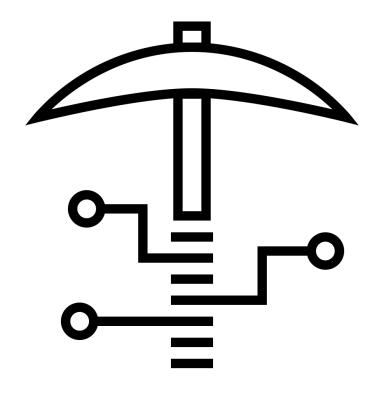
Mining

Consensus

Mining



Definition

Mining is the mechanism used in most cryptocurrencies to systematically give rights to add data to the blockchain.

Five Mining Actions

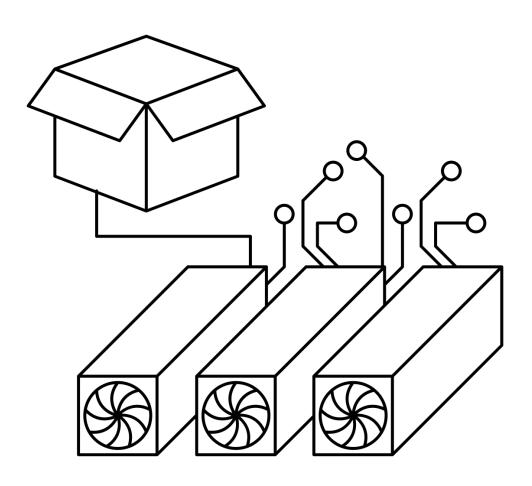
- Validate transactions
- Propagate transactions
- Validate blocks
- Propagate blocks
- Store the data

Mining Incentives

Giving the miner of each block (the node that puts the block on the blockchain) a block reward

Giving the miner transaction fees which are paid by those conducting the transactions

Proof-of-Work Mining



Definitions

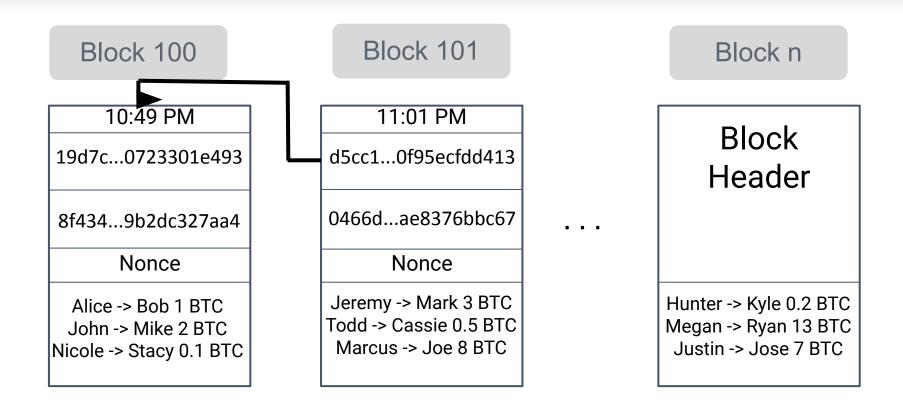
Proof-of-Work (PoW)

mining allows us to give the right to add the next block on the blockchain by creating a game that consumes electricity (work).

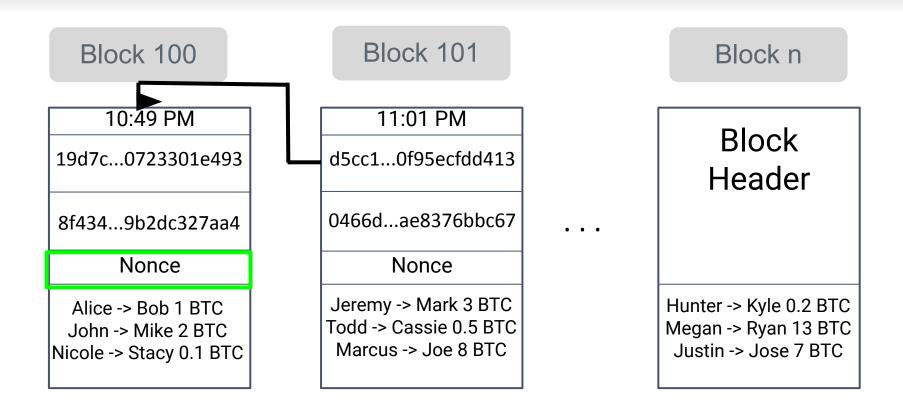
Mining Difficulty Rate

can be thought of as the hash of the block header must contain a certain number of 0's at the beginning.

