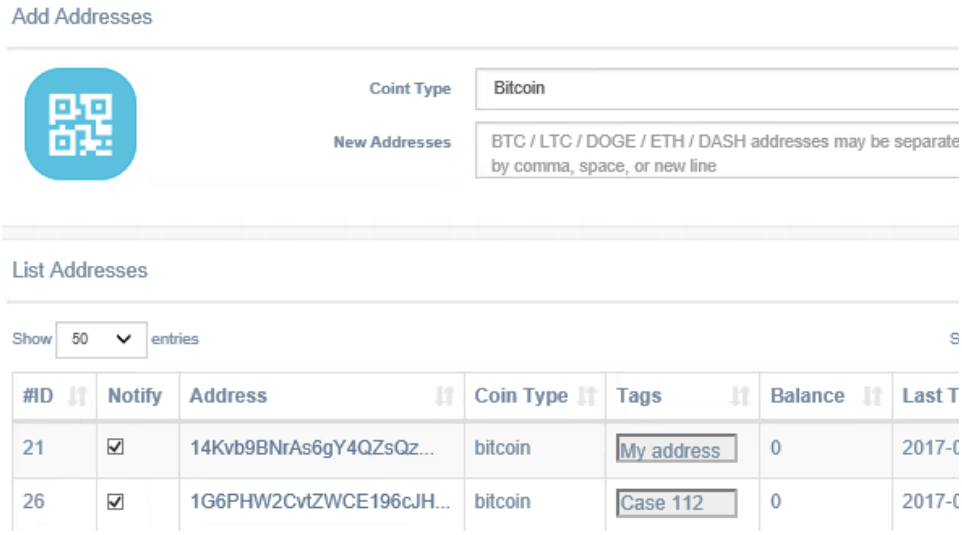
BitBulls.com, CointoPal.com and many other services are controlled by the same person.

Keep originating and destination address and IP address for a period of 2-3 months.

- Contact details: dr.michael.moriarty@yandex.com

Setting up a notification on bitcoin transactions

Once the investigators have a list of bitcoin addresses of interest, they may wish to monitor these addresses for any signs of activity. Addresswatcher.com is a website that sends email notifications whenever there is any incoming or outgoing payment to a specific bitcoin address.



This is currently the only website that allows the monitoring of altcoins – litecoin, doge, ethereum and dash in addition to bitcoin. Email notifications are sent within 5 minutes of any change in the balance of the address.

The tool has no access to a private key and hence it does not allow interference with the address in any way. Also, for suspects there is no possibility of them discovering out that their bitcoin address is being monitored for any changes in balance.

Addresswatcher does not cluster addresses into wallets so a list of suspect's addresses must be provided. On the other hand, the website does support bulk importation of addresses in different formats so it is possible to copy/paste data from .csv files or Excel.

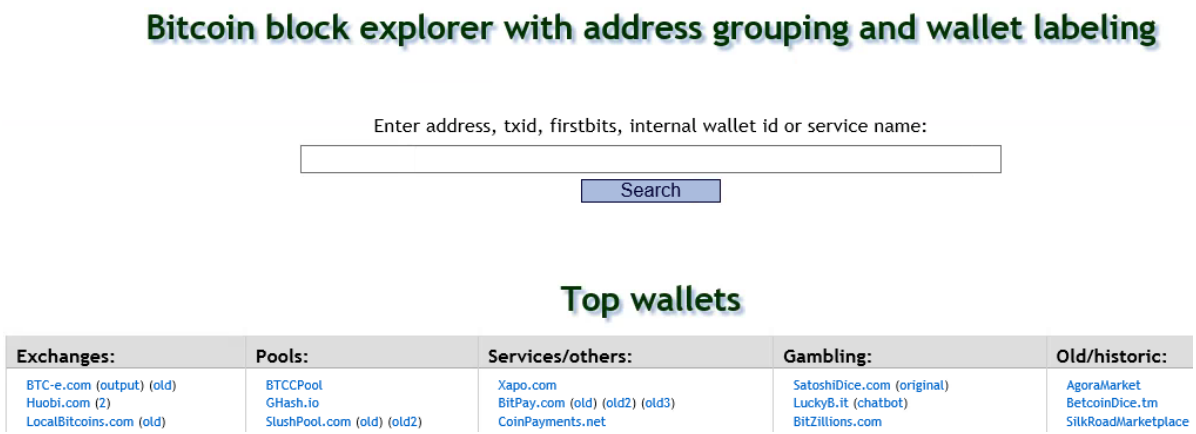
The website can "watch" for changes on up to 1,000 addresses per account. Anyone can subscribe to notifications on any address whether they own that address or not.

However, at the same time, it may be an indication that there is a link between the subscriber and the address of interest. Often it may be an owner of the bitcoin address who wants to get alerts anytime there is a movement on his account. Other interested parties may include a suspect awaiting a payment from victims or an investigator. For this reason, investigators may think twice before using work IP or email address.

Attribution of bitcoin addresses a.k.a. identification of suspects

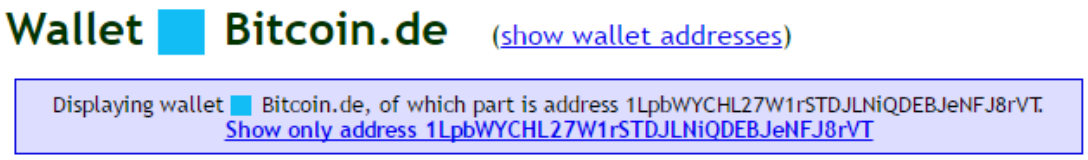
Attribution is not something that could be sorted out by the blockchain itself. The pseudonymous nature of the blockchain only keeps bitcoin addresses without any links to real identities. Therefore, tracing of the transaction in the blockchain is usually followed by the next step that will combine the information received from the blockchain with data received from other sources.

Walletexplorer.com remains the best publicly available and free-to-use tool that links bitcoin addresses with known entities including exchangers, mining pool, gaming sites, wallets or darknets. Developed in the first half of 2014 by Czech programmer Ales Janda, it got noticed by bitcoin enthusiasts and some investigators later that year. To this date it remains a powerful tool especially for those without access to a more sophisticated commercial alternative.



The developer of the website currently works at Chainalysis and does not update Walletexplorer any longer. The website, however, keeps parsing blockchain so the latest data are still available, perhaps with a slight delay to allow for processing of the latest incoming data.

Walletexplorer is straightforward to use and the results are easy to interpret. It works like a search engine for bitcoin addresses; when a bitcoin address can be linked to a known entity, the name of the entity is provided.



The tool also includes blockchain explorer, but unlike blockchain.info, Walletexplorer works with wallets rather than addresses and for this reasons the results are more informative and are easier to interpret. In the example below, we can see that 0.01329836 BTC were received from an unknown address. The transactions are ordered by date starting with the latest transaction so this transaction was preceded by a transaction that resulted in 0.35 BTC being sent to Huobi, one of the largest Chinese exchanges.

