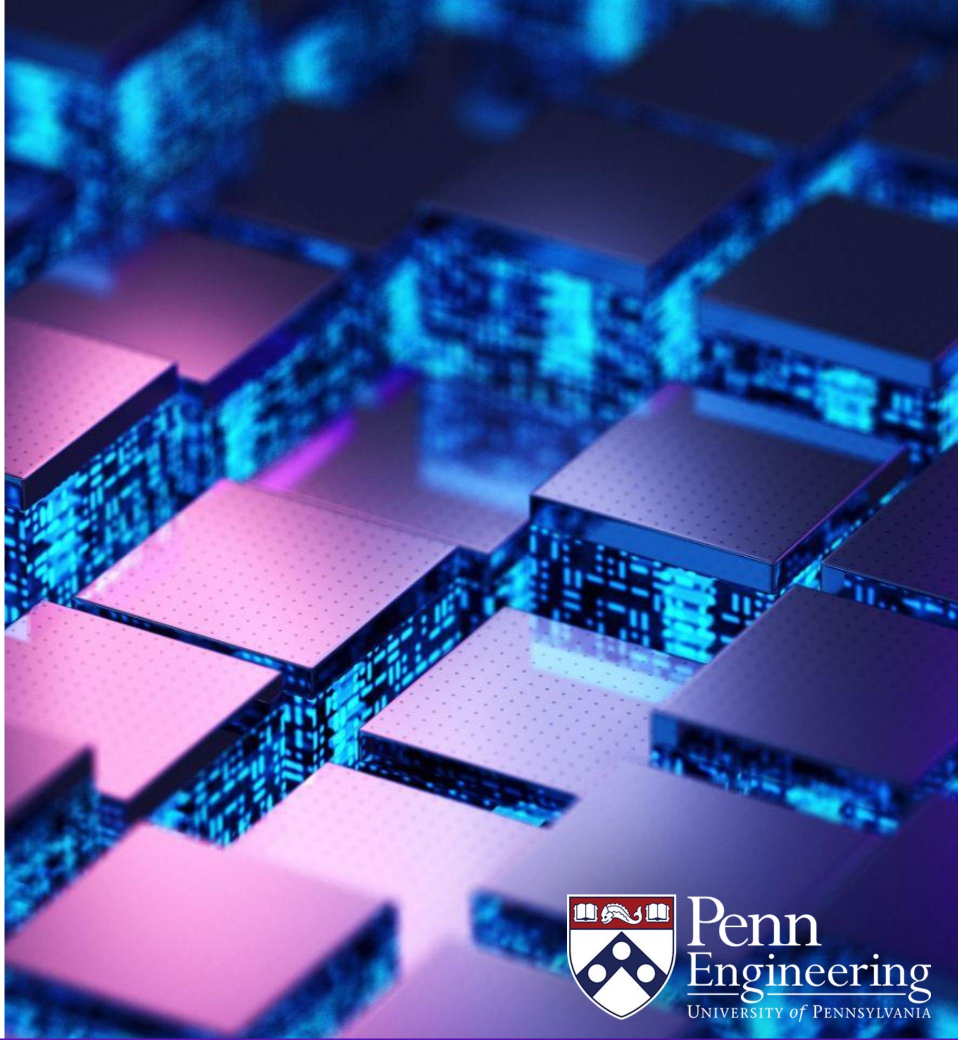
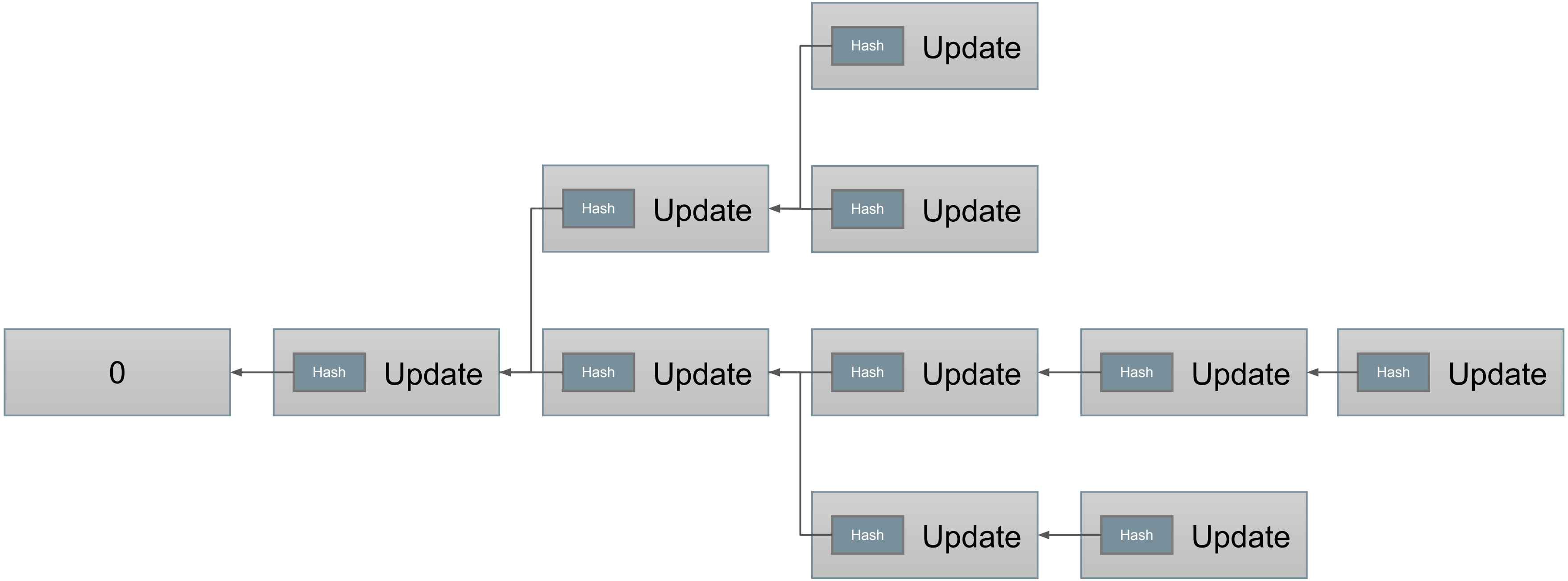
EAS 5830: BLOCKCHAINS

