Blockchains & Cryptocurrencies

Bitcoin Mechanics - II

Instructor: Abhishek Jain
Johns Hopkins University - Spring 2021

*Many slides based on NBFMG

Housekeeping

- Initial list of ideas for course projects added on course website
- Some are cryptography heavy, others less so
- Will be adding more through the week
- You can choose other topics
- Feel free to ask for opinion

Last Week

- PoW puzzles and Bitcoin Consensus
- Bitcoin Transaction Format and Simple Smart-Contracts

Today

- Bitcoin Transaction Format (Contd.)
- Bitcoin Network
- Soft/Hard forks
- Key management
- Mining (maybe…)

Along the way, start identifying directions for improvements (or, motivation for altcoins)

Bitcoin blocks

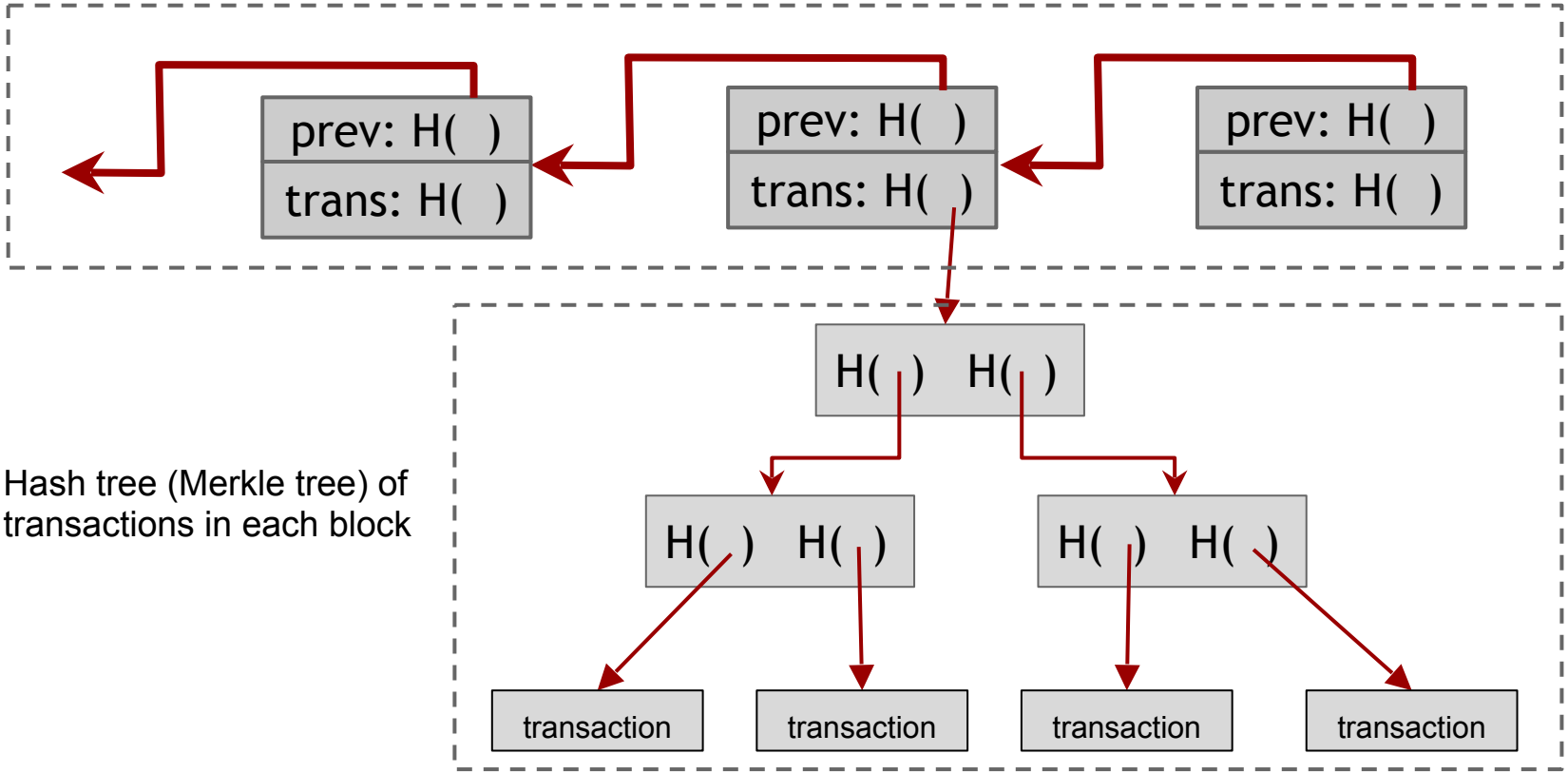
Bitcoin blocks

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

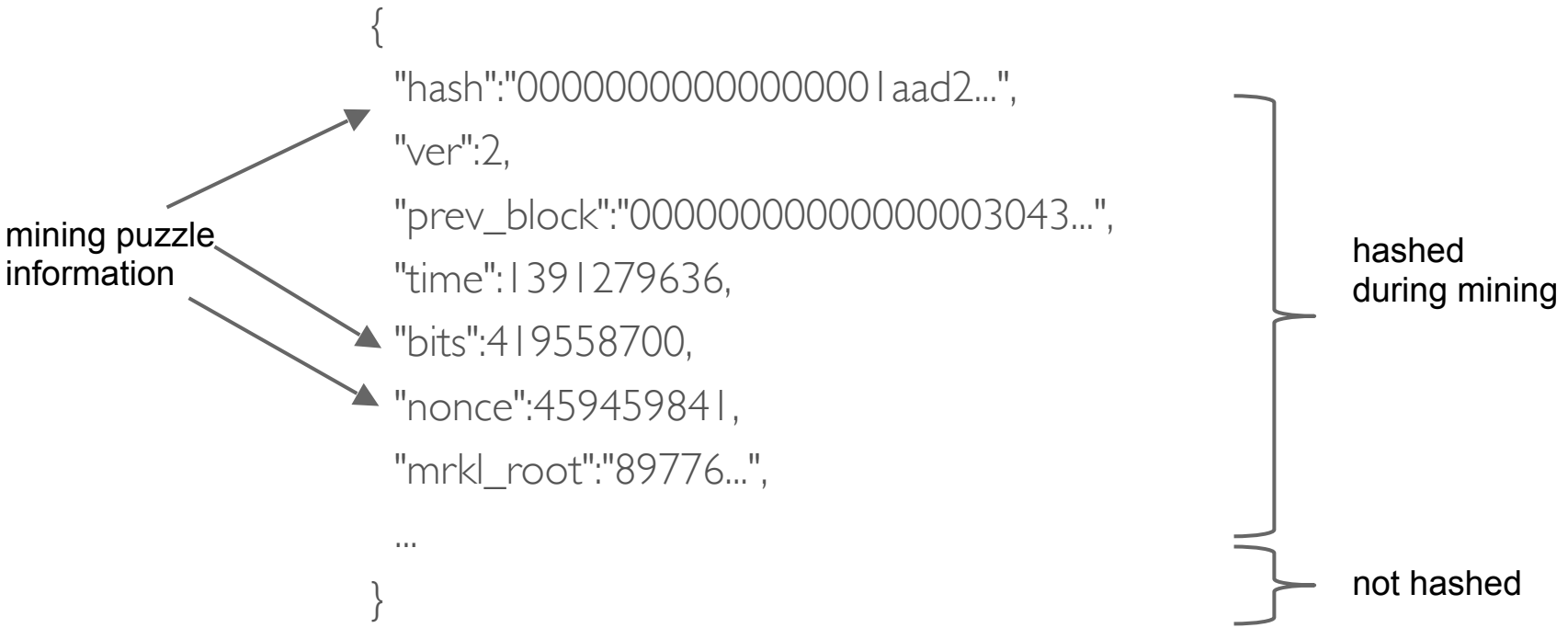
The real deal: a classical Bitcoin block

