Blockchain and Digital Currencies

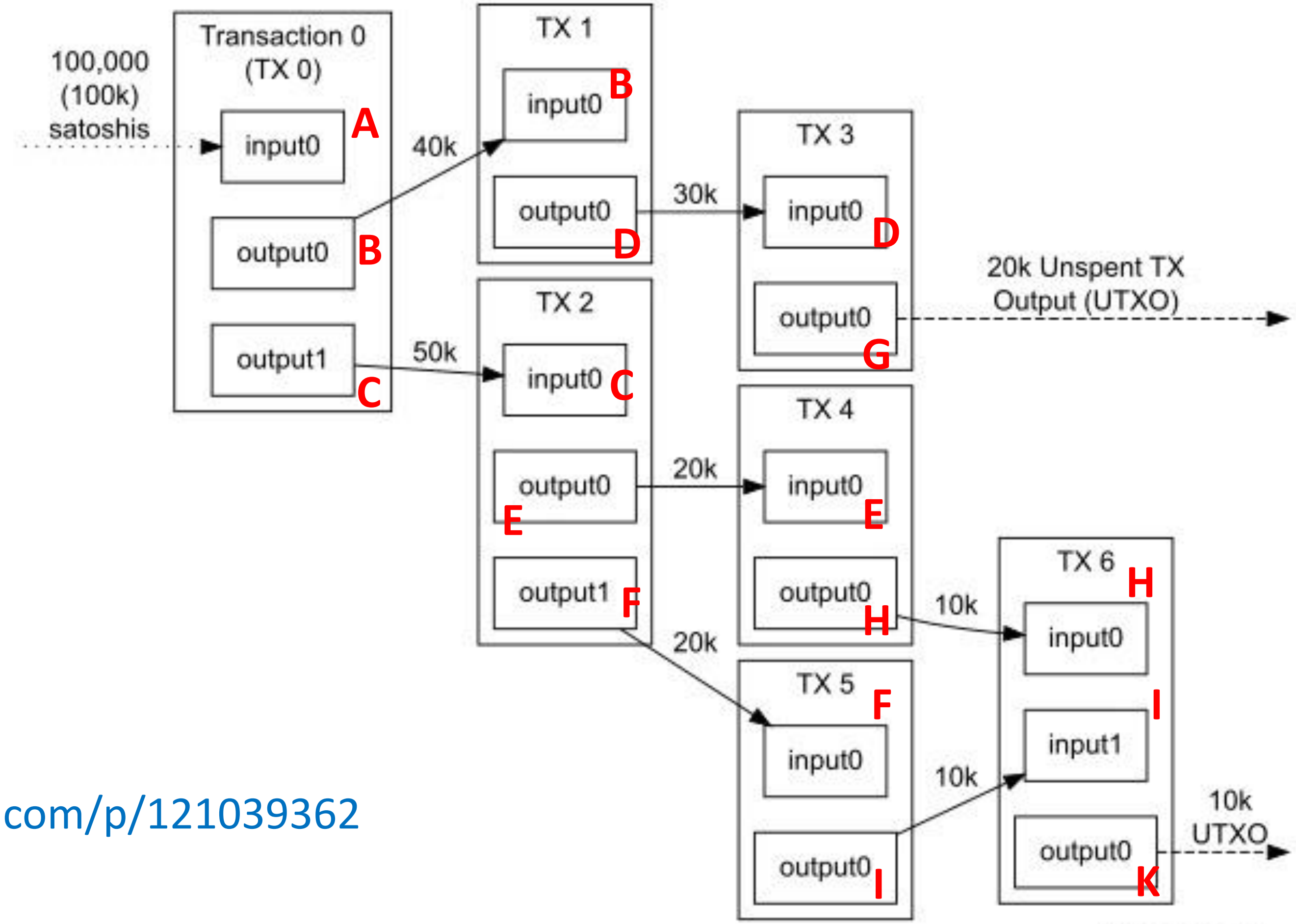
Lecture 6

PHBS 2024 M3

Agenda

- Double Spending Attack
- UTXO
- Bitcoin Network

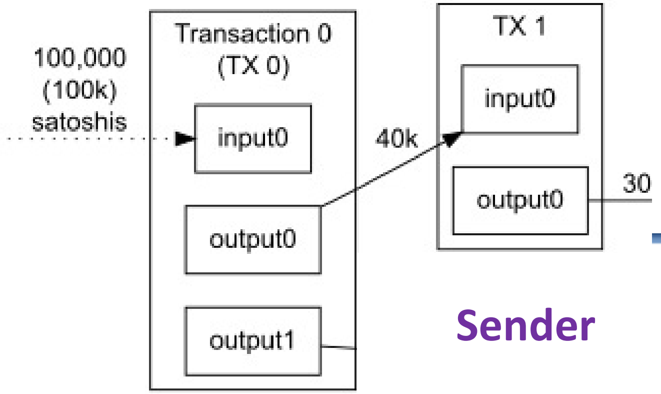
Transactions Cause Ownership Transfer



https://zhuanlan.zhihu.com/p/121039362

Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Transactions Need Verification

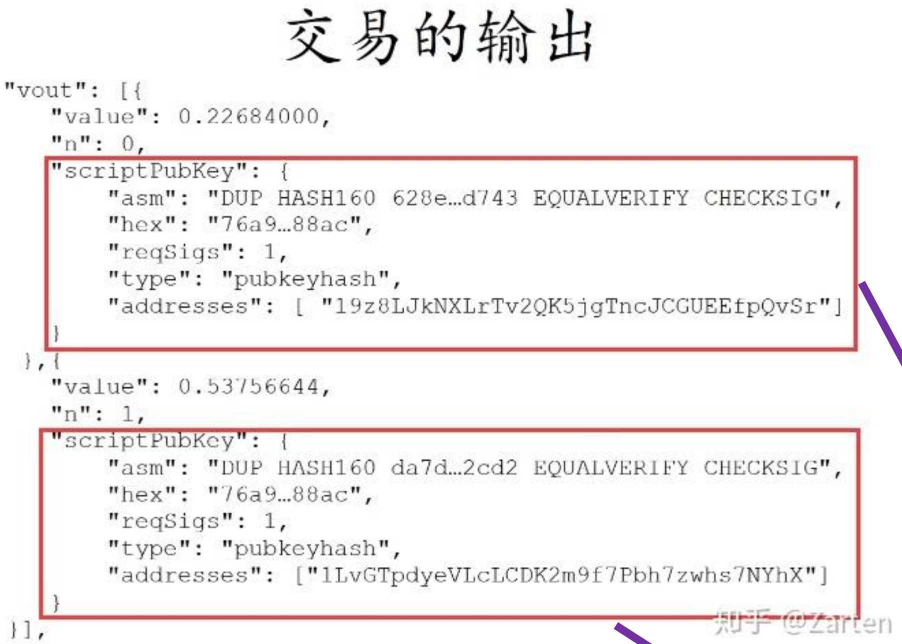


Sender

- Transaction verifications are done by miners
- Verifications usually consist of 2 parts for every single input:
  1. The user who initiates the transaction (sender) has the money
  2. The user who initiates the transaction (sender) can use the money

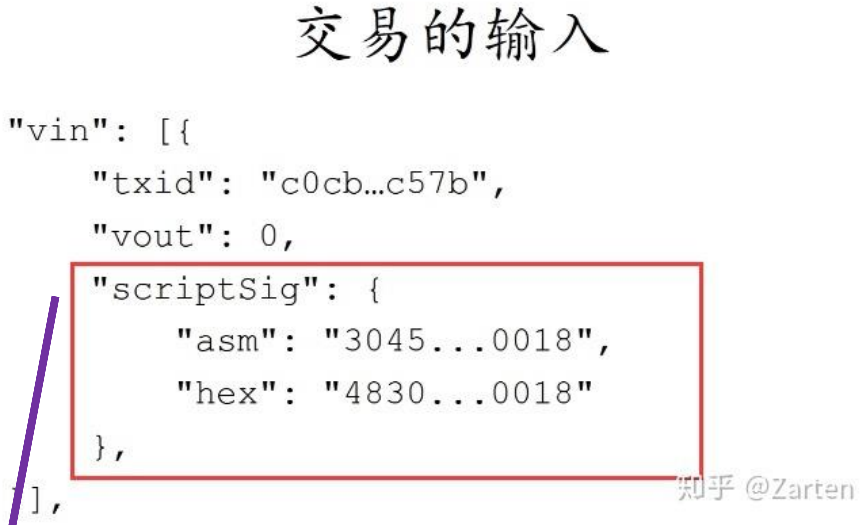
- The 1st part is done by matching the sender's pubkey to the incoming transaction's destination recipient address
- The 2nd part is done by executing the concatenated signature script (scriptSig) and output script (scriptPubKey)

ScriptSig and ScriptPubKey



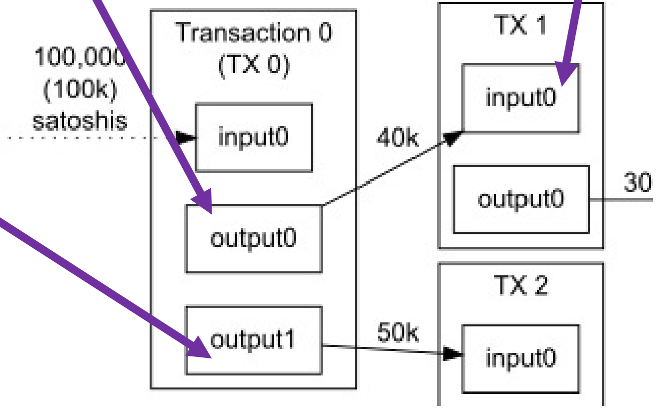
交易的输出

```
"vout": [{
   "value": 0.22684000,
   "n": 0,
   "scriptPubKey": {
       "asm": "DUP HASH160 628e…d743 EQUALVERIFY CHECKSIG",
       "hex": "76a9…88ac",
       "reqSigs": 1,
       "type": "pubkeyhash",
       "addresses": [ "19z8LJkNXLrTv2QK5jgTncJCGUEEfpQvSr"]
   }
 },{
   "value": 0.53756644,
   "n": 1,
   "scriptPubKey": {
       "asm": "DUP HASH160 da7d…2cd2 EQUALVERIFY CHECKSIG",
       "hex": "76a9…88ac",
       "reqSigs": 1,
       "type": "pubkeyhash",
       "addresses": ["1LvGTpdyeVLcLCDK2m9f7Pbh7zwhs7NYhX"]
   }
}],
```



