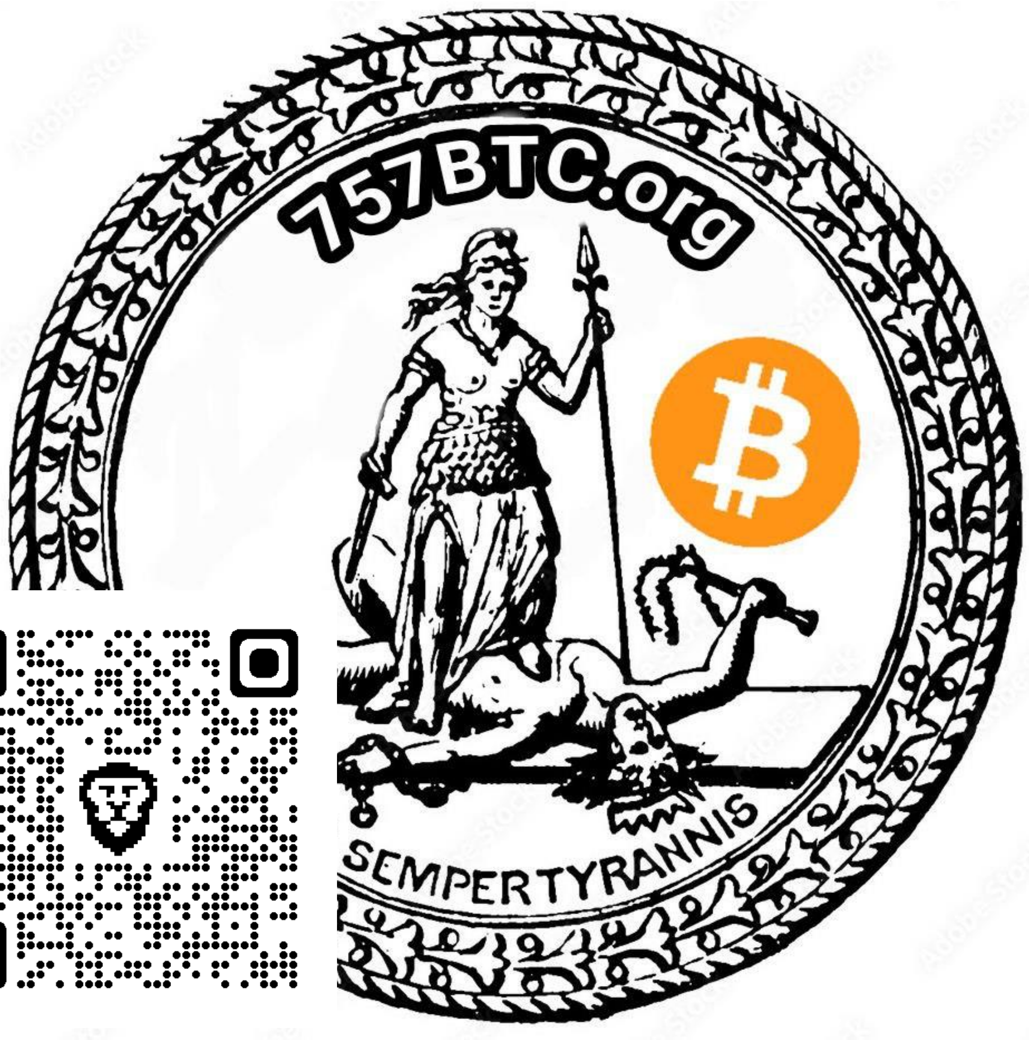
Mempool Policy

757BTC

https://www.757btc.org/

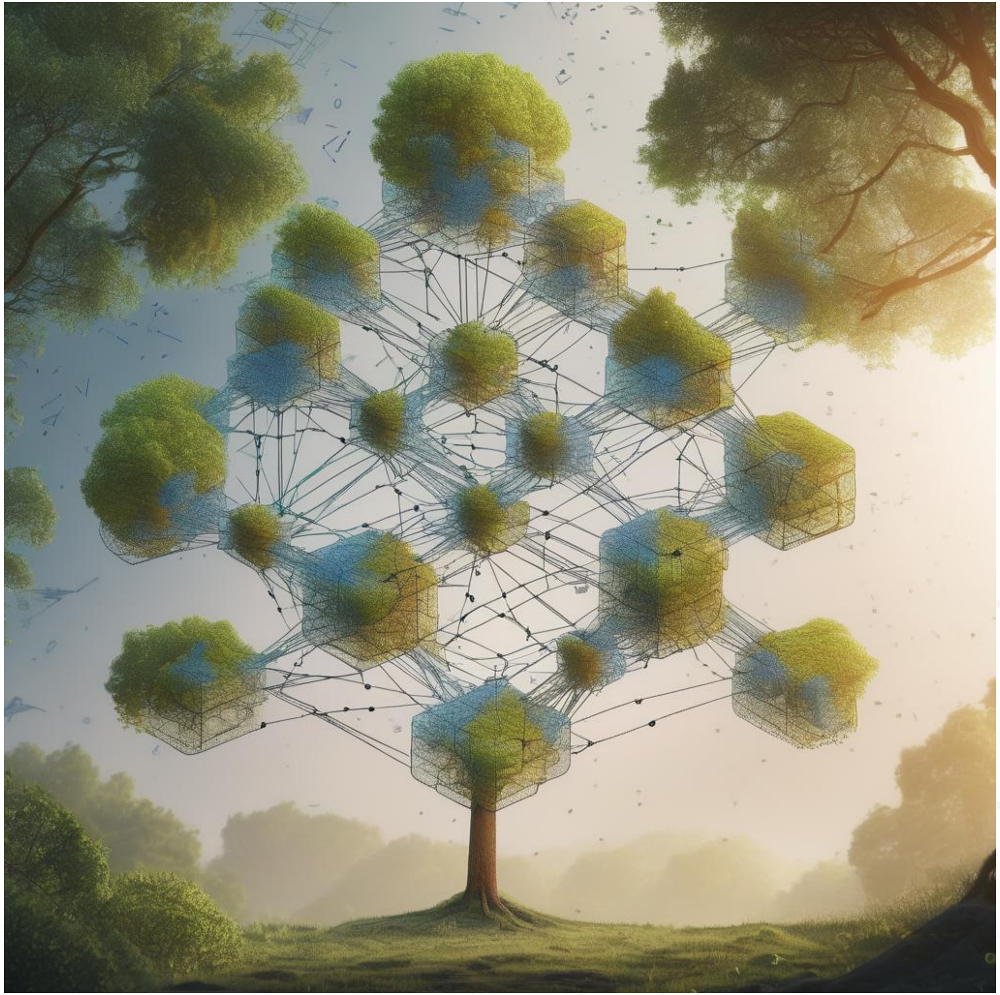


Topics

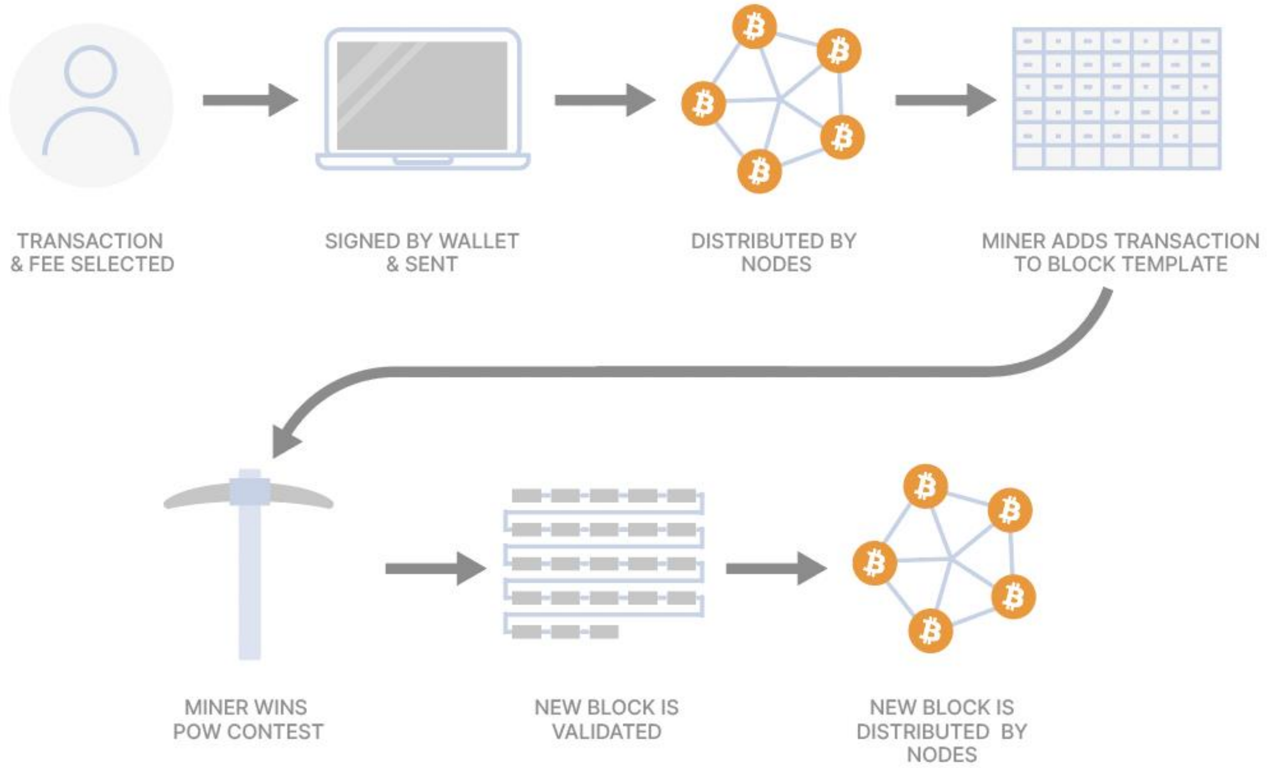
- Mempool What it is
- Mempool Propagation