2016-07-08 07:14:40	[017821f5c9] +0.01329836	179.41653738	9448927ac0e572e6b514…
2016-07-08 07:14:40	-0.35 (-0.0019054) Huobi.com-2 fee	179.40323902	d5e735a29b7a9be92707…

After an exchanger or other entity is identified, it can be queried about a suspicious transaction or a bitcoin address. As the vast the majority of exchangers are compliant it is usually only a matter of time until LE receives a reply to its queries that can identify a suspect.

The wallet-based approach has some clear advantages compared to the transaction-based approach. While it is certainly possible to use Walletexplorer as the default free blockchain explorer, one has to be aware of the false positives and false negatives when browsing the transactions. For this reason, it is best to use Walletexplorer along with blockchain.info; the latter is a source of more reliable information while Walletexplorer brings an added value on top of what is discovered through blockchain.info.

How the website works

The website clusters addresses into wallets, mostly by grouping input addresses of multi-input transactions and change addresses. Once clusters of a notable size are identified, any of the addresses in the cluster needs to be identified through passive or active reconnaissance. This may for example include registering into many different online services or sending a small fee to a known entity and then waiting until the receiving address merges with other addresses in the wallet. One identified address of the cluster is enough to label all remaining addresses in the cluster.

There are two issues with this approach. First, transactions that involve mixing of inputs from different users together may be erroneously clustered together. This creates an issue with false positives, or addresses mistakenly linked to an incorrect entity. The website gradually became efficient in identifying mixing transactions and took a healthy conservative approach in order to minimise the occurrence of false positives.

Second, if a known service has bitcoin addresses that were never merged with other addresses, these addresses are not linked to the entity. Therefore, an address may be owned by a well-known exchanger but Walletexplorer would not have it linked. This can be described as a false negative. The success rate of Walletexplorer is highly dependent on the transaction behaviour of bitcoin entities; it is 100 % for some while considerably lower for the others.

Commercial tracing and attribution tools for investigators

There are commercial tools available on the market that are customised to cater for an investigator's needs. These are often superior to a combination of the open source tools as they may offer:

- improved clustering of addresses;
- a higher number of identified entities;
- an improved user interface;
- the possibility to import/export data;
- references to bitcoin addresses and transactions harvested from both the clear web and darknet;
- further functionality, such as searching for the shortest path to an entity that can identify the suspect;
- assistance with specific investigation-related queries.

Generally, the software providers are very open and forthcoming when it comes to the possibility of testing their products before committing to a purchase. Therefore, law enforcement agencies may examine the tools and test their advantages compared to publicly available alternatives.

For more information, it may be a good idea to check a webinar organised by Blockchain Alliance on bitcoin tracing tools that quickly introduces the key products. The links to webinar are available on the Europol Virtual Currency Taskforce LE ONLY section of the website.

Presentations of Bitcoin Tracing Tools: Information session organised by Blockchain Alliance

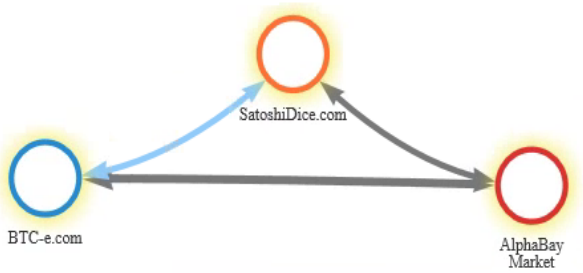
Now you can watch or re-watch practical sessions on bitcoin tracing tools organised by Blockchain Alliance using the following links:

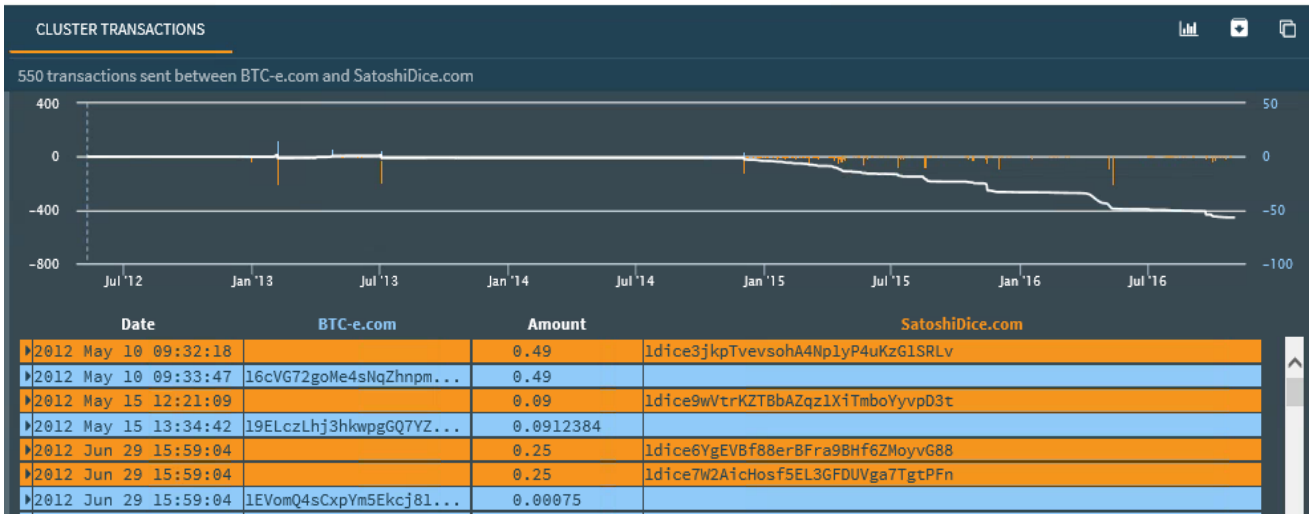
- Elliptic Presentation and Recording
- BlockSeer Presentation and Recording
- CipherTrace Presentation and Recording
- Skry (formerly Coinalytics) Presentation and Recording
- BitFury Presentation and Recording
- Chainalysis Recording

Covering each commercial tool is outside the scope of this guide. However, the next four pages provide a brief overview:

Visual examples of commercial tools

Chainalysis is the primary commercial tool used by Europol's EC3. The tool has advanced clustering in place and the largest number of identified entities. It clearly visualises transactions among different wallets and instantly provides a list of all transactions among any selected entities. As one would expect, the output may be filtered and sorted.

