Lecture 30
Mining Principles

ECE 422: Reliable and Secure Systems Design

UNIVERSITY OF ALBERTA

Instructor: An Ran Chen
Term: 2024 Winter

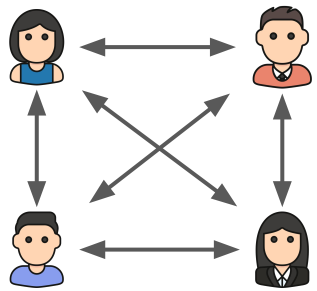
Schedule for today

- Key concepts from last class
  - A basic protocol
  - Challenges in a distributed ledger system
- Who maintain and create new blocks?
  - Proof-of-Work (PoW)
- Mining principles
  - Role of miners
  - Difficulty adjustment + The Longest Chain Rule
  - The 51% Attack

Peer-to-peer network

Assume the network is between Alice, Bob, Carol and Dave

- Alice pays 10 BTC to Bob
- Bob pays 2 BTC to Charlie
- Charlie pays 1 BTC to Dave …



List of transactions

A → B: 10 BTC

B → C: 2 BTC

C → D: 1 BTC

…

Once the list reach ~4,000 transactions

- List of transactions is packaged into a block
- The block is connected to the chain of all prior transactions (i.e., blockchain)

A → B: 2 BTC	A → B: 33 BTC	A → B: 10 BTC
B → C: 9 BTC	B → C: 1 BTC	B → C: 2 BTC
C → D: 3 BTC	C → D: 5 BTC	C → D: 1 BTC
…	…	…

Challenges in a distributed ledger system

There are two main challenges in the basic protocol:

- Why maintain and create new blocks?
  - Fact: Everyone uses the system to make transitions
  - What is the incentive of recording transactions for other people?
    - E.g., roommate agreement, Alice and Bob only make transactions with each other
    - Why should they help create the sticky note (with other roommates' transactions)?
- Who maintain and create new blocks?
  - Fact: Network delays exist, everyone has a ledger with different transactions order
  - Whose ledger do we rely on?
    - E.g., roommate agreement, every roommate has their own ledger
    - Whose notebook do we use to update the sticky note?

Who maintain and create new blocks?

Proof-of-Work (PoW) is a consensus algorithm which is used to verify transactions and create new blocks.

- In PoW, participants (miners) compete to solve complex mathematical puzzles
    - Puzzles are difficult to solve but easy to verify the solution
- First one to find a valid solution gets the rights to create new blocks (and its block creation rewards)

This process of “mining” for the solution is referred to as Bitcoin mining.

Schedule for today

- Key concepts from last class
  - A basic protocol
  - Challenges in a distributed ledger system
- Who maintain and create new blocks?
  - Proof of Work (PoW)
- Mining principles
  - Role of miners
  - Difficulty adjustment + The Longest Chain Rule
  - The 51% Attack

Proof-of-Work as a consensus problem

Byzantine General Problem is a consensus problem:

- Problem: Message may be sent by traitors
- Consistency: All royal lieutenants must execute the same order
- Validity: All royal lieutenants must obey the order of commanding general

Proof-of-Work also needs to deal with a consensus problem:

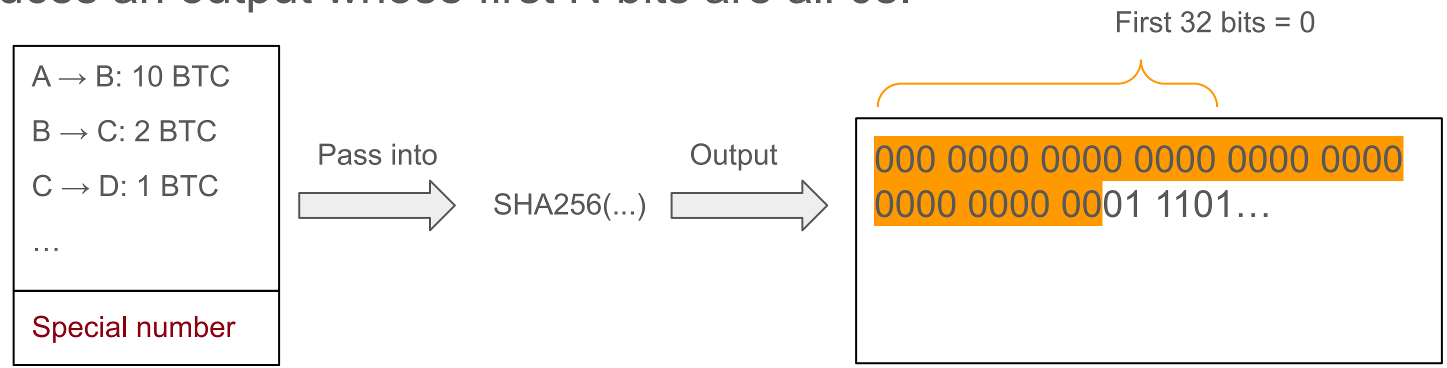
- Problem: Block with fake transactions may be sent by malicious users
- Consistency: All honest nodes record the same blockchain
- Validity: All honest nodes record the blockchain coming from a honest node

