Bitcoin Consensus

Enze “Alex” Liu

a.k.a. TA #2

e7liu@ucsd.edu

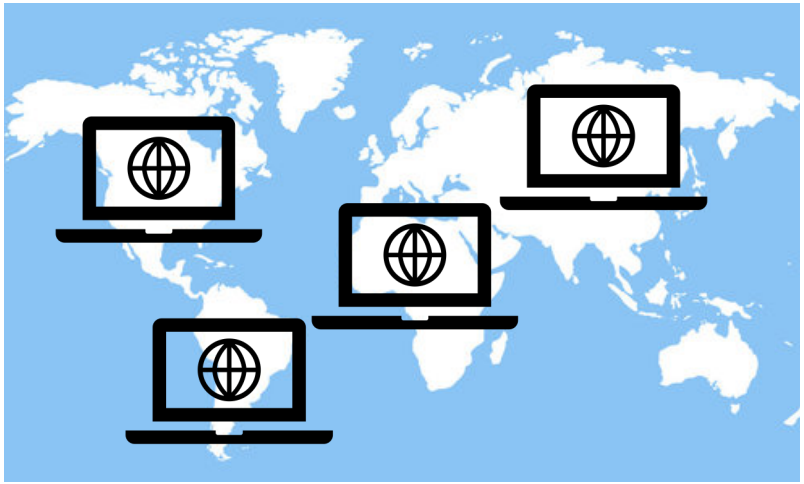
Slides Partially from Dan Boneh

Recap of the Last Lecture

- Wallet
  - Cloud vs Self-hosted
  - Custodial vs Non-custodial
  - Hardware vs Software
- Signing a transaction
  - $Sign\_prviatekey(transaction)$
- How do I tell others about my transaction?
- How to reach consensus?

How do I tell others about my transaction?

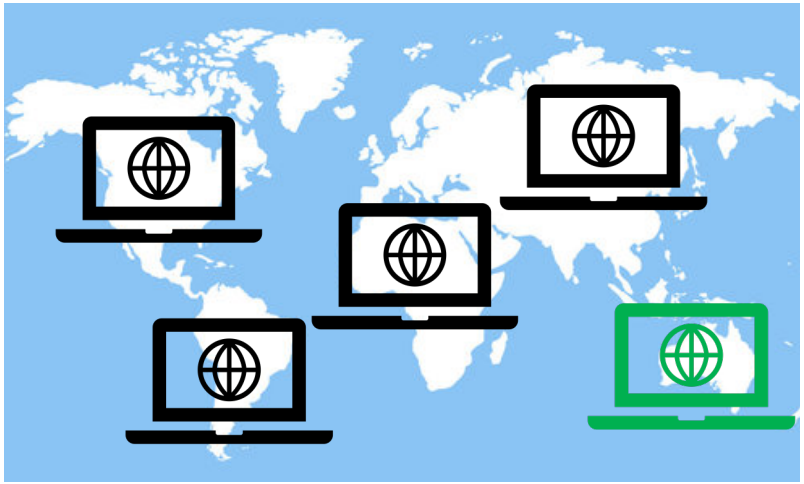
- How do I find others (a.k.a. nodes)?
  - Option 1: centralized, global database of nodes



Node 1	North America
Node 2	South America
Node 3	Africa
Node 4	Asia

How do I tell others about my transaction?

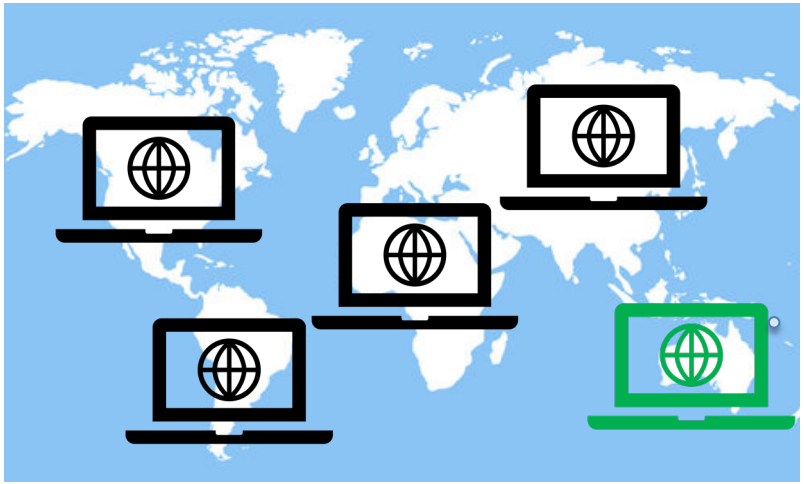
- How do I find others (a.k.a. nodes)?
  - Option 1: centralized, global database of nodes



Node 1	North America
Node 2	South America
Node 3	Africa
Node 4	Asia
Node 5	Australia