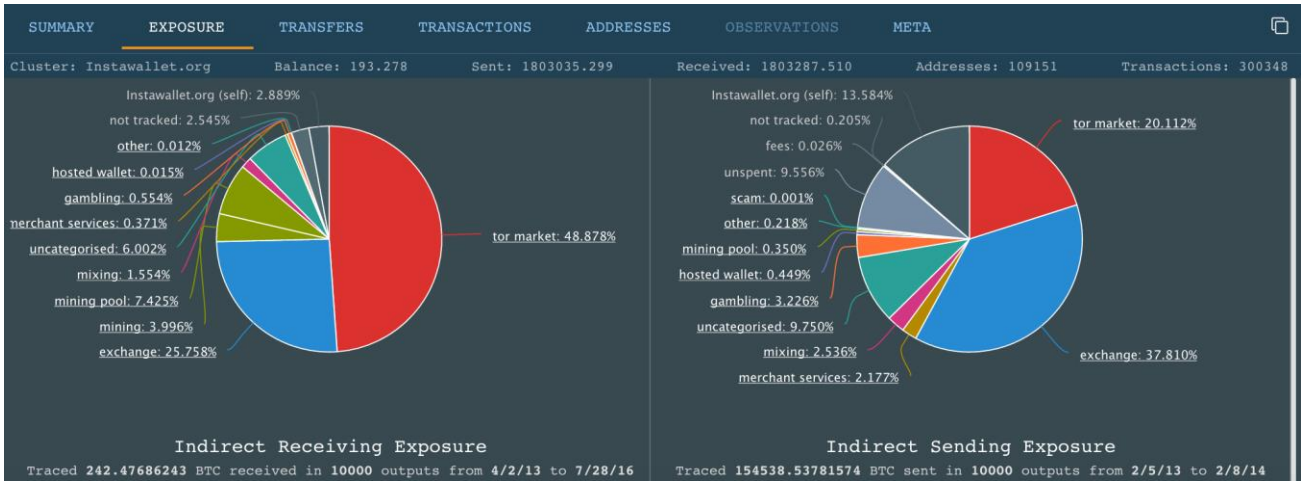




All transactions can be exported into a *.csv file for further processing.

Date/time	BTC-E	SatoshiDice	Amount
10/05/2012 09:32		1dice3jkpTvevsohA4Np1yP4uKzG1SRLv	0.49
10/05/2012 09:33	16cVG72goMe4sNqZhnpmnqfCMZ1uSFbUit		0.49
15/05/2012 12:21		1dice9wVtrKZTBbAZqz1XiTmboYyvpD3t	0.09
15/05/2012 13:34	19ElczLhj3hkwpgGQ7YznvsSvj2ySymn3U		0.09
29/06/2012 15:59		1dice6YgEVBf88erBFra9BHf6ZmoyvG88	0.25
29/06/2012 15:59		1dice7W2AicHosf5EL3GFDUVga7TgtPFn	0.25

Chainalysis is the only product that determines exposure — the amount of bitcoins flowing either directly or indirectly to and from an investigated wallet based on up to 10 000 of the latest incoming and outgoing transactions. This is a quick way to estimate the origin and destination of funds.



The pie charts are interactive so it is possible to drill down into a specific segment and see the breakdown of a particular category of activity down to the names of individual entities. The tool also automatically identifies closest path to a known entity — even if these are multiple hops of transactions away.

Chainalysis also runs a spider collecting additional information about bitcoin addresses in both the clearweb (Bitcointalk, Facebook, Reddit, etc.) and in the deepweb.

The additional information may help to identify the suspect or at least move the investigator one step closer to a real identity:

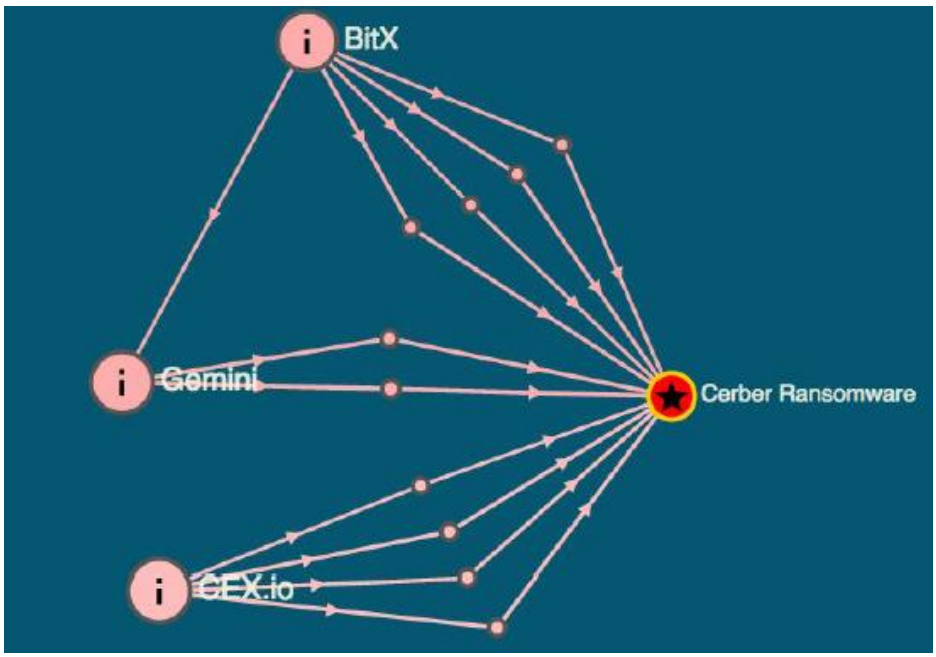
(jonson234) Help me for btc transition

DATE: Thu, 11 Jun 2015 05:01:10 GMT

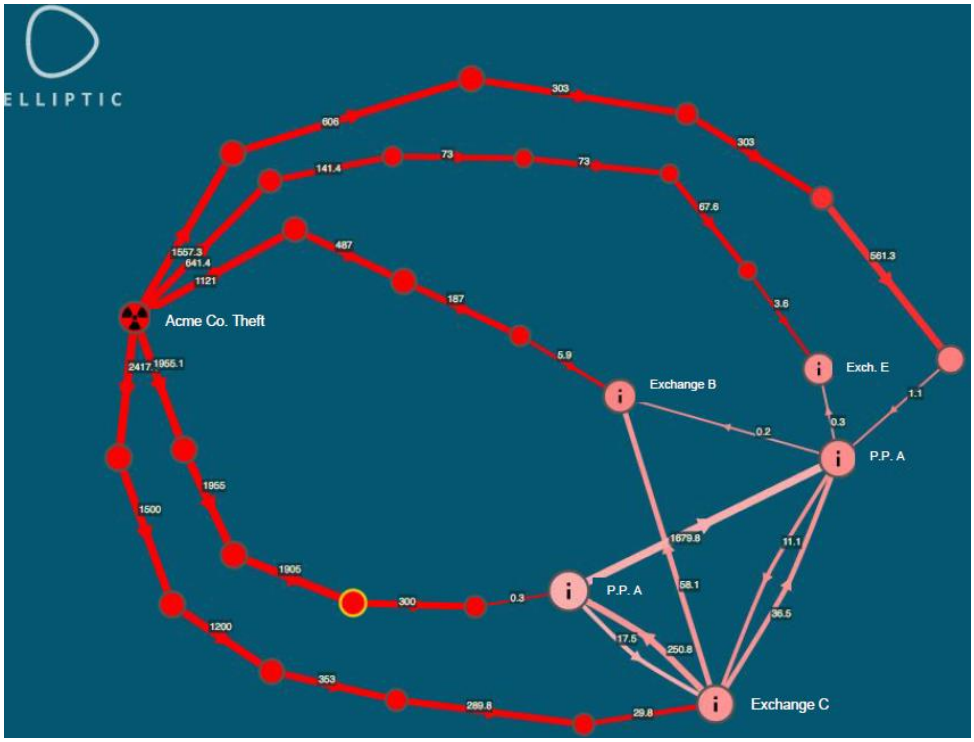
sir i am used old id which was - 1355Me1o14NsciyoFWJvVtUqdR4sGk4k9b after few days iam change my btc id

Also, as mentioned on page 29, Chainalysis is the only bitcoin tracing tool that is actively collecting IP addresses leaked by certain types of bitcoin wallets.

