



BITS Pilani
Pilani Campus

Blockchain Technology (BITS F452)

Dr. Ashutosh Bhatia, Dr. Kamlesh Tiwari
Department of Computer Science and Information Systems



BITS Pilani
Pilani Campus

BITCOIN: Blocks and P2P Network

Source: Bitcoin and Cryptocurrency Technologies Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder

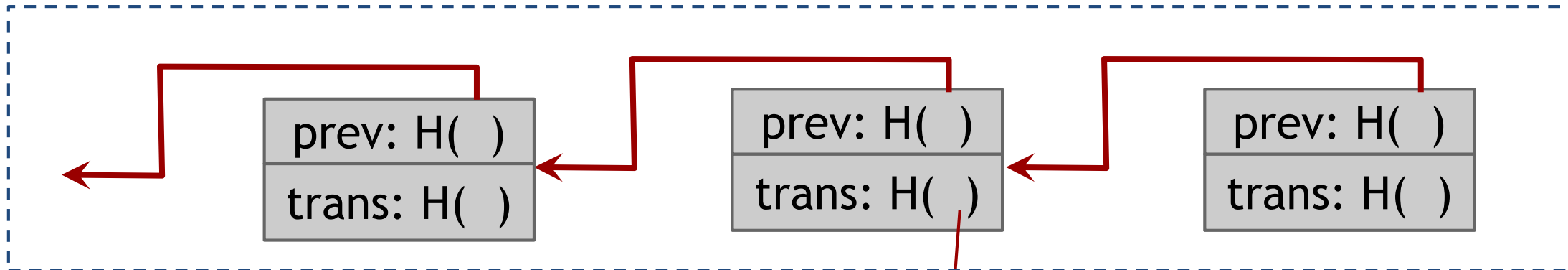
Bitcoin blocks

Why bundle transactions together?

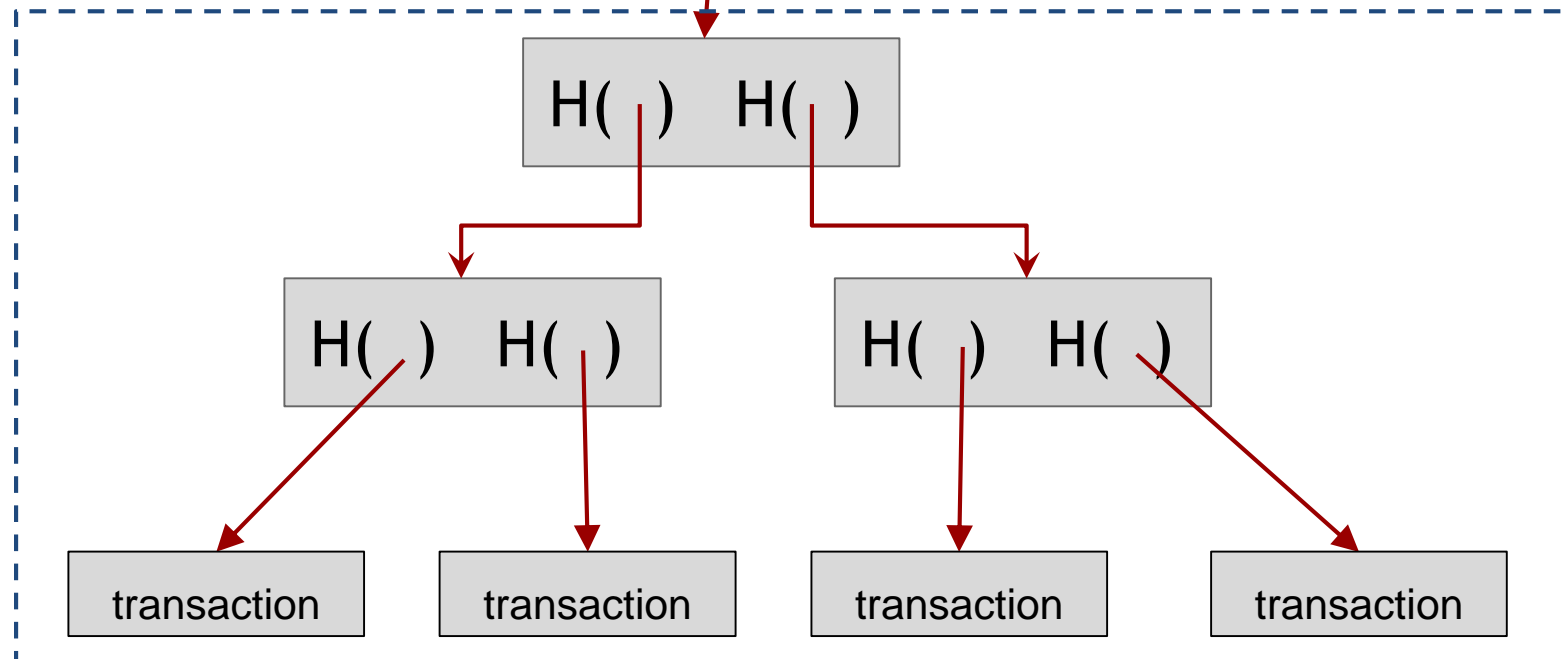
- Single unit of work for miners
- Limit length of hash-chain of blocks
 - Faster to verify history