- Mempool Policy
- Current Debate (2025)
- What can we do

Blockchain 101

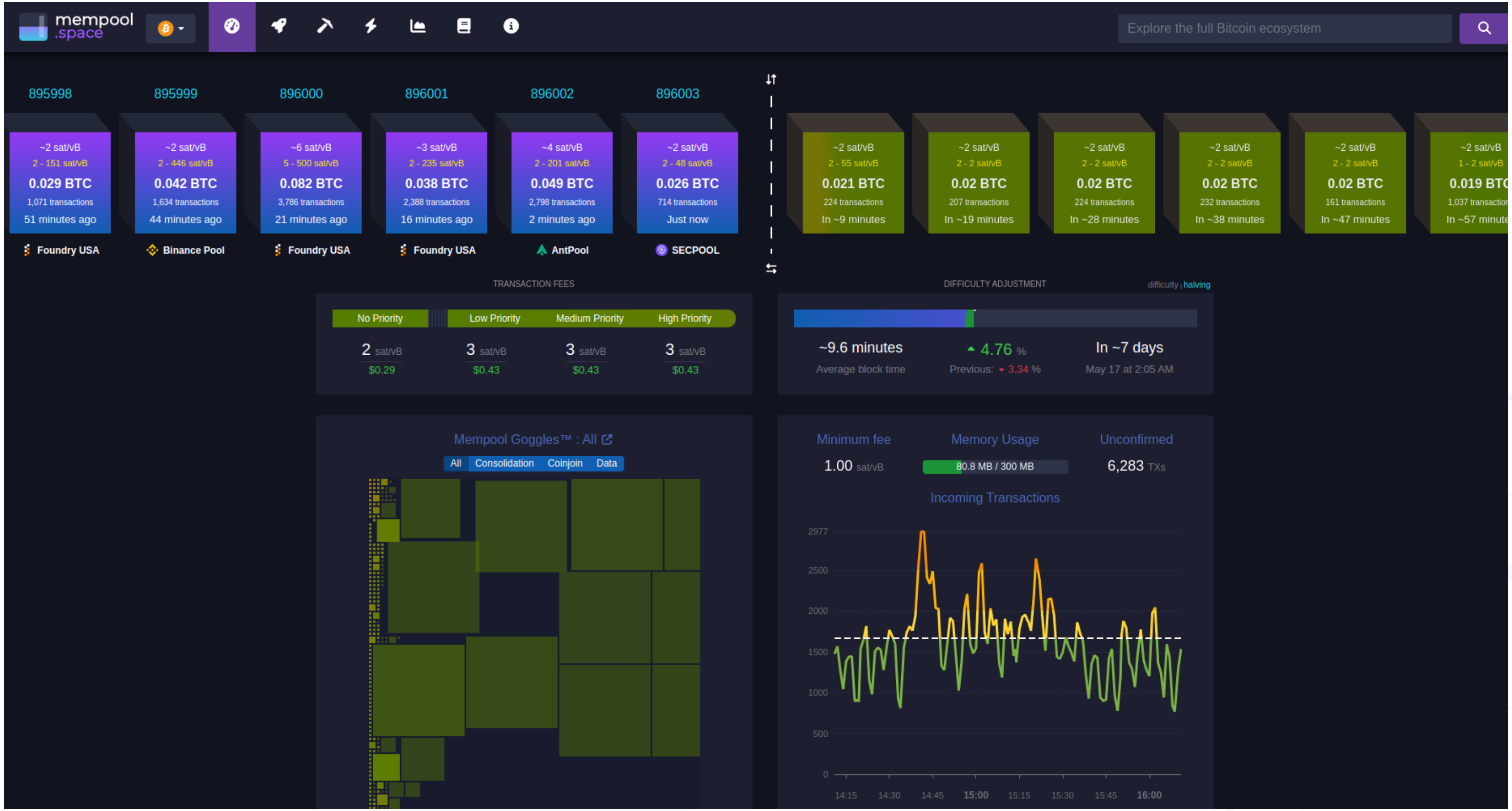
- Data structure
- Immutability
- Transparency
- Decentralization
- Digital Scarcity