block header

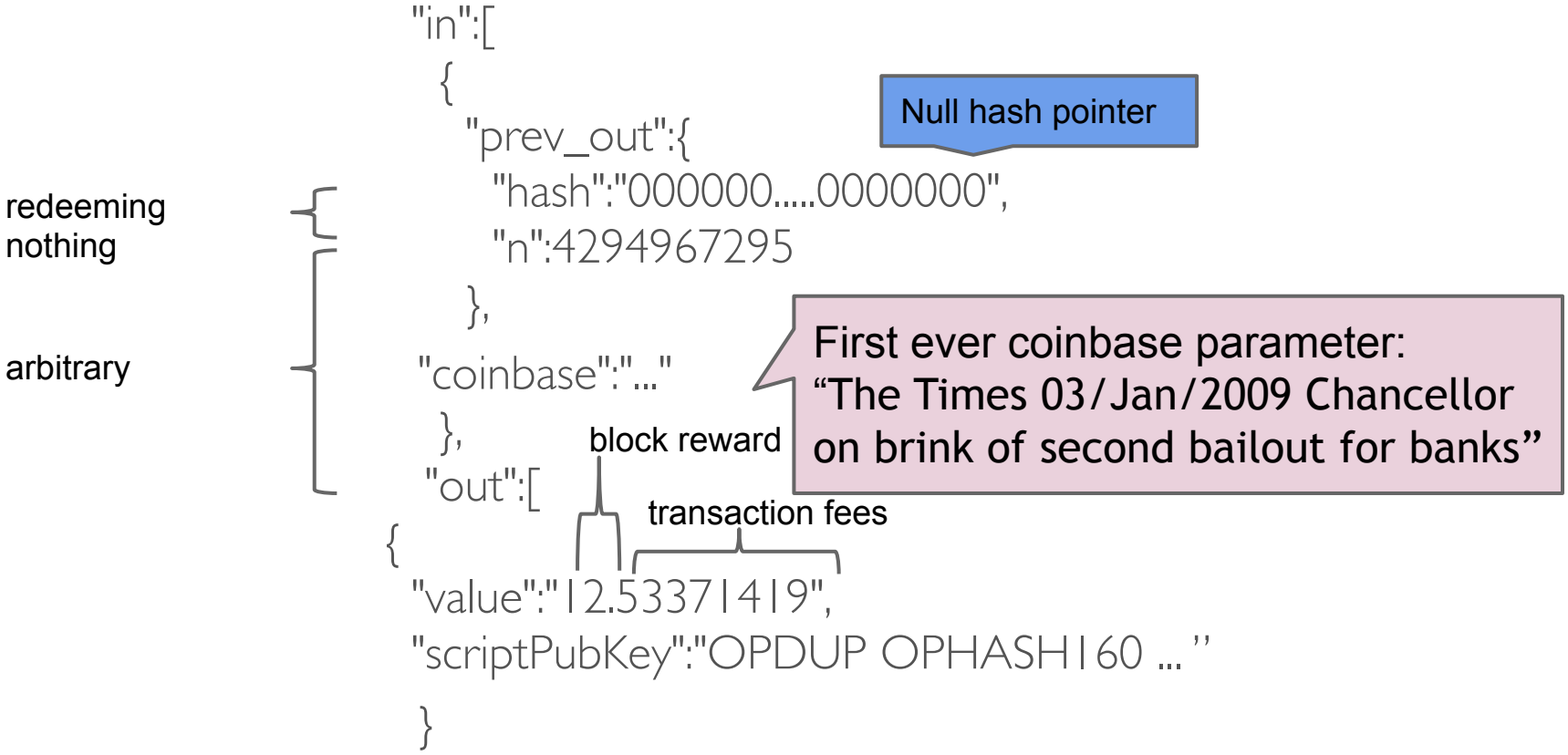
transaction data


```
{
  "hash":"0000000000000000001aad2...",
  "ver":2,
  "prev_block":"0000000000000000003043...",
  "time":1391279636,
  "bits":419558700,
  "nonce":459459841,
  "mrkl_root":"89776...",
  "n_tx":354,
  "size":181520,
  "tx":[
    ...
  ],
  "mrkl_tree":[
    "6bd5eb25...",
    ...
    "89776cdb..."
  ]
}
```