Bitcoin block structure

Hash chain of blocks



Hash tree (Merkle tree)
of transactions in each
block



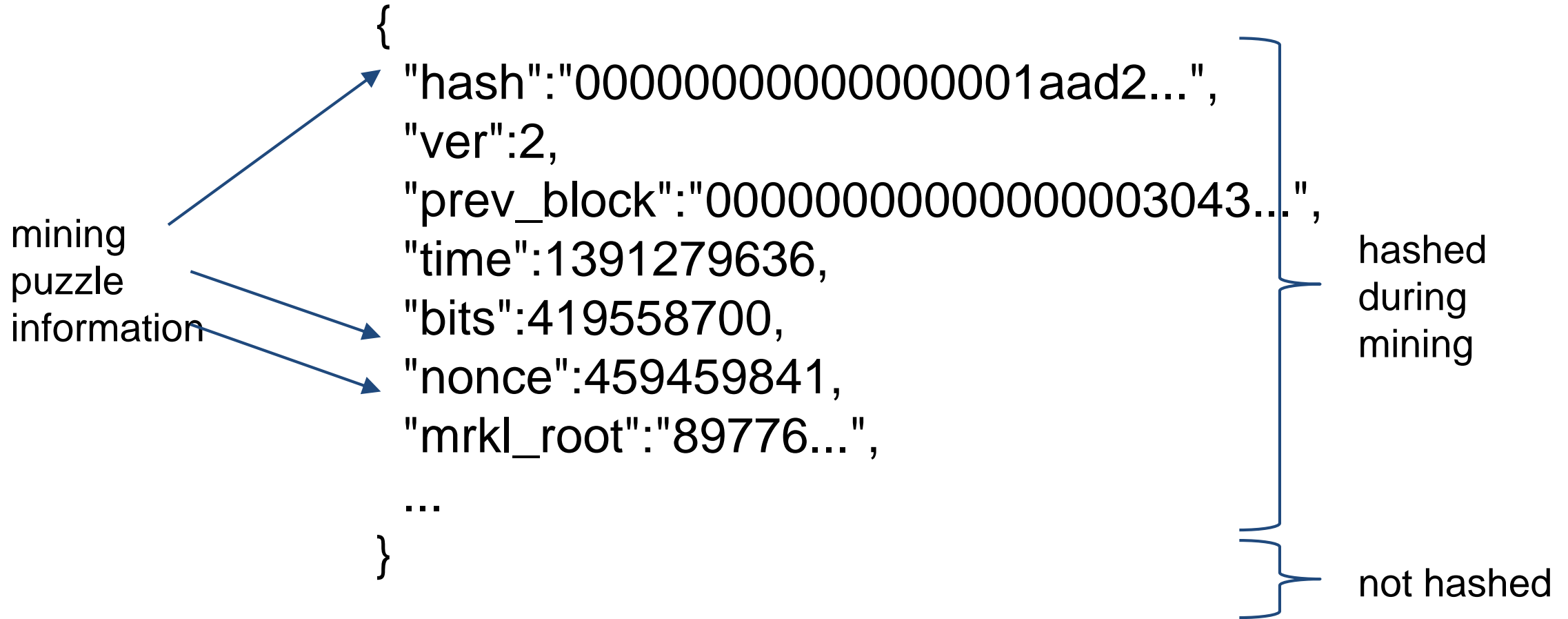
The real deal: a Bitcoin block

block
header

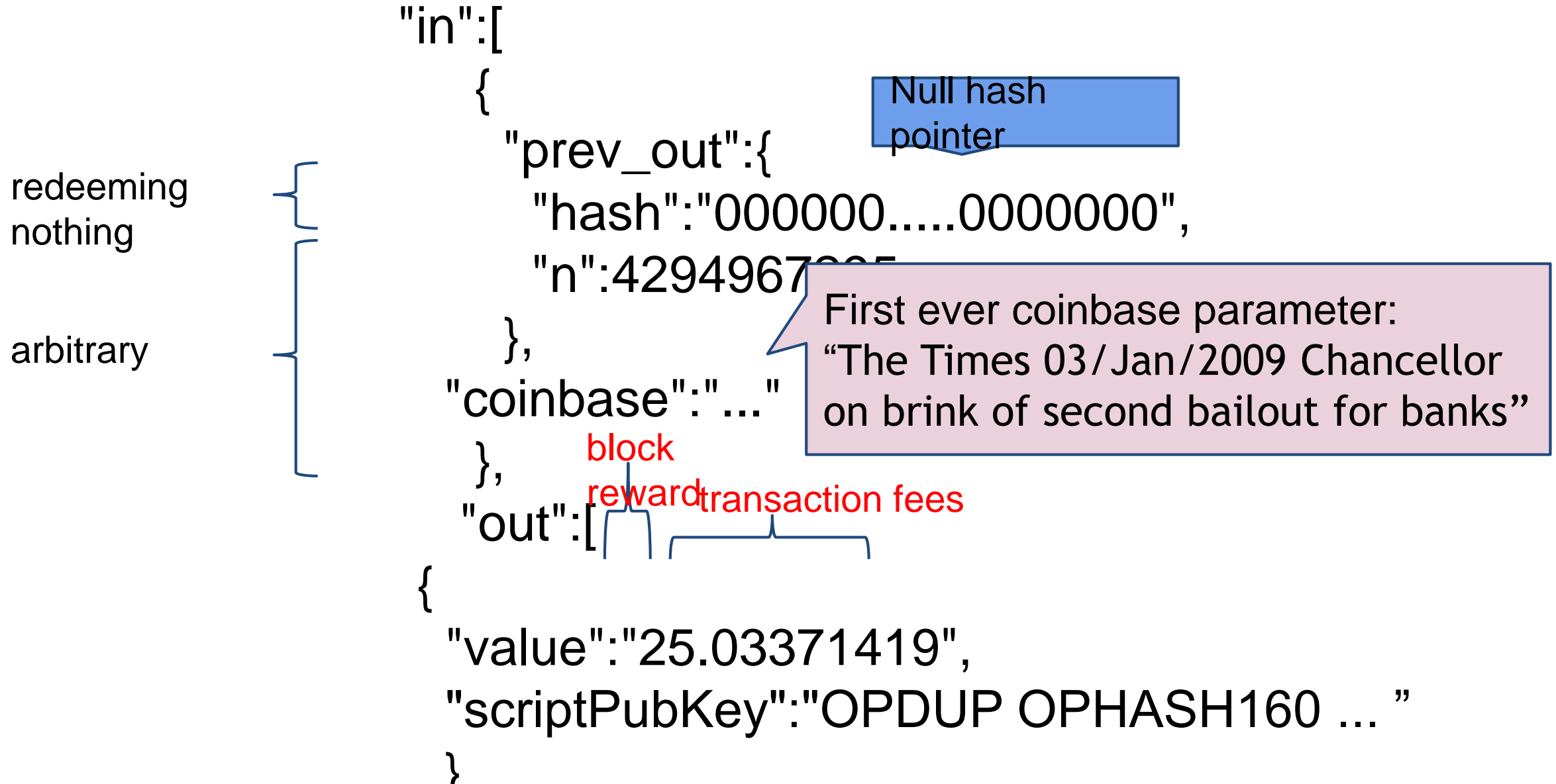
transaction
data

```
{  
  "hash":"000000000000000001aad2...",  
  "ver":2,  
  "prev_block":"000000000000000003043...",  
  "time":1391279636,  
  "bits":419558700,  
  "nonce":459459841,  
  "mrkl_root":"89776...",  
  "n_tx":354,  
  "size":181520,  
  "tx":[  
    ...  
  ],  
  "mrkl_tree":[  
    "6bd5eb25...",  
    ...  
    "89776cdb..."  
  ]  
}
```

The real deal: a Bitcoin block header



The real deal: coinbase transaction



See for yourself!