Transaction Process


TRANSACTION & FEE SELECTED
SIGNED BY WALLET & SENT
DISTRIBUTED BY NODES
MINER ADDS TRANSACTION TO BLOCK TEMPLATE
MINER WINS POW CONTEST
NEW BLOCK IS VALIDATED
NEW BLOCK IS DISTRIBUTED BY NODES

Mempool



895998	895999	896000	896001	896002	896003
~2 sat/vB	~2 sat/vB	~6 sat/vB	~3 sat/vB	~4 sat/vB	~2 sat/vB
2 - 151 sat/vB	2 - 446 sat/vB	5 - 500 sat/vB	2 - 235 sat/vB	2 - 201 sat/vB	2 - 48 sat/vB
0.029 BTC	0.042 BTC	0.082 BTC	0.038 BTC	0.049 BTC	0.026 BTC
1,071 transactions	1,634 transactions	3,786 transactions	2,388 transactions	2,798 transactions	714 transactions
51 minutes ago	44 minutes ago	21 minutes ago	16 minutes ago	2 minutes ago	Just now
Foundry USA	Binance Pool	Foundry USA	Foundry USA	AntPool	SECPOOL

~2 sat/vB	~2 sat/vB	~2 sat/vB	~2 sat/vB	~2 sat/vB	~2 sat/vB
2 - 55 sat/vB	2 - 2 sat/vB	2 - 2 sat/vB	2 - 2 sat/vB	2 - 2 sat/vB	1 - 2 sat/vB
0.021 BTC	0.02 BTC	0.02 BTC	0.02 BTC	0.02 BTC	0.019 BTC
224 transactions	207 transactions	224 transactions	232 transactions	161 transactions	1,037 transactio
In ~9 minutes	In ~19 minutes	In ~28 minutes	In ~38 minutes	In ~47 minutes	In ~57 minute

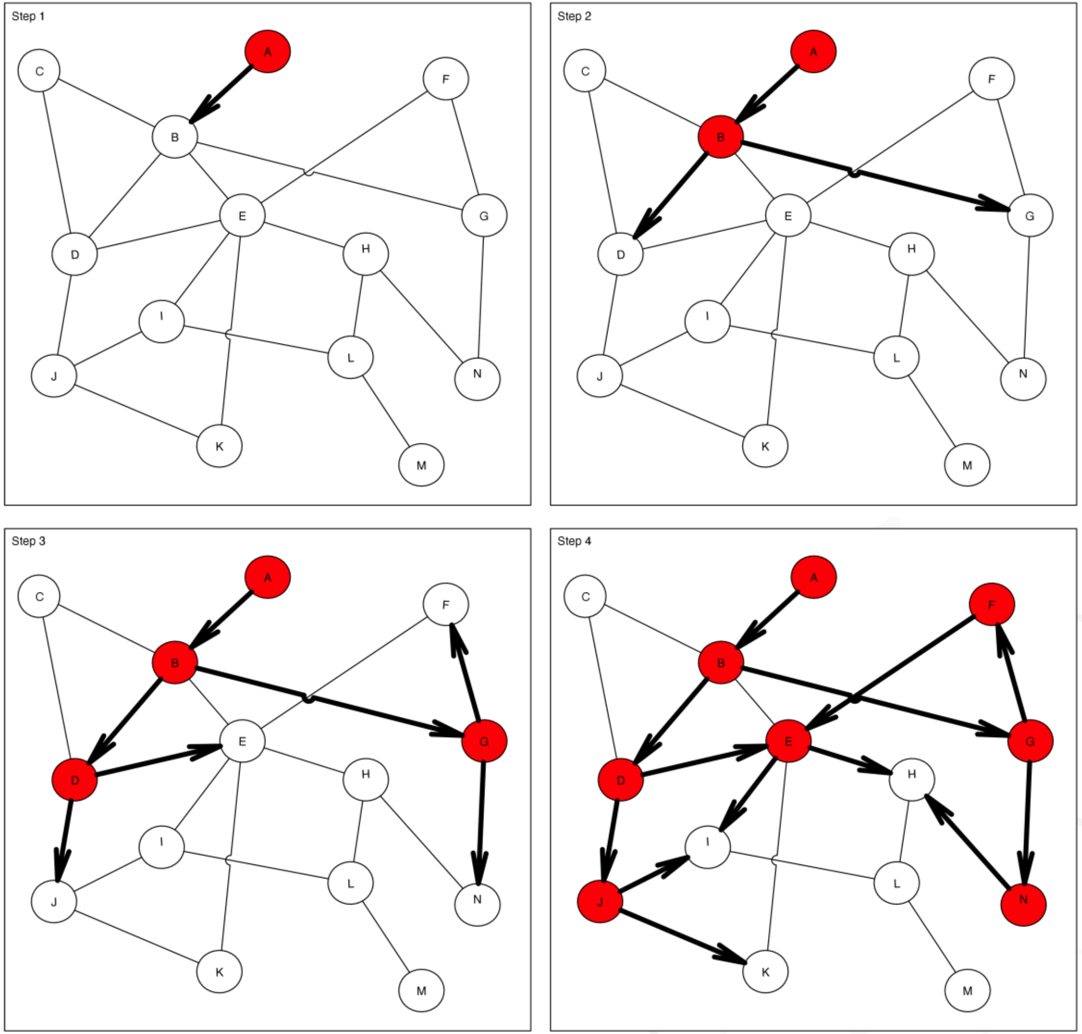
No Priority	Low Priority	Medium Priority	High Priority
2 sat/vB	3 sat/vB	3 sat/vB	3 sat/vB
$0.29	$0.43	$0.43	$0.43

~9.6 minutes	▲ 4.76 %	In ~7 days
Average block time	Previous: ▼ 3.34 %	May 17 at 2:05 AM

