

A close-up photograph of a white boat's hull and anchor chain against a dark blue sea. The boat's hull is white with some weathering and a metal plate. A thick, rusty anchor chain is attached to the hull. The water is a deep, dark blue.

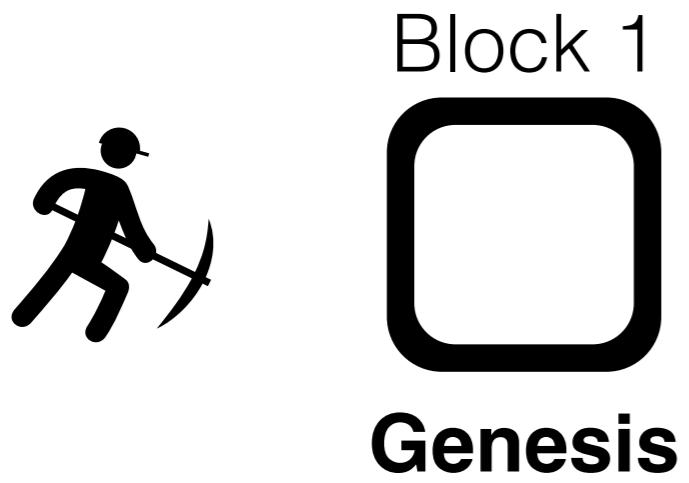
**Mining
Proof of Work**

How to mine

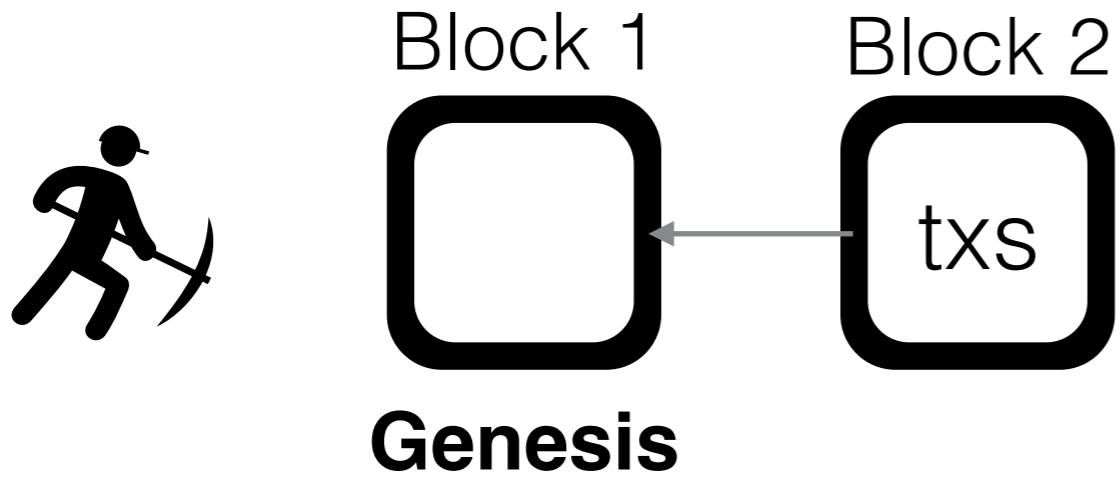


1. Join the P2P network, listen for transactions, validate all incoming transactions
2. Listen for new blocks, build on valid blocks
3. Construct a block template
4. Find a nonce that validates the new block
5. Tell all the other miners
6. Receive reward

