08. Fundamentals of Blockchain Technologies

이형태

2019학년도 2학기

What is a Blockchain?

- A distributed cryptographic ledger shared amongst all nodes participating in a network, over which every transaction is recorded.
- Blockchain serves as the underlying technology of several cryptocurrencies such as Bitcoin.
- The concept and its implementation was created in 2008/2009 and announced in a 9-page paper written by Satoshi Nakamoto.

What is a Blockchain? (Cont.)

Ledger

The foundation of accounting, as ancient as writing and money (Mesopotamia $<$ 5000 B.C.).

Cryptographic

The procedures and protocols to append new data to the ledger implies the use of cryptographic techniques.

Distributed

Not a single entity is the owner of the data, but it is replicated in every participant of the network.

What is a Blockchain? (Cont.)

Bitcoin

was the first and most popular *peer-to-peer* **value** exchange network.

Satoshi Nakamoto

is a pseudonym of an anonymous individual or group that developed the idea of Blockchain and Bitcoin.

Basic Advantages of Blockchain

- Suppress the necessity of trusted third-party (i.e. financial institutions and banks).
- Move trust from central authorities to decentralized secure protocol.
- Create an economical system not driven by central institutions.
- Empower people.
- Enable almost immediate transactions.
- Offer lower fees than traditional banking.
- Let people become their own bank.

A Bit More Background

- Since Bitcoin appearance in 2009, several other cryptocurrencies emerged.
- Currently most of them are based on some kind of