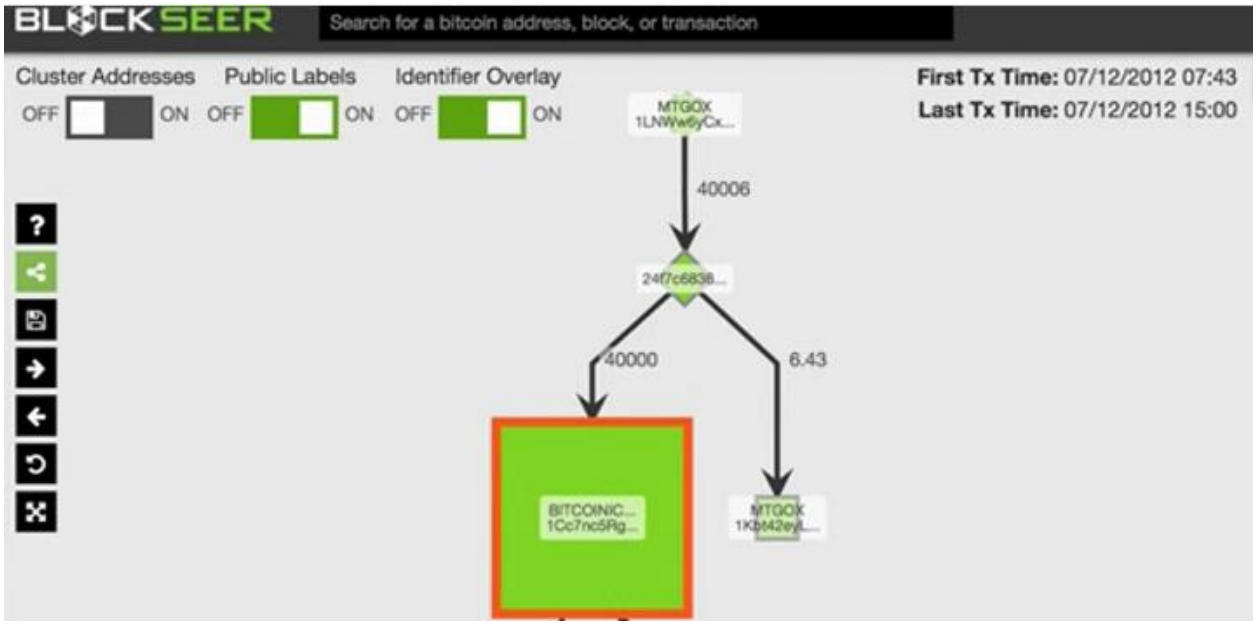
Elliptic is another interesting commercial tool that automatically trawls the blockchain. Similar to Chainalysis, its key selling point is an ability to identify the closest link between a suspect's address and an entity that can provide more information about the suspect:



In some cases, automatic exploration of multiple hops may disclose an interesting picture.



Another interesting tool is **BlockSeer**, which gives the impression of being an interesting mix of blockchain.info and Walletexplorer. While this is a cruder-looking tool without many bells and whistles, it allows for a dynamic switch between information on address and entity view through the 'Cluster addresses' option.



These tools have more to offer so the companies may be contacted with a request for further information:

Chainalysis — Jonathan Levin, Co-founder, jonathan@chainalysis.com

Elliptic — Kevin Beardsley, Head of Business Development, kevin@elliptic.co

BlockSeer — Danny Yang, Founder, danny@blockseer.com

Ciphertrace — Dave Jevans, dave@ciphertrace.com

Bitfury — Varun Gupta, vg@bitfury.com

Skry — Fabio Federici, Co-founder, fabio@skry.tech

Bitanalysis — Daan Kleiman, Head of Marketing at Bitonic, daan@bitonic.nl

Criminals buying and selling bitcoin

Most criminals do not wish to keep their proceeds in bitcoin and may seek for ways to convert it into a fiat currency (€ or $). Conversely, those who wish to pay for goods of a criminal nature are interested in purchasing bitcoin.

It should be kept in mind that the compliant entities are not limited to virtual currency exchangers. Payment-processing agents, online wallets, gaming sites and other online services can also assist LE investigations. Nevertheless, it is usually exchangers who can reliably identify their clients due to the nature and amount of data they store.

The following options are available for buying or selling bitcoins:

1. an online exchanger, vast majority of whom are nowadays willing to cooperate with LE[30];
2. private transactions between users owning large amounts of assets;
3. exchange during agreed physical appointments or ad hoc meetups of the bitcoin community;
4. mining using one's own or rented hardware;
5. a purchase of goods or services – both online and offline;
6. Payment card schemes such as Xapo or Cryptopay.me, that issue prepaid Visa or Mastercard that can be used at shops or ATMs;
7. Bitcoin ATM.

Those tracing transactions using blockchain.info have to realise that once bitcoins are deposited to an account at any service provider, the visibility of what is happening with them is lost. The suspect may convert between bitcoin and alternative virtual currencies or fiat currency but none of the transactions is recorded in the bitcoin blockchain as all real-time trades are processed by a centralised database managed by the service provider.

Example: Recent trading activity on Poloniex.com where DASH was converted to Bitcoin. These transactions never make it to the blockchain and only traders and Poloniex know about these:

TRADE HISTORY MARKET TRADES MY TRADES

Date	Type	Price (BTC)	Amount (DASH)	Total (BTC)
2017-01-02 13:22:00	Sell	0.01140000	212.00000000	2.41680000
2017-01-02 13:21:57	Sell	0.01140000	1.00000000	0.01140000
2017-01-02 04:38:59	Sell	0.01140290	50.09445652	0.57122207

Later, the suspects may withdraw bitcoins from the service provider. This transaction usually requires a request at the exchange followed by a confirmation of the transfer by email. The withdrawal transaction will appear in the blockchain:

DEPOSIT HISTORY Export Complete Deposit History

Status (Confirmations)	Coin	Amount
Complete	BTC	0.40000000
2017-01-05 08:05:53		
Address: 1LdYQ6Ju6mYzKQmXXvCY26X6gZbDVdUJ		
Txid: 784855ebea70cc6f5025261e3c8fa60b7360e270f81b09f05a21f7f6a7292f7b		

[30] The list of entities which have complied with LE requests can be seen in Appendix 3 at the last page of this guide

And indeed, if we check the receiving address in Walletexplorer, we will have a proof that it was really recorded in the blockchain and it is a part of Poloniex wallet:

Nevertheless, the provider may send bitcoins from any bitcoin address he owns (e.g. C) to any address specified by the client (D) while previously deposited bitcoins were sent by client from address A are withdrawn by someone else (B), thus breaking the transaction flow.

