



# OECD International Academy for Tax Crime Investigation

*Anti-Money Laundering: Current Trends, Prosecutions,  
and the Challenges around Cryptocurrencies*

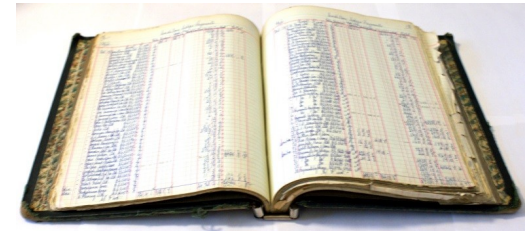


## Bitcoin Blockchain Explorers

# BLOCKCHAIN EXPLORERS: THE BASICS

# Blockchain Explorers

- The Bitcoin blockchain is a public digital ledger that documents every Bitcoin transaction that has ever taken place.
- Blockchain explorers allow you to view information:
  - Sending & Receiving addresses
  - Dates & Times
  - Amounts
  - Much more...
- Blockchain explorers allow you to search for:
  - Block numbers
  - Addresses
  - Transaction hashes



<https://www.blockchain.com/charts/n-transactions-per-block>

<https://www.blockchain.com/charts/avg-block-size>

# Blockchain Explorers

- Many blockchain explorers allow you to view data from different blockchains.
- Blockchain explorers take the raw data from blockchains and present it to you in a human readable way.
- Different blockchain explorers may present the data more usefully.

# Blockchain Explorers

- Don't identify wallets
- Don't identify owners
- Don't identify change addresses
- Do provide more extensive transaction data than tracing tools like Chainalysis
- Do provide greater access to data contained in transaction messages
- Do allow you to corroborate tracing tool conclusions
- Often provide multiple language support

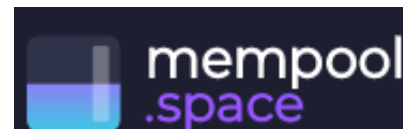
# Language Support



English
Español
Português
Русский
Türkçe
Italiano
Español (Latinoamérica)
Français
Deutsch



English	ENG
Español	SPA
Français	FRA
Italiano	ITA
Nederlands	DUT
Português	POR
Русский	RUS
中文	CHI
فارسی	PER
Bahasa Indonesia	IND
Türkçe	TUR
日本語	JPN
한국어	KOR
Deutsch	DEU



العربية	Nederlands
Català	日本語
Čeština	Norsk
Deutsch	Polski
English	Português
Español	Română
فارسی	Русский
Français	Slovenščina
한국어	Suomi
हिन्दी	Svenska
Italiano	ไทย
עברית	Türkçe
ქართული	Українська
Magyar	Tiếng Việt
Македонски	中文

# Blockchain Timestamps

[https://en.bitcoin.it/wiki/Block\\_timestamp](https://en.bitcoin.it/wiki/Block_timestamp)

- Bitcoin uses UTC time.
- Block times are accurate only to **within two hours**.

A timestamp is accepted as valid if it is greater than the median timestamp of previous 11 blocks, and less than the network-adjusted time + **2 hours**. Network-adjusted time" is the median of the timestamps returned by all nodes connected to you. As a result, **block timestamps are not exactly accurate** and they do not need to be to operate.

# Some Bitcoin Blockchain Explorers

- **Bitinfocharts:** <https://bitinfocharts.com/>
- **Blockchain.com:** <https://www.blockchain.com/>
- **Blockstream:** <https://blockstream.info/>
- **Blockchair:** <https://blockchair.com/>
- **Mempool:** <https://Mempool.Space/>
- **CoinMarketCap:** <https://blockchain.coinmarketcap.com/>
  - CoinMarketCap Block Explorer Guide: <https://coinmarketcap.com/guides/blockexplorer#guide-main>



# ADDRESSES

# Addresses

- You can search for addresses in an explorer and it will provide you with a list of all the sending and receiving transactions the address has participated in.
- You may be able to identify the other addresses that are in the same wallet by looking at their spending patterns.
  - Addresses that co-spend must be in the same wallet

<https://blockstream.info/>

## Address ⓘ

USD BTC

This address has transacted 2 times on the Bitcoin blockchain. It has received a total of 60.87000000 BTC (\$1,177,094.93) and has sent a total of 60.87000000 BTC (\$1,177,094.93). The current value of this address is 0.00000000 BTC (\$0.00).