Consensus rule: Trust the node that has done the most of work

Mining principle

Proof-of-Work is about finding a special number:

- Combined with the other information from the block and applied SHA256 produces an output whose first N bits are all 0s.



However, this is very difficult!

Review on hash functions

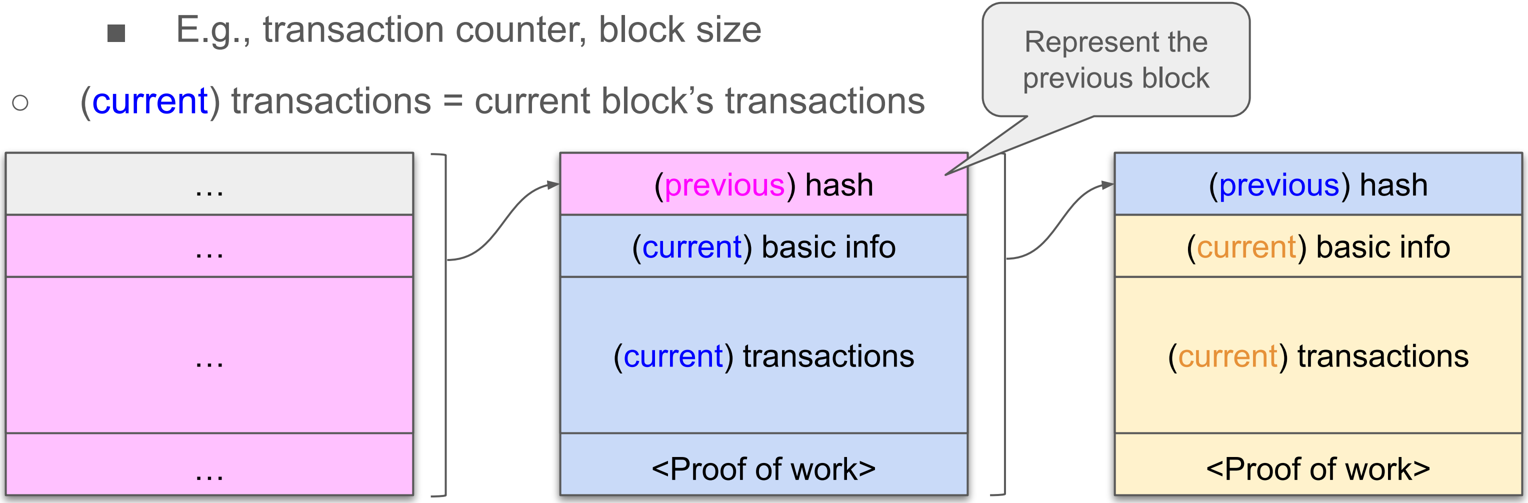
Proof-of-Work uses hash functions to associate the amount of work done with a block of transactions.

- Hash functions are irreversible
  - Analogy to jigsaw puzzles: cutting the paper into one million pieces of jigsaw puzzle and shuffling it
- Easy to apply the hash function, hard to find the original data
  - Analogy to birthday problem: hard to guess the person based on a birthday
- SHA256 produces a hash of 64 hexadecimal characters / 256 bits
  - SHA256(?) = 110 1000 1110 0110 0101 0110 …
  - Brute force is the only solution

Finding the special number

Step 1: Package current block's data into a string

- string = (previous) hash + (current) basic info + (current) transactions
  - (previous) hash: previous block's hash value
  - (current) basic info: current block's basic information
    - E.g., transaction counter, block size
  - (current) transactions = current block's transactions



