Bitcoin Consensus Protocol

Two Security Mechanisms

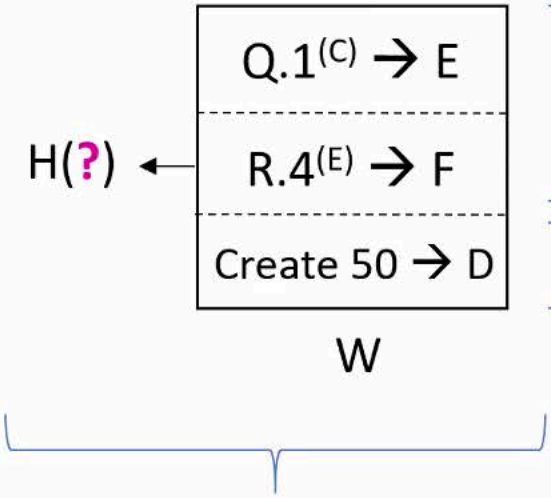
- Financially reward nodes for following the protocol properly
- Randomly select a node each round so no single entity has too much influence.

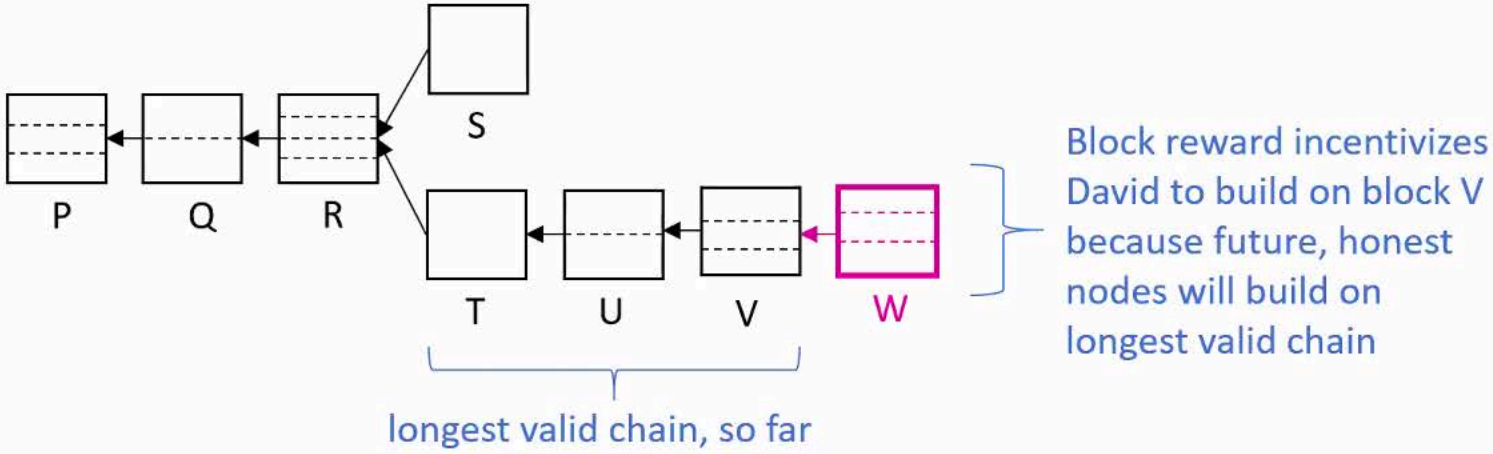
Bitcoin Consensus Protocol
Block Reward Incentive

- Block reward mechanism incentivizes nodes to propose blocks that will end up on the long-term consensus chain.

