Lecture #2: How Bitcoin Achieves Decentralization

Lecture 2.1 Centralization vs. Decentralization

Competing paradigms that underline many digital technologies

Aspects of decentralization in Bitcoin

Peer-to-peer network:
  Open to anyone, low barrier to entry
Mining:
  Open to anyone, but inevitable concentration of power
  Often seen as undesirable
Updates to software:
  Core developers trusted community, have great power

Lecture 2.2 Distributed Consensus

Why consensus protocols?
Traditional motivation: reliability in distributed systems
Distributed key-value store enables various applications:
DNS, public key directory, stock trades.

Defining distributed consensus
The protocol terminates and all correct nodes decide on the same value.
This value must have been proposed by some correct node.

How consensus could work in Bitcoin
At any given time:

- All nodes have a sequence of blocks of transactions they've reached consensus on
- Each node has a set of outstanding transactions it's heard about

Many impossibility results

- **Byzantine generals problem**
- Fischer-Lynch-Paterson (deterministic nodes): consensus impossible win a single faulty node

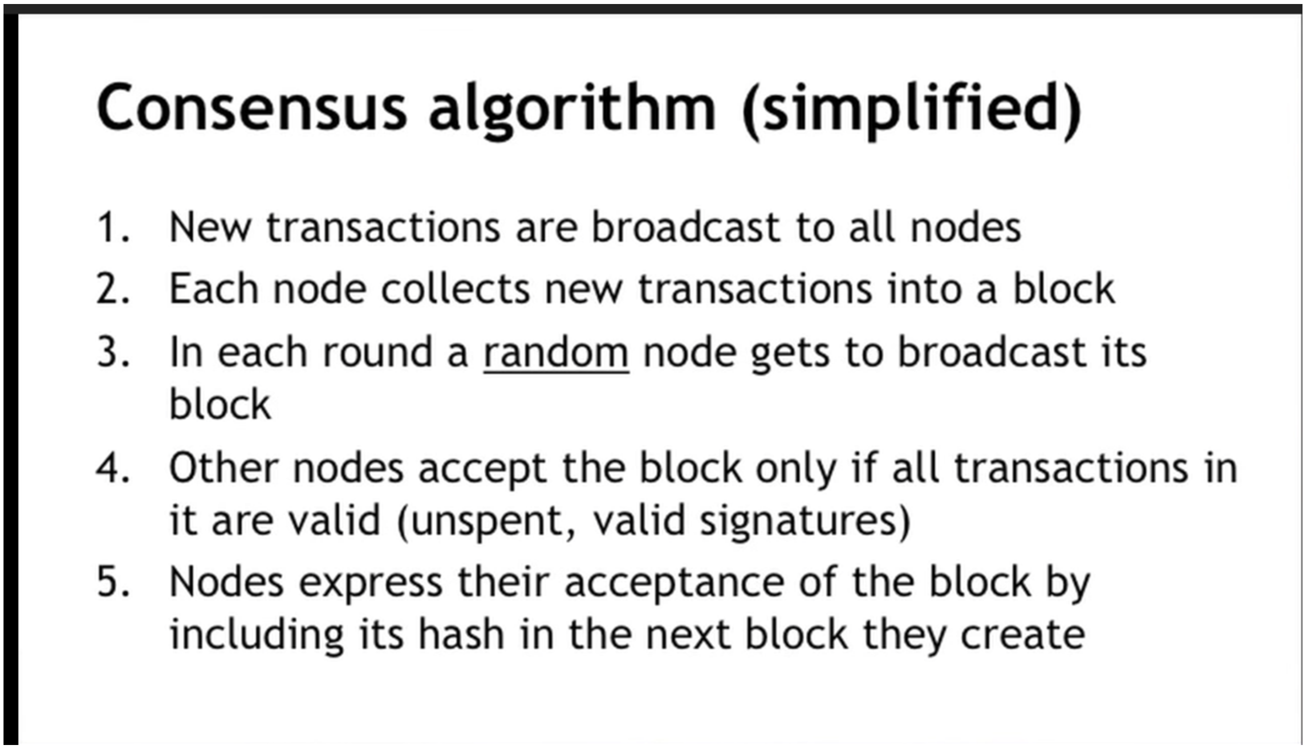
Some well-known protocols
Example: **Paxos, Raft**
Never produce inconsistent result, but can (rarely) get stuck

Some things Bitcoin does differently
Introduce incentives
Embraces randomness
  Does away with the notion of a specific end-point
  Consensus happens over long time scales - about 1 hour

Lecture 2.3 Consensus without Identity: the blockchain

Why identity?
Pragmatic: some protocols need node IDs
Security: assume less than 50% malicious

Why don’t Bitcoin nodes have identities?
Identity is hard in a P2P system — Sybil attack
Pseudonymity is a goal of Bitcoin



Consensus algorithm (simplified)

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create

Recap
Protection against invalid transactions is cryptographic, but enforced by consensus.
Protection against double-spending is purely by consensus.
You’re never 100% sure a transaction is in consensus branch. Guarantee is probabilistic.

Lecture 2.4 Incentives and proof of work
Incentives 1: block reward
Creator of block gets to

- include special coin-creation transaction in the block
- choose recipient address of this transaction

Block creator gets to ‘collect’ the reward only if the block ends up on long-term consensus branch!

Incentive 2: transaction fees
Creator of transaction can choose to make output value less than input value.
Remainder is a transaction fee and goes to block creator.
Purely voluntary, like a tip

Proof of work
To approximate selecting a random node:

Select nodes in proportion to a resource that no one can monopolize

- In proportion to computing power: proof-of-work
- In proportion to ownership: proof-of-stake

PoW property 1: difficult to compute
PoW property 2: parametrizable cost; Goal: average time between blocks = 10 min
Prob(Alice wins next block) = fraction of global hash power she controls
PoW property 3: trivial to verify; Nonce must be published as part of block

Key security assumption
Attacks infeasible if majority of miners weighted by hash power follow the protocol

For individual miner:
Mean time to find block = 10 minutes/fraction of hash power

Lecture 2.5 Putting it all together

Mining economics
If mining reward(block reward + Tx fees) > hardware + electricity cost -> Profit

Complications:
- fixed vs. variable costs
- rewards depends on global hash rate

What can a '51% attacker' do?
Steal coins from existing address? No possible, because attackers have to subvert crypto theory.
Suppress some transactions?

- From the blockchain: Possible
- From the P2P network: Impossible, because attackers cannot control the network

Change the block reward? Not possible, cannot change bitcoin software
Destroy confidence in Bitcoin? Possible