交易的输入

```
"vin": [{
    "txid": "c0cb…c57b",
    "vout": 0,
    "scriptSig": {
        "asm": "3045...0018",
        "hex": "4830...0018"
    },
  }],
```



解锁脚本（scriptSig）
又称为输入脚本

锁定脚本（scriptPubKey）
又称为输出脚本

https://zhuanlan.zhihu.com/p/121039362

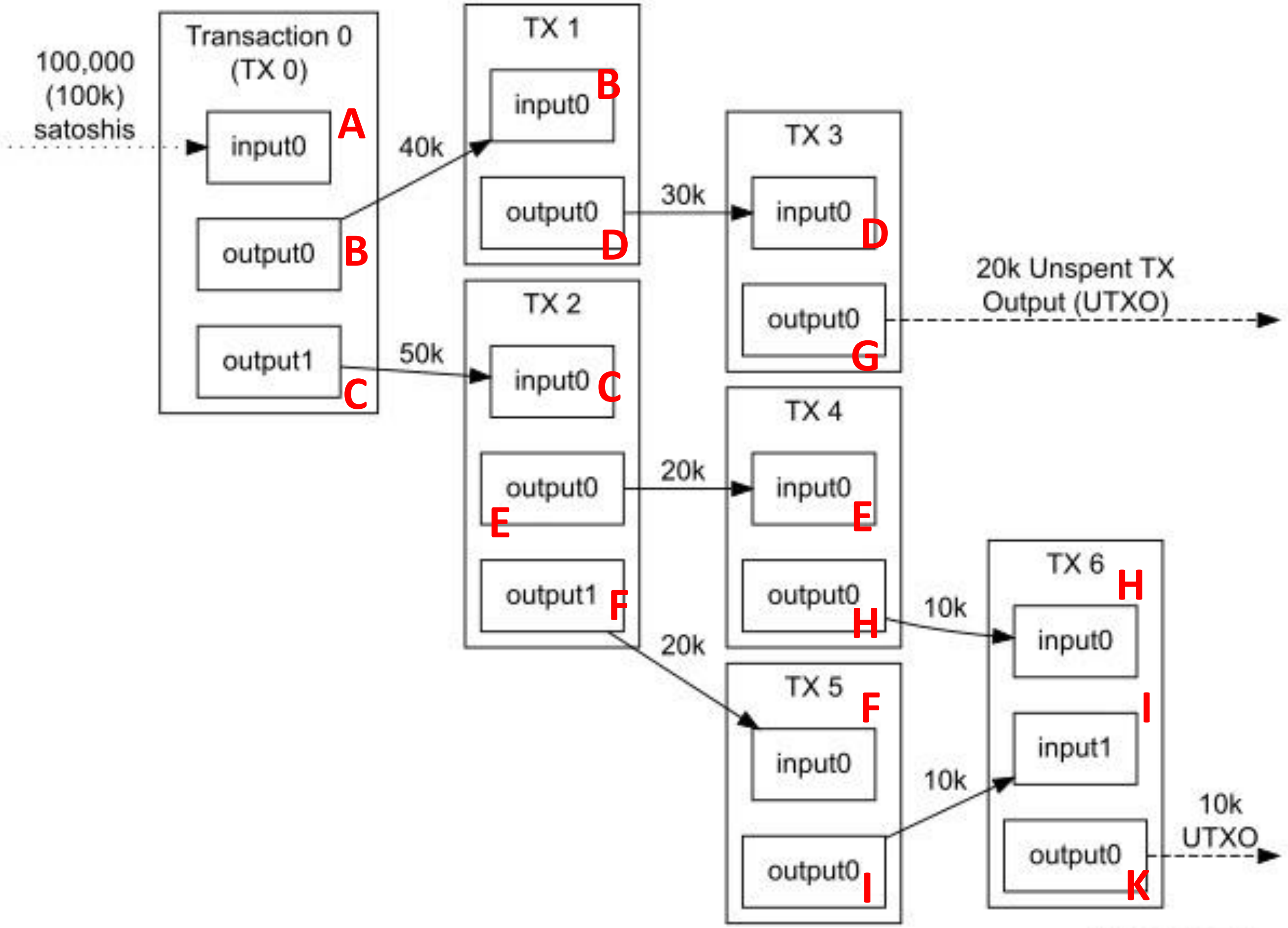
More Questions

1, what kind of signatures are required for each transaction?

2, can transaction TX 3 be booked into the blockchain more than once?

3, when verifying a transaction, do we care about its output?

4, what if we initiate another transaction very similar to TX 3 with the only difference of output set to P (a brand new address)?



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Double-Spending

☑ What is this about? What is the usage?

Main design challenge in all digital currencies

Extra Requirement

A valid transaction consumes (and destroys) some coins,
and creates new coins of the same total value

Transaction valid if:

- consumed coins valid (address verification),
- not already consumed,
- total value out = total value in (including the tips paid to miners),
- signed by owners of all consumed coins

Coins are Immutable

A valid transaction consumes (and destroys) some coins,
and creates new coins of the same total value

Coins are **Immutable**:

They cannot be

- transferred,
- subdivided, or
- combined

Example - Subdivide Coin:

1. create new transaction
2. consume (destroy) your coin
3. pay out two new coins to yourself

A(7) -> A(2), A(5) _signedby(A)

UTXO

☑ What is this about? What is the usage?

- The term UTXO refers to unspent transaction output
- The amount of Bitcoin someone has left remaining after executing a transaction.
- Any coin can be created once and consumed only once. Thus, the Bitcoin blockchain is transaction based ledger, not account based.

How UTXO Gets Updated?

- Each node keeps a set of UTXO to its best knowledge

在第一次作业的时候我们看到了 UtxoPool 的结构，可以永远存储

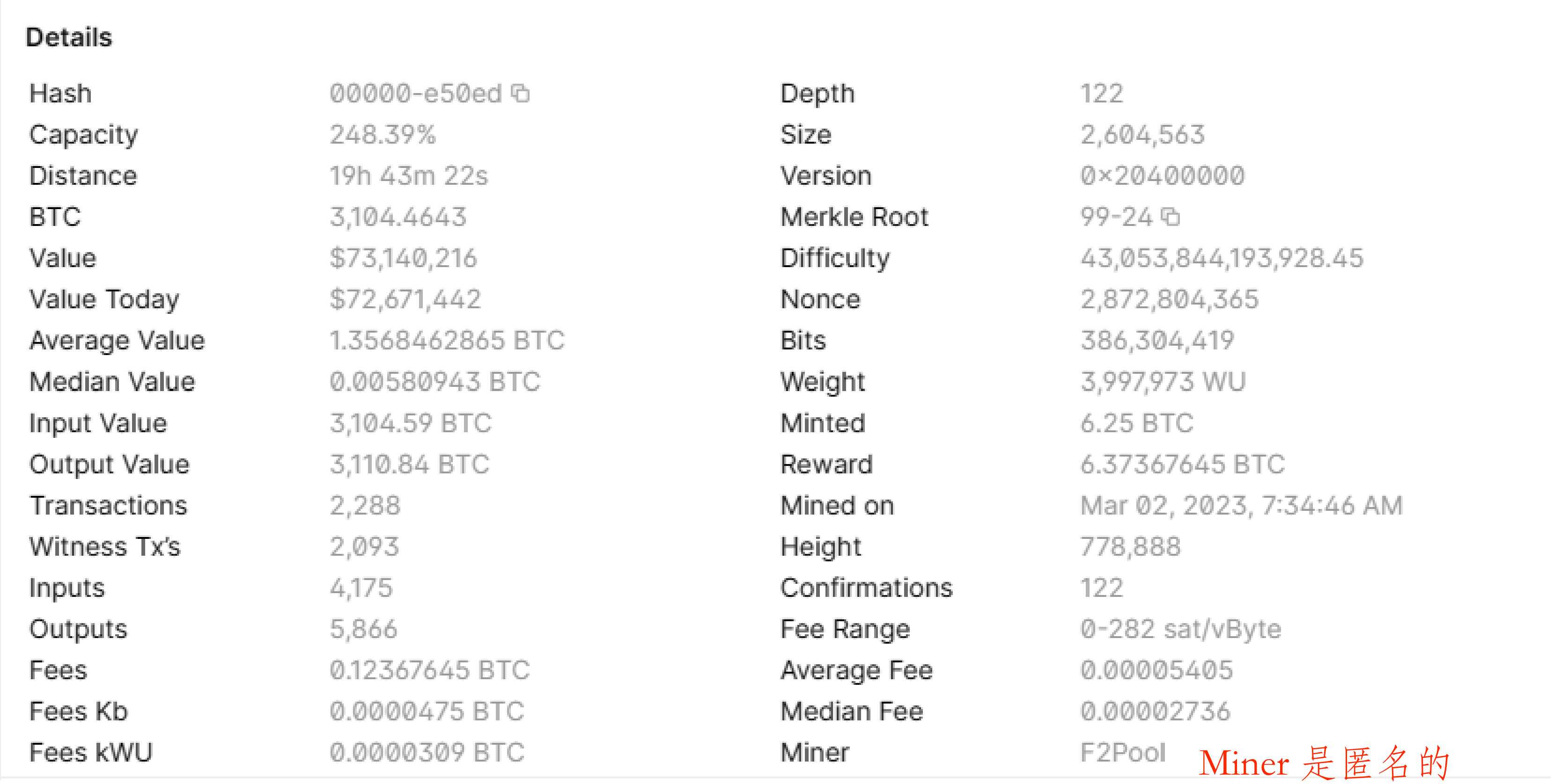
- Each node verifies the blockchain and updates the UTXO on its own

- Will those transactions not included in the Blockchain affect the UTXO status?