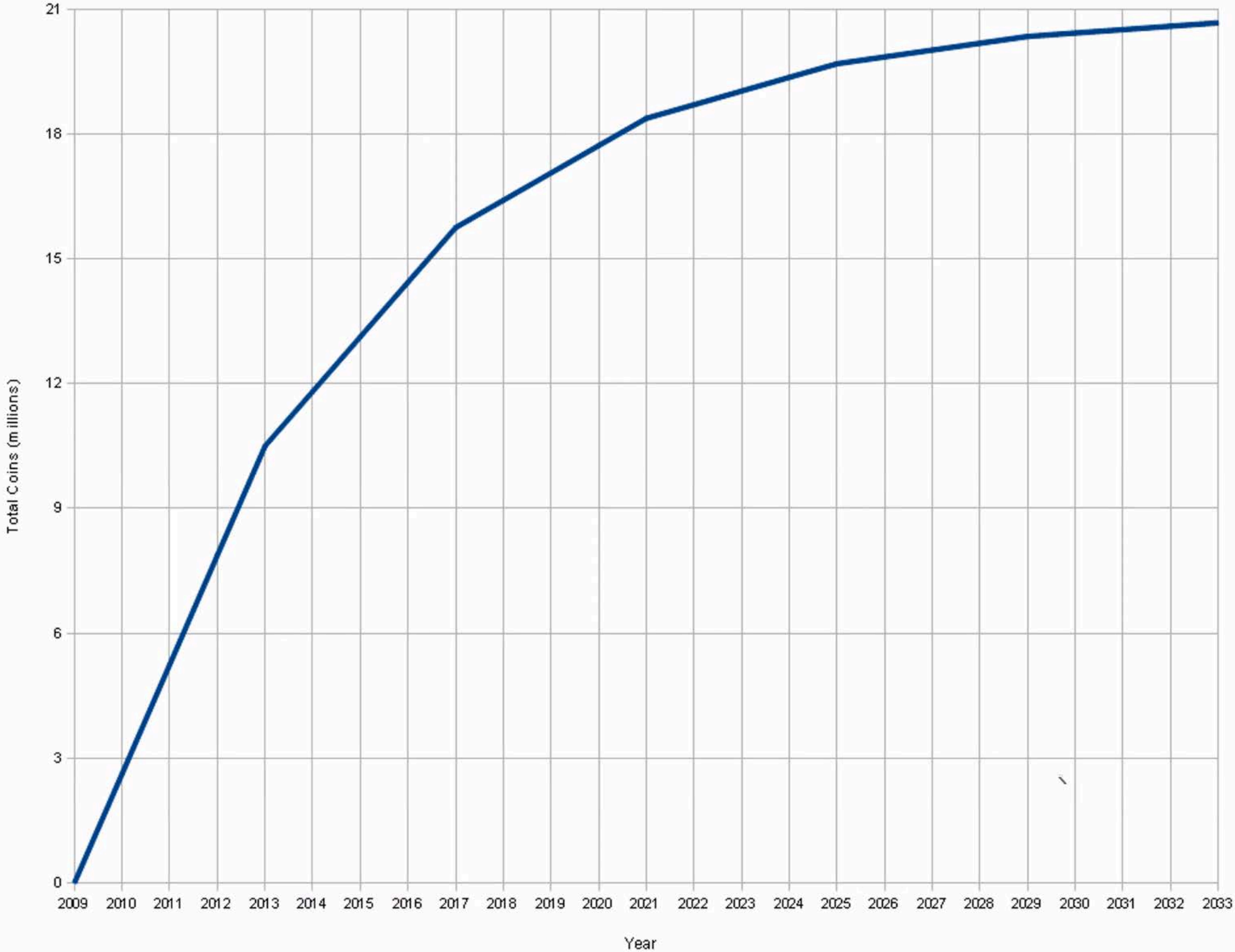
David is the randomly selected node that gets to propose his block in round 6.

David





Block reward is halved every four years



Bitcoin Consensus Protocol

- Three remaining unaddressed challenges:

    1. Selecting a node randomly to propose a block
    2. Preventing instability caused by any node possibly selected to propose a block
    3. Defending against Sybil attacks

- **Proof of Work** is a mechanism that addresses all three challenges
    - A node can propose a block if it solves a computationally-expensive cryptographic puzzle.
    - A node continually competes with other nodes to solve the puzzle first.

Bitcoin Consensus Protocol
Proof of Work

Proof of Work: A node can only propose a block if it solves a computationally-expensive cryptographic puzzle.

David needs to provide "**PROOF**-of-work" if he wants to propose a block.

