The Hague, 10/05/2021

EDOC# 1163486

Business Area/Team O3 EC3

Bitcoin Guide for Investigators:

Following the Money

Contents

The Objective of this Guide

The guide should serve as a source of practical information on Bitcoin tracing.

It builds on the foundations provided by the EC3 Cryptocurrency Guide for Investigators released in 2016 and does not replicate the information covered by that product.

What is covered?

- ✓ Key terminology a cryptocurrency investigator has to master
- ✓ Overview of Bitcoin wallets and addresses
- ✓ Understanding Bitcoin transactions
- ✓ Identification of payment and change addresses
- ✓ Following the money
- ✓ Custom clusters
- ✓ Dealing with exchanges
- ✓ Advanced blockchain search
- ✓ Tracing of Bitcoin forks

What is not covered?

- ✗ Bitcoin fundamentals
- ✗ Altcoins (other than Bitcoin forks)
- ✗ Bitcoin forensics and dealing with encrypted wallets
- ✗ Bitcoin seizure
- ✗ Bitcoin abuse and crime trends
- ✗ Bitcoin legislation issues

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 Cryptocurrency community at EPE, where this guide will be distributed.

A Necessary Introduction into Key Bitcoin Vocabulary

To keep this section as short as possible, we briefly define the purpose of the key bitcoin artefacts. For broader descriptions, please refer to the Bitcoin Guide for Investigators released in 2016:

Bitcoin address can be publicly shared with others to receive bitcoins.

Bitcoin private key should be kept secret as it allows sending funds from an associated Bitcoin address.

Bitcoin seed was introduced later and contains a compilation of private keys in a wallet. Therefore, an owner of the seed can reconstruct the private keys and move / seize funds.

Bitcoin transaction is permanently stored in the Bitcoin blockchain; Each transaction has a unique ID and contains information on addresses sending and receiving funds.

Bitcoin wallet is an application that provides an overview of transactions and the ability to store and send funds. Wallets store a collection of private keys and the corresponding addresses. One user can have multiple wallets and each of these wallets can contain one or more (even thousands) of private keys and addresses.

Bitcoin Artefacts and their Format

Cryptocurrency investigators, forensic examiners and first responders should be familiar with the following formats of bitcoin artefacts. Note that these typically differ for most cryptocurrencies.

Bitcoin address either starts with number *1* or *3* and is between 26 and 35 characters long. Also valid is the so-called bech32 address format introduced in 2017 that starts with *bc1* and is longer – up to 90 characters. However, typically the addresses are 42 characters long.

Examples:

19TVazHWmyLWz5ApdPQcsZ3iKNpd8o5evx

3HRZjedwF2AJejNTtgznWnas4E6froNP5r

bc1qffr3ufaccf3nnz9aaw54gmafkud078q8m96teg

The following regular expression can be used to search for all above types of Bitcoin addresses:

\b([13][a-km-zA-HJ-NP-Z1-9]{25,34})|bc(0([ac-hj-np-z02-9]{39}|[ac-hj-np-z02-9]{59})|1[ac-hj-np-z02-9]{8,87})\b

Other relevant regular expressions related to private keys and altcoin addresses can be found on EPE.

Bitcoin private key

Bitcoin private key is typically 51 or 52 characters long starting with 5, 6, K or L:

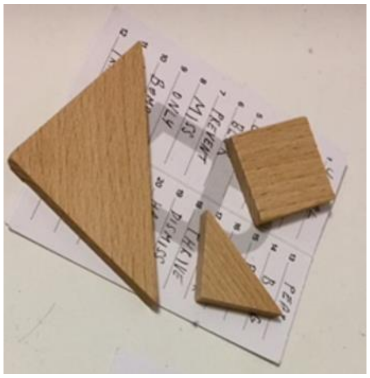
Examples:

5HpvLqZUrtiv1MDoAxr4MJaL37cBPVSkAS2pcZbujroBiyXzqvC

KwGWSZLMyDHzxYFUnyVXnca72LAGrGYdWdV39xu5nAnrLFXXpYgW

Bitcoin seed

It is also known as a mnemonic phrase and is typically formed of 12, 16, 18, 20 or 24 standalone words. These are typically English words that do not form a sentence. If a seed with one additional word is discovered, the final word may be a passphrase.

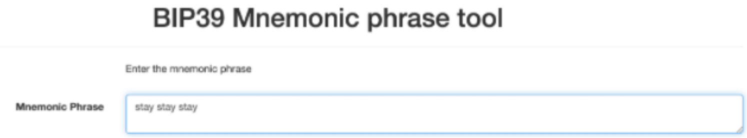


This is an example of a 20-word seed phrase generated by Electrum wallet: *tremble together beautiful constants howler gluttons dowden portends subversives pulitzer unimpeded candice dobra igloos holier hedging hern condescending hyacinths iceland*

The Bitcoin seed, once imported, will generate private keys so there is no need to record those anymore. Since it is much easier to backup Bitcoin seeds than a possibly large number of private keys, the use of seeds became popular over the years. The majority of popular wallets have already implemented this feature.

Although there have been standardization efforts by the developers, it may not be possible to easily recover a seed generated by one wallet in another. So – the seed generated by e.g. Blockchain.com, Exodus and Trezor are not compatible.

Therefore, if a seed is recovered at a crime scene, it is important to know which type of wallet generated it. If this cannot be established, investigators can use tools developed by Austrian and Dutch colleagues. A link to this tool along with the necessary documentation can be found at Cryptocurrency Community on EPE (Europol Platform for Experts): EPE(LE ONLY) > Library > MNEMONIC PHRASE TOOL FROM FIOD.



BIP39 Mnemonic phrase tool

Enter the mnemonic phrase

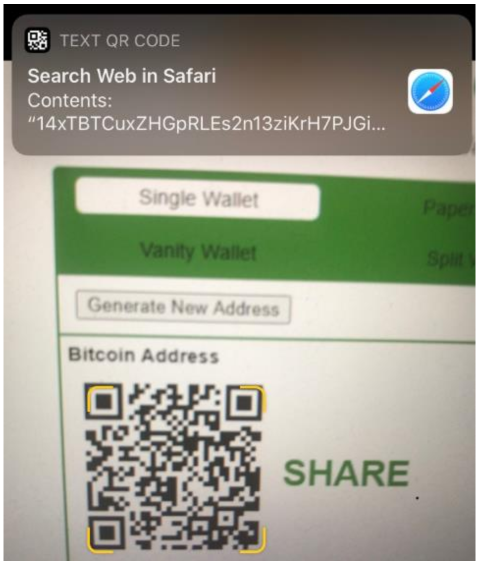
Mnemonic Phrase: stay stay stay

This very useful tool will establish in which wallet the seed was created and which private keys and cryptocurrency addresses can be derived from the seed. This may turn out to be crucial information when seizing funds from the suspect.

Bitcoin Transaction ID is a standardized 64 hexadecimal characters long string:

Example:

94be21f4bd3a249ffe04b7dc2917201f07201069bd0a7c763665b30834c488ba



TEXT QR CODE

Search Web in Safari

Contents:

“14xTBTCuxZHGpRLEs2n13ziKrH7PJGi...

Cryptocurrency addresses and private keys are often presented in the form of **Quick Response (QR) codes**.

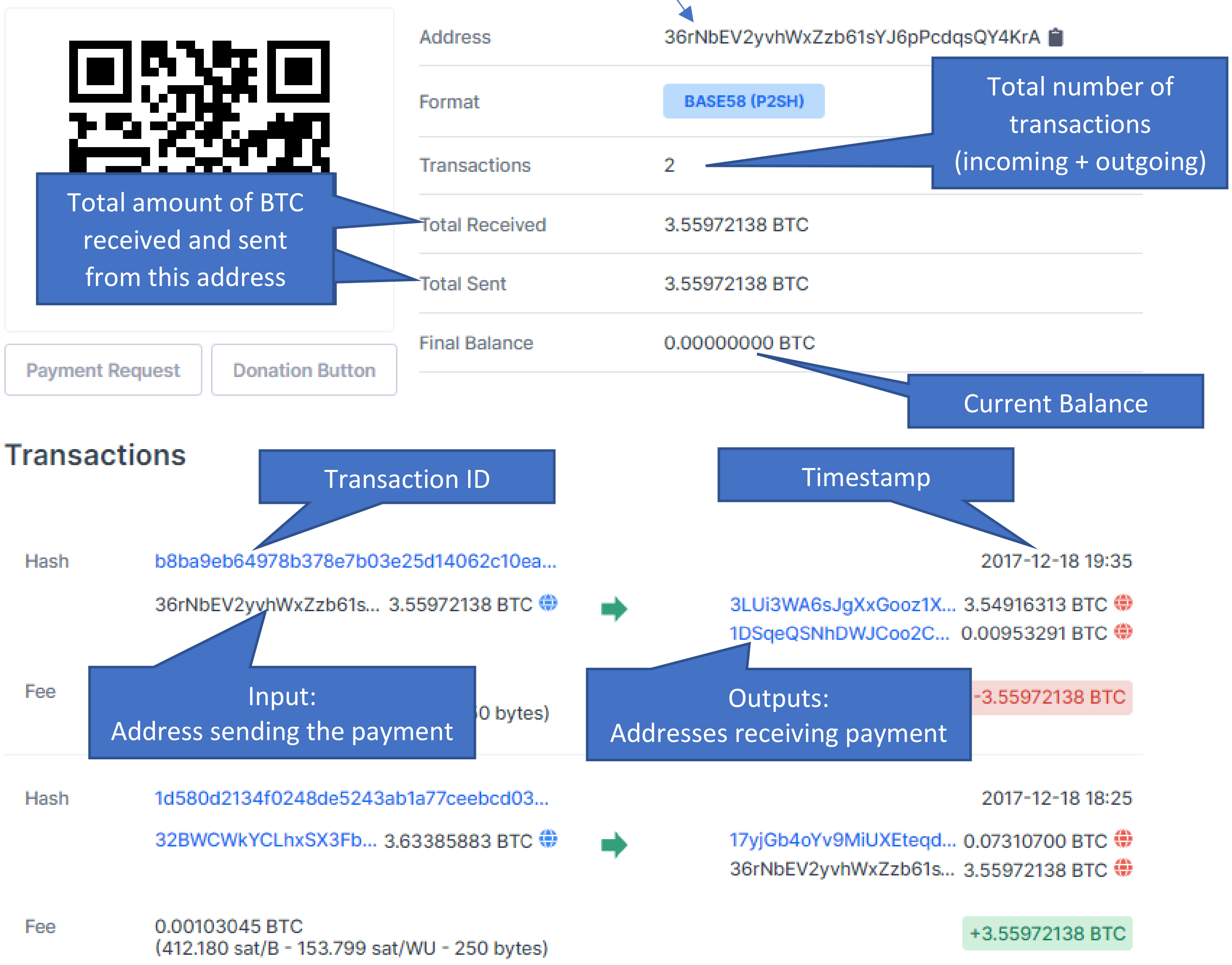
If such an artefact is discovered at the crime scene, it can be “deciphered” using any QR code reader application or most bitcoin wallets. Also, your default camera app *may* have a functionality to automatically interpret QR codes – you can test it on the photo on the right.

At EC3, we have received countless contributions containing various identifiers in different formats. Some of these are either altcoins – cryptocurrencies other than Bitcoin, some are string identifiers linked to different services.

For example, the string in the following format: *7d711a7c-8db6-4a81-9976-e9acb87dcb73* is generated by the Blockchain.com for each wallet they operate and this wallet provider would have to be contacted in order to get any meaningful information behind this unique identifier.

Checking Bitcoin Address

It is quite straightforward to check the current balance and a list of transactions for any bitcoin address. In the example below, we take a look at 36rNbEV2yvhWxZzb61sYJ6pPcdqsQY4KrA using blockchain.com:



Address	36rNbEV2yvhWxZzb61sYJ6pPcdqsQY4KrA
Format	BASE58 (P2SH)
Transactions	2
Total Received	3.55972138 BTC
Total Sent	3.55972138 BTC
Final Balance	0.00000000 BTC

Total number of transactions (incoming + outgoing)

Total amount of BTC received and sent from this address

Current Balance

Transactions

Transaction ID

Timestamp

Hash b8ba9eb64978b378e7b03e25d14062c10ea... 2017-12-18 19:35

36rNbEV2yvhWxZzb61s... 3.55972138 BTC → 3LUi3WA6sJgXxGooz1X... 3.54916313 BTC
1DSqeQSNhDWJCoo2C... 0.00953291 BTC

Fee ...0 bytes) -3.55972138 BTC

Input:
Address sending the payment

Outputs:
Addresses receiving payment

Hash 1d580d2134f0248de5243ab1a77ceebcd03... 2017-12-18 18:25

32BWCWkYCLhxSX3Fb... 3.63385883 BTC → 17yjGb4oYv9MiUXEteqd... 0.07310700 BTC
36rNbEV2yvhWxZzb61s... 3.55972138 BTC

Fee 0.00103045 BTC
(412.180 sat/B - 153.799 sat/WU - 250 bytes) +3.55972138 BTC

Things to know:

- This information is updated in real-time as it collects information from the blockchain as well as from the bitcoin network. This means that the unconfirmed transactions are shown here as well.
- The timestamps show the time when the transaction was validated (i.e. inserted into the blockchain). This may have been seconds, minutes and in rare cases even hours after the transaction was sent (i.e. signed and broadcasted by a user's wallet to the Bitcoin network).

- The date is shown in European format YYYY-MM-DD and the timestamp time zone is the local time (as opposed to many tools that show transaction time in UTC).
- The address we are checking (36rNb…) is shown at the top of the page as a simple text, while other addresses such as 17yjGb… are shown as links so that their balance and transactions can be inspected with one click.
- The addresses receiving payment are followed by the following icon: 🌐
  The red colour means the recipient already spent the payment; a green colour, on the other hand, would mean that the funds are still in the recipient's address.
- You may check the address on many other Bitcoin blockchain explorers, such as btc.com or blockchair.com.

Questions:

1) The address entered at Blockchain.com was not found at all. What does this mean?

2) The address entered at Blockchain.com shows no incoming transaction. How would you interpret this information?

3) What can we find out about 1N2gAnVmA2FSXHtQgH3cCstEkVuRRP9tQ6?

4) What can we find out about 13zz6vXs5bXj4G8dxAt214vGQ25EsmrZ7B?

5) What can we find out about 1HngHpuzyZTBv4KSase8DXznVAEPdqTfFs?

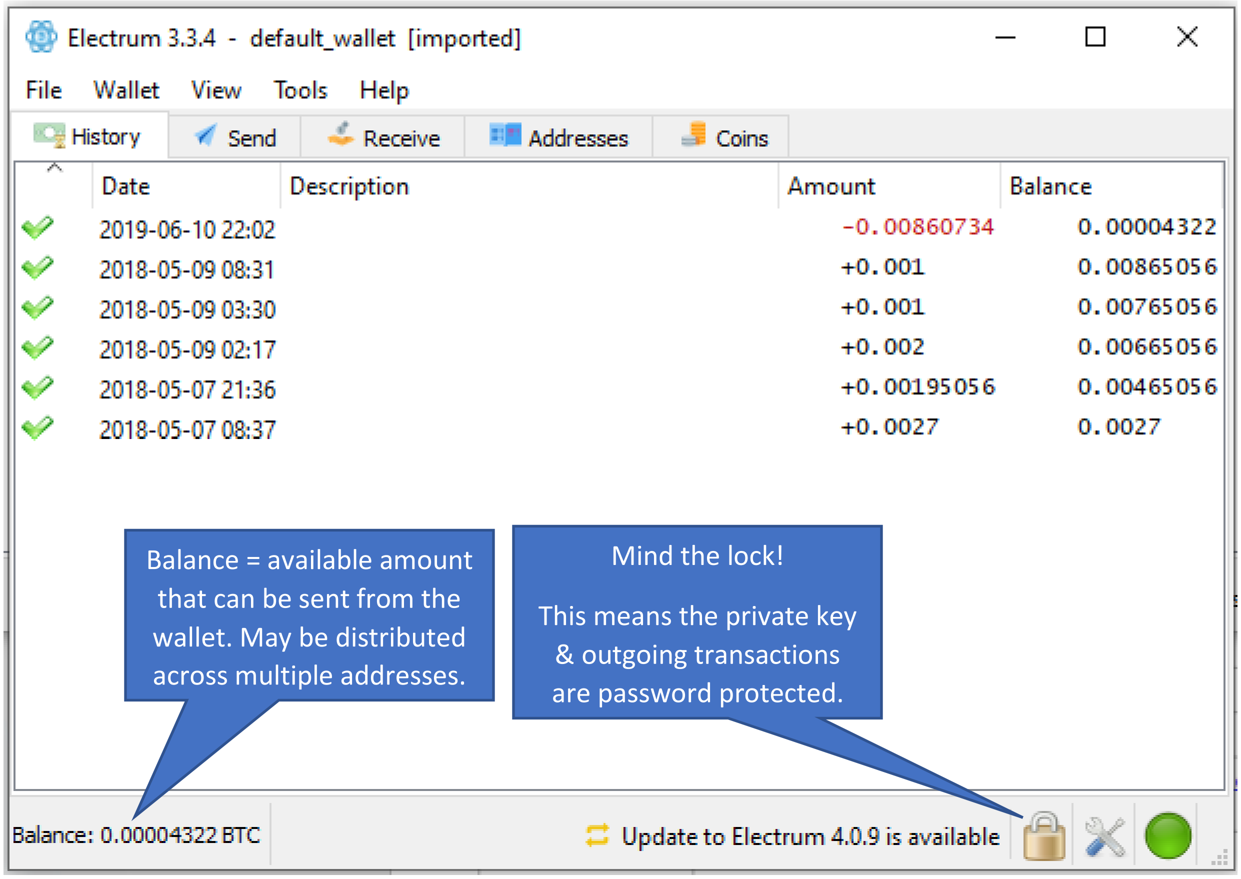
Responses:

1) The address is an incorrectly formatted bitcoin address. Either the string is not a bitcoin address or it has been altered / mis-typed.
2) An address without incoming transactions will inevitably have a balance of 0. This is a valid bitcoin address but it has not received any funds so we cannot trace it – at least not in the Bitcoin blockchain. The only thing that we can do is search for the address using OSINT or monitor the address using a commercial tracing tool.
3) The address has a balance of 0.0001 BTC. It received 0.2299 BTC and then sent 0.2297 BTC on while paying 0.0001 BTC as a transaction fee. Thus, 0.0001 BTC is a remainder on the address.
4) This is not a valid bitcoin address. It does not pass the checksum validation and therefore cannot be found on Blockchain.com. There are tools online that can establish whether the address is valid or not (for example http://lenschulwitz.com/base58).
5) Address has 0 balance and without incoming or outgoing payments there is nothing to trace. However, this address may still exist in other blockchains. Perhaps it may be worth the effort to check the address using Bitcoin Cash explorer…

Cryptocurrency Wallets

There is a one-to-many relationship between a user and wallets. One user can have multiple wallets in different forms – desktop, mobile phone application, online, hardware, and, occasionally, even paper wallets that are less common nowadays as the more security aware users have shifted to hardware wallets.

The wallets store private keys and present users with easy-to-use interfaces. Also, they show balances and details of transactions and allow for the sending and receiving of funds:



Date	Description	Amount	Balance
2019-06-10 22:02		-0.00860734	0.00004322
2018-05-09 08:31		+0.001	0.00865056
2018-05-09 03:30		+0.001	0.00765056
2018-05-09 02:17		+0.002	0.00665056
2018-05-07 21:36		+0.00195056	0.00465056
2018-05-07 08:37		+0.0027	0.0027

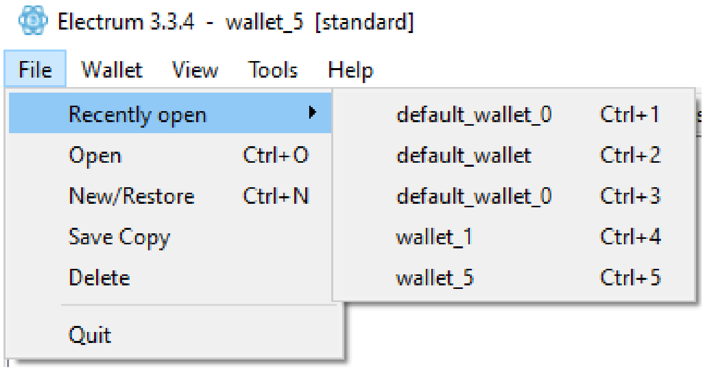
Balance = available amount that can be sent from the wallet. May be distributed across multiple addresses.

Mind the lock!

This means the private key & outgoing transactions are password protected.

Balance: 0.00004322 BTC

Update to Electrum 4.0.9 is available



Note that a single wallet application can contain several cryptocurrency wallets. This is a common scenario with hardware wallets where a user can create wallets for different purposes, such as a low balance dummy wallet to be handed over to law enforcement when the situation calls for it.

The wallet may store any number of private keys with corresponding addresses. The private keys linked to addresses that were used in the past and have 0 balance are not discarded – any of the addresses may receive funds in the future, so the private keys are kept in order to further sending the funds.

Most Popular Cryptocurrency Wallets

Please keep in mind that the list is far from complete – there are dozens of desktop, mobile and online wallets so for practical reasons we only list some of the most popular ones:

Computer and mobile phone wallets

BitcoinCore Jaxx edge

Electrum Exodus Mycelium Atomic Green Wallet Bread wallet

Privacy-focused wallets

Samourai Wasabi

Online wallets

coinbase bitpay Blockchain.com

Xapo

Paper wallets

bitaddress.org
Open Source JavaScript Client-Side Bitcoin Wallet Generator

BRAINWALLET.IO

Hardware wallets

TREZOR Ledger keepkey

There are cryptocurrency wallets available for all operating systems (Windows/Linux/Mac). The oldest wallet is Bitcoin Core, but it is not relevant for most users, as it runs as a full bitcoin node for which a download of the full blockchain (well over 300 Gb) is required. The majority of wallets are “light wallets” – they connect to trusted sources to access the blockchain. This provides a reasonable trade-off between convenience and security for most users and allows mobile wallets apps to exist.

Samourai (Android only) and Wasabi (multiplatform) appeared in 2018 to address an area many other Bitcoin wallets neglected: privacy. Both wallets natively integrate mixing techniques so that the user no longer has to use an external mixing service to launder (possibly tainted) Bitcoins.

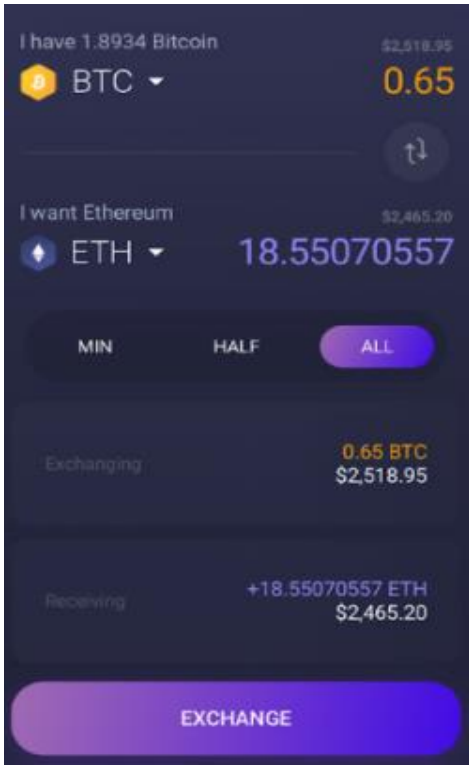
Wallets with In-built Conversion

While some wallets only support one currency, increasing number of wallets manage multiple cryptocurrencies. Exodus, for example, supports over 100 cryptocurrencies in both its desktop and mobile application.

Some wallets go even further and allow for cryptocurrency conversion. In order for this to work, the wallet must use cryptocurrency exchange APIs – for example, Exodus mainly uses Binance, CoinSwitch and HitBTC for the conversion.

Such conversion is very convenient for legitimate users as they do not have to create an account at an exchange. However, it also provides welcome options for criminals who do not have to associate their identity with the conversion.

Should the conversion take place, the investigator will see a suspect’s interaction with the above exchanges, however, the exchange will not be able to provide Know-Your-Customer (KYC) data upon request.



I have 1.8934 Bitcoin

BTC $2,518.95 0.65

I want Ethereum

ETH $2,465.20 18.55070557

Exchanging 0.65 BTC $2,518.95

Receiving +18.55070557 ETH $2,465.20

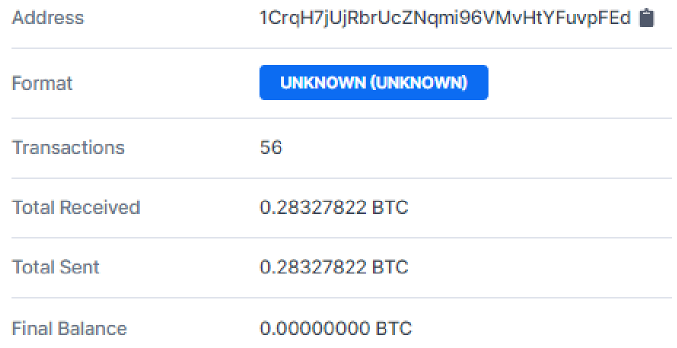
The previous page primarily focused on Bitcoin and multicurrency wallets. Most larger cryptocurrencies have their dedicated wallet(s), for example MyEthereumWallet (MEW) is a wallet dedicated to storing Ethers and Ethereum-based tokens.

Keep in mind that the situation with wallets changes. Some wallets that used to be popular are no longer supported (Armory, MultiBit), while others were acquired by cryptocurrency companies (CoPay transformed into BitPay wallet), so instead of providing extended information on wallets here, we recommend you to check updated sources (e. g. https://walletscrutiny.com/walletSupport/) for more information.

Address v. Wallet v. Cluster

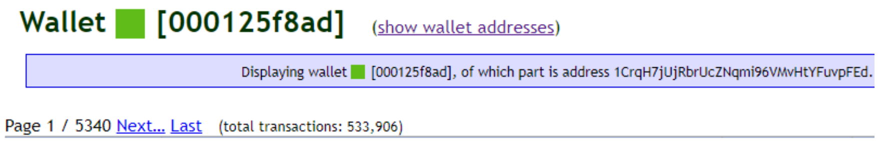
The relationship between the wallet and address is obvious – the wallet manages the private keys and consequently controls the funds on the corresponding bitcoin addresses. How to search for wallets and addresses?

Let us look at an address *1CrqH7jUjRbrUcZNqmi96VMvHtYFuvpFEd*. Using an address-focused blockchain explorer, we see that the address sent or received 56 transactions:



Address	1CrqH7jUjRbrUcZNqmi96VMvHtYFuvpFEd
Format	UNKNOWN (UNKNOWN)
Transactions	56
Total Received	0.28327822 BTC
Total Sent	0.28327822 BTC
Final Balance	0.00000000 BTC

Using the wallet-focused website walletexplorer.com, we see a much higher amount of transactions – well over 500,000 controlled by wallet [000125f8ad]. You can ignore the name of the wallet as this is merely a unique identifier used by Walletexplorer and does not provide further information:

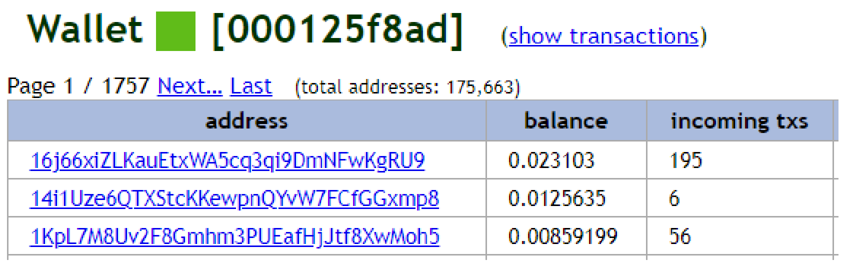


Wallet 🟩 [000125f8ad] (show wallet addresses)

Displaying wallet 🟩 [000125f8ad], of which part is address 1CrqH7jUjRbrUcZNqmi96VMvHtYFuvpFEd.

Page 1 / 5340 Next... Last (total transactions: 533,906)

Thus, using Walletexplorer we discovered that the address belongs to an unidentified service. If we choose to check the wallet addresses, we see over 175 thousand results – no personal wallet would be this active:

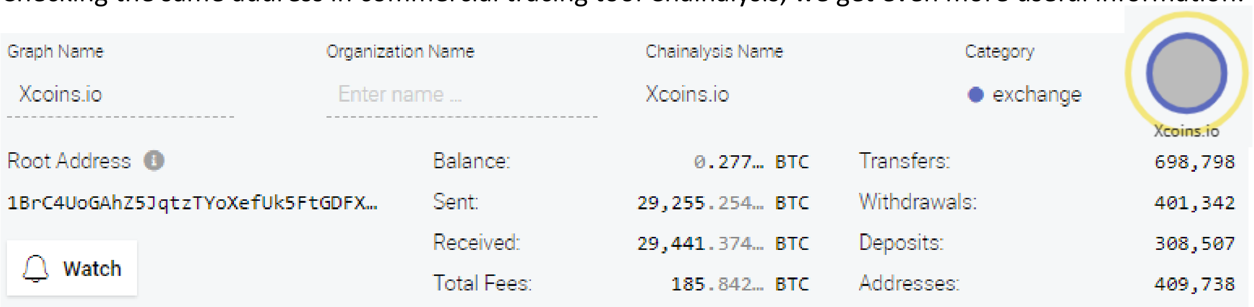


Wallet 🟩 [000125f8ad] (show transactions)

Page 1 / 1757 Next... Last (total addresses: 175,663)

address	balance	incoming txs
16j66xiZLKauEtxWA5cq3qi9DmNFwKgRU9	0.023103	195
14i1Uze6QTXStcKKewpnQYvW7FCfGGxmp8	0.0125635	6
1KpL7M8Uv2F8Gmhm3PUEafHjJtf8XwMoh5	0.00859199	56

Checking the same address in commercial tracing tool Chainalysis, we get even more useful information:



Graph Name	Organization Name	Chainalysis Name	Category
Xcoins.io	Enter name ...	Xcoins.io	● exchange

Root Address

1BrC4UoGAhZ5JqtzTYoXefUk5FtGDFX…

Balance:	0.277… BTC	Transfers:	698,798
Sent:	29,255.254… BTC	Withdrawals:	401,342
Received:	29,441.374… BTC	Deposits:	308,507
Total Fees:	185.842… BTC	Addresses:	409,738

While Walletexplorer identified over 175,000 addresses in the wallet, Chainalysis found over 400,000. Furthermore, it managed to identify the service as Xcoins.io, a US-based cryptocurrency company that may respond to law enforcement enquiries.

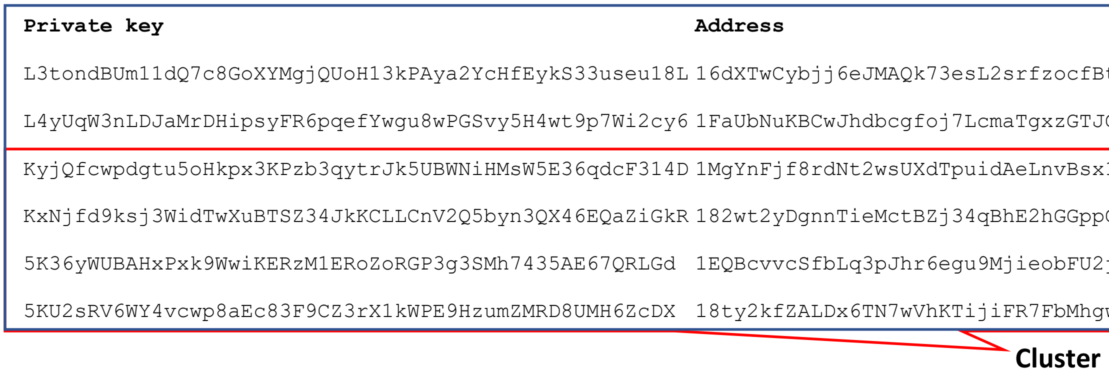
This simple example demonstrates that blockchain explorers alone cannot be used for cryptocurrency investigations – not only do they not identify the entities, they do not even cluster addresses into wallets. While Walletexplorer attempts to do both, its dataset is inferior to commercial tracing tools.

Clustering of Addresses is far from perfect

An important task of a tracing tool is to cluster addresses into a wallet and to label it with the name of the entity. The previous example showed that not all tools are created equal. Some have better clustering and identification, which greatly influences the practicality of the tool.