Address	1Bb4mQ6G6wqdnRuCqA7YZSMsGnB59DS9cU
Format	BASE58 (P2PKH)
Transactions	2
Total Received	60.87000000 BTC
Total Sent	60.87000000 BTC
Final Balance	0.00000000 BTC

Blockstream Explorer
Bitcoin
Liquid

Dashboard
Blocks
Transactions

### Address

1Bb4mQ6G6wqdnRuCqA7YZSMsGnB59DS9cU

CONFIRMED TX COUNT	2
CONFIRMED RECEIVED	1 output (60.87 BTC)
CONFIRMED SPENT	1 output (60.87 BTC)
CONFIRMED UNSPENT	No outputs

<https://blockstream.info/>

<https://blockchair.com/>

<https://bitinfocharts.com/bitcoin/>

# Exercise

## Wannacry Ransomware Address

- Use a **blockchair.com** as well as **Blockstream.info** to examine the following address:

**115p7UMMngo1pMvkpHijcRdfJNXj6LrLn**

1. How many Bitcoins has it received in total?
2. What date and time was the first donation?
3. What was the date and time of the last donation?
4. Is the same date and time given in both blockchain explorers?
5. Examine the address timeline in Bitinfocharts
  - Does Bitinfocharts give you a better picture of the address activity?

# Wannacry - Blockchair



Address

115p7UMMngoj1pMvvpHijcRdfJNXj6LrLn

## Balance

0.46702392 BTC · 9,042.63 USD

Total received

14.87769994 BTC · 30,258.40 USD

Total spent

14.41067602 BTC · 39,250.36 USD



Wallet statement



Wallet statement



BLOCKCHAIR

info@blockchair.com

https://blockchair.com

12/05/2017 - 10/10/2022 (Part 1/1)

## WALLET STATEMENT

BITCOIN

WALLET ADDRESS: 115p7UMMngoj1pMvvpHijcRdfJNXj6LrLn

STATEMENT PERIOD: 12/05/2017 - 10/10/2022


### BTC BALANCE SUMMARY:

STARTING BALANCE (12/05/2017)	0.00000000 BTC	0.00 USD
TOTAL RECEIVED	14.87769994 BTC	30,259.36 USD
TOTAL SENT	14.41067602 BTC	39,250.36 USD
ENDING BALANCE (10/10/2022)	0.46702392 BTC	9,042.63 USD

### HISTORY OF TRANSACTIONS: 12/05/2017 - 10/10/2022

#	TIME		AMOUNT (BTC)	AMOUNT (USD)	TRANSACTION HASH
1	2017-05-12 13:34:58	Received	0.15000000	273.87	01b9e19b74335b6ab5f56abee48a861ed e31d997a64d4d624748ae65921c8e86

# Wannacry - Blockstream

 Blockstream Explorer


BitcoinLiquid

DashboardBlocksTransactions

Search for block height, hash, transaction, or address

## Address

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn




CONFIRMED TX COUNT	124
CONFIRMED RECEIVED	122 outputs (14.87769994 BTC)
CONFIRMED SPENT	112 outputs (14.41067602 BTC)
CONFIRMED UNSPENT	10 outputs (0.46702392 BTC)