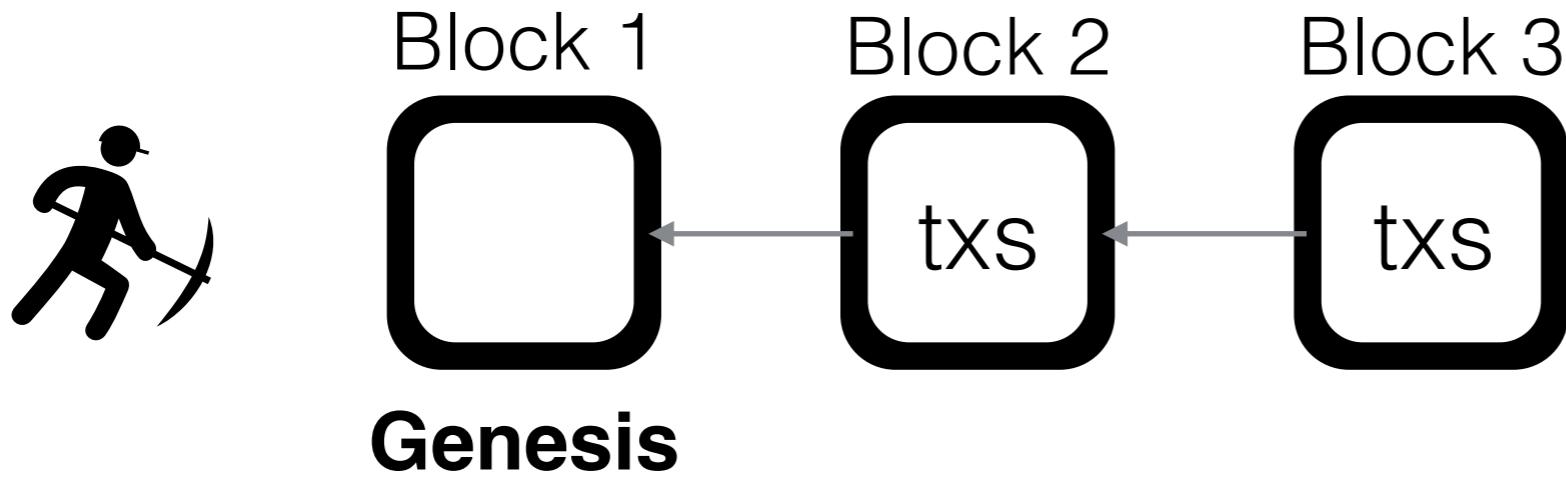
Blockchain



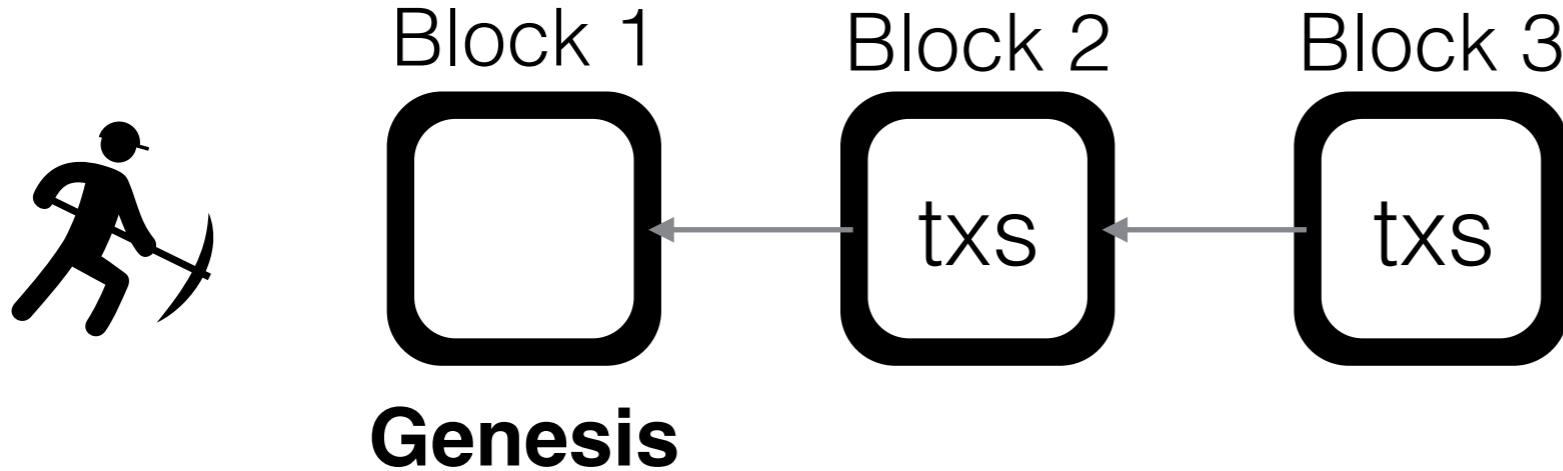
Blockchain



Blockchain



Blockchain

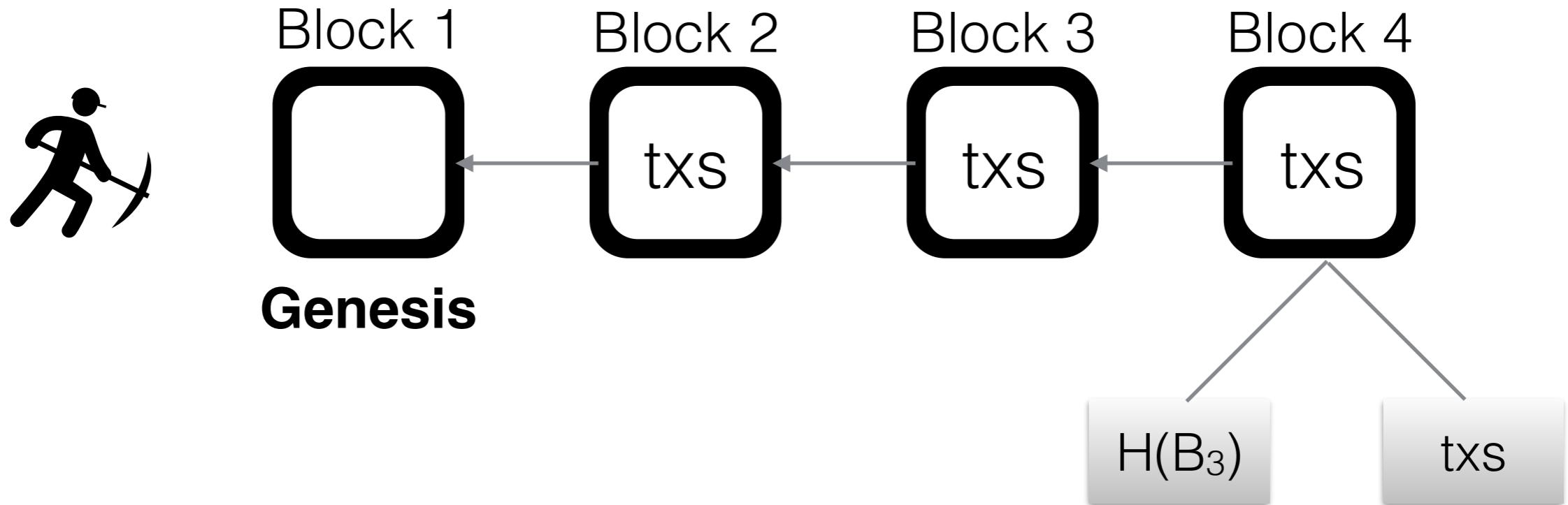


Mining

- Find Nonce N, s.t.

$$\text{Hash}(\text{Hash}(B_3)|\text{txs}|N) < \text{target}$$

Blockchain

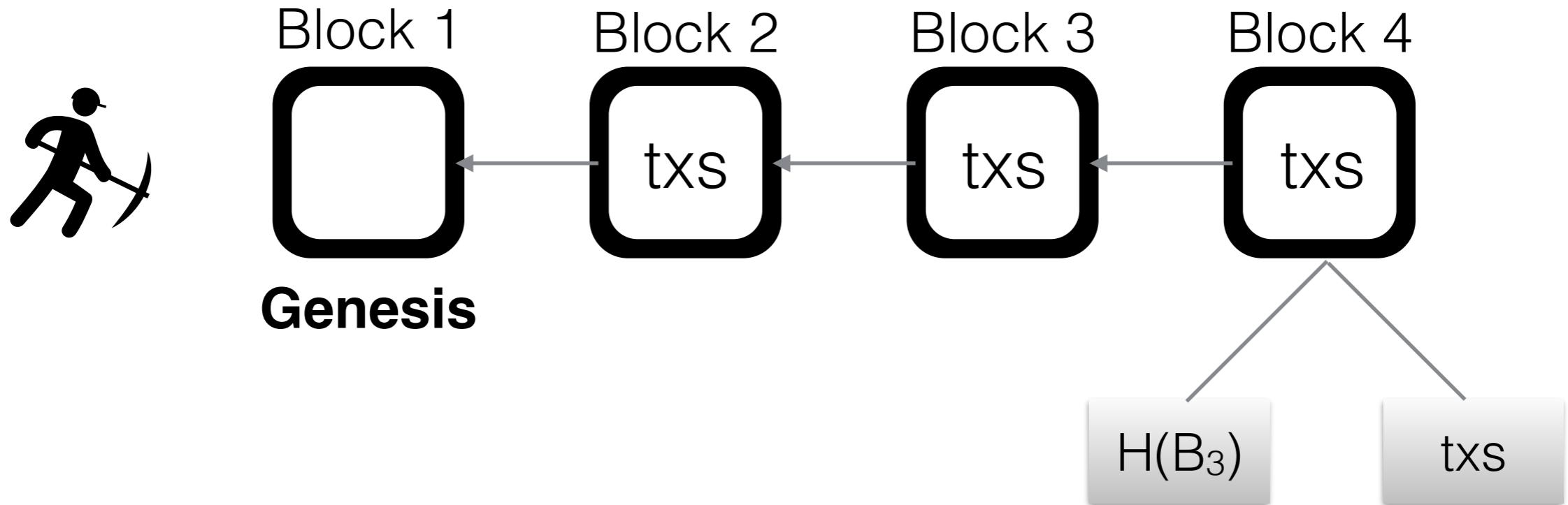


Mining

- Find Nonce N, s.t.