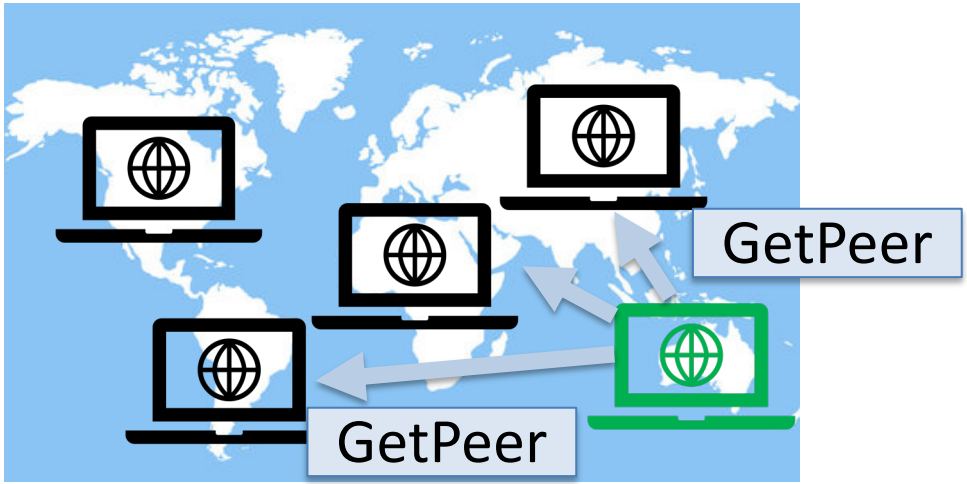
How do I tell others about my transaction?

- How do I find others (a.k.a. nodes)?
  - Bitcoin Solution: decentralized, peer-2-peer (P2P) network



How do I tell others about my transaction?

- How do I find others (a.k.a. nodes)?
  - Bitcoin Solution: decentralized, peer-2-peer (P2P) network



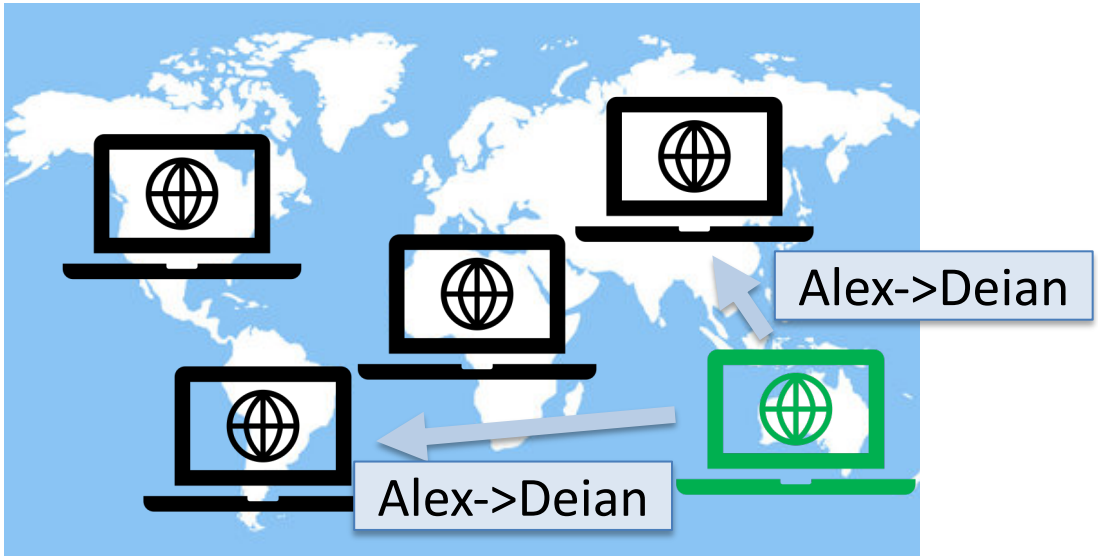
How do I find the first set of peers?

How do I tell others about my transaction?

- How do I find others (a.k.a. nodes)?
  - Bitcoin Solution: decentralized, peer-2-peer (P2P) network
    - Scales
    - No global state
    - No single trusted party
    - Join and leave anytime
    - Problems?