## Transaction



01b9e19b74335b6ab5f56abee48a861ede31d997a64d4d624748ae65921c8e86






Blockstream Explorer

 Bitcoin
 Liquid


Dashboard
Blocks
Transactions

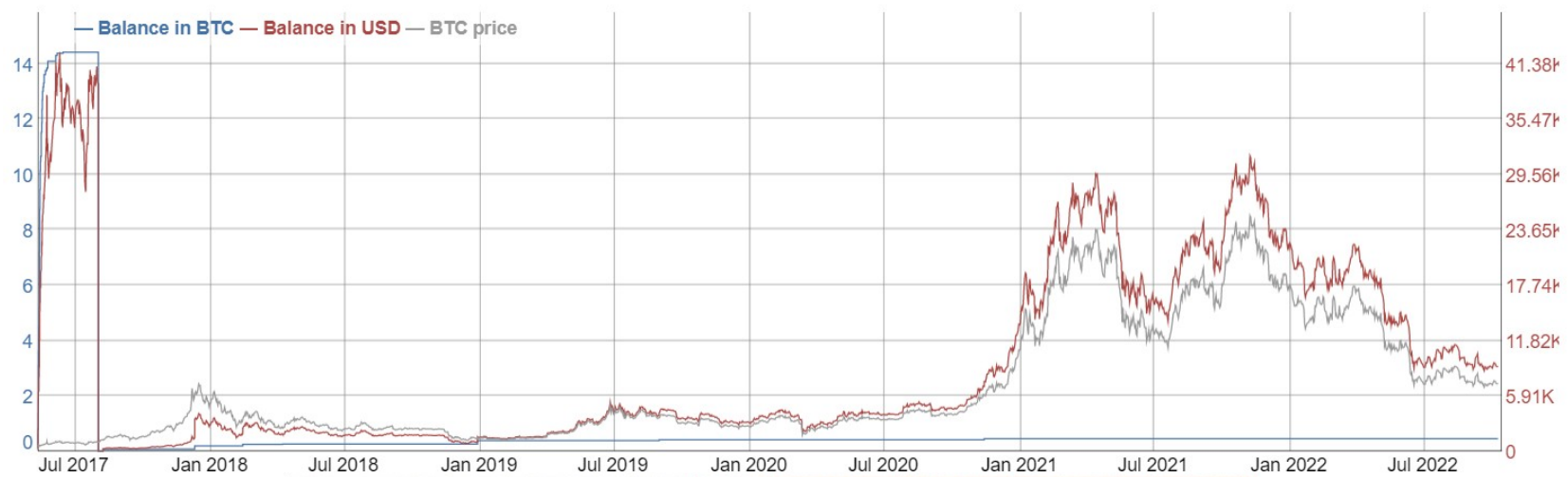
Search for block height, hash, transaction, or address



 Transaction

14449446275da0bf11825d14733fcc28f7264f8a2c3a506752f92fddb8e1aa16


STATUS	101179 Confirmations
INCLUDED IN BLOCK	0000000000000000000000008746b94257e056b29166411f64681e4aaa86fea57869
BLOCK HEIGHT	656858
BLOCK TIMESTAMP	2020-11-14 02:08:23 GMT -5
TRANSACTION FEES	0.0011388 BTC (129.4 sat/vB)
SIZE	880 B
VIRTUAL SIZE	880 vB
WEIGHT UNITS	3520 WU
VERSION	1
LOCK TIME	0





# TRANSACTIONS

# “Coinbase Transaction”

(The reward that was paid to the miner)

Block Reward	6.25000000 BTC
--------------	----------------

Fee Reward	0.04385193 BTC
------------	----------------

## Block Transactions ⓘ

Fee 0.00000000 BTC  
(0.000 sat/B - 0.000 sat/WU - 351 bytes)  
(0.000 sat/vByte - 324 virtual bytes)

6.29385193 BTC

Hash [d6eedf232a48df9d911c35f14c4911abdd1111660ec778...](#)

2022-01-28 06:37

COINBASE (Newly Generated Coins)