$$\text{Hash}(\text{Hash}(B_3)|\text{txs}|N) < \text{target}$$

Blockchain



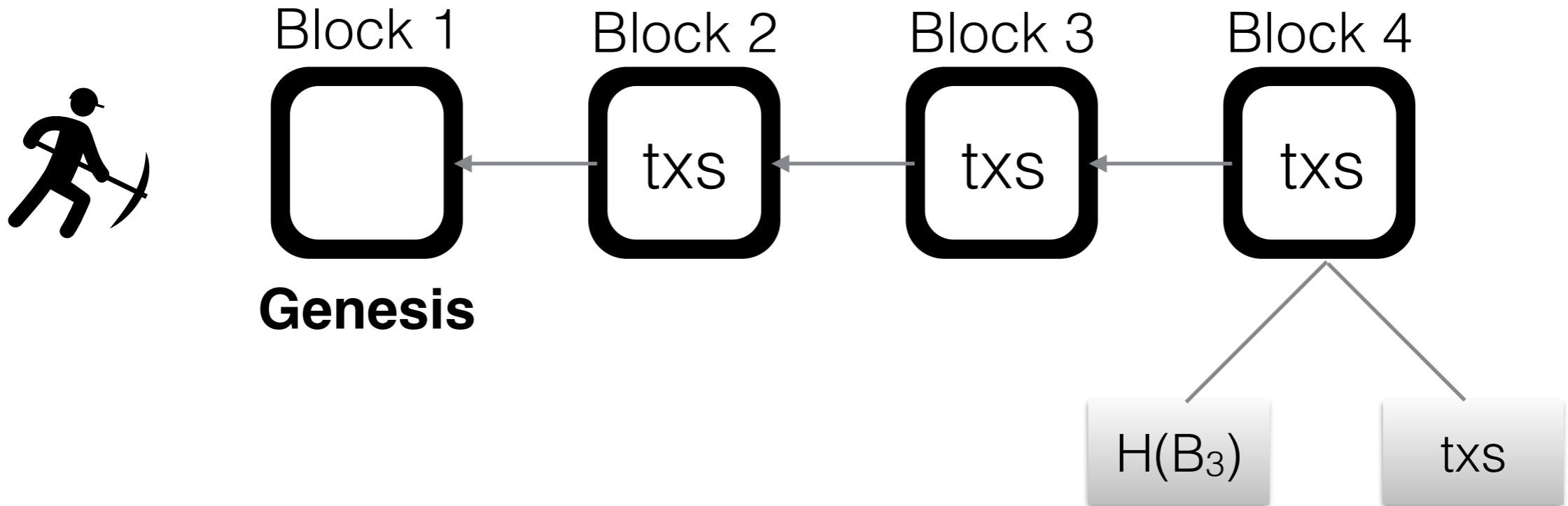
Mining

- Find Nonce N, s.t.

$$\text{Hash}(\text{Hash}(B_3)|\text{txs}|N) < \text{target}$$

Best known
approach: **Brute Force**

Blockchain



Mining

- Find Nonce N, s.t.

$$\text{Hash}(\text{Hash}(B_3)|\text{txs}|N) < \text{target}$$

Best known approach: **Brute Force**

Controls the **difficult**

Mining Difficulty

Mining Difficulty

$\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < \text{target} = 0x000^{**}$

Mining Difficulty

$\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < \text{target} = 0x000^{**}$

$\text{Hash}(\text{Block_3} | \text{merkle_root} | 0xbeed) = 0x03ef..$

Mining Difficulty

$\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < \text{target} = 0x000^{**}$

~~- $\text{Hash}(\text{Block_3} | \text{merkle_root} | 0xbeed) = 0x03ef..$~~

Mining Difficulty

$\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < \text{target} = 0x000^{**}$

~~$\text{Hash}(\text{Block_3} | \text{merkle_root} | 0xbeed) = 0x03ef..$~~

$\text{Hash}(\text{Block_3} | \text{merkle_root} | 0xbeee) = 0x12ef..$

Mining Difficulty

$\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < \text{target} = 0x000^{**}$

~~$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeed) = 0x03ef..$~~

~~$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeee) = 0x12ef..$~~

Mining Difficulty

$\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < \text{target} = 0x000^{**}$

~~$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeed) = 0x03ef..$~~

~~$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeee) = 0x12ef..$~~

$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeef) = 0x000f..$

Mining Difficulty

$\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < \text{target} = 0x000^{**}$

~~$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeed) = 0x03ef..$~~

~~$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeee) = 0x12ef..$~~

$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeef) = 0x000f..$



Mining Difficulty

$\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < \text{target} = 0x000^{**}$

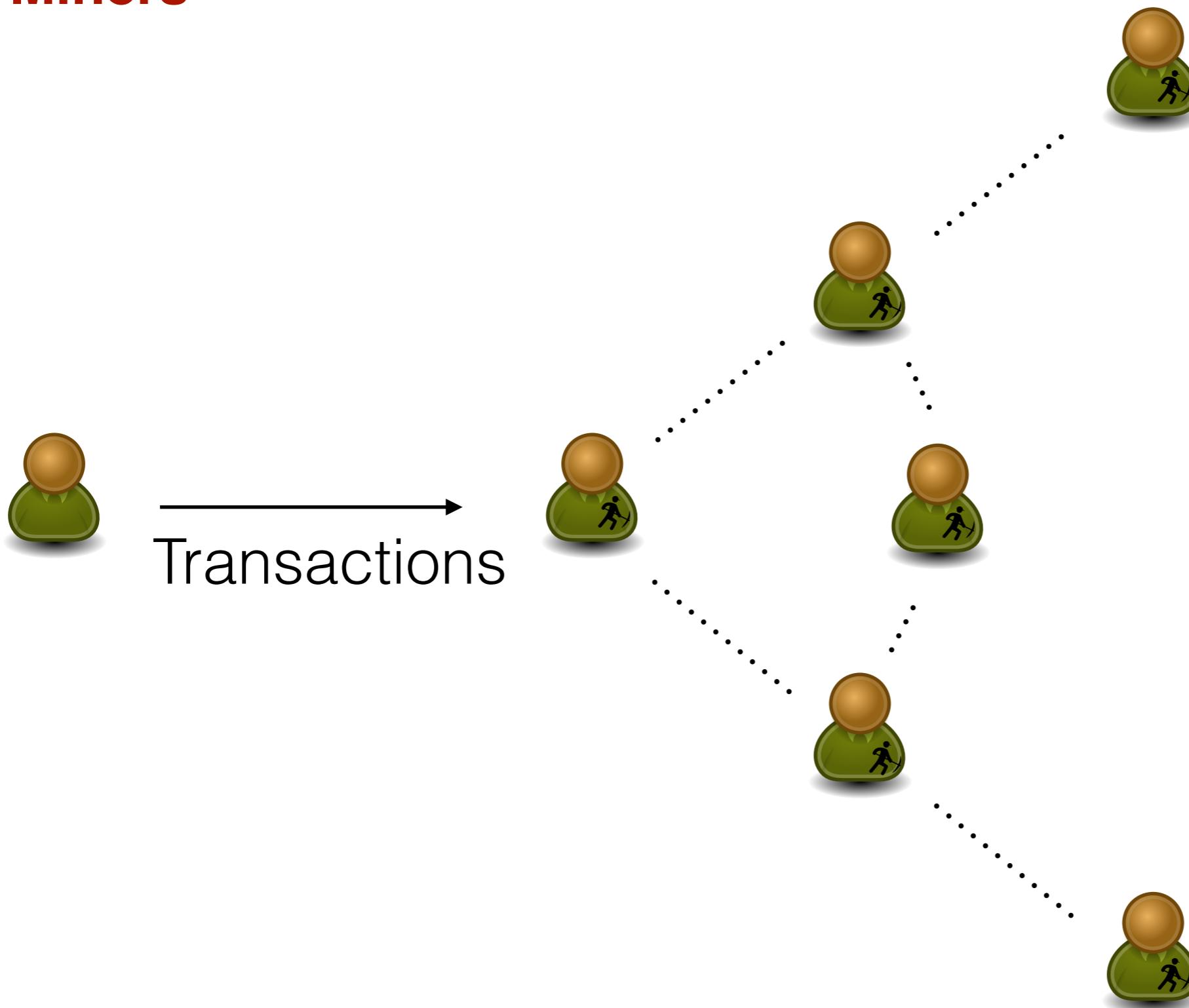
~~$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeed) = 0x03ef..$~~