只有有效的被识别到的才会有影响，没有装在 Block 里面实际上没有发生

Real Block Example

- Bitcoin block 778888, https://www.blockchain.com/explorer/blocks/btc/778888



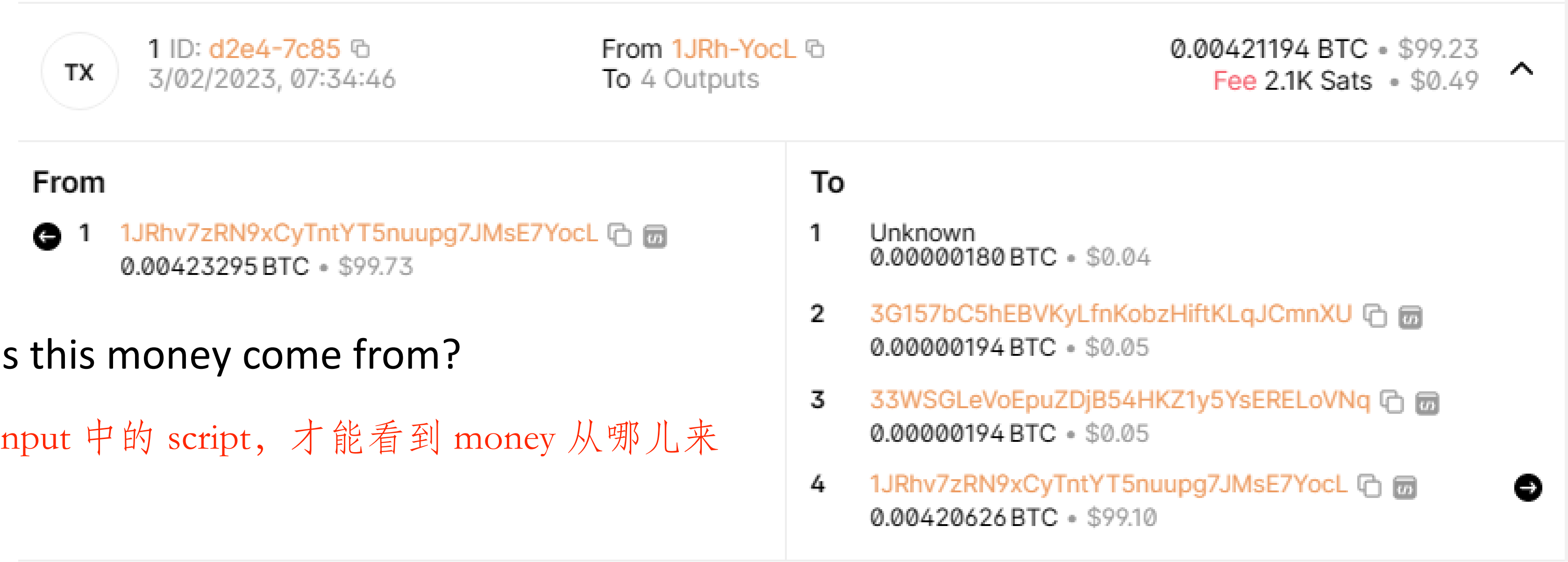
Details

Hash	00000-e50ed	Depth	122
Capacity	248.39%	Size	2,604,563
Distance	19h 43m 22s	Version	0x20400000
BTC	3,104.4643	Merkle Root	99-24
Value	$73,140,216	Difficulty	43,053,844,193,928.45
Value Today	$72,671,442	Nonce	2,872,804,365
Average Value	1.3568462865 BTC	Bits	386,304,419
Median Value	0.00580943 BTC	Weight	3,997,973 WU
Input Value	3,104.59 BTC	Minted	6.25 BTC
Output Value	3,110.84 BTC	Reward	6.37367645 BTC
Transactions	2,288	Mined on	Mar 02, 2023, 7:34:46 AM
Witness Tx's	2,093	Height	778,888
Inputs	4,175	Confirmations	122
Outputs	5,866	Fee Range	0-282 sat/vByte
Fees	0.12367645 BTC	Average Fee	0.00005405
Fees Kb	0.0000475 BTC	Median Fee	0.00002736
Fees kWU	0.0000309 BTC	Miner	F2Pool

Miner 是匿名的

Real Transaction Example

- Transaction ID d2e48fba0960e476f4f5bc74dcb1f19ef1856f7ae4b85d0beba40523cc507c85, https://www.blockchain.com/explorer/transactions/btc/d2e48fba0960e476f4f5bc74dcb1f19ef1856f7ae4b85d0beba40523cc507c85



TX 1 ID: d2e4-7c85
3/02/2023, 07:34:46

From 1JRh-YocL
To 4 Outputs

0.00421194 BTC • $99.23
Fee 2.1K Sats • $0.49

From

1 1JRhv7zRN9xCyTntYT5nuupg7JMsE7YocL
0.00423295 BTC • $99.73

To

1 Unknown
0.00000180 BTC • $0.04

2 3G157bC5hEBVKyLfnKobzHiftKLqJCmnXU
0.00000194 BTC • $0.05

3 33WSGLeVoEpuZDjB54HKZ1y5YsERELoVNq
0.00000194 BTC • $0.05

4 1JRhv7zRN9xCyTntYT5nuupg7JMsE7YocL
0.00420626 BTC • $99.10

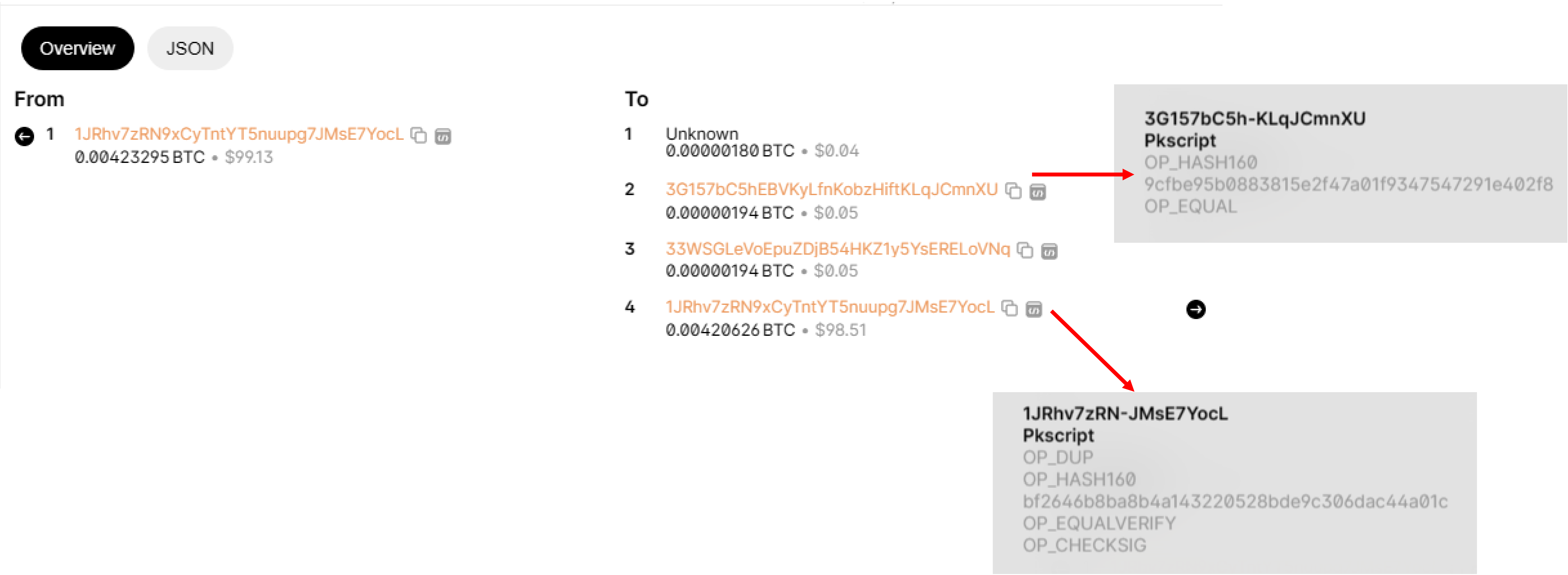
Where does this money come from?

需要读 input 中的 script，才能看到 money 从哪儿来

Has the money been spent?

Real Transaction ScriptPubKey Examples

Remember to click the JSON button to see the JSON script



From

1 1JRhv7zRN9xCyTntYT5nuupg7JMsE7YocL
0.00423295 BTC • $99.13

To

1 Unknown
0.00000180 BTC • $0.04

2 3G157bC5hEBVKyLfnKobzHiftKLqJCmnXU
0.00000194 BTC • $0.05

3 33WSGLeVoEpuZDjB54HKZ1y5YsERELoVNq
0.00000194 BTC • $0.05

4 1JRhv7zRN9xCyTntYT5nuupg7JMsE7YocL
0.00420626 BTC • $98.51

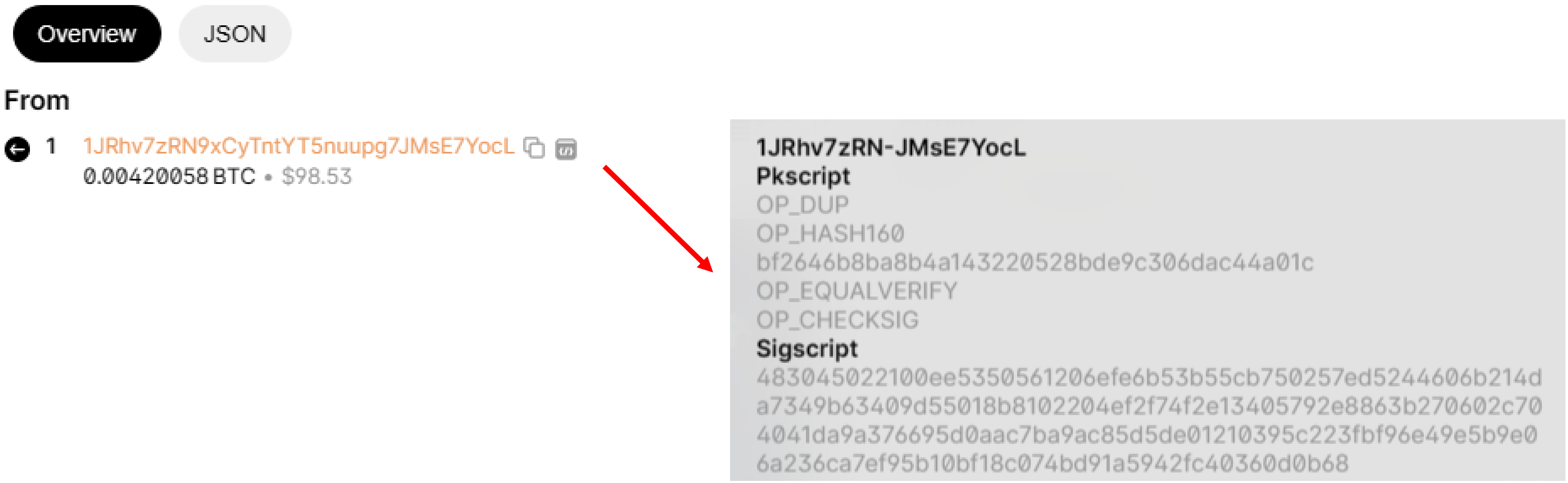
3G157bC5h-KLqJCmnXU
Pkscript
OP_HASH160
9cfbe95b0883815e2f47a01f9347547291e402f8
OP_EQUAL