Transaction View information about a bitcoin transaction

151b750d1f13e76d84e82b34b12688811b23a8e3119a1cba4b4810f9b0ef408d

1KryFUt9tXHvaoCYTNPbqpWPJKQ717YmL5




1KvrdrQ3oGqMAiDTMEYCcdDSnVaGNW2YZh
1KryFUt9tXHvaoCYTNPbqpWPJKQ717YmL5

1.0194 BTC
3.458 BTC

9 Confirmations

4.4774 BTC

Summary

Size	257 (bytes)
Received Time	2014-08-05 01:55:25
Included In Blocks	314018 (2014-08-05 02:00:40 +5 minutes)
Confirmations	9 Confirmations
Relayed by IP 	Blockchain.info
Visualize	View Tree Chart

Inputs and Outputs

Total Input	4.4775 BTC
Total Output	4.4774 BTC
Fees	0.0001 BTC
Estimated BTC Transacted	1.0194 BTC
Scripts	Show scripts & coinbase

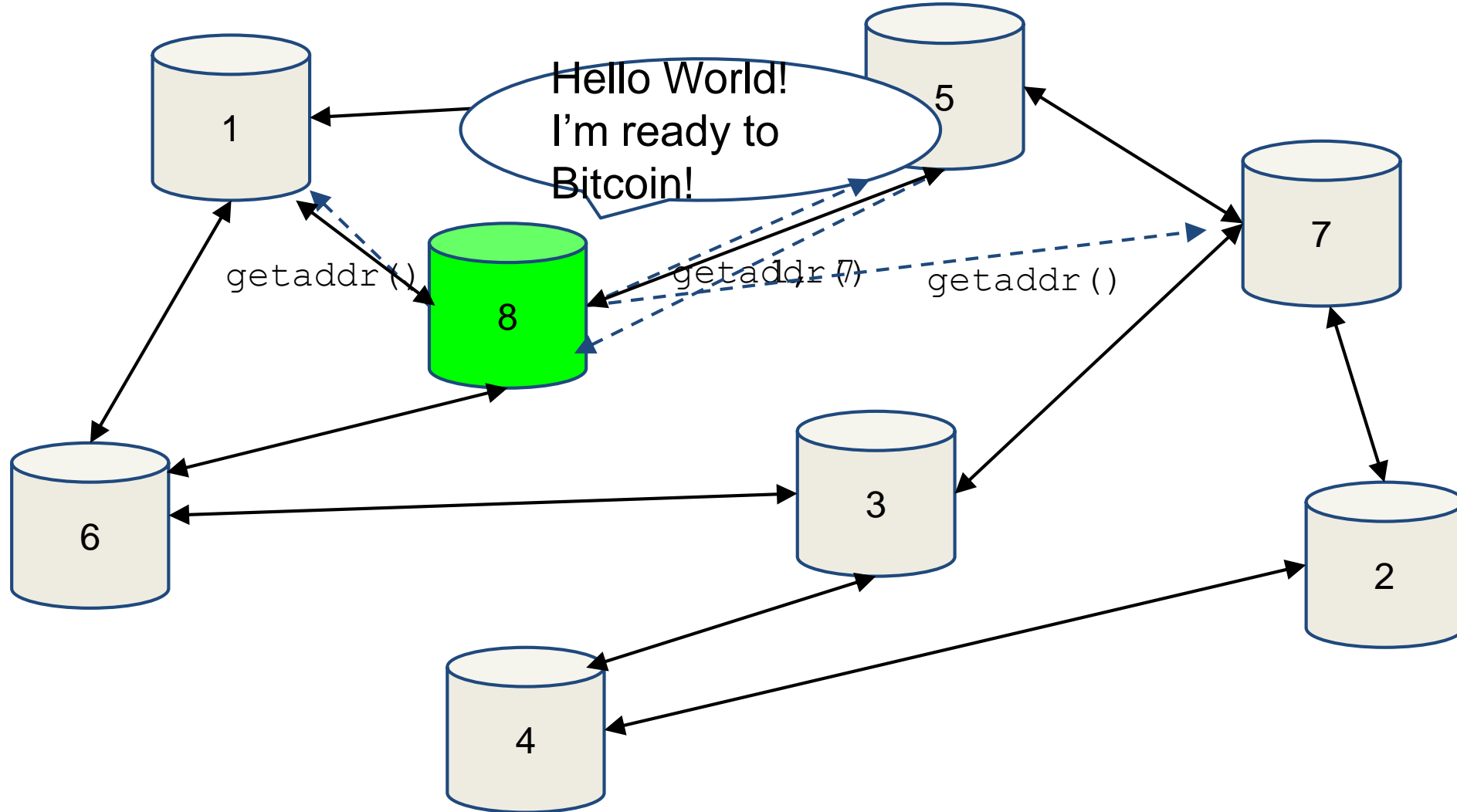
blockchain.info (and many other sites)

The Bitcoin network

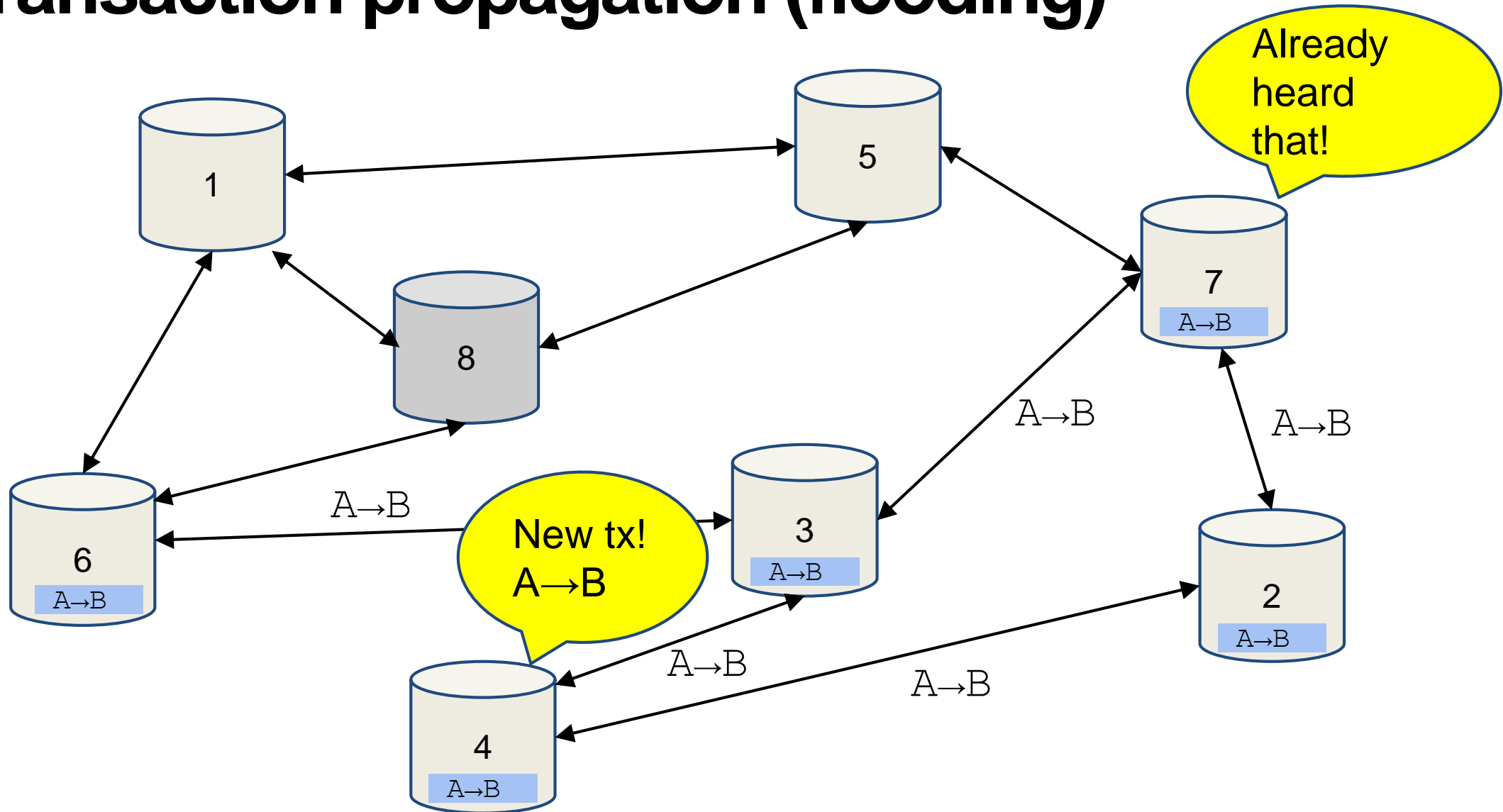
Bitcoin P2P network

- 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)