David

David's proposed block W

H(**V**)

$Q.1^{(C)} \rightarrow E$
$R.4^{(E)} \rightarrow F$
Create 50 → D
PROOF

W

Broadcasted transactions

Block reward

Puzzle solution

SHA-256 (PROOF ∘ PrevHptr ∘ Tx_1 ∘ Tx_2 ∘ Tx_3 ∘ ... ∘ Tx_i) < TARGET

Parent block hash

Broadcasted transactions and block reward

Current difficulty level

Bitcoin Consensus Protocol
Puzzle Difficulty

SHA-256 (PROOF ◦ PrevHptr ◦ Tx_1 ◦ Tx_2 ◦ Tx_3 ◦ ... ◦ Tx_i) < TARGET

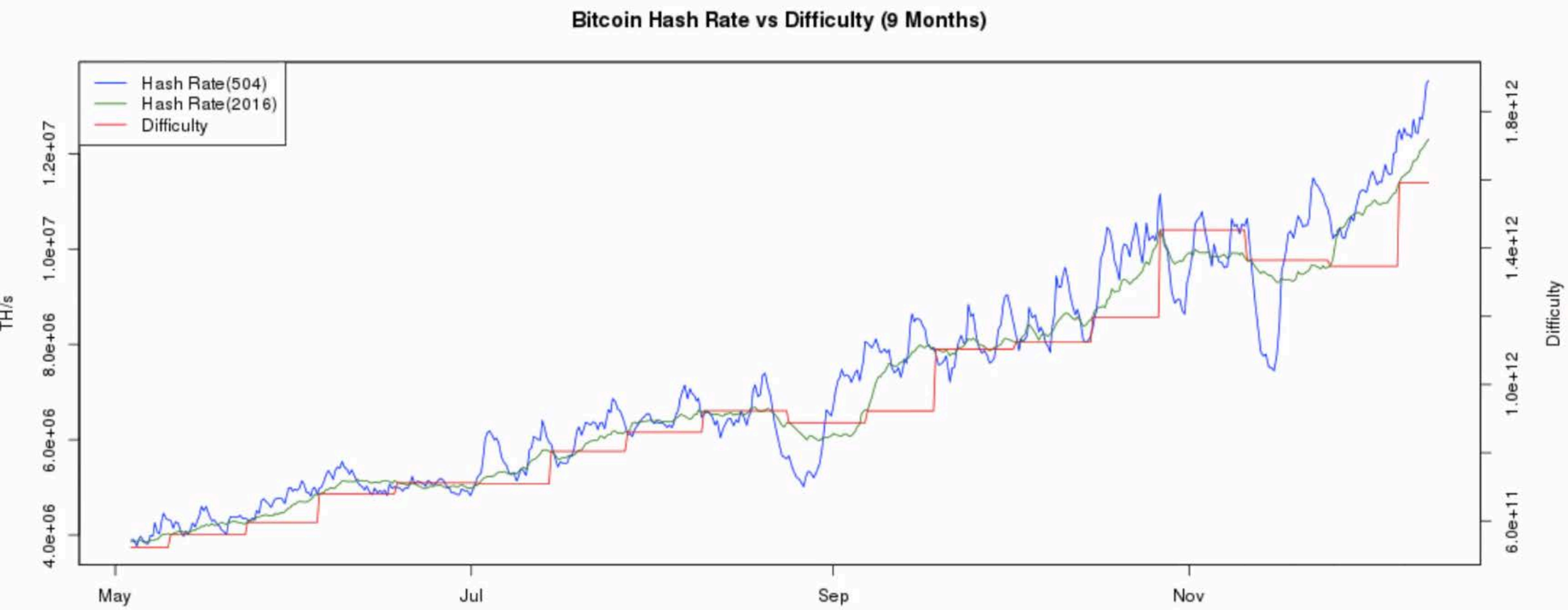
- Solving a proof-of-work puzzle can only be performed by trying random values for **PROOF** and checking if it satisfies the condition above.
- Puzzle difficulty can be increased by decreasing the value of **TARGET**.
- TARGET is recalculated every 2016 blocks:

$$TARGET_{i+1} = TARGET_i * [\text{duration of mining last 2016 blocks} / (2016 * 10 \text{ minutes})]$$

- $TARGET_{i+1}$: Next difficulty level
- $TARGET_i$: Current difficulty level
- duration of mining last 2016 blocks: Chain-specific value calculated using block timestamps.
- (2016 * 10 minutes): Goal duration of mining 2016 blocks

- TARGET needs to be periodically recalculated to keep **block interval** at 10 minutes
- Block interval affected by:
  1. Miners joining or leaving the network as exchange rate fluctuates.
  2. Mining hardware becomes more efficient over time.