Nakamoto Consensus

Professor Brett Hemenway Falk

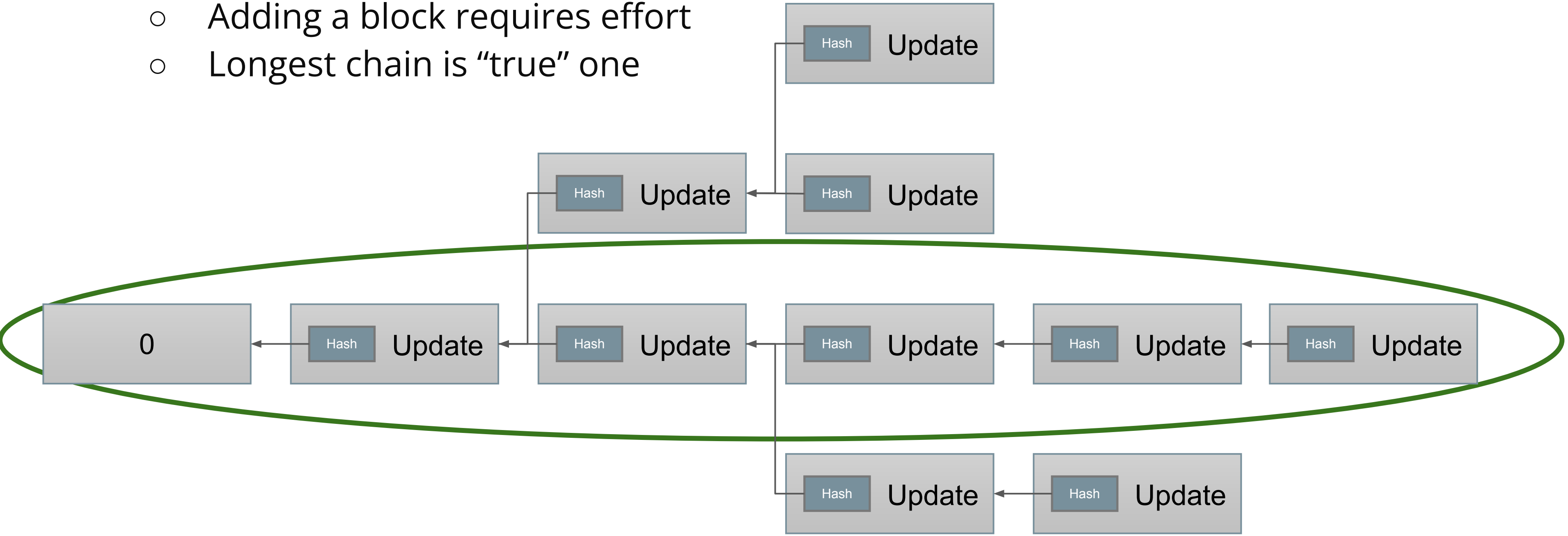


Hash chains are append only



Agreeing on last block

- Satoshi's idea
  - Adding a block requires effort
  - Longest chain is "true" one

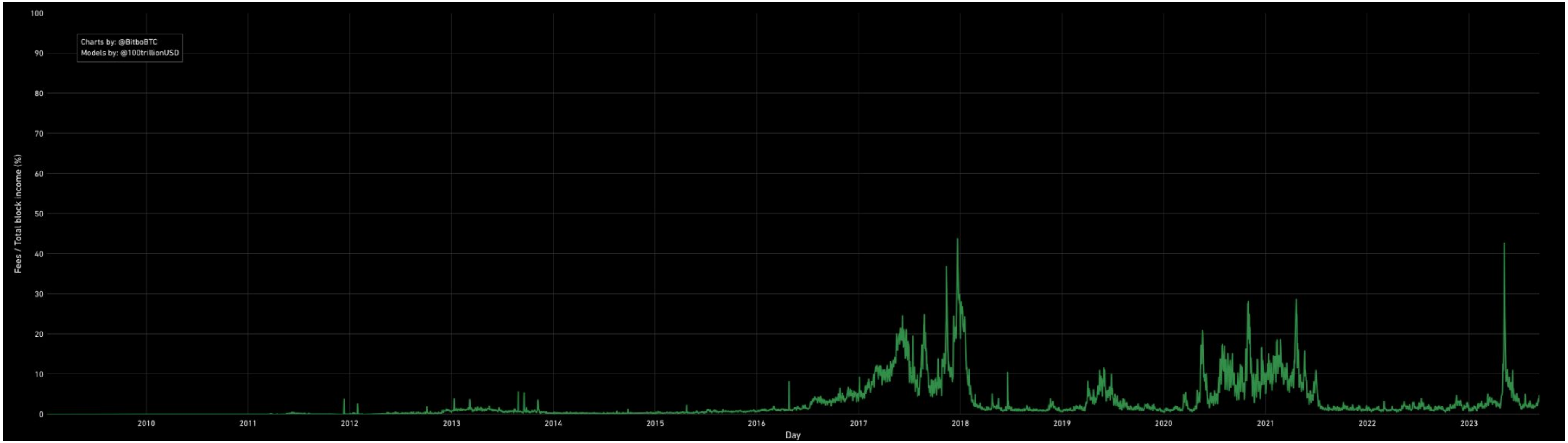


Difficulty

- A bitcoin block is only “valid” if its hash is less than a “target” value
- Mining Process:
  - Pack a block full of transactions
  - Add a random 4-byte nonce
  - Check if hash of the block is less than the target difficulty
  - If not, repeat with a new nonce
    - Or a new timestamp, or a new Coinbase Tx
  - Each miner can check many nonces in parallel
- All miners are doing this simultaneously and independently