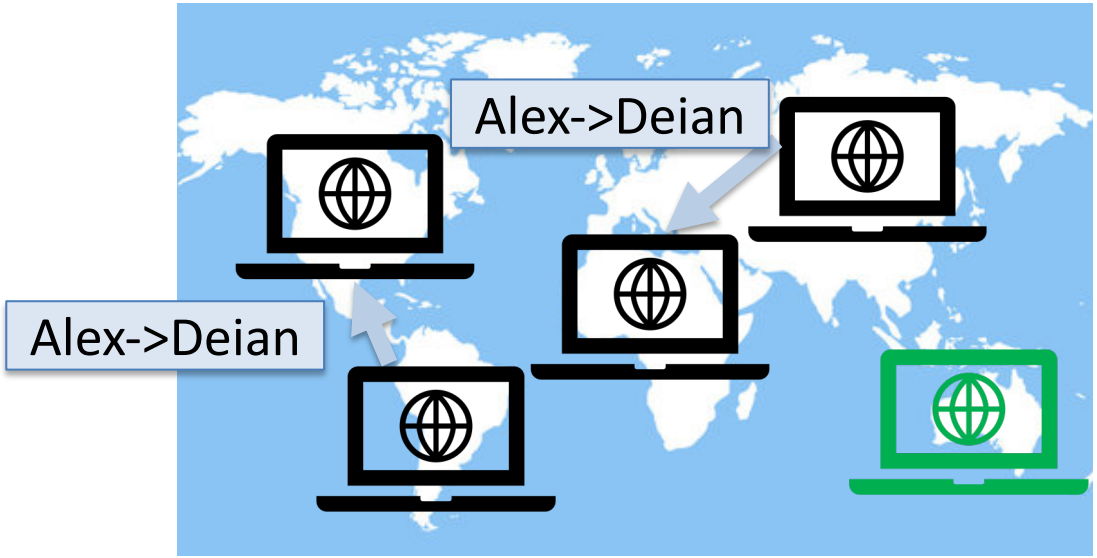
How do I tell others about my transaction?

- How do I tell others about my transaction?
  - The flooding protocol



How do I tell others about my transaction?

- How do I tell others about my transaction?
  - The flooding protocol



Recap

How do I tell others about my transaction?

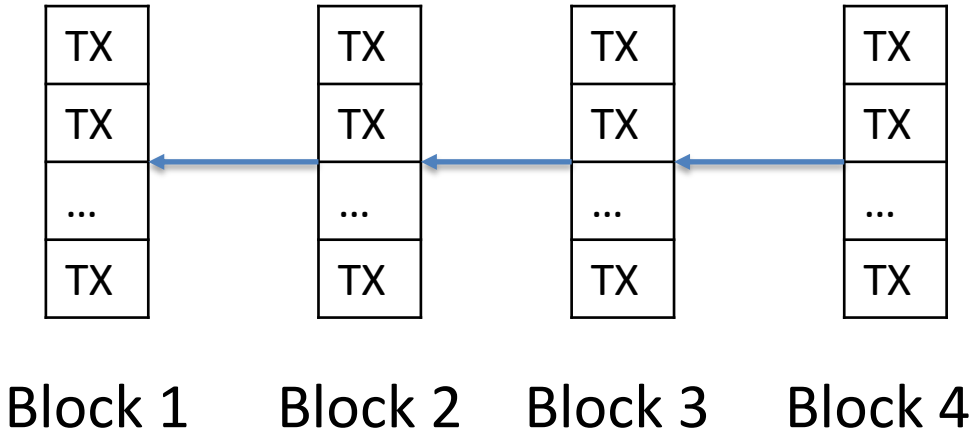
- Discover nodes in a peer-2-peer network
- Broadcast transaction through flooding

How to reach consensus?

- Consensus -- Agreement on transactions that happened
  - How to store transactions?
  - Consensus mechanism

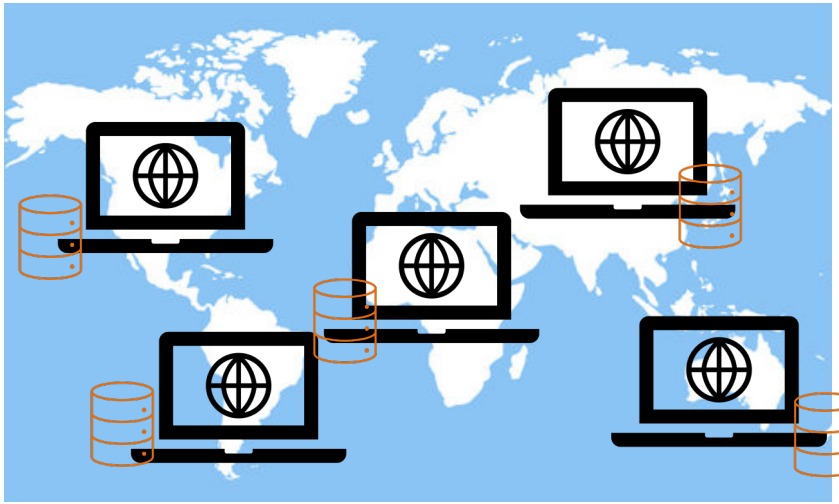
How to reach consensus?

- How to store transactions?
  - Transactions are organized into blocks



How to reach consensus?

- How to store transactions?
  - Transactions are organized into blocks
  - Each node stores a copy of all the blocks



How to reach consensus?

- Consensus Mechanism
  - Producing a new block
  - Reaching agreement on the order of blocks

How to reach consensus?

- Background: The Byzantine Fault Tolerance Problem

Commander

General

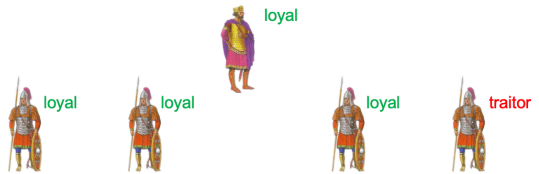
General

General

General

How to reach consensus?

