OECD International Academy for Tax Crime Investigation

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

OECD

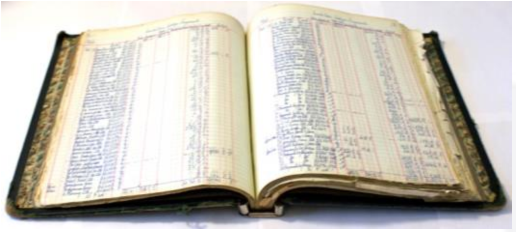
Bitcoin Blockchain Explorers

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

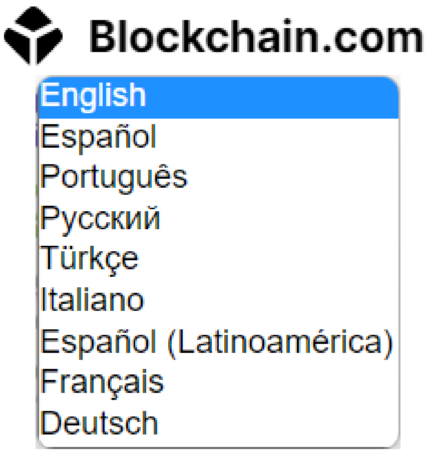
- Many blockchain explorers allow you to view data from different blockchains.
- Blockchain explorers take the raw data from blockchains and present it to you in a human readable way.
- Different blockchain explorers may present the data more usefully.

Blockchain Explorers

- Don’t identify wallets
- Don’t identify owners
- Don’t identify change addresses

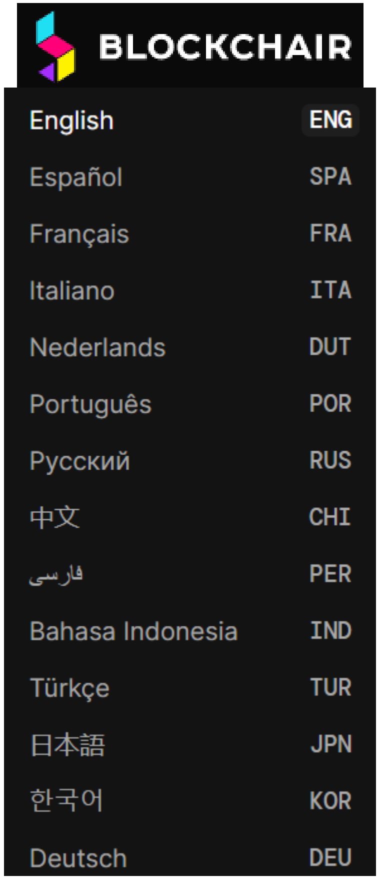
- Do provide more extensive transaction data than tracing tools like Chainalysis
- Do provide greater access to data contained in transaction messages
- Do allow you to corroborate tracing tool conclusions
- Often provide multiple language support

Language Support



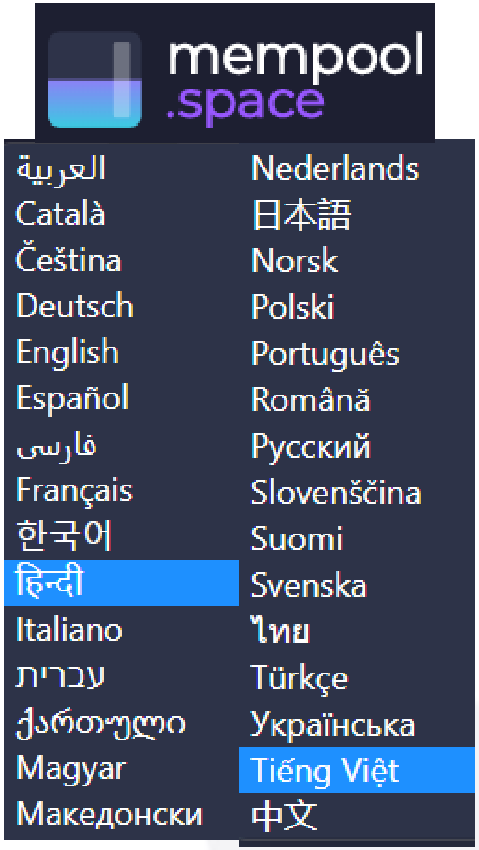
Blockchain.com

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



BLOCKCHAIR

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



mempool
.space

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

Note: Blockchain Timestamps

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.