1JRhv7zRN-JMsE7YocL
Pkscript
OP_DUP
OP_HASH160
bf2646b8ba8b4a143220528bde9c306dac44a01c
OP_EQUALVERIFY
OP_CHECKSIG

Real Transaction ScriptSig Examples

Because a single address can receive many incoming coins, which are immutable, so it is very important to match the exact transaction for each coin received in this address. **Try clicking the outgoing arrow**.

https://www.blockchain.com/explorer/transactions/btc/7f9d0b629e9c77cd014e65518ce16e22bee8ec7640571ea7826cb367700351fe



From

1 1JRhv7zRN9xCyTntYT5nuupg7JMsE7YocL
0.00420058 BTC • $98.53

1JRhv7zRN-JMsE7YocL

Pkscript

```
OP_DUP
OP_HASH160
bf2646b8ba8b4a143220528bde9c306dac44a01c
OP_EQUALVERIFY
OP_CHECKSIG
```

Sigscript

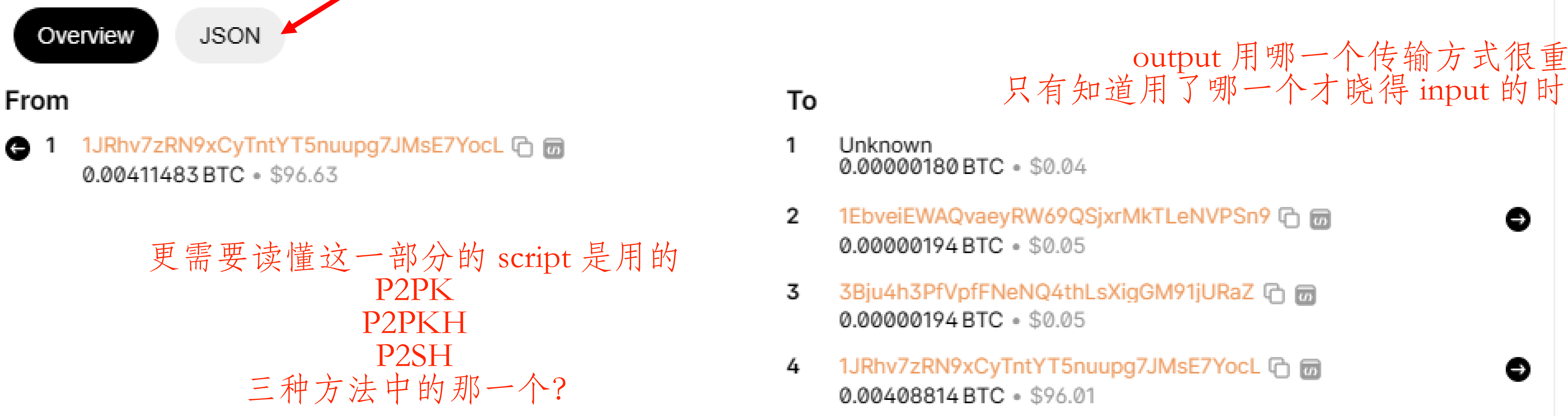
```
483045022100ee5350561206efe6b53b55cb750257ed5244606b214d
a7349b63409d55018b8102204ef2f74f2e13405792e8863b270602c70
4041da9a376695d0aac7ba9ac85d5de01210395c223fbf96e49e5b9e0
6a236ca7ef95b10bf18c074bd91a5942fc40360d0b68
```

Keep Following the Spent Coins

Because a single address can receive many incoming coins, which are immutable, so it is very important to match the exact transaction for each coin received in this address. **Try clicking the outgoing arrow**.

https://www.blockchain.com/explorer/transactions/btc/741fb93f5dbd172be933d8650c256999d0ed49c7d405006d2879ca8a88a7033b

Remember to click the JSON button to see the JSON script



Overview JSON

From

← 1 1JRhv7zRN9xCyTntYT5nuupg7JMsE7YocL
0.00411483 BTC • $96.63

To

1 Unknown
0.00000180 BTC • $0.04

2 1EbveiEWAQvaeyRW69QSjxrMkTLeNVPSn9 →
0.00000194 BTC • $0.05

3 3Bju4h3PfVpfFNeNQ4thLsXigGM91jURaZ
0.00000194 BTC • $0.05

4 1JRhv7zRN9xCyTntYT5nuupg7JMsE7YocL →
0.00408814 BTC • $96.01

output 用哪一个传输方式很重要
只有知道用了哪一个才晓得 input 的时候如何取钱

更需要读懂这一部分的 script 是用的
P2PK
P2PKH
P2SH
三种方法中的那一个?

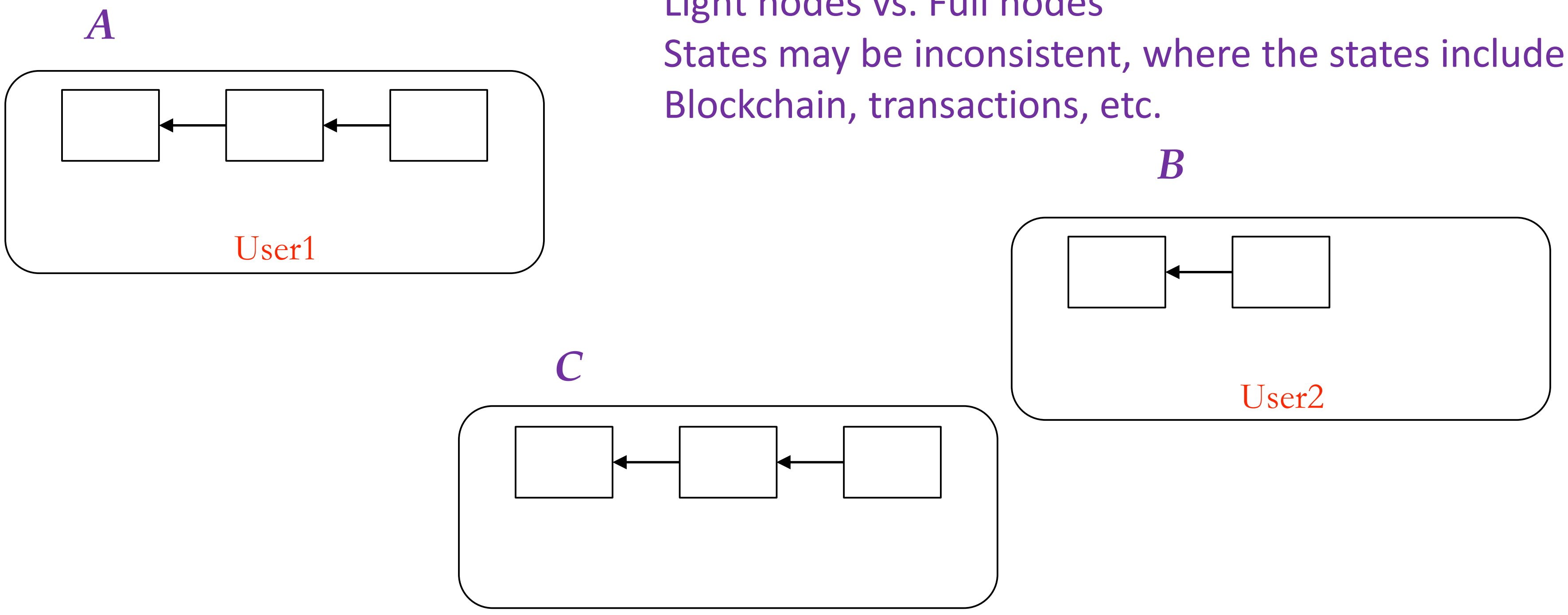
Bitcoin Network

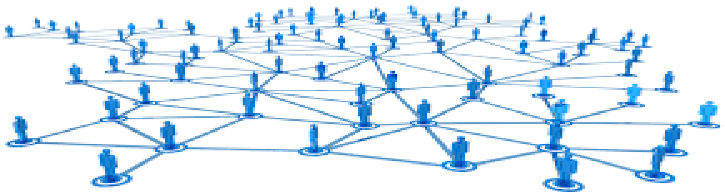
How Bitcoin Network Works

- Two layers of network:
  - Application layer: Bitcoin Blockchain 底层载体
  - Network layer: P2P network 载体联结的方式
- Distributed consensus protocol for application layer
- Simple, robust, best-effort, not very efficient

How Bitcoin Network Works

Light nodes vs. Full nodes
States may be inconsistent, where the states include Blockchain, transactions, etc.