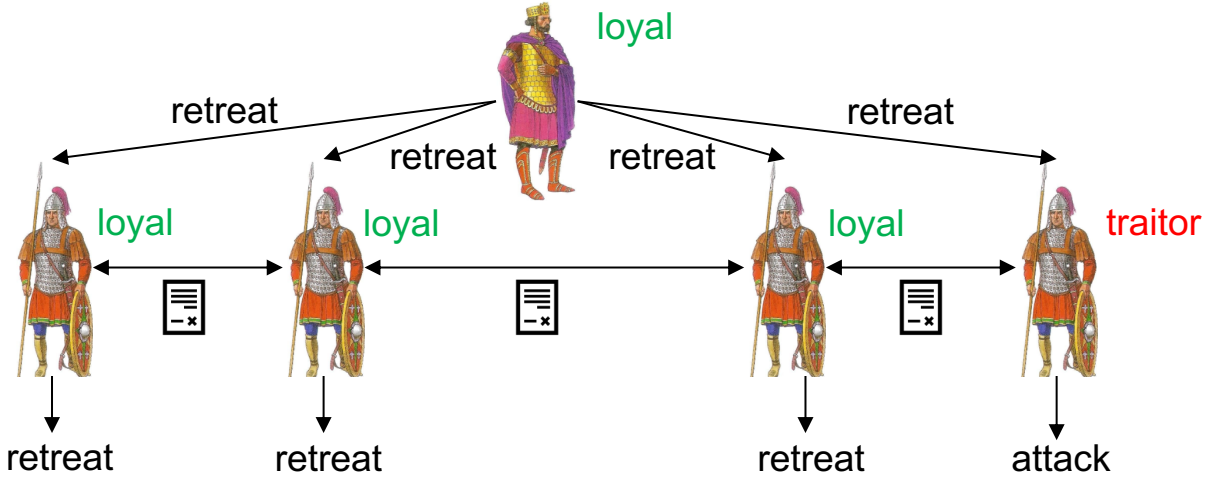
- Background: The Byzantine Fault Tolerance Problem
  - There are n generals (where n is fixed), one of which is the *commander*.
  - Some generals are *loyal*, and some of them can be *traitors* (including the commander).
  - The commander sends out an order that is either *attack* or *retreat* to each general.
  - If the commander is loyal, it sends the *same* order to all generals.
  - All generals take an action after some time.



Byzantine Generals Problem

Goal:

- **Agreement: No** two loyal generals take **different** actions.
- **Validity:** If the commander is loyal, then all loyal generals must take the action **suggested by the commander**.
- **Termination:** All loyal generals must eventually take some action.



Byzantine Generals Problem

Bitcoin Consensus Goal:

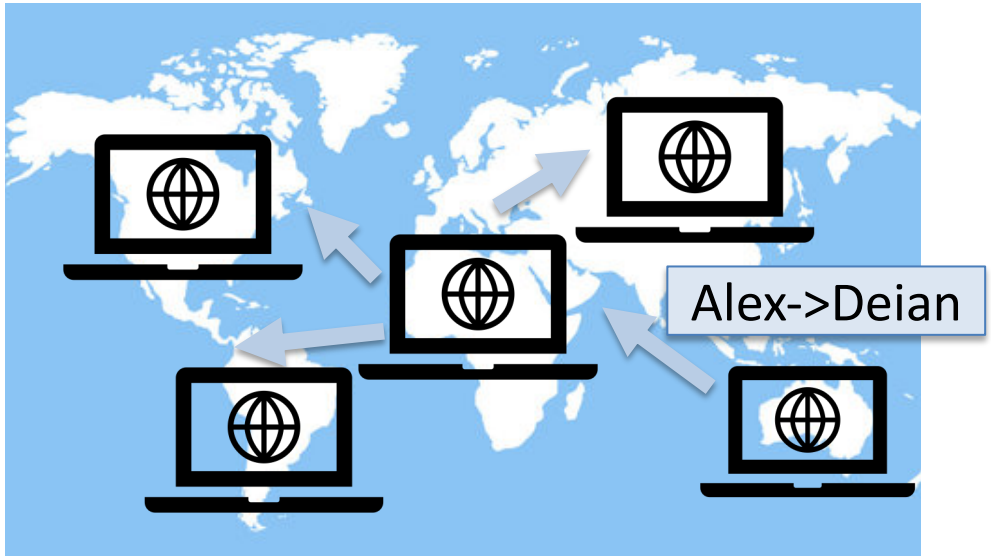
- **Agreement: No** two loyal nodes take **different** actions.
- **Validity:** If the commander node is loyal, then all loyal nodes must take the action **suggested by the commander**.
- **Termination:** All loyal nodes must eventually take some action.

How to reach consensus?