Consensus

- Anyone can build a block (if they can make the hash small enough)
- You can build on any block you like
- If you build a block you can claim
  - Block rewards
  - Transaction fees



Charts by: @BitboBTC
Models by: @100trillionUSD

Bitcoin block rewards

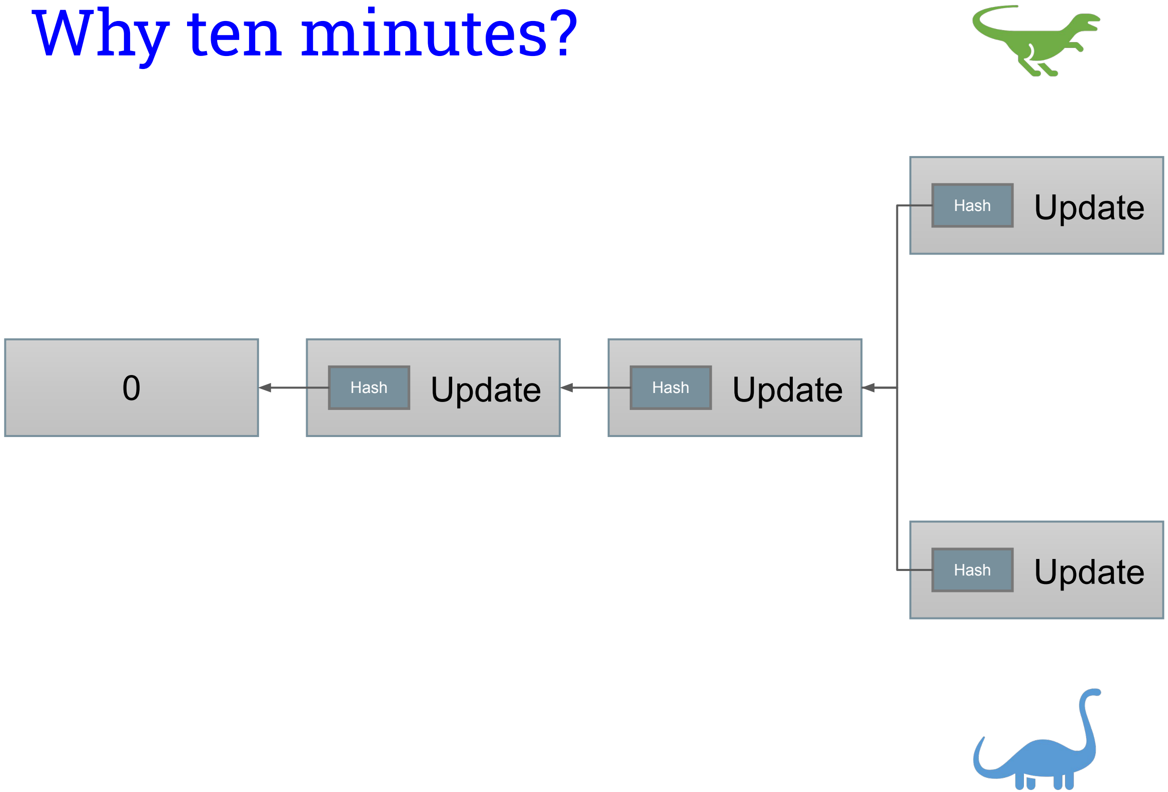
- Block rewards were initial 50 BTC / block
- Block rewards halve every 210,000 blocks (approximately every 4 years)
  - 50 → 25 → 12.5 → 6.25
- All Bitcoin in existence came from block rewards – initially there were no BTC in circulation, but the total supply of BTC is asymptotically increasing towards 21 million

$$50 \cdot 210,000 \cdot \left(\sum_{t=0}^{\infty} \frac{1}{2^t} \right) = 50 \cdot 210,000 \cdot 2 = 21,000,000$$