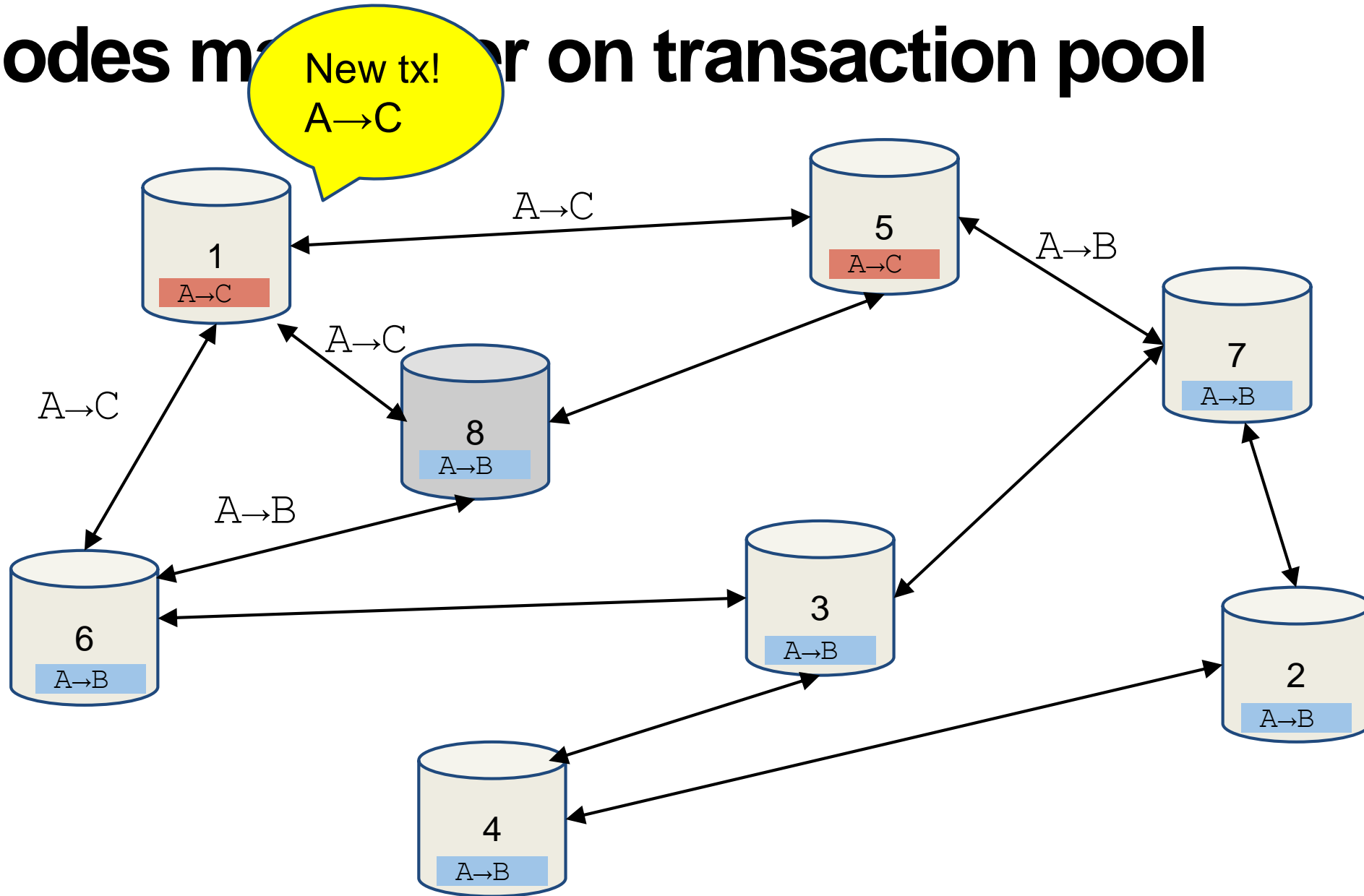


Should I relay a proposed transaction?

- Transaction valid with current block chain(default)
 - Run script for each previous output being redeemed and ensure that script returns true!
- 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...
Well-behaving nodes implement them!
Some nodes may ignore them!

Nodes must agree on transaction pool



Race conditions

Transactions or blocks may *conflict*

- Default behavior: accept what you hear first
- Network position matters
- Miners may implement other logic!

Stay tune for the lecture on mining!