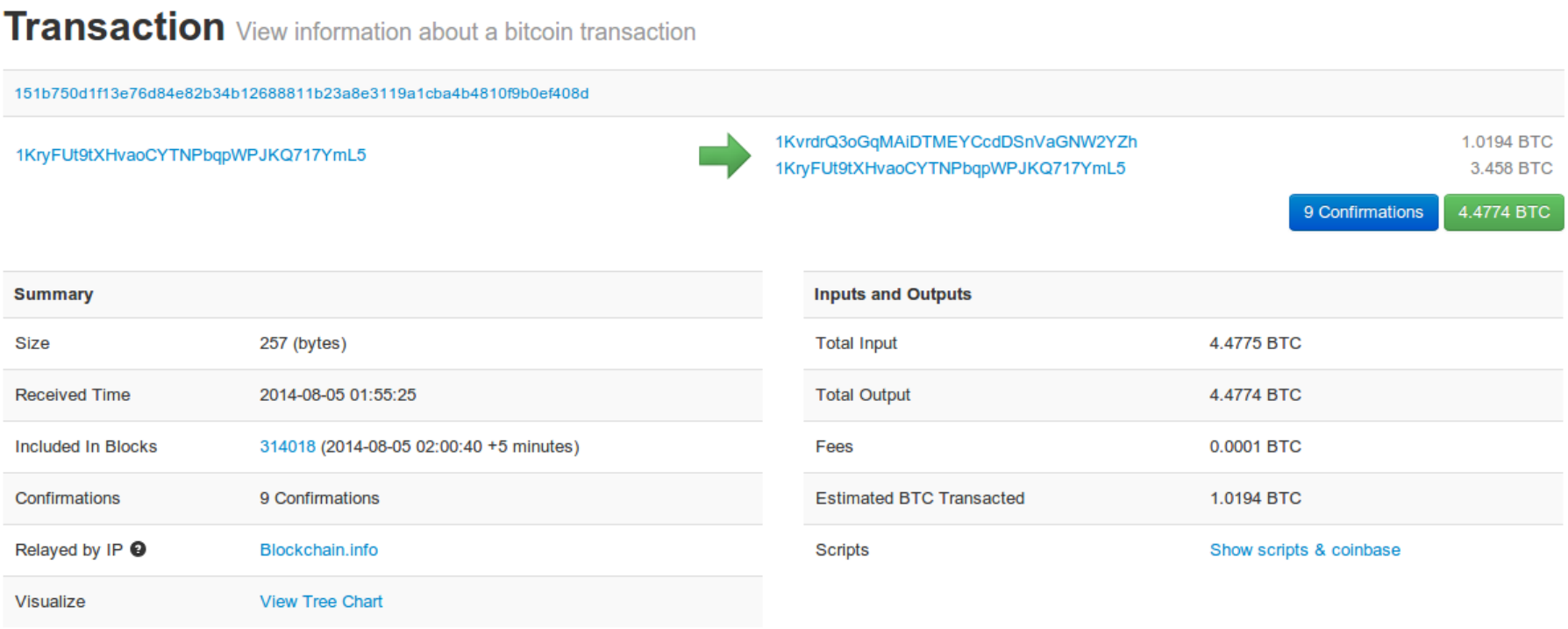
The real deal: block header



The real deal: coinbase transaction



See for yourself!



Transaction View information about a bitcoin transaction

151b750d1f13e76d84e82b34b12688811b23a8e3119a1cba4b4810f9b0ef408d

1KryFUt9tXHvaoCYTNPbqpWPJKQ717YmL5

1KvrdrQ3oGqMAiDTMEYCcdDSnVaGNW2YZh 1.0194 BTC
1KryFUt9tXHvaoCYTNPbqpWPJKQ717YmL5 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

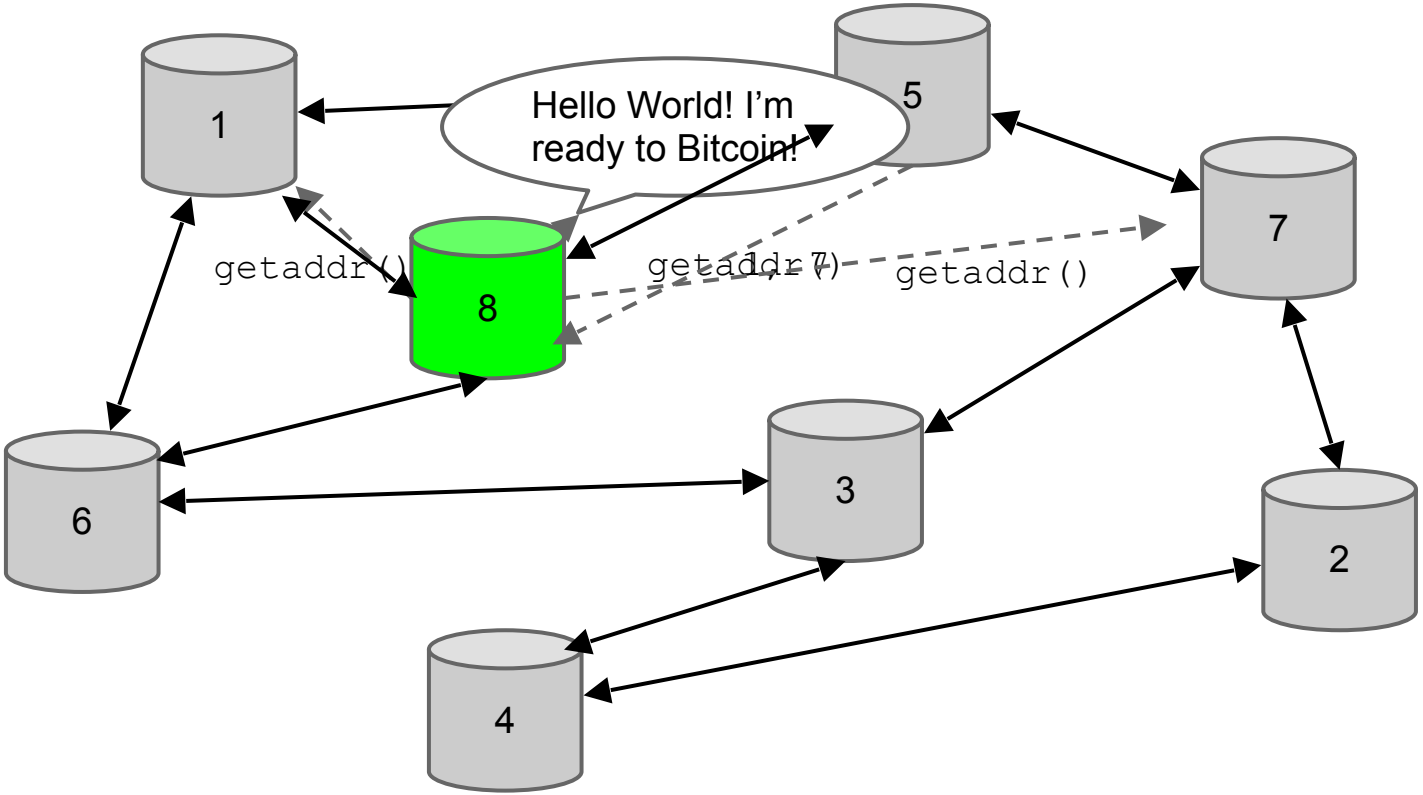
blockchain.info (and many other sites)