Minimum fee	Memory Usage	Unconfirmed
1.00 sat/vB	80.8 MB / 300 MB	6,283 TXs

Mempool Features

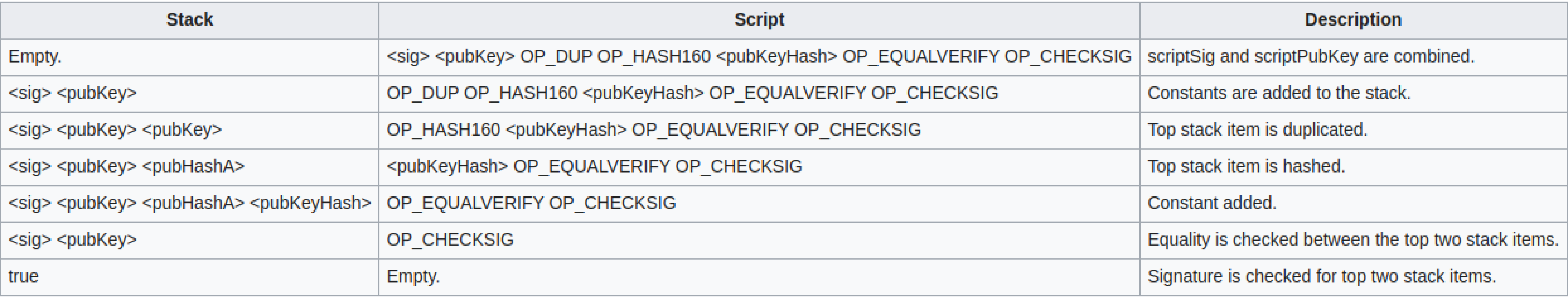
- There is no “the mempool”
- Every full node maintains their own
- List of pending transactions
- Peer to Peer network utilizing Gossip Network Protocols


Step 1
A C F B E G D H I L N J K M
Step 2
A C F B E G D H I L N J K M
Step 3
A C F B E G D H I L N J K M
Step 4
A C F B E G D H I L N J K M

Bitcoin Transaction Components

- Version number
- Inputs
    - previous tx
    - output index
    - unlocking script
    - sequence number
- Outputs
    - amount in sats
    - locking script defining spending conditions
        - OP_RETURN
- Locktime
- Witness Data
    - Signatures
    - Public Keys
    - “Other data”
- Transaction ID
- Transaction weight
- Transaction Fee

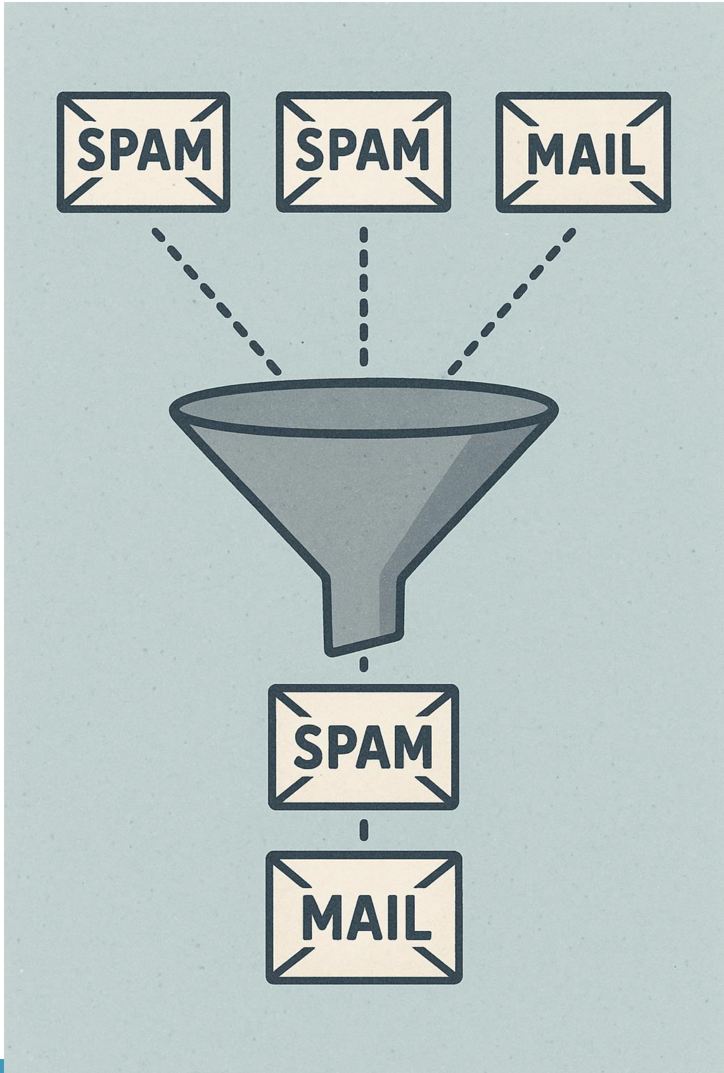
Bitcoin Transactions as a STACK



Stack	Script	Description
Empty.	<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	scriptSig and scriptPubKey are combined.
<sig> <pubKey>	OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Constants are added to the stack.
<sig> <pubKey> <pubKey>	OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is duplicated.
<sig> <pubKey> <pubHashA>	<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG	Top stack item is hashed.
<sig> <pubKey> <pubHashA> <pubKeyHash>	OP_EQUALVERIFY OP_CHECKSIG	Constant added.
<sig> <pubKey>	OP_CHECKSIG	Equality is checked between the top two stack items.
true	Empty.	Signature is checked for top two stack items.

Mempool Policy

- Set by individual full nodes
- If you run your own node you can choose what transactions you want to keep
- Example of filters include
  - data: limit byte size for op_return
  - rejectparasites: identifies non monetary program code in script such as OP_FALSE and OP_IF