So far in this section we used the term *wallet* to describe an entity identified by Walletexplorer or Chainalysis. Nevertheless, the reality is a bit more complicated, as tracing tools often fail to identify all addresses in a wallet:

Wallet



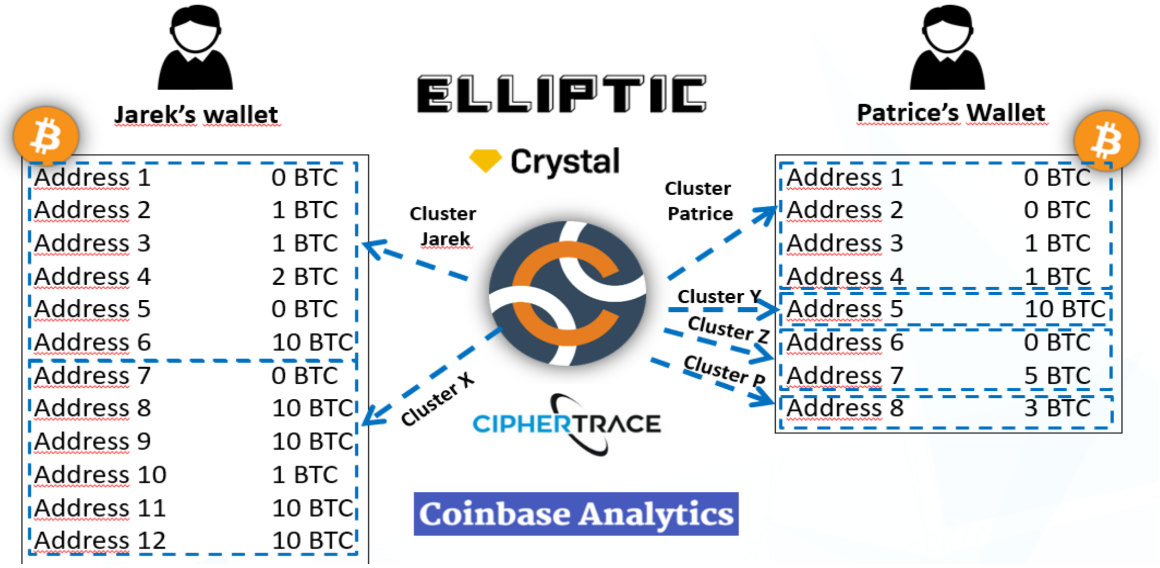
Private key	Address
L3tondBUm11dQ7c8GoXYMgjQUoH13kPAya2YcHfEykS33useu18L	16dXTwCybjj6eJMAQk73esL2srfzocfBt5
L4yUqW3nLDJaMrDHipsyFR6pqefYwgu8wPGSvy5H4wt9p7Wi2cy6	1FaUbNuKBCwJhdbcgfoj7LcmaTgxzGTJGW
KyjQfcwpdgtu5oHkpx3KPzb3qytrJk5UBWNiHMsW5E36qdcF314D	1MgYnFjf8rdNt2wsUXdTpuidAeLnvBsx1m
KxNjfd9ksj3WidTwXuBTSZ34JkKCLLCnV2Q5byn3QX46EQaZiGkR	182wt2yDgnnTieMctBZj34qBhE2hGGppGD
5K36yWUBAHxPxk9WwiKERzM1ERoZoRGP3g3SMh7435AE67QRLGd	1EQBcvvcSfbLq3pJhr6egu9MjieobFU2jr
5KU2sRV6WY4vcwp8aEc83F9CZ3rX1kWPE9HzumZMRD8UMH6ZcDX	18ty2kfZALDx6TN7wVhKTijiFR7FbMhgwP

As the tracing tools often fail to identify all addresses in the wallet, what the investigator actually sees is often merely a subsection of the wallet – a cluster. Often, the tools cannot determine with 100% certainty when an address belongs to a certain cluster and when it does not. The tools generally prefer to take a careful approach and keep these two entities separate. Therefore, false negatives are much more common than false positives, as the tools prefer to take a conservative approach to clustering and labeling.

As shown in the above example, a wallet may control six bitcoin addresses but only four are actually displayed by the cluster in a tracing tool. Naturally, this has far-reaching consequences for the investigator, for example, the address that is missing could have been in a wallet of an identified service, could be the one that sends funds to an identified service, or could link a suspect to a criminal activity.

Let us consider the following scenario. We have two users – Jarek and Patrice.

Jarek has 12 addresses in his wallet, 55 BTC in total. Patrice has 8 addresses with 20 BTC sitting in this wallet. However, this key information may be displayed in a distorted way due to the fact that not all of Jarek's and Patrice's addresses are clustered correctly:



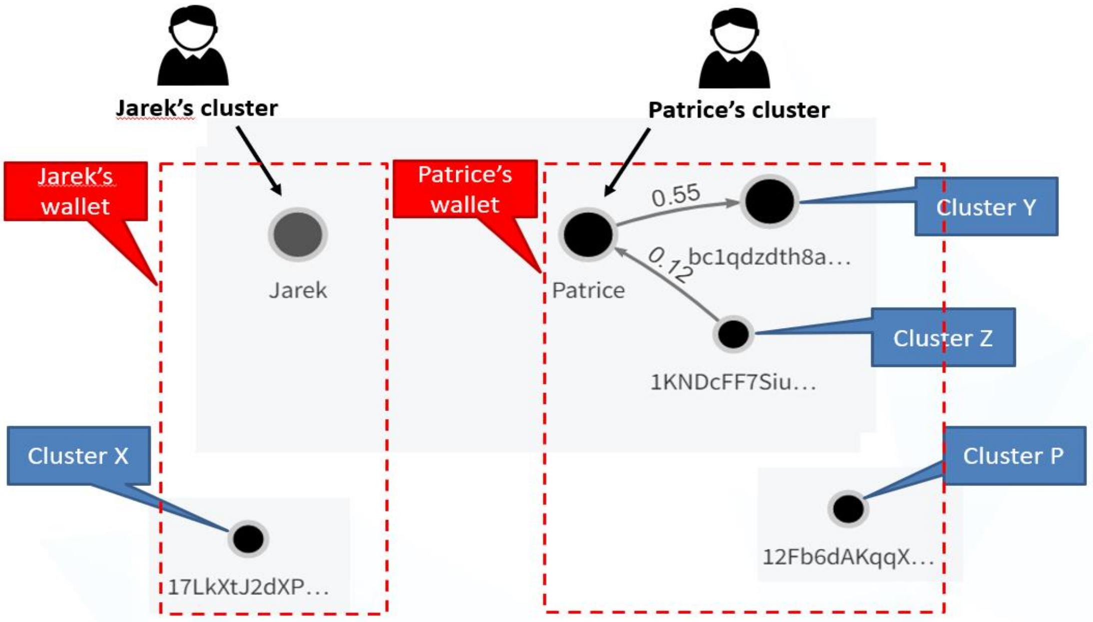
Jarek's wallet	
Address 1	0 BTC
Address 2	1 BTC
Address 3	1 BTC
Address 4	2 BTC
Address 5	0 BTC
Address 6	10 BTC
Address 7	0 BTC
Address 8	10 BTC
Address 9	10 BTC
Address 10	1 BTC
Address 11	10 BTC
Address 12	10 BTC

Patrice's Wallet	
Address 1	0 BTC
Address 2	0 BTC
Address 3	1 BTC
Address 4	1 BTC
Address 5	10 BTC
Address 6	0 BTC
Address 7	5 BTC
Address 8	3 BTC

The commercial tracing tools may depict Jarek's wallet in two separate clusters and Patrice's wallet in four with no apparent indication given to the investigator that some of these clusters belong together. Ideally, we would see only two clusters, which we could rename to Jarek and Patrice, containing 12 and 8 addresses respectively:

Jarek
Patrice

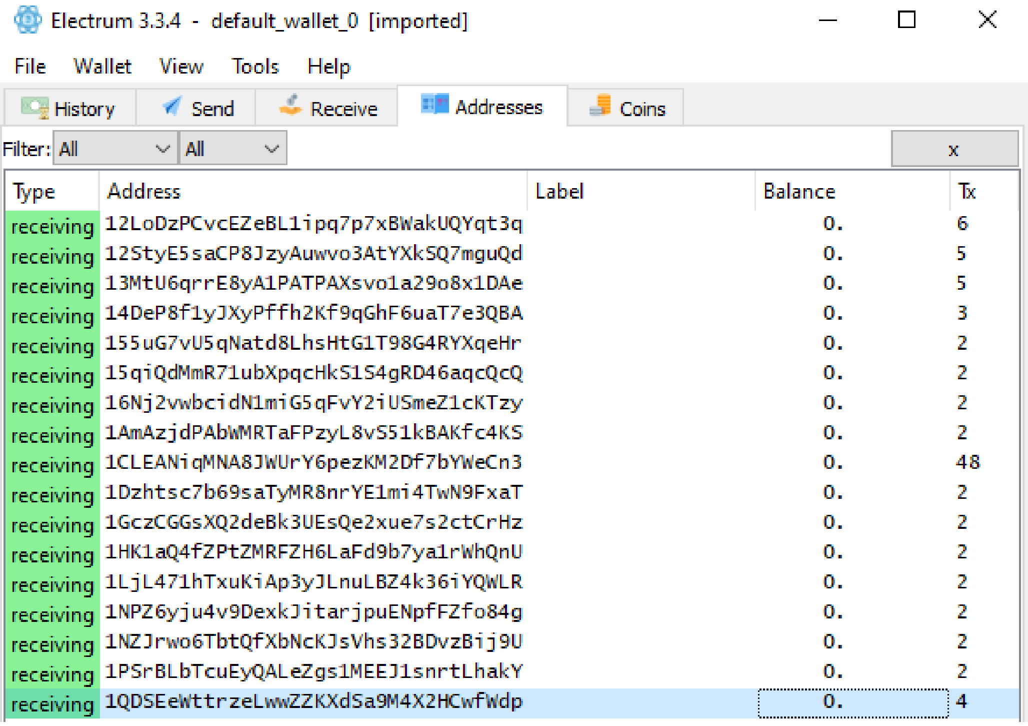
Instead, the tools fail to cluster the addresses together. So what we actually get is this – again, without any indication that clusters Y, Z and P actually belong to the cluster owned by Patrice. There may be a transaction among the individual addresses but the addresses may also appear to be completely standalone (for example, newly created addresses may have received funds without spending it and the tools have no way of knowing they should merge the clusters together):



An experienced cryptocurrency investigator needs to know what the limitations of the tools are and <u>not to take information displayed by the tracing tool for granted</u>. Through experience, the investigators learn to mitigate some of the deficiencies of the tracing tools, for example by applying change address techniques discussed later in this guide.

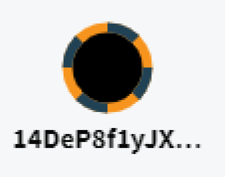
A Real-world Example:

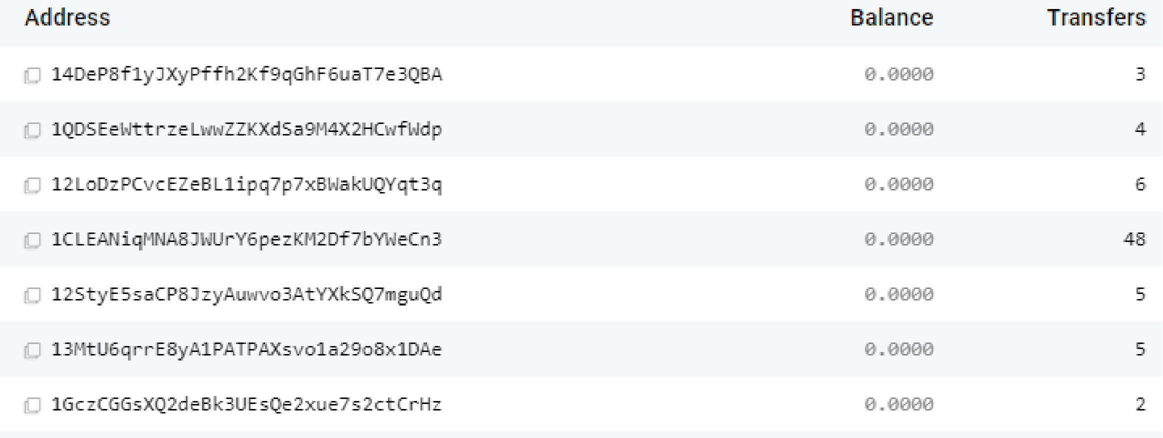
The following Electrum wallet stores 17 private keys with corresponding addresses:



Type	Address	Label	Balance	Tx
receiving	12LoDzPCvcEZeBL1ipq7p7xBWakUQYqt3q		0.	6
receiving	12StyE5saCP8JzyAuwvo3AtYXkSQ7mguQd		0.	5
receiving	13MtU6qrrE8yA1PATPAXsvo1a29o8x1DAe		0.	5
receiving	14DeP8f1yJXyPffh2Kf9qGhF6uaT7e3QBA		0.	3
receiving	155uG7vU5qNatd8LhsHtG1T98G4RYXqeHr		0.	2
receiving	15qiQdMmR71ubXpqcHkS1S4gRD46aqcQcQ		0.	2
receiving	16Nj2vwbcidN1miG5qFvY2iUSmeZ1cKTzy		0.	2
receiving	1AmAzjdPAbWMRTaFPzyL8vS51kBAKfc4KS		0.	2
receiving	1CLEANiqMNA8JWUrY6pezKM2Df7bYWeCn3		0.	48
receiving	1Dzhtsc7b69saTyMR8nrYE1mi4TwN9FxaT		0.	2
receiving	1GczCGGsXQ2deBk3UEsQe2xue7s2ctCrHz		0.	2
receiving	1HK1aQ4fZPtZMRFZH6LaFd9b7ya1rWhQnU		0.	2
receiving	1LjL471hTxuKiAp3yJLnuLBZ4k36iYQWLR		0.	2
receiving	1NPZ6yju4v9DexkJitarjpuENpfFZfo84g		0.	2
receiving	1NZJrwo6TbtQfXbNcKJsVhs32BDvzBij9U		0.	2
receiving	1PSrBLbTcuEyQALeZgs1MEEJ1snrtLhakY		0.	2
receiving	1QDSEeWttrzeLwwZZKXdSa9M4X2HCwfWdp		0.	4

However, when we try to display one of the addresses in Chainalysis, we get the following cluster with 7 addresses:



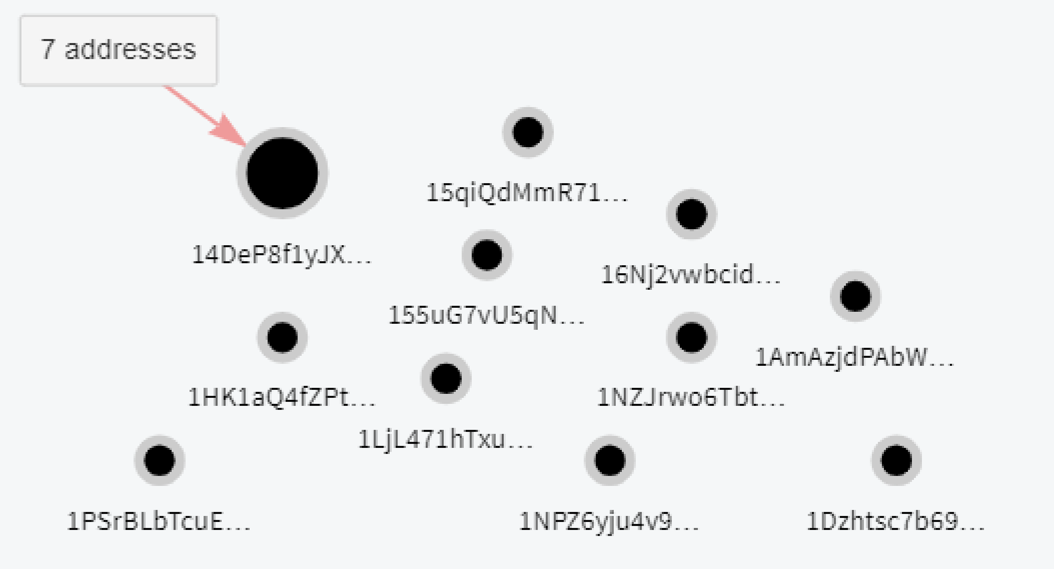


Address	Balance	Transfers
14DeP8f1yJXyPffh2Kf9qGhF6uaT7e3QBA	0.0000	3
1QDSEeWttrzeLwwZZKXdSa9M4X2HCwfWdp	0.0000	4
12LoDzPCvcEZeBL1ipq7p7xBWakUQYqt3q	0.0000	6
1CLEANiqMNA8JWUrY6pezKM2Df7bYWeCn3	0.0000	48
12StyE5saCP8JzyAuwvo3AtYXkSQ7mguQd	0.0000	5
13MtU6qrrE8yA1PATPAXsvo1a29o8x1DAe	0.0000	5
1GczCGGsXQ2deBk3UEsQe2xue7s2ctCrHz	0.0000	2

Where Did the Other 10 Addresses Go?

All addresses were involved in at least 2 transactions with a final balance of 0. This means these addresses had to receive BTC and spend it and therefore these addresses will certainly be recorded in the blockchain.

However, the tracing tool did not establish that the addresses belong to the same wallet so we can find the addresses in separate clusters:



Chainalysis identified one cluster containing 7 addresses, while the remaining 10 addresses were not added to the same cluster and contain 1 address each. Note that the addresses do not transact with each other so there is not much to suggest that all these addresses indeed belong to the same wallet.

Coming back to the correct terminology, what we see on the chart are:

- 1 wallet
- 11 clusters
- 17 addresses

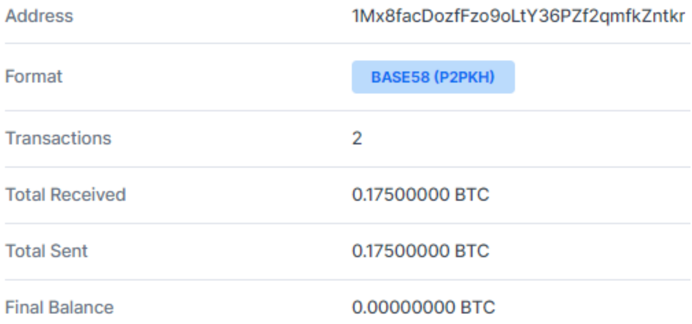
Q&A: Wallet v. Cluster v. Address

To review the understanding of the topic try to answer the following three questions:

1) Take a look at address *1Mx8facDozfFzo9oLtY36PZf2qmfkZntkr*. How many BTC did it receive?
2) How many addresses can we identify in the same cluster?
3) How many bitcoins were received by the same wallet?

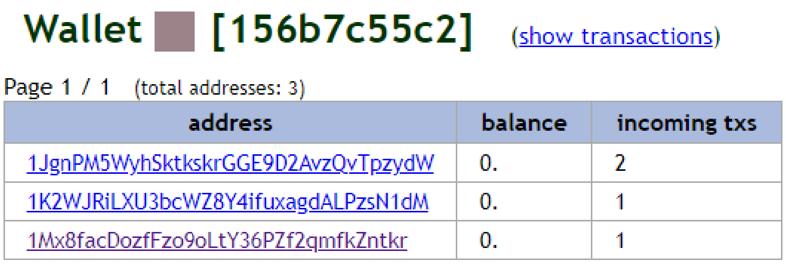
Answers:

1) The address received 0.175 BTC in 2016 as we can see in any blockchain explorer as these typically provide address-focused information; the amount was later fully spent.



Address	1Mx8facDozfFzo9oLtY36PZf2qmfkZntkr
Format	BASE58 (P2PKH)
Transactions	2
Total Received	0.17500000 BTC
Total Sent	0.17500000 BTC
Final Balance	0.00000000 BTC

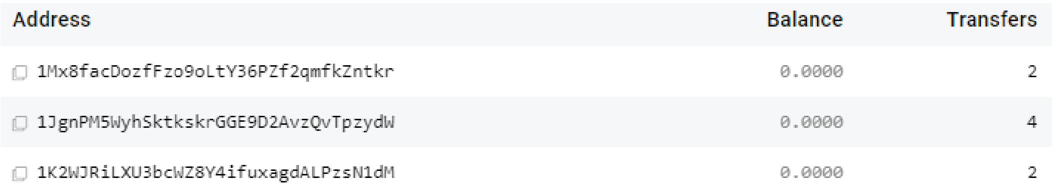
2) Commercial tracing tools aggregate addresses into clusters and each tool uses different logic and methods so the number of addresses in the cluster may vary across the tools. In this particular case, we will get the same information from publicly available Walletexplorer as from Chainalysis – 3 addresses in the cluster:



Wallet ■ [156b7c55c2] (show transactions)

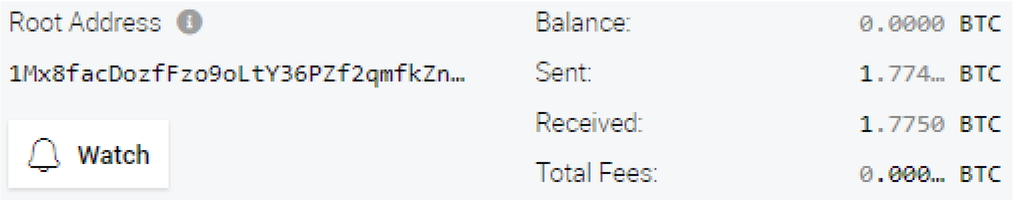
Page 1 / 1 (total addresses: 3)

address	balance	incoming txs
1JgnPM5WyhSktkskrGGE9D2AvzQvTpzydW	0.	2
1K2WJRiLXU3bcWZ8Y4ifuxagdALPzsN1dM	0.	1
1Mx8facDozfFzo9oLtY36PZf2qmfkZntkr	0.	1



Address	Balance	Transfers
1Mx8facDozfFzo9oLtY36PZf2qmfkZntkr	0.0000	2
1JgnPM5WyhSktkskrGGE9D2AvzQvTpzydW	0.0000	4
1K2WJRiLXU3bcWZ8Y4ifuxagdALPzsN1dM	0.0000	2

3) By now we should be familiar with the difference between a cluster and a wallet. The entity we see on the screen is a cluster and one wallet may be visualized as one or more clusters. Therefore, we know that the cluster of three identified addresses gives us a total of 1.775 BTC:



Root Address		
1Mx8facDozfFzo9oLtY36PZf2qmfkZn…	Balance:	0.0000 BTC
	Sent:	1.774… BTC
	Received:	1.7750 BTC
	Total Fees:	0.000… BTC

However, the actual number of addresses in the wallet may be higher and therefore the amount received by all addresses is unknown. Due to conservative clustering employed by the tools it is safe to say that the wallet should have received at least 1.775 BTC.

Bitcoin / Altcoin Address Autocomplete

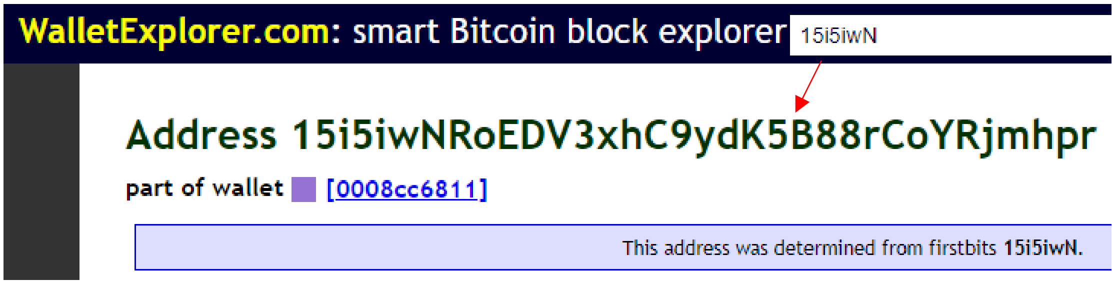
Due to the length of BTC addresses, these are more often copy/pasted rather than typed out. However, all cryptocurrency investigators will sooner or later get into a position where they have to transcribe addresses that are found on hardcopies, stored as an image or displayed on another mobile or computer screen. Even worse, investigators can find themselves in a situation when they only know part of the address.

To deal with this issue, the commercial tracing tools have an autocomplete feature, where typically 7 or 8 characters allow for determining the full bitcoin address.

Most publicly available free blockchain explorers, including Blockchain.com, have not yet adopted autocomplete. However, Walletexplorer and Smartbit implemented this feature. Be careful when using Walletexplorer though – if there are multiple addresses that match the initial string, it will show only one of the addresses. Therefore, you should double-check whether the address corresponds to the address you aimed to enter.

Examples:

Walletexplorer autocomplete:



WalletExplorer.com: smart Bitcoin block explorer

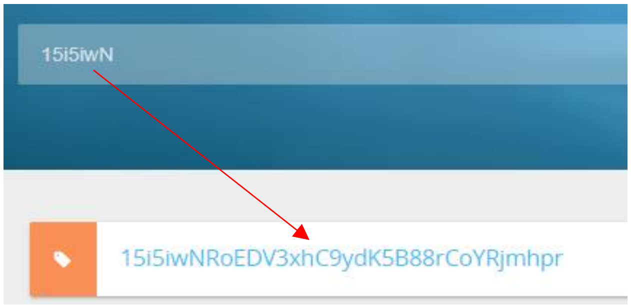
15i5iwN

Address 15i5iwNRoEDV3xhC9ydK5B88rCoYRjmhpr

part of wallet [0008cc6811]

This address was determined from firstbits **15i5iwN**.

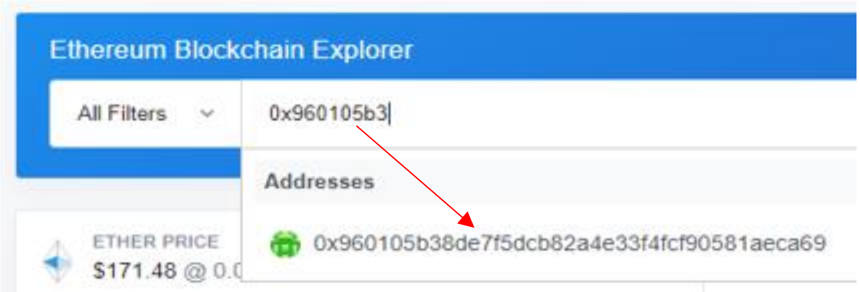
Smartbit autocomplete:



15i5iwN

15i5iwNRoEDV3xhC9ydK5B88rCoYRjmhpr

Altcoin blockchain explorers typically do not offer autocomplete. A notable exception here is Etherscan that autocompletes Ethereum addresses:



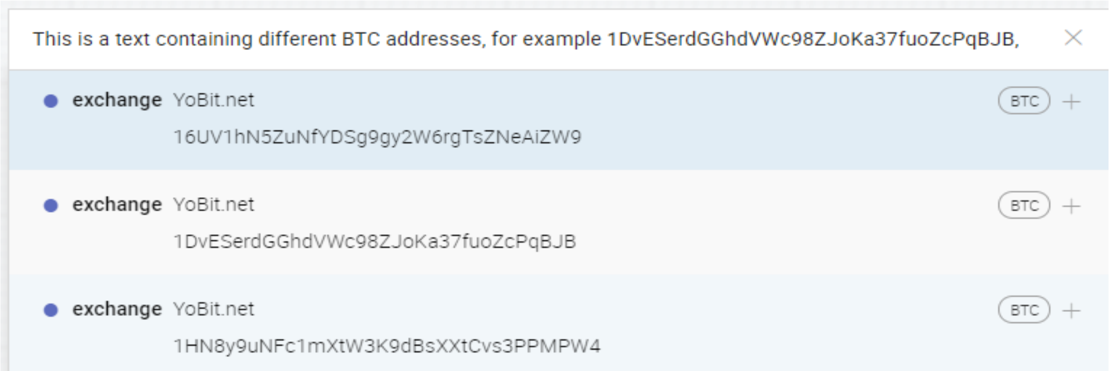
0x960105b3

0x960105b38de7f5dcb82a4e33f4fcf90581aeca69

Commercial tools make the input process even more convenient. Chainalysis can digest any text:

This is a text containing different BTC addresses, for example 1DvESerdGGhdVWc98ZJoKa37fuoZcPqBJB, 1HN8y9uNFc1mXtW3K9dBsXXtCvs3PPMPW4 and 16UV1hN5ZuNfYDSg9gy2W6rgTsZNeAiZW9

The superfluous information is taken out and the three above addresses will be added into the chart.



This is a text containing different BTC addresses, for example 1DvESerdGGhdVWc98ZJoKa37fuoZcPqBJB,

● **exchange** YoBit.net BTC +
16UV1hN5ZuNfYDSg9gy2W6rgTsZNeAiZW9

● **exchange** YoBit.net BTC +
1DvESerdGGhdVWc98ZJoKa37fuoZcPqBJB

● **exchange** YoBit.net BTC +
1HN8y9uNFc1mXtW3K9dBsXXtCvs3PPMPW4

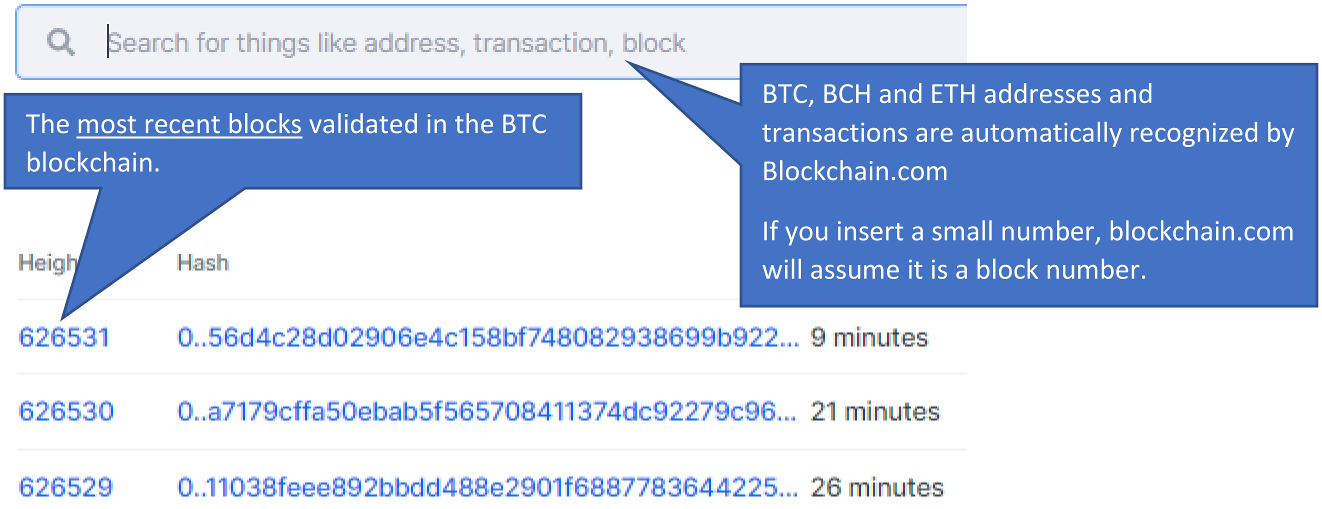
Sometimes, however, autocomplete can be a bit of a nuisance. When we try to add one of the above addresses (e.g., 1DvESerdGGhdVWc98ZJoKa37fuoZcPqBJB) into the chart, it will not be added as a single address. Instead, Chainalysis will include it as part of a wallet: in this case, a large exchange. If the wallet belongs to an exchange, it may easily contain over a million addresses.

This creates two problems. First, you will not be able to copy/paste the address autocompleted by Chainalysis as the address will be buried among many other addresses in the wallet. The workaround here would be to autocomplete the address in another tool.

More importantly, you cannot easily display incoming and outgoing transactions from the address, as you would be showing transactions of random users of the exchange. To display individual addresses in Chainalysis, you have to use so-called *custom clusters,* which will be discussed later in this guide.

Understanding Bitcoin Transactions

The Bitcoin blockchain is formed of blocks containing bitcoin transactions. Each of these is supposed to be mined on average once per 10 minutes so many blocks have been mined since bitcoin came into existence. The first block, mined on January 3, 2009, had a number (or height) of 0. In April 2021, the block-height grew to over 679,000.