Proof-of-Work: Example (1/8)



Proof-of-Work: Example (2/8)



Proof-of-Work: Example (3/8)

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

1

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

11:01 PM

Hash of Previous Block Header

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

Hash Function



d5cc1...0f95ecfdd413

Proof-of-Work: Example (4/8)

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

2

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

11:01 PM

Hash of Previous Block Header

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

Hash Function



81b6c...4ac542baa06

Proof-of-Work: Example (5/8)

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

3

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

11:01 PM

Hash of Previous Block Header

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

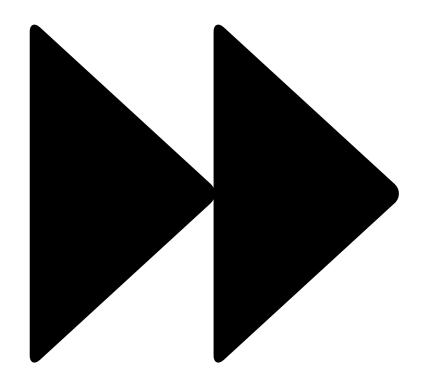
Block Header

Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

Hash Function



3a27d...391d7d06ee5



Proof-of-Work: Example (6/8)

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

7531

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

11:01 PM

Hash of Previous Block Header

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

Hash Function



00000...3b1dad26gy5

Proof-of-Work: Example (7/8)

Block 100

10:49 PM

19d7c...0723301e493

8f434...9b2dc327aa4

7531

Alice -> Bob 1 BTC John -> Mike 2 BTC Nicole -> Stacy 0.1 BTC Block 101

11:01 PM

00000...3b1dad26gy5

0466d...ae8376bbc67

Nonce

Jeremy -> Mark 3 BTC Todd -> Cassie 0.5 BTC Marcus -> Joe 8 BTC Block n

Block Header

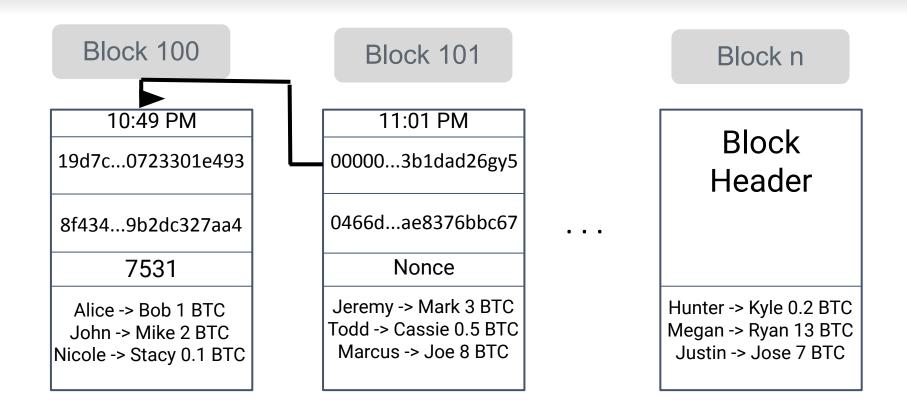
Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

Hash Function

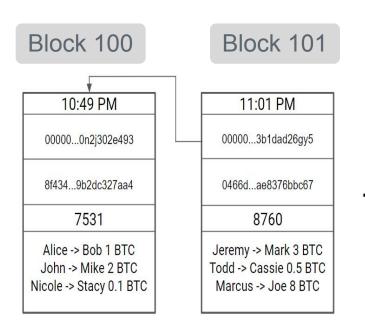


00000...3b1dad26gy5

Proof-of-Work: Example (8/8)



Blockchain + Current State



Block n

Block Header

Hunter -> Kyle 0.2 BTC Megan -> Ryan 13 BTC Justin -> Jose 7 BTC

Alice: 5 BTC Bob: 2 BTC John: **21 BTC** Joe: 1 BTC Amy: 0.6 BTC Leslie: 43 BTC

8 BTC Tim: 0.3 BTC

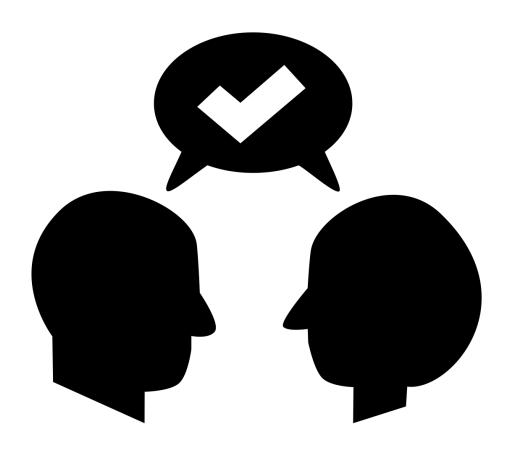
Nicole:

Jesse: 11 BTC

Steven: 17 BTC Darren: 3 BTC

0.1 BTC Jose:

Consensus



Definition

Consensus is the ability for all honest participants to come to agreement over a single truthful version of the blockchain in a trustless manner.

Consensus Algorithm
is the algorithmic
process in which a
blockchain network
achieves consensus.