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

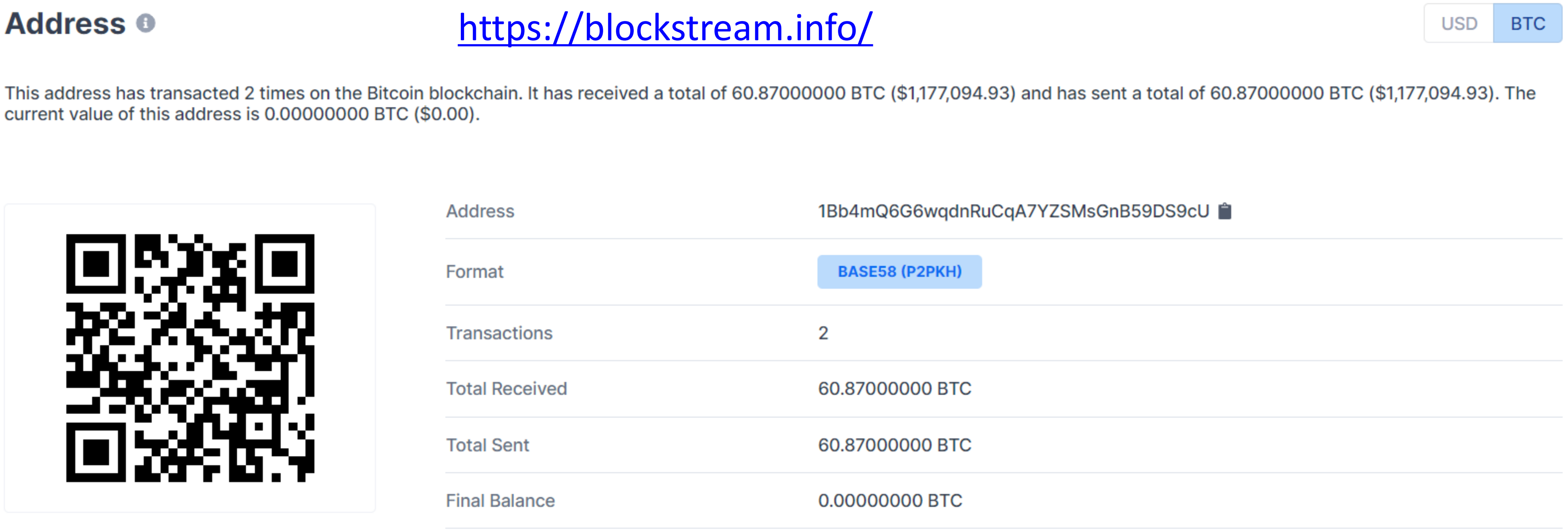
ADDRESSES

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/

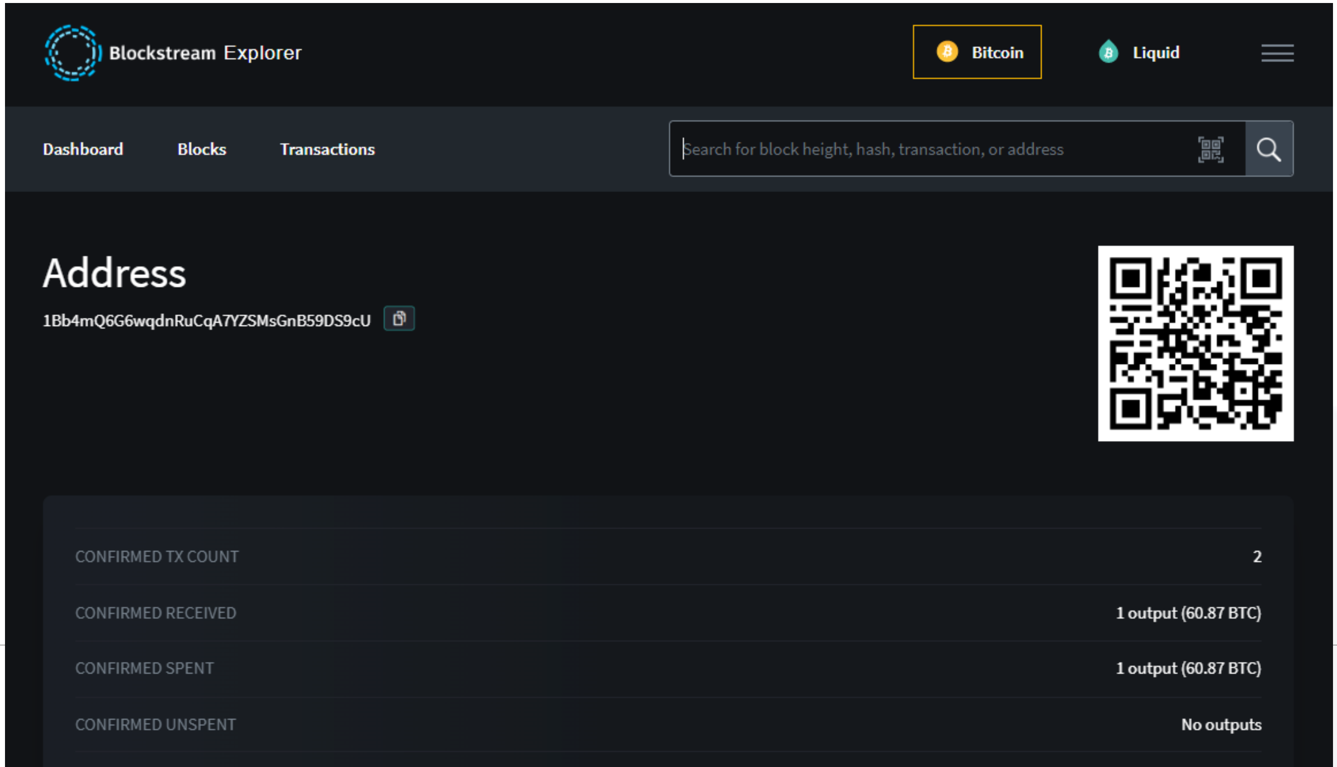


Address

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



Address

1Bb4mQ6G6wqdnRuCqA7YZSMsGnB59DS9cU

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

Exercise
Address analysis

- Examine the following Address in Blockchain.com https://www.blockchain.com/

  1FZEeDbvHG3xRaNFjU9jnKiEHLFKVBEsrU

- How many times did it receive Bitcoins?
- How many sending transactions did it make?
- How many other addresses can you identify as belonging to the same wallet?
  - Look for addresses that co-spend with it.

Exercise
Task Force Russich fundraising address

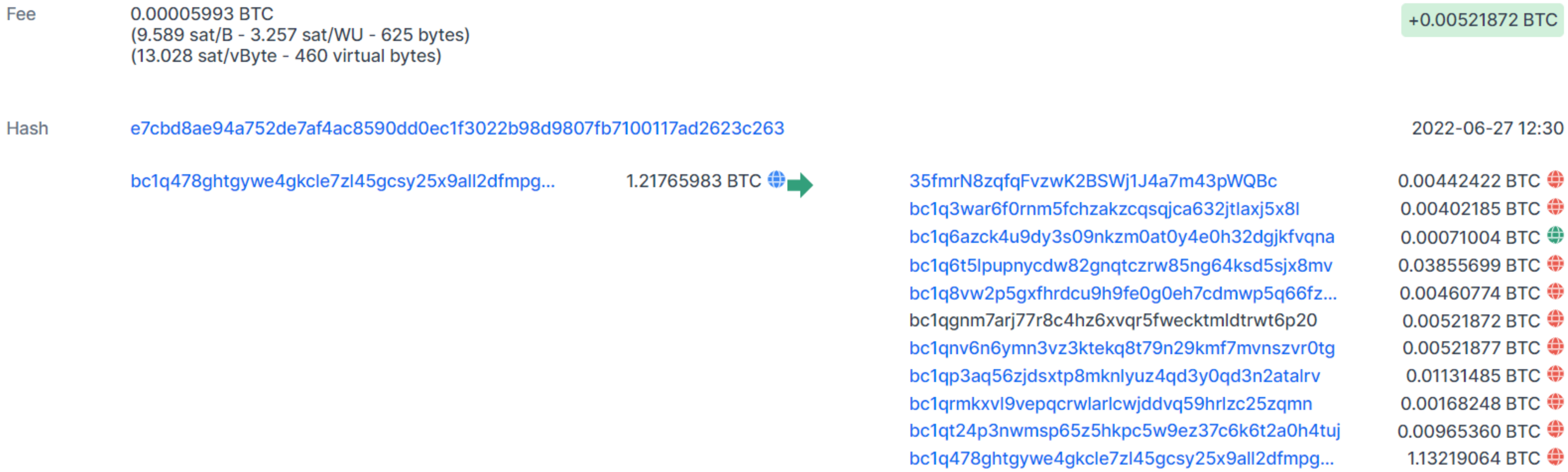
- Use a **blockchain.com** as well as **Mempool.Space** to examine the following address

bc1qgnm7arj77r8c4hz6xvqr5fwecktmldtrwt6p20

1. How many Bitcoins has it received in total?
2. What date and time was the first donation?
3. Is the same date and time given in both blockchain explorers?
4. Was the address set up after the start of the war in Ukraine?

https://www.blockchain.com/
https://Mempool.Space/

Task Force Russich first donation Blockhain.com – Blockchain.com



Fee 0.00005993 BTC
(9.589 sat/B - 3.257 sat/WU - 625 bytes)
(13.028 sat/vByte - 460 virtual bytes)