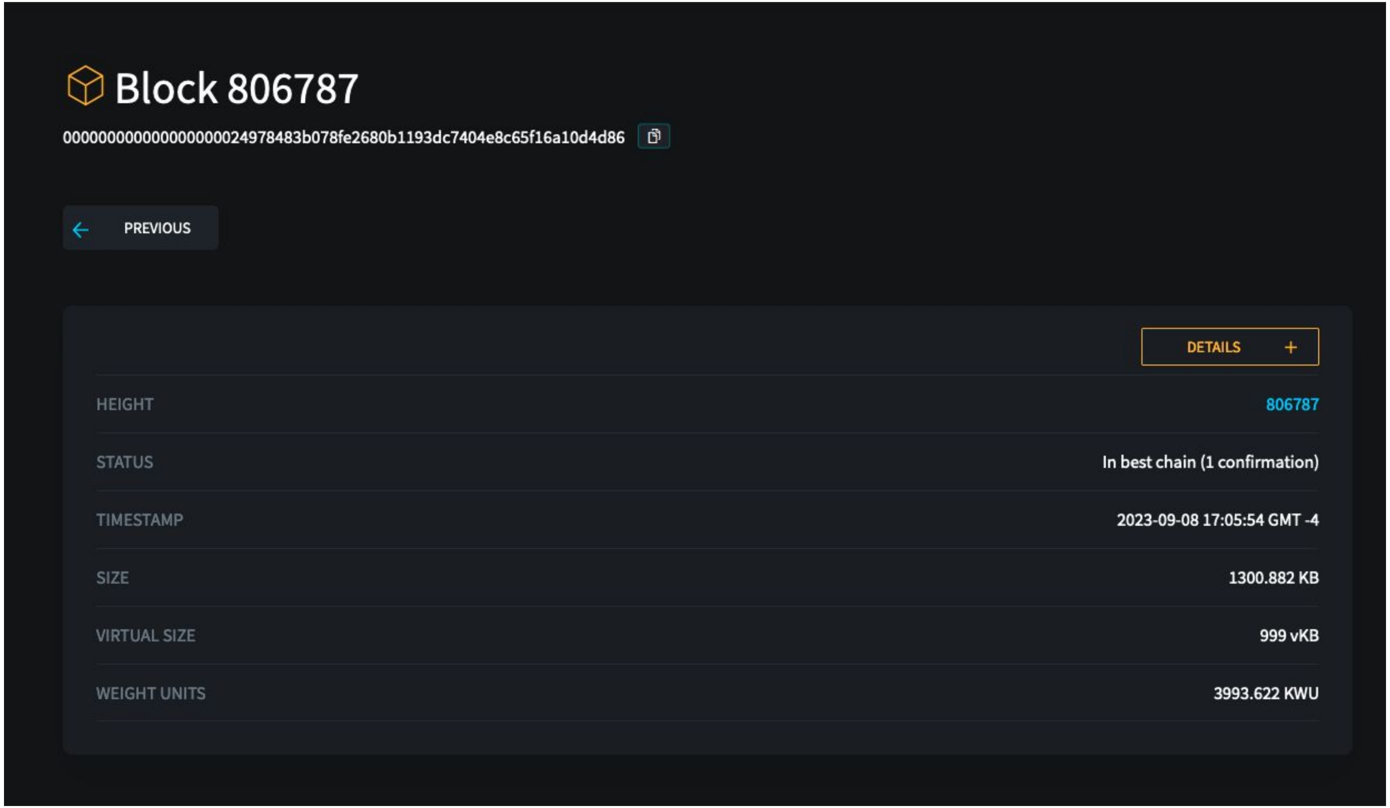
Adjusting the difficulty

- Initial target: $\texttt{0x}\overbrace{\texttt{00000000}}^{\text{8 hex zeros is 32 leading zeros in bit representation}}\texttt{ffff0000000000000000000000000000000000000000000000000000}$
  - On average about 2^{32} ~ 4 billion trials
- Difficulty defined to be: initial target / current target
- The target block hash is set by the Bitcoin network
  - Difficulty is adjusted every 2016 blocks (approximately 2 weeks)
  - If the average time between blocks is longer than 10 minutes, difficulty is decreased
  - If the average time between blocks is shorter than 10 minutes, difficulty is increased

Why ten minutes?



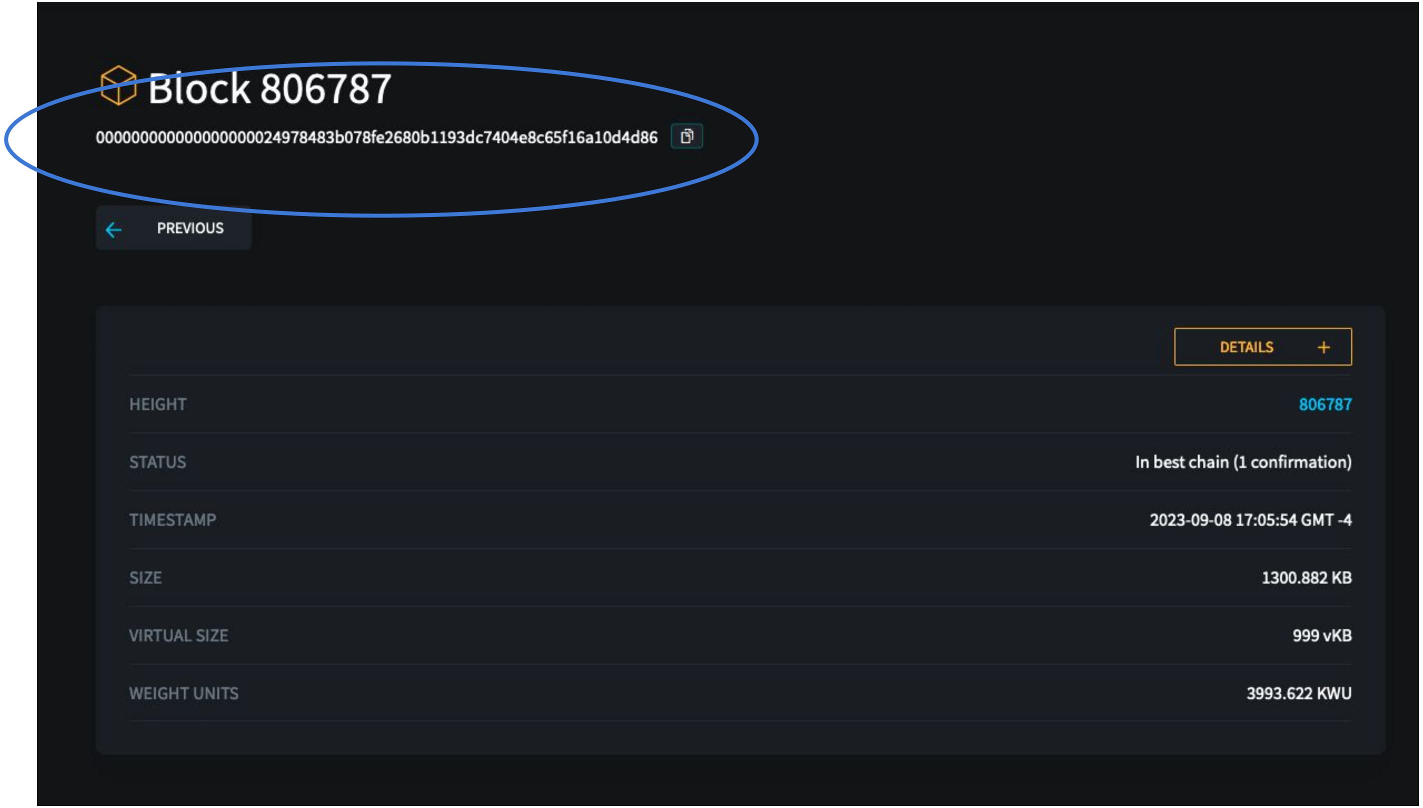
- Suppose Alice and Bob are mining independently
- What if they both solve a PoW puzzle at the same time?