Search for things like address, transaction, block

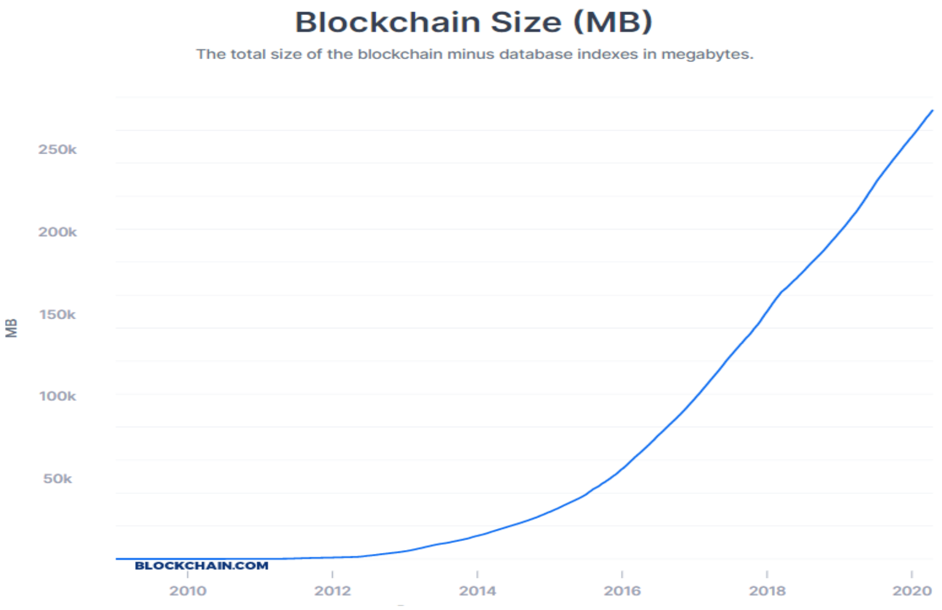
The most recent blocks validated in the BTC blockchain.

BTC, BCH and ETH addresses and transactions are automatically recognized by Blockchain.com

If you insert a small number, blockchain.com will assume it is a block number.

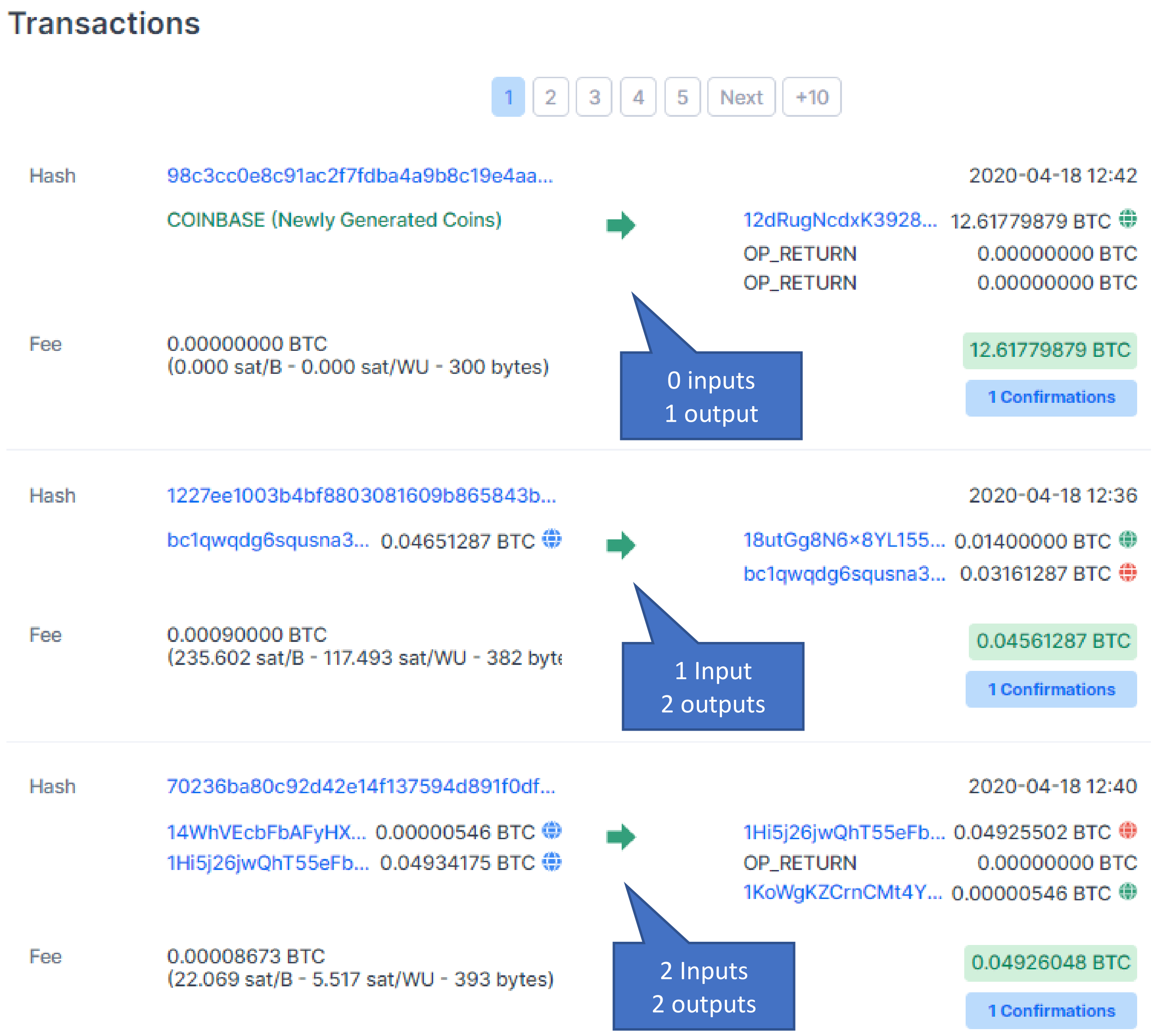
Heigh	Hash	
626531	0..56d4c28d02906e4c158bf748082938699b922...	9 minutes
626530	0..a7179cffa50ebab5f565708411374dc92279c96...	21 minutes
626529	0..11038feee892bbdd488e2901f6887783644225...	26 minutes

Each of the blocks contains transactions collected, verified and confirmed by the miner. The blocks are limited by size (1.3-1.4 Mb) and can fit up to almost 3,000 transactions. Since all the content is stored in the blockchain permanently, it is no surprise that its size has grown to over 330 Gb as of February 2021:



This means that for most investigators it is impractical to download and interpret the blockchain data directly. Instead, they choose to trust the publicly available or commercial tracing tools.

Bitcoin transactions are more complicated than bank account transfers, where there is one payer and one recipient account per transaction. In bitcoin blockchain, each of the transactions may have multiple inputs (addresses from which BTC is sent) and outputs (addresses receiving BTC):



Transactions

1 2 3 4 5 Next +10

Hash 98c3cc0e8c91ac2f7fdba4a9b8c19e4aa... 2020-04-18 12:42

COINBASE (Newly Generated Coins) → 12dRugNcdxK3928... 12.61779879 BTC
OP_RETURN 0.00000000 BTC
OP_RETURN 0.00000000 BTC

Fee 0.00000000 BTC
(0.000 sat/B - 0.000 sat/WU - 300 bytes)

0 inputs
1 output

12.61779879 BTC
1 Confirmations

Hash 1227ee1003b4bf8803081609b865843b... 2020-04-18 12:36

bc1qwqdg6squsna3... 0.04651287 BTC → 18utGg8N6x8YL155... 0.01400000 BTC
bc1qwqdg6squsna3... 0.03161287 BTC

Fee 0.00090000 BTC
(235.602 sat/B - 117.493 sat/WU - 382 byt

1 Input
2 outputs

0.04561287 BTC
1 Confirmations

Hash 70236ba80c92d42e14f137594d891f0df... 2020-04-18 12:40

14WhVEcbFbAFyHX... 0.00000546 BTC
1Hi5j26jwQhT55eFb... 0.04934175 BTC → 1Hi5j26jwQhT55eFb... 0.04925502 BTC
OP_RETURN 0.00000000 BTC
1KoWgKZCrnCMt4Y... 0.00000546 BTC

Fee 0.00008673 BTC
(22.069 sat/B - 5.517 sat/WU - 393 bytes)

2 Inputs
2 outputs

0.04926048 BTC
1 Confirmations

The next few pages will explain how to interpret these transactions.

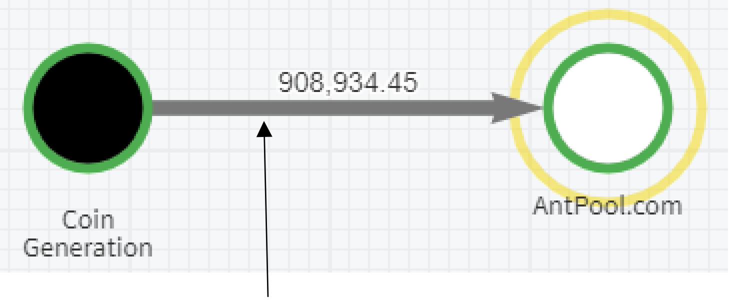
Interpreting Bitcoin Transactions - Inputs

We will focus on the input side first – the funds that are to be sent have to originate from somewhere and the origin can be:

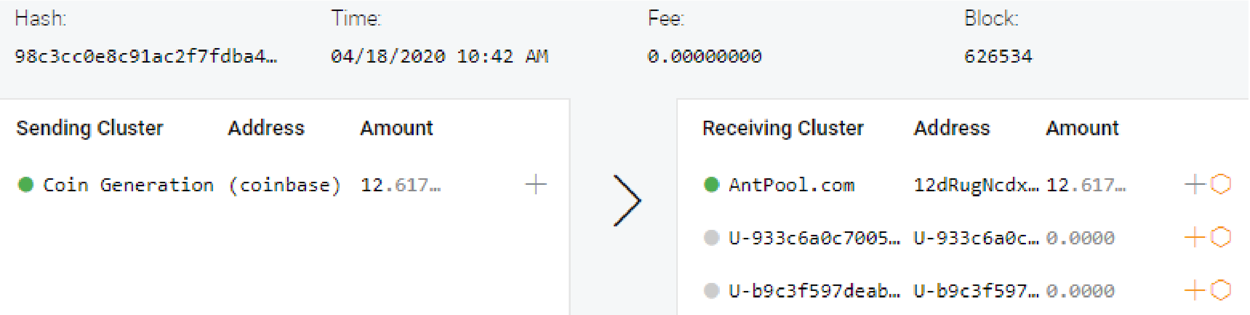
1) Zero input transactions

Whenever new bitcoins are mined, the corresponding transaction will have 0 inputs. For example, the first transaction on the previous page shows COINBASE (Newly Generated Coins) instead of an address on blockchain.com explorer. Note, that the term *COINBASE* used here means a transaction where the miner receives the reward and this has nothing to do with Coinbase exchange!

Commercial tools show such transactions as coin generation of newly mined coins that came out of nothing and are sent to an address of the Bitcoin miner. In Chainalysis, the transaction ID *98c3cc0e8c91ac2f7fdba4a9b8c19e4aada7be4a24f6e354ebf5626526eee393* would be displayed in the following way:



When we select the link to check all individual transactions where the reward was sent to the miner, including the one shown on the previous page:



Hash:	Time:	Fee:	Block:
98c3cc0e8c91ac2f7fdba4…	04/18/2020 10:42 AM	0.00000000	626534

Sending Cluster	Address	Amount
Coin Generation	(coinbase)	12.617…

Receiving Cluster	Address	Amount
AntPool.com	12dRugNcdx…	12.617…
U-933c6a0c7005…	U-933c6a0c…	0.0000
U-b9c3f597deab…	U-b9c3f597…	0.0000

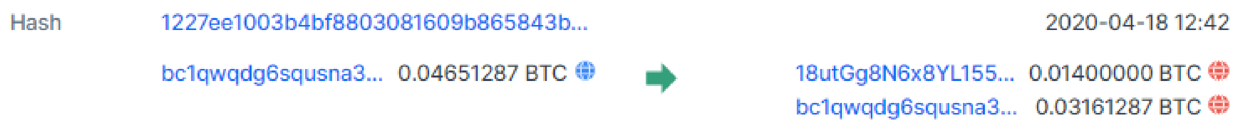
Therefore, the commercial tool displays the same transaction detail but with an additional benefit of an identified miner. The mining reward 12.61779879 BTC consists of two parts – a static reward of 12.5 BTC and 0.11779879 BTC from the transaction fees from all transactions the miner collected into the block. In May 2020, the static reward was halved to 6.25 BTC and in 2024 another halving will bring it to 3.125.

These transactions with 0 inputs are relatively rare – there is only one transaction per block that generates the new coins. The miners will put it at the first position in the block they mine.

Typically, these transactions are not directly connected to criminal activity and usually not subject to LE enquiries.

2) Single Input Transactions

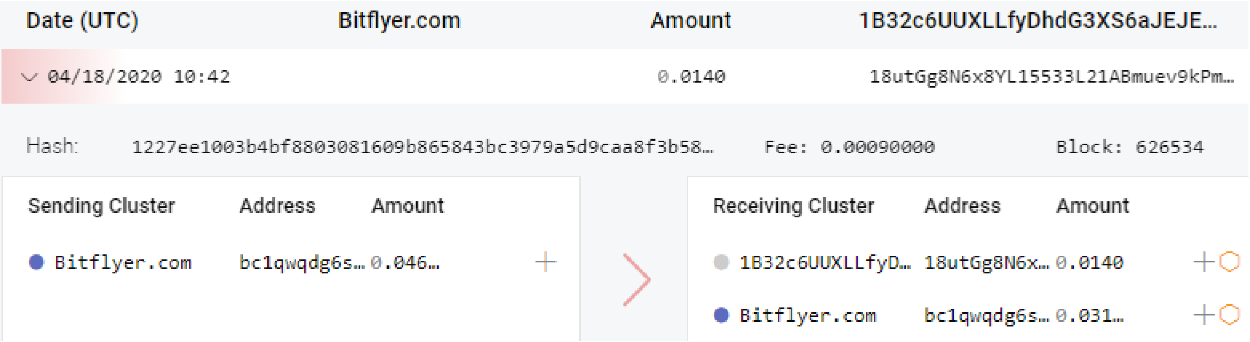
The following is an example of a much more common transaction that contains one input: *1227ee1003b4bf8803081609b865843bc3979a5d9caa8f3b58dd1f233dcf8e76*, first on blockchain.com:



Hash 1227ee1003b4bf8803081609b865843b... 2020-04-18 12:42

bc1qwqdg6squsna3... 0.04651287 BTC → 18utGg8N6x8YL155... 0.01400000 BTC
bc1qwqdg6squsna3... 0.03161287 BTC

Chainalysis provides attribution for this transaction. This time, the transaction represents a withdrawal from an exchange called Bitflyer:



Date (UTC)	Bitflyer.com	Amount	1B32c6UUXLLfyDhdG3XS6aJEJE...
04/18/2020 10:42		0.0140	18utGg8N6x8YL15533L21ABmuev9kPm...

Hash: 1227ee1003b4bf8803081609b865843bc3979a5d9caa8f3b58... Fee: 0.00090000 Block: 626534

Sending Cluster	Address	Amount
● Bitflyer.com	bc1qwqdg6s...	0.046...

Receiving Cluster	Address	Amount
● 1B32c6UUXLLfyD...	18utGg8N6x...	0.0140
● Bitflyer.com	bc1qwqdg6s...	0.031...

Just by looking at the above transaction, we know that the address bc1qwq... on the input side had to previously receive 0.04651287 BTC and now it has to spend this amount fully to make a payment.

This is how Bitcoin payments work – if an address receives one payment of 2 BTC, this amount is referred to as *UTXO* (*Unspent Transaction Output*). This transaction output has to be spent completely, so if receiver later pays 0.5 BTC, a full amount of 2 BTC will have to be spent to make the transaction happen. What happens with the rest of the bitcoins? As we will soon demonstrate, they will return to the sender's wallet.

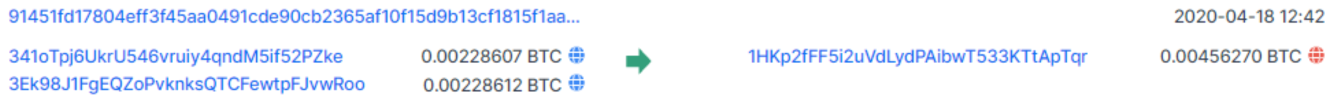
A single address may receive one or several UTXOs. In the latter case, the payment from the address can be made using one or more of these UTXOs depending on the amount of funds required for the transaction.

The Bitcoin wallet usually does the address administration in the background so the user does not have to be bothered about the process. The investigator, on the other hand, has to be able to explain what happened.

3) Multiple Input Transactions

Multiple input transactions are also common – this typically occurs when the amount of previously received funds on an address (UTXO) is not sufficient to send the payment or if the payer deliberately decides to spend multiple UTXOs. In such cases, multiple UTXOs are merged together in order to send the payment.

For example, in transaction 91451fd17804eff3f45aa0491cde90cb2365af10f15d9b13cf1815f1aa4fb6c3 the payer decided to fully spend two UTXOs. As a result, we can see a transaction with two inputs, where addresses spend previously received amounts of 0.00228607 and 0.00228612 BTC respectively. And since all funds (minus a small transaction fee) land on the output address *1HKp2fFF…*, there is no need to return any unspent funds back to the payer:

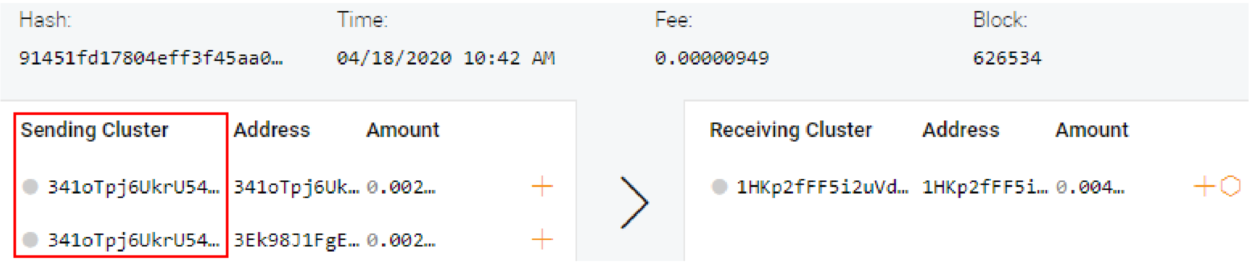


91451fd17804eff3f45aa0491cde90cb2365af10f15d9b13cf1815f1aa...				2020-04-18 12:42
341oTpj6UkrU546vruiy4qndM5if52PZke	0.00228607 BTC	➡	1HKp2fFF5i2uVdLydPAibwT533KTtApTqr	0.00456270 BTC
3Ek98J1FgEQZoPvknksQTCFewtpFJvwRoo	0.00228612 BTC			

The fact that the two addresses are on the input side of the above transaction indicates that <u>both addresses were in the same wallet</u>. In order to send the transaction, a wallet had to retrieve private keys to both addresses to sign the transaction. This occurs in real-time as soon as the user hits the send button in the wallet.

We can merge all addresses on the input side of the transaction and consider these to be sent from the same wallet. This is often referred to as the "*co-spend heuristics*" as the addresses were assigned into the same cluster based on their co-spending behaviour.

Analysing this transaction using Chainalysis does not provide any attribution. However, the tool confirms the rule we have just learned – the two addresses on the input side indeed belong to the same cluster:

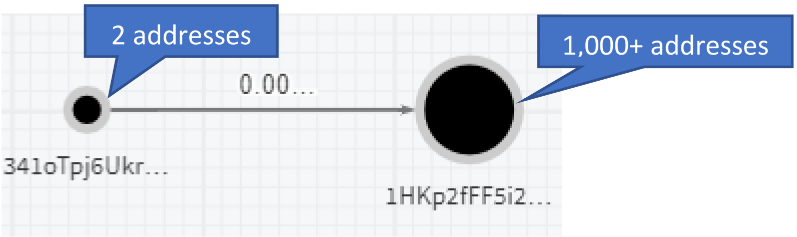


Hash:	Time:	Fee:	Block:
91451fd17804eff3f45aa0…	04/18/2020 10:42 AM	0.00000949	626534

Sending Cluster	Address	Amount
341oTpj6UkrU54…	341oTpj6Uk…	0.002…
341oTpj6UkrU54…	3Ek98J1FgE…	0.002…

Receiving Cluster	Address	Amount
1HKp2fFF5i2uVd…	1HKp2fFF5i…	0.004…

Looking at this transaction using a commercial tracing tool, we can also come to the following assumption: There are only two addresses present in cluster *341oTpj6…* This may represent a private wallet. The funds are very likely moving to a different wallet as indicated by a different format of the receiving address starting with number *1*. Since the receiving cluster contains a very large number of addresses and transactions, it is very likely managed by a service the tool failed to identify:

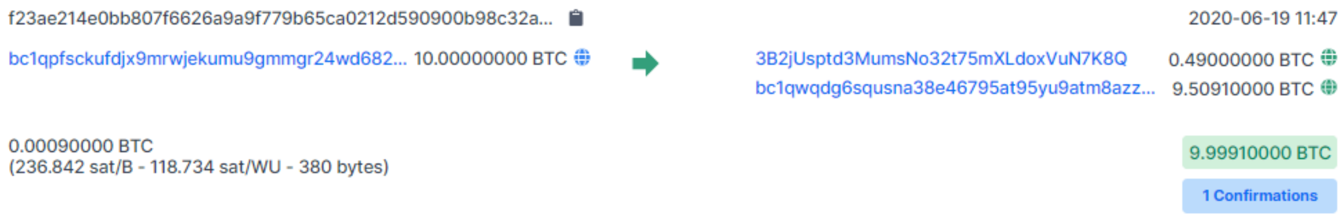


Interpreting Bitcoin Transactions – Outputs

In order to investigate the flow of funds, it is necessary to understand different types of bitcoin transactions and to interpret their meaning.

The most often seen type of transaction looks like the one below – with 1 input and 2 outputs:

Example: f23ae214e0bb807f6626a9a9f779b65ca0212d590900b98c32a45274ceab7de9



f23ae214e0bb807f6626a9a9f779b65ca0212d590900b98c32a...

2020-06-19 11:47

bc1qpfsckufdjx9mrwjekumu9gmmgr24wd682... 10.00000000 BTC

3B2jUsptd3MumsNo32t75mXLdoxVuN7K8Q 0.49000000 BTC

bc1qwqdg6squsna38e46795at95yu9atm8azz... 9.50910000 BTC

0.00090000 BTC
(236.842 sat/B - 118.734 sat/WU - 380 bytes)

9.99910000 BTC

1 Confirmations

How to interpret this transaction:

The transaction has a unique ID f23ae…; there is no other transaction with this ID in the bitcoin blockchain. Looking at the transaction, we see that an address bc1qpf… is spending 10 BTC. This means that the address spends 10 BTC it previously received in course of one or multiple transactions. The 10 BTC are thus deducted from the balance of this address.

Where do the 10 BTC go? 9.9991 BTC is sent to two addresses on the output side, 3B2jU… and bc1qwq… The remainder, which is 0.0009 BTC is a transaction fee. This is paid by the party making the payment – the owner of bc1qpf… The payer decides how large the transaction fee is; to make sure the fee is adequate the amount is typically suggested by the wallet. The fee is independent of the amount transferred; instead it is affected by size of the transaction in bytes – the larger the transaction the higher the fee.

Note that the fee is not shown on the output side. The reason is that the fee will be collected by a miner and at the time the transaction is constructed and signed by the payer it is not yet known who the lucky miner will be so there is no way of knowing his address.

Understanding Change Address

In traditional financial transfers, there is typically only one account sending the payment and one receiving the payment. Therefore, it may seem counter-intuitive to see multiple addresses on the output side; One of these has to be the recipient, so what is the explanation for the second address?

Bitcoin and most other cryptocurrencies use a so-called change address. This means they fully spend the previously received amount to send funds to a recipient's address and the remainder is returned back to the wallet that sent the transaction.

Since this may sound a bit abstract, let's demonstrate it by using the above transaction:

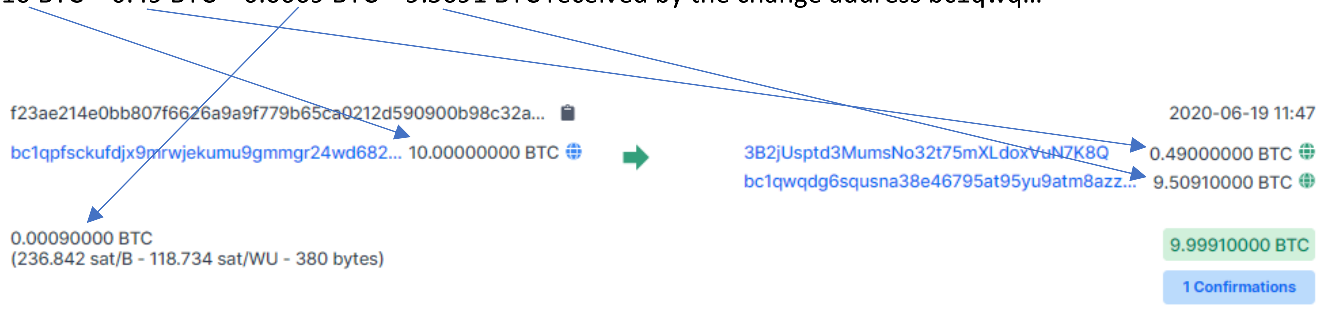
The address bc1qpf… is spending the full amount of 10 BTC it previously received. However, since the payer sent a smaller amount, the remainder will be sent to the change address.

Therefore, we can express it by the following simple formula:

Amount sent – Amount received by the recipient – Transaction fee = Amount sent to the change address

Which, applied on the transaction means:

10 BTC – 0.49 BTC – 0.0009 BTC = 9.5091 BTC received by the change address bc1qwq…



f23ae214e0bb807f6626a9a9f779b65ca0212d590900b98c32a… 2020-06-19 11:47

bc1qpfsckufdjx9mrwjekumu9gmmgr24wd682… 10.00000000 BTC

3B2jUsptd3MumsNo32t75mXLdoxVuN7K8Q 0.49000000 BTC

bc1qwqdg6squsna38e46795at95yu9atm8azz… 9.50910000 BTC

0.00090000 BTC
(236.842 sat/B - 118.734 sat/WU - 380 bytes)

9.99910000 BTC

1 Confirmations

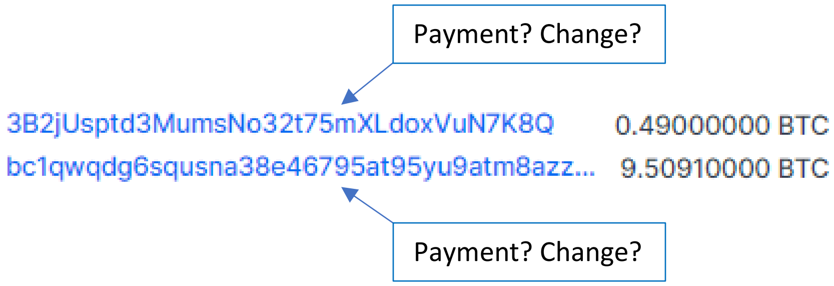
How many change addresses can there be in a transaction?

While there may be multiple addresses on both input and output sides, there is either no change – if the amount is fully spent and therefore there is no need for the change transaction – or one change address. There is no reason for multiple change addresses within the same transaction.

Determining Change Address

Now we know why the transaction had two addresses on the output side. However, looking at the transaction, it may be difficult to distinguish between the two addresses on the output side. One of them is an address of the recipient and the other one is the change. But which one is which?

In essence, there are nine ways that *may* help you to distinguish between the two:

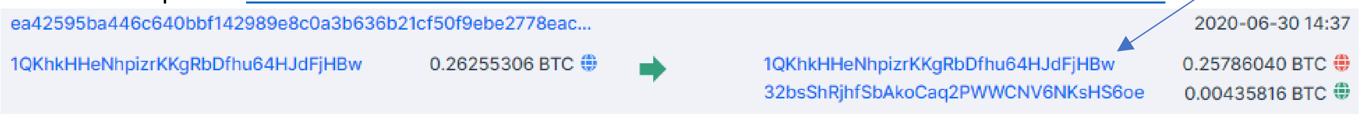


3B2jUsptd3MumsNo32t75mXLdoxVuN7K8Q 0.49000000 BTC
bc1qwqdg6squsna38e46795at95yu9atm8azz... 9.50910000 BTC

1) **Repeat addresses**

If the same address is featured on both input and output side, it is almost certainly a change address. In this scenario, the change returns not only back to payer's wallet but also to the same address.

Example: Tx ea42595ba446c640bbf142989e8c0a3b636b21cf50f9ebe2778eac921dc8550c



ea42595ba446c640bbf142989e8c0a3b636b21cf50f9ebe2778eac... 2020-06-30 14:37
1QKhkHHeNhpizrKKgRbDfhu64HJdFjHBw 0.26255306 BTC → 1QKhkHHeNhpizrKKgRbDfhu64HJdFjHBw 0.25786040 BTC
32bsShRjhfSbAkoCaq2PWWCNV6NKsHS6oe 0.00435816 BTC

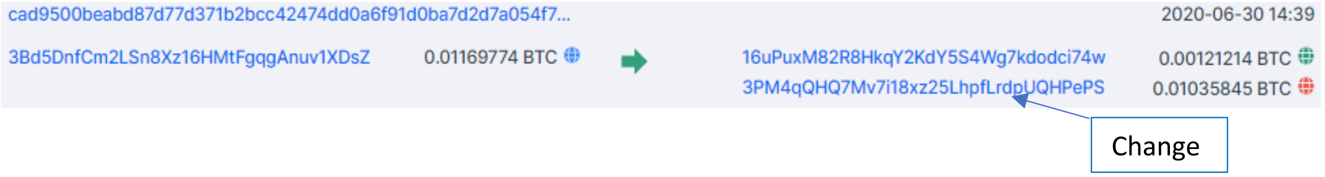
The address 1QKhkHHeNhpizrKKgRbDfhu64HJdFjHBw appears on both input and output side so we can assume this is the change. Consequently, our interpretation of the transaction is that the address 32bsShRjhfSbAkoCaq2PWWCNV6NKsHS6oe must have received the payment of 0.00435816 BTC while the change of 0.25786040 BTC returned back to payer's address.

2) **Repeat address format**

More often than not, the address on the input side is not repeated on the output side. Here we can resort to a much less accurate estimate based on the format of the address. Bitcoin addresses start with 1, 3 and bc1 and most wallets prefer to stick to one of these formats.

Therefore, a wallet from which an address starting with 1 sends funds to two addresses, one of them starting with 1 and the other one with 3, it is much more likely that the address starting with 1 is the change address. A wallet that has already created an address starting with number 1 has a higher probability of creating a change address starting with the same number:

Example: Tx cad9500beabd87d77d371b2bcc42474dd0a6f91d0ba7d2d7a054f7d025a96aec



cad9500beabd87d77d371b2bcc42474dd0a6f91d0ba7d2d7a054f7... 2020-06-30 14:39

3Bd5DnfCm2LSn8Xz16HMtFgqgAnuv1XDsZ	0.01169774 BTC	➡	16uPuxM82R8HkqY2KdY5S4Wg7kdodci74w	0.00121214 BTC
			3PM4qQHQ7Mv7i18xz25LhpfLrdpUQHPePS	0.01035845 BTC

Change

There are two addresses on the output side, one starting with 1 and the other with 3. Since the transaction originated from an address starting with number 3 (3Bd5DnfCm2LSn8Xz16HMtFgqgAnuv1XDsZ) it is more likely that the output address 3PM4qQHQ7Mv7i18xz25LhpfLrdpUQHPePS is the change and that consequently the payment was sent to 16uPuxM82R8HkqY2KdY5S4Wg7kdodci74w.

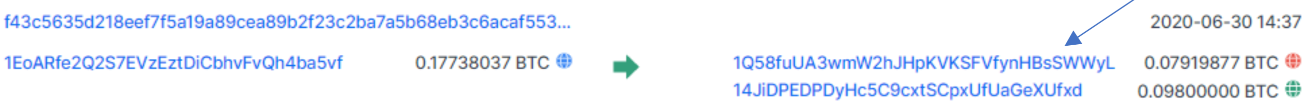
Naturally, the wallet algorithm may change over time, resulting in a possible change of the address format. However, if you trace transactions that take place in a reasonably short period apart (hours/days/weeks) you may assume that the wallet has not been updated in the meantime and the address format algorithm has remained unchanged. This method is not 100% reliable (practically nothing in cryptocurrency analysis is), however, you should still apply it to determine the change with a decent degree of certainty.