~~$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeee) = 0x12ef..$~~

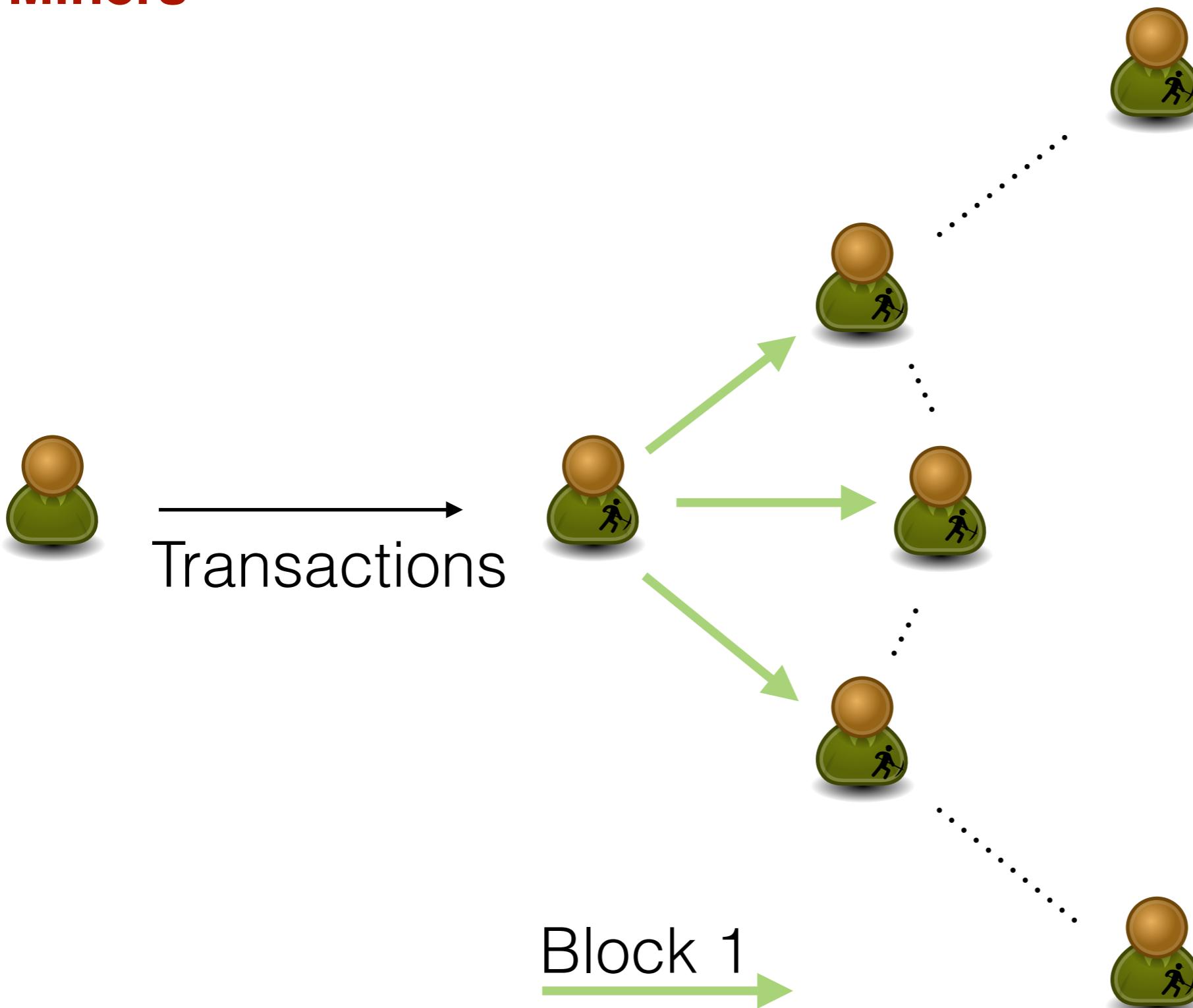
$\text{Hash}(\text{Block}_3 | \text{merkle_root} | 0xbeef) = 0x000f..$