+0.00521872 BTC

Hash e7cbd8ae94a752de7af4ac8590dd0ec1f3022b98d9807fb7100117ad2623c263

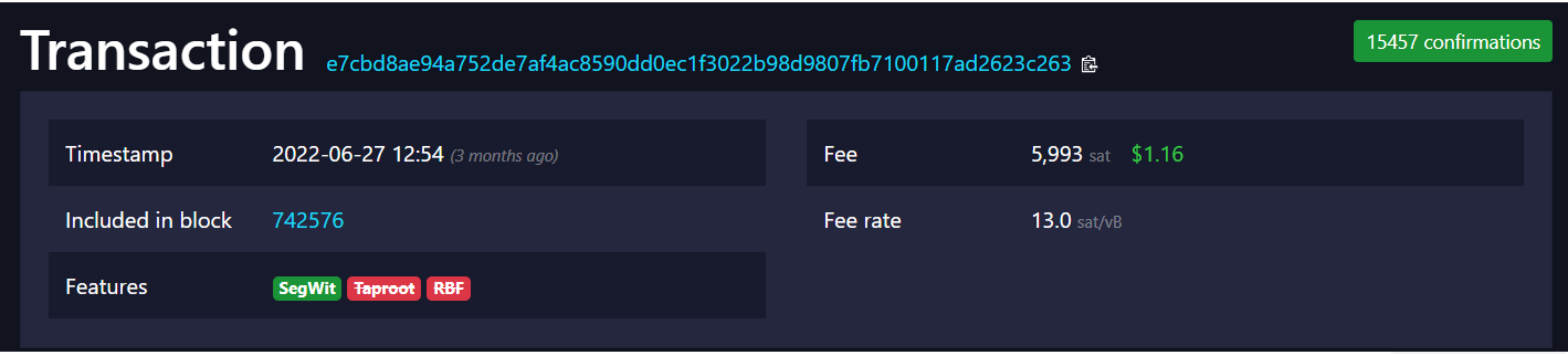
2022-06-27 12:30

bc1q478ghtgywe4gkcle7zl45gcsy25x9all2dfmpg... 1.21765983 BTC →

35fmrN8zqfqFvzwK2BSWj1J4a7m43pWQBc	0.00442422 BTC
bc1q3war6f0rnm5fchzakzcqsqjca632jtlaxj5x8l	0.00402185 BTC
bc1q6azck4u9dy3s09nkzm0at0y4e0h32dgjkfvqna	0.00071004 BTC
bc1q6t5lpupnycdw82gnqtczrw85ng64ksd5sjx8mv	0.03855699 BTC
bc1q8vw2p5gxfhrdcu9h9fe0g0eh7cdmwp5q66fz...	0.00460774 BTC
bc1qgnm7arj77r8c4hz6xvqr5fwecktmldtrwt6p20	0.00521872 BTC
bc1qnv6n6ymn3vz3ktekq8t79n29kmf7mvnszvr0tg	0.00521877 BTC
bc1qp3aq56zjdsxtp8mknlyuz4qd3y0qd3n2atalrv	0.01131485 BTC
bc1qrmkxvl9vepqcrwlarlcwjddvq59hrlzc25zqmn	0.00168248 BTC
bc1qt24p3nwmsp65z5hkpc5w9ez37c6k6t2a0h4tuj	0.00965360 BTC
bc1q478ghtgywe4gkcle7zl45gcsy25x9all2dfmpg...	1.13219064 BTC

+$101.19

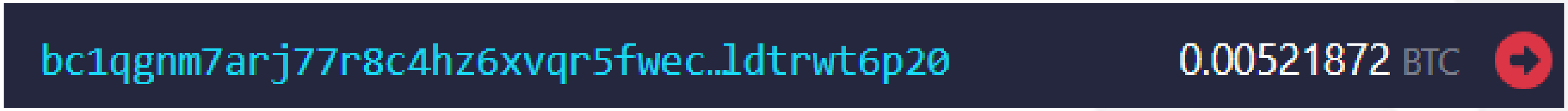
Task Force Russich first donation Blockhain.com – Mempool.space



Transaction e7cbd8ae94a752de7af4ac8590dd0ec1f3022b98d9807fb7100117ad2623c263

15457 confirmations

Timestamp	2022-06-27 12:54 *(3 months ago)*	Fee	5,993 sat $1.16
Included in block	742576	Fee rate	13.0 sat/vB
Features	SegWit ~~Taproot~~ RBF		



bc1qgnm7arj77r8c4hz6xvqr5fwec…ldtrwt6p20 0.00521872 BTC

https://blockstream.info/
https://blockchair.com/
https://bitinfocharts.com/bitcoin/

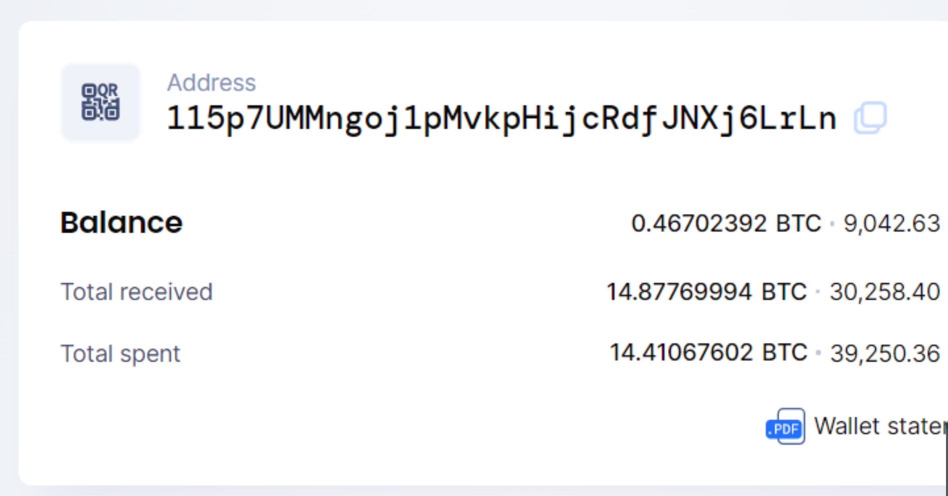
Exercise
Wannacry Ransomware Address

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

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

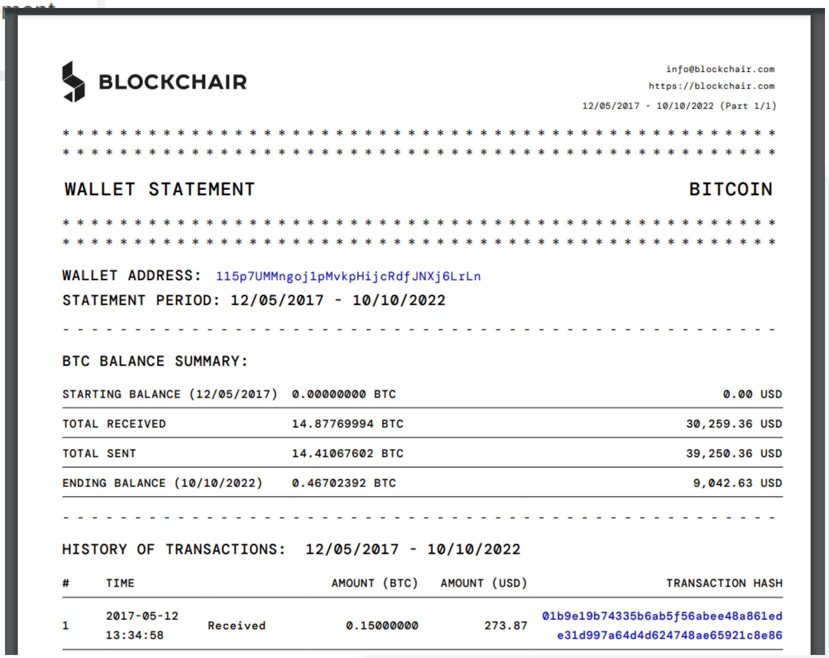
1. How many Bitcoins has it received in total?
2. What date and time was the first donation?
3. What was the date and time of the last donation?
4. Is the same date and time given in both blockchain explorers?
5. Examine the address timeline in Bitinfocharts
   - Does Bitinfocharts give you a better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

Wannacry - Blockchair



Address
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

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



BLOCKCHAIR

info@blockchair.com
https://blockchair.com
12/05/2017 - 10/10/2022 (Part 1/1)

WALLET STATEMENT BITCOIN

WALLET ADDRESS: 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
STATEMENT PERIOD: 12/05/2017 - 10/10/2022

BTC BALANCE SUMMARY:

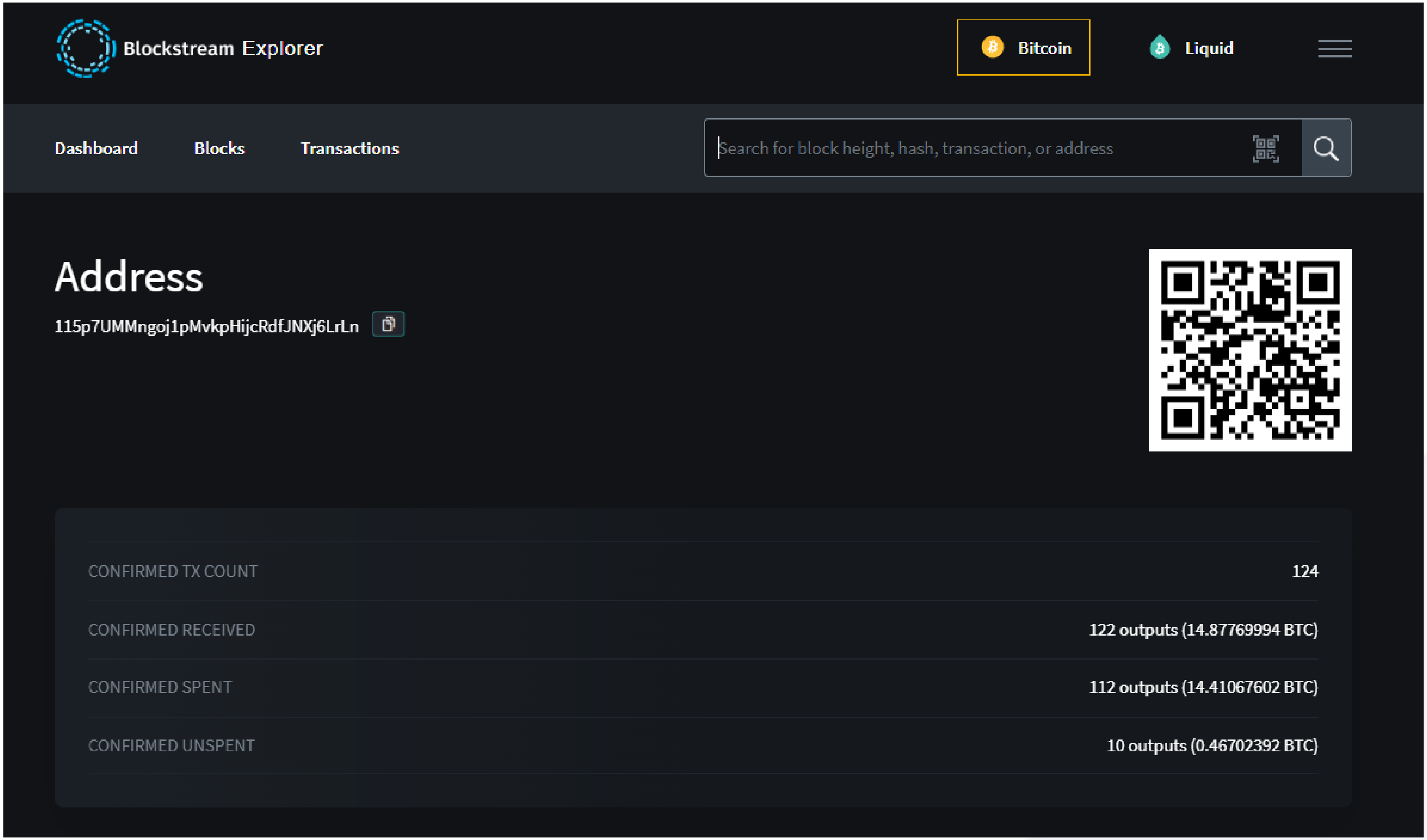
STARTING BALANCE (12/05/2017)	0.00000000 BTC	0.00 USD
TOTAL RECEIVED	14.87769994 BTC	30,259.36 USD
TOTAL SENT	14.41067602 BTC	39,250.36 USD
ENDING BALANCE (10/10/2022)	0.46702392 BTC	9,042.63 USD