Hence, tracing using Blockchain Explorer alone is not very efficient and investigators have to rely on Walletexplorer or a commercial tool to identify exchangers and other relevant parties, who can identify suspects and provide LE with further details on their transactions.

LE, unlike regular users, can approach the exchangers with a request for information. The following opportunities exist for the investigator at each step in the suspect's activity:

Action	Investigation opportunities
Suspect obtains a wallet	If the wallet is Bitcoin Core or another wallet downloaded from a public source, it is almost impossible to identify the user. No registration is required to download most software wallets. If the user sets up an online wallet (Blockchain.info, Coinbase, Circle, Xapo, etc.), the online provider may be queried about IP logs and the data provided by the user.
Suspect generates a bitcoin address	There is no visibility into new bitcoin addresses generated using software wallets. Some online wallet providers may keep a record of the new address generated/requested by the user even if no payment has been received to this address.
Suspect receives or deposits bitcoins to his or her wallet or online account	Transfer is almost instantly visible on blockchain explorers and after the first confirmation it features in the blockchain. Some online services wait for three to six confirmations before they update the client's balance. The service provider can be queried about the user and the transactions.
Suspect makes transfers within the online platform (e.g. BTC trade or gambling)	Transfer is usually not projected on the blockchain. The online services keep a separate balance outside the blockchain and for the outside observer they act as a complete black box. However, LE can request assistance and get a list of all the user's actions.
Suspect withdraws bitcoins from the service	Once the user requests the withdrawal and confirms it, the online service may take extra time to verify the request. Once approved, the transfer is almost instantly available on blockchain explorers and after the first confirmation it features in the blockchain. Service provider can be queried about the user and the transactions.

Sending requests to exchangers and other compliant entities

Since 2015, Europol's EC3 has had the privilege of hosting meetings between representatives of LE and the most popular VC exchangers. One of the outcomes of the meetings was a list of recommendations LE should follow in order to make the data request as efficient as possible:

- The request should be submitted by email to the official single point of contact listed at the end of this guide
- Each LE request should be case specific. When requesting information for several different cases, please submit each case separately
- The name, position and contact details of the officer requesting the data as well as those of the authorising officer should be provided
- If possible, include a link to a public website that states a contact phone number exchangers can use to verify the authenticity of the person who sent the request
- "LE request" should be clearly mentioned in the subject of the email, containing a unique reference number whenever applicable
- The request should be either submitted in English or the language corresponding to the country where the exchanger operates (e.g. German for Bitcoin.de)
- The request should be sent in two formats:
    - A scanned copy of an official document, ideally on a letterheaded paper, signed by an authorised person
    - A request in editable format, such as *.pdf, *.doc(x), *.xls(x), from which it is easy to copy/paste data
- Involvement of suspect in criminal activity should be briefly yet clearly described
- Legal grounds (which piece of legislation authorises the request) should be provided
- Requests should be limited to a reasonable number of bitcoin addresses/transactions. Requesting details on dozens of addresses and transactions is a time consuming exercise for exchangers
- Requests should be narrowed down in order to only demand relevant data. Some bitcoin addresses may have a large number of incoming/outgoing transactions so it might be better to provide specific transaction IDs or a relevant date range
- When providing an address or a transaction ID, it should be specified whether the investigator is interested in information on the sender or receiver
- An indication of urgency/deadline should be provided. Requests for urgent replies have to be justified
- As some of the exchangers inform their clients about LE enquiry the investigators may want to explicitly ask the exchangers not to reveal the on-going investigation accompanied by a justification

Those who do not have a template for the request may use the one supplied on the following page:

Law Enforcement request for bitcoin facilitated crimes recommended by Europol's EC3

Reference Number: *(First two characters of country, surname of investigator, his year of birth, Case ID, Case Message ID)*	E.g. NL_Smith_81_1_1 Case and message should start with number one and increase incrementally, e.g. second request related to the first case is _1_2		
Requested by: *(Name, Position, Agency, Phone, Email, Address, Country)*			
Approved by: *(Name, Position, Agency, Phone, Email, Address, Country)*			
Purpose of the request *(Identify client, confirm a transaction, freeze assets)*	E.g. In order to assist our investigation we request identification of the above suspect.		
Description of Crime *(Including name of the legislation and a breach of a specific §)*	E.g. An unidentified suspect was selling a large number of narcotics on several dark markets in early 2017. It has been established he consequently sent at least 15 bitcoins to his account at XXXXX exchange. Suspect's bitcoin addresses and transactions are listed in the following box:		
Items to be queried: *Username, Full name,* *Bitcoin address (from-to)* *Bitcoin transaction id,* *Transaction id,* *IP logs (from-to),* *Email address, Phone,* *Credit Card, Bank account*	Please note that the more information is requested the longer it takes to answer the request. Historical IP logs in particular should be restricted to a meaningful period. It may be necessary/practical to attach an excel sheet but before you do that think about streamlining the request.		
Results to be received: *Username, Full name, VC addresses linked to account* *IP logs, Transaction history, Contact details, Payment method, Device_ID, Message/Chat logs, ID and Proof of Address, Selfie*	Please specify if the report should focus on sender or receiver and type of data you expect to receive		
Public PGP Key *Leave empty if you do not use PGP*			
Permission to notify client *If not, provide rationale*	No	**Urgency** *(Normal / High)* *If high, provide rationale*	Normal
Please keep this document as doc/docx/rtf/odt or digitally readable PDF			

Approaching non-compliant entities

Providers of services that may seem to obstruct the process could be exposed to 'by-the-book' investigatory techniques, where the server may be seized in order to verify whether the logs needed to investigate criminal activity are indeed irretrievable and whether they have been deleted in a forensically secure fashion. Sometimes, the imminent possibility of having the infrastructure seized leads to a more willing cooperation by the service provider. Of course, such an approach has to be in line with the relevant legislation and a prosecutor should be consulted first.

Naturally, such an approach cannot be applied against services in the darknet, where the location of the infrastructure is unknown.

EC3 is interested to hear of any non-compliant entities. Please share your experience on this topic in the LE-Only part of the Virtual Currency Taskforce on SPACE.