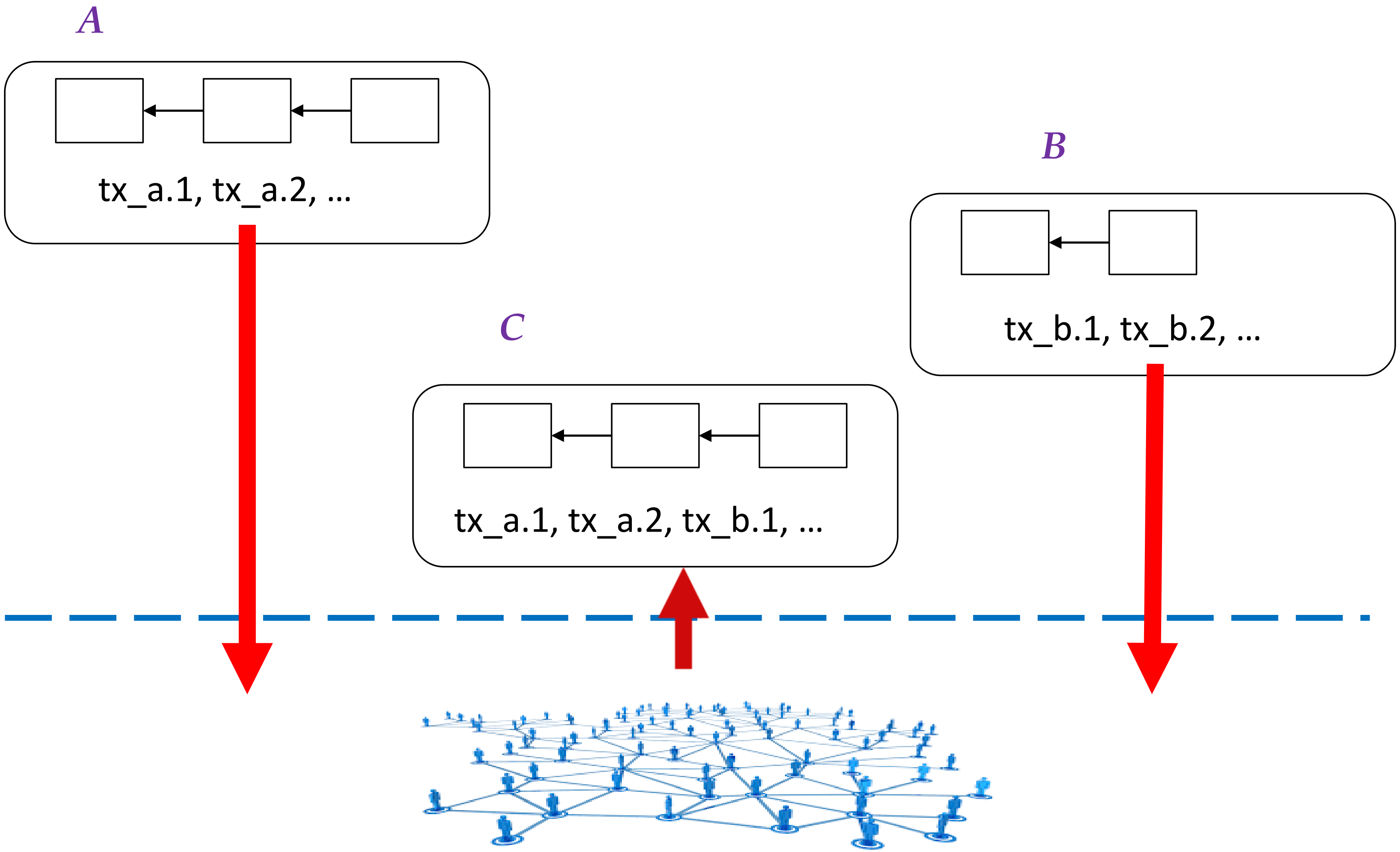




How Transactions Are Handled

- Transactions are generated by nodes, either users and miners
  - Coinbase transactions by miners
  - Transfer transactions by users
- When a transaction is generated by a node, it gets broadcasted into the P2P network

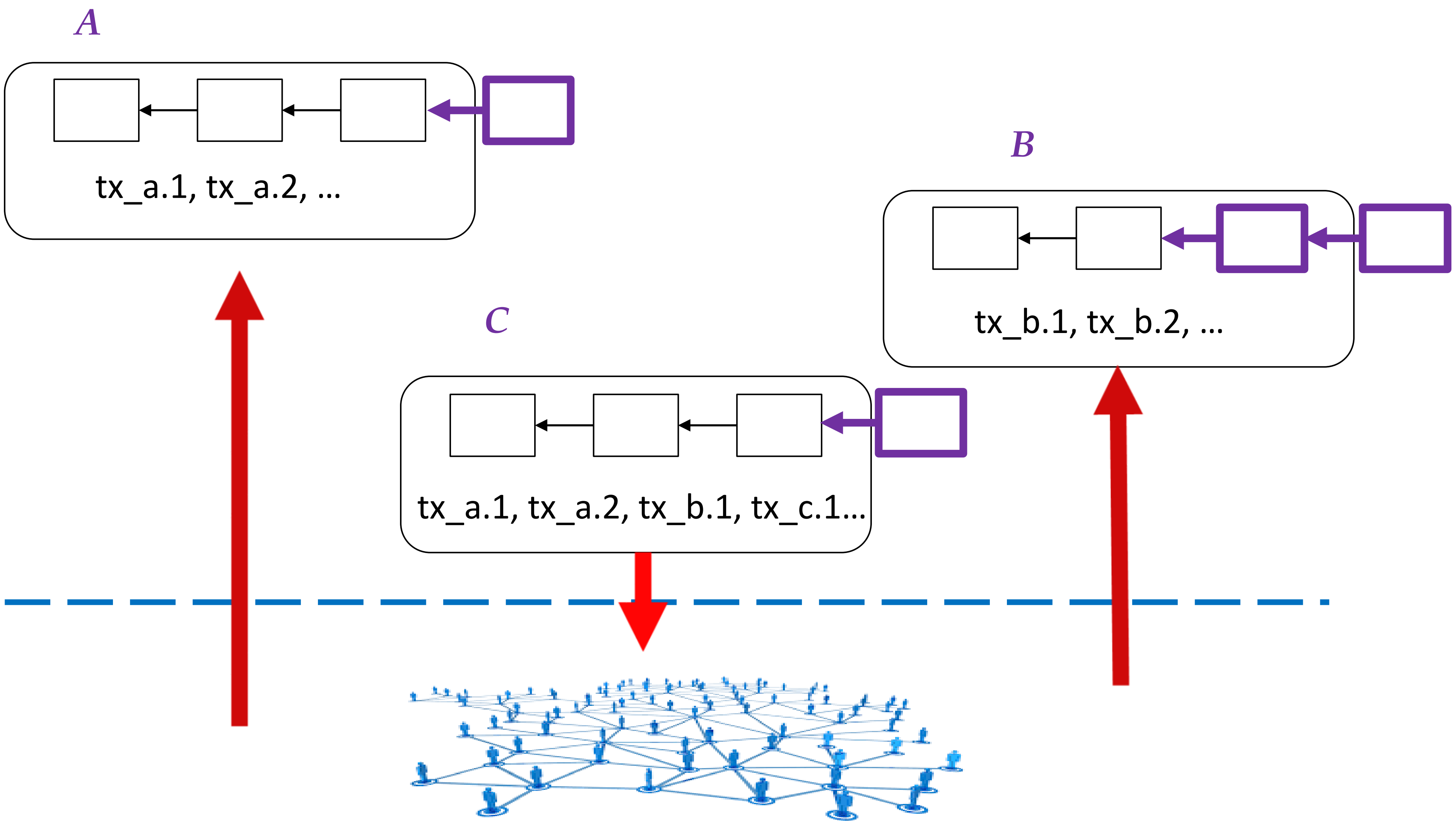
How Transactions Are Handled



How Blocks Are Handled

- Transactions are saved and verified by miner nodes, and packaged by miner nodes into a block
- The block gets broadcasted via the P2P network as soon as possible
- Transactions already packaged into blockchain will be marked by nodes to be excluded when packaging new blocks