Block propagation nearly identical

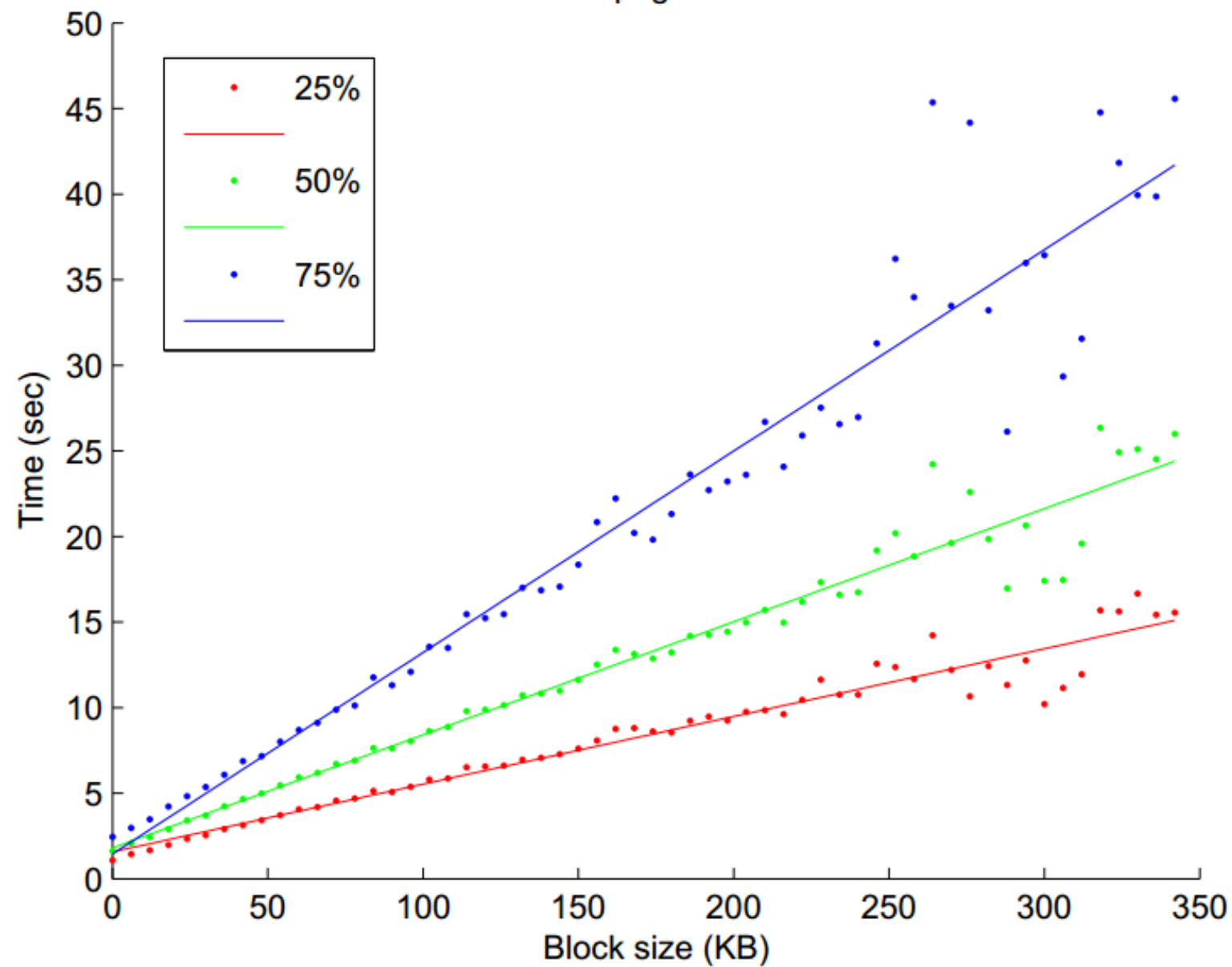
Relay a new block when you hear it if:

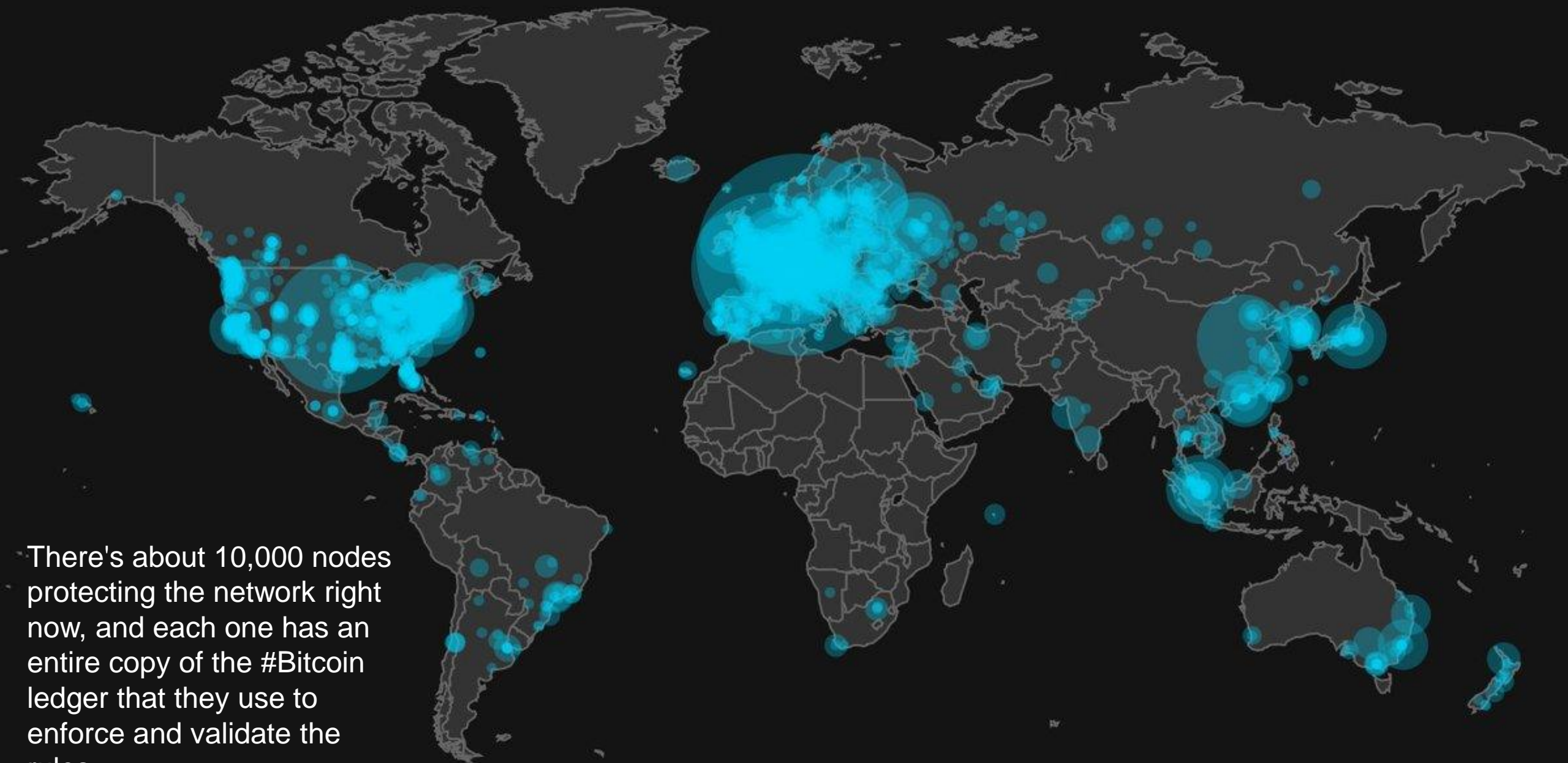
- Block meets the hash target
- Block has all valid transactions
 - Run *all* scripts, even if you wouldn't relay
- Block builds on current longest chain
 - Avoid forks



Sanity check
Also may be ignored...

Block Propagation Times





There's about 10,000 nodes protecting the network right now, and each one has an entire copy of the #Bitcoin ledger that they use to enforce and validate the rules.

How big is the network?