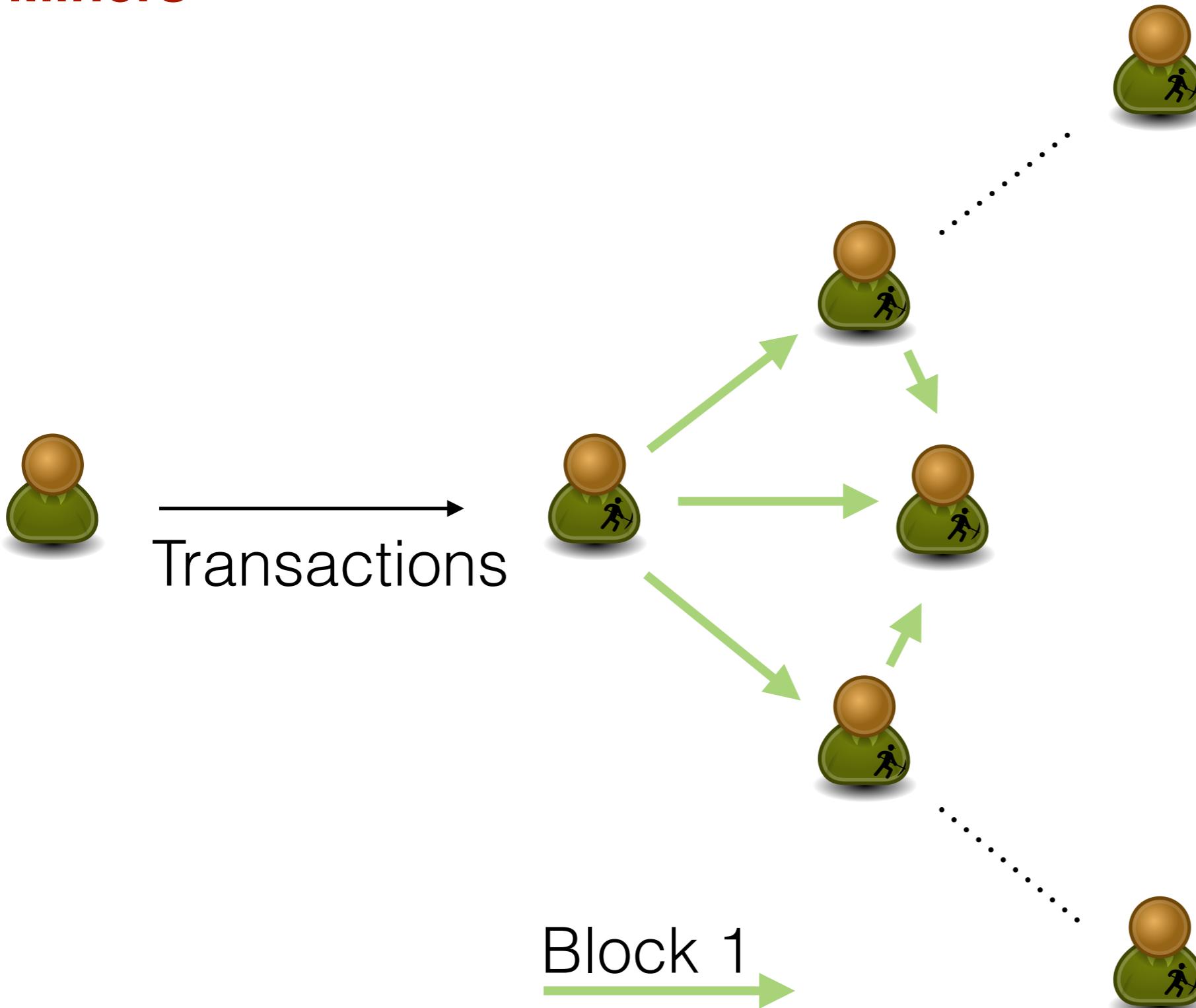
Miners



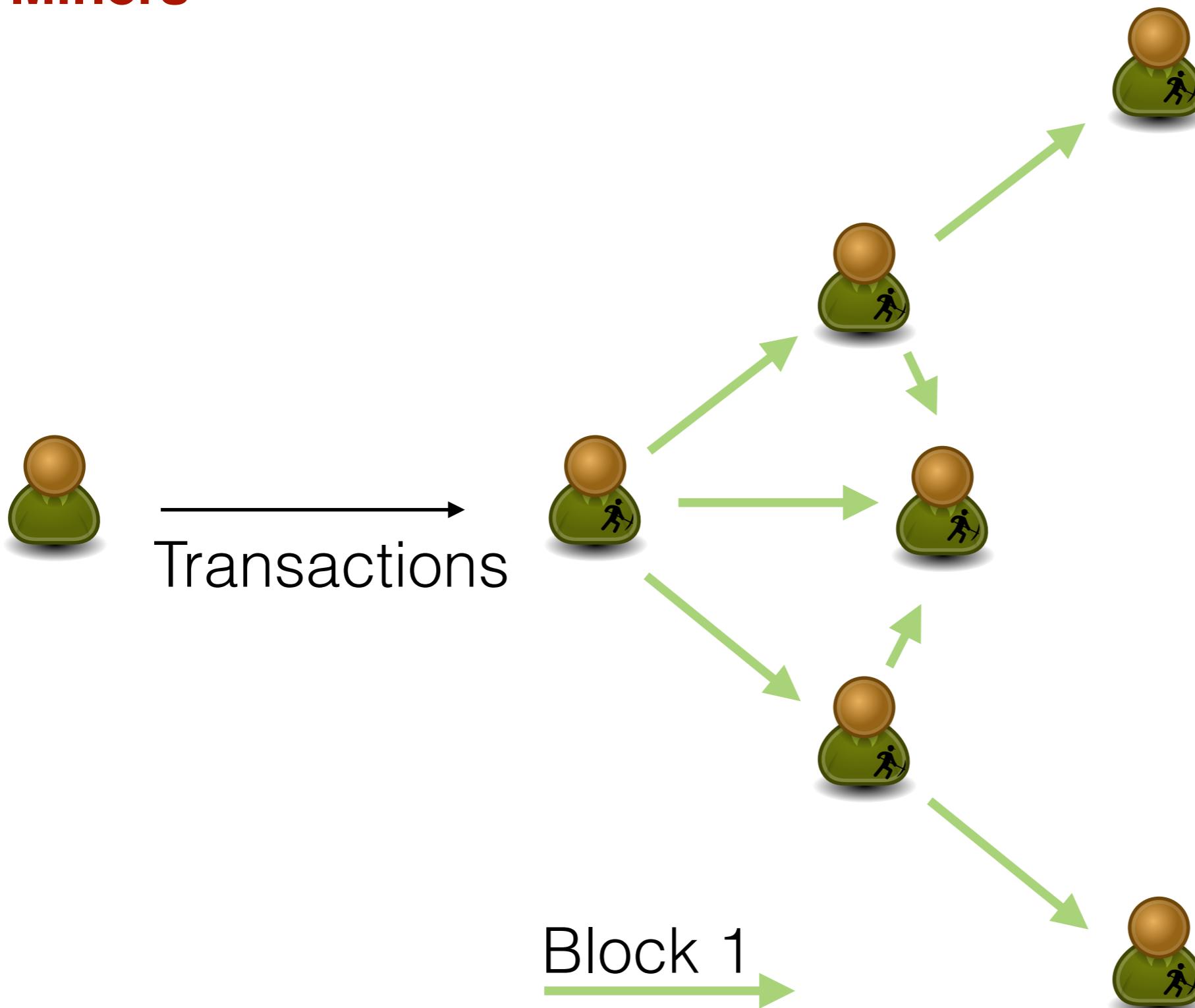
Miners



Miners