- Consensus mechanism: strawman solution
  - Assume: all nodes have reached agreement on the current state
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, a randomly-selected node proposes its block
  - Other nodes accept the block only if all transactions in it are valid (unspent & valid signatures)
  - Nodes express their acceptance of the block by including its hash in the next block they create

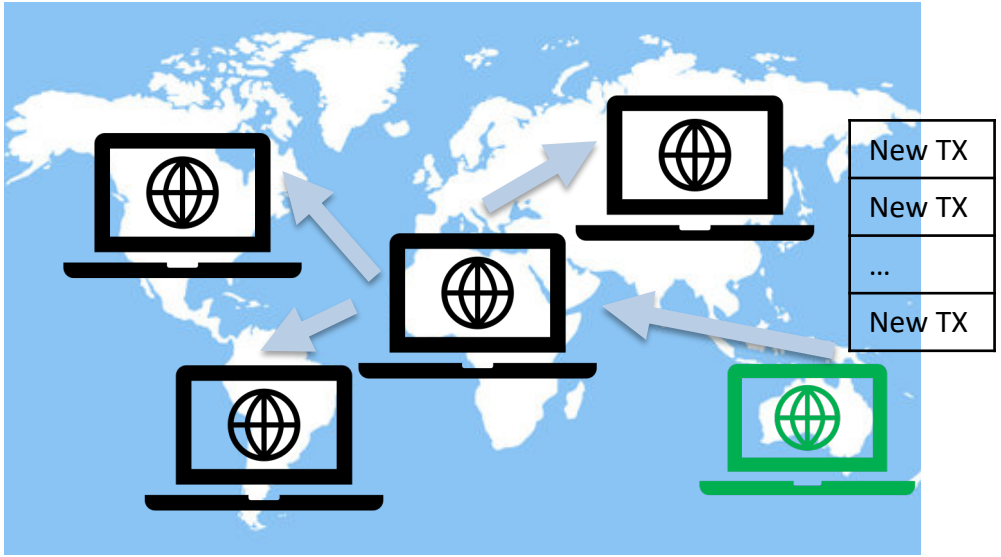
How to reach consensus?

- Nodes broadcast new transactions



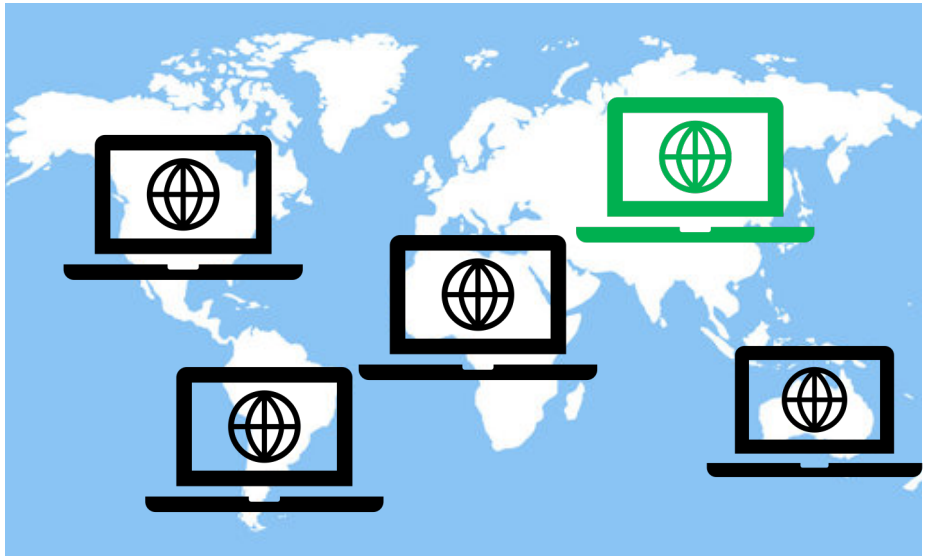
How to reach consensus?

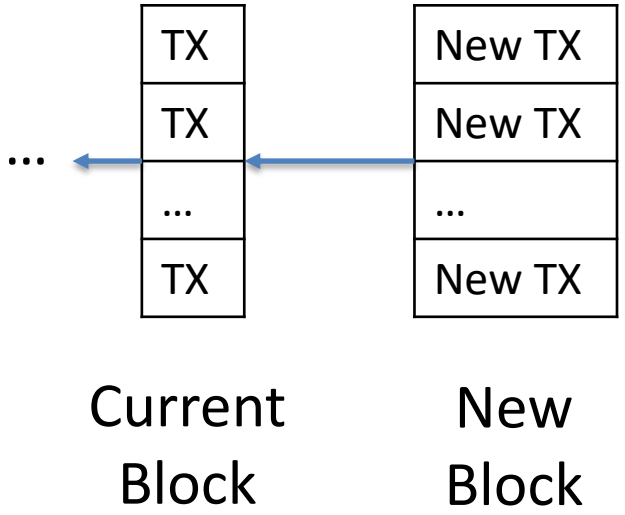
- A randomly-selected node creates and proposes its block



How to reach consensus?

- Nodes validate the block and include its hash in the next block they create





How to reach consensus?