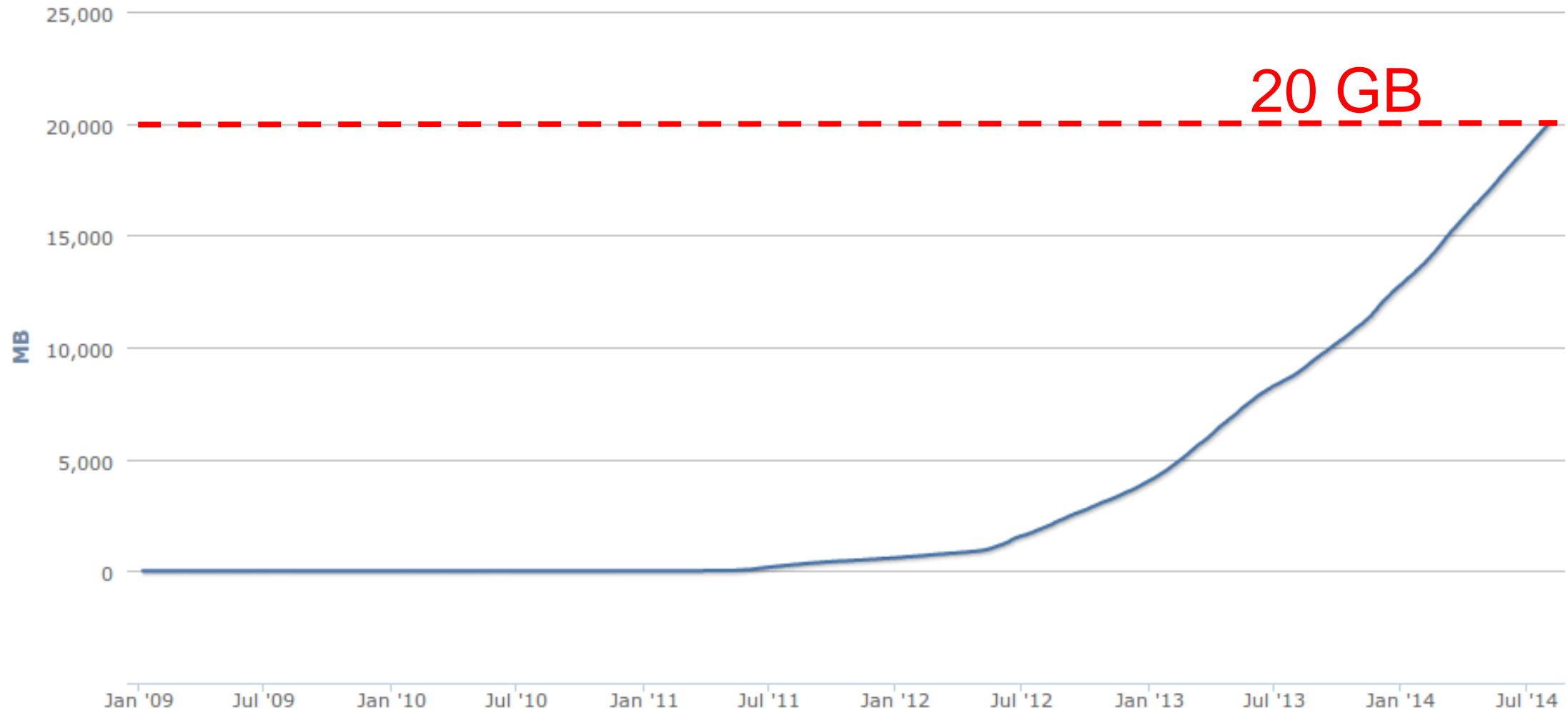
- Impossible to measure exactly
- Estimates-up to 1M IP addresses/month
- Only about 5-10k “full nodes”
 - Permanently connected
 - Fully-validate
- This number may be dropping!

Fully-validating nodes

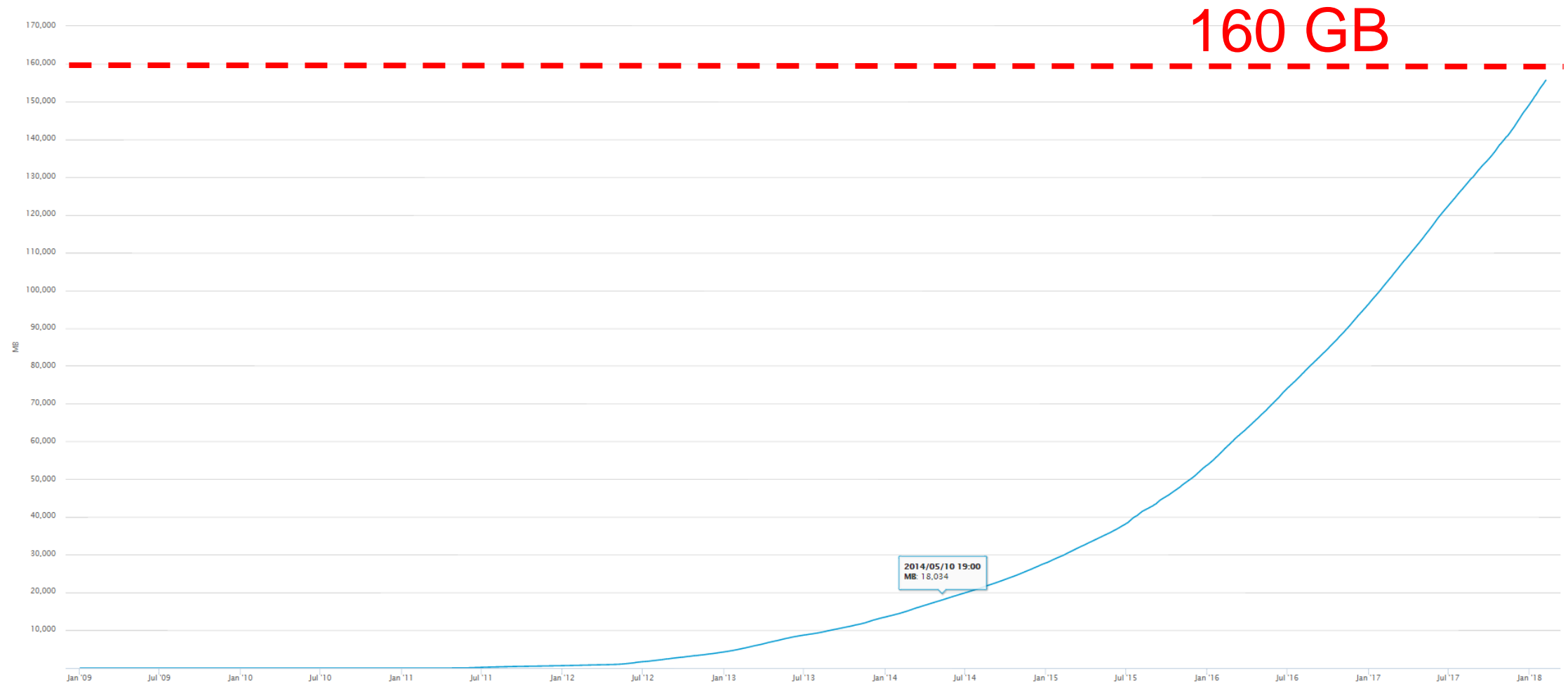
- Permanently connected
- Store entire block chain
- Hear and forward every node/transaction

Storage costs (in 2014)