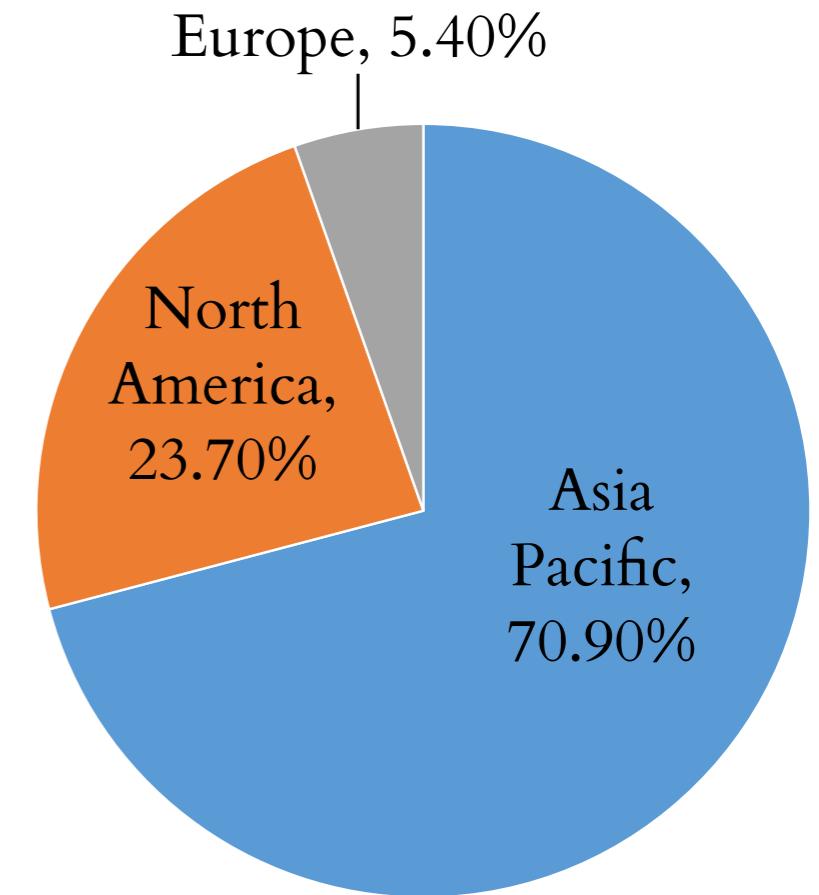
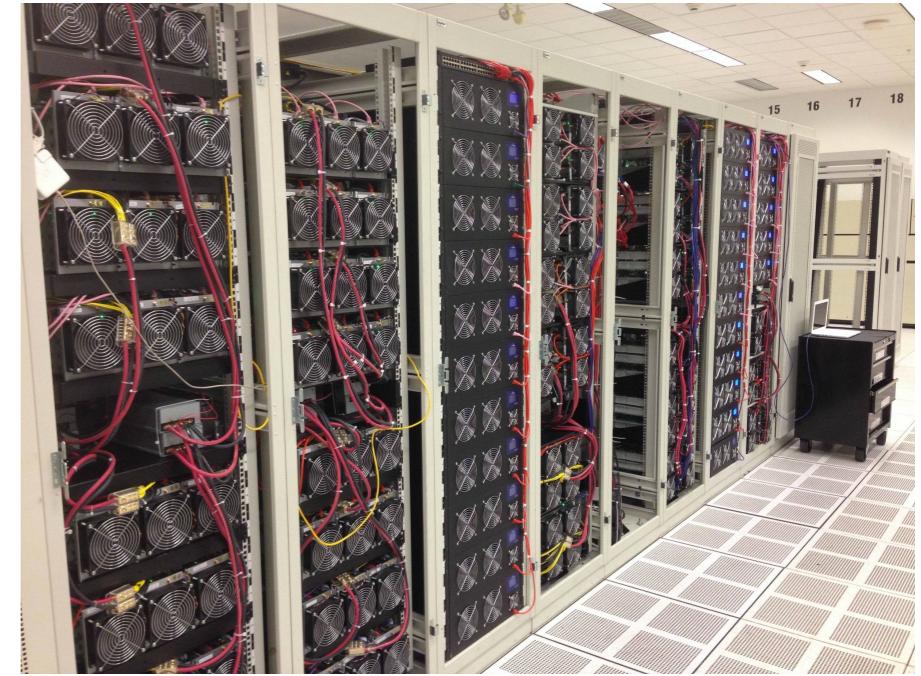
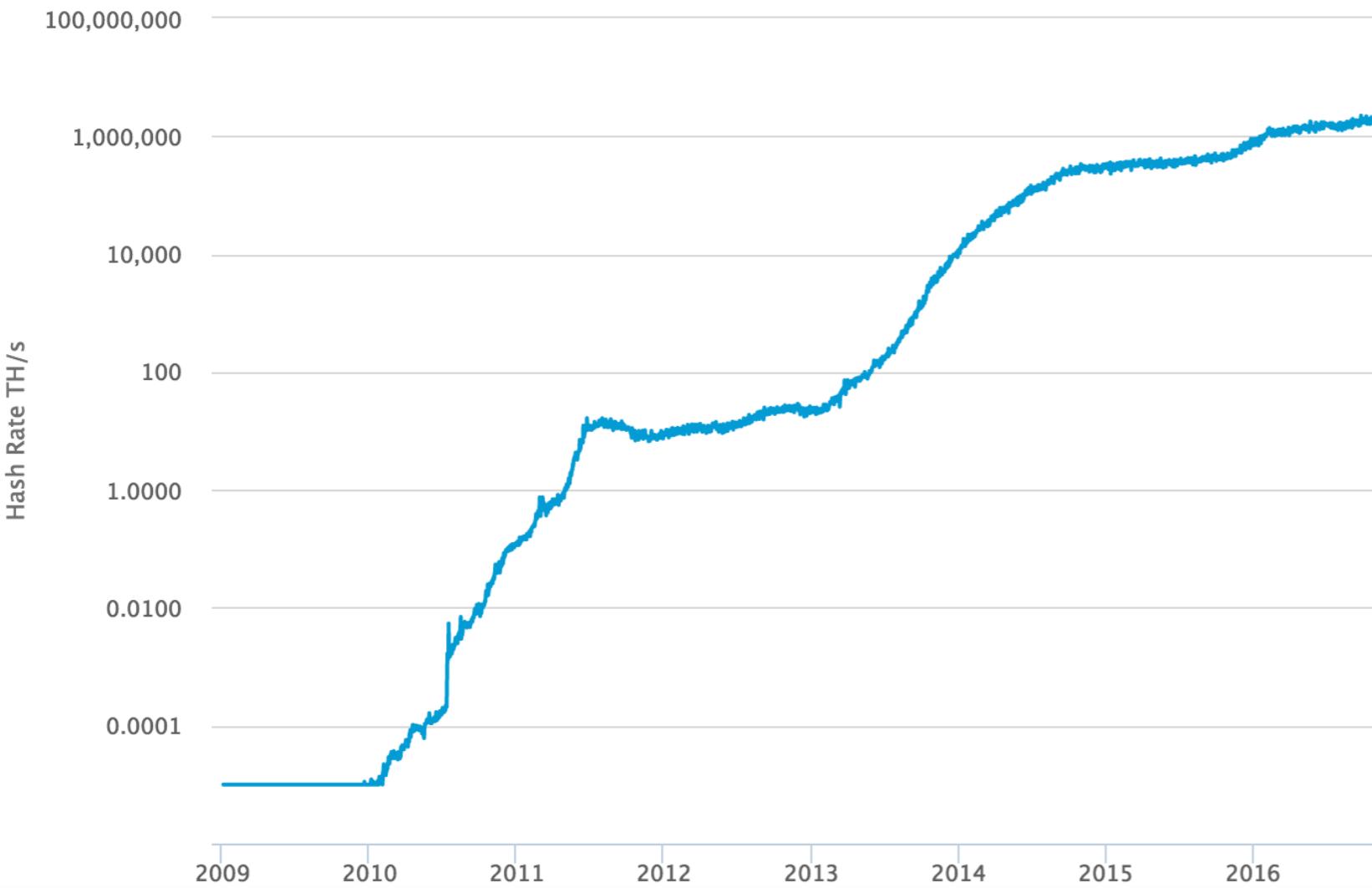
Miners