The Bitcoin network

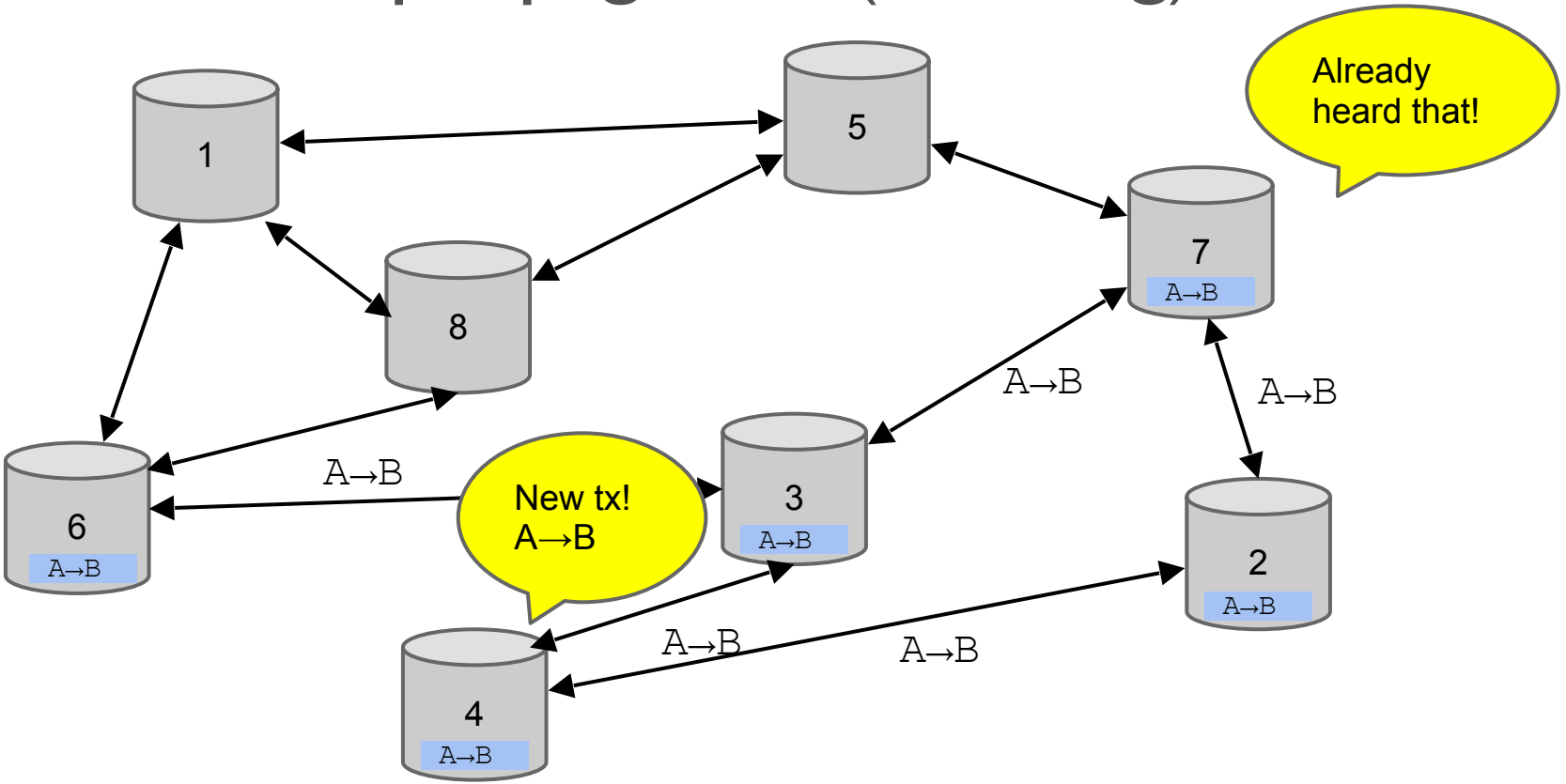
Bitcoin P2P network

- 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

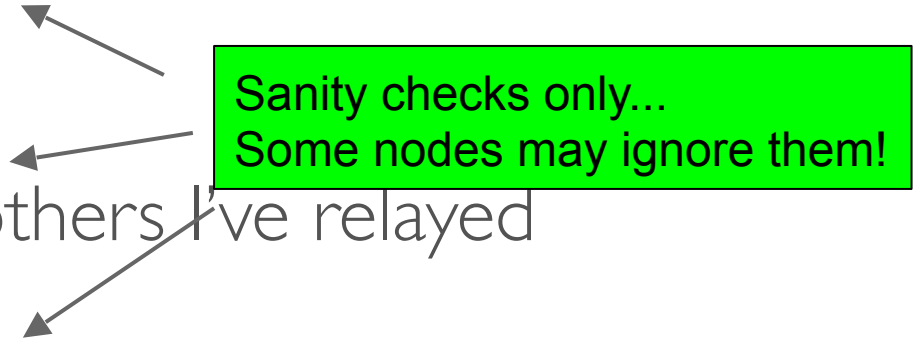


Transaction propagation (flooding)