Blockchain Size
Source: blockchain.info

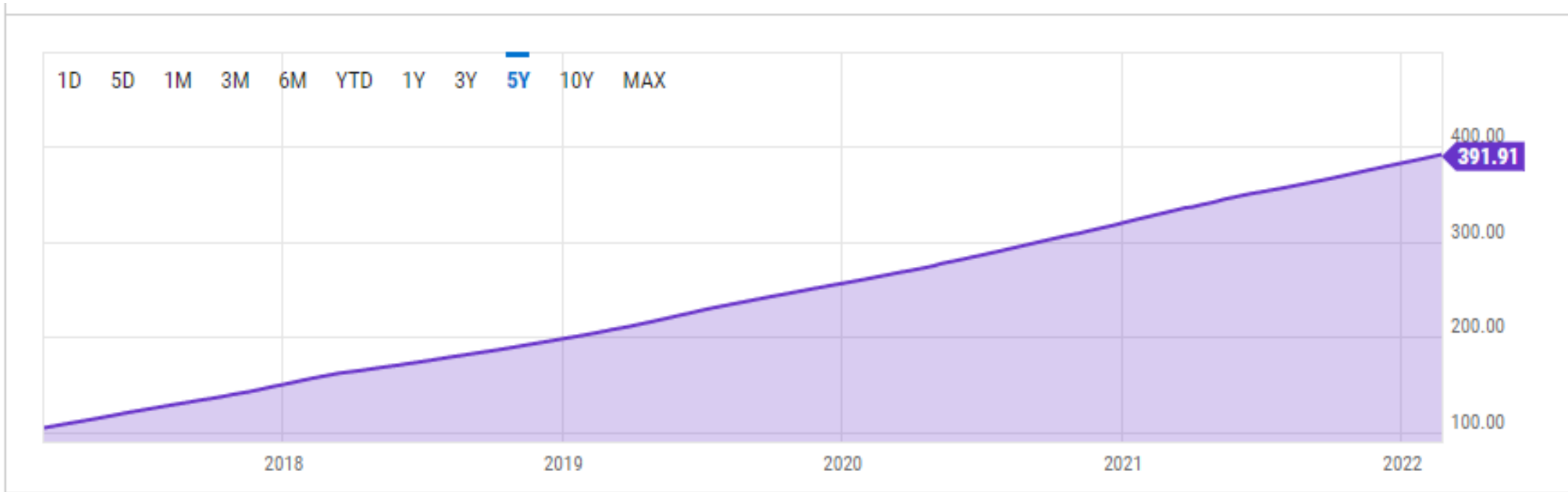


Storage costs (in 2018)



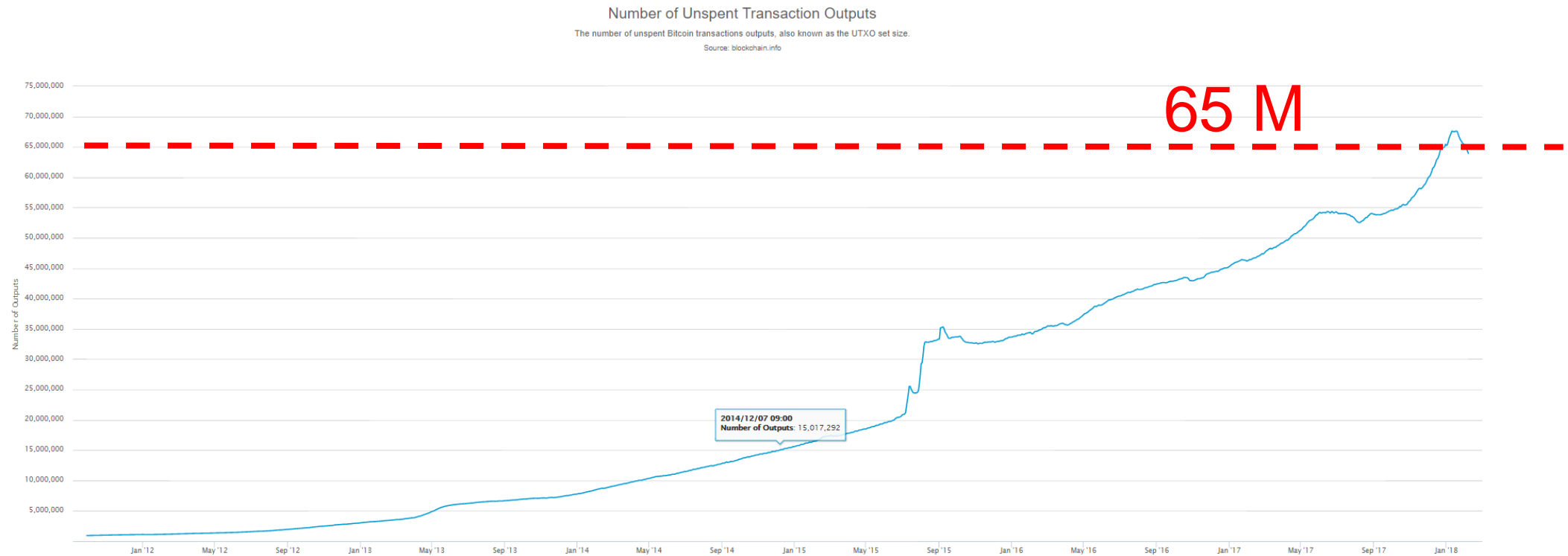
Source: blockchain.info

Storage costs (in 2022)