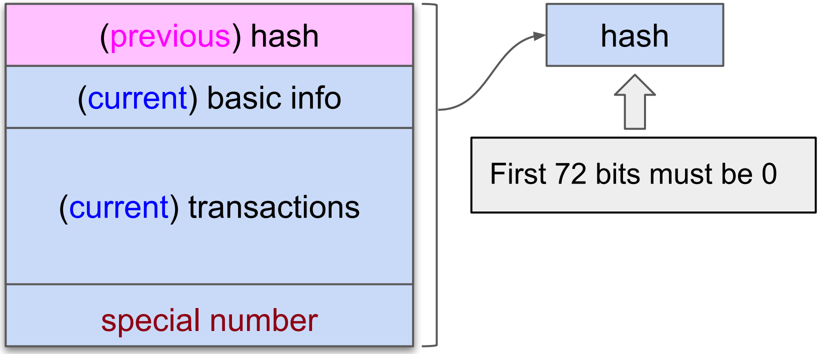
Finding the special number

Step 1: Package current block's data into a string

- string = (previous) hash + (current) basic info + (current) transactions

Step 2: Find a special number

- Add the special number to the string
- Calculate SHA-256(string + special number) = 256-bits number
- Requirement: First 72 bits must be all 0s



Finding the special number

Step 1: Package current block’s data into a string

- string = (previous) hash + (current) basic info + (current) transactions

Step 2: Find a special number

- Requirement: First 72 bits must be all 0s

These two steps are very difficult to complete, but very easy to verify:

- Compute SHA-256(string + special number)
- Check if the has gives 72 leading 0s

This proof of work is tied to the list of transactions

- Any change to the transactions also changes the hash

Mining difficulty

The difficulty of finding the special number is very high:

- Probability of first digit as a 0 is = ½
- Probability of first two digits as 0s is = ½ x ½ = ¼
- …
- Probability of first 72 digits as 0s is = $1/2^{72}$ = 1 out of $(2^{36})^2$
  $\cong$ 1 out of $(69 \text{ billions})^2$

SHA-256(string + special number) $\left\{\begin{array}{l}\text{0000 0000 0000 0000 0000 0000 0000} \\ \text{0000 0000 0000 0000 0000 0000 0000} \\ \text{0000 0000 0000 0000 1010 1110 …}\end{array}\right.$

Schedule for today

- Key concepts from last class
  - A basic protocol
  - Challenges in a distributed ledger system
- Who maintain and create new blocks?
  - Proof-of-Work (PoW)
- Mining principles
  - Role of miners
  - Difficulty adjustment + The Longest Chain Rule
  - The 51% Attack

Bigger picture on mining

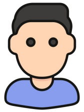
From the Bitcoin miner's perspective:

- Mining is similar to a lottery system
- Everyone try to find the special number first
- Once found, broadcast the blockchain (i.e., ledger) to Bitcoin users

From the Bitcoin user's perspective:

- No need to listen or record other people's transactions
- Listen for block broadcasts from miners
- Compute the hash value to verify the "work done"
- Update their own copy of the blockchain (i.e., ledger)

Example on mining



Bob as a Bitcoin user

Carol as a lucky miner

Step 1) As a Bitcoin user, Bob makes transactions to Alice

Step 2) Carol captures Bob’s transactions

Step 3) Carol finds the special number and broadcasts the blockchain

Step 4) Bob verifies the block and updates his copy of the blockchain

Step 5) Carol receives a small transaction fee

Schedule for today

- Key concepts from last class
  - A basic protocol
  - Challenges in a distributed ledger system
- Who maintain and create new blocks?
  - Proof-of-Work (PoW)
- Mining principles
  - Role of miners
  - Difficulty adjustment + The Longest Chain Rule
  - The 51% Attack

Difficulty adjustment

With more participants and more computing power, the difficulty of the hash problem increases accordingly.