- Consensus mechanism: strawman solution
  - Assume: all nodes have reached agreement on the current state
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, a randomly-selected node proposes its block
  - Other nodes accept the block only if all transactions in it are valid (unspent & valid signatures)
  - Nodes express their acceptance of the block by including its hash in the next block they create

Issues with this solution?

How to reach consensus?

- One Issue - Sybil attack

How to reach consensus?

- Bitcoin Solution – Proof of Work (PoW)
  - Core idea: each node solves a hash puzzle (aka mining)
  - Puzzle:
    - Hash(BlockData||nonce) == 0x000000a2fb…

Hard to solve

Difficulty

Requirements (formally)

- Hard to compute
- Easy to verify
- Parameterizable

Difficulty adjusted every 2016 blocks (roughly 2 weeks) to ensure that a block is produced roughly every 10 minutes

How to reach consensus?

- Bitcoin Solution – Proof of Work (PoW)
  - Core idea: each node solves a hash puzzle (aka mining)
  - Puzzle:
    - Hash(BlockData||nonce) == 0x000000a2fb…
  - Your control of the network:
    - # of nodes → amount of compute power

How to reach consensus?

- Consensus mechanism: revised solution #1
  - Assume: all nodes have reached agreement on the current state
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, the node that solves the puzzle proposes
  - Other nodes accept the block only if all transactions and nonce in it are valid (unspent & valid signatures)
  - Nodes express their acceptance of the block by including its hash in the next block they create

How to reach consensus?

- What if two nodes solve the puzzle at the same time?
  - Conflict resolves until the next block is produced

- What if different nodes have different chains of blocks?
  - The longest chain wins (Formally: the chain with the most difficulty)

How to reach consensus?

- Consensus mechanism: revised solution #2
  - ~~Assume: all nodes have reached agreement on the current state~~
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, the node that solves the puzzle proposes
  - Other nodes accept the block only if all transactions and nonce in it are valid (unspent & valid signatures), and it is the longest
  - Nodes express their acceptance of the block by including its hash in the next block they create

How to reach consensus?

- Consensus mechanism: revised solution #2
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, the node that solves the puzzle proposes
  - Other nodes accept the block only if all transactions and nonce in it are valid (unspent & valid signatures), and it is the longest chain
  - Nodes express their acceptance of the block by including its hash in the next block they create

How to reach consensus?

- What's the incentive to solve the puzzle?
  - The proposing node gets some reward
  - Special TX in each block, named "coinbase", that rewards the node that solves the puzzle
  - Additional: transaction fee

How to reach consensus?

- Consensus mechanism: revised solution #3
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, the node that solves the puzzle proposes and gets some reward
  - Other nodes accept the block only if all transactions and nonce in it are valid (unspent & valid signatures), and it is the longest chain
  - Nodes express their acceptance of the block by including its hash in the next block they create

How to reach consensus?

- Consensus mechanism: revised solution #3
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, the node that solves the puzzle proposes and gets some reward
  - Other nodes accept the block only if all transactions and nonce in it are valid (unspent & valid signatures), and it is the longest chain
  - Nodes express their acceptance of the block by including its hash in the next block they create

Exercise: Agreement? Validity? Termination?

How to reach consensus?

- Consensus mechanism: revised solution #3
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, the node that solves the puzzle proposes and gets some reward
  - Other nodes accept the block only if all transactions and nonce in it are valid (unspent & valid signatures), and it is the longest chain
  - Nodes express their acceptance of the block by including its hash in the next block they create

Q1: Can a malicious node forge a transaction?

How to reach consensus?

- Consensus mechanism: revised solution #3
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, the node that solves the puzzle proposes and gets some reward
  - Other nodes accept the block only if all transactions and nonce in it are valid (unspent & valid signatures), and it is the longest chain
  - Nodes express their acceptance of the block by including its hash in the next block they create

Q2: Can a malicious node deny a transaction?

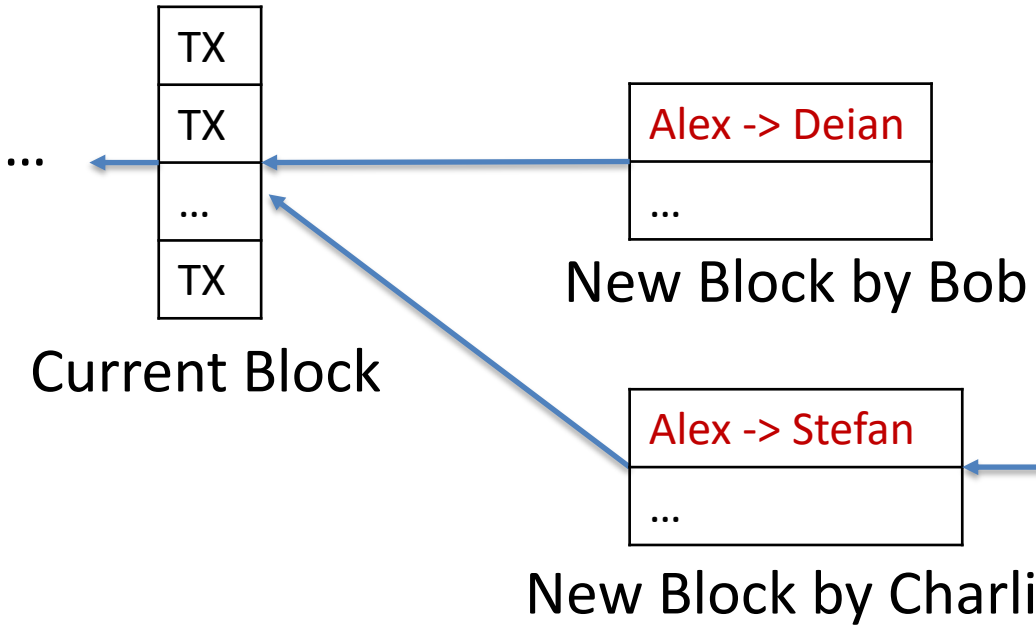
How to reach consensus?