How Blocks Are Handled



Bitcoin P2P Network

Global Bitcoin Nodes Distribution – Bitnodes https://bitnodes.io/

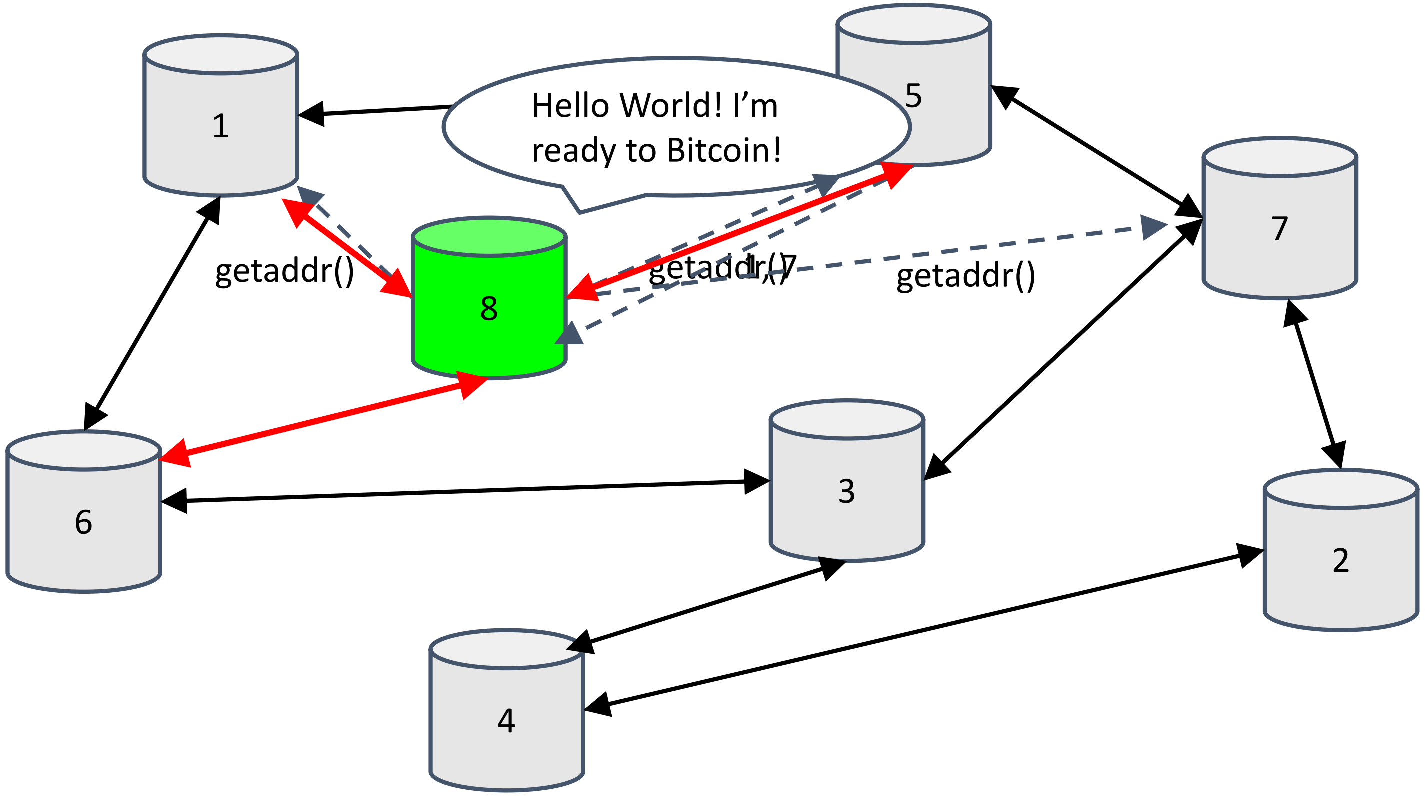
Participants can

- publish transactions
- insert transactions into block chain

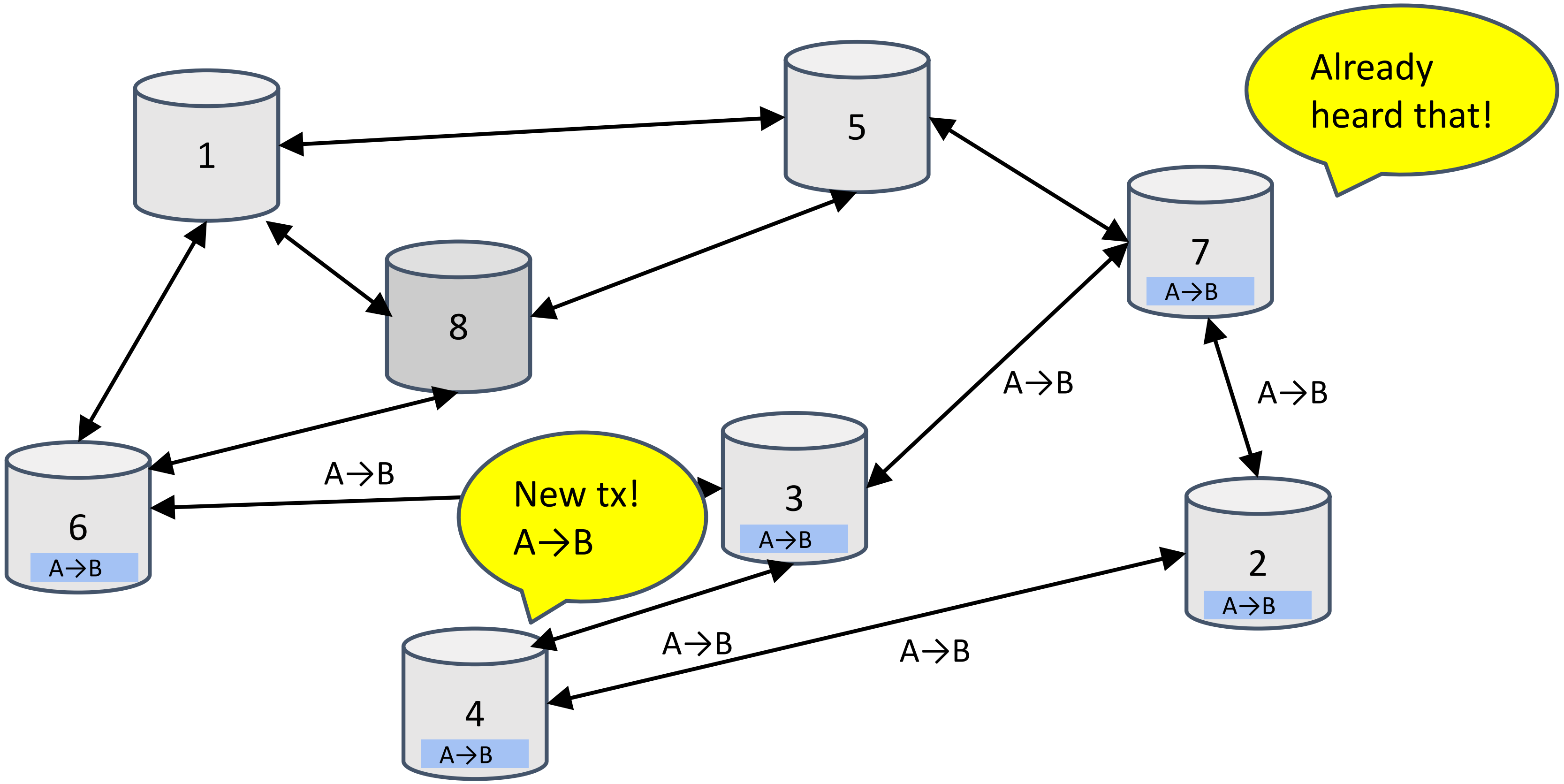
The network:

- – Ad-hoc protocol (runs on TCP port 8333)
- – Ad-hoc network with random topology
- – All nodes are equal
- – New nodes can join at any time
- – Forget non-responding nodes after 3 hr

Joining the Bitcoin P2P Network



Transaction Propagation (Flooding)



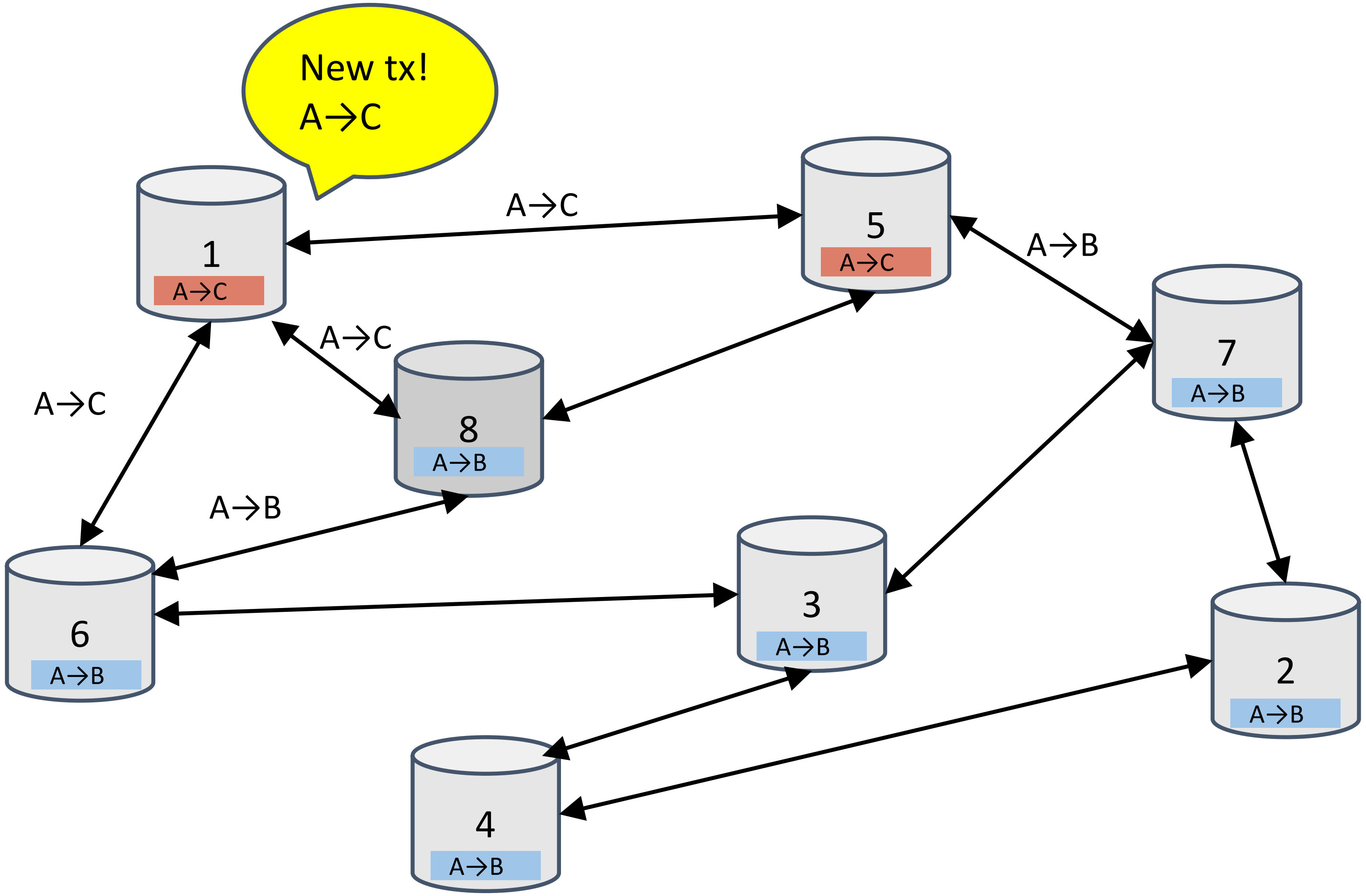
广播是为了自己，获取更多信息，这是博弈论的一个经典应用

Should I relay a proposed Transaction?

- Transaction valid with current block chain
- (default) script matches a whitelist
  - Avoid unusual scripts
- Haven't seen before
  - Avoid infinite loops
- Doesn't conflict with others I've relayed
  - Avoid double-spends

Sanity checks only...
Some nodes may ignore them!