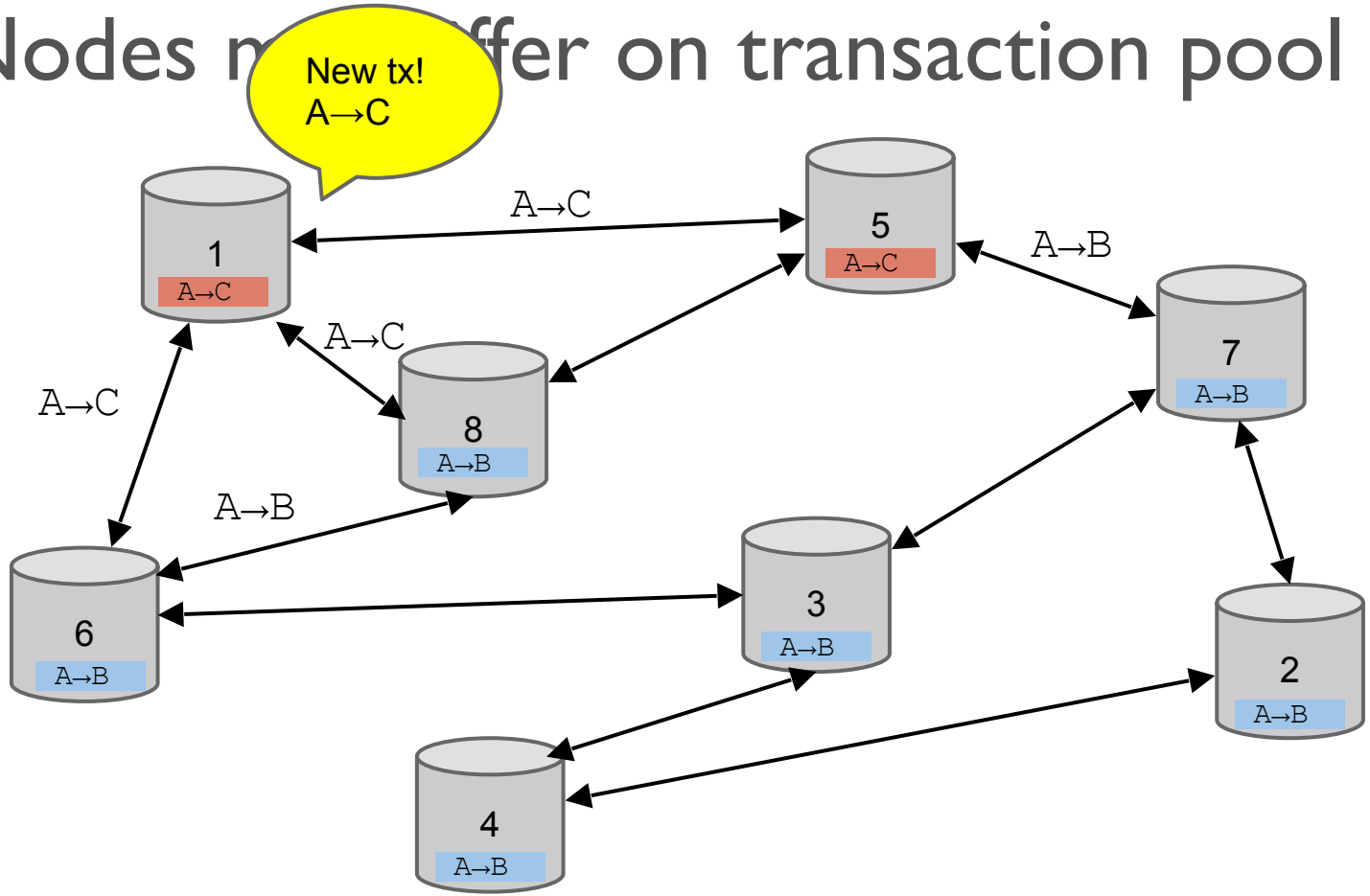


Should I relay a proposed transaction?

- Transaction valid with current block chain
- (default) 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



Nodes m ffer on transaction pool



Race conditions

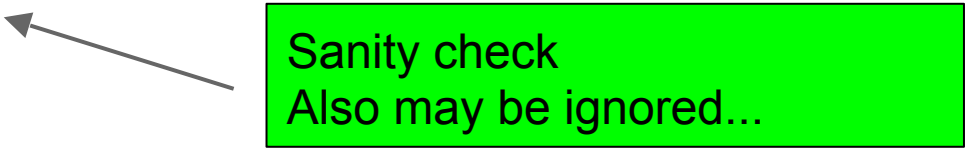
Transactions or blocks may ***conflict***

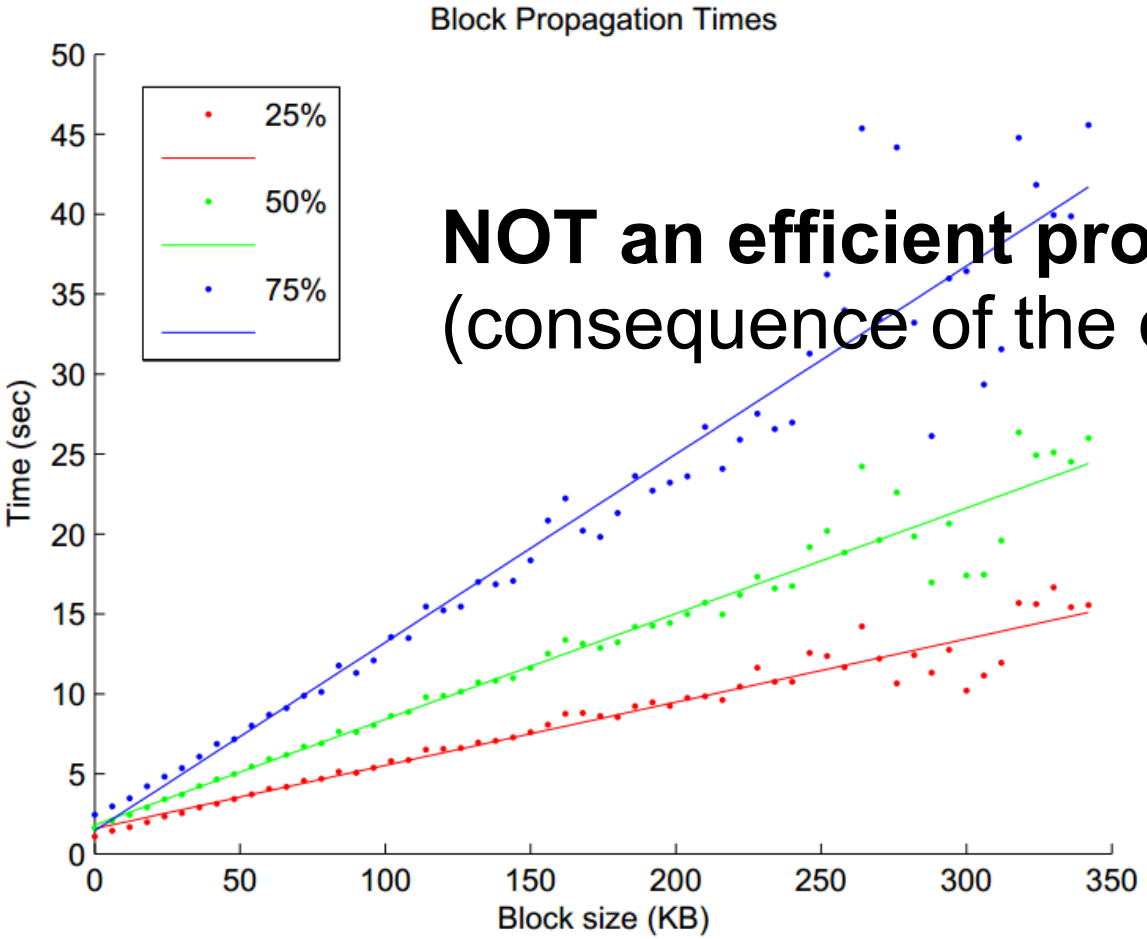
- Default behavior: accept what you hear first
- Network position matters
- Miners may implement other logic!

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





NOT an efficient protocol
(consequence of the design)

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

How big is the network?

- Unclear how 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!