Bitcoin scalability issues

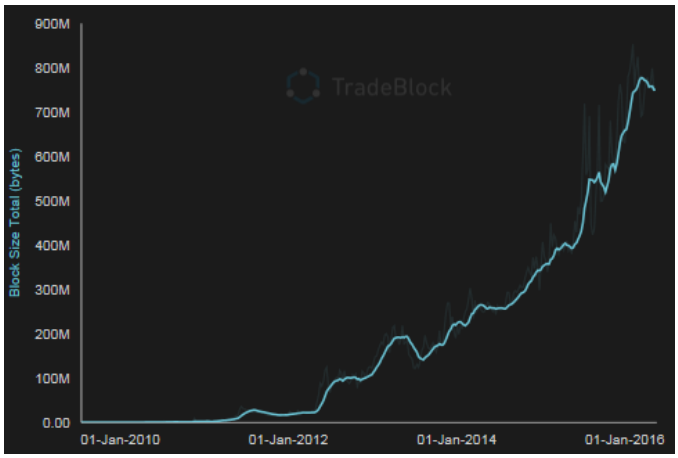
One of the topics that are heavily discussed by the bitcoin community is the maximum block size and corresponding scalability issues. These issues are more serious than many are willing to concede and could ultimately contribute to a downturn of bitcoin and its replacement by an alternative cryptocurrency. The debate is hence of relevance to LE as the demise of bitcoin would probably give rise to other cryptocurrencies, many of which are designed to provide a much higher level of anonymity than one can achieve with bitcoin. On the other hand, once bitcoin solves the scalability issues it will be ready to become a global currency having a much wider adoption and usage.

Throughout 2016, many of the blocks were dangerously close to the maximum allowed capacity of a bitcoin block, which is 1 megabyte.

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
412407	26 minutes	1777	13,129.34 BTC	BTCC Pool	989.07
412406	30 minutes	1730	16,228.55 BTC	AntPool	998.13
412405	36 minutes	1972	14,389.46 BTC	AntPool	998.07
412404	39 minutes	1772	13,933.80 BTC	F2Pool	999.88
412403	42 minutes	2101	11,332.07 BTC	F2Pool	999.65
412402	43 minutes	1860	34,379.73 BTC	BitFury	998.16

Source: blockchain.info.

Additionally, some miners decide to mine blocks well below the 1 Mb limit. This means that the average size of the block is even lower in practice, having average of around 800 Kb per block, which was first hit in January 2016.

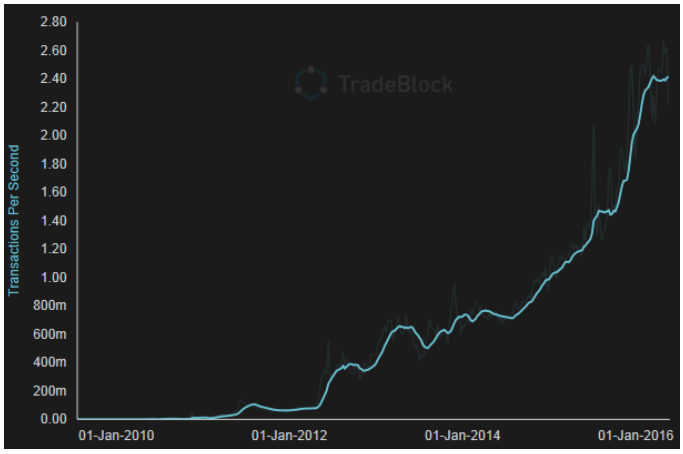


Source: TradeBlock.

If bitcoin were to become a global currency and its usage become comparable with the volumes processed by credit card companies, the block size would be in gigabytes.

If there were no significant changes made to bitcoin, there would be little room left for bitcoin to scale. Any growth would be limited by the software ceiling that would prohibit processing of more

than about seven transactions per second and that would essentially preclude bitcoin from becoming an efficient global medium of exchange. The practical limit is even lower as many transactions contain multiple inputs and outputs, which results in higher sizes and consequently fewer transactions that fit into the 800 Kb bucket. Thus, in May 2016 bitcoin hit a practical ceiling of about 2.4 transactions per second and has not come any lower since then.



Source: TradeBlock.com

This ceiling would essentially disqualify bitcoin from becoming a popular global currency. Visa, in comparison, handles an average of around 2 000 transactions per second and is capable of processing up to 56 000 transactions per second. The current limit posed on bitcoin could be increased but the exact way of implementing this is a topic sparking heated discussion among different groups of bitcoin supporters.

In May 2016 the size of the blockchain increased to about 70 Gb. Bearing in mind the relatively low cost of storage, hobbyists may still run full bitcoin nodes using their desktop computers. However, given the pace at which the blockchain keeps growing, which is faster than the size of storage media, it may reach several terabytes in a not-so-distant future. This will result in a decrease in the size of the bitcoin network caused by the gradual elimination of enthusiasts voluntarily providing their hardware to support the network, which is likely to lead to a higher centralisation of the network.

What may happen in the future is that the size of the transaction volume will increase notably, bloating the size of the blockchain. In essence, there are three scenarios as to how the situation may develop:

1. Block size will be increased, leading to the blockchain growing at a very fast pace.
2. Block size will be kept, which will restrict the number of transactions that may be processed, lead to increasing fees for sending payments and greatly limit the practical use of bitcoin for financial transactions.
3. Block size will be kept and the majority of the transactions will somehow be processed off the blockchain and only their digests will be recorded in the bitcoin blockchain. Bitcoin developers are already working on solutions such as *Segregated Witness*, which decreases the size of transactions in the blockchain by removing the signature, or *Lightning Network*, where the majority of transaction would be stored outside bitcoin blockchain. This would allow almost limitless scaling of bitcoin.

Can bitcoin be shut down?

This may sound like a very controversial question — probably because it indeed is so. Bitcoin is a revolutionary and disruptive technology that made the impossible possible and will benefit humanity in ways that are not yet obvious to us nowadays.

It should be made clear that EC3 does not, in any way, consider or advocate attacking bitcoin infrastructure with the purpose of taking it down. While the negative consequences of a takedown would be immediate and obvious for everyone involved, benefits would be limited and short lived at best and would disappear with the arrival of a more resilient and less transparent technology.

Still, given that resilience is one of the crucial aspects of bitcoin technology, and given the number of occasions on which this question has been put forward, we should address the question as there are ways of hurting technology to such an extent that it could lead to its demise. These include:

A 51 % attack conducted through collusion with existing miners or investing into a separate mining facility could be purchased at huge cost. The lower-cost alternatives include cutting the largest miners off the network or seizing their existing mining devices — which would not be legal or ethical.

In theory, researchers might discover a way to break ECDSA — a method used to generate a public key out of the private key. This highly unlikely scenario would mean that the attackers could discover the private keys of bitcoin users and steal their coins, making bitcoin unsafe to use. However this would require the compromising of multiple hashing algorithms.