- Bitcoin automatically adjusts the difficulty after every 2,016 new blocks (in other words, every two weeks)
- New difficulty based on the number of participants in the Mining network and their combined computational power

Week 1

Requirement: First 72 bits must all be 0s

→

Week 3

Requirement: First 73 bits must all be 0s

Example of difficulty adjustment

Suppose there are 10,000 mining nodes on the network

- Assuming a processing time of 1.4×10^{13} checks/sec per mining node
- In 10 minutes, total computational power = 8×10^{19} checks
  - 1.4×10^{13} checks/sec x 10,000 nodes x 600 seconds = 8×10^{19} checks
- Given n = 66, 1 out of (2^{66}) = 7×10^{19} hash checks
- Therefore, the difficulty is adjusted to n = 66

New requirement: First 66 bits must be all 0s

Difficulty adjustment

The actual hash difficulty is not about the leading zeros.

- It is about matching a target hash that is updated by the network every two weeks
- To ensure the block time maintains at a constant 10 minutes regardless of the network's computational power

Such adjustment ensures the network's security and stability by regulating the rate at which new blocks are added to the blockchain:

- When more miners join the network, the computational power increases and the difficulty level is adjusted to keep the block generation time constant
- If many miners leave the network, lowering the hash rate, the difficulty decreases

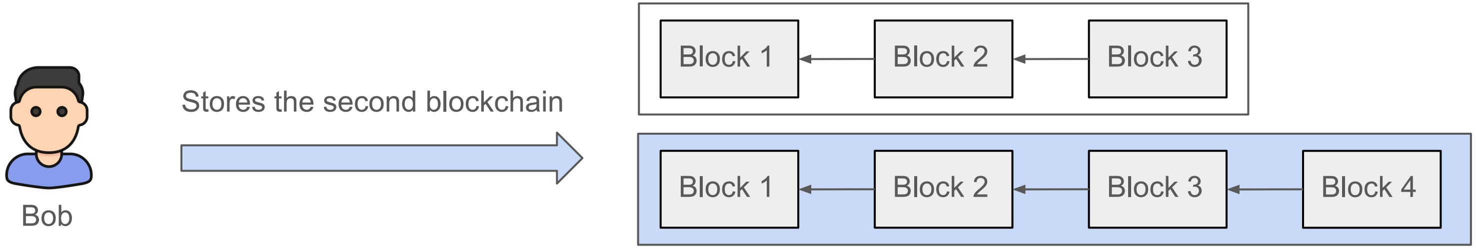
The Longest Chain Rule

The Longest Chain Rule allows every node on the network to agree on the same blockchain (e.g., same transaction history).

- Solving a consensus problem
- Protecting the immutability of the blockchain

Example of application:

- As a Bitcoin user, Bob receives two conflicting blockchains from miners
- Bob must always use the longest blockchain (i.e., with the most work)



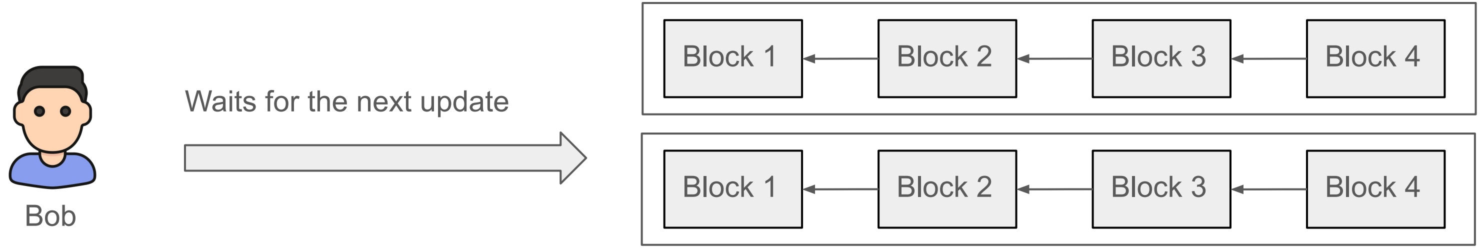
The Longest Chain Rule

The Longest Chain Rule allows every node on the network to agree on the same blockchain (e.g., same transaction history).