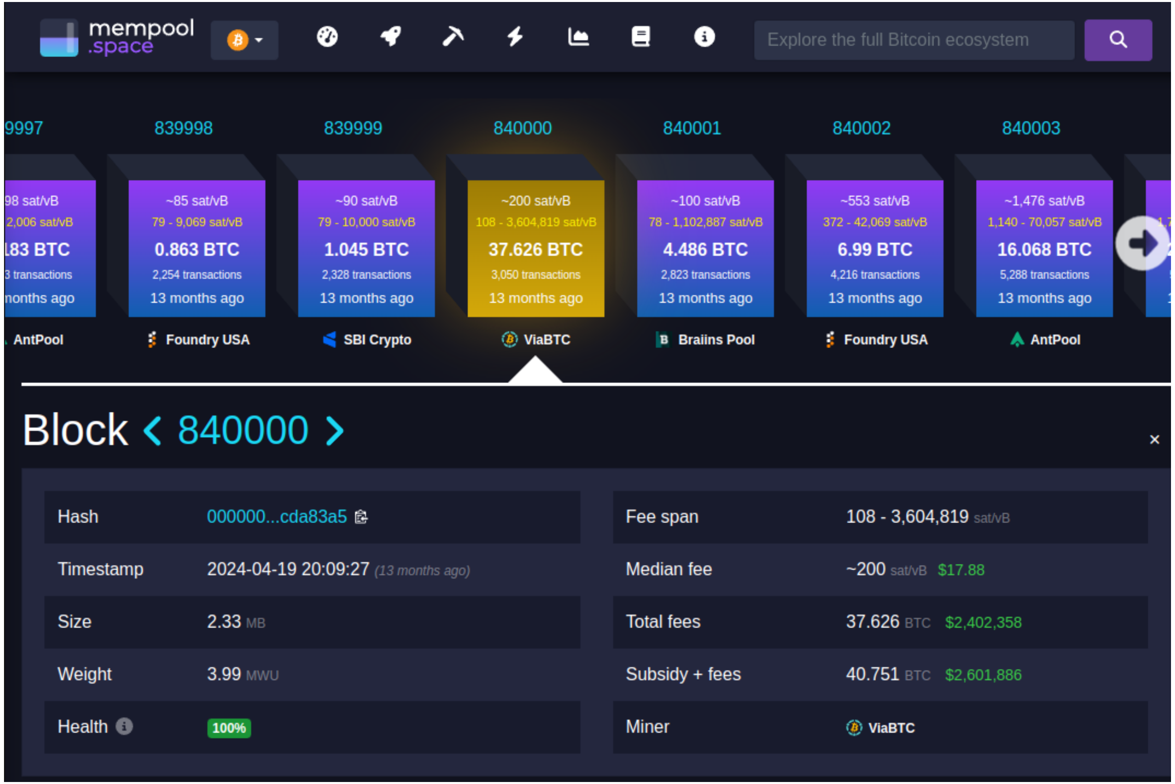


Current Debate

- Does Spam exist?
- What is appropriate data for the Bitcoin Blockchain?
- Who gets to decide?
- What did Satoshi Nakamoto originally intend?

SPAM®
Classic
Ingredients: Pork with Ham, Salt, Water, Modified Potato Starch, Sugar, Sodium Nitrite
U.S. INSPECTED AND PASSED BY DEPARTMENT OF AGRICULTURE
Serving Suggestion
NET WT 12 OZ (340g)

Some Examples Of Arbitrary Data on Blockchain



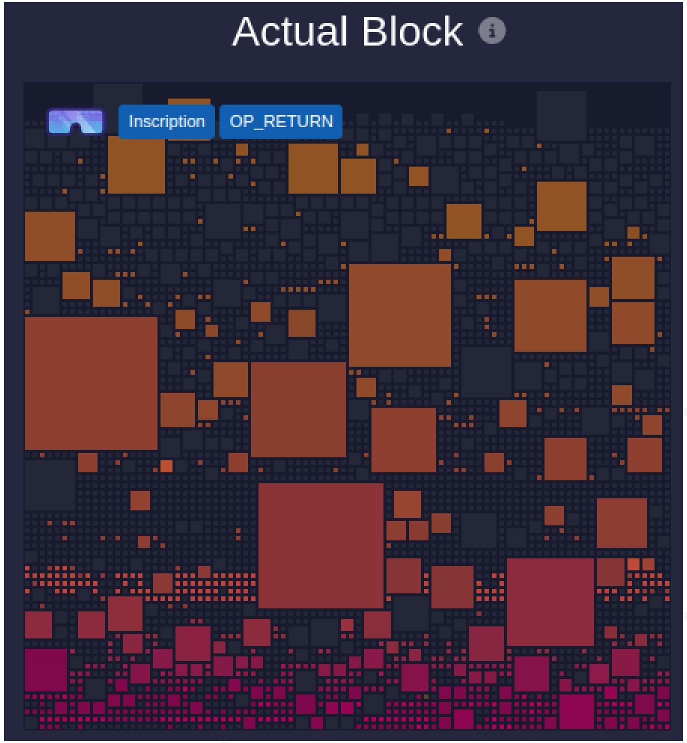
mempool .space

Explore the full Bitcoin ecosystem

9997	839998	839999	840000	840001	840002	840003
98 sat/vB	~85 sat/vB	~90 sat/vB	~200 sat/vB	~100 sat/vB	~553 sat/vB	~1,476 sat/vB
2,006 sat/vB	79 - 9,069 sat/vB	79 - 10,000 sat/vB	108 - 3,604,819 sat/vB	78 - 1,102,887 sat/vB	372 - 42,069 sat/vB	1,140 - 70,057 sat/vB
l83 BTC	0.863 BTC	1.045 BTC	37.626 BTC	4.486 BTC	6.99 BTC	16.068 BTC
3 transactions	2,254 transactions	2,328 transactions	3,050 transactions	2,823 transactions	4,216 transactions	5,288 transactions
nonths ago	13 months ago	13 months ago	13 months ago	13 months ago	13 months ago	13 months ago
AntPool	Foundry USA	SBI Crypto	ViaBTC	Braiins Pool	Foundry USA	AntPool

Block < 840000 >

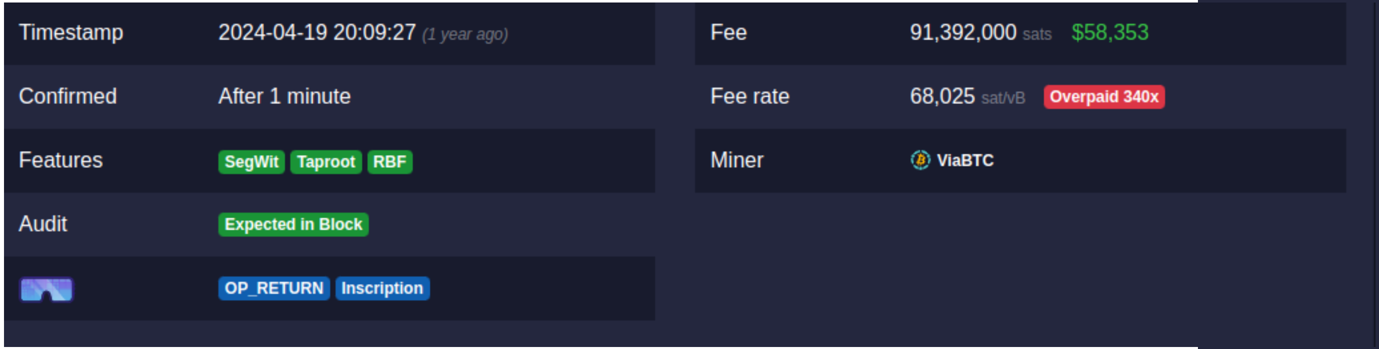
Hash	000000...cda83a5	Fee span	108 - 3,604,819 sat/vB
Timestamp	2024-04-19 20:09:27 *(13 months ago)*	Median fee	~200 sat/vB $17.88
Size	2.33 MB	Total fees	37.626 BTC $2,402,358
Weight	3.99 MWU	Subsidy + fees	40.751 BTC $2,601,886
Health	100%	Miner	ViaBTC