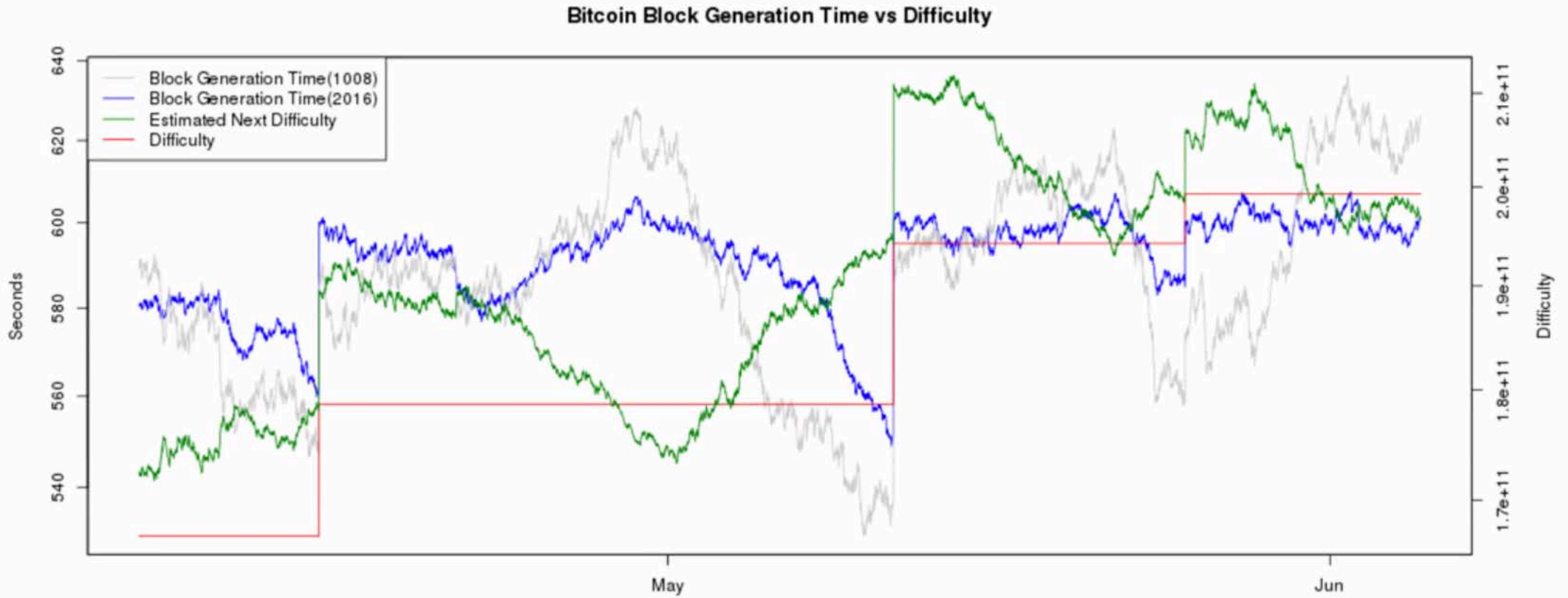
Bitcoin Consensus Protocol
Puzzle Difficulty



- **"Difficulty"** series is a step function that changes every 2016 blocks
- **"Hash Rate"** series is an estimate of how many tera-hashes per second the entire Bitcoin network is computing
- Note how the hash rate is modulated by the periodic recalculation of the difficulty

Reference: bitcoinwisdom.com

Bitcoin Consensus Protocol
Puzzle Difficulty



- **"Difficulty"** series is a step function that changes every 2016 blocks
- **"Block Generation Time"** series is how quickly new blocks are found. Bitcoin adjusts the difficulty to keep the block generation time at 10 minutes
- Note how the block generation time is modulated to 10 minutes by the periodic recalculation of the difficulty

Reference: bitcoinwisdom.com

Bitcoin Consensus Protocol
51% Hashpower Attacker

Attack Method	Effect
Attacker steals bitcoins by forging signatures.	Not possible. Forging signatures is cryptographically infeasible.
Attacker steals bitcoins by including an invalid transaction in his proposed block. Pretends block is valid, continues to build upon it, and makes it on the longest chain.	Not possible. Honest nodes can easily detect invalid transactions and will not build upon an invalid block. Thus, a fork will be created and honest nodes will continue building on the valid chain. Merchants will wait for confirmations only on valid chains.
Attacker mounts denial of service on specific victim by ignoring his transactions.	Not possible, assuming attacker does not fully control the network. Eventually an honest node will mine a block which will include the victim's transactions.
Attacker destroys confidence in Bitcoin by controlling 51% hashpower.	Possible. Users will lose confidence in the currency as decentralized ledger, causing exchange rate to plummet.