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

.PDF Wallet statement

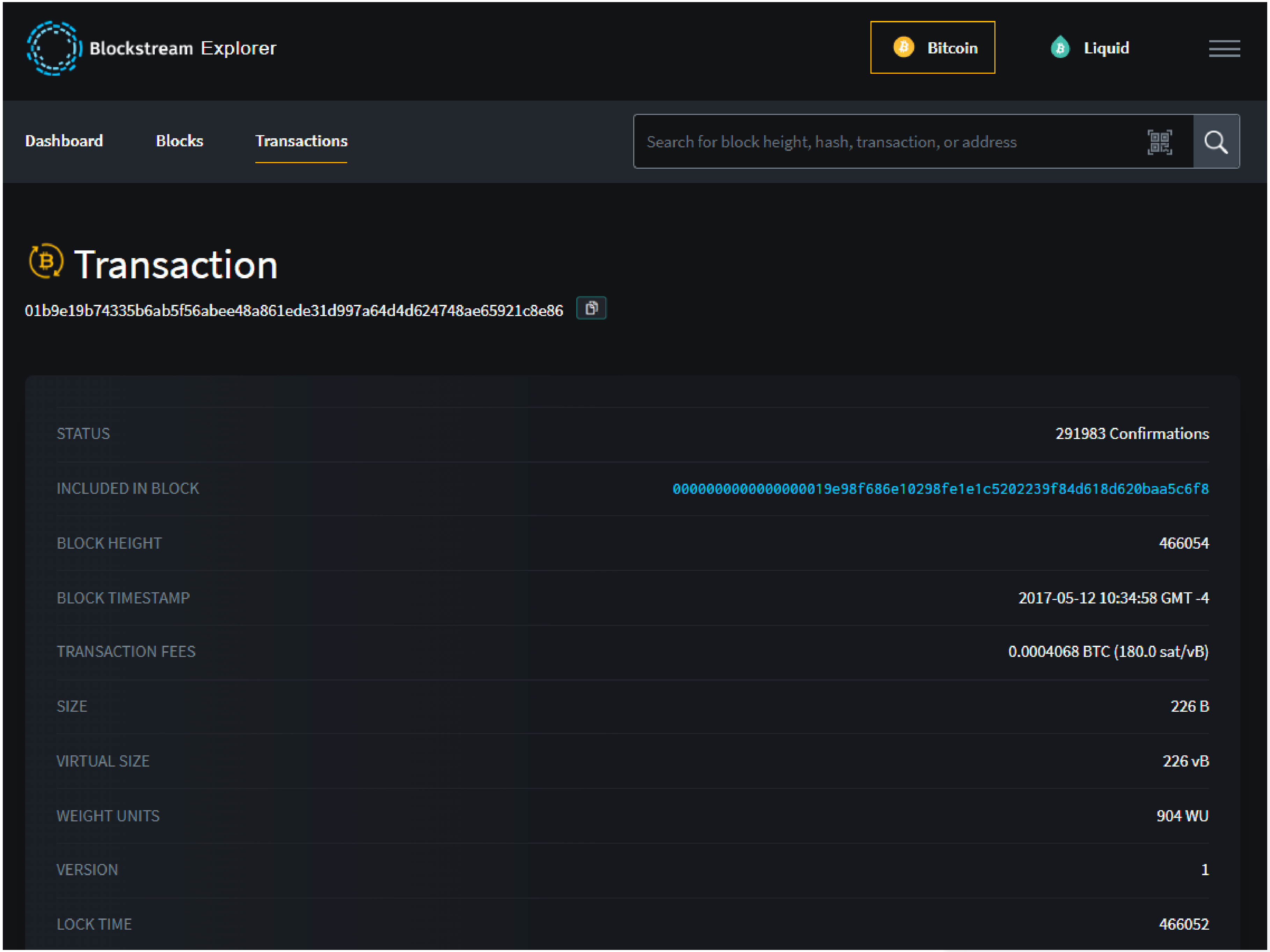
Wannacry - Blockstream



Address

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

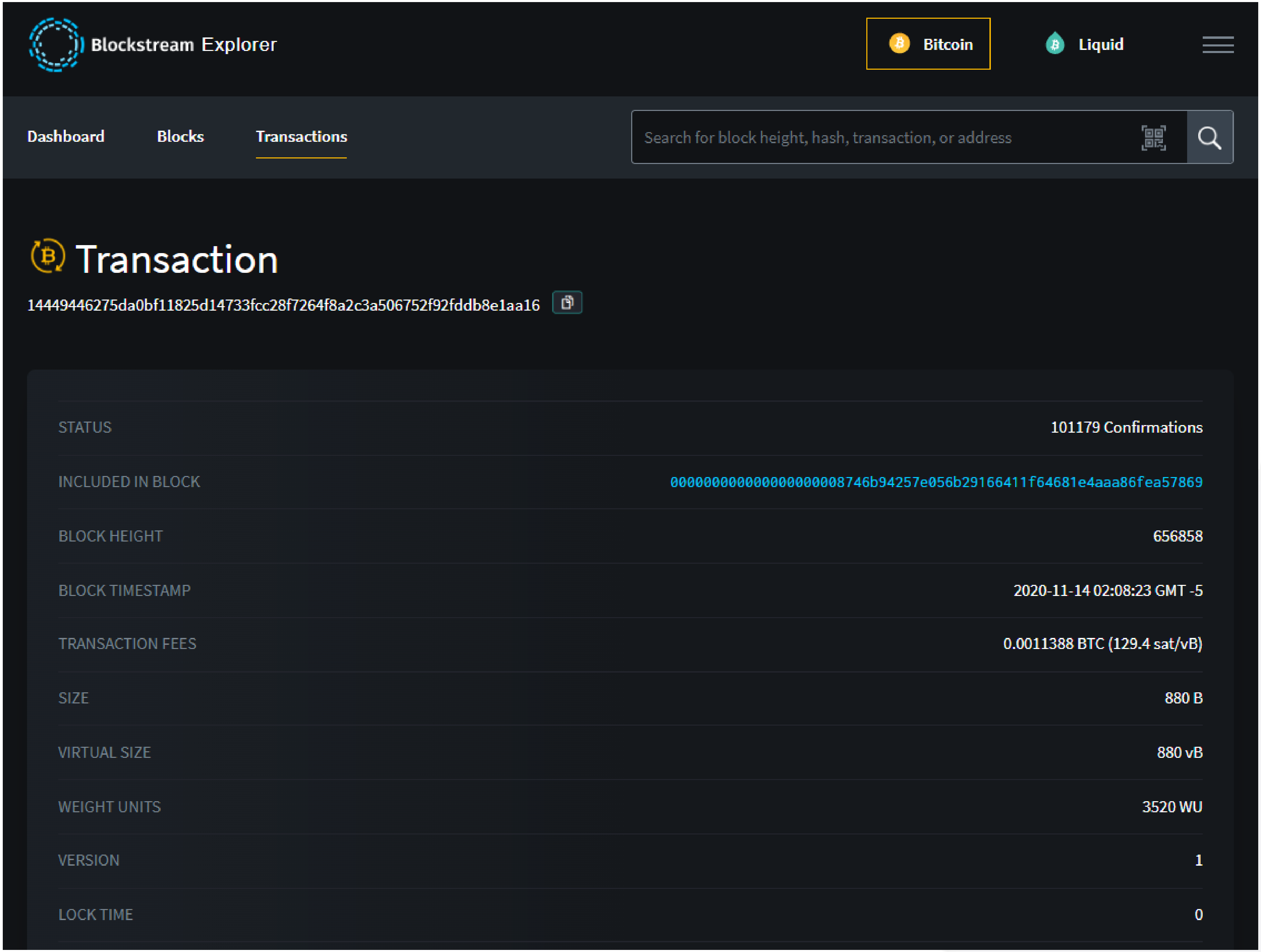
CONFIRMED TX COUNT	124
CONFIRMED RECEIVED	122 outputs (14.87769994 BTC)
CONFIRMED SPENT	112 outputs (14.41067602 BTC)
CONFIRMED UNSPENT	10 outputs (0.46702392 BTC)



Transaction

01b9e19b74335b6ab5f56abee48a861ede31d997a64d4d624748ae65921c8e86

STATUS	291983 Confirmations
INCLUDED IN BLOCK	0000000000000000019e98f686e10298fe1e1c5202239f84d618d620baa5c6f8
BLOCK HEIGHT	466054
BLOCK TIMESTAMP	2017-05-12 10:34:58 GMT -4
TRANSACTION FEES	0.0004068 BTC (180.0 sat/vB)
SIZE	226 B
VIRTUAL SIZE	226 vB
WEIGHT UNITS	904 WU
VERSION	1
LOCK TIME	466052

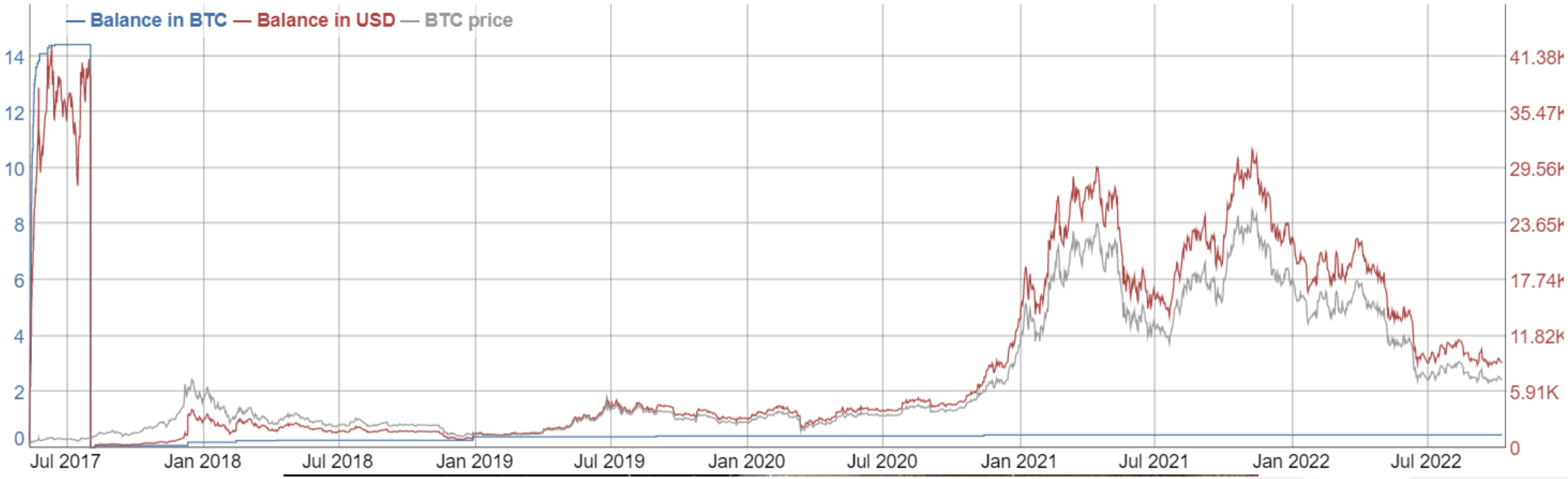


Transaction

14449446275da0bf11825d14733fcc28f7264f8a2c3a506752f92fddb8e1aa16

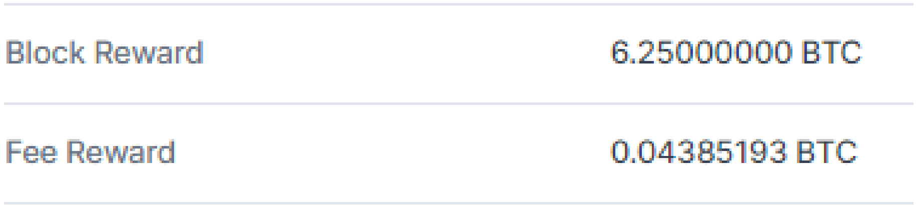
STATUS	101179 Confirmations
INCLUDED IN BLOCK	00000000000000000000008746b94257e056b29166411f64681e4aaa86fea57869
BLOCK HEIGHT	656858
BLOCK TIMESTAMP	2020-11-14 02:08:23 GMT -5
TRANSACTION FEES	0.0011388 BTC (129.4 sat/vB)
SIZE	880 B
VIRTUAL SIZE	880 vB
WEIGHT UNITS	3520 WU
VERSION	1
LOCK TIME	0