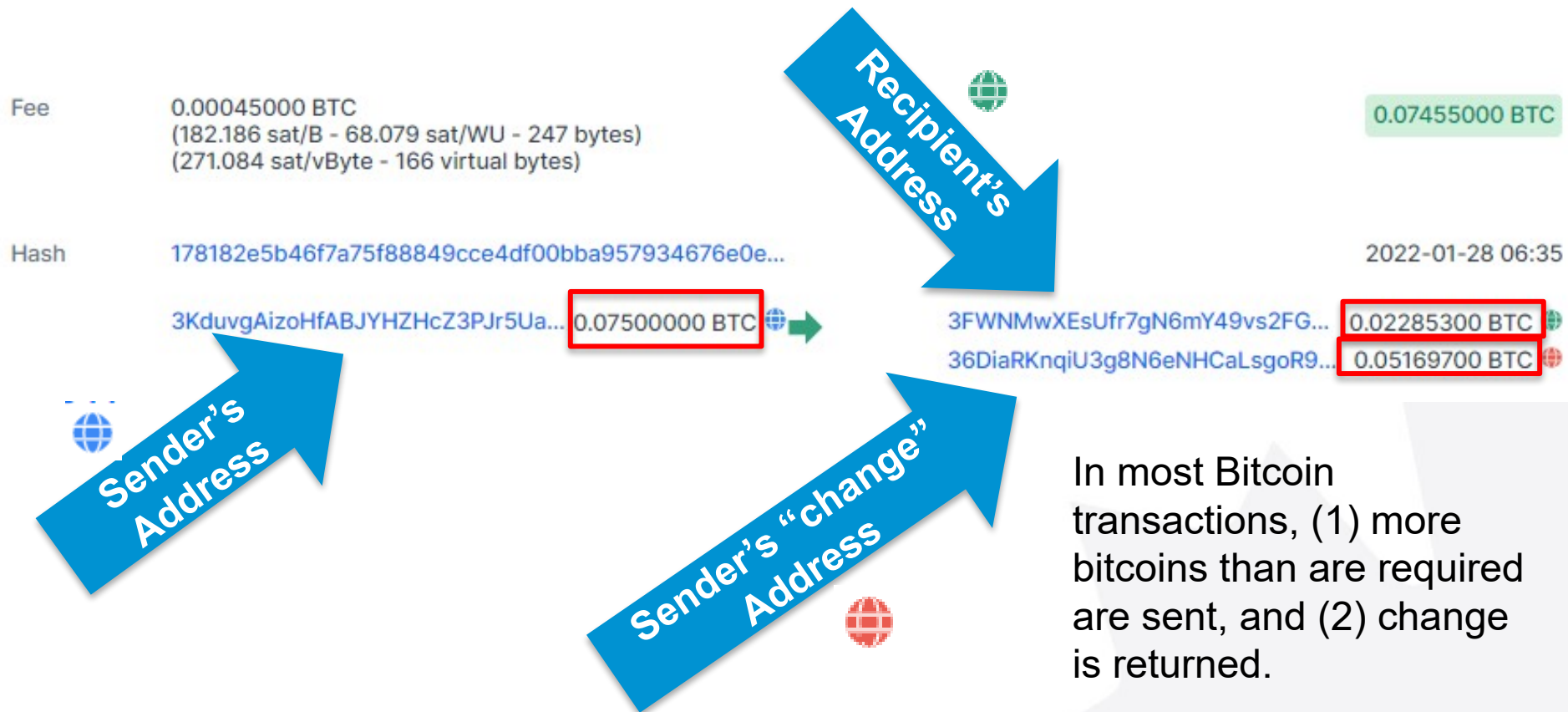
[12dRugNcdxK39288NjcDV4GX7rM...](#) 6.29385193 BTC

OP\_RETURN 0.00000000 BTC

OP\_RETURN 0.00000000 BTC

OP\_RETURN 0.00000000 BTC

# Simple Transactions



# Simple Transaction



More than one addresses' BTC were required to make up enough BTC to send to the recipient.