Block 806787

0000000000000000000024978483b078fe2680b1193dc7404e8c65f16a10d4d86

HEIGHT	806787
STATUS	In best chain (1 confirmation)
TIMESTAMP	2023-09-08 17:05:54 GMT -4
SIZE	1300.882 KB
VIRTUAL SIZE	999 vKB
WEIGHT UNITS	3993.622 KWU

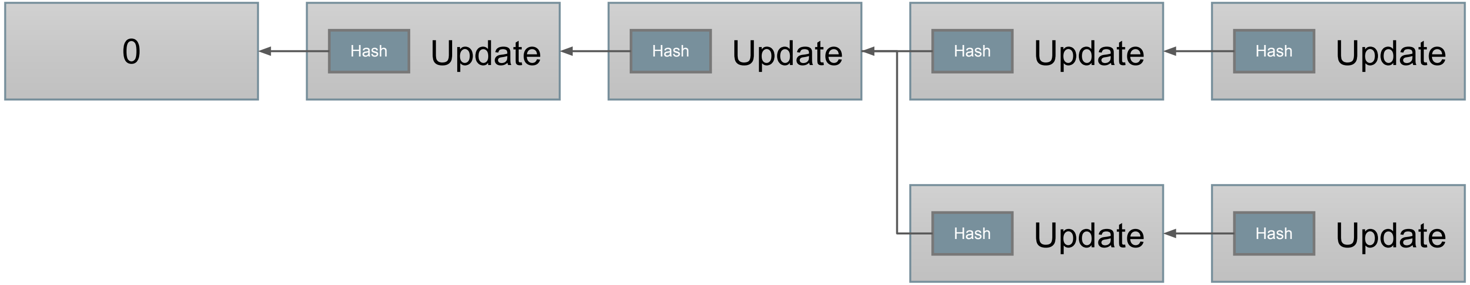


Block 806787

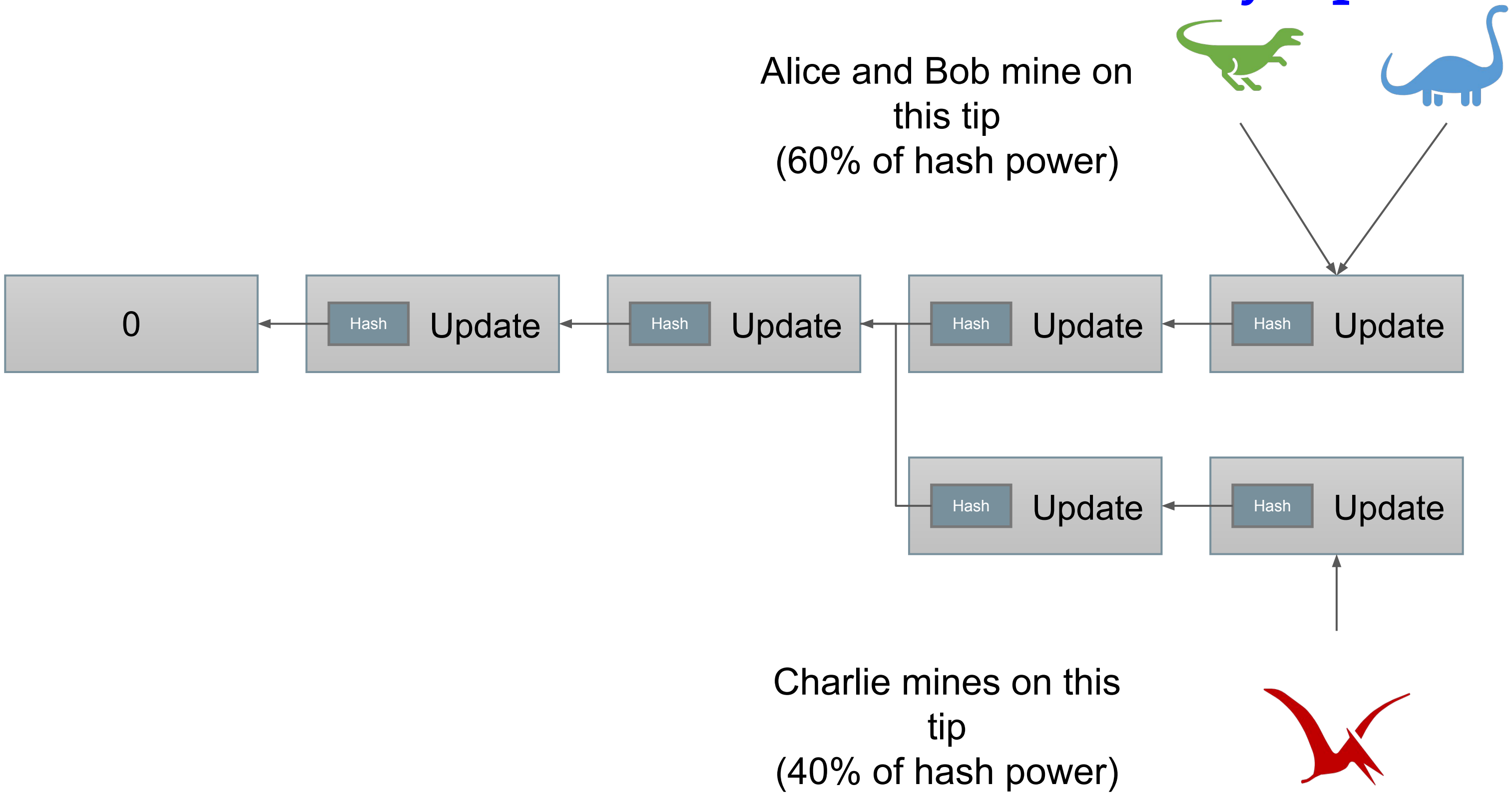
0000000000000000000249784 83b078fe2680b1193dc7404e8c65f16a10d4d86