BitInfoCharts

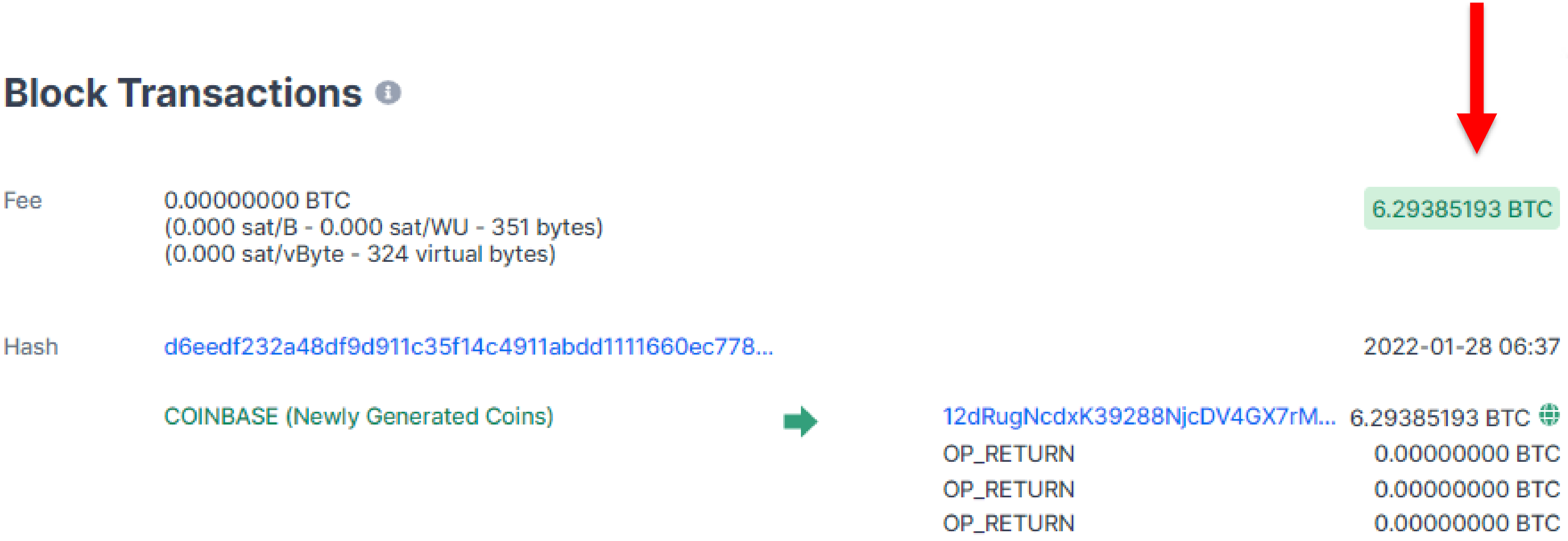


TRANSACTIONS

“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

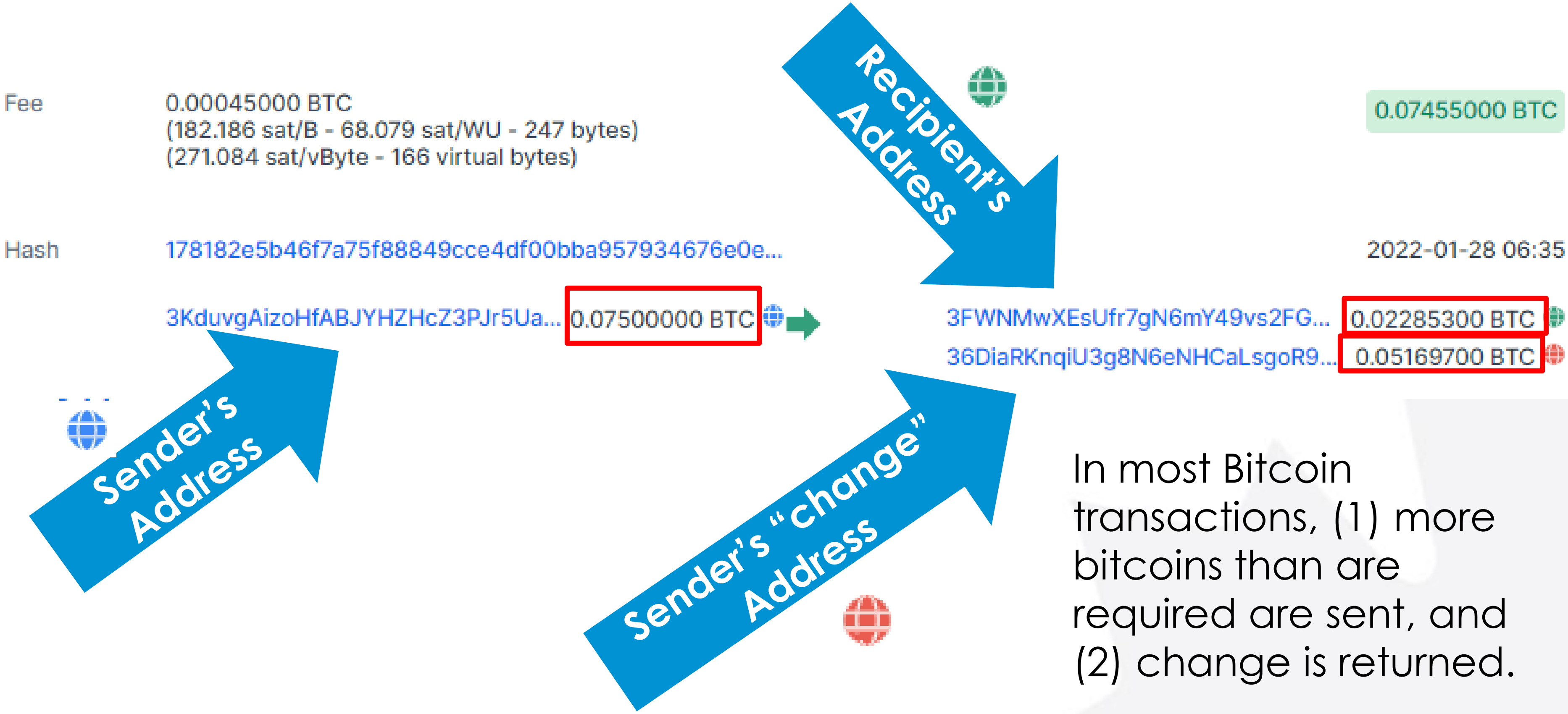
Hash d6eedf232a48df9d911c35f14c4911abdd1111660ec778...