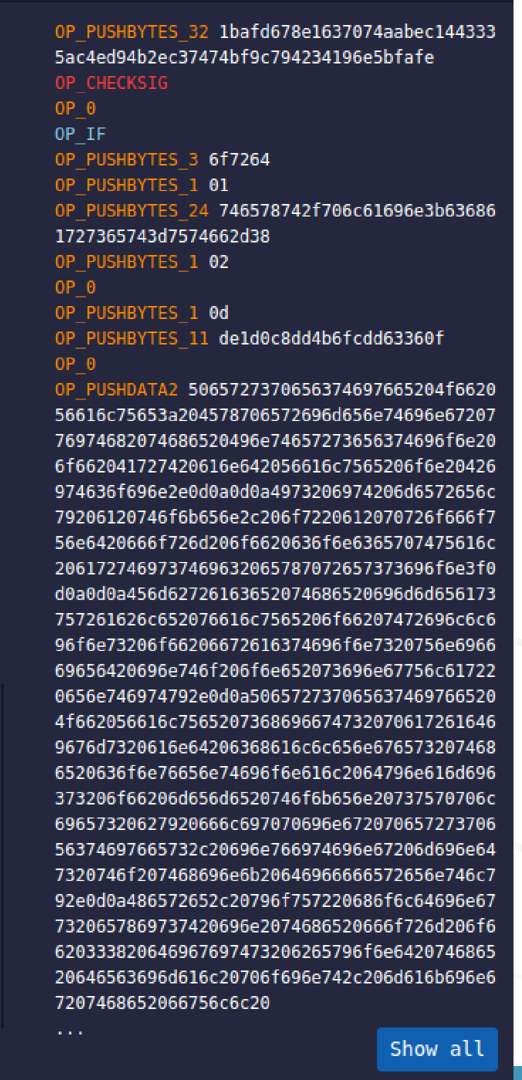
Actual Block

Runestone/Ordinals Example

- Embedding data into the Witness for pay to taproot script
  - OP_PUSHDATA2
- Large amounts of data makes for heavy blocks
- Extra data means higher fees for miners



Timestamp	2024-04-19 20:09:27 *(1 year ago)*	Fee	91,392,000 sats $58,353
Confirmed	After 1 minute	Fee rate	68,025 sat/vB Overpaid 340x
Features	SegWit Taproot RBF	Miner	ViaBTC
Audit	Expected in Block		
	OP_RETURN Inscription		