3) Round amount

People often prefer sending round numbers, such as 0.1 BTC – therefore the round amounts are typically suggesting the payment. The other amount is typically anything but round – based on calculation of the change on the previous page it is rather unlikely for the change amount to look like a round number:

Example: Tx f43c5635d218eef7f5a19a89cea89b2f23c2ba7a5b68eb3c6acaf553dc68fd79

Change



f43c5635d218eef7f5a19a89cea89b2f23c2ba7a5b68eb3c6acaf553... 2020-06-30 14:37

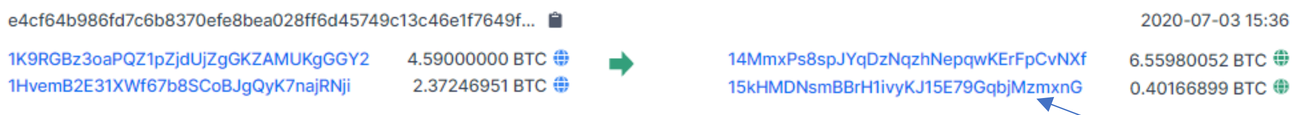
1EoARfe2Q2S7EVzEztDiCbhvFvQh4ba5vf	0.17738037 BTC	➡	1Q58fuUA3wmW2hJHpKVKSFVfynHBsSWWyL	0.07919877 BTC
			14JiDPEDPDyHc5C9cxtSCpxUfUaGeXUfxd	0.09800000 BTC

A round amount of 0.098 BTC was sent to 14JiDPEDPDyHc5C9cxtSCpxUfUaGeXUfxd. Therefore, this address has received the payment and consequently 1Q58fuUA3wmW2hJHpKVKSFVfynHBsSWWyL is the change address generated in the payer's wallet that received the non-round remainder.

4) Amount in a transaction with multiple inputs

Transaction can also have multiple input addresses. This typically happens when the sender attempts to send an amount that is higher than the amount available on one of his addresses. In such case, multiple input addresses have to be combined in order to send the payment.

Example: Tx e4cf64b986fd7c6b8370efe8bea028ff6d45749c13c46e1f7649f82f7aa60b83



e4cf64b986fd7c6b8370efe8bea028ff6d45749c13c46e1f7649f...   2020-07-03 15:36

1K9RGBz3oaPQZ1pZjdUjZgGKZAMUKgGGY2 4.59000000 BTC
1HvemB2E31XWf67b8SCoBJgQyK7najRNji 2.37246951 BTC

14MmxPs8spJYqDzNqzhNepqwKErFpCvNXf 6.55980052 BTC
15kHMDNsmBBrH1ivyKJ15E79GqbjMzmxnG 0.40166899 BTC

Change

In the above example, 4.59 BTC and 2.37246951 BTC are merged in order to send either 6.55980052 BTC or 0.40166899 BTC. Which one was it?
Naturally, it would make no sense to combine the addresses to send the smaller amount – in such case we would only have one address on the input side. Therefore, the amount sent had to be 6.55980052.

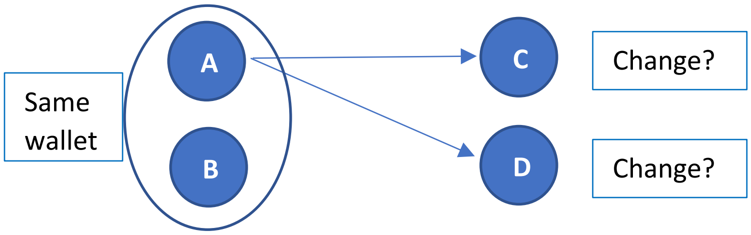
Transaction fee is calculated based on the size of a transaction in bytes and every additional input address that has to be signed increases the fee. As a result, the majority of wallets try to minimize the cost for the user and automatically choose the lowest possible number of inputs. Hence, merging two large input amounts only to pay 0.40166899 BTC would not make sense and therefore this has to be the change.

5) Observation of future transactions

If we observe historical transactions, it is possible that future transactions will help us establish the change address. Consider the following example:

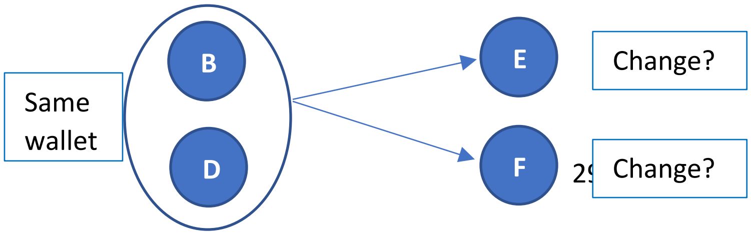
Let's assume a wallet contains addresses A and B. In the course of transaction 1, A sends funds to C and D and we do not know which one is the change.

Transaction 1:



Later, transaction 2 combines addresses B and D on the input side, sending funds to E and F. What does this mean? Since addresses B and D were together in the same wallet, D had to be the change address that was created in the wallet after transaction 1 and therefore C had to be the payment address.

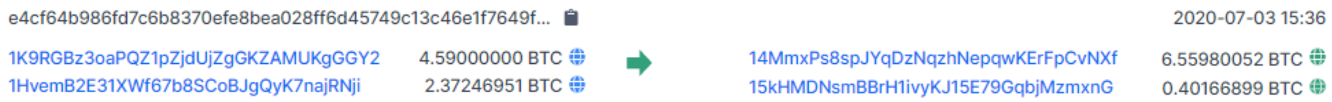
Transaction 2:



Thus, it may not have been possible to identify change address after transaction 1. However, the second transaction has proven that the change address in transaction 1 was address D.

6) Use of a commercial tool

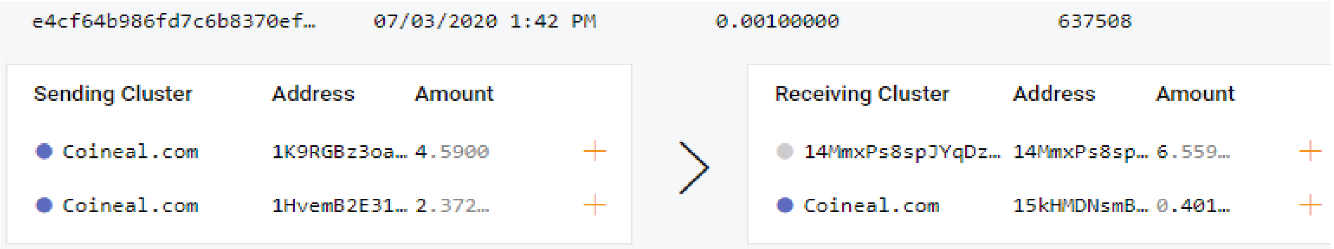
Commercial tools use some of the above methods to determine the change address. Consider again transaction e4cf64b986fd7c6b8370efe8bea028ff6d45749c13c46e1f7649f82f7aa60b83:



e4cf64b986fd7c6b8370efe8bea028ff6d45749c13c46e1f7649f... 2020-07-03 15:36

1K9RGBz3oaPQZ1pZjdUjZgGKZAMUKgGGY2	4.59000000 BTC	14MmxPs8spJYqDzNqzhNepqwKErFpCvNXf	6.55980052 BTC
1HvemB2E31XWf67b8SCoBJgQyK7najRNji	2.37246951 BTC	15kHMDNsmBBrH1ivyKJ15E79GqbjMzmxnG	0.40166899 BTC

Based on the amount we established, that address receiving 0.40166899 BTC should be the change address. Chainalysis validates this hypothesis as we see that the amount indeed returned to the address managed by the same entity:



e4cf64b986fd7c6b8370ef… 07/03/2020 1:42 PM 0.00100000 637508

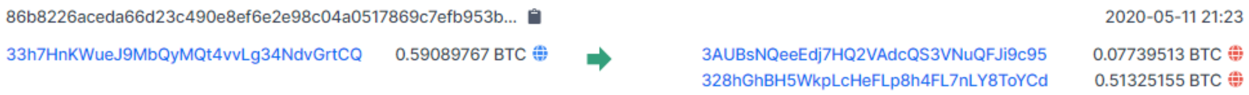
Sending Cluster	Address	Amount	Receiving Cluster	Address	Amount
Coineal.com	1K9RGBz3oa…	4.5900	14MmxPs8spJYqDz…	14MmxPs8sp…	6.559…
Coineal.com	1HvemB2E31…	2.372…	Coineal.com	15kHMDNsmB…	0.401…

7) Focus on metadata

Most investigators determine the change address by looking at the amounts or address format. However, many change addresses cannot be determined that easily and you will often encounter a scenario where it is nearly impossible to distinguish between the payment and the change address.

Consider the following scenario:

Transaction 86b8226aceda66d23c490e8ef6e2e98c04a0517869c7efb953be55ee9190ae3e has one input, two outputs. All outputs are in the same format, the output address does not appear on the input side, and the amounts do not give a clear indication of the change address:

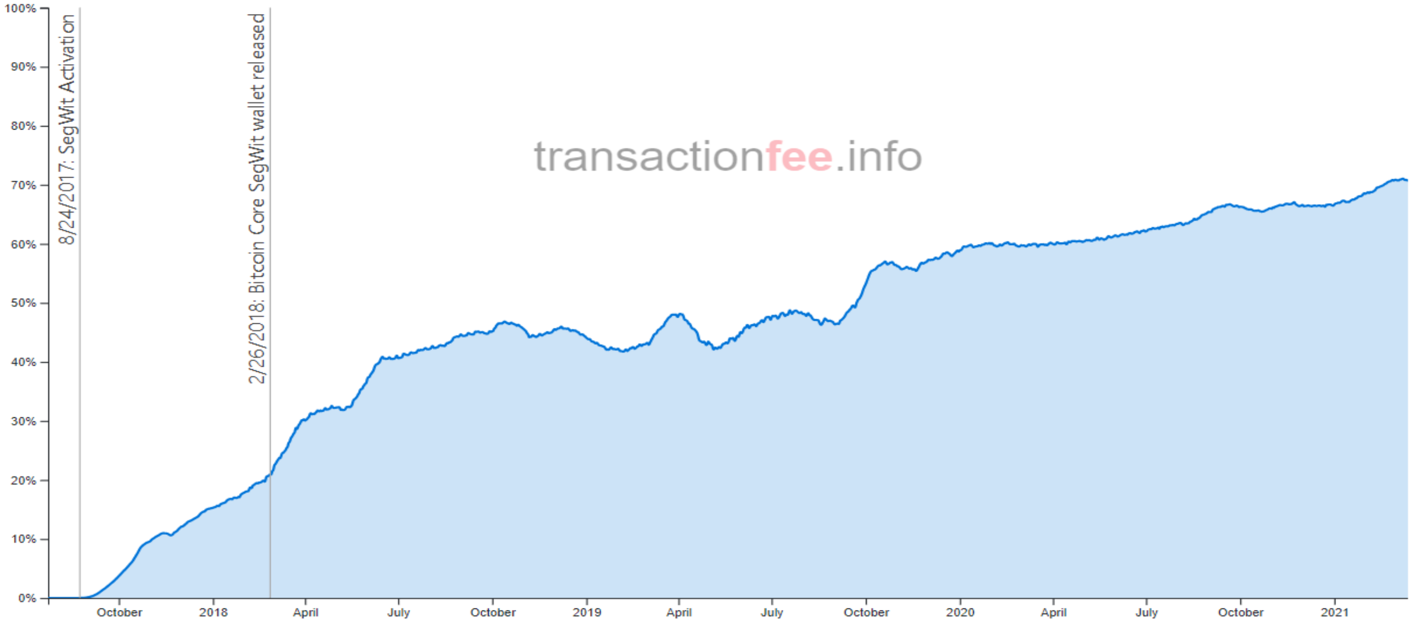


86b8226aceda66d23c490e8ef6e2e98c04a0517869c7efb953b... 2020-05-11 21:23

33h7HnKWueJ9MbQyMQt4vvLg34NdvGrtCQ	0.59089767 BTC	3AUBsNQeeEdj7HQ2VAdcQS3VNuQFJi9c95	0.07739513 BTC
		328hGhBH5WkpLcHeFLp8h4FL7nLY8ToYCd	0.51325155 BTC

On the first sight, there is nothing here to help us. However, we could use different tools to find the metadata including version, indication of *Segwit, transaction version, multisignature, type of multisignature and locktime*.

Segwit, or *Segregated Witness* was a change in protocol that separated transactions from signatures, which resulted in several improvements including a higher number of transactions that can be stored within one block. The upgrade took place in 2017, however, it took some time before the share of Segwit transactions adoption increased. In March 2021, 70% of Bitcoin transactions are Segwit transactions:



Source: *https://transactionfee.info/charts/payments-spending-segwit/*

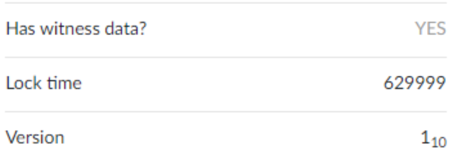
How to recognize whether the address is Segwit?

Address format	**Segwit?**
Address starting with 1…	Not Segwit!
Address starting with 3…	May be Segwit…
Address starting with bc1…	Segwit!

Thus, all addresses starting with bc1 are SegWit addresses, while some addresses starting with 3 and none of the addresses starting with 1 are Segwit addresses.

Transaction version is another useful attribute; It can either be 1 or 2. Version 2 has been available for many years but some wallets still create transaction with version 1.

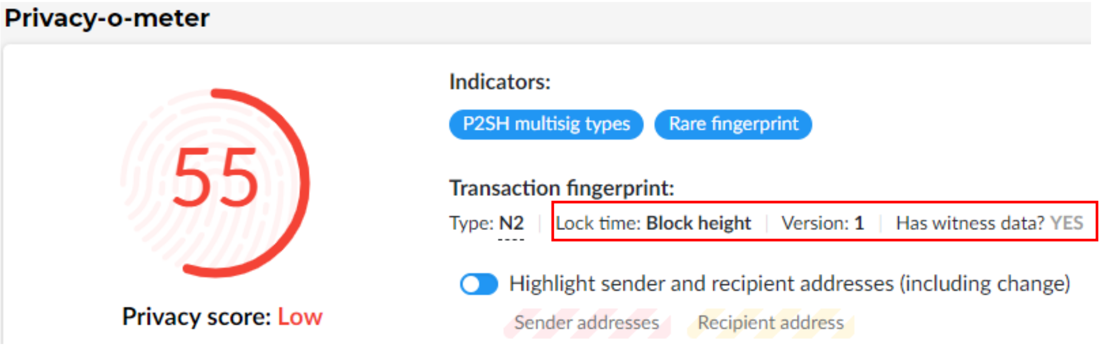
Consider displaying the transaction on blockchain.com and blockchair. While blockchain.com does not give any indication of Segwit or Version, the information is visible on blockchair (you may need to click on *Click to see more*):



Has witness data?	YES
Lock time	629999
Version	1_{10}

Here we see that the transaction is Segwit (it has witness data) and version 1.

Blockchair also offers a tool called Privacy-o-meter, that can help identify payment and the change:



Privacy-o-meter

55

Privacy score: Low

Indicators:

P2SH multisig types | Rare fingerprint

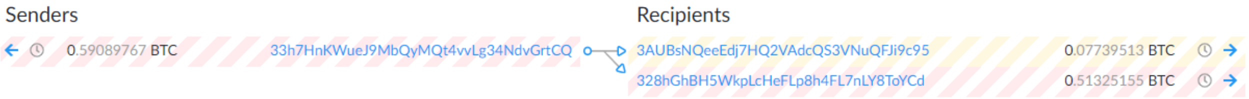
Transaction fingerprint:

Type: N2 | Lock time: Block height | Version: 1 | Has witness data? YES

Highlight sender and recipient addresses (including change)

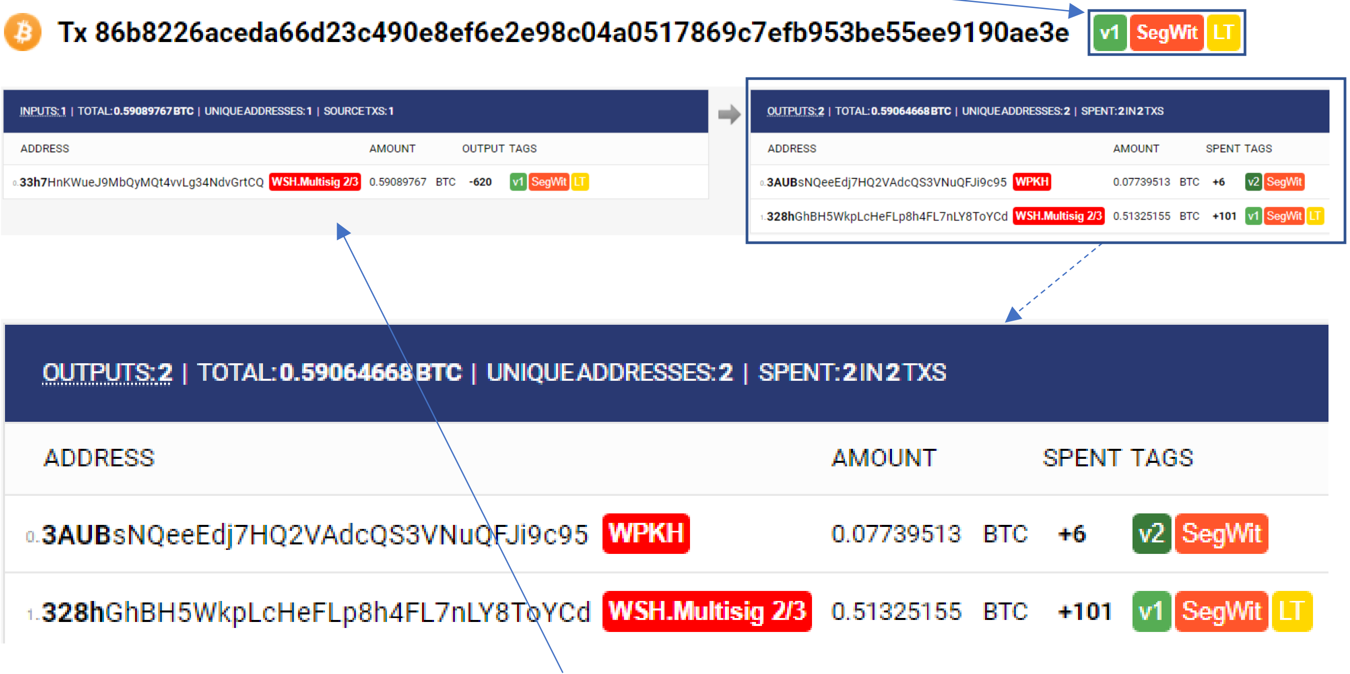
Sender addresses | Recipient address

On many occasions, the tool can highlight the change address with red colour and the payment with yellow. Here it indicates that the second address on the Output side – 328hG… is the change:



Senders		Recipients	
0.59089767 BTC	33h7HnKWueJ9MbQyMQt4vvLg34NdvGrtCQ	3AUBsNQeeEdj7HQ2VAdcQS3VNuQFJi9c95	0.07739513 BTC
		328hGhBH5WkpLcHeFLp8h4FL7nLY8ToYCd	0.51325155 BTC

Commercial tools can also offer additional metadata information. Chainalysis offers a blockchain explorer BEX that displays the following data about the transaction. The transaction has been signed from version 1 wallet that uses Segwit and Locktime:



Tx 86b8226aceda66d23c490e8ef6e2e98c04a0517869c7efb953be55ee9190ae3e v1 SegWit LT

INPUTS:1 | TOTAL:**0.59089767 BTC** | UNIQUE ADDRESSES:**1** | SOURCE TXS:**1**

ADDRESS	AMOUNT			OUTPUT TAGS
0.**33h7**HnKWueJ9MbQyMQt4vvLg34NdvGrtCQ WSH.Multisig 2/3	0.59089767	BTC	**-620**	v1 SegWit LT

OUTPUTS:2 | TOTAL:**0.59064668 BTC** | UNIQUE ADDRESSES:**2** | SPENT:**2 IN 2 TXS**

ADDRESS	AMOUNT			SPENT TAGS
0.**3AUB**sNQeeEdj7HQ2VAdcQS3VNuQFJi9c95 WPKH	0.07739513	BTC	**+6**	v2 SegWit
1.**328h**GhBH5WkpLcHeFLp8h4FL7nLY8ToYCd WSH.Multisig 2/3	0.51325155	BTC	**+101**	v1 SegWit LT

OUTPUTS:2 | TOTAL:0.59064668 BTC | UNIQUE ADDRESSES:2 | SPENT:2 IN 2 TXS

ADDRESS AMOUNT SPENT TAGS

0.3AUBsNQeeEdj7HQ2VAdcQS3VNuQFJi9c95 WPKH 0.07739513 BTC +6 v2 SegWit

1.328hGhBH5WkpLcHeFLp8h4FL7nLY8ToYCd WSH.Multisig 2/3 0.51325155 BTC +101 v1 SegWit LT

Also, we can see that the input address used multisignature 2/3 – this means that at least two private keys out of three associated with this address have to sign the transaction in order to make the payment.

Assuming the change address will later create a transaction using the same or very similar metadata we compare the change candidates:

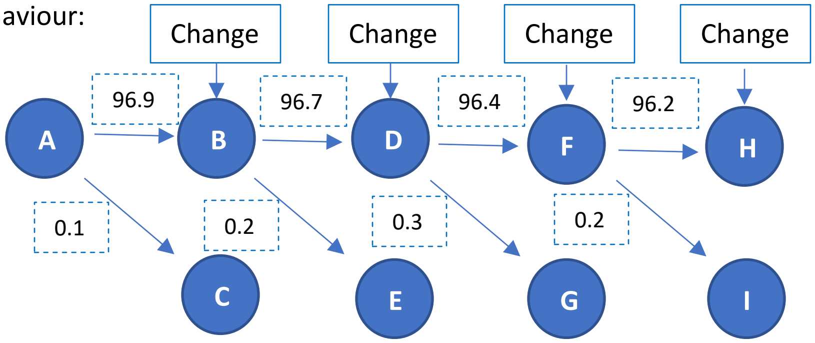
Address 3AUBs…	version 2	Segwit yes	Lock Time no	Multisig no
Address 328hG…	version 1	Segwit yes	Lock Time no	Multisig 2/3

The logic here is simple – you check the parameters of the transaction sent by the user's wallet and compare it to the parameters of the outputs. The more similarities there are, the higher the likelihood that the output is a change address.

Given the fact that the transaction was sent with version 1 and locktime and the input address used segwit 2/3, we see it is much more similar to change address candidate 2 – and therefore it is much more likely that the change address is 328hG.

8) Follow the patterns

If none of the above steps give us a good indication, we have to make assumptions based on multiple transactions and consider whether these are made by the same person. Consider the following peeling behaviour:



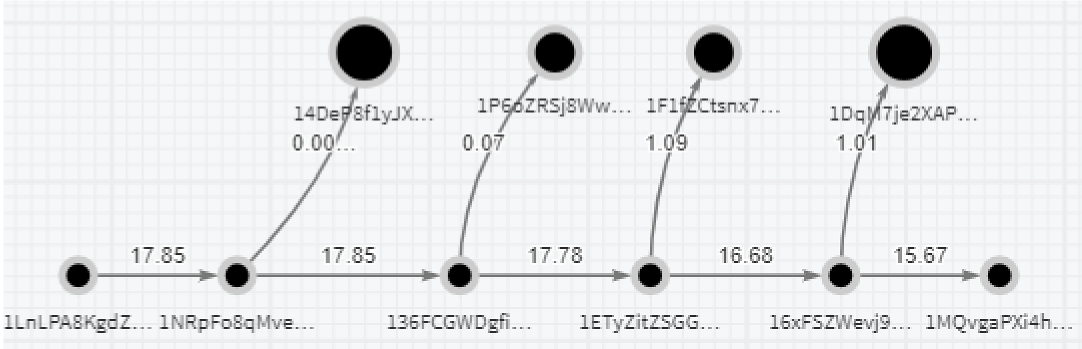
On the above BTC flow, address A has 97 BTC. We can see the peeling pattern, which makes it obvious that addresses C, E, G and I are other wallets receiving payments, while the slowly decreasing main stash of funds kept returning back to the original wallet on addresses B, D F and H.

Even after the first transaction, it was a bit more likely that someone sends 0.1 BTC and receives the remaining 96.9 BTC back, rather than sending almost everything and having some breadcrumbs coming back. After checking the subsequent transactions, the picture became clearer.

There are other patterns to watch out for – we can check the time of the transactions to find out whether these are sent within consistent time frames, fee per byte that could be relatively consistent for each wallet across transactions done within several hours or services the user regularly interacts with.

Understanding the peeling chain is important – often you can follow the change addresses in order to find out what the suspect does with his funds after his peeling chain behaviour ends.

The following chart shows a practical example of the peel chain – we start with address *1LnLPA8KgdZwSn7NmFTfj18w95TcDG4Us8* and by following its subsequent transactions the pattern quickly emerges – a small amount of funds is sent to other parties, either private wallets or unidentified services, while the main chunk of funds keeps coming back to new change addresses created by the same wallet:

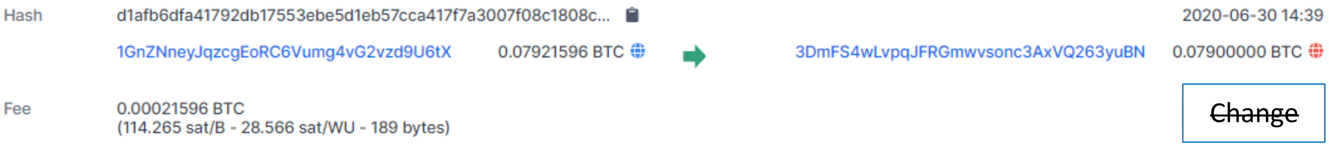


Here we can visually establish the change addresses (1NRpF, 136FCG, 1ETyZi, 16xFSZ and 1MQvga) and claim, with a high degree of probability, that these belong to the same wallet as the initial 1LnLP. address.

9) No change

If there is only one address on the output side, we can consider this to be the payment to the recipient. The full amount that was sent minus the transaction fee is received by the address on the output side – so there is no need to return any change back to the payer.

No change address: Tx d1afb6dfa41792db17553ebe5d1eb57cca417f7a3007f08c1808c06697078e87



Hash d1afb6dfa41792db17553ebe5d1eb57cca417f7a3007f08c1808c... 2020-06-30 14:39

1GnZNneyJqzcgEoRC6Vumg4vG2vzd9U6tX 0.07921596 BTC → 3DmFS4wLvpqJFRGmwvsonc3AxVQ263yuBN 0.07900000 BTC

Fee 0.00021596 BTC
(114.265 sat/B - 28.566 sat/WU - 189 bytes)

~~Change~~

Address 1GnZNneyJqzcgEoRC6Vumg4vG2vzd9U6tX sent all funds (0.07921596 BTC) minus transaction fee of 0.00021596 BTC to 3DmFS4wLvpqJFRGmwvsonc3AxVQ263yuBN, which received 0.079 BTC so there was nothing left to return to the payer.

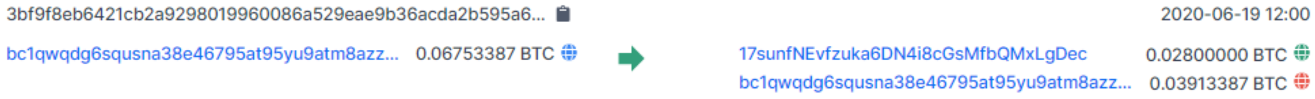
This transaction is often popular when a cryptocurrency user wishes to send all funds from one wallet onto another. Very often, this transaction shows no change of ownership.

This makes sense, as typically when a person makes a payment for goods or services or sends funds to someone else, it is common to send a specific amount rather than all the funds that are sitting on one or multiple addresses in the wallet. Hence, if a user sends exactly the amount assigned to one or more of his addresses in one output, there is no need for change, which often means that the output address is still managed by the same person.

Exercise – A Payment or a Change?:

Take a look at the following eight transactions and identify the change addresses:

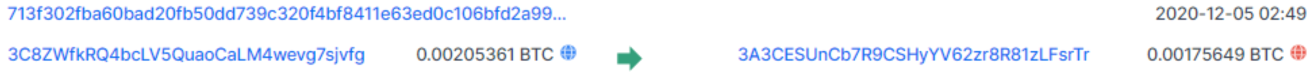
1) Tx 3bf9f8eb6421cb2a9298019960086a529eae9b36acda2b595a6f720b1e1ec9c3



3bf9f8eb6421cb2a9298019960086a529eae9b36acda2b595a6... 2020-06-19 12:00

bc1qwqdg6squsna38e46795at95yu9atm8azz... 0.06753387 BTC ➡ 17sunfNEvfzuka6DN4i8cGsMfbQMxLgDec 0.02800000 BTC
bc1qwqdg6squsna38e46795at95yu9atm8azz... 0.03913387 BTC

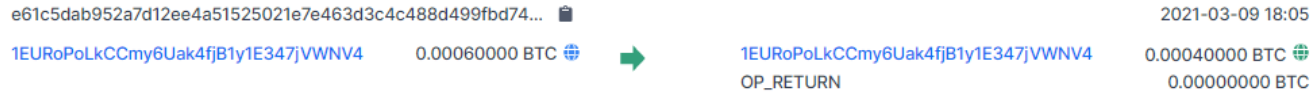
2) Tx: 713f302fba60bad20fb50dd739c320f4bf8411e63ed0c106bfd2a994e6743e74



713f302fba60bad20fb50dd739c320f4bf8411e63ed0c106bfd2a99... 2020-12-05 02:49

3C8ZWfkRQ4bcLV5QuaoCaLM4wevg7sjvfg 0.00205361 BTC ➡ 3A3CESUnCb7R9CSHyYV62zr8R81zLFsrTr 0.00175649 BTC

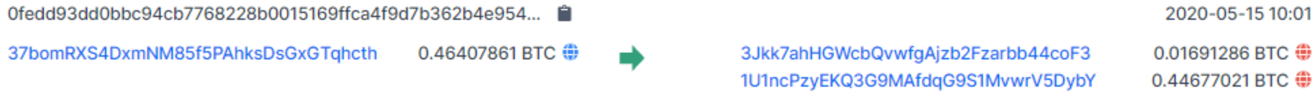
3) Tx: e61c5dab952a7d12ee4a51525021e7e463d3c4c488d499fbd74ba0d14de2edc7



e61c5dab952a7d12ee4a51525021e7e463d3c4c488d499fbd74... 2021-03-09 18:05

1EURoPoLkCCmy6Uak4fjB1y1E347jVWNV4 0.00060000 BTC ➡ 1EURoPoLkCCmy6Uak4fjB1y1E347jVWNV4 0.00040000 BTC
OP_RETURN 0.00000000 BTC

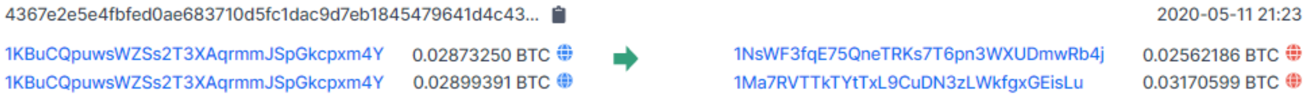
4) Tx: 0fedd93dd0bbc94cb7768228b0015169ffca4f9d7b362b4e954207e2990a5d96



0fedd93dd0bbc94cb7768228b0015169ffca4f9d7b362b4e954... 2020-05-15 10:01

37bomRXS4DxmNM85f5PAhksDsGxGTqhcth 0.46407861 BTC ➡ 3Jkk7ahHGWcbQvwfgAjzb2Fzarbb44coF3 0.01691286 BTC
1U1ncPzyEKQ3G9MAfdqG9S1MvwrV5DybY 0.44677021 BTC

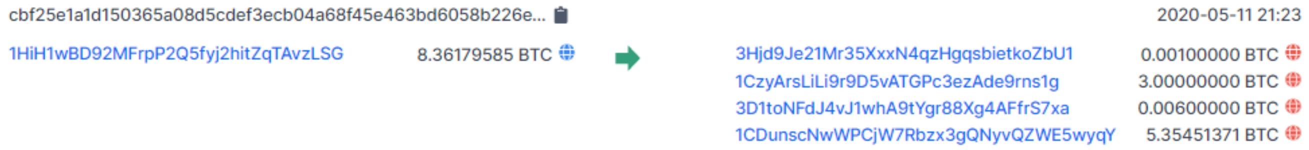
5) Tx: 4367e2e5e4fbfed0ae683710d5fc1dac9d7eb1845479641d4c43ff2df5809119



4367e2e5e4fbfed0ae683710d5fc1dac9d7eb1845479641d4c43... 2020-05-11 21:23

1KBuCQpuwsWZSs2T3XAqrmmJSpGkcpxm4Y 0.02873250 BTC
1KBuCQpuwsWZSs2T3XAqrmmJSpGkcpxm4Y 0.02899391 BTC ➡ 1NsWF3fqE75QneTRKs7T6pn3WXUDmwRb4j 0.02562186 BTC
1Ma7RVTTkTYtTxL9CuDN3zLWkfgxGEisLu 0.03170599 BTC

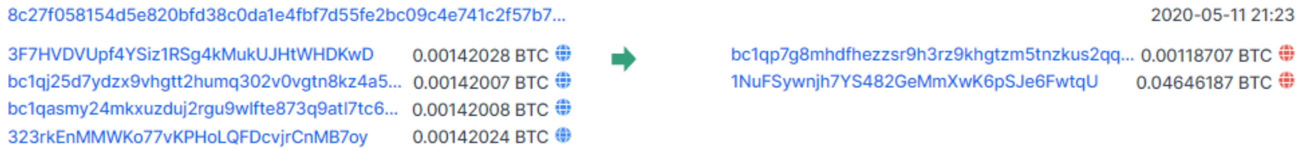
6) Tx: cbf25e1a1d150365a08d5cdef3ecb04a68f45e463bd6058b226eb612d1d4544c



cbf25e1a1d150365a08d5cdef3ecb04a68f45e463bd6058b226e... 2020-05-11 21:23

1HiH1wBD92MFrpP2Q5fyj2hitZqTAvzLSG 8.36179585 BTC ➡ 3Hjd9Je21Mr35XxxN4qzHgqsbietkoZbU1 0.00100000 BTC
1CzyArsLiLi9r9D5vATGPc3ezAde9rns1g 3.00000000 BTC
3D1toNFdJ4vJ1whA9tYgr88Xg4AFfrS7xa 0.00600000 BTC
1CDunscNwWPCjW7Rbzx3gQNyvQZWE5wyqY 5.35451371 BTC

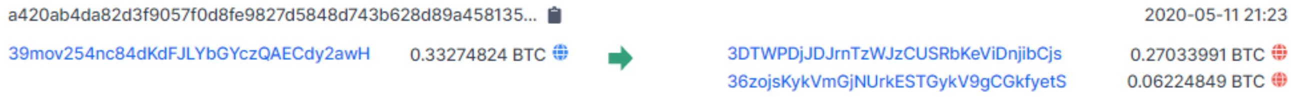
7) Tx: 8c27f058154d5e820bfd38c0da1e4fbf7d55fe2bc09c4e741c2f57b7ba5e1456



8c27f058154d5e820bfd38c0da1e4fbf7d55fe2bc09c4e741c2f57b7... 2020-05-11 21:23

3F7HVDVUpf4YSiz1RSg4kMukUJHtWHDKwD 0.00142028 BTC
bc1qj25d7ydzx9vhgtt2humq302v0vgtn8kz4a5... 0.00142007 BTC
bc1qasmy24mkxuzduj2rgu9wlfte873q9atl7tc6... 0.00142008 BTC
323rkEnMMWKo77vKPHoLQFDcvjrCnMB7oy 0.00142024 BTC ➡ bc1qp7g8mhdfhezzsr9h3rz9khgtzm5tnzkus2qq... 0.00118707 BTC
1NuFSywnjh7YS482GeMmXwK6pSJe6FwtqU 0.04646187 BTC

8) Tx: a420ab4da82d3f9057f0d8fe9827d5848d743b628d89a458135351eda64da971



a420ab4da82d3f9057f0d8fe9827d5848d743b628d89a458135...