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



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

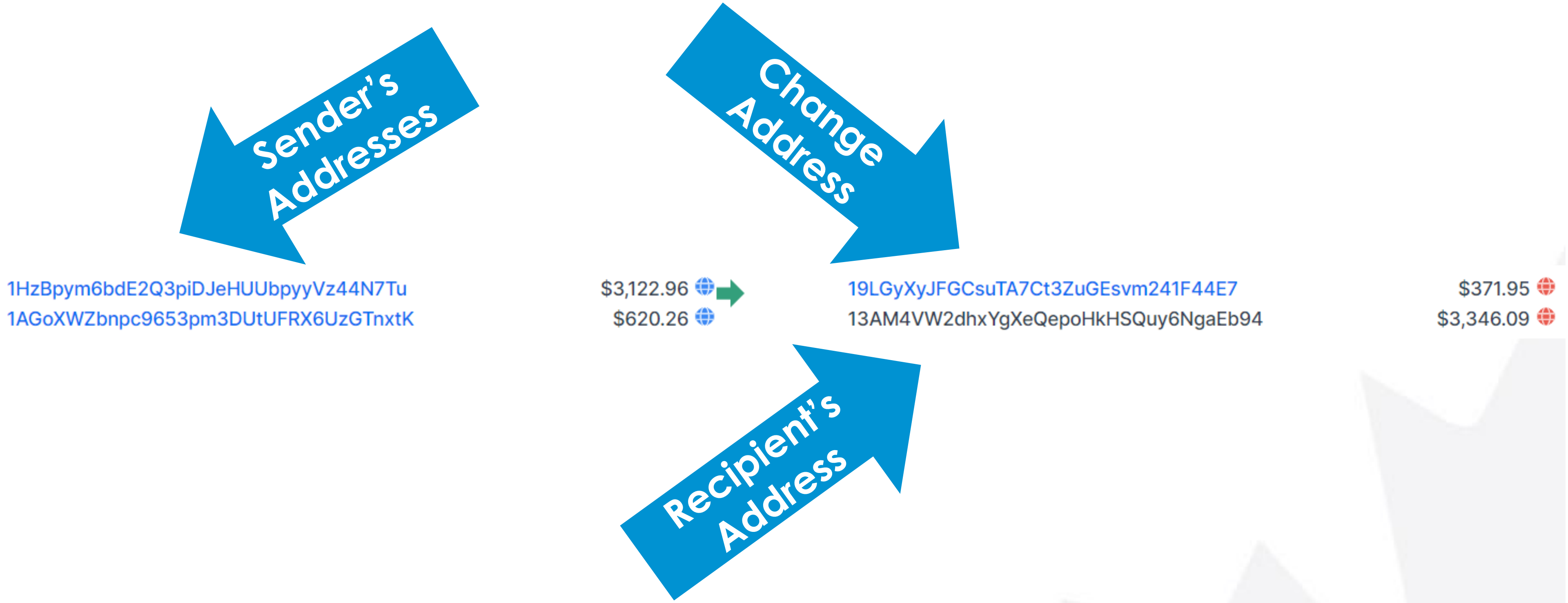
Recipient's Address

Sender's Address

Sender's "change" Address

In most Bitcoin transactions, (1) more bitcoins than are required are sent, and (2) change is returned.

Simple Transaction



Sender's Addresses

Change Address

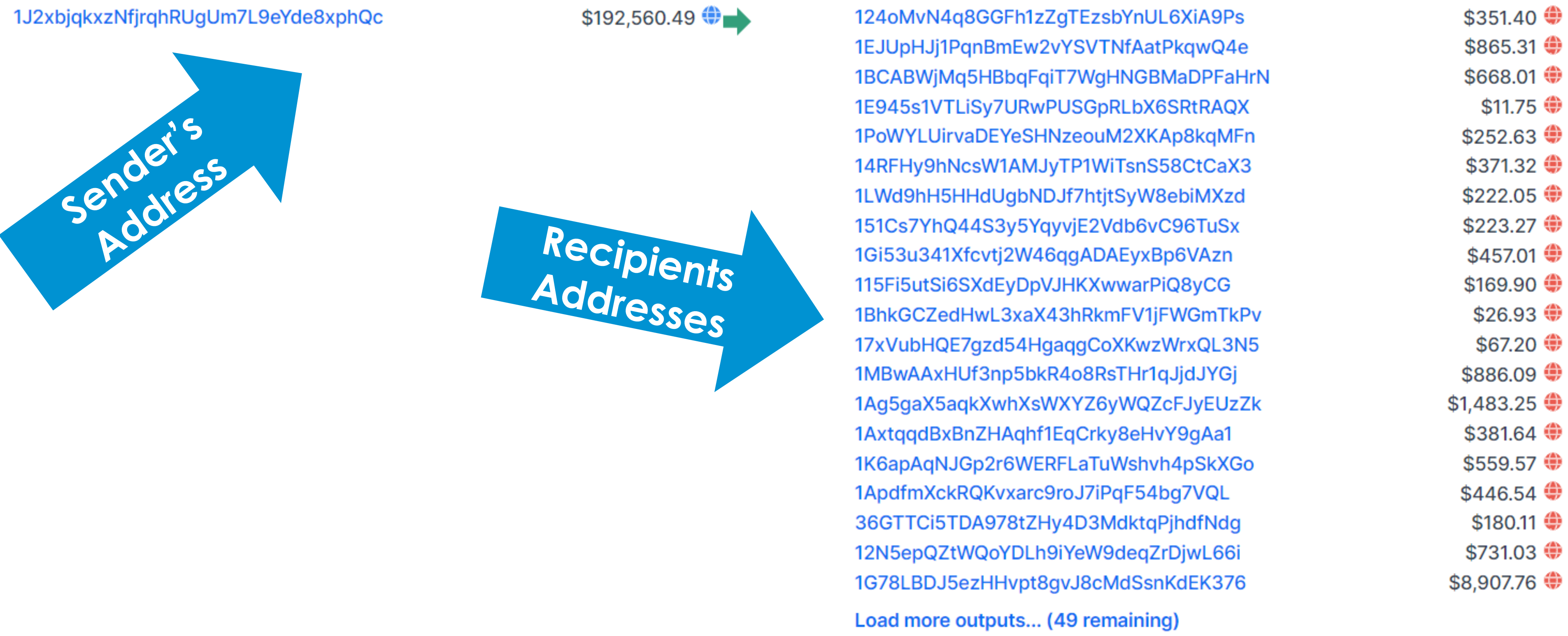
1HzBpym6bdE2Q3piDJeHUUbpyyVz44N7Tu $3,122.96
1AGoXWZbnpc9653pm3DUtUFRX6UzGTnxtK $620.26

19LGyXyJFGCsuTA7Ct3ZuGEsvm241F44E7 $371.95
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 $3,346.09

Recipient's Address

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

Service Transactions



Sender's Address

Recipients Addresses

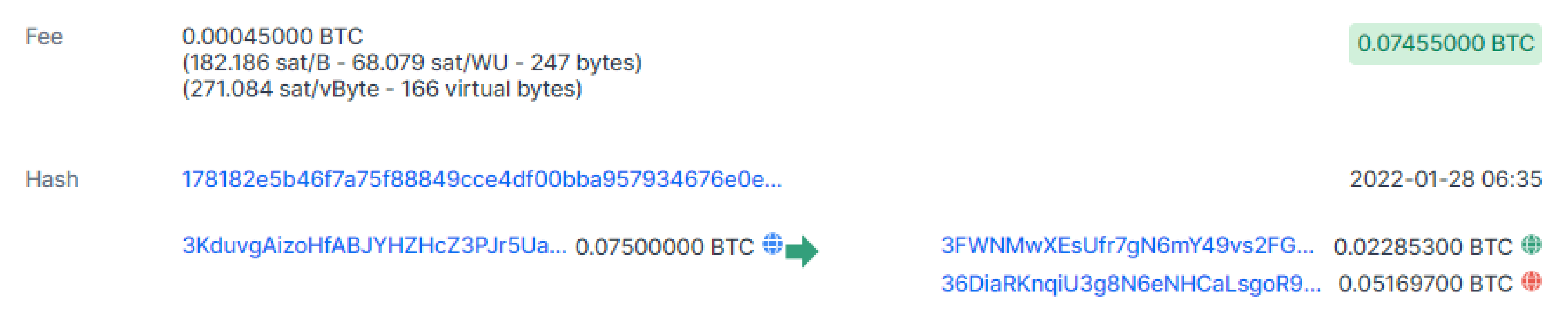
1J2xbjqkxzNfjrqhRUgUm7L9eYde8xphQc	$192,560.49