*(old numbers, might be outdated)

Fully-validating nodes

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

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

Hard-coded limits in Bitcoin

- 10 min. average creation time per block
- 1 M bytes in a block
- 20,000 signature operations per block
- 23M total bitcoins maximum
- 50,25,12.5,6.25… 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 tran

Improving throughput:
strong motivation for Altcoins

Compare

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

Cryptographic limits in Bitcoin

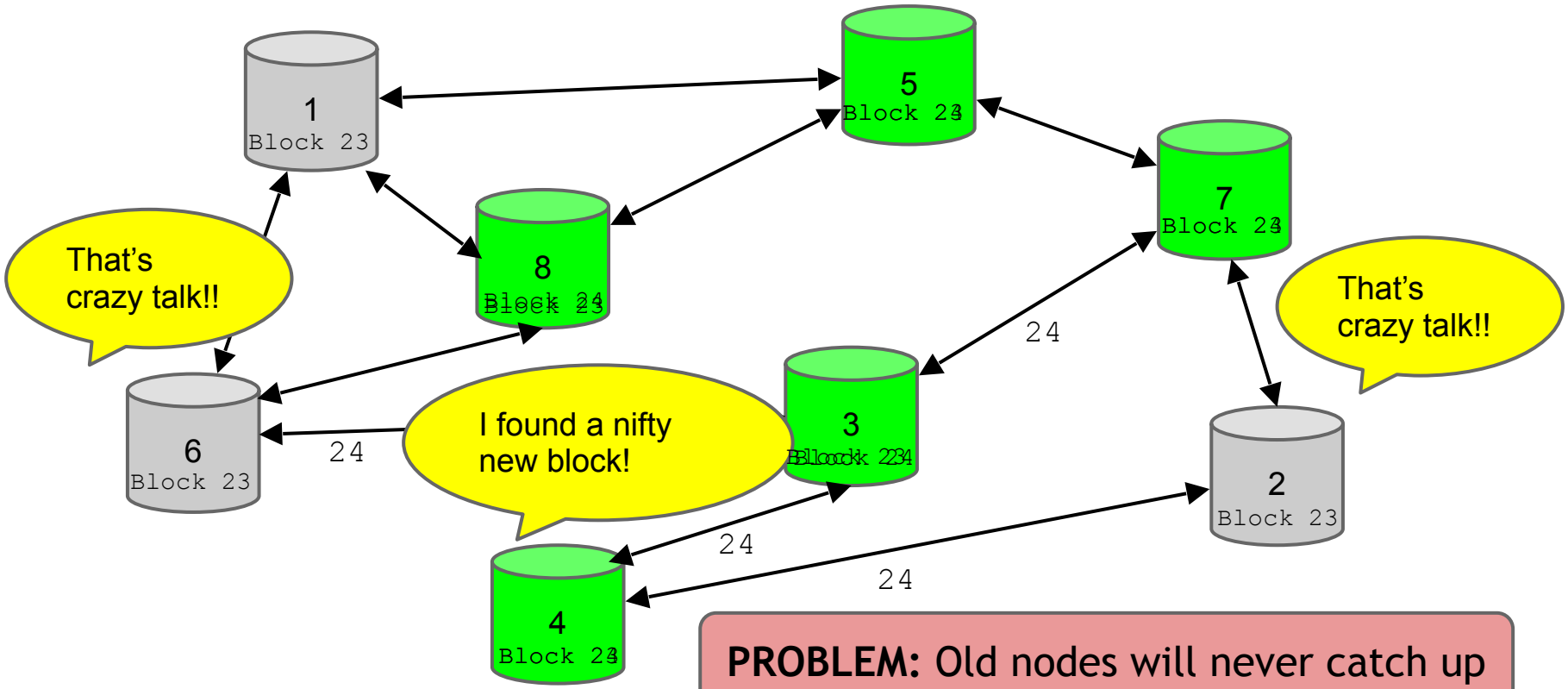
- Only 1 signature algorithm (ECDSA/P256)
- Hard-coded hash functions

Some of these crypto primitives used here might break by 2040 (e.g., collision-found in hash function, or powerful quantum computer breaks ECDSA)...

Why not update Bitcoin software to overcome these limitations?

- Many of these changes require "hard forks", which are currently considered unacceptable

“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

<signature>
<<pubkey> OP_CHECKSIG>

OP_HASH160
<hash of redemption script>
OP_EQUAL

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 unspent transaction tree in each block

Hard forks

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

Currently seem unlikely to happen

Many of these issues addressed by Altcoins

Key Management

To spend a Bitcoin, you need to know:

* some info from the public blockchain, and
* the owner's secret signing key

So it's all about key management.

Goals (for Bitcoin Key management)

availability: You can spend your coins.

security: Nobody else can spend your coins.

convenience

Simplest approach: store key in a file,
on your computer or phone

- Very convenient
- As available as your device.
  - device lost/wiped ⇒ key lost ⇒ coins lost
- As secure as your device
  - device compromised ⇒ key leaked ⇒ coins stolen

Wallet software

Keeps track of your coins, provides nice user interface.

Nice trick: use a separate address/key for each coin.

- benefits privacy (looks like separate owners)
- wallet can do the bookkeeping, user needn't know

Encoding addresses

Encode as text string: base58 notation

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz

or use QR code

Hot storage

online

convenient but risky

Cold storage

offline

archival but safer

separate keys

Hot storage

online

Cold storage

offline

hot secret key(s)

cold address(es)

payments

cold secret key(s)

hot address(es)

Secret sharing [Shamir]