HEIGHT	806787
STATUS	In best chain (1 confirmation)
TIMESTAMP	2023-09-08 17:05:54 GMT -4
SIZE	1300.882 KB
VIRTUAL SIZE	999 vKB
WEIGHT UNITS	3993.622 KWU

Miners can direct their hash towards any tip



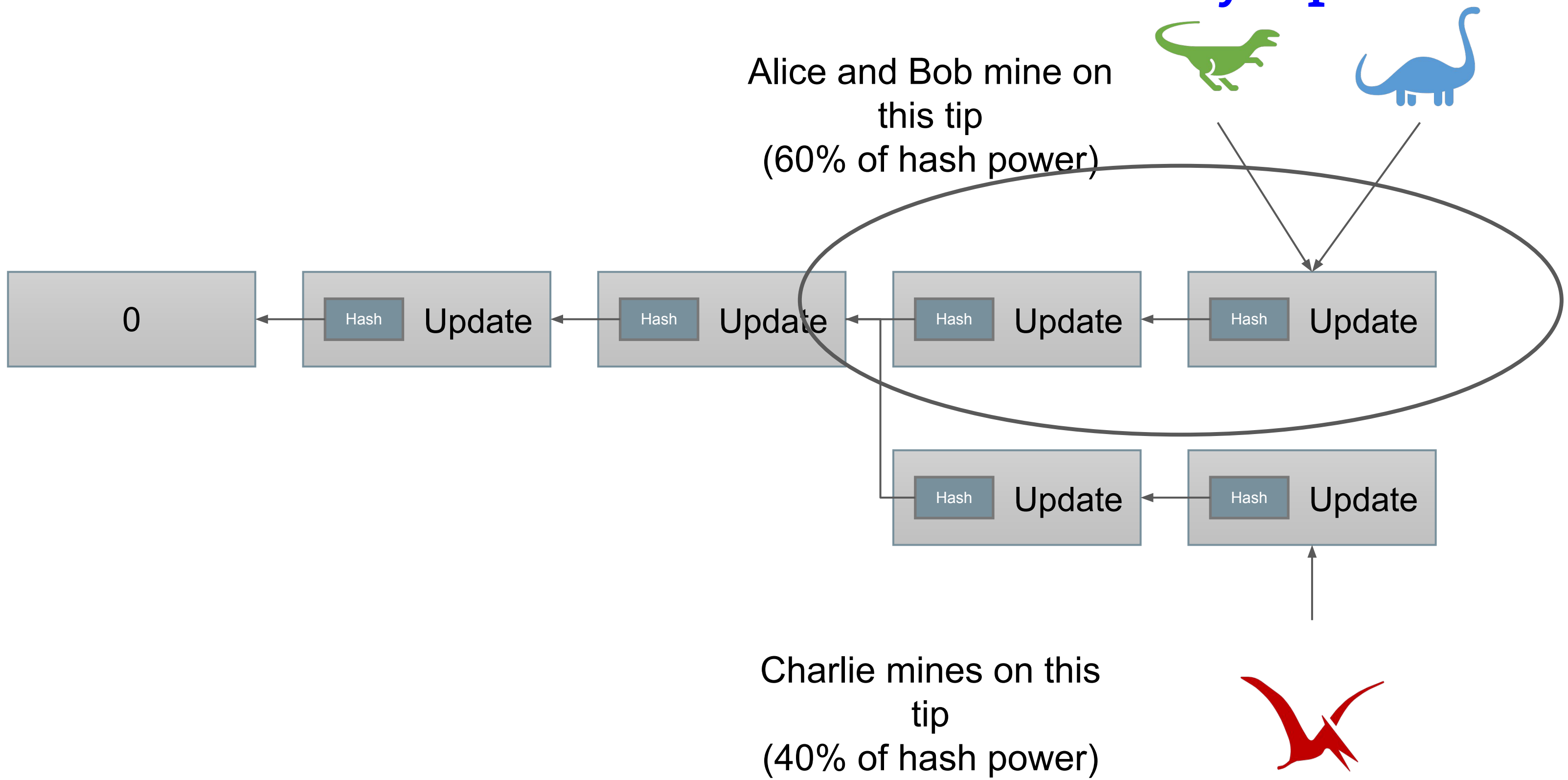
Miners can direct their hash towards any tip