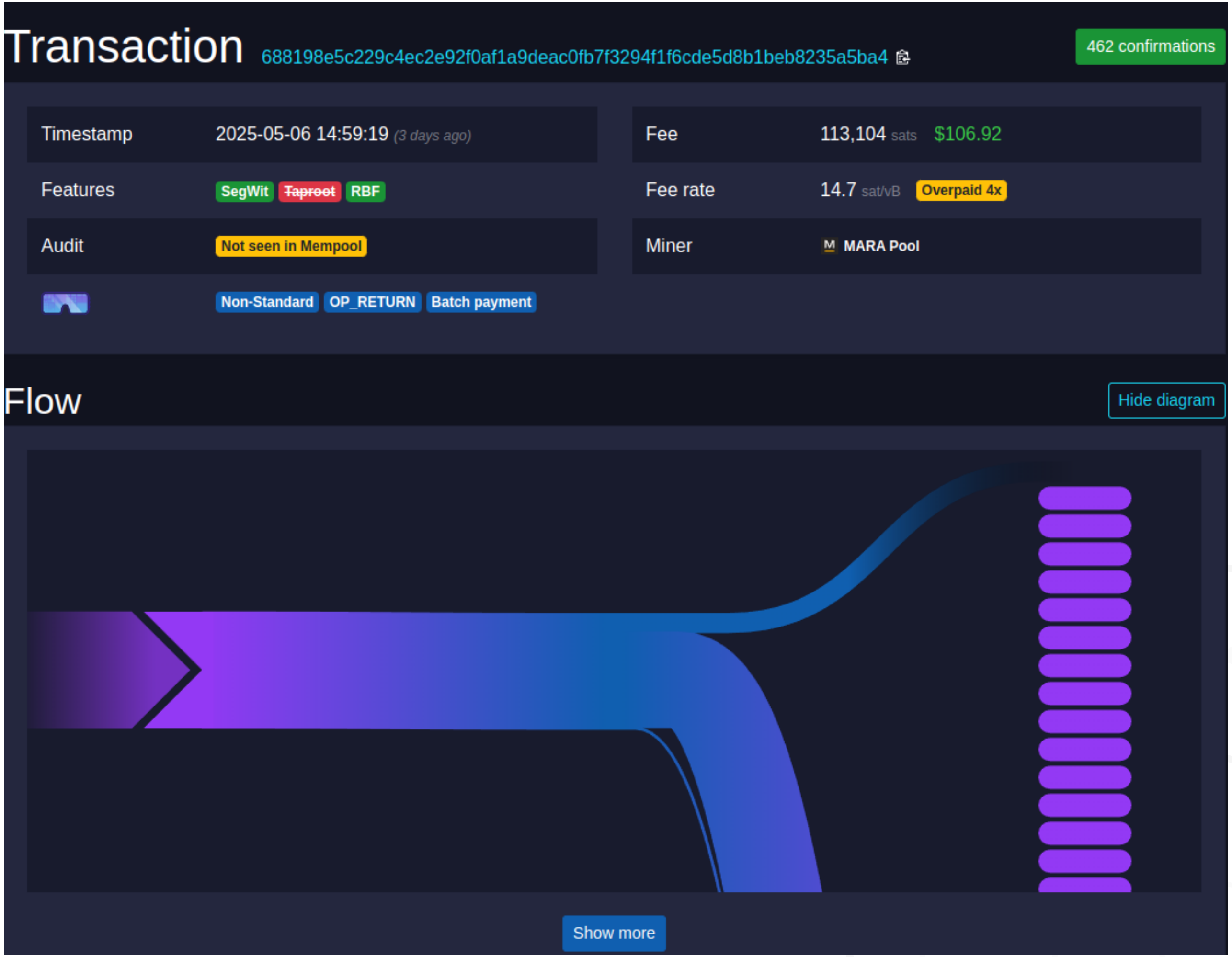


P2TR tapscript

```
OP_PUSHBYTES_32 1bafd678e1637074aabec144333
5ac4ed94b2ec37474bf9c794234196e5bfafe
OP_CHECKSIG
OP_0
OP_IF
OP_PUSHBYTES_3 6f7264
OP_PUSHBYTES_1 01
OP_PUSHBYTES_24 746578742f706c61696e3b63686
1727365743d7574662d38
OP_PUSHBYTES_1 02
OP_0
OP_PUSHBYTES_1 0d
OP_PUSHBYTES_11 de1d0c8dd4b6fcdd63360f
OP_0
OP_PUSHDATA2 5065727370656374697665204f6620
56616c75653a20457870657269656e74696e67207
769746820746865204e746572656374696f6e20
6f662041727420616e642056616c7565206f6e20426
974636f696e2e0d0a0d0a4973206974206d6572656c
79206120746f6b656e2c206f7220612070726f666f7
56e6420666f726d206f6620636f6e6365707475616c
206172746973746963206578707265737369f6e3f0
d0a0d0a456d627261636520746865206d6d656173
757261626c652076616c7565206f66207472696c6c6
96f6e73206f6620666172616374696f6e7320756e6966
69656420696e746f206f6e652073696e67756c61722
0656e746974792e0d0a50657273706563746976652
4f662056616c7565207368696674732070617261646
9676d7320616e64206368616c6c656e676573207468
6520636f6e76656e74696f6e616c2064796e616d696
373206f66206d656d6520746f6b656e20737570706c
6965732062792066c697070696e6720706572737065
56374697665732c20696e766974696e67206d696e64
7320746f207468696e6b20646966666572656e746c7
92e0d0a486572652c20796f757220686f6c64696e67
732065786973747420696e2074686520666f726d206f6
620333820646967697473206265796f6e6420746865
20646563696d616c20706f696e742c206d616b696e6
7207468652066756c6c20
...
```

Show all

OP_RETURN Example



Transaction 688198e5c229c4ec2e92f0af1a9deac0fb7f3294f1f6cde5d8b1beb8235a5ba4

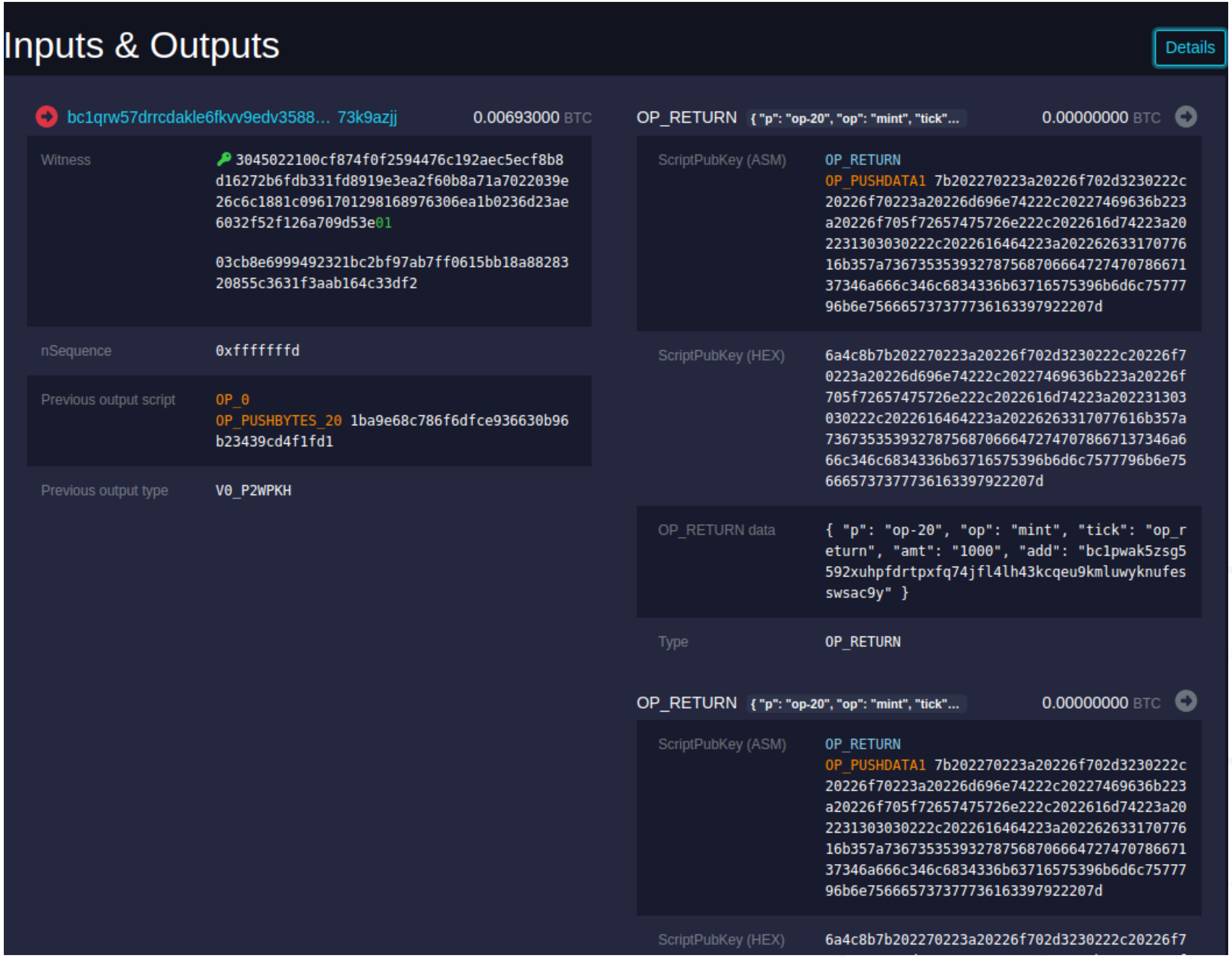
462 confirmations

Timestamp	2025-05-06 14:59:19 *(3 days ago)*	Fee	113,104 sats $106.92
Features	SegWit ~~Taproot~~ RBF	Fee rate	14.7 sat/vB Overpaid 4x
Audit	Not seen in Mempool	Miner	MARA Pool
	Non-Standard OP_RETURN Batch payment		