Nodes may differ on Transaction Pool

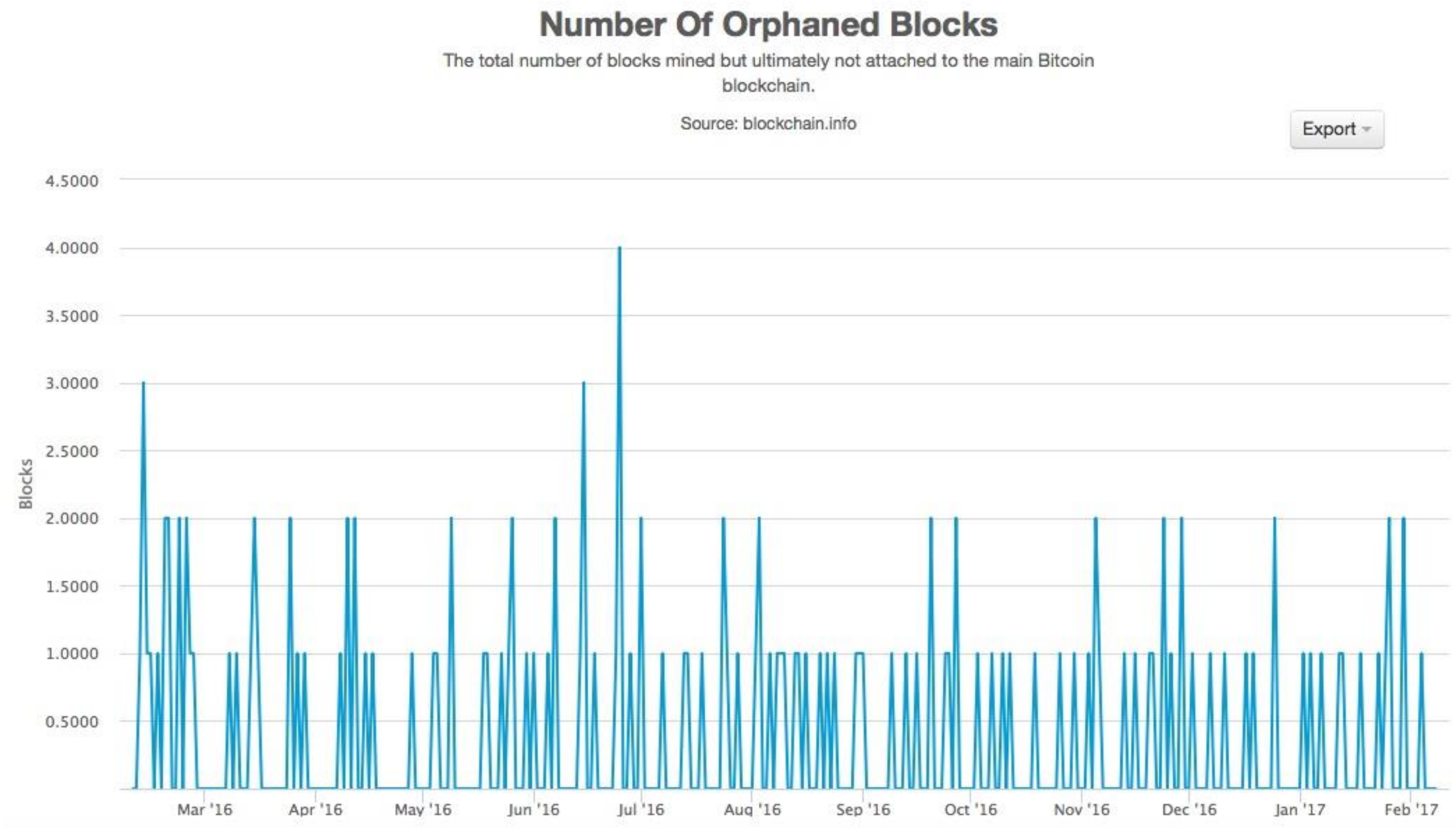


Race Conditions

Transactions or blocks may conflict

- This is called **“race condition”**
- Default behavior: accept what you hear first
- Tie broken by whoever mines next block
  - picks only one transaction/block
- Network position matters
- Miners may implement other logic!

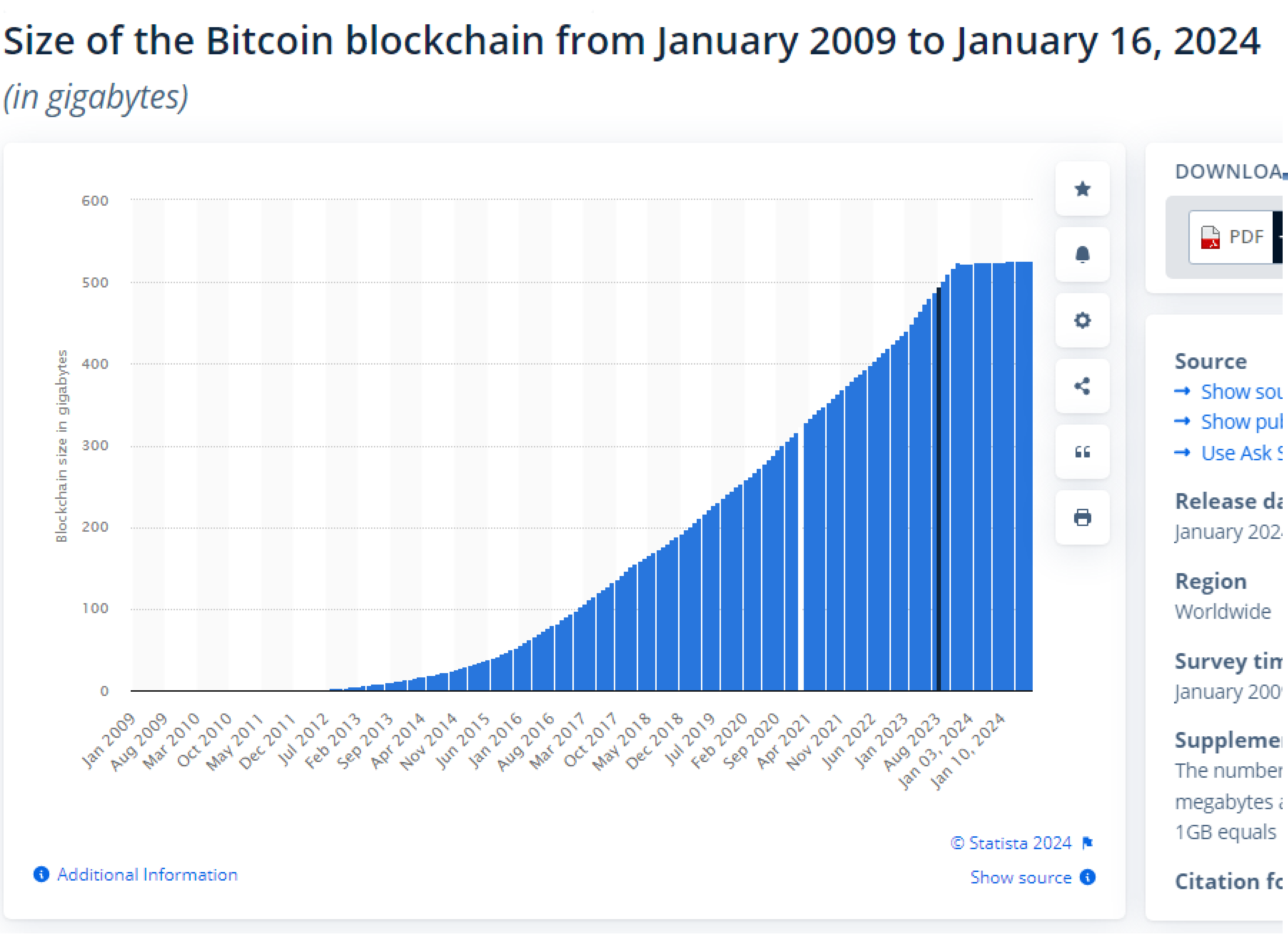
Orphaned Blocks



Number Of Orphaned Blocks

The total number of blocks mined but ultimately not attached to the main Bitcoin blockchain.

Source: blockchain.info



Size of the Bitcoin blockchain from January 2009 to January 16, 2024

(in gigabytes)

Source

→ Show sou

→ Show pul

→ Use Ask S

Release da

January 202

Region

Worldwide

Survey tim

January 200

Suppleme

The number
megabytes a
1GB equals

Citation fo

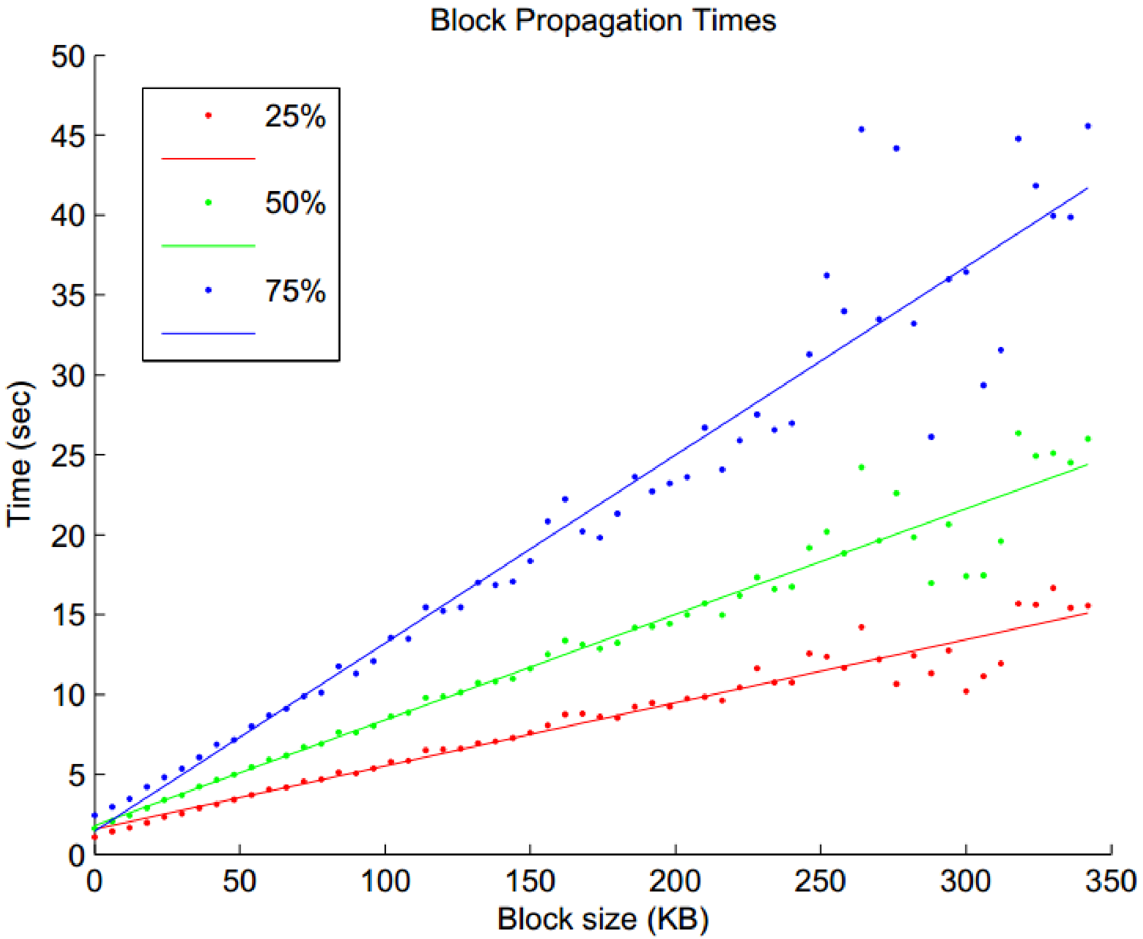
Block Propagation

Propagation of blocks is nearly identical:

Relay a new block when you hear it if:

1. Block meets the hash target
2. Block has all valid transactions
   - Run *all* scripts, even if you wouldn't relay
3. Block builds on current longest chain
   - Avoid forks

Latency of Flooding Algorithm



Source: Yonatan Sompolinsky and Aviv Zohar: “Accelerating Bitcoin’s Transaction Processing” 2014

Size of the Network

Q: How big is the Network?

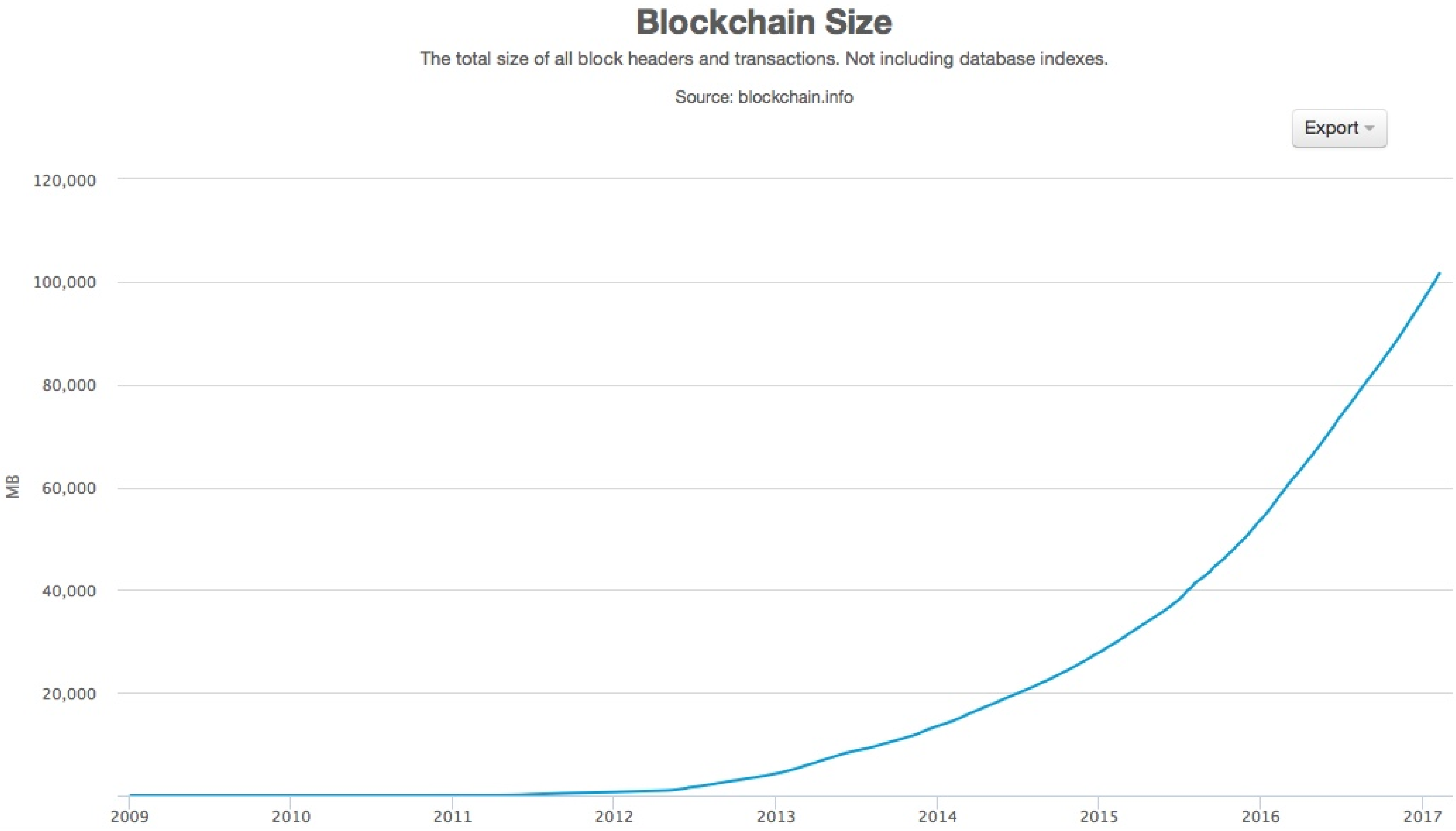
Impossible to measure exactly

- Estimates-up to 1M IP addresses/month
- Only about 5-10k “full nodes”
  - Permanently connected
  - Fully-validating
- This number may be dropping!

Fully-validating Nodes:

- Permanently connected
- Store entire block chain
- Hear and forward every node/transaction

Storage Costs

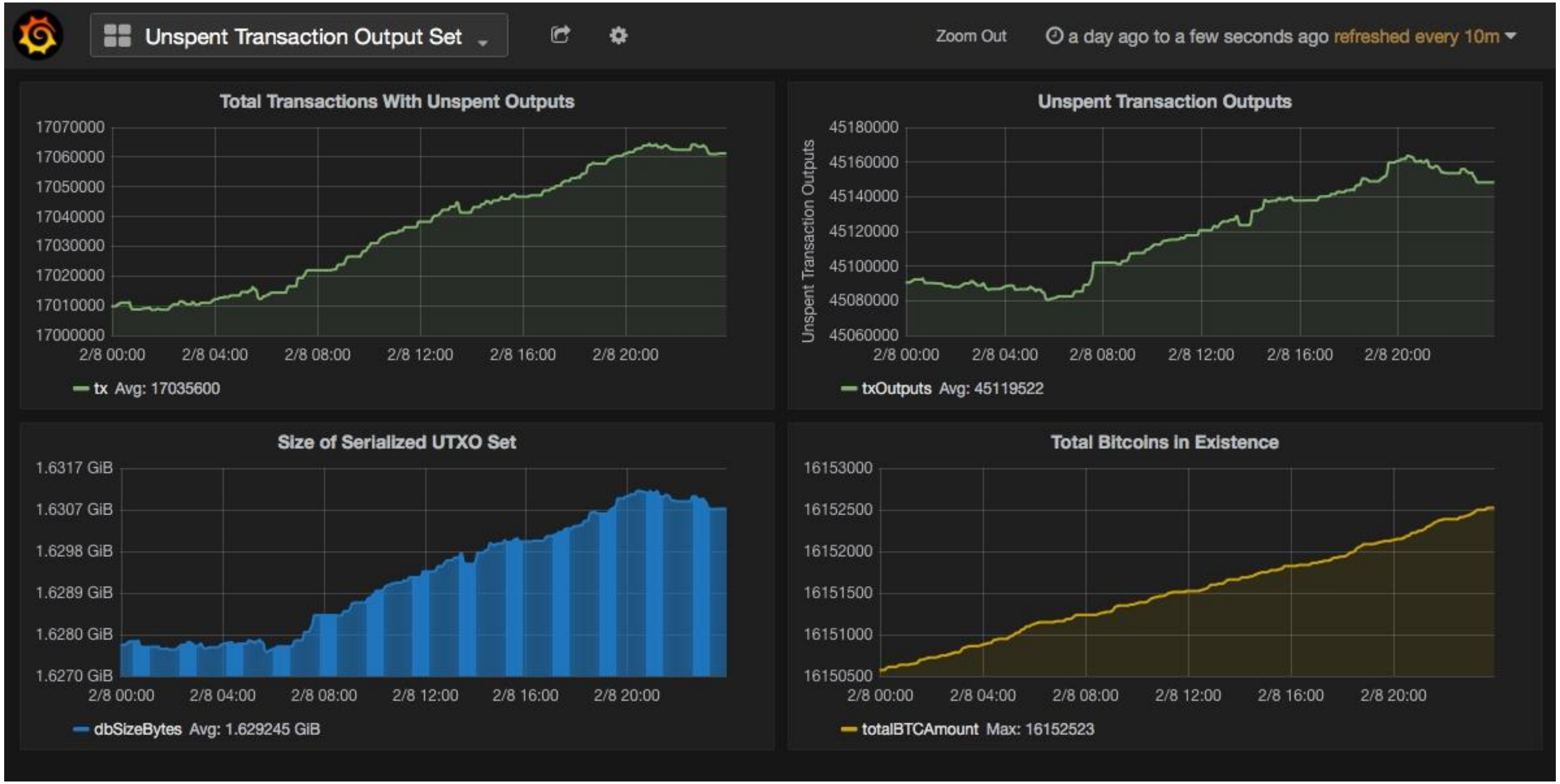


Blockchain Size

The total size of all block headers and transactions. Not including database indexes.

Source: blockchain.info

Unspent Transaction Output fits in RAM



Thin/SPV Clients (not fully-validating)

Idea: don't store everything

- Store block headers only

Request transactions as needed

- To verify incoming payment

Trust fully-validating nodes

1000x cost savings!

Software Diversity

- About 90% of nodes run “Core Bitcoin” (C++)
  - Some are out of date versions
- Other implementations running successfully
  - BitcoinJ (Java)
  - Libbitcoin (C++)
  - btcd (Go)
- “Original Satoshi client”