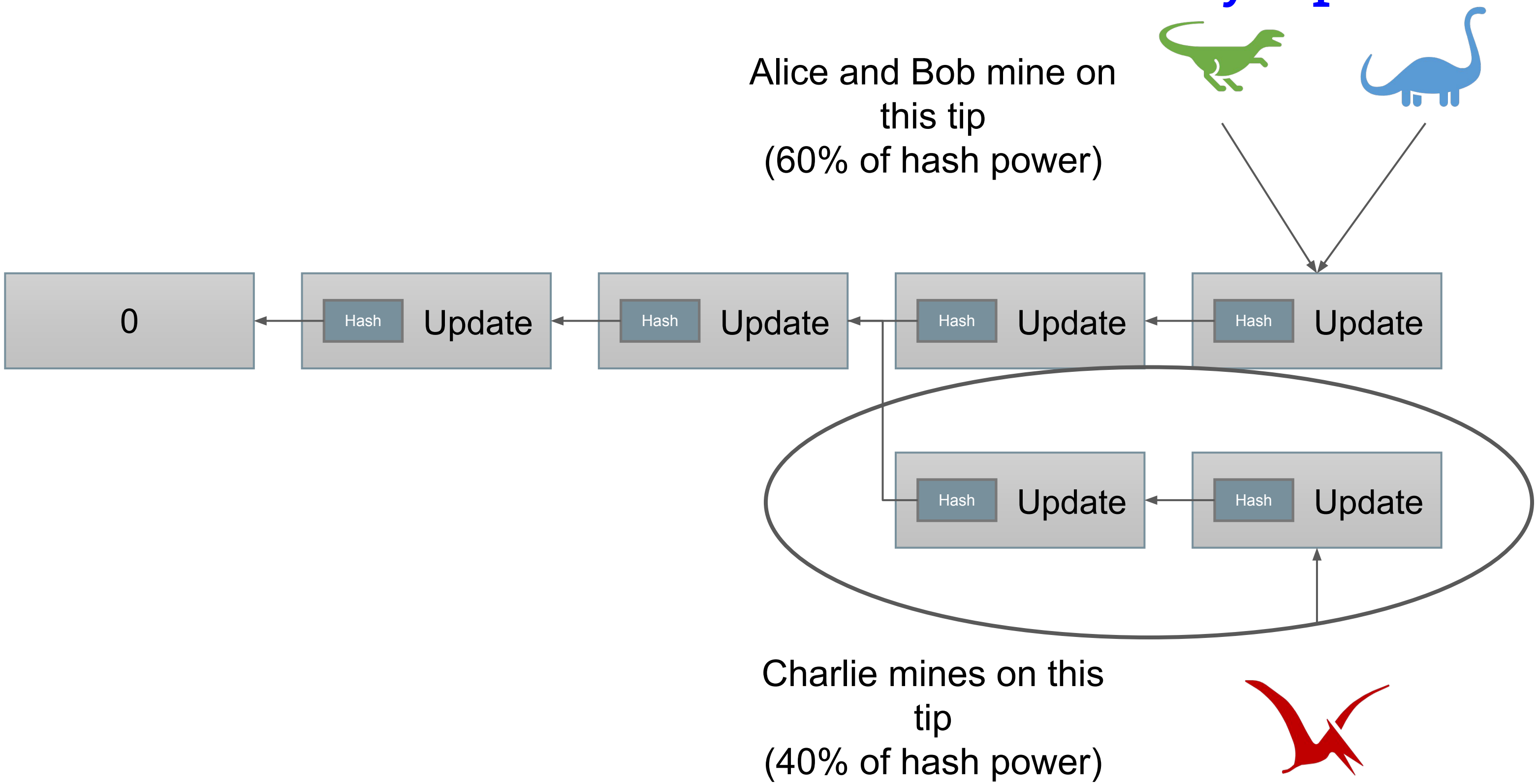
Alice and Bob mine on this tip
(60% of hash power)

Charlie mines on this tip
(40% of hash power)

Miners can direct their hash towards any tip


Alice and Bob mine on this tip (60% of hash power)
0
Hash
Update
Hash
Update
Hash
Update
Hash
Update
Hash
Update
Hash
Update
Charlie mines on this tip (40% of hash power)

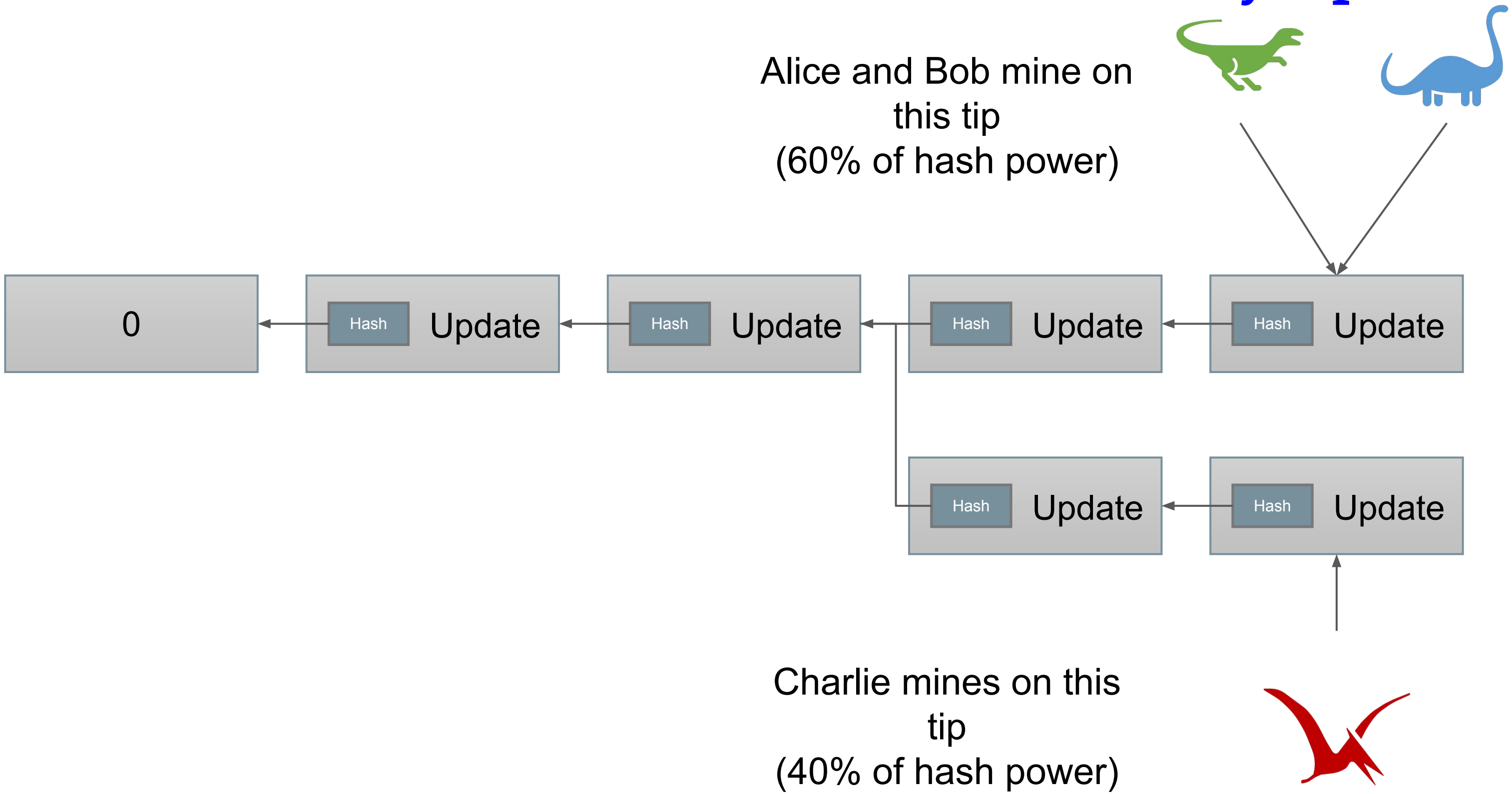
Miners can direct their hash towards any tip