All means of converting fiat currency to bitcoin could be obstructed or made illegal through international legislation. This would push bitcoin users either to trade into the darknet or to adopt alternative anonymity measures or payment methods. Similarly, takedowns of centralised platforms — exchangers, payment processors, markets, gaming sites, miners or mixers — would push these to the darknet or made them resilient through decentralisation.

A malicious code could be smuggled into the bitcoin client to wreak havoc among those using that particular version of bitcoin client. There are many types and versions of bitcoin wallets out there that could be attacked; however compromising the reference client Bitcoin Core would require a lot of effort. As the client is open source software, the malicious part of the code would have to be overlooked by many expert coders.

ISPs could decide to throttle bitcoin traffic. The easiest way to do this would be to block incoming traffic to port 8333 bitcoin uses. To counter this measure, bitcoin users would have to obfuscate their traffic, probably through the use of VPNs, or set their bitcoin clients to use a different port. At the end of the day this would be little more than an inconvenience for the community.

Needless to say, some of the above scenarios would only hurt the system rather than taking it down. As long as there is at least one miner present in the system, it would still be up and running — in the same way as happened back in 2009, when there was a sole miner getting all bitcoins for a period of several months.

Once again, the purpose of this chapter was not to offer advice on how to target the bitcoin network. Instead, the main purpose was to illustrate the obvious drawbacks and questionable benefits such approach would bring.

Another payment method might supersede bitcoin and the critical mass of users would move to the superior system. However, it is relatively unlikely that the new payment method would bring more transparency than existing cryptocurrencies. Nowadays, a voluntary transition of the bitcoin community to a competing technology seems to be most probable scenario that could lead to gradual demise of bitcoin.

Evolution

Cryptocurrencies are here to stay in one form or another. Bitcoin has to be seen as what it is — the first attempt at a global distributed currency. It remains to be seen whether it will sort out current scalability issues and retain its dominant market share and status of a leading cryptocurrency. There will be a constant inflow of new cryptocurrencies offering innovative features with the ambition to coexist along bitcoin and perhaps even supersede it.

The behaviour of criminals using cryptocurrencies will continue to be shaped and cultivated by LE activity. LE will thus ultimately actively contribute to the evolution: evolution into what may become a decentralised and completely anonymous form that is fit to survive government attacks.

Following the above logic, increasing the efficiency of LE investigators is likely to result in the following developments for criminal transactions:

- an increasing use of mixers;
- the move of exchange services to the darknet and other platforms, making mapping of infrastructure difficult or impossible;
- an increasing adoption of altcoins being adapted to provide a higher degree of anonymity, such as currencies with inbuilt mixing capabilities or hidden public keys;
- new criminal products on the market such as the offer of VC accounts opened by money mules;
- a combination of bitcoin and traditional payment mechanisms, such as debit and credit cards;
- the emergence of bitcoin wallets providing increasing anonymity through inbuilt mixers;
- the emergence of P2P exchangers completely missing KYC;
- criminal abuse of smart contracts.

Appendix 1: Basic bitcoin terminology

Altcoin: a cryptocurrency other than bitcoin

Blockchain: a complete list of all bitcoin transactions

Block: a container enclosing bitcoin transactions; chains of blocks form the blockchain

bitcoin: the first decentralised virtual currency / cryptocurrency

BTC: abbreviation for bitcoin

Client: end-user software that generates private key and sends payments

Cold wallet: wallet stored on an offline device or paper; not susceptible to hacking or malware

Confirmation: validation of transactions performed on average once every 10 minutes

Cryptocurrency: currency based on cryptography; essentially any decentralised currency like bitcoin

Miner: a person or a group of people confirming bitcoin transactions

Mining pool: a group of miners working together and sharing the proceeds

Mixer: a service that makes tracing of transactions very difficult

Node: a client that propagates transactions across the bitcoin network to other nodes

Private key: secret key allowing the sending of bitcoin payments; the owner of this key controls the bitcoins

Public key: publicly known key derived from the private key; when encoded it is a bitcoin address

Seizure: movement of bitcoins from a suspect's addresses to an address controlled by investigator

Transaction: a payment; essentially a movement of bitcoins from one address to another

UTXO: unspent transaction output, essentially a "balance" on the bitcoin address

Wallet: online or offline application that stores private keys and manages payments

Appendix 2: Format of keys and addresses

In practice, many bitcoin users have not seen their private and public key, and quite often they do not have a real need to do so. Investigators and first responders, on the other hand, should know that both public and private keys, as well as bitcoin addresses, can be represented in different shapes and forms.

A private key is longer than a bitcoin address. The length of the private key is fixed to 51 characters and often starts with number 5. Only alphanumerical characters are allowed. Both private keys and bitcoin addresses are case sensitive.

Example of a **private key**:
5HueCGU8rMjxEXxiPuD5Bdku4MkFqeZyd4dZ1jvhTVqvbTLvyTJ

There is one more format called compressed private key. This format is 52 characters long and starts with the letters L or K. The support of compressed public keys began in March 2012 with the introduction of Bitcoin QT client 0.6.

Example of a **compressed private key**:
KyoPrwwmvSZymMrJLRhePV6jTFFpGU6uMVLv5nQhkMM4dpDKaMgG

In contrast, the usual format of the public key is:

04D0DE0AAEAEFAD02B8BDC8A01A1B8B11C696BD3D66A2C5F10780D95B7DF42645CD85228A6FB2
9940E858E7E55842AE2BD115D1ED7CC0E82D934E929C97648CB0A

However, this format is relatively rarely seen in the real world because the public keys are hashed in order to get a bitcoin address. A corresponding **bitcoin address** derived from the above public key is:

1Gaehh7TsJAHuUAeKZcXf5CnwuGuGgyX2S

The vast majority of bitcoin addresses start with number 1, followed by another 25 to 34 alphanumerical characters. In addition to the common bitcoin addresses, bitcoin also allows the generation of so-called P2SH (Pay to Script Hash), where a script decides what will happen with a transaction. Such addresses start with the number 3 and are often used for multi-signature transactions, where multiple private keys have to sign a transaction. An example of a P2SH address is:

3QJmV3qfvL9SuYo34YihAf3sRCW3qSinyC

Many use the terms bitcoin address and public key interchangeably. This is not exactly correct but it is not a serious mistake since the bitcoin address can be derived from the public key. When an investigator sends a subscriber enquiry on a public key to a bitcoin exchanger that is in fact a bitcoin address the exchanger will still understand the request.

However it is important to get the terminology right. With the advent of big data an increasing number of investigations will be done in an automated way, where different types of data are cross-

referenced against each other, and therefore correct labelling is essential to support future investigative efforts.

Bitcoin private and public key conversions — technical description

A suspect may store public and private keys in different formats. Therefore, it is useful to be aware of the steps required for the conversion and have a reference, should such conversions be required. It may be surprisingly difficult to discover an easy-to-understand, step-by-step description of a conversion between a private key, a public key and a bitcoin address and therefore the process is listed below.