Mining



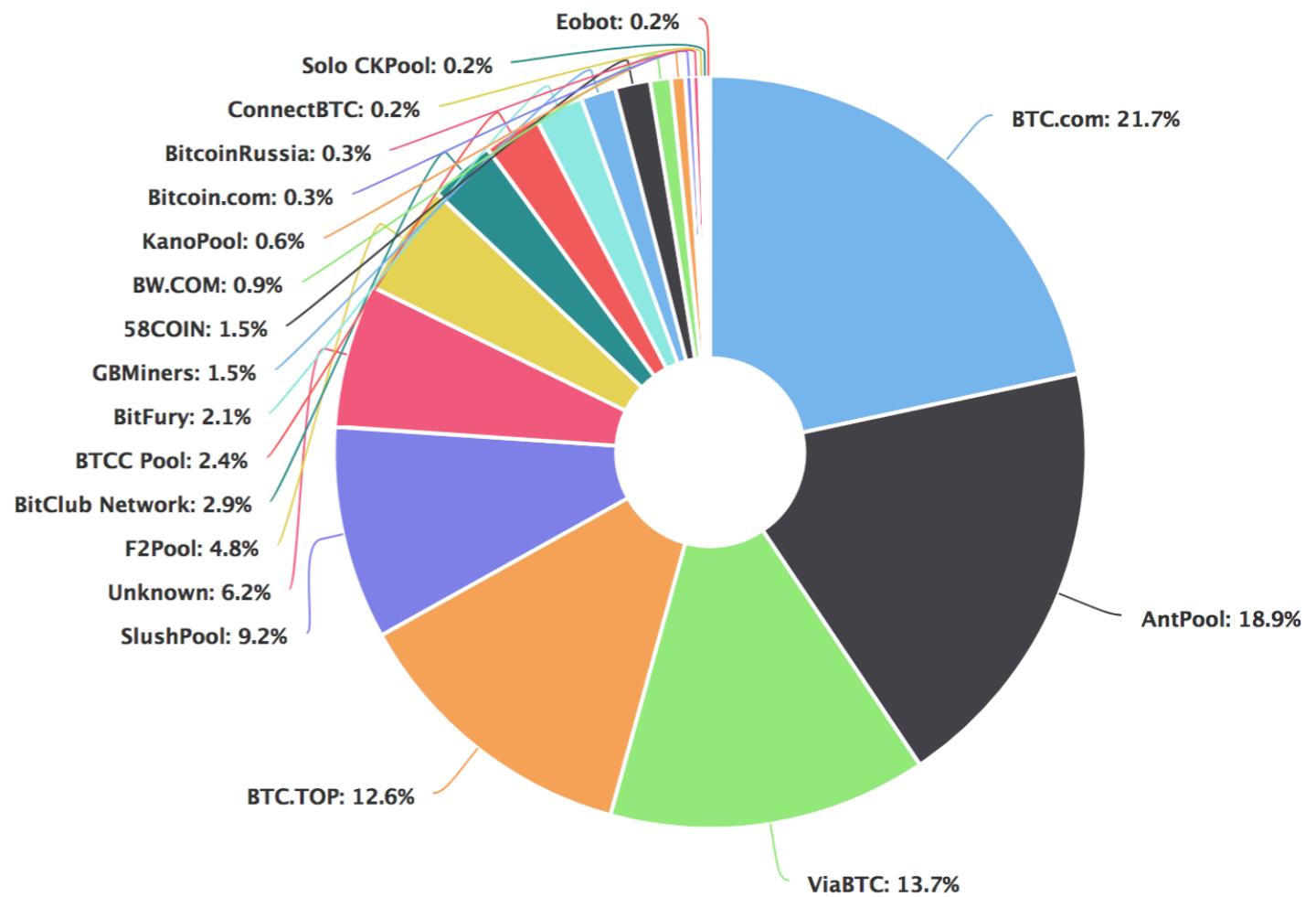
- From CPU to GPU to ASICs



Mining Pools



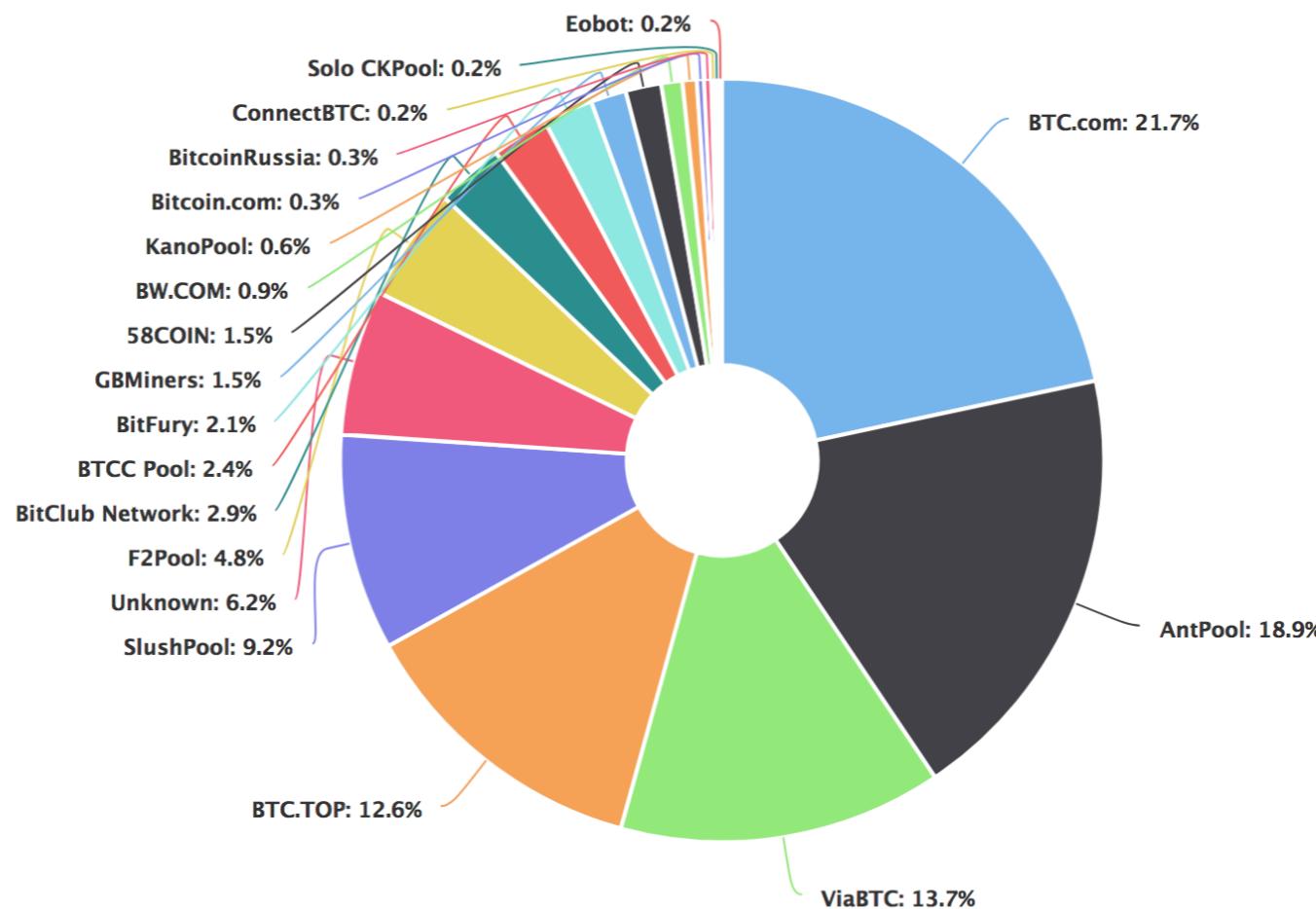
- Probability of finding a block alone is very small
- Unite in Mining pools
- Payout is done proportional to the work