Alice and Bob mine on this tip
(60% of hash power)

Charlie mines on this tip
(40% of hash power)

Miners can direct their hash towards any tip

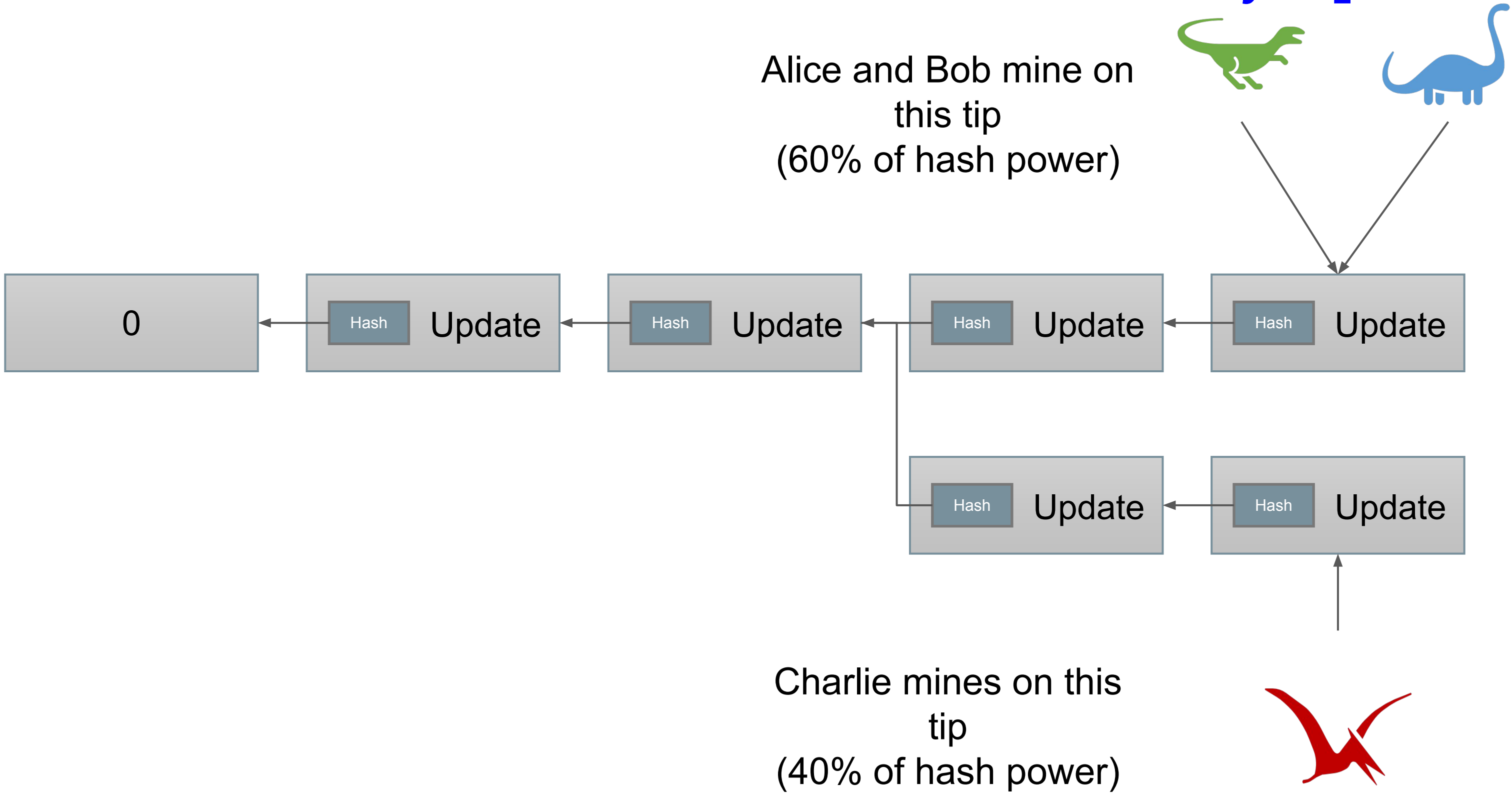


Alice and Bob mine on this tip
(60% of hash power)

Charlie mines on this tip
(40% of hash power)

Alice and Bob should produce blocks faster than Charlie – Top chain grows faster

Miners can direct their hash towards any tip



Alice and Bob mine on this tip
(60% of hash power)

Produce a block every 10/.6 = 16.6 minutes

Charlie mines on this tip
(40% of hash power)

Produce a block every 10/.4 = 25 minutes

Finality

- Bitcoin has “eventual” finality
  - It is common to wait 6 blocks for “finality”
  - Thorchain waits longer for larger transactions