- Consensus mechanism: revised solution #3
  - Nodes broadcast new transactions
  - Each node organizes new transactions into a block
  - In each round, the node that solves the puzzle proposes and gets some reward
  - Other nodes accept the block only if all transactions and nonce in it are valid (unspent & valid signatures), and it is the longest chain
  - Nodes express their acceptance of the block by including its hash in the next block they create

Q3: Can a malicious node double spend?

How to reach consensus?

- Double-spending

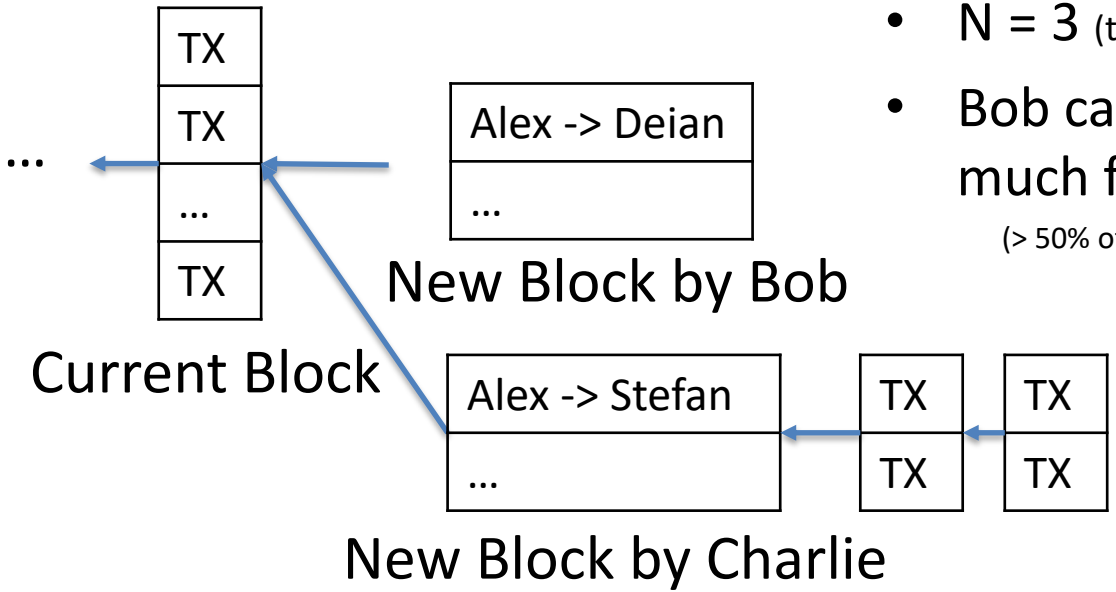


Possible Solutions:

- Confirm when TX first broadcasted
- Confirm when TX confirmed by a blocks
- Confirm when TX is confirmed by N blocks

How to reach consensus?