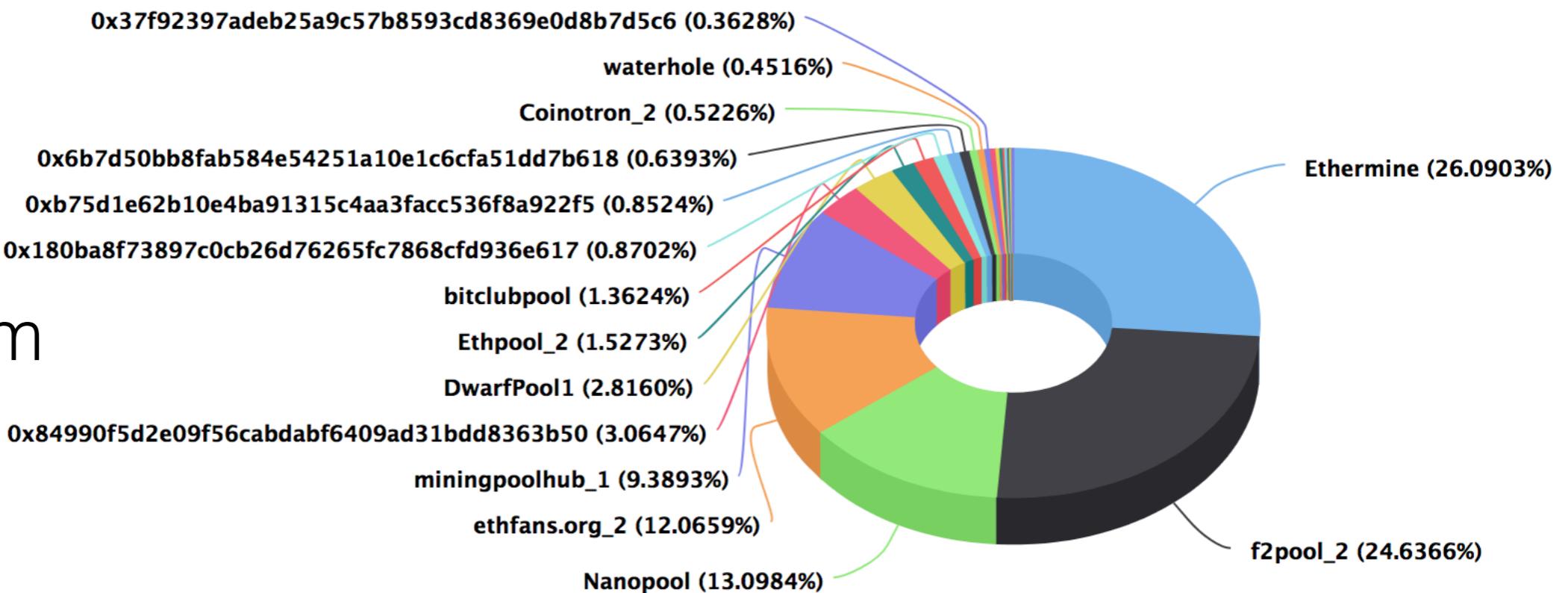
Mining Pools



Bitcoin



Ethereum



Mining Pools



- Probability of finding a block alone is very small

Mining Pools



- Probability of finding a block alone is very small

AntMiner S7



Advertised Capacity:

4.73 Th/s

Power Efficiency:

0.25 W/Gh

Weight:

8.8 pounds

Guide:

Yes

Price:

\$479.95



Mining Pools



- Probability of finding a block alone is very small

AntMiner S7



Advertised Capacity:

4.73 Th/s

Power Efficiency:

0.25 W/Gh

Weight:

8.8 pounds

Guide:

Yes

Price:

\$479.95



Bitcoin Mining Calculator and Profitability Calcul

Bitcoin Mining Calculator is used to calculate mining profitability for Bitcoin mining. Enter your Bitcoin mining hardware - dollars per kilowatt hour (\$/kWh). The current Bitcoin difficulty, Bitcoin block reward, and Bitcoin price w

Hash Rate (GH/s):	Power (Watts):
4730.00	2600.00
Power Cost (\$/kWh):	Pool Fees %:
0.10	0.00
Bitcoin Difficulty:	Block Reward:
2227847638503.63000000	12.50000000
Bitcoin to Dollar (USD):	Hardware Costs (USD):
13000.03000000	0.00
<input type="button" value="Calculate"/>	

Bitcoin Mining Calculator Summary

Days to generate one block mining solo: **23413.72 Day(s)** (can vary greatly depending on your luck)

Days to generate one BTC: **1873.10 Day(s)** (can vary greatly depending on the current exchange rates)

Days to break even: **N/A** (can vary greatly depending on the current exchange rates)

Miners



Solo Miner



Pool Operator



Pool Members

Miners



Solo Miner



Pool Operator

Solution/Share



Pool Members

Miners



Solo Miner



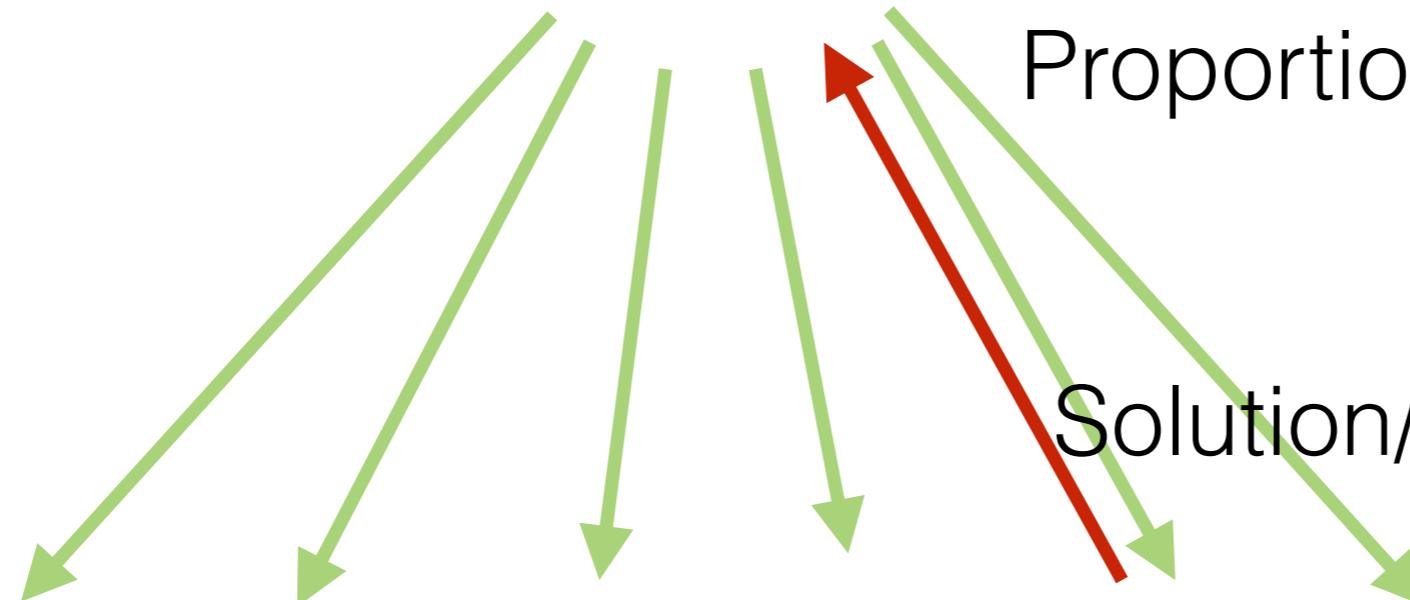
Pool Operator

Proportional Reward

Solution/Share



Pool Members



Mining Difficulty and Target in a Pool

Bitcoin's difficulty:

Pool's difficulty:

Mining Difficulty and Target in a Pool

Bitcoin's difficulty: $\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < T = 0x000^{**}$

Pool's difficulty:

Mining Difficulty and Target in a Pool

Bitcoin's difficulty: $\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < T = 0x000^{**}$

Pool's difficulty: $\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < t = 0x00^{**}$

Mining Difficulty and Target in a Pool

Bitcoin's difficulty: $\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < T = 0x000^{**}$

Pool's difficulty: $\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < t = 0x00^{**}$

- Difficulty of $t \ll T$

Mining Difficulty and Target in a Pool

Bitcoin's difficulty: $\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < T = 0x000^{**}$

Pool's difficulty: $\text{Hash}(\text{Hash}(B_3) | \text{txs} | N) < t = 0x00^{**}$

$\text{Hash}(\text{Block_3} | \text{merkle_root} | 0xbeef) = 0x000f..$



Transactions chosen
by pool operator.

Coinbase transaction
pays pool.

- Difficulty of $t \ll T$