124oMvN4q8GGFh1zZgTEzsbYnUL6XiA9Ps	$351.40
1EJUpHJj1PqnBmEw2vYSVTNfAatPkqwQ4e	$865.31
1BCABWjMq5HBbqFqiT7WgHNGBMaDPFaHrN	$668.01
1E945s1VTLiSy7URwPUSGpRLbX6SRtRAQX	$11.75
1PoWYLUirvaDEYeSHNzeouM2XKAp8kqMFn	$252.63
14RFHy9hNcsW1AMJyTP1WiTsnS58CtCaX3	$371.32
1LWd9hH5HHdUgbNDJf7htjtSyW8ebiMXzd	$222.05
151Cs7YhQ44S3y5YqyvjE2Vdb6vC96TuSx	$223.27
1Gi53u341Xfcvtj2W46qgADAEyxBp6VAzn	$457.01
115Fi5utSi6SXdEyDpVJHKXwwarPiQ8yCG	$169.90
1BhkGCZedHwL3xaX43hRkmFV1jFWGmTkPv	$26.93
17xVubHQE7gzd54HgaqgCoXKwzWrxQL3N5	$67.20
1MBwAAxHUf3np5bkR4o8RsTHr1qJjdJYGj	$886.09
1Ag5gaX5aqkXwhXsWXYZ6yWQZcFJyEUzZk	$1,483.25
1AxtqqdBxBnZHAqhf1EqCrky8eHvY9gAa1	$381.64
1K6apAqNJGp2r6WERFLaTuWshvh4pSkXGo	$559.57
1ApdfmXckRQKvxarc9roJ7iPqF54bg7VQL	$446.54
36GTTCi5TDA978tZHy4D3MdktqPjhdfNdg	$180.11
12N5epQZtWQoYDLh9iYeW9deqZrDjwL66i	$731.03
1G78LBDJ5ezHHvpt8gvJ8cMdSsnKdEK376	$8,907.76

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 obtain KYC information.



```
Fee     0.00045000 BTC                                                       0.07455000 BTC
        (182.186 sat/B - 68.079 sat/WU - 247 bytes)
        (271.084 sat/vByte - 166 virtual bytes)

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?

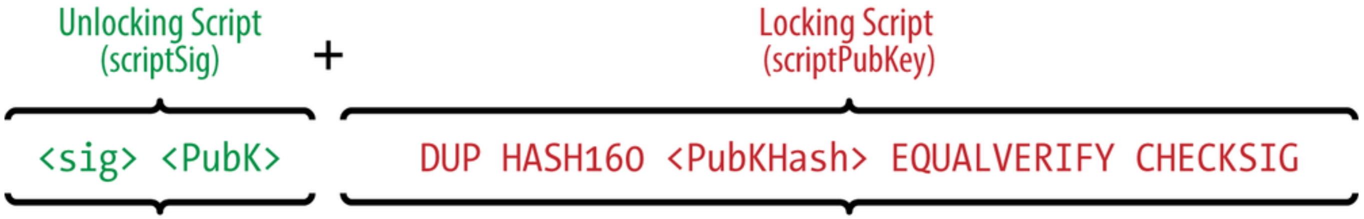
- Export the transaction information from BlockChair by clicking on “Transaction Receipt”

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

Bitcoin transactions are scripts

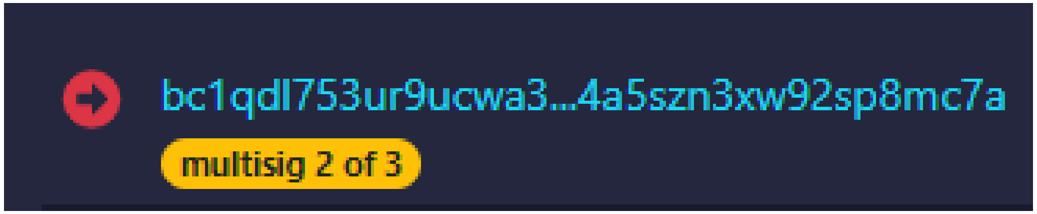


Unlocking Script (scriptSig) + Locking Script (scriptPubKey)

```
<sig> <PubK>    DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
```

- Transaction scripts may contain special instructions & information in the form of OP_CODES
  - Time Lock
  - Multisignature
  - Messages
  - Etc.
- **Scripts are preserved on the Blockchain** and can be accessed using a blockchain explorer

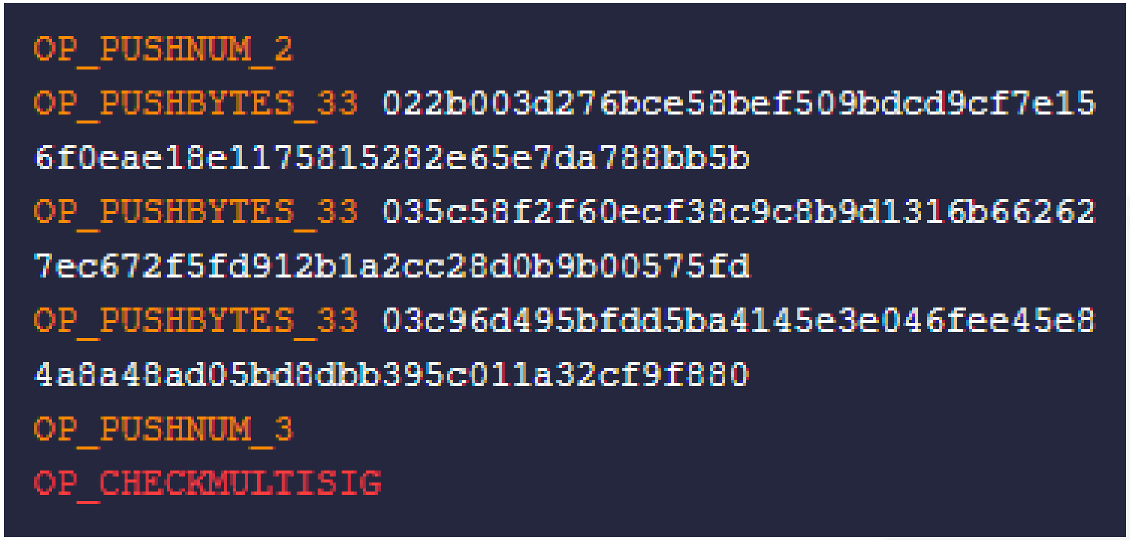
Multisig Data



bc1qdl753ur9ucwa3...4a5szn3xw92sp8mc7a

multisig 2 of 3

- Was the address that sent the transaction Multisig?
- If so, how may many keys were used?
  - E.g. Did the sending address require (and use) 2 out of 3 existing keys to authorize it?



```
OP_PUSHNUM_2
OP_PUSHBYTES_33 022b003d276bce58bef509bdcd9cf7e15
6f0eae18e1175815282e65e7da788bb5b
OP_PUSHBYTES_33 035c58f2f60ecf38c9c8b9d1316b66262
7ec672f5fd912b1a2cc28d0b9b00575fd
OP_PUSHBYTES_33 03c96d495bfdd5ba4145e3e046fee45e8
4a8a48ad05bd8dbb395c011a32cf9f880
OP_PUSHNUM_3
OP_CHECKMULTISIG
```

Multisig Data (cont.)

- 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.

Exercise Multisig

https://mempool.space/
https://www.blockchain.com/

- **Use Mempool.space to discover if the sending addresses were Multisig and, if so, how many signatures were required and used?**
  1. 149105220183a6db95104e420d91dfd1c18289a9a2ad1b88a25a7da379e92ca3
  2. A1a982f681b7aba7d23d1e238e3c5823344571faef19d83f7d86980feef12188
  3. 1331d1e0210b6b163811c514f2324e5b025d79216007ff3f3267b3996ff94d75
  4. 065c9db2550fcde438bc458a4f0e21eb527b49c5c2d3f7306399527e6ec864ee
- Can you find the same info in Blockchain.com

Answer

149105220183a6db95104e420d91dfd1c18289a9a2
ad1b88a25a7da379e92ca3 – **2 of 3**

A1a982f681b7aba7d23d1e238e3c5823344571faef
19d83f7d86980feef12188 – **not multisig**

1331d1e0210b6b163811c514f2324e5b025d792160
07ff3f3267b3996ff94d75 – **2 of 2**

065c9db2550fcde438bc458a4f0e21eb527b49c5c2
d3f7306399527e6ec864ee – **2 of 3**

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

Exercise
Messages in the Bitcoin blockchain

1. How did one person welcome his son’s birth into the world? **(Look at the OP_RETURN data decoded.)**
   - https://blockchair.com/bitcoin/transaction/9f07de305678adcc965a0856a2591c44236e09afefb03c4a43993519127a6697