# Service Transactions



Service transactions are batched to save fees

# Following transactions

- You can follow transactions forward or backward by looking up the addresses involved and finding where the bitcoins came from or went.
- Following transactions may lead you to Exchanges or other money service businesses where you can serve production orders and/or obtain KYC information.

Fee	0.00045000 BTC (182.186 sat/B - 68.079 sat/WU - 247 bytes) (271.084 sat/vByte - 166 virtual bytes)	0.07455000 BTC
Hash	178182e5b46f7a75f88849cce4df00bba957934676e0e...	2022-01-28 06:35
	3KduvgAizoHfABJYHZHcZ3Pjr5Ua... 0.07500000 BTC 	3FWNMwXEsUfr7gN6mY49vs2FG... 0.02285300 BTC 
		36DiaRKnqiU3g8N6eNHCaLsgoR9... 0.05169700 BTC 

# Exercise

## WannaCry Ransomware Address

**13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94**

1. Find a transaction that sent bitcoins to the WannaCry Address
2. Did the transaction send bitcoins to other more than two addresses at the same time?
  - How many?
3. What would two receiving addresses suggest?
4. What would more than two receiving addresses suggest?

<https://www.blockchain.com/explorer>



# Exercise

## WannaCry Ransomware Transaction

8def6458a46234ab0e040602e7852ff5cf58650f3f1102803b1d4bca4cc293a1

- Look up this WannaCry address sending transaction
  1. Did the transaction send bitcoins to more than two addresses at the same time?
  2. What does that suggest about the Wannacry address?

<https://www.blockchain.com/explorer>

# Transaction Exercise

<https://blockchair.com/>

<https://blockchair.com/>

**91aae9ca97764b101a1238a0134db12e64b15596b5e8bcfd7a3eae24c9944482**

- Use Blockchain.com as well as Blockchair to examine the transaction.
  1. Are the transaction amounts in BTC the same?
  2. Are the transaction amounts in USD the same?
  3. Are the time stamps the same?
- Export the transaction information from BlockChair by clicking on “Transaction Receipt”



Transaction receipt

# IDENTIFYING MULTISIGNATURE ADDRESSES

# Blockchain Transaction Scripts

- Blockchain transactions are complex scripts, and these scripts are stored in the blockchain.
- Script analysis can provides blockchain explorers with a large amount of information about a transaction:
  - Multisignature data
  - Replace by fee data
  - Segregated Witness data
  - Coinbase data
  - OP\_RETURN data

# Multisignature Identifying

- To verify if an address required multiple signatures to spend during a transaction:
  1. Search for the transaction in Mempool.Space (<https://Mempool.Space/>)
  2. Examine the “**Inputs and Outputs**” for a yellow bubble indicating whether the sending address was multisig (and how many signatures were used)
  3. Click on “**Details**” to see the script.
    - The first OP\_PUSHNUM\_# indicates the number of keys used.
    - The second OP\_PUSHNUM\_# indicates the total number of possible keys for the multisig address.

# MESSAGES IN THE BLOCKCHAIN

# Messages or data can be inserted into the Bitcoin blockchain

- Messages can be created using **vanity addresses**.
- Messages can be added by miners into **Coinbase transactions**.
- Messages of up to 80 bytes can be inserted during user transactions by the sender by using the **OP\_RETURN** function.

# Exercise

## Messages in the Bitcoin blockchain

1. What was the message inserted into the first bitcoin transaction? (**Look at the “Technical Details” Coinbase Data.**)
  - <https://blockchair.com/bitcoin/block/0>
2. What was the November 20, 2016 WikiLeaks Message made using bitcoin addresses in a transaction. (**Look at the first characters in the receiving addresses.**)
  - <https://www.blockchain.com/btc/tx/fc722ce39094500690a4d4676fe475520d6a0af590336b73202010ca260bbd20>