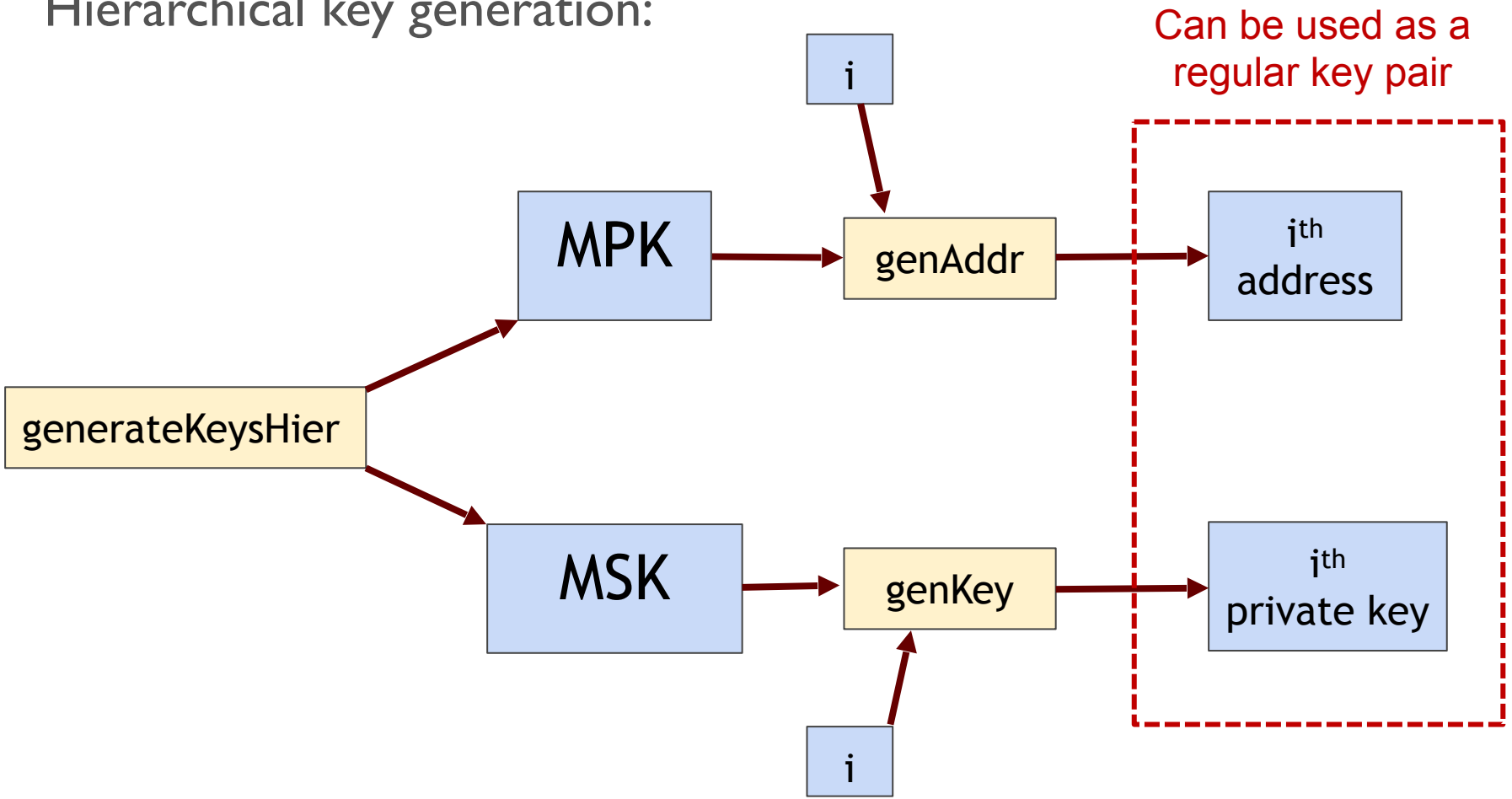
- **Share(S):** Output a tuple $S_1,\ldots,S_n$
- **Reconstruct($x_1,\ldots,x_k$):** Output a value S*

k-Privacy: For any (S,S'), and any subset X of < k indices, the following two distributions are statistically close:

$$\{(S_1,\ldots,S_n) \leftarrow Share(S) : (S_i | i \in X)\},$$

$$\{(S'_1,\ldots,S'_n) \leftarrow Share(S') : (S'_i | i \in X)\}.$$

Hierarchical key generation:



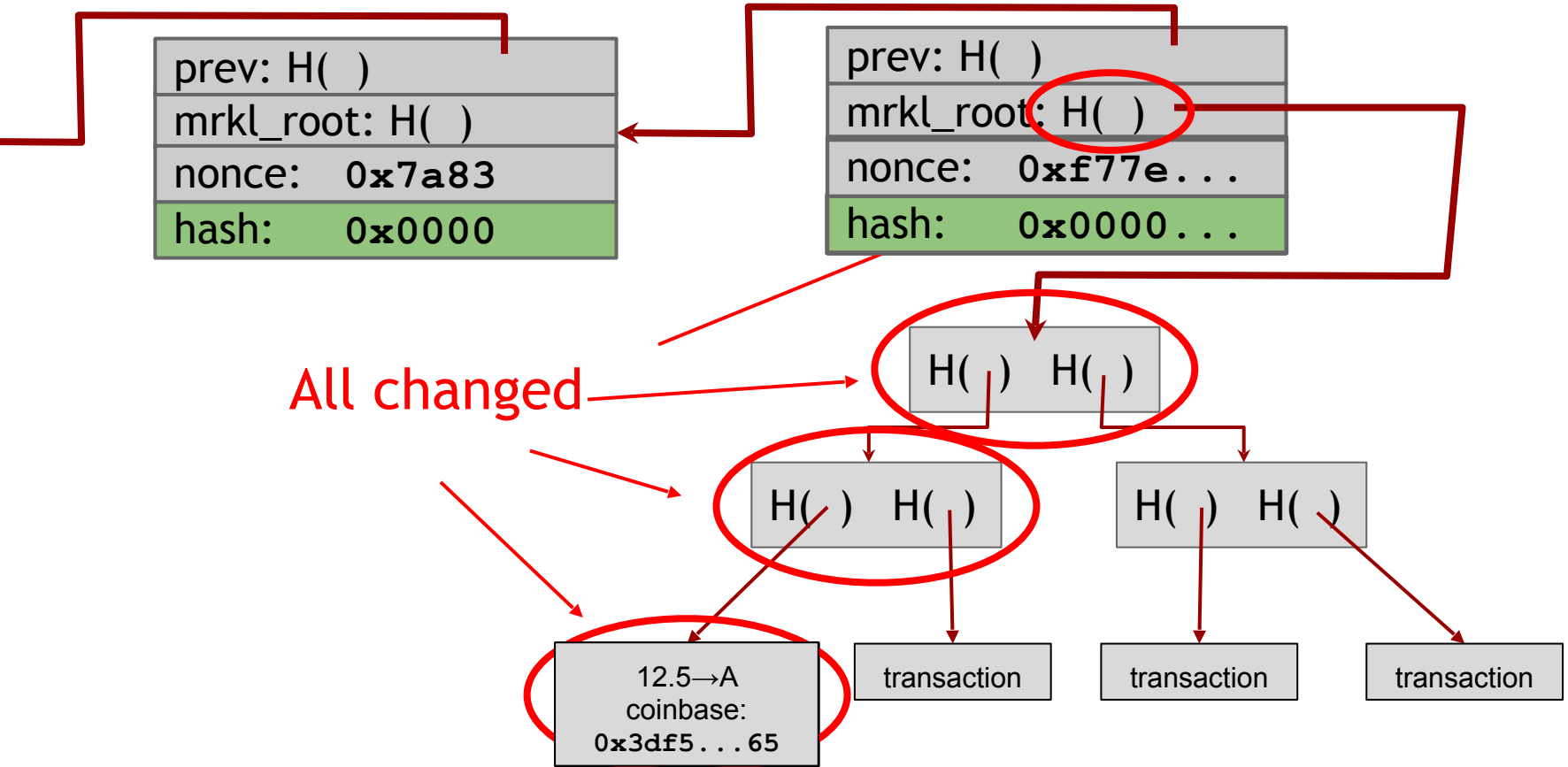
Bitcoin Mining

Mining Bitcoins in 6 easy steps

1. Join the network, listen for transactions
    a. Validate all proposed transactions
2. Listen for new blocks, maintain block chain
    a. When a new block is proposed, validate it
3. Assemble a new valid block
4. Find the nonce to make your block valid
5. Hope everybody accepts your new block
6. Money!