- Solving a consensus problem
- Protecting the immutability of the blockchain

Example of application:

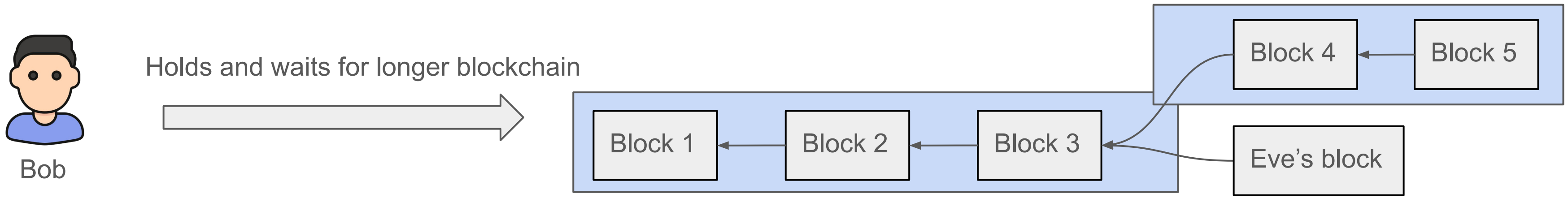
- For blockchains with the same length, Bob waits for the next block that makes one of blockchain longer



Why Proof-of-Work works?

Suppose Eve tries to send a block with fraudulent transactions:

- Eve first needs to find the special number based on the fraudulent transactions before everyone else, and broadcasts the blockchain
- Bob verifies the blockchain and copies it over
- However, Bob continues to listen to the broadcast
    - Any longer blockchain will replace the current one
    - For Bob to keep Eve's blockchain, Eve needs to keep extending the blockchain



Schedule for today

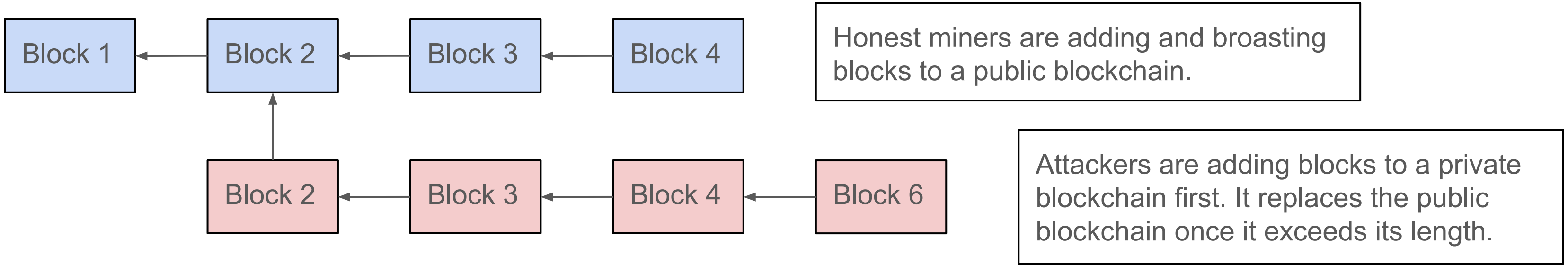
- Key concepts from last class
  - A basic protocol
  - Challenges in a distributed ledger system
- Who maintain and create new blocks?
  - Proof-of-Work (PoW)
- Mining principles
  - Role of miners
  - Difficulty adjustment + The Longest Chain Rule
  - The 51% Attack

The 51% Attack

Now assuming Eve owns 51% of the total computational power on the network

- Theoretically, Eve has the power to alter the blockchain
- By always creating the longest blockchain
- This assumption is known as The 51% Attack

A 51% Attack is an attack performed by a group of miners who control more than 50% of the network's mining power.



The 51% Attack

How it works? Attackers with majority network control the blockchain

- Interrupt the recording of new blocks
- Rewrite parts of the blockchain and reverse their own transactions

However, in real-life settings

- Only smaller networks can be targets for 51% attacks

While possible, this is incredibly costly for the attacker:

- Great amounts of computing power (cost of electricity)
- Honest miners will stop mining (no rewards)

Recap on mining principle

Mining is about creating a new block and verifying the transactions:

- First miner to find the special number gets to create the new block
  - Each block is represented by SHA-256(string + special number)
- Transactions are considered verified once the miner solves the hash problem
  - Proof-of-Work
- Difficulty of the hash problem is based on the total computational power in the network
  - Difficulty adjustment

What happens when a malicious node (pretending to be a Bitcoin user) broadcasts a fake transaction?

Next class: Related concepts to Bitcoin

- Next class: Wednesday, April 3
  - Happy Good Friday and Easter Monday
- Half lecture on Bitcoin
  - Proof-of-Work as a consensus problem
    - Byzantine Fault-Tolerance
  - Transactions recordings as an integrity problem
    - Digital signatures
- Half lecture on Automated Testing
  - Overview of learning objectives + Demo