- 51% attack

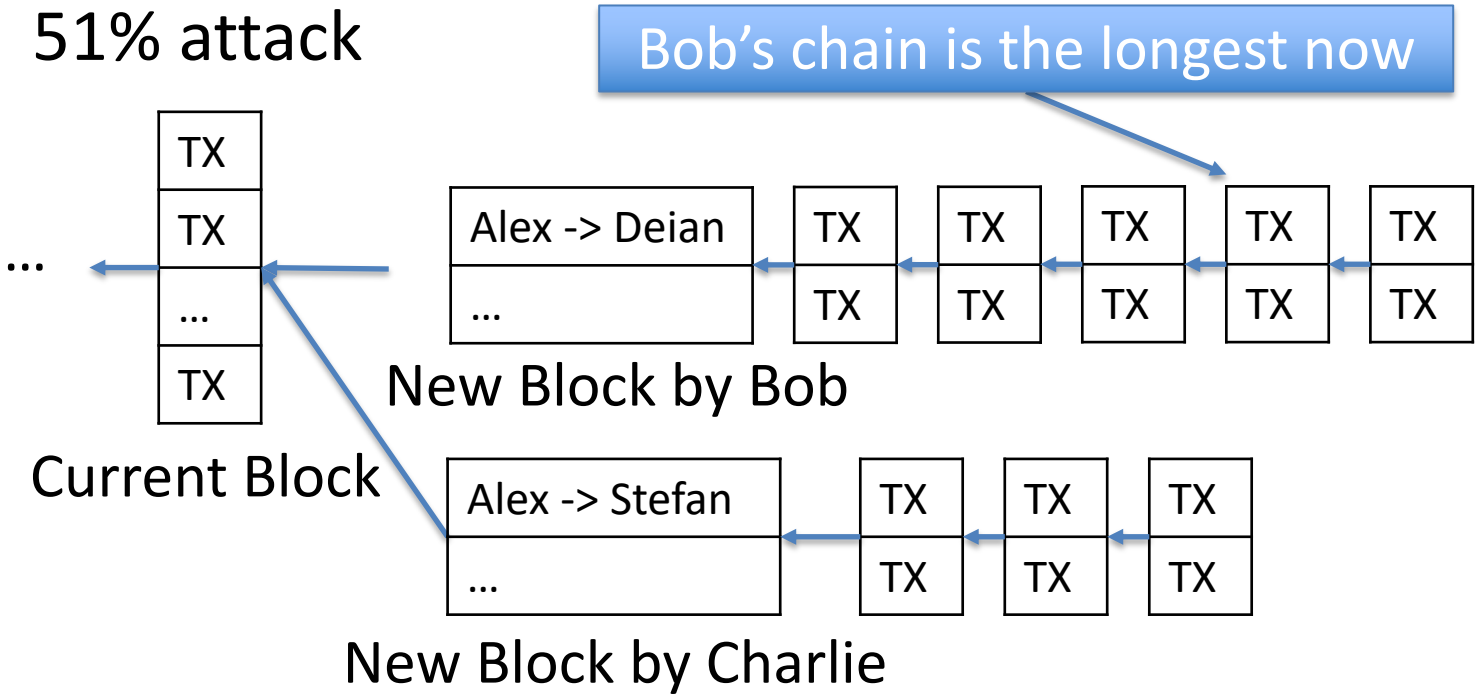


Imagine:

- N = 3 (typically 6)
- Bob can produce a block much faster than Charlie
  (> 50% of the global computation)

How to reach consensus?

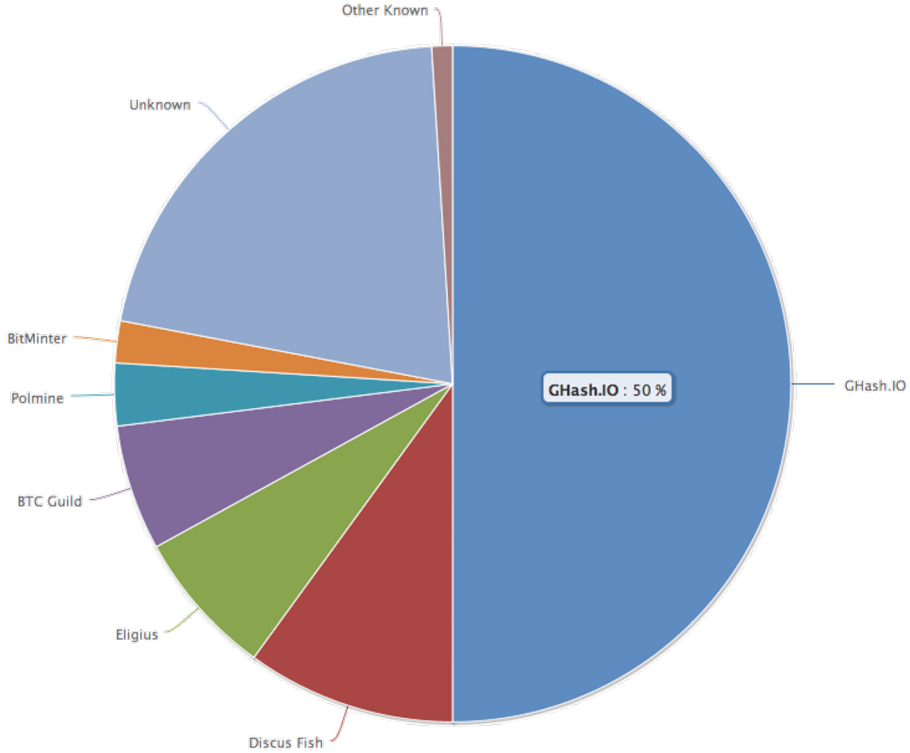
- 51% attack



How to reach consensus?

What can a 51% attacker do?

Does 51% attack happen in practice?



Ghash.IO had >50% in 2014

- Gave up mining power

Recap

- Consensus Mechanism
  - Producing a new block --- the node that solves the puzzle first
  - Reaching agreement on the order of blocks --- longest chain

END OF LECTURE

Next lecture: Ethereum