Useful to Bitcoin network

Finding a valid block



CPU mining (numbers from 2014)

```
while (1){
    HDR[kNoncePos]++;
    IF (SHA256(SHA256(HDR)) < (65535 << 208)/ DIFFICULTY)
        return;
}
```

Throughput on a high-end PC = 10-20 MHz ≈ 2^{24}

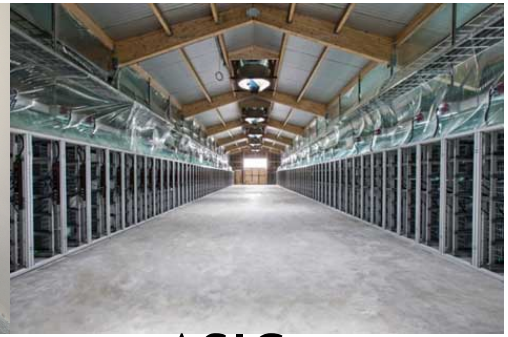
139,461 years to find a block!

Evolution of mining

CPU

GPU

FPGA



ASIC

Huge energy consumption (in 2017, annual rate nearly as high as Denmark)!

The future

- Can small miners stay in the game?
- Would we be better off without ASICs?
- Should we implement consensus without proofs of work?

Motivation for Altcoins

Mining pools

Economics of being a small miner

- In 2014, expected revenue: ≈$1,000/month
- High probability (~50%) of not mining a block within a year

Mining pools

- **Goal:** pool participants all attempt to mine a block with the same coinbase recipient
  - send money to key owned by pool manager
- Distribute revenues to members based on how much work they have performed
  - minus a cut for pool manager

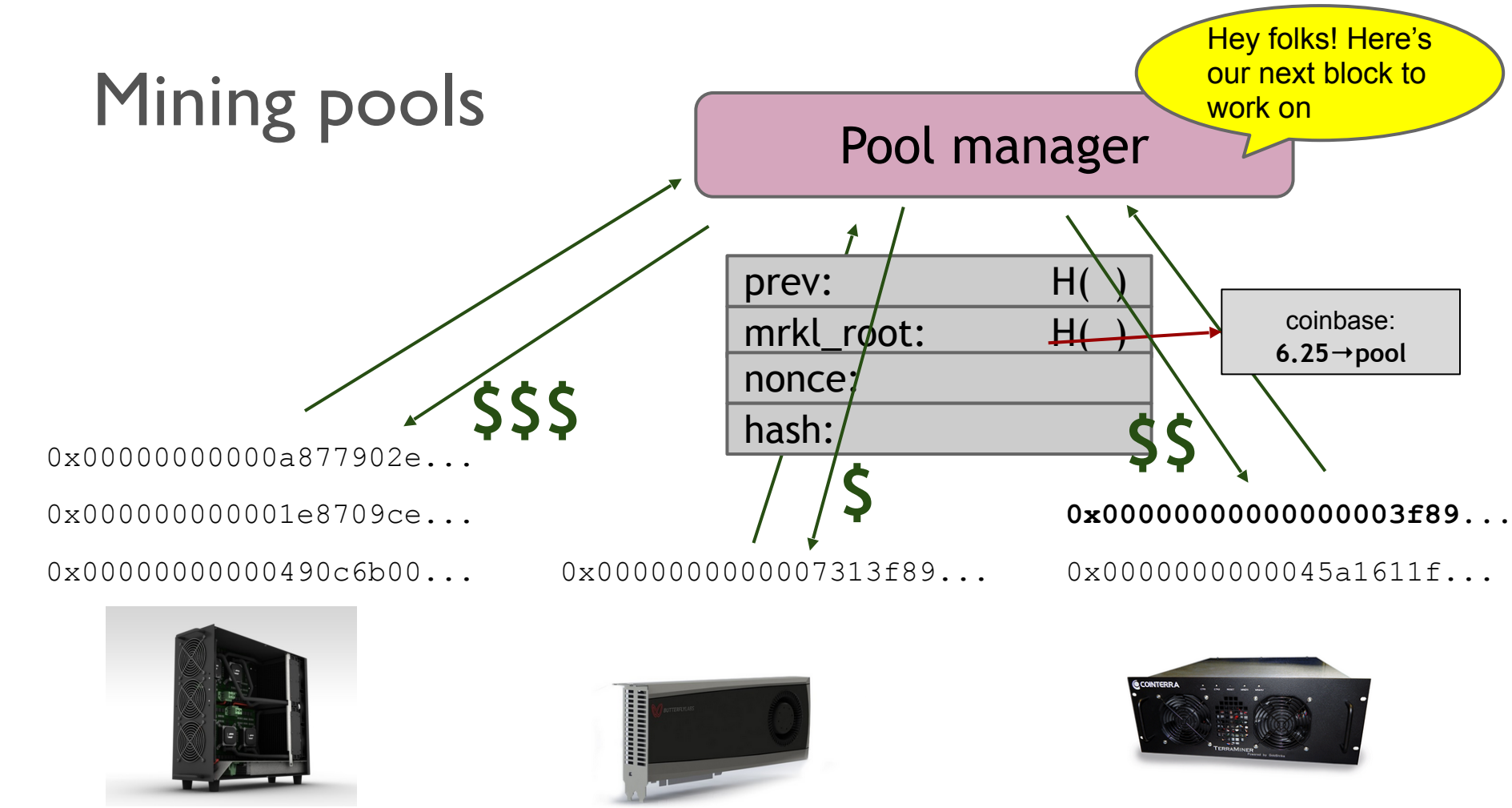
How do we know how much work members perform?

Mining shares

Idea: prove work with "near-valid blocks" (shares)

```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
00000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
0090488133779E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
0000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E777613845618 1FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
000000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

Mining pools



Mining pool history

- First pools appear in late-2010
  - Back in the GPU era!
- By 2014: around 90% of mining pool-based
- June 2014: GHash.io exceeds 50% (!)

Are mining pools a good thing?

- Pros
  - Make mining more predictable
  - Allow small miners to participate
  - More miners using updated validation software
- Cons
  - Lead to centralization
  - Discourage miners from running full nodes

Question: Can we prevent pools?