Flow

OP_RETURN Unspendable OUTPUTS

With Arbitrary Text DATA



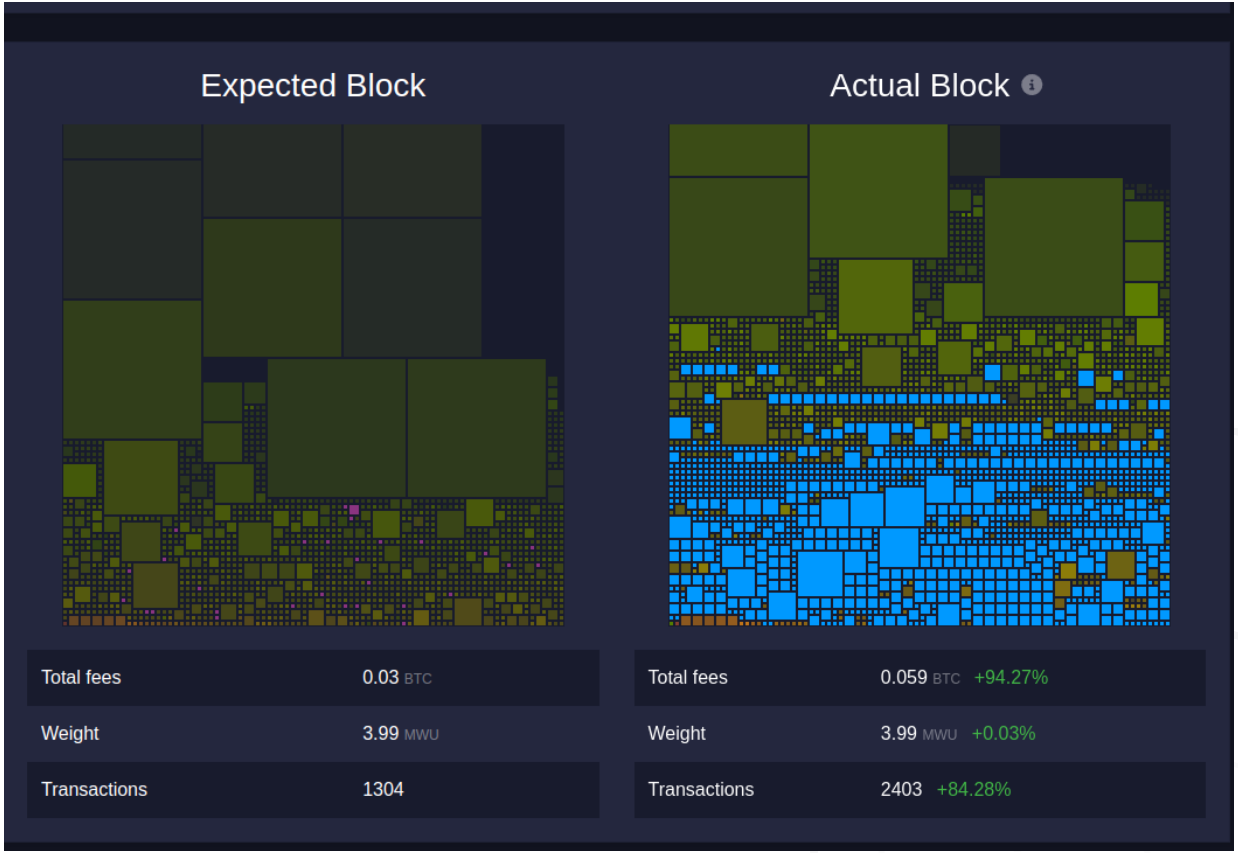
Inputs & Outputs

```
bc1qrw57drrcdakle6fkvv9edv3588… 73k9azjj          0.00693000 BTC

Witness                  3045022100cf874f0f2594476c192aec5ecf8b8
                         d16272b6fdb331fd8919e3ea2f60b8a71a7022039e
                         26c6c1881c0961701298168976306ea1b0236d23ae
                         6032f52f126a709d53e01

                         03cb8e6999492321bc2bf97ab7ff0615bb18a88283
                         20855c3631f3aab164c33df2

nSequence                0xfffffffd

Previous output script   OP_0
                         OP_PUSHBYTES_20 1ba9e68c786f6dfce936630b96
                         b23439cd4f1fd1

Previous output type     V0_P2WPKH
```

```
OP_RETURN { "p": "op-20", "op": "mint", "tick"...          0.00000000 BTC

ScriptPubKey (ASM)   OP_RETURN
                     OP_PUSHDATA1 7b202270223a20226f702d3230222c
                     20226f70223a20226d696e74222c20227469636b223
                     a20226f705f72657475726e222c2022616d74223a20
                     2231303030222c202261646422a20226263317077 6
                     16b357a736735353932787568706664727470786671
                     37346a666c346c6834336b63716575396b6d6c75777
                     96b6e75666573737773616339792207d

ScriptPubKey (HEX)   6a4c8b7b202270223a20226f702d3230222c20226f7
                     0223a20226d696e74222c20227469636b223a20226f
                     705f72657475726e222c2022616d74223a202231303
                     030222c202261646422 3a2022626331707761 6b357a
                     73673535393278756870666472747078667137346a6
                     66c346c6834336b63716575396b6d6c7577796b6e75
                     66657373777361633979 22207d

OP_RETURN data       { "p": "op-20", "op": "mint", "tick": "op_r
                     eturn", "amt": "1000", "add": "bc1pwak5zsg5
                     592xuhpfdrtpxfq74jfl4lh43kcqeu9kmluwyknufes
                     swsac9y" }

Type                 OP_RETURN

OP_RETURN { "p": "op-20", "op": "mint", "tick"...          0.00000000 BTC

ScriptPubKey (ASM)   OP_RETURN
                     OP_PUSHDATA1 7b202270223a20226f702d3230222c
                     20226f70223a20226d696e74222c20227469636b223
                     a20226f705f72657475726e222c2022616d74223a20
                     2231303030222c2022616464223a20226263317077 6
                     16b357a736735353932787568706664727470786671
                     37346a666c346c6834336b63716575396b6d6c75777
                     96b6e75666573737773616339792207d

ScriptPubKey (HEX)   6a4c8b7b202270223a20226f702d3230222c20226f7
```

Out of Band Non-Standard Transactions?

- Libre Relay (Peter Todd)
  - Core fork with no op_return limits
- Miners run that and allow people to broadcast non-standard transactions
- The mining pool running Libre is typically the only miner working for those transactions
- This means they can charge a premium
- This also means, if you run a filtering core, you will not include those transactions in your mempool
- Because of this your current fee calculation will be different



Expected Block

Total fees	0.03 BTC
Weight	3.99 MWU
Transactions	1304

Actual Block

Total fees	0.059 BTC	+94.27%
Weight	3.99 MWU	+0.03%
Transactions	2403	+84.28%

What Can we Do

- Its an open protocol and free open source software
- Run what you like
- Interact with the system the way you want to as long as you are following the protocol you can

- Filter if you want
    - but understand that there is more happening in the mempool that you are not going to see
    - your mempool will not be as full
    - you also won't propagate the non-standard transaction

- Run unfiltered if you want
    - but understand your mempool will be filled with arbitrary data
    - other nodes might block your transactions that you share (if they are non-standard)

Remember

"Free speech is like fire - it spreads from mind to mind, impossible to contain once ignited." - Thomas Paine

- It is true you cannot stop individuals from out of band transactions
- Because out of band transactions are possible, non-standard transactions can and will occur
- This comes at a cost….
  - Can the individuals taking advantage of the system sustain this effort?
  - Can this behavior be sustained in a high fee environment for long?