(a) Private key from binary/hex to private key in the most common format

On the fundamental level, the private key is a 256-bit string, which means that it can be stored in the form of 256 1s and 0s. The number of possible values is beyond comprehension and for practical purposes it is essentially infinite. This is the reason why private keys can even be generated offline — there is simply no need to check whether the newly generated key already exists as one can safely assume it does not.

The private key can also be represented as a 32-byte string represented by 64 hexadecimal (including 0-9 and A-F) characters:

1E79423A4ED27608A15A2616A2B0E5E52CED330AC530EDCC32C8FFC6A520AED1

Since the above number is way too long, it is generally expressed using a shorter format such as WIF (Wallet Import Format), two examples of which were demonstrated on the previous page. This is by far the most popular and practical representation of a private key.

The following process will briefly explain the steps taken to generate the private key in the WIF format. Should the private key be recovered in binary or hexadecimal format, the investigator can apply the following steps to get the private key that can be imported into a wallet:

1. Private key in binary format

0001111001111001010000100011101001001110110100100111011000001000101000010101101000100110000101101010000101011000011100101111001010010110011101101001100110000101011000010100110000111011011100110000110010110010001111111111000110101001010010000010101110110101 0001

2. Convert to private key in hexadecimal format

1E79423A4ED27608A15A2616A2B0E5E52CED330AC530EDCC32C8FFC6A520AED1

3. Add 80 before the string

801E79423A4ED27608A15A2616A2B0E5E52CED330AC530EDCC32C8FFC6A520AED1

4. Apply SHA256 to the previous result

FA9A14AA9B812D27E4D71EA352BB6976D95A6FEBAFE7C970B6C83ECE948AF0BE

5. Again apply SHA256 to the previous result

FC9DE33EB831759045B78595DE663D522DD8F36E5889B80D71CDF7299E81DF66

6. Take the first 8 characters, which is a checksum

FC9DE33E

7. Add it at the end of the string that was the result of step 2

801E79423A4ED27608A15A2616A2B0E5E52CED330AC530EDCC32C8FFC6A520AED1FC9DE33E

8. Apply Base58 hash to the previous string to get the private key in WIF

5J3hzQ41KoJX64H5YRTqS9YB9LVGacU2qusL37Ys1eVpJTgnr4u

(b) Public key and bitcoin address

There is even a slightly longer procedure required to get a bitcoin address out of the public key. Note that three different hashing algorithms are used.

1. Public key in hexadecimal format

044C32014849A98AA9B0236E218DC75168BA157F6827823555F6BE486DD0E382678E9D1A3619A7D CCFC05293E80DA0C045B2ACD0A0E798E43BBD2A78DD1900B6FD

2. Calculate SHA256 hash of the above result

55F35EA94FF3B8C89E13C0A4C8A51EA1729153C2C693BE0CF6724966C9C3FB7C

3. Calculate RIPEMD160 hash of the above result

E0C765BE0E2A45180318FC137FECC631D9249745

4. Add 00 in front of the above string

00E0C765BE0E2A45180318FC137FECC631D9249745

5. Calculate SHA256 hash of the above result

3D8A1705CE355746E8E5AC05928C8A09E27F7D74BCE08F4527D486C8FC400EB5

6. Calculate SHA256 hash of the above result again

D8241ACB9EC07A596982DF97F9F45D26662D80D8532F9025BBF2AACD5FC92A73

7. Take the first 4 bytes (8 characters) or the above result

D8241ACB

8. Append these to the result of step 4

00E0C765BE0E2A45180318FC137FECC631D9249745D8241ACB

9. Calculate Base58 hash of the above

1MVXEM6N3atFqoBpRC1CrCZiFpSgQc3tLr

So, finally, *1MVXEM6N3atFqoBpRC1CrCZiFpSgQc3tLr* is the resulting bitcoin address.

One may wonder why there are so many steps involved in deriving a bitcoin address. The key reason is security. If one of the hashing algorithms has a backdoor or gets compromised, there are still other algorithms to be broken to revert the bitcoin address to the public key and the public key to the private key. The second reason is length — hashing allows the bitcoin address to be made shorter than the public key. Finally, Base58 algorithm was chosen because it prevents people confusing 0 with O or 1 with I (capital i) or l (lowercase L) by omitting these characters altogether.

Gobittest.appspot.com is an excellent website that offers scripts to automate all the above calculations.

Those interested in forensic examination of hard drives should check a section on *practical bitcoin forensics* that describes *BTCscan*, a Python tool searching for bitcoin addresses and private keys.

Appendix 3: LE contacts on virtual currency exchangers

Exchanger	Name	Role	Contact
Bitcoin.de	*Jan Vorndamme*	Compliance Specialist	*jv2015@bitcoin.de*
Bitfinex	*Stuart Hoegner*	CEO	*stu@bitfinex.com*
BitMyMoney	*Robert R. Nederhoed*	CEO	*rr.nederhoed@gmail.com*
Bitonic	*Daan Kleiman*	Marketing	*daan@bitonic.nl*
BitPay	*Timo Dijkstra*	Compliance Director	*timo@bitpay.com,* *cc jeremie@bitpay.com*
Bitplaats	*Lennert Vlemmings*	CEO	*l.vlemmings@bitplaats.nl*
Bitstamp	*Stephane Leloup*	Chief Compliance Officer	*stephane.leloup@bitstamp.net*
Blockchain.info	*Marco Santori*	Global Policy Counsel	*marco@blockchain.com*
BTC-e	-	-	*compliance@btc-e.com*
Circle	*John Beccia*	Chief Compliance Officer	*jbeccia@circle.com*
Coinbase	*John Kothanek*	Sr. Director	*john.kothanek@coinbase.com*
Cryptopay	*Alexey Gunyashov*	Compliance Officer	*alexey@cryptopay.me*
Cubits	*Simona Camilleri*	Compliance Manager	*legal@cubits.com*
Gatecoin	*Aurelien Menant*	CEO	*a@gatecoin.com*
itBit	*Erik Wilgenhof Plante*	Chief Compliance Officer	*erik@itbit.com*
Kraken	*Mindy Yang Salvati*	Chief Compliance Officer	*lawenforcement@kraken.com*
LiteBit.EU	*Kenny Rokven*	General Manager	*k.rokven@2525.ventures*
LocalBitcoins	*Nikolaus Kangas*	CEO	*Should be contacted via Finnish Police - directly or via Interpol/Europol. When in doubt contact Annina.Salonen@poliisi.fi*
OKCOIN	*Tim Byun*	Chief Risk Officer	*tim@OKCoin.com*
Poloniex	*Curtis Hale*	Compliance Officer	*curtis@poloniex.com*
SpectroCoin	*Justas Dobiliauskas*	Co-Founder	*j.dobiliauskas@spectrofinance.lt*
Simplecoin.cz	*Pavel Niedoba*	CEO	*info@simplecoin.cz*
Xapo	*Martin Kopacz*	Chief Compliance Officer	*martin.kopacz@xapo.com*