2020-05-11 21:23

39mov254nc84dKdFJLYbGYczQAECdy2awH	0.33274824 BTC	3DTWPDjJDJrnTzWJzCUSRbKeViDnjibCjs	0.27033991 BTC
		36zojsKykVmGjNUrkESTGykV9gCGkfyetS	0.06224849 BTC

Exercise Solutions:

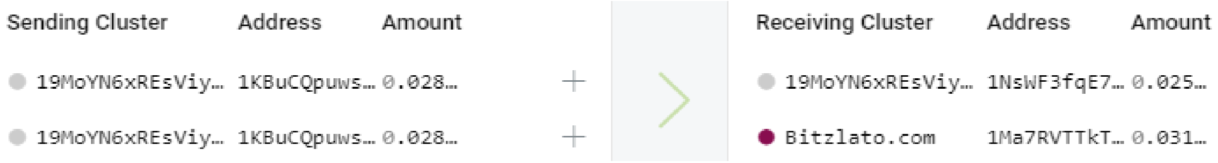
1) The change address is bc1qwq… The other address received a round amount and, more importantly, the change address features on both the input and output side.

2) There is no change address as there is only one output, which is the address that received all funds, minus the transaction fee. It is likely that there was no change of ownership here.

3) There is no change address. The same address sent funds to itself (this is indeed possible) and the other output is an OP_RETURN, the purpose of which is to store data, often text, in the blockchain.

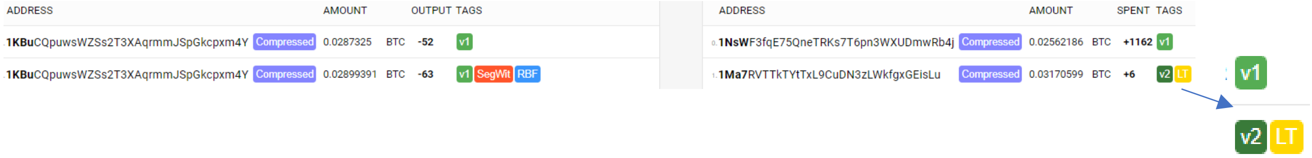
4) The change address is 3Jkk7a, which has the same address format starting with 3 as the address on the input side.

5) The change address is 1NsWF3. There are a number of indications for this – first, most wallets would not spend two inputs of 0.028… BTC in order to spend 0.025… as that generates a bigger transaction than necessary and results in higher transaction fee. Second, the commercial tool identified one of the outputs as a known entity that does not feature on the input side, suggesting the other address is the change. Moreover, the change address was then assigned into the same cluster 19MoYN:



Sending Cluster	Address	Amount	Receiving Cluster	Address	Amount
● 19MoYN6xREsViy…	1KBuCQpuws…	0.028…	● 19MoYN6xREsViy…	1NsWF3fqE7…	0.025…
● 19MoYN6xREsViy…	1KBuCQpuws…	0.028…	● Bitzlato.com	1Ma7RVTTkT…	0.031…

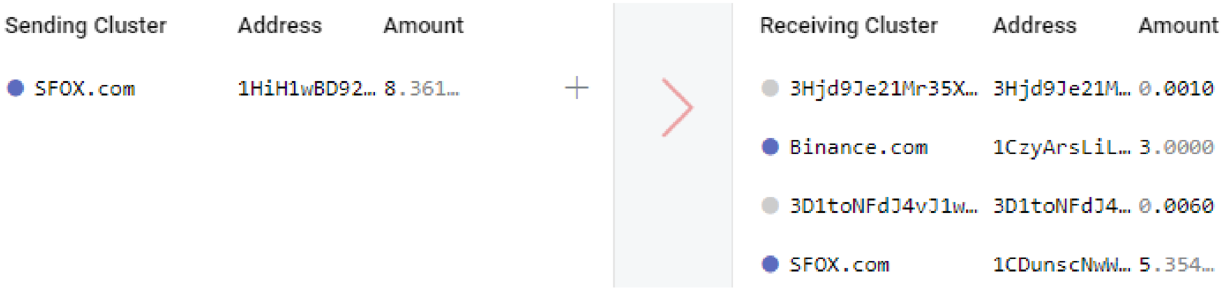
Finally, the transaction was sent from a version 1 wallet, whereas the address 1Ma7RV was later sent from a version 2 wallet. The following screenshot is from Chainalysis BEX but the version information for transactions from both output addresses can also be examined by Blockchair.com:



ADDRESS		AMOUNT		OUTPUT	TAGS
1KBuCQpuwsWZSs2T3XAqrmmJSpGkcpxm4Y	Compressed	0.0287325	BTC	-52	v1
1KBuCQpuwsWZSs2T3XAqrmmJSpGkcpxm4Y	Compressed	0.02899391	BTC	-63	v1 SegWit RBF

ADDRESS		AMOUNT		SPENT	TAGS
0. 1NsWF3fqE75QneTRKs7T6pn3WXUDmwRb4j	Compressed	0.02562186	BTC	+1162	v1
1. 1Ma7RVTTkTYtTxL9CuDN3zLWkfgxGEisLu	Compressed	0.03170599	BTC	+6	v2 LT

6) The change address is 1CDuns. While the transaction looks cryptic in a traditional blockchain explorer, a commercial tool makes determining the change address easy:



Sending Cluster	Address	Amount
● SFOX.com	1HiH1wBD92…	8.361…

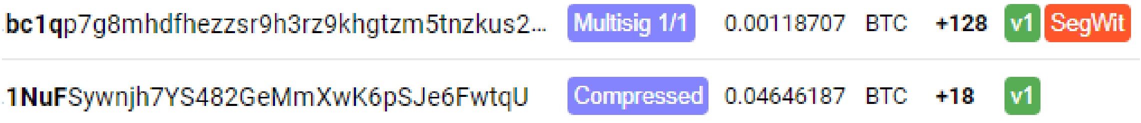
Receiving Cluster	Address	Amount
● 3Hjd9Je21Mr35X…	3Hjd9Je21M…	0.0010
● Binance.com	1CzyArsLiL…	3.0000
● 3D1toNFdJ4vJ1w…	3D1toNFdJ4…	0.0060
● SFOX.com	1CDunscNwW…	5.354…

Since the address came from SFOX entity, the output ending at SFOX must be the change address.

If the tracing tool fails to identify the change address, we may have to use a method of exclusion: since the input address starts with 1, we exclude the two addresses starting with 3. Then, we check the version of the transaction – it is version 1. Looking at transactions sent from 1CzyArs, we see it uses version 2, whereas the address 1CDuns is sent from a version 1 wallet, therefore it is the best candidate for a change address, even without any attribution made by the commercial tools.

Generally, when we see a transaction with more than three outputs, it is often a transaction made by a service rather than a private user. This was also true for the transaction, where we witnessed a withdrawal from SFOX exchange sending funds to three different clients.

7) The transaction had 36 inputs (only 4 are shown to save space) in total and all of them started with 3 or bc1. Therefore, bc1qp7… is a much better change address candidate. Also, the transaction was sent from SegWit compatible wallet and the 1NuFSy address does not match this parameter.



bc1qp7g8mhdfhezzsr9h3rz9khgtzm5tnzkus2…	Multisig 1/1	0.00118707	BTC	+128	v1	SegWit
1NuFSywnjh7YS482GeMmXwK6pSJe6FwtqU	Compressed	0.04646187	BTC	+18	v1	

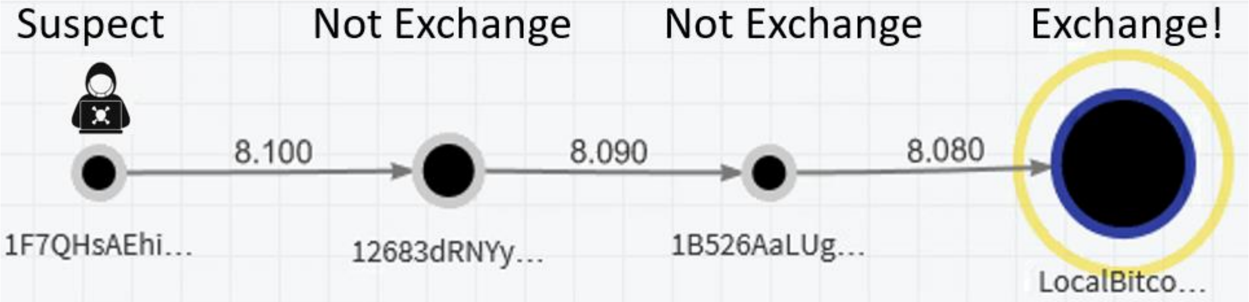
Finally, some commercial tools would assign the bc1qp7… to the same entity that created the transaction, confirming that this is indeed a change address.

8) In this case, we may not be able to determine the change address just by looking at the transaction in isolation. Sometimes, despite the best effort taken, all best practices and approaches fail, and it may turn out to be impossible to distinguish between the payment and the change.

The tracing tools and metadata do not help here, so the only chance to determine the change may be inspecting the addresses on different tools; failing that, it may be useful to follow both addresses and see which one is more consistent with the behaviour of the user, looking at variables such as amounts transacted, temporal analysis or used services.

Following the Money

The tracing usually starts with an address or a transaction made by the suspect and the objective is usually to find the most convincing route to a LE friendly exchange or a payment processor. Since suspects often do not send criminally obtained funds straight to the exchange, the investigator often has to follow the flow of funds from one address to another, until he finds the identification point:

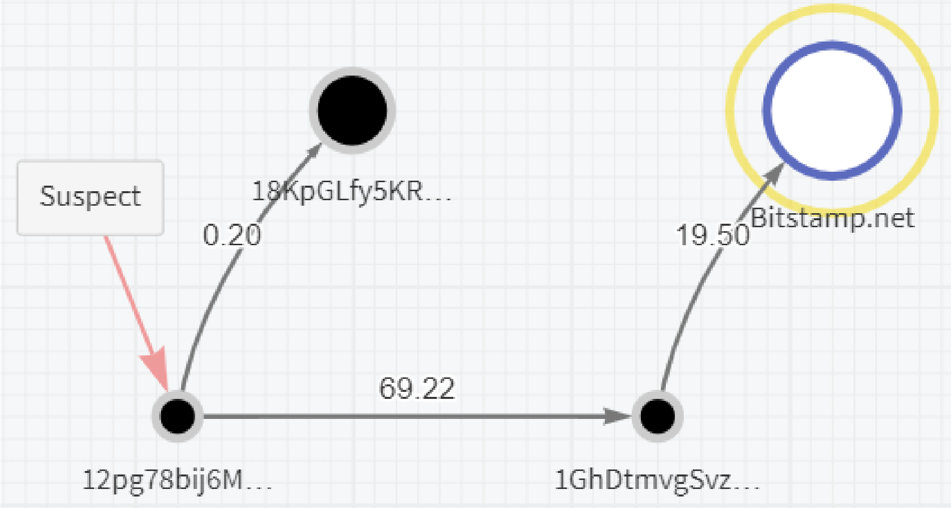


It is very important to know, when to continue and when to stop with the analysis. After all, it is always better to fail to identify a service used by the suspect rather than coming to a wrong conclusion and follow funds of users that are completely unrelated to the suspect.

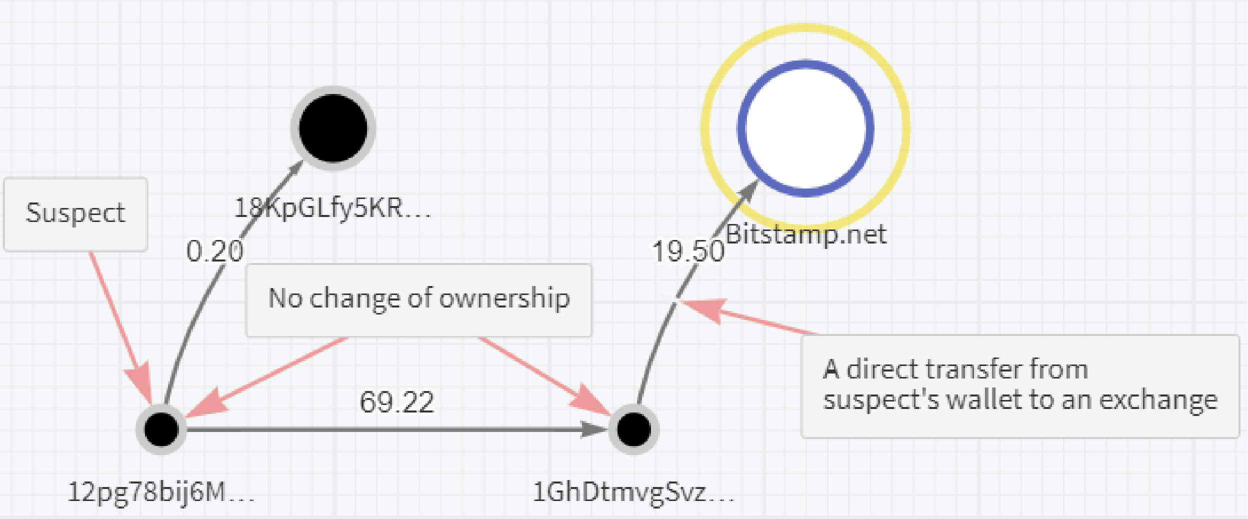
As observed in the previous chapter, it is relatively safe to trace the change addresses. A suspect may send a few transactions, resulting in change addresses in his wallet and ultimately he may send a transfer from one of the change addresses to an exchange – in such case, LE cooperative exchange should be contacted without any hesitation.

Consider the following example:

The suspect who owns the address 12pg78b… sends a transaction with outputs 18KpGLf… and 1GhDtmv…. One step further, we identify a direct transaction from 1GhDtmv… to Bitstamp. The question here is – should we ask Bitstamp to provide us with the identity of their client who received 19.5 BTC from 1GhDtmv…? Are we sure that the person who owns that wallet is the suspect we are after - or is there a possibility that the ownership may have changed?



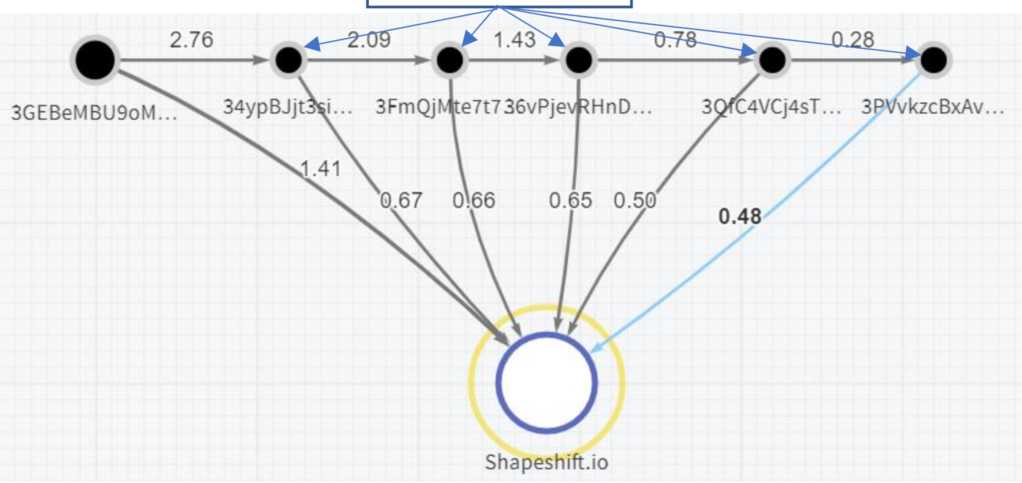
Using the know-how from the previous chapter, we quickly identify 18KpGLf… as a payment and therefore the other output address must be the change going back to the suspect's wallet. Therefore, we can observe a direct transaction from the suspect's wallet to an account at Bitstamp:



So – the address 1GhDtmv… definitely belongs to the suspect and the transfer to the exchange should certainly be queried. Is the suspect also owner of the account at the exchange? While this is very likely we do not have 100% certainty. The most probable scenario here is that the suspect sent funds to his account at Bitstamp, however, he may have also sent funds to someone else who provided him with the deposit address at the exchange.

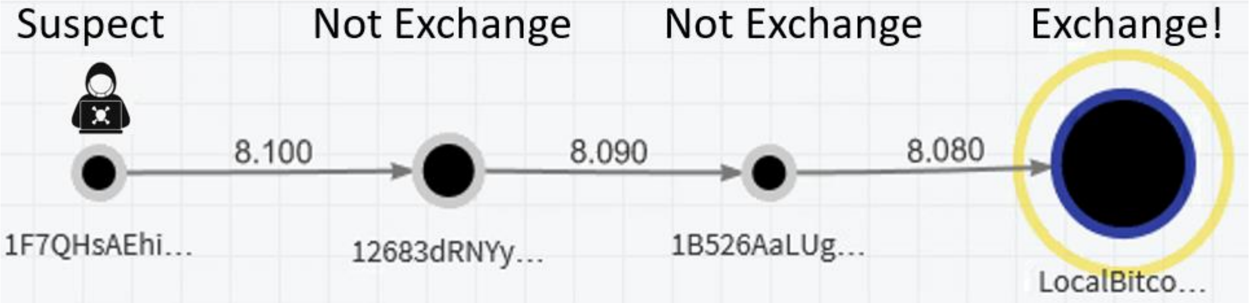
Enquiry at the exchange that determines the identity of the suspect may provide open source information that may render the suspect a viable candidate for an interview or a house search. Even if the suspect ultimately turns out to be a money mule or an innocent recipient of funds from the suspect, his information about the deposit transaction may be crucial to advance the investigation.

Sometimes, following the change reveals a very clear pattern of the user continuously sending funds into the same service. The user may do so to stay under KYC or daily deposit limit or may have another motivation, for example depositing round numbers of crypto or amounts corresponding to a certain amount of USD or EUR:

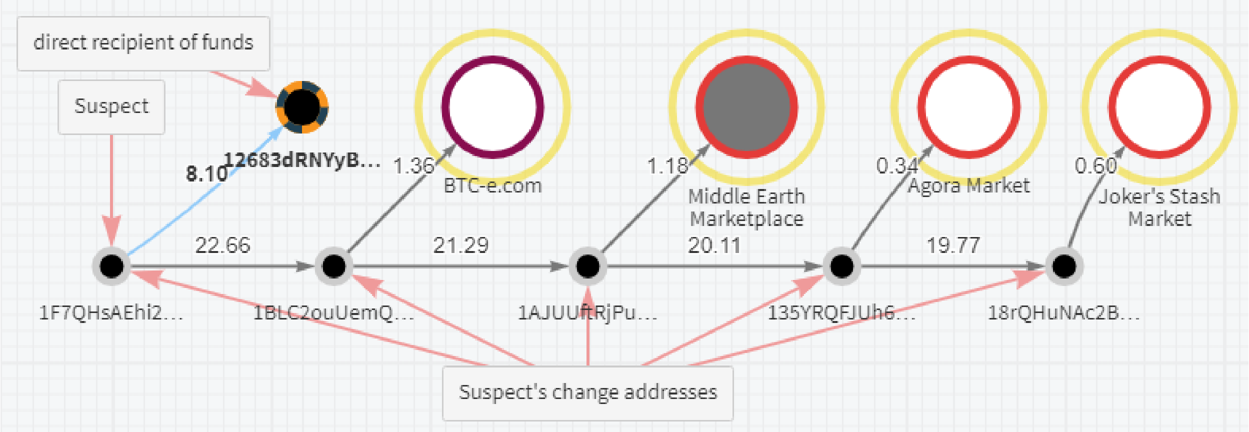


Following the Change not an Option?

When following the change is not an option, we may follow the payments as well but we have to be careful as the ownership may change with each additional hop. Let's consider the scenario from the previous page. Here, the suspect (1F7QHsA…) made several transactions, one of which landed at 12683d…:

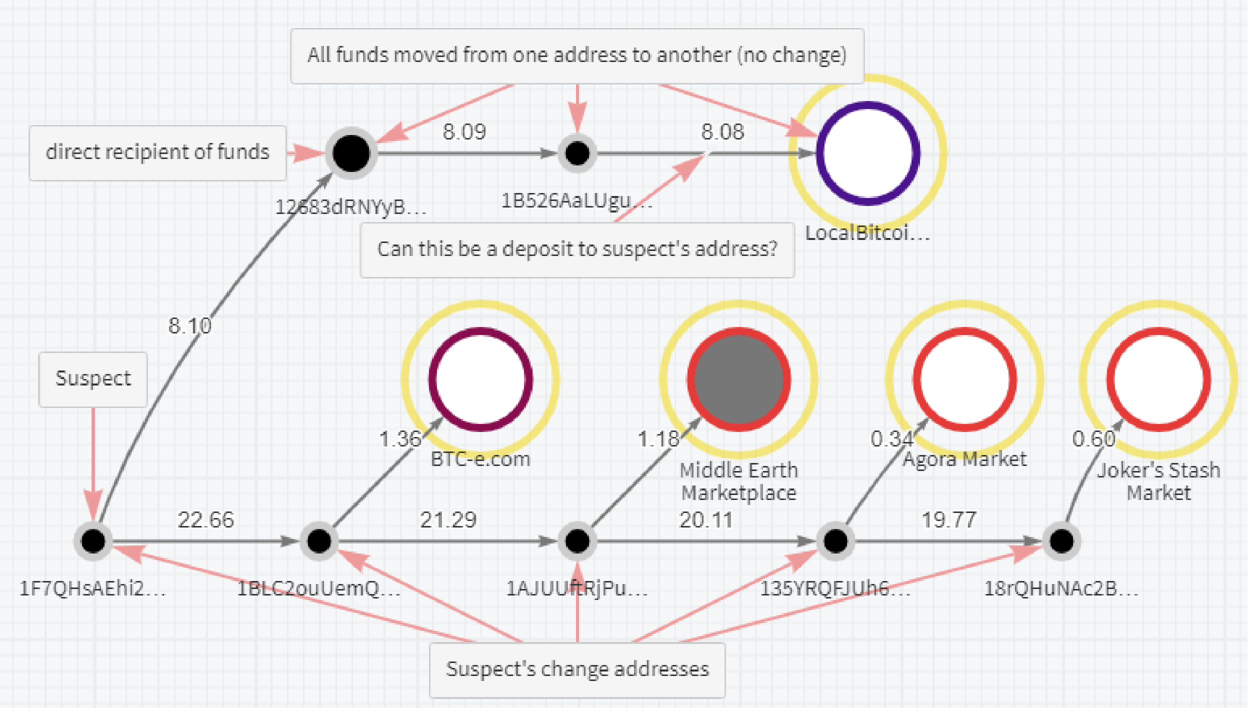


While the path to LocalBitcoins looks tempting, we can quickly discover that 12683d… is not a change address – it is an address that received funds from the suspect – either he forwarded 8.1 BTC to himself or he sent it to someone else. To play it safe, we should try to follow the change transaction from 1F7QHsA… first:



As the screenshot indicates, it may not be possible to establish identity of the suspect by contacting any of the 4 entities as these include 3 now extinct dark web marketplaces and BTC-e that was taken down by US authorities. Assuming the investigator does not have access to any of the dark web datasets, and queries of BTC-e dataset fail to establish the identity of the suspect, it is possible to continue tracing down the peelchain. This means following larger amount of funds, from which small chunks are shaved, one after another - and try to identify other services that received funds from the suspect.

Failing to identify a suitable service when following the change, we may focus the attention at the address that received the funds from the suspect – 12683d…. We can see that all 8.1 BTC minus the transaction fee is sent to another address (1B526Aa…) and from there the pattern repeats and funds end up at LocalBitcoins:



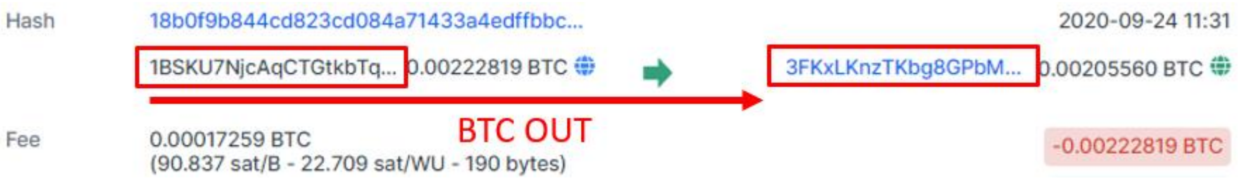
Should the investigator approach LocalBitcoins? Indeed, if there is no promising direct transaction, he may have to follow less promising leads. In the above example, the ownership may have changed between suspect's address 1F7QHsA… and 12683d. However, since the owner of 12683d very likely sent funds to LocalBitcoins, it is advisable to contact the exchange in an effort to identify the suspect or someone who received funds from him.

In this particular investigation, the investigator's effort paid off – the suspect indeed kept sending funds from one of his wallet to another, moving all funds on without a change all the way to the exchange, which resulted in the identification and detection of the suspect behind DD4BC (DDoS for Bitcoin extortion campaigns) as described by the following press release.

Private v. Service Wallets

As demonstrated earlier in this document, we should ideally follow change addresses but if that is not an option, following the payment addresses may work as well. However, there is always a point when one has to stop and that point is a service. Once the suspect sends a payment to a service, identified or not, the tracing has to stop there. Either the investigator is able to query the service or not - but by no means he should trace through the service.

For example, when looking at address 1BSKU7Nj… that sends funds to 3FKxLKn…, we may be tempted to follow the money from that address:



Hash 18b0f9b844cd823cd084a71433a4edffbbc... 2020-09-24 11:31

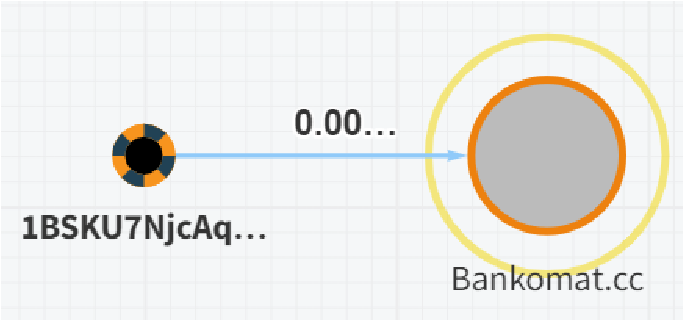
1BSKU7NjcAqCTGtkbTq... 0.00222819 BTC → 3FKxLKnzTKbg8GPbM... 0.00205560 BTC

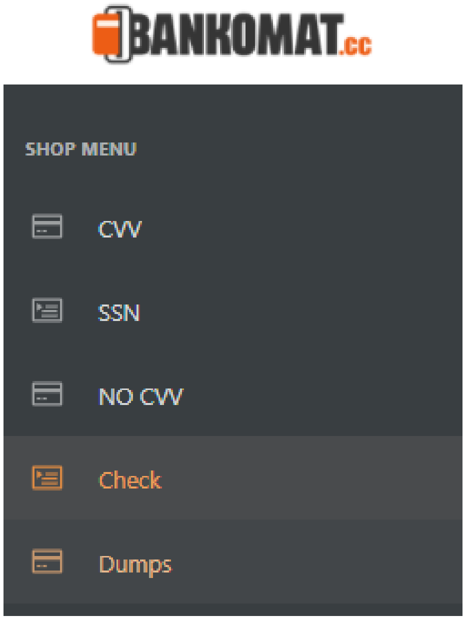
BTC OUT

Fee 0.00017259 BTC
(90.837 sat/B - 22.709 sat/WU - 190 bytes)

-0.00222819 BTC

However, a commercial tracing tool established that the address 3FKxLKn… is a deposit address at Bankomat.cc and therefore our tracing has to end there – regardless whether this lead is promising or not:

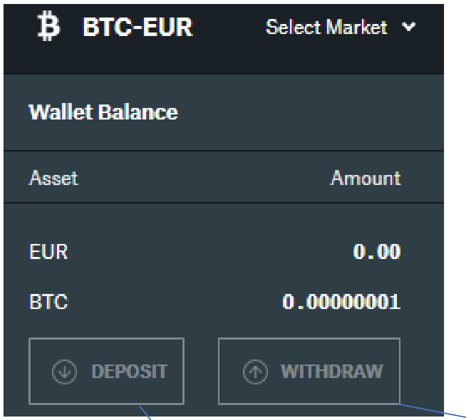




Since Bankomat.cc is a darkweb marketplace (still active in April 2021), sending a request to the administrators of the marketplace is not a viable option. The only thing we figured out is that the suspect made a deposit into this marketplace, likely with an intention to purchase compromised payment card details.