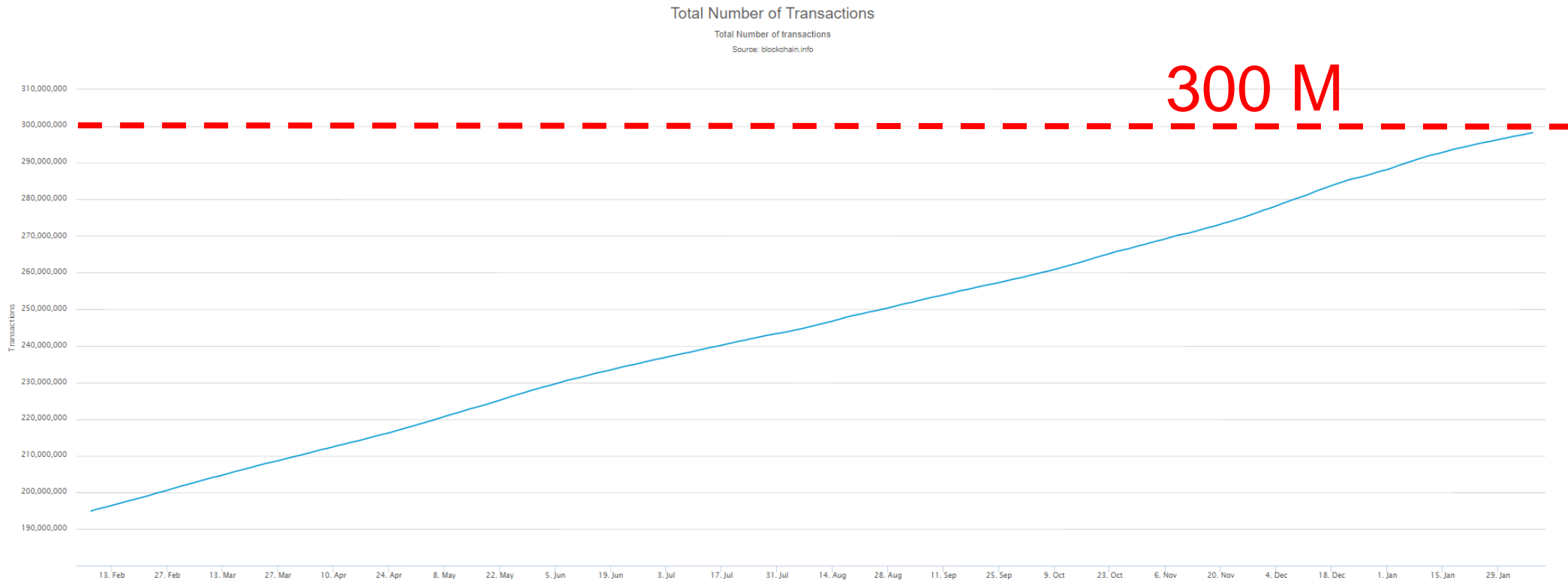
Tracking the UTXO set

- **U**nspent **T**ransaction **O**utput
 - Should be stored in memory - everything else can be stored on disk, why?



Tracking the UTXO set

- Currently ~65 M UTXOs
 - Out of 300 M transactions
- Can require several Gigabytes to store – can it fit in the RAM of a standard computer?



Thin/SPV clients (not fully-validating)

SPV – Simplified Payment Verification (e.g., Wallet nodes)

Idea: Don't store everything

- Store block headers – verify the puzzle was solved correctly, but cannot verify every transaction in each block!
- Validate only those transactions that affect them → By requesting transactions as needed
 - To verify incoming payment
 - Trust fully-validating nodes

1000x cost savings! Requires only a few tens of Megabytes (compare to tens of Gigabytes needed for fully validating nodes)

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”

Limitations & Improvements

Hard-coded limits in Bitcoin

- 10 min. average creation time per block
- 1 M bytes in a block
- 20,000 signature operations per block
- 100 M *satoshis* per bitcoin
- 23M total bitcoins maximum
- 50,25,12.5... bitcoin mining reward

These affect
economic
balance of
power too
much to
change now

Throughput limits in Bitcoin

- 1 M bytes/block (10 min)
- >250 bytes/transaction
- 7 transactions/sec 😞

Compare to:

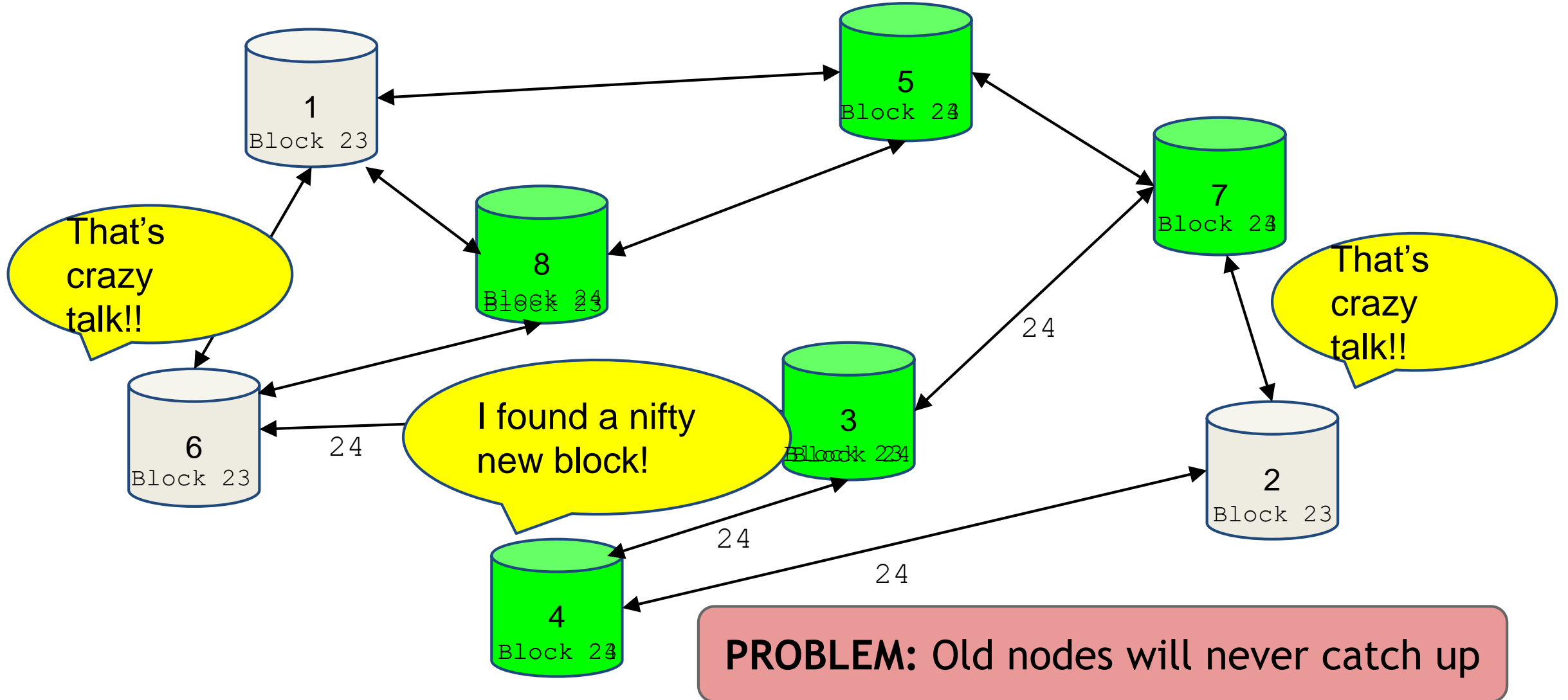
- VISA: 2,000-10,000 transactions/sec
- PayPal: 50-100 transaction/sec

Cryptographic limits in Bitcoin

- Only 1 signature algorithm (ECDSA/P256)
- Hard-coded hash functions

Crypto primitives might break by 2040...

“Hard-forking” changes to Bitcoin



Soft forks

Observation: we can add new features which only *limit* the set of valid transactions

Need majority of nodes to enforce new rules

Old nodes will approve

RISK: Old nodes might mine now-invalid blocks

Soft fork example: pay to script hash

<Redeem Script> 2 PubKey1 PubKey2 PubKey3 PubKey4 PubKey5 CHECKMULTISIG

Old nodes <Redeem Script> OP_HASH160 <hash of redemption script> EQUAL

New Nodes <Redeem Script> OP_HASH160 <hash of redemption script> EQUAL

2 PubKey1 PubKey2 PubKey3 PubKey4 PubKey5 CHECKMULTISIG

} Two executions

Old nodes will just approve the hash, not run the embedded script

Soft fork possibilities

- New signature schemes
- Extra per-block metadata
 - Shove in the coinbase parameter
 - Commit to UTXO tree in each block

Hard forks

- New op codes
- Changes to size limits
- Changes to mining rate
- Many small bug fixes

Currently seem very unlikely to happen

Stay tuned for the lecture on altcoins!