The tracing stops here and the investigator has to find another thread to follow. Monitoring a dark market for transactions following the deposit, searching for any external evidence of transactions (e.g., feedback comment), is laborious and may not yield any results as many marketplaces operate a wallet where buyers may send deposits to long before they decide to make any purchases.

A Service is a BLACKBOX

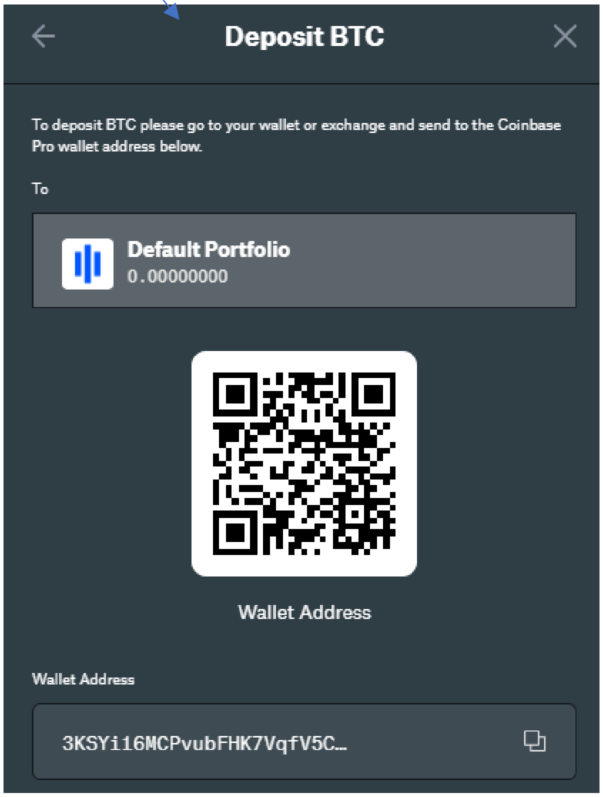


Wallet Balance

Asset	Amount
EUR	0.00
BTC	0.00000001

In any case, we cannot continue tracing this payment thread any further because we do not know what happens on the platform. The services are a complete blackbox for an investigator as there is no way of establishing what happens once the funds are deposited there just by observing the transactions in the blockchain.

The deposits may be routed to an internal wallet of the service or may be used to fund withdrawals of other users of the service. One way or the other – we cannot trace though the service because if we do, we will end up following money flows made by unrelated parties.



Deposit BTC

To deposit BTC please go to your wallet or exchange and send to the Coinbase Pro wallet address below.

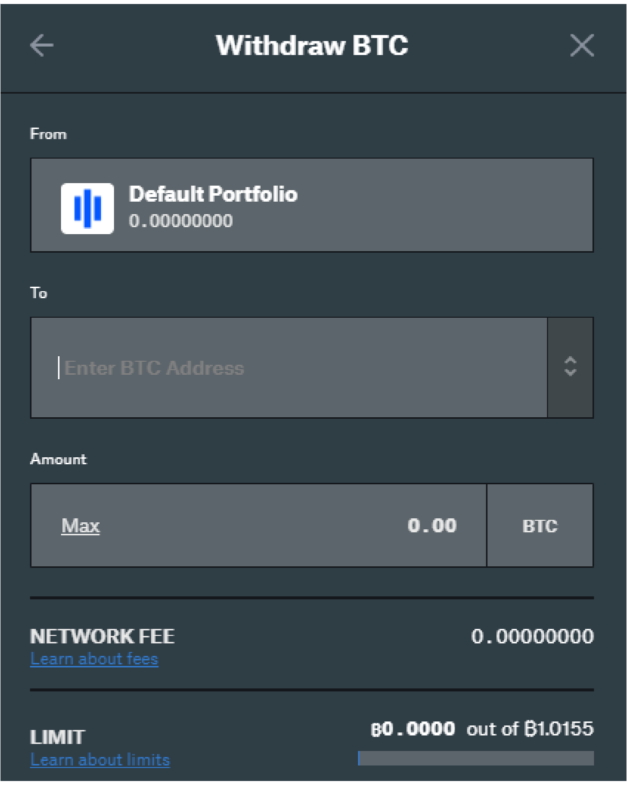
To

Default Portfolio
0.00000000

Wallet Address

Wallet Address

3KSYi16MCPvubFHK7VqfV5C...



Withdraw BTC

From

Default Portfolio
0.00000000

To

Enter BTC Address

Amount

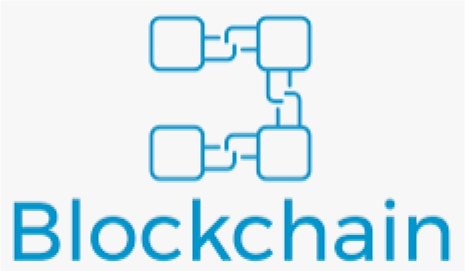
Max 0.00 BTC

NETWORK FEE 0.00000000
Learn about fees

LIMIT ₿0.0000 out of ₿1.0155
Learn about limits

The above diagram shows an example of one of the most popular exchanges – Coinbase. The exchange assigns a unique deposit address to every client. Note that some services, including Coinbase, use a different address for every deposit while others (e.g. Binance) still encourage address reuse for deposits.

The withdrawal address is entered by the client. They may decide to leave funds on the exchange briefly for a quick conversion to another asset followed by an almost immediate withdrawal or they may leave the funds on the exchange for months or even years. Whenever funds are left at the exchange, it is the exchange who has access to the private keys and is in full control of the funds.

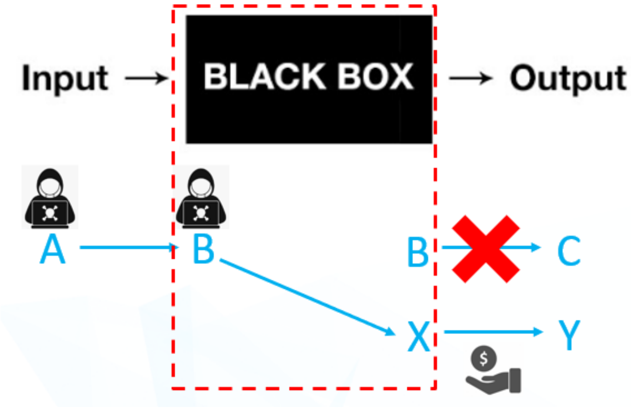


When withdrawing funds, the client has to provide their own address that will receive the coins from the exchange. This is often a new address for every withdrawal. Keep in mind that while deposits and withdrawals appear on the blockchain, any other movement of funds on the exchange takes place in the internal database of the exchange.

So – for example when user converts one cryptocurrency into another or if he sells cryptocurrency for EUR, this action is not recorded on the exchange. A client who moves BTC to an exchange in order to sell it for EUR will only leave trace in the form of a deposit transaction to an exchange while withdrawal will take place usually via a bank transfer.

Implications for the investigator:

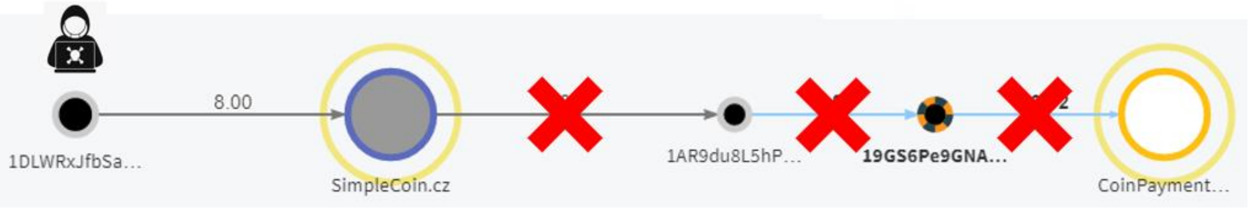
1) When the user makes a deposit to a service, the transaction appears in the blockchain.
2) Whatever happens on the exchange is a mystery – unless the service provides an explanation. The internal transaction carried out by the service may only be recorded in a centralized database without leaving any traces in the blockchain.
3) Any non-cooperative service (non-responsive party or a dark web platform) is from a practical point of view a mixer.
4) The suspect may use the service to swap assets so the funds may leave the service via a transaction on another cryptocurrency blockchain or a completely different asset.



As the diagram depicts, the transaction where BTC is sent from a suspect to his account at an exchange is visible in the blockchain. He may use the platform to convert BTC to USD, which he withdraws – either to his bank account or, more likely, online services such as Skrill, Webmoney or Perfect Money. Another popular option is a conversion to a privacy coin (Monero/DASH/ZCash) or Stablecoin (USDT/USDC) that can be converted to BTC or USD on another exchange.

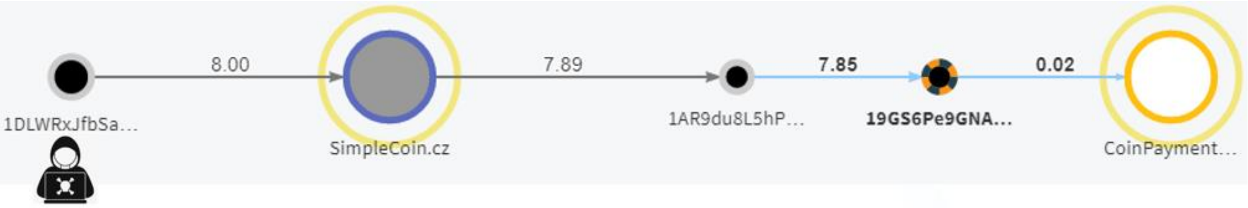
Never ever trace through the service:

Ideally, you should never see a chart like this:



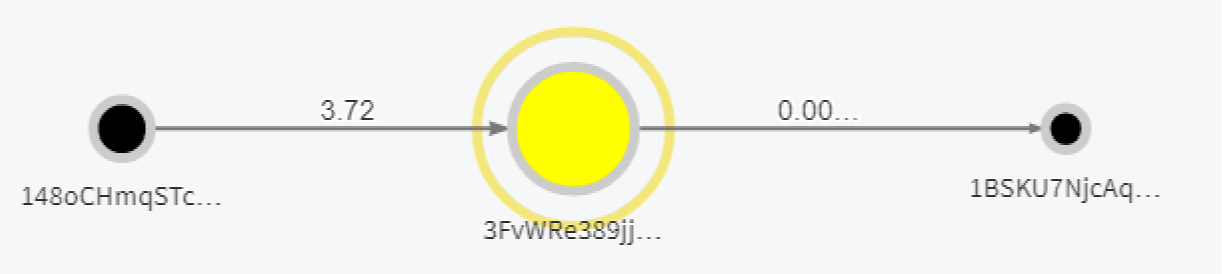
Here, the funds are traced through a service. This should never be done without getting the intelligence from SimpleCoin first – whatever takes place with the funds after they are sent to the exchange is unknown – unless of course the exchange itself clarifies what happened.

Should it not be possible to identify the suspect, the exchanges may provide a list of deposit and withdrawal addresses that may lead to other services. Only if SimpleCoin confirms the withdrawal address of the suspect – in this case 1AR9du8L, we may be able to trace the funds to other entities:



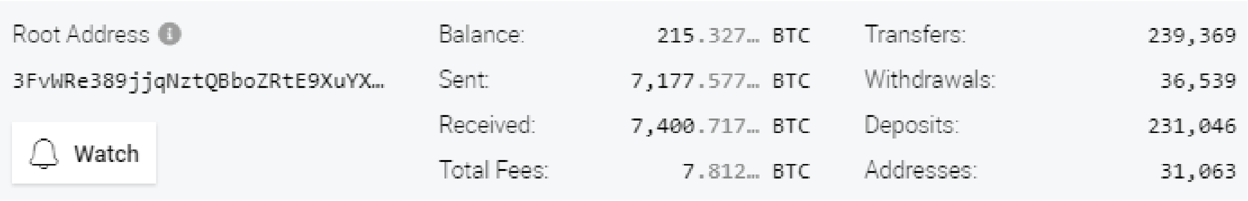
Unidentified services – a hidden danger

Thus, an experienced investigator will never trace through a service. However, as mentioned before, many services are not correctly clustered and identified. Often, you may encounter the following scenario:



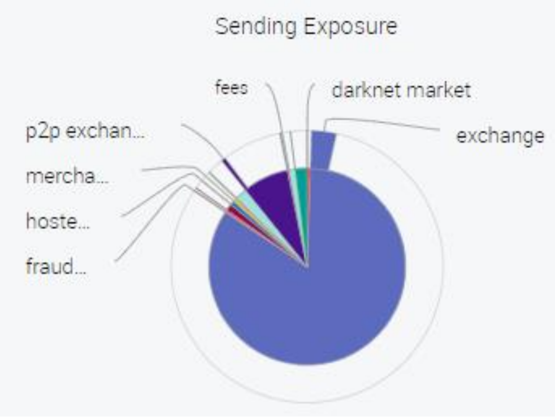
The suspect sends funds from 148oCHm to 3F4XtS8… which was a part of a large unknown cluster 3FvWRe3 in Chainalysis.

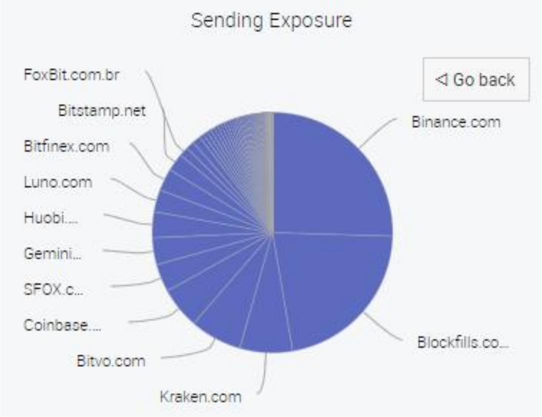
When can we assume that this is a service and stop tracing right at this point? By checking the cluster we can see over 30,000 addresses – making it blatantly obvious this may not be a private wallet:



Root Address ⓘ	Balance:	215.327… BTC	Transfers:	239,369
3FvWRe389jjqNztQBboZRtE9XuYX…	Sent:	7,177.577… BTC	Withdrawals:	36,539
🔔 Watch	Received:	7,400.717… BTC	Deposits:	231,046
	Total Fees:	7.812… BTC	Addresses:	31,063

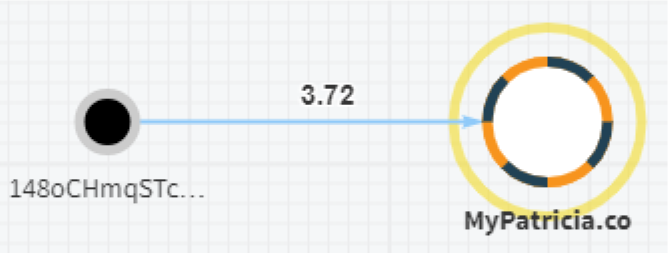
Moreover, the withdrawals from the cluster ended up at different services and a large number of exchanges:





This is a clear indication of a service – no private user would interact with such a large amount of exchanges.

Later in 2020, Chainalysis confirmed our hypothesis and managed to identify the service, so now it is obvious the cluster indeed is a service, identified as MyPatricia.co:



There are two lessons here for the investigator:

1) If you discover a cluster with a large number of addresses or transactions (hundreds or more, especially within a short timeframe) or a cluster that interacts with a very diverse range of services, including exchanges serving audiences in different regions, this is very likely an unidentified service.
2) It is a good practice to review old cases – the tracing tools constantly improve and just one identified service on the chart may completely change the course of the investigation.

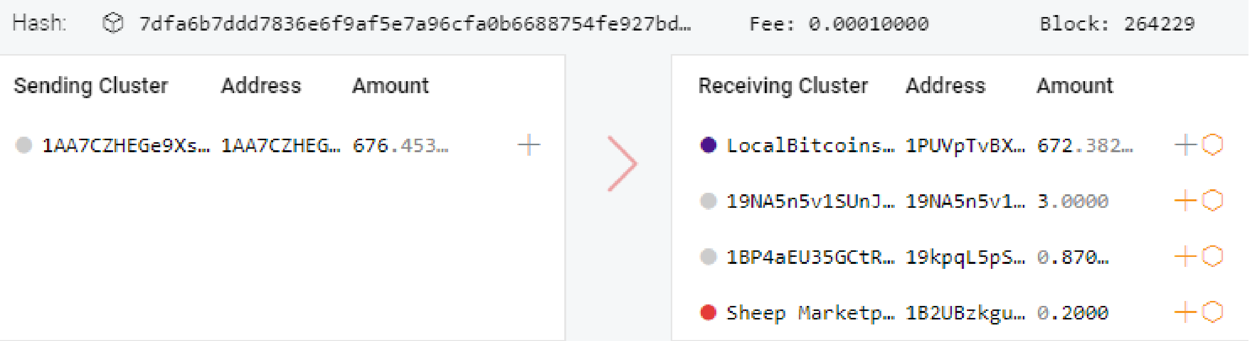
Nothing is as simple as it seems in cryptocurrency tracing and sometimes even clusters with 1 or a few addresses may be part of an unidentified entity. The investigators may easily confuse these with a private wallet and continue tracing transactions of unrelated individuals. Some services intentionally prevent spending inputs together to make algorithms of tracing tools less effective.

While some exchanges and payment processors have nearly all addresses clustered and identified, some exchanges, gaming sites, dark markets and mixers may have a large proportion of their addresses unclustered, which naturally negatively impacts any investigative tracing efforts.

How to Recognize an Unidentified Service?

So – we know that we have to stop tracing whenever we find a service – identified or not. This logically raises the question of how we can determine that a cluster belongs to a service when even commercial tools may fail to do so. Here are the most important indications of services:

1) Large activity – number of addresses/transactions/deposits/withdrawals
2) Large number of diverse parties to which cluster sends funds, often geographically dispersed (e.g. German and Korean exchange, where there is a small likelihood that a person would interact with both).
3) A large number of transactions within a short time frame
4) Outgoing transactions with 3 and more outputs. While some private wallets are capable of creating transactions with multiple outputs, vast number of private transactions only have one recipient and therefore only 1 or 2 outputs.
   The services, on the other hand, like to bundle different withdrawals together to save on transaction fees and this often results in transactions with multiple outputs.
   For example:



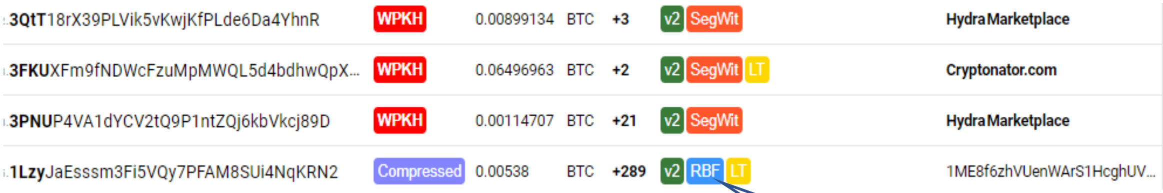
Hash: 7dfa6b7ddd7836e6f9af5e7a96cfa0b6688754fe927bd… Fee: 0.00010000 Block: 264229

Sending Cluster	Address	Amount
1AA7CZHEGe9Xs…	1AA7CZHEG…	676.453…

Receiving Cluster	Address	Amount
● LocalBitcoins…	1PUVpTvBX…	672.382…
● 19NA5n5v1SUnJ…	19NA5n5v1…	3.0000
● 1BP4aEU35GCtR…	19kpqL5pS…	0.870…
● Sheep Marketp…	1B2UBzkgu…	0.2000

   Although the deposit side is unidentified, the transaction likely originates from a service rather than a private wallet.

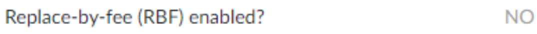
5) Use of multisignature – very few individuals use multisignature (i.e., a requirement for multiple private keys to sign a transaction before it can be spent). Therefore, if Blockchair.com or BEX indicate use of multisignature, this significantly increases the probability of a service.
6) Highly consistent behavioral patterns. For example, a consistent movement of funds 3 blocks after the funds are sent to the deposit address of the cluster. People are not consistent; services are.
7) Replace-by-fee (RBF) feature, which allows for increasing the transaction fee for a recent transaction in order to shorten its confirmation time, only tends to be used by private wallets. So, transactions that have this feature disabled have higher likelihood of being a service:



3QtT18rX39PLVik5vKwjKfPLde6Da4YhnR	WPKH	0.00899134	BTC	+3	v2 SegWit	Hydra Marketplace
3FKUXFm9fNDWcFzuMpMWQL5d4bdhwQpX…	WPKH	0.06496963	BTC	+2	v2 SegWit LT	Cryptonator.com
3PNUP4VA1dYCV2tQ9P1ntZQj6kbVkcj89D	WPKH	0.00114707	BTC	+21	v2 SegWit	Hydra Marketplace
1LzyJaEsssm3Fi5VQy7PFAM8SUi4NqKRN2	Compressed	0.00538	BTC	+289	v2 RBF LT	1ME8f6zhVUenWArS1HcghUV…

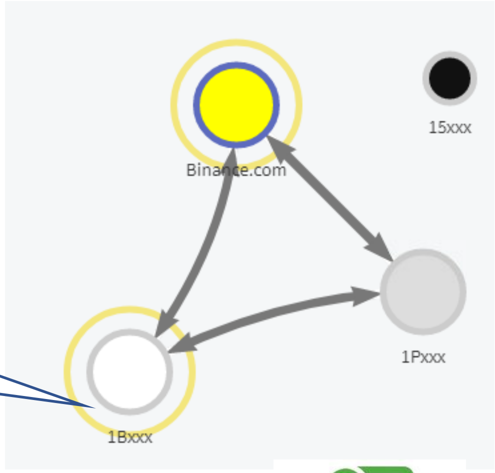
A higher likelihood of a private wallet

The above identification comes from BEX; a free alternative is again Blockchair.com providing the same information in a somewhat simpler way:



Replace-by-fee (RBF) enabled? NO

8) A cluster that has a large proportion of transactions linked to another entity (e.g. exchange or dark market) may be a part of an exchange or may be an associated service using the API of a larger entity. The latter is sometimes referred to as a 'nested service'. If our suspect interacts with such entity, we may try sending the address to the associated exchange and ask if they recognize the address:



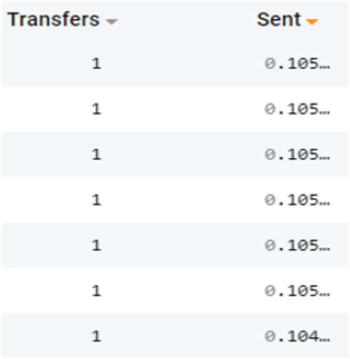
Looks like an unidentified service, where 70% of withdrawals go to Binance.com

This is a part of Binance swapper using Binance API.

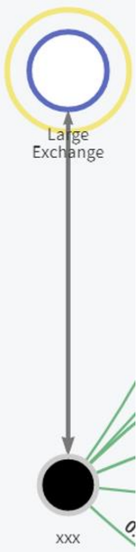
If so. Binance will advise.

9) Criminals like to reuse what works.
For example, if you observe a suspect's transactions aggregating in a wallet and from there we see 10 outgoing transactions, 2 of which were sent straight into a mixer, there is a good chance that some or all of the other transactions were also sent into the mixer - although the tracing tool have not identified it that way.

10) Observe the entity and analyse its behaviour.
Consider an unidentified cluster may belong to an ATM Machine – its behaviour corresponds with expected behaviour of the ATM cluster:
The cluster should contain many transactions, where the number of withdrawals is considerably higher than the number of deposits. Many of the withdrawals are smaller, around 20-50 EUR worth of BTC while some withdrawals should be just below the usual KYC limit of 1,000 USD/EUR.



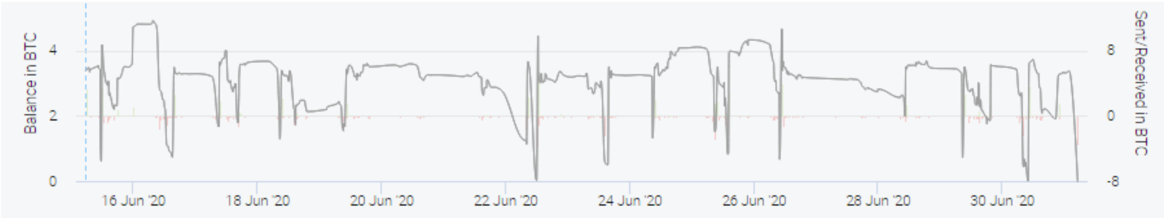
Transfers	Sent
1	0.105…
1	0.105…
1	0.105…
1	0.105…
1	0.105…
1	0.105…
1	0.104…



We can also expect that there will be an automated process topping up the internal wallet of a Bitcoin ATM every time the cryptocurrency balance drops below a certain level. Most deposits to ATM should come from the same exchange, while withdrawals should be fragmented and most withdrawals should be sent to private wallets.

While this may be an indication of a Bitcoin ATM, other services heavily using API of a larger exchange, for example crypto-to-crypto swappers, may also look the same on the chart.

Observe the following behaviour of a Bitcoin ATM – the unidentified cluster was live for 2 weeks after which Bitcoin ATM started using another set of addresses. Within these two weeks, we can see a clear pattern of the balance being replenished – whenever it dropped below 2 BTC, a deposit from an exchange followed to keep the balance positive and ready to service any withdrawal requests:



Contacting the Exchange

Majority of large exchanges and other services comply with law enforcement requests and can provide useful information.

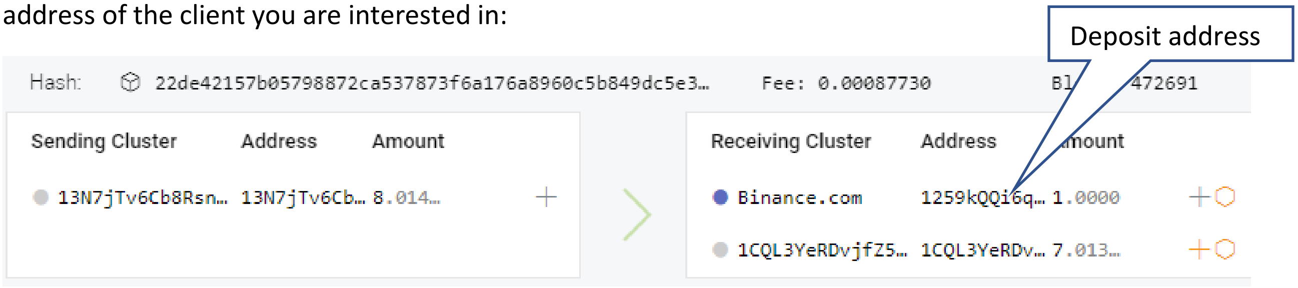
In order to properly request data from an exchange, be sure to attach searchable unique identifiers in the cleartext. This will simplify the process for an exchange and they might be able to return information more quickly. Scanned copies containing addresses or transactions always have to be accompanied by an Excel spreadsheet, .txt or .csv file containing the unique identifiers in an editable format.

Note that in some cases the content of the file may be changed by a PDF convertor. A botched conversion has already resulted in several requests to exchanges that generated negative results so even if a PDF document sent to a cryptocurrency service is editable, it is a good practice to attach the unique identifiers separately.

The standards for contacting the services differ considerably. For a list of recommended contacts, tips on how to request data from each exchange and evaluation of their cooperation with law enforcement please refer to the *Cryptocurrency Services Review Guide* released in January 2021. Should you need access to the Guide, please contact o3@europol.europa.eu.

What exactly should be requested?

In most cases, investigators will identify a deposit address within a service. Pay attention to include a correct address – i.e. not the address of the cluster provided by commercial tools but the deposit address of the client you are interested in:



Deposit address

Hash: 22de42157b05798872ca537873f6a176a8960c5b849dc5e3… Fee: 0.00087730 Bl 472691

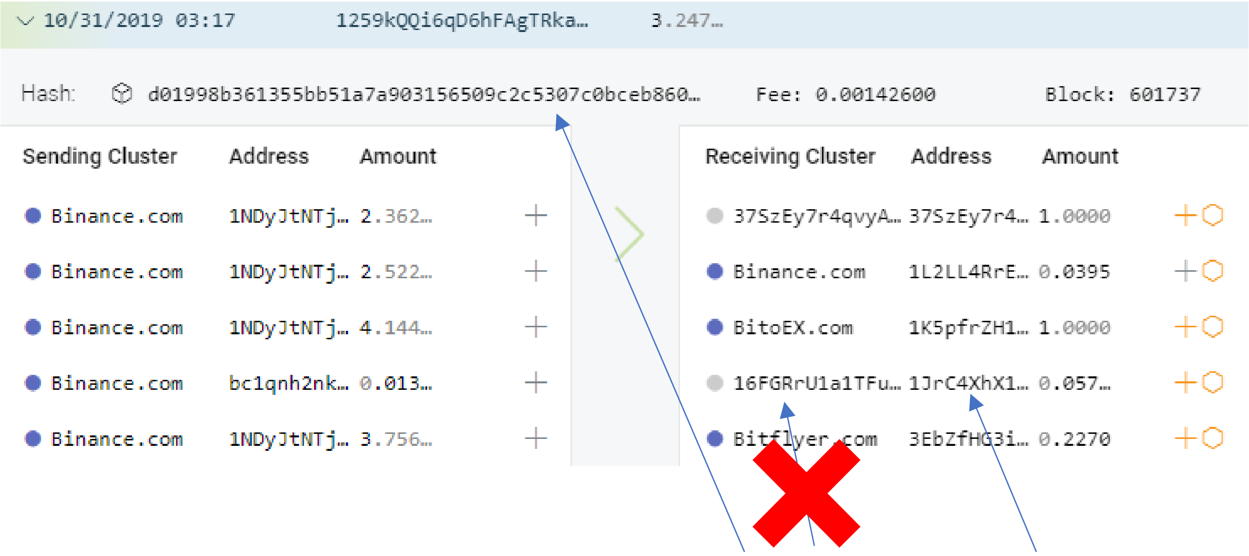
Sending Cluster	Address	Amount
13N7jTv6Cb8Rsn…	13N7jTv6Cb…	8.014…

Receiving Cluster	Address	mount
Binance.com	1259kQQi6q…	1.0000
1CQL3YeRDvjfZ5…	1CQL3YeRDv…	7.013…

To make the request clear, it is a good idea to also include the corresponding transaction ID and the deposited amount; for the above transaction it is *22de42157b05798872ca537873f6a176a8960c5b849dc5e33344a6241ae4ee6c* and 1 BTC respectively.

Please refrain from including custom identification provided by the tracing tools such as names of clusters provided by Chainalysis or hashes of wallets shown in Walletexplorer.

For withdrawal transactions it is even more important to be specific as usually one withdrawal services multiple clients. Therefore, it is necessary to include the transaction ID of the withdrawal along with the suspect's withdrawal address. Again, pay special attention to avoid confusing suspect's withdrawal address with the cluster. In the example below, we are interested in an address that withdrew 0.057 BTC from Binance:



10/31/2019 03:17 1259kQQi6qD6hFAgTRka… 3.247…

Hash: d01998b361355bb51a7a903156509c2c5307c0bceb860… Fee: 0.00142600 Block: 601737

Sending Cluster	Address	Amount	Receiving Cluster	Address	Amount
Binance.com	1NDyJtNTj…	2.362…	37SzEy7r4qvyA…	37SzEy7r4…	1.0000
Binance.com	1NDyJtNTj…	2.522…	Binance.com	1L2LL4RrE…	0.0395
Binance.com	1NDyJtNTj…	4.144…	BitoEX.com	1K5pfrZH1…	1.0000
Binance.com	bc1qnh2nk…	0.013…	16FGRrU1a1TFu…	1JrC4XhX1…	0.057…
Binance.com	1NDyJtNTj…	3.756…	Bitflyer.com	3EbZfHG3i…	0.2270

If we are interested in the suspect's withdrawal, we mention the Transaction ID and the withdrawal address of the suspect, along with the withdrawn amount.

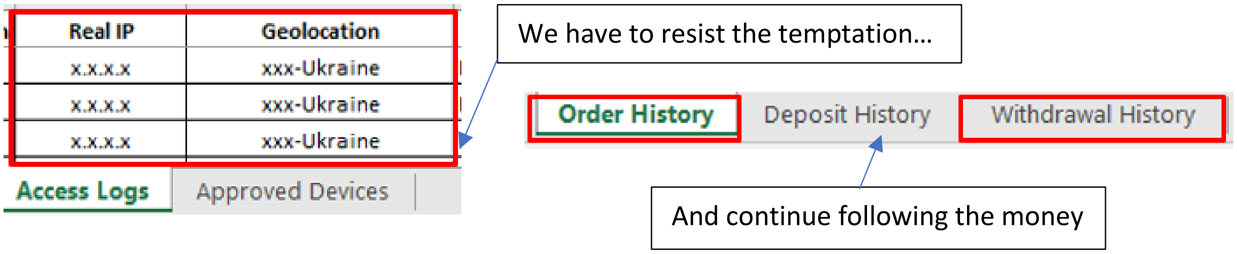
Nested Exchanges

Sometimes, you will identify a client at an exchange who is responsible for thousands of transactions. While it is possible that the suspect you are after is very entrepreneurial, chances are that he may be running a nested exchange and only mediates transactions on behalf of his clients.

There is a large number of swappers that mainly convert funds from one cryptocurrency into another using APIs of large exchanges, such as Binance or Huobi. In such cases, the large exchanges can only identify owner of the swapper rather than the suspect using the service.

What to do if you encounter this scenario? All is not lost – the large exchanges still have the logs of all incoming and outgoing transactions. So – if the suspect used a small swapper service to convert BTC to ETH, this should be apparent from the logs. Most swappers are not extremely busy, so if there is a deposit of 0.6 BTC and a few minutes later several ETH corresponding to the ETH/BTC rate that day is sent to an ETH address, you will know what to do.

The key here is to avoid identifying administrator of the swapper as the suspect; instead it is necessary to pair incoming with outgoing transactions and continue with the tracing, possibly on another blockchain.



Real IP	Geolocation
x.x.x.x	xxx-Ukraine
x.x.x.x	xxx-Ukraine
x.x.x.x	xxx-Ukraine

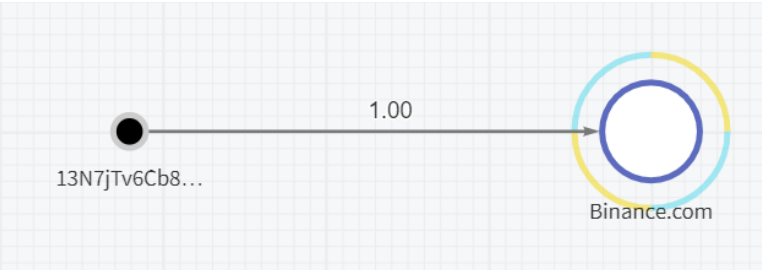
We have to resist the temptation…

And continue following the money

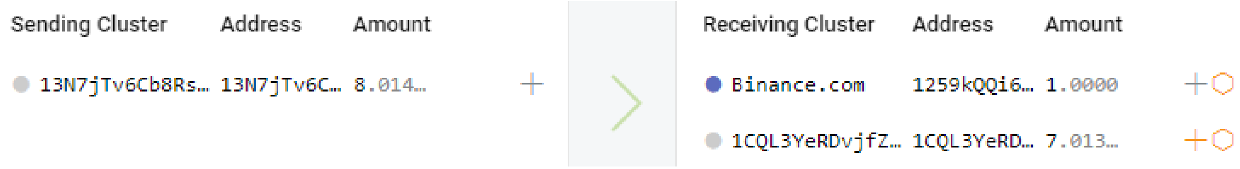
Custom Clusters

Often, we are interested in an address rather than a cluster. This happens, when a suspect deposits funds into an exchange and there is a good possibility that he may reuse the same address multiple times.

In such scenario, it may not be enough to see the individual deposit into the exchange – we also want to see other deposits received by the deposit address… but how to do it?

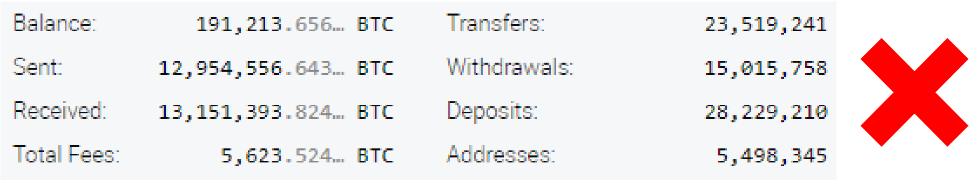


Here, we see that 1 BTC was deposited to Binance deposit address 1259kQQ…



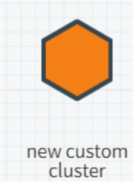
Sending Cluster	Address	Amount	Receiving Cluster	Address	Amount
13N7jTv6Cb8Rs…	13N7jTv6C…	8.014…	● Binance.com	1259kQQi6…	1.0000
			1CQL3YeRDvjfZ…	1CQL3YeRD…	7.013…

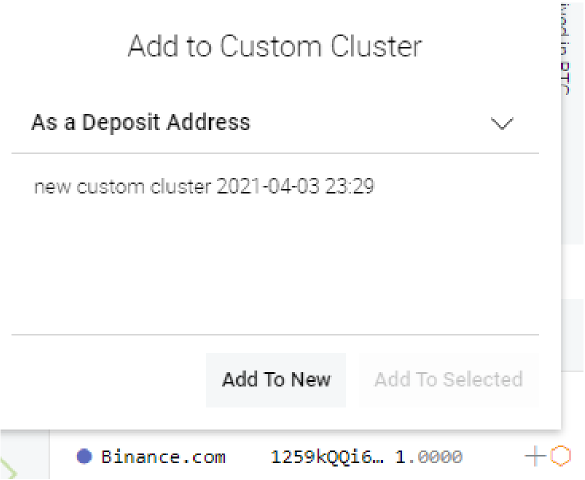
However, if we want to check the address on a cluster-based tool like Chainalysis, we only get an aggregated information of all users who deposited or withdrawn funds from Binance – which is not helpful if we are only interested in the deposits into one single address:



Balance:	191,213.656… BTC	Transfers:	23,519,241
Sent:	12,954,556.643… BTC	Withdrawals:	15,015,758
Received:	13,151,393.824… BTC	Deposits:	28,229,210
Total Fees:	5,623.524… BTC	Addresses:	5,498,345

What we need at this point is to add a single deposit address into the chart and we can do it by creating a so-called Custom Cluster:





Add to Custom Cluster

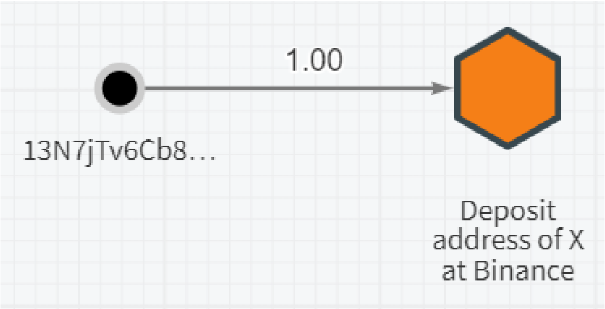
As a Deposit Address

new custom cluster 2021-04-03 23:29

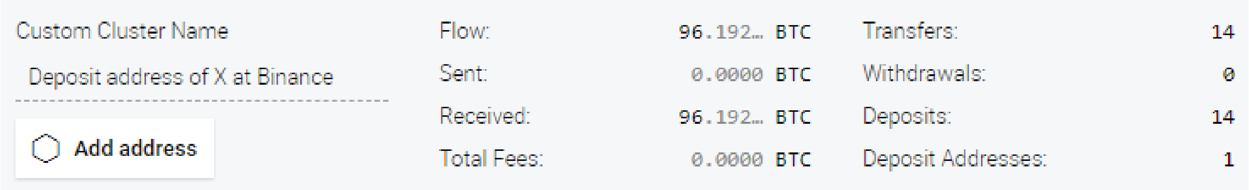
● Binance.com 1259kQQi6… 1.0000

Commercial tools cluster addresses into clusters, label these with real-world identities and visualize them.
Some tools use color-coding schemes to highlight legitimate v. criminal services.

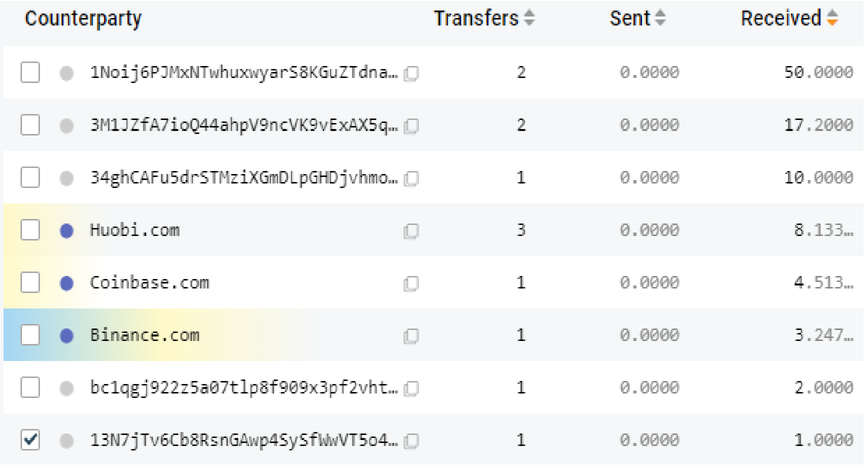
Using a custom cluster, we can narrow down the Binance cluster into one single address:



All of a sudden, we discover that our suspect has received another 95 BTC of deposits from different addresses and services to the same deposit address (a reminder – default behavior of many exchanges including Binance is to reuse the deposit address).



Custom Cluster Name	Flow:	96.192… BTC	Transfers:	14
Deposit address of X at Binance	Sent:	0.0000 BTC	Withdrawals:	0
	Received:	96.192… BTC	Deposits:	14
⬡ Add address	Total Fees:	0.0000 BTC	Deposit Addresses:	1



	Counterparty	Transfers	Sent	Received
□	● 1Noij6PJMxNTwhuxwyarS8KGuZTdna…	2	0.0000	50.0000
□	● 3M1JZfA7ioQ44ahpV9ncVK9vExAX5q…	2	0.0000	17.2000
□	● 34ghCAFu5drSTMziXGmDLpGHDjvhmo…	1	0.0000	10.0000
□	● Huobi.com	3	0.0000	8.133…
□	● Coinbase.com	1	0.0000	4.513…
□	● Binance.com	1	0.0000	3.247…
□	● bc1qgj922z5a07tlp8f909x3pf2vht…	1	0.0000	2.0000
☑	● 13N7jTv6Cb8RsnGAwp4SySfWwVT5o4…	1	0.0000	1.0000

This way, we can find about incoming funds to the suspect's address at Binance without having to contact the exchange.

This also means that we now can send simultaneous requests to other exchanges without having to wait for the results of the request sent to Binance.

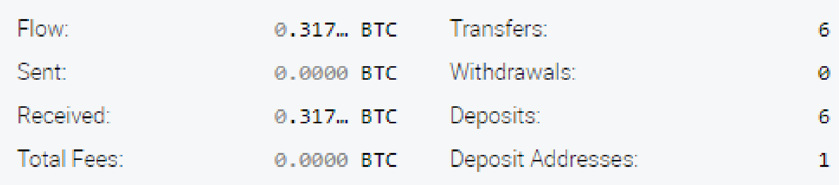
Custom Clusters Q&A:

Questions

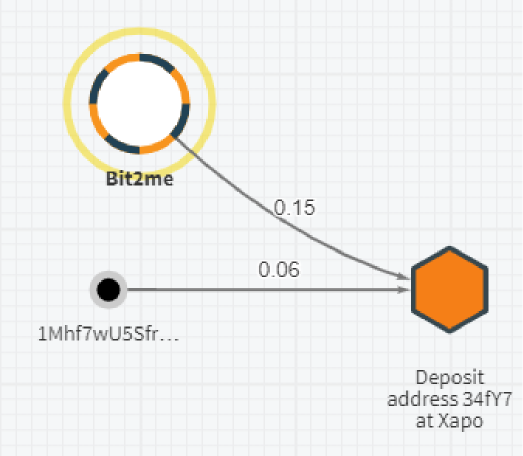
1) Take a look at address *1Mhf7wU5SfrZLEsnZir7zqcfqFJhfy9viw.* To which exchange it is sending funds?
2) How many BTC arrived at the deposit address?
3) What is the name of an exchange that sent funds directly to the user's deposit address?

Answers:

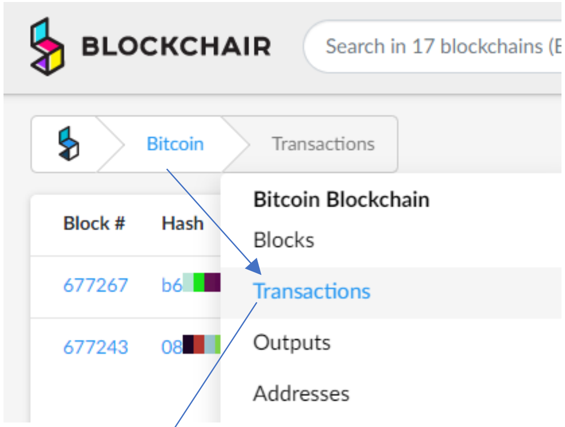
1) Xapo
2) 0.31785983 (by April 2021)
3) Bit2me



Flow:	0.317… BTC	Transfers:	6
Sent:	0.0000 BTC	Withdrawals:	0
Received:	0.317… BTC	Deposits:	6
Total Fees:	0.0000 BTC	Deposit Addresses:	1



Advanced Bitcoin Blockchain Search



BLOCKCHAIR

Search in 17 blockchains (E

Bitcoin > Transactions

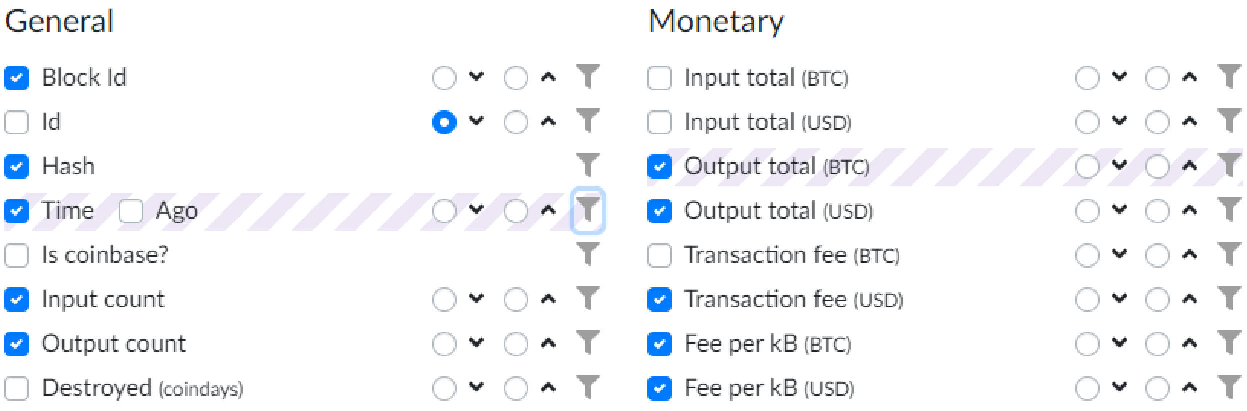
Block #	Hash
677267	b6
677243	08

Bitcoin Blockchain
- Blocks
- Transactions
- Outputs
- Addresses

At the beginning of 2021, EC3 Cyber Intelligence published a Cyberbit on advanced blockchain search using publicly available site blockchair.com.

This is a very flexible and powerful tool that performs advanced search better and faster than the majority of commercial tools.

The most useful filters for cryptocurrency investigators include Time and Output Total. Using these two filters, we can search for a specific amount during a selected timeframe:



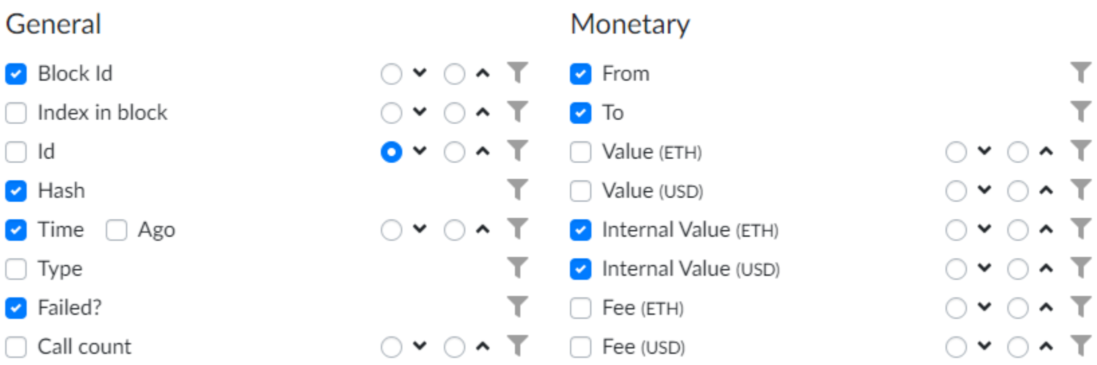
General
- ☑ Block Id
- ☐ Id ●
- ☑ Hash
- ☑ Time ☐ Ago
- ☐ Is coinbase?
- ☑ Input count
- ☑ Output count
- ☐ Destroyed (coindays)

Monetary
- ☐ Input total (BTC)
- ☐ Input total (USD)
- ☑ Output total (BTC)
- ☑ Output total (USD)
- ☐ Transaction fee (BTC)
- ☑ Transaction fee (USD)
- ☑ Fee per kB (BTC)
- ☑ Fee per kB (USD)

Such an approach could be applicable when searching for a specific amount demanded by a suspect of ransomware, or when you retrieve or intercept a message about a specific amount being sent by a suspect. Note that the tool can search outputs in both BTC and USD.

The tool is easy to use – you have to click at the funnel ▽ icon next to the field you would like to edit. Once you provide the parameters, the results above your query will update automatically. Please note that the time is queried and displayed in UTC format and the amounts are queried in Satoshi, which means that 1 BTC = 100,000,000 units.

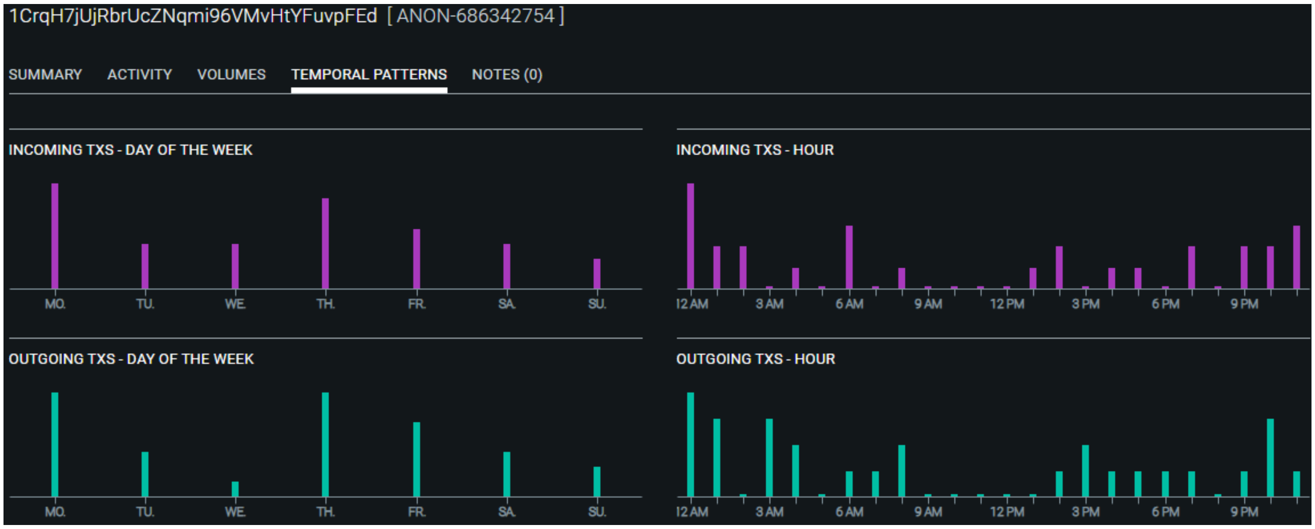
If this was not impressive enough, the tool provides support for many other blockchains, including ETH:



General
- ☑ Block Id
- ☐ Index in block
- ☐ Id ●
- ☑ Hash
- ☑ Time ☐ Ago
- ☐ Type
- ☑ Failed?
- ☐ Call count

Monetary
- ☑ From
- ☑ To
- ☐ Value (ETH)
- ☐ Value (USD)
- ☑ Internal Value (ETH)
- ☑ Internal Value (USD)
- ☐ Fee (ETH)
- ☐ Fee (USD)

Another publicly available tool is oxt.me that provides free temporal analysis for any submitted address. As an example, for address 1CrqH7jUjRbrUcZNqmi96VMvHtYFuvpFEd the tool displays the following day/time breakdown of the incoming and outgoing transactions:



There are two issues that you should be aware of when using this tool. Firstly, it only works on per-address basis, so it is not possible to get statistics for a cluster with many addresses. Additionally, as with most online tools, there is a concern of sharing sensitive data with the tools. In this particular case the concern may be real as the tool is closely associated with Samourai wallet, which is a privacy-oriented Android wallet.

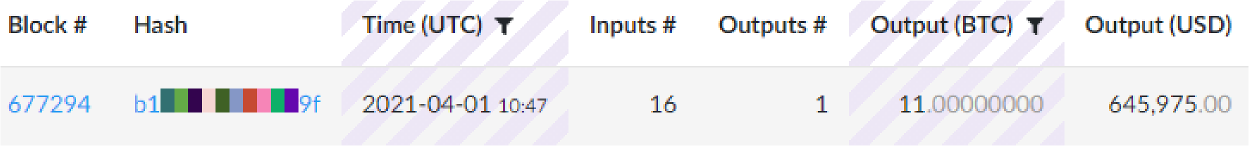
Advanced Search Q&A:

Your team intercepted a message that a suspect received 11 BTC deposit for his money laundering service on April 1, 2021 – so we have to search for an output with an exact value.

1) What was the ID of the Bitcoin transaction?
2) To which exchange the suspect subsequently sent it?
3) What was the deposit address at the exchange?
4) How many BTC did the address receive in total?

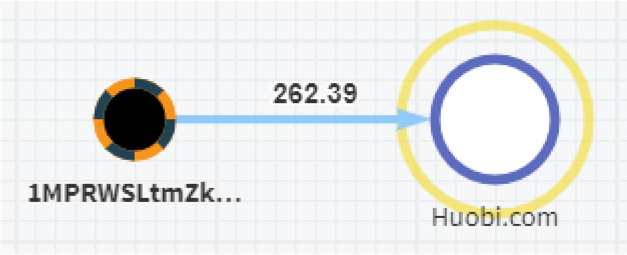
Answers:

1) The transaction in question was b132707164a94733044ef6d6d23f61258597c6c64a32f685b70db0686407ae9f



Block #	Hash	Time (UTC)	Inputs #	Outputs #	Output (BTC)	Output (USD)
677294	b1■■■■■■■■■■9f	2021-04-01 10:47	16	1	11.00000000	645,975.00

2) Naturally, the site does not provide any attribution so we have to use a commercial tool. As a result of this transaction, the suspect received 11 BTC to address 1MPRWSLtmZkvbdQVhk6iBkjmWaWRwpiLAK. He then sent the funds to Huobi:



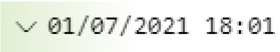
3) The deposit address was *1L1xSXttdsBAPVjVfyoyCg3RZbdHinT5G5*

4) Using the custom cluster function, we can see it has already been a large number; Well over 12,000 BTC by April 2021 and counting. The high number of transactions and volume suggests this could be a nested service – probably a swapper service using Huobi API.

Not all Timestamps Show What You Expect

When looking at timestamps, keep in mind that these typically show transaction *validation* time rather than time when the transaction actually took place.

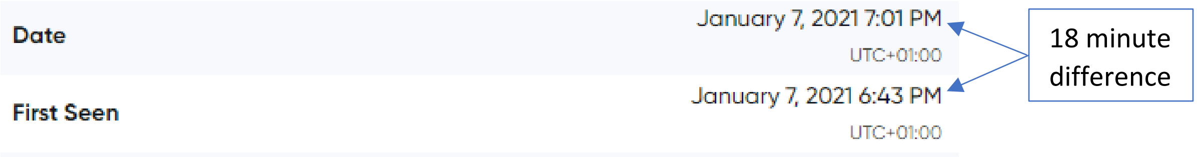
For example, when looking at transaction ID *15c7ab1119941f8c7d73bed76a630cd5dd36fa2faeae226b8009f20015983bea*, Chainalysis timestamp is 18:01. This is a time when the transaction was recorded in the blockchain in UTC format:



```
∨ 01/07/2021 18:01
```

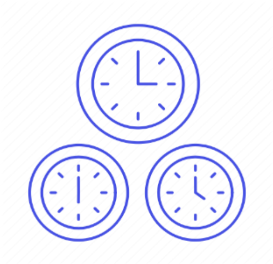
In order to find out an arguably more practical time – the time when the transaction was actually first observed (usually a fraction of the second after it is actually sent) – we have to use a blockchain explorer that collects this information. Surprisingly, there is only a handful of them; one such explorer can be found at https://explorer.bitcoin.com/btc.

Here, the transaction 15c7ab1119941f8c7d73bed76a630cd5dd36fa2faeae226b8009f20015983bea is shown with both relevant times – time when the transaction was sent and when it was validated. As you may notice, the difference between the two can sometimes be quite substantial.



Date	January 7, 2021 7:01 PM UTC+01:00
First Seen	January 7, 2021 6:43 PM UTC+01:00

18 minute difference



As you know, the BTC blocks are on average validated once every 10 minutes - but 30 or more minute gaps between the blocks are not a rare occurrence. Additionally, if a user decides to skimp on the transaction fee, the transaction may easily float around mempool for hours before it is validated.

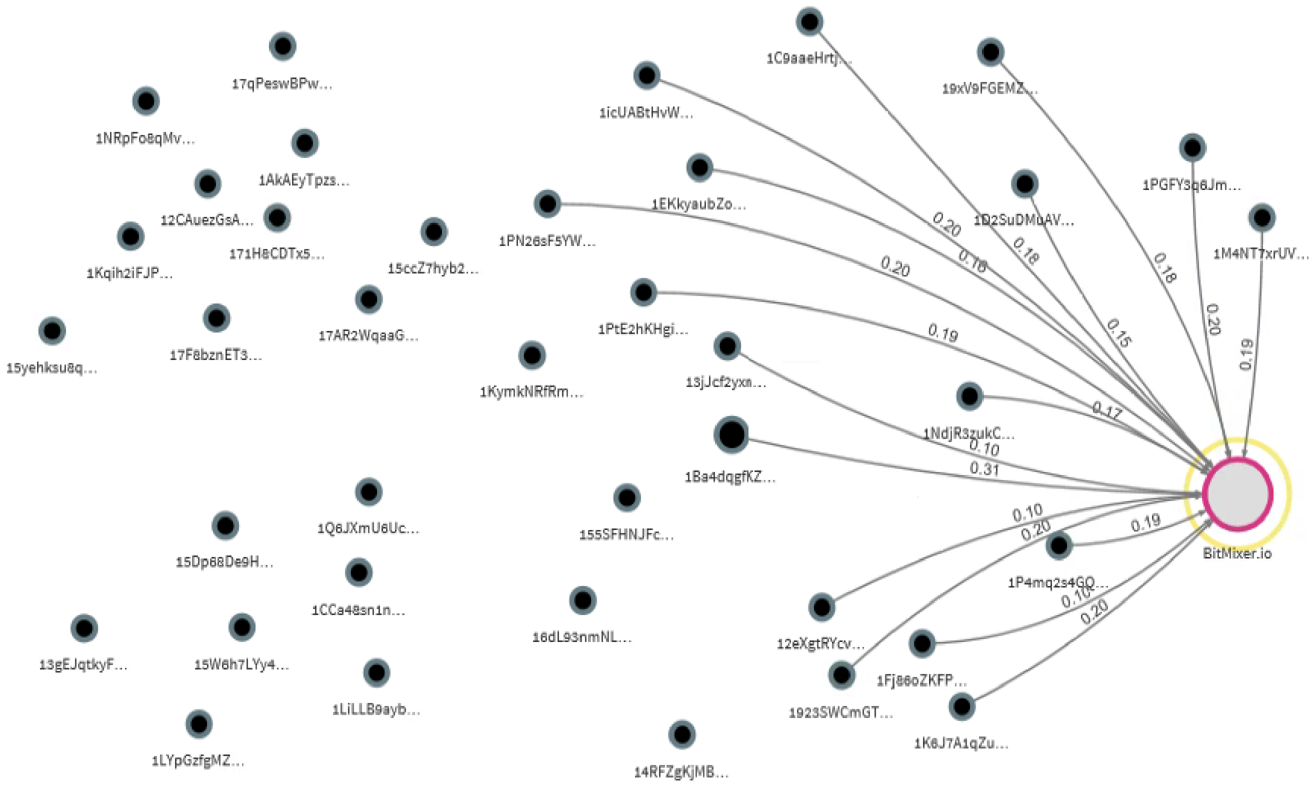
In most cases, block validation time is sufficient, however, at EC3 we already assisted several investigations where the exact time was of essence, for example when cross-referencing timestamps from Trezor logs with corresponding activity of a suspect's addresses in the blockchain. In some of these cases, an exact determination of time was required and this had to be established outside of the commercial tracing tools.

Bitcoin Mixers

Centralised Mixers:

In April, 2017, we sent 50 test transactions into Bitmixer.io. Bitmixer intentionally used a high number of wallets to actively pose challenges to the common heuristics employed by tracing tools. The efforts seemed to be successful as none of the deposits was identified by Chainalysis or any of the other tools.

Good news is that tools do improve over time. Six months later, Chainalysis managed to identify about 50% of the transactions. This means that the other half of the addresses were false negatives – addresses not identified by the software, while there were no false positives – addresses incorrectly assigned to a wrong entity:



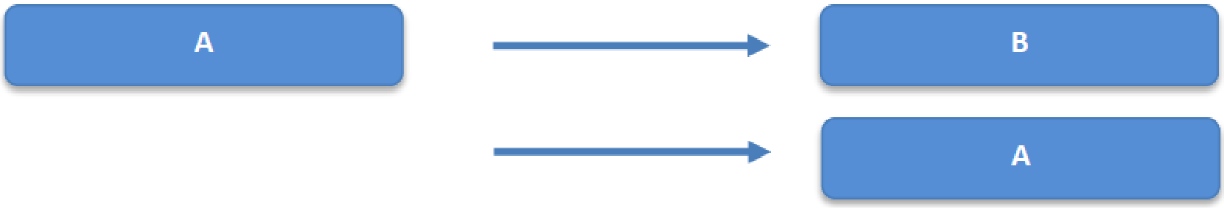
Based on our ad hoc observations, Chainalysis had an approximately similar identification rate with Bestmixer – a very popular mixer that was later taken down by Dutch law enforcement.

Needless to say, EC3 may assist with demixing of historical cases involving both Bitmixer, for which we developed a demixing tool, as well as Bestmixer, as a courtesy of Dutch colleagues who shared data with Europol.

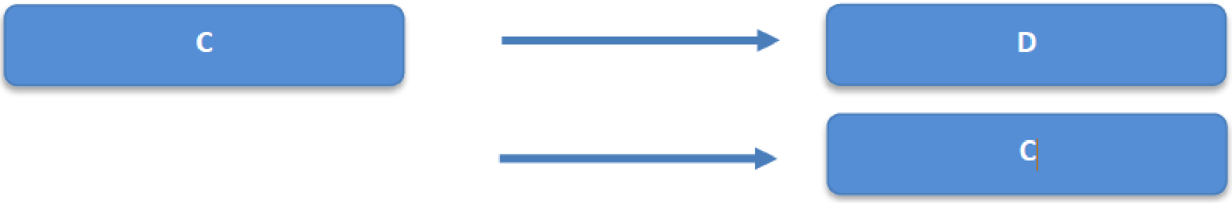
Decentralised Mixers

CoinJoin works by merging transactions signed by several users into one so that investigators cannot conclusively prove the link between the source and destination addresses. In order to make CoinJoin transaction work, it is still necessary to introduce an intermediary that will bring the participants together so that their funds may be merged within the same transaction - so most CoinJoin implementations are not fully decentralised.

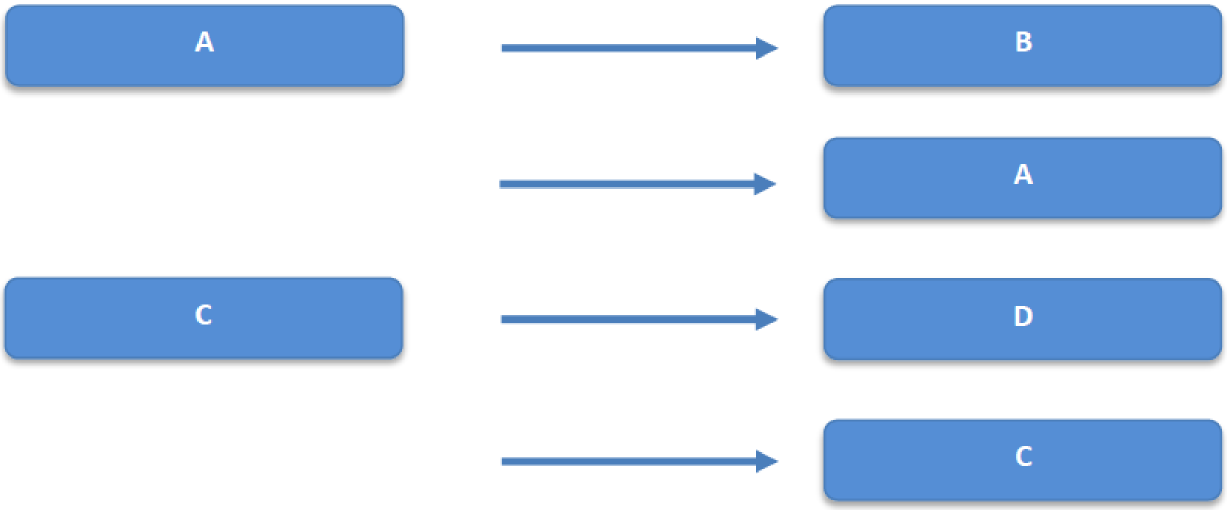
Transaction 1: Address A sends a payment to Address B and gets a change back:



Transaction 2: Address C sends a payment to Address D and gets a change back:



So far so good. However, Coinjoin does a misleading thing by merging these two transactions together so the final results look like this - a transaction that merges inputs and outputs sent by different parties(!):



This creates two issues for investigators:

1) It may be difficult to correctly pair inputs with relevant outputs.

2) This creates a challenge for bitcoin tracing tools that may erroneously cluster the input addresses belonging to different wallets (such as A and C above) together. Thus, CoinJoin goes against the basic clustering employed by the tracing tools and when ignored, it has potential to completely corrupt clustering and identification of entities. Fortunately, most tracing tools learned to recognize CoinJoin patterns and do not attempt to merge input addresses of these transactions.

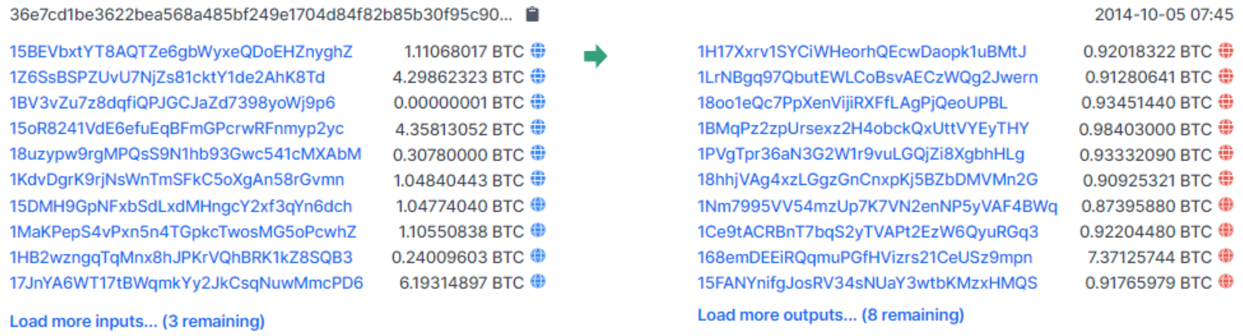
The most popular historical example of CoinJoin used to be SharedCoin operated by blockchain.info, providing users with increased levels of privacy especially between 2014 and 2016, with well over 10 million addresses involved in CoinJoin mixing.

After Blockchain.info stopped the mixing service, centralized mixers took over and despite some efforts, such as JoinMarket, the worthy successor came in 2018 when Wasabi Wallet started operating - and this service is still popular in April 2021. So far, Chainalysis identified almost 2 million addresses involved in Wasabi mixing.

Wasabi constitutes a considerable upgrade over the bugged SharedCoin that was fully deanonymized by German investigators; Should you run into an old case where SharedCoin needs demixing, consider contacting EC3. Wasabi, on the other hand, was partially deanonymized by Chainalysis, which can - under certain circumstances - demix coins of less careful users.

Good news is that that both CoinJoin types of transactions are easy to recognize:

Example of SharedCoin Transaction (2014)



36e7cd1be3622bea568a485bf249e1704d84f82b85b30f95c90...

15BEVbxtYT8AQTZe6gbWyxeQDoEHZnyghZ	1.11068017 BTC
1Z6SsBSPZUvU7NjZs81cktY1de2AhK8Td	4.29862323 BTC
1BV3vZu7z8dqfiQPJGCJaZd7398yoWj9p6	0.00000001 BTC
15oR8241VdE6efuEqBFmGPcrwRFnmyp2yc	4.35813052 BTC
18uzypw9rgMPQsS9N1hb93Gwc541cMXAbM	0.30780000 BTC
1KdvDgrK9rjNsWnTmSFkC5oXgAn58rGvmn	1.04840443 BTC
15DMH9GpNFxbSdLxdMHngcY2xf3qYn6dch	1.04774040 BTC
1MaKPepS4vPxn5n4TGpkcTwosMG5oPcwhZ	1.10550838 BTC
1HB2wzngqTqMnx8hJPKrVQhBRK1kZ8SQB3	0.24009603 BTC
17JnYA6WT17tBWqmkYy2JkCsqNuwMmcPD6	6.19314897 BTC

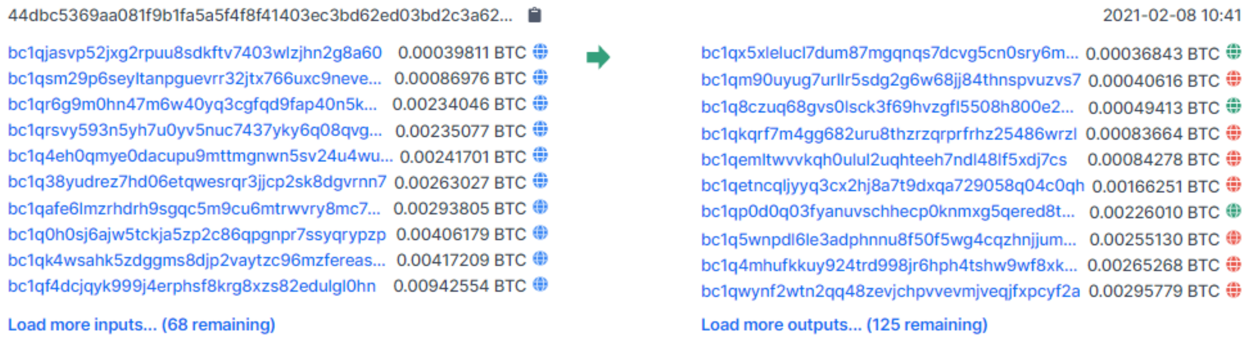
Load more inputs... (3 remaining)

2014-10-05 07:45

1H17Xxrv1SYCiWHeorhQEcwDaopk1uBMtJ	0.92018322 BTC
1LrNBgq97QbutEWLCoBsvAECzWQg2Jwern	0.91280641 BTC
18oo1eQc7PpXenVijiRXFfLAgPjQeoUPBL	0.93451440 BTC
1BMqPz2zpUrsexz2H4obckQxUttVYEyTHY	0.98403000 BTC
1PVgTpr36aN3G2W1r9vuLGQjZi8XgbhHLg	0.93332090 BTC
18hhjVAg4xzLGgzGnCnxpKj5BZbDMVMn2G	0.90925321 BTC
1Nm7995VV54mzUp7K7VN2enNP5yVAF4BWq	0.87395880 BTC
1Ce9tACRBnT7bqS2yTVAPt2EzW6QyuRGq3	0.92204480 BTC
168emDEEiRQqmuPGfHVizrs21CeUSz9mpn	7.37125744 BTC
15FANYnifgJosRV34sNUaY3wtbKMzxHMQS	0.91765979 BTC

Load more outputs... (8 remaining)

Example of Wasabi Transaction (2021)



44dbc5369aa081f9b1fa5a5f4f8f41403ec3bd62ed03bd2c3a62...

bc1qjasvp52jxg2rpuu8sdkftv7403wlzjhn2g8a60	0.00039811 BTC
bc1qsm29p6seyltanpguevrr32jtx766uxc9neve...	0.00086976 BTC
bc1qr6g9m0hn47m6w40yq3cgfqd9fap40n5k...	0.00234046 BTC
bc1qrsvy593n5yh7u0yv5nuc7437yky6q08qvg...	0.00235077 BTC
bc1q4eh0qmye0dacupu9mttmgnwn5sv24u4wu...	0.00241701 BTC
bc1q38yudrez7hd06etqwesrqr3jjcp2sk8dgvrnn7	0.00263027 BTC
bc1qafe6lmzrhdrh9sgqc5m9cu6mtrwvry8mc7...	0.00293805 BTC
bc1q0h0sj6ajw5tckja5zp2c86qpgnpr7ssyqrypzp	0.00406179 BTC
bc1qk4wsahk5zdggms8djp2vaytzc96mzfereas...	0.00417209 BTC
bc1qf4dcjqyk999j4erphsf8krg8xzs82edulgl0hn	0.00942554 BTC

Load more inputs... (68 remaining)

2021-02-08 10:41

bc1qx5xlelucl7dum87mgqnqs7dcvg5cn0sry6m...	0.00036843 BTC
bc1qm90uyug7urllr5sdg2g6w68jj84thnspvuzvs7	0.00040616 BTC
bc1q8czuq68gvs0lsck3f69hvzgfl5508h800e2...	0.00049413 BTC
bc1qkqrf7m4gg682uru8thzrzqrprfrhz25486wrzl	0.00083664 BTC
bc1qemltwvvkqh0ulul2uqhteeh7ndl48lf5xdj7cs	0.00084278 BTC
bc1qetncqljyyq3cx2hj8a7t9dxqa729058q04c0qh	0.00166251 BTC
bc1qp0d0q03fyanuvschhecp0knmxg5qered8t...	0.00226010 BTC
bc1q5wnpdl6le3adphnnu8f50f5wg4cqzhnjjum...	0.00255130 BTC
bc1q4mhufkkuy924trd998jr6hph4tshw9wf8xk...	0.00265268 BTC
bc1qwynf2wtn2qq48zevjchpvvevmjveqjfxpcyf2a	0.00295779 BTC

Load more outputs... (125 remaining)

Back in 2014-2016 transactions with a large number of outputs were not as common as they are now so SharedCoin was easy to spot.

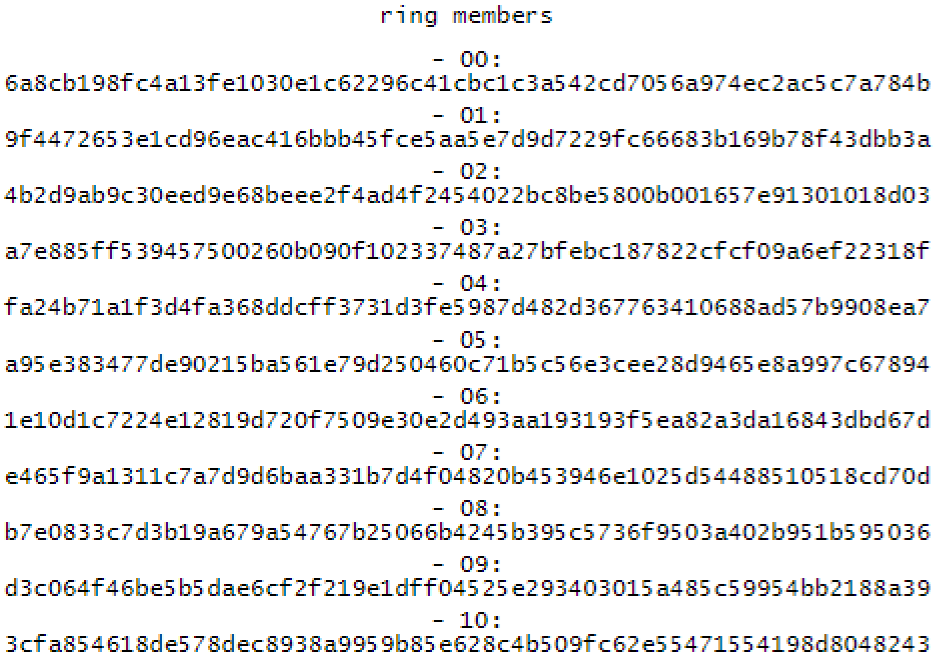
Although busy transactions are more common nowadays, CoinJoin transactions still stand out. With Wasabi, which is the most popular current CoinJoin implementation, transactions with over 100 inputs and 100 outputs are not uncommon, and with all addresses starting with bc1, and relatively standardized amounts, Wasabi transactions are immediately identifiable.

This is good news as investigators should always know when a suspect started using a mixer and when to stop with their tracing and possibly request deanonymization service, albeit with uncertain results, from the commercial tracing tools.

Privacy Coins

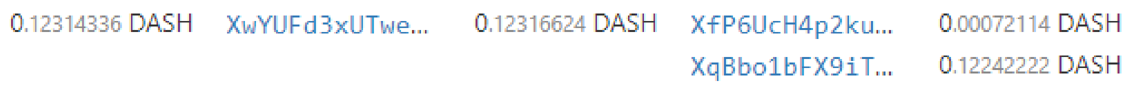
Another popular form of mixing is the use of privacy coins that started appearing since 2014. A privacy coin that features most frequently in cryptocurrency investigations is Monero, which uses stealth addresses (not searchable in the blockchain), RingCT (hidden amounts) and Ring Signatures (unrelated decoy inputs to confuse observers), combination of which prevents traditional cryptocurrency tracing.

Example of Monero input side – addresses are stealth, we do not know which one is actually controlled by the user and what is the amount sent:



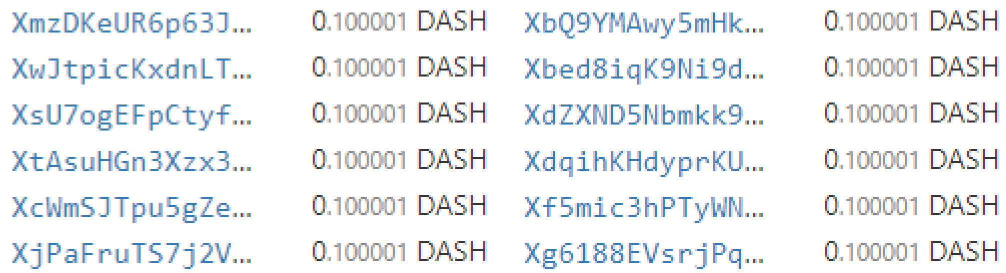
```
                          ring members

                             - 00:
6a8cb198fc4a13fe1030e1c62296c41cbc1c3a542cd7056a974ec2ac5c7a784b
                             - 01:
9f4472653e1cd96eac416bbb45fce5aa5e7d9d7229fc66683b169b78f43dbb3a
                             - 02:
4b2d9ab9c30eed9e68beee2f4ad4f2454022bc8be5800b001657e91301018d03
                             - 03:
a7e885ff539457500260b090f102337487a27bfebc187822cfcf09a6ef22318f
                             - 04:
fa24b71a1f3d4fa368ddcff3731d3fe5987d482d367763410688ad57b9908ea7
                             - 05:
a95e383477de90215ba561e79d250460c71b5c56e3cee28d9465e8a997c67894
                             - 06:
1e10d1c7224e12819d720f7509e30e2d493aa193193f5ea82a3da16843dbd67d
                             - 07:
e465f9a1311c7a7d9d6baa331b7d4f04820b453946e1025d54488510518cd70d
                             - 08:
b7e0833c7d3b19a679a54767b25066b4245b395c5736f9503a402b951b595036
                             - 09:
d3c064f46be5b5dae6cf2f219e1dff04525e293403015a485c59954bb2188a39
                             - 10:
3cfa854618de578dec8938a9959b85e628c4b509fc62e55471554198d8048243
```

There are also privacy coins with optional privacy, such as DASH or ZCASH – where it is up to the users if they wish to create transactions that are as transparent as bitcoin:



0.12314336 DASH	XwYUFd3xUTwe...	0.12316624 DASH	XfP6UcH4p2ku...	0.00072114 DASH
			XqBbo1bFX9iT...	0.12242222 DASH

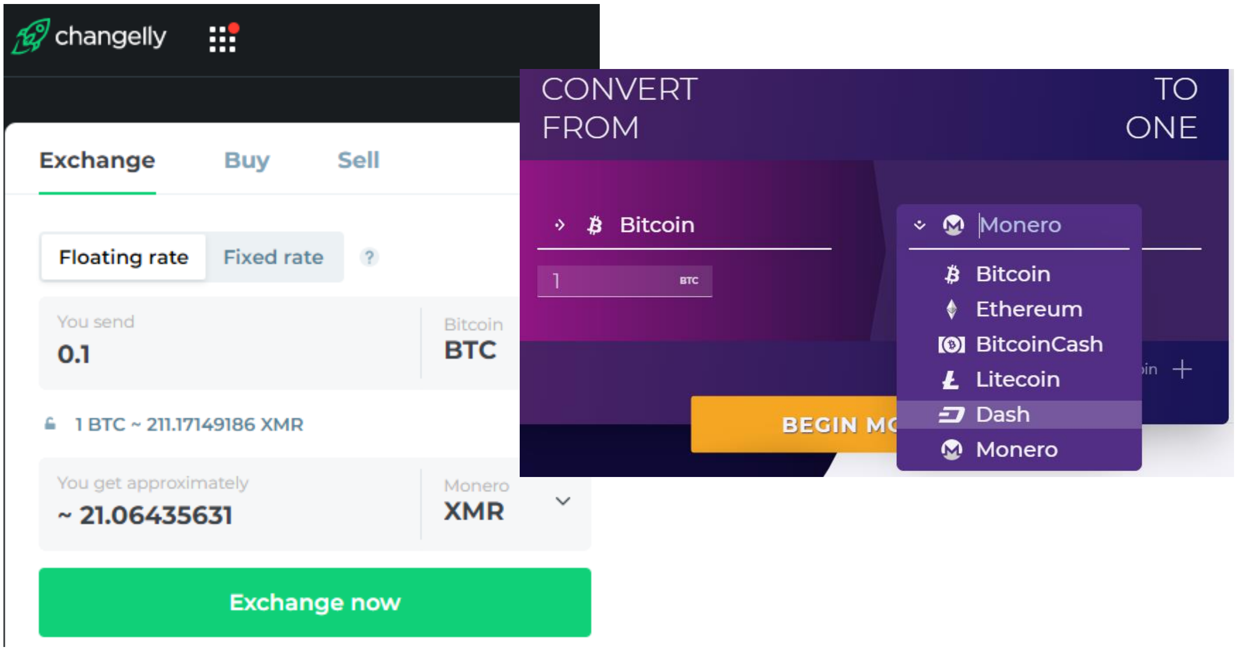
But – they may decide to obfuscate it through ZCash shielded transaction or several rounds of Dash coinjoin mixing with standardized amounts:



XmzDKeUR6p63J...	0.100001 DASH	XbQ9YMAwy5mHk...	0.100001 DASH
XwJtpicKxdnLT...	0.100001 DASH	Xbed8iqK9Ni9d...	0.100001 DASH
XsU7ogEFpCtyf...	0.100001 DASH	XdZXND5Nbmkk9...	0.100001 DASH
XtAsuHGn3Xzx3...	0.100001 DASH	XdqihKHdyprKU...	0.100001 DASH
XcWmSJTpu5gZe...	0.100001 DASH	Xf5mic3hPTyWN...	0.100001 DASH
XjPaFruTS7j2V...	0.100001 DASH	Xg6188EVsrjPq...	0.100001 DASH

Despite the altcoin communities attacking each other and claiming the other coin privacy features are lacking, any correct use of Monero, Dash or ZCash cannot currently be reliably demixed by LE agencies. In particularly serious investigations commercial tracing companies can be consulted but the success is far from guaranteed.

In recent years, many exchanges have either refused to list privacy coins or decided to delist privacy coins to become compliant with increasing regulatory requirements, where privacy coins clearly go against the necessity to prove the origin of funds required by AML legislation. At the same time, there are still large exchanges where privacy coins can be stored and traded; as well as instant crypto-to-crypto swappers such as https://www.morphtoken.com/ that allow conversion between Bitcoin and other coins including privacy coins without any user identification.



You send 0.1 Bitcoin BTC

1 BTC ~ 211.17149186 XMR

You get approximately ~ 21.06435631 Monero XMR

Altcoins: Bitcoin Forks

When talking about altcoins, in 2021 we still refer to all cryptocurrencies that are not Bitcoin. There are thousands of altcoins but as of April 2021, the market value of Bitcoin is still higher than the market value of all other currencies combined. While coverage of altcoins is beyond the scope of this Bitcoin guide, we will take a quick look at Bitcoin forks.

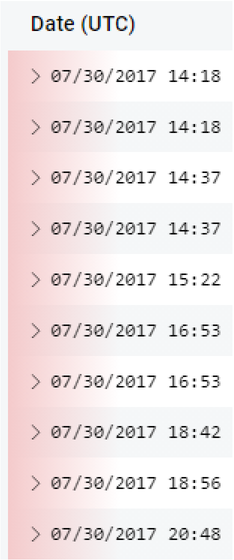
A fork results when one part of the community disagrees with the overall direction of the rest of the community and creates their version of the coin. Naturally, this has consequences for both users and investigators – while both coins will share the common blockchain up until the point of the fork, after the fork each of the coin movement will be recorded in a separate blockchain.

The most important split investigators need to be aware of occurred when Bitcoin split into Bitcoin (BTC) and Bitcoin Cash (BCH) due to community disagreement on how to solve scalability and other technical issues.

The split occurred in 1st of August 2017. It is important to remember this date because if you happen to investigate a crime that happened before this date, your suspect may have left traces on both Bitcoin blockchains afterwards.

Both Bitcoins and Bitcoin Cash have since experienced minor forks, for example Bitcoin later split into Bitcoin Gold, Bitcoin Diamond and many other forks that were of no interest to anyone.

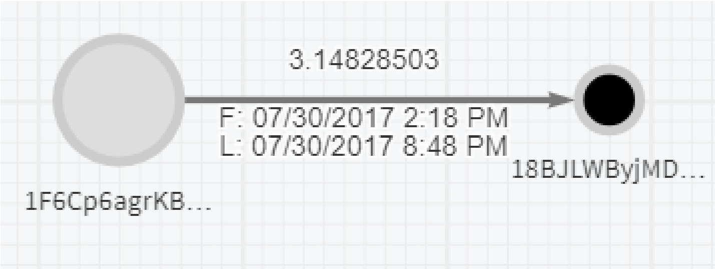
A practical example:



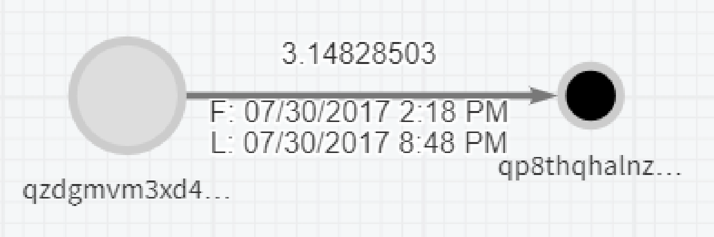
Date (UTC)
> 07/30/2017 14:18
> 07/30/2017 14:18
> 07/30/2017 14:37
> 07/30/2017 14:37
> 07/30/2017 15:22
> 07/30/2017 16:53
> 07/30/2017 16:53
> 07/30/2017 18:42
> 07/30/2017 18:56
> 07/30/2017 20:48

Consider the following 10 transactions, all sent from 1F6Cp6a… to 18BJLWB… (in this case the addresses are the same as the names of the clusters). All transactions were sent on July 30, 2017.

This is how the transaction looks like in a Bitcoin blockchain:



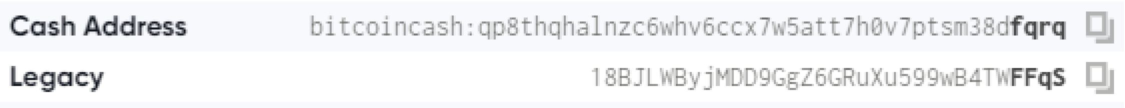
The same 10 transactions can also be observed in the Bitcoin Cash Blockchain:



In other words, there is no difference between the two blockchains apart from the address format.

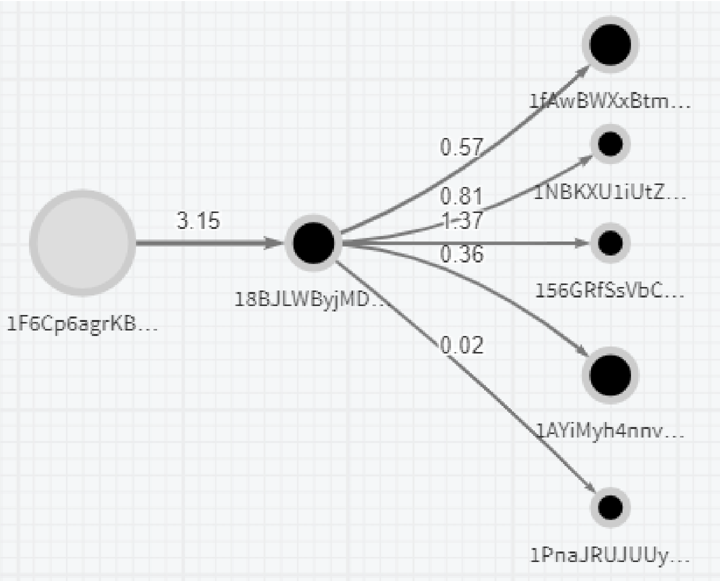
When Bitcoin forked into BTC and BCH, both coins kept the same address format, which was not a good idea. It resulted in users mistakenly sending funds from BTC to BCH addresses, leading to an understandable frustration in the communities. A few months after the split, Bitcoin Cash developers decided to change the address format to addresses started with q as can be observed on the above chart. At https://tools.bitcoin.com/cash-address-converter/ you may find a conversion tool between BTC and BCH – the tool works both ways.

Some blockchain explorers have the conversion built in and both address formats are queried as needed:

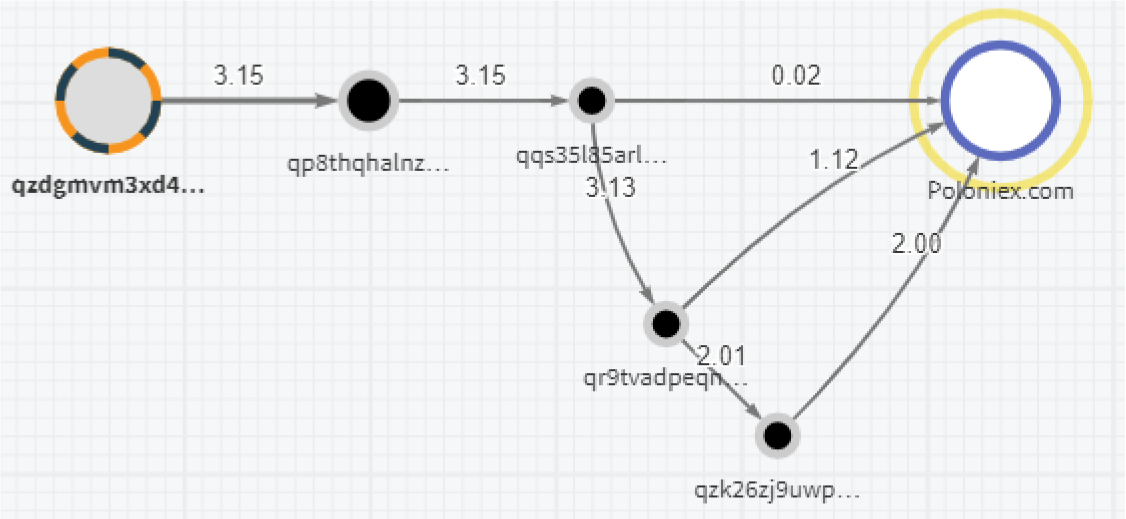


Cash Address	bitcoincash:qp8thqhalnzc6whv6ccx7w5att7h0v7ptsm38d**fqrq**
Legacy	18BJLWByjMDD9GgZ6GRuXu599wB4TW**FFqS**

The address format issue aside, BTC and BCH transactions that occurred before the fork are common for both exchanges, however, when we follow the transactions of the above addresses after August 1, the BTC and BCH transaction will differ – consider the following BTC chart where the tracing does not immediately produce a desirable outcome:

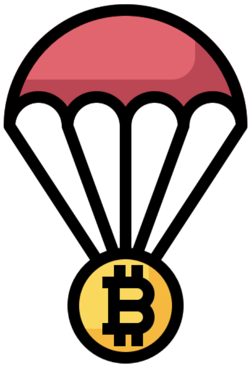


On the other hand, looking at the transaction in the Bitcoin Cash blockchain is very easy to follow as all funds have been sent to Poloniex exchange:



Bitcoin forks and airdrops – A friend or foe?

Is Bitcoin fork an opportunity or a threat? Certainly, an opportunity! Not only you may have twice as many opportunities to trace the suspect; many Bitcoin users see these forks as a welcome freebie they can instantly monetise by sending it straight to an exchange to convert it to Bitcoin - which certainly creates opportunities for investigators. There are no mixers in place for newly created coins and in many cases the investigator will observe direct transfers to an exchange.



The same situation applies to airdrops. A good example of an airdrop was Bitcoin Gold, which many users expected to drop in value soon after the introduction. Therefore, many forwarded their BTG straight to an exchange supporting the altcoin, right after the airdrop coins could have been moved in November 2017.

Such action naturally helps to identify users who would otherwise keep their Bitcoins untouched.

A list of Bitcoin forks can be seen at https://forkdrop.io; Note that most of the airdrops have close to 0 value.

Next Steps

The best learning material is hands-on practice – interaction with cryptocurrency wallets, services and on the job experience!

For those who prefer a more structured introduction into the topic, we recommend:

1) An online course on Bitcoin Fundamentals (free and certified) https://www.unic.ac.cy/blockchain/free-mooc/. The university also offers MSc. in Digital Currency, which is rather pricey.

2) A book on Cryptocurrency Investigations by Nick Furneaux - Investigating-Cryptocurrencies-Understanding-Extracting-Blockchain is available on Amazon. This does a great job covering fundamentals but does not address practical tracing using commercial tools.

3) A book *Tips and Tricks for Analysing Virtual Currency Transactions* by Filip Lacroix from Belgian Federal Police. A very comprehensive resource full of practical information – a masterpiece that took years to compile. The book can be downloaded from (EPE LE ONLY -> Library -> Education for Cryptocurrency Investigators)

4) There is a number of cryptocurrency investigation courses, the best ones are delivered by companies developing tracing tools. For agencies with limited resources, there is a number of live and pre-recorded webinars prepared by the tracing companies.

Europol Materials

5) Strategic publications, the most practical being the first *Bitcoin Guide for Investigators* and recently published *Cryptocurrency Services Review Guide*, evaluating exchanges and the assistance they provide to LE agencies. A number of shorter reports and thematic Cyberbits are also available.

6) EPE (Europol Platform for Experts): https://epe.europol.europa.eu - if you do not have login credentials please send us a request at o3@europol.europa.eu

   - Cryptocurrencies Group contains a list of contacts on over 2,300 investigators, as well as relevant publications and presentations from previously hosted cryptocurrency conferences: https://epe.europol.europa.eu/group/europol-virtual-currencies-taskforce
   - SIRIUS – a great resource on online service providers: https://epe.europol.europa.eu/group/law-enforcement-forum
   - BIN Checker Service for financial investigators: https://epe.europol.europa.eu/group/bin-checker-service
   - Digital Forensics Investigations for computer forensic examiners: https://epe.europol.europa.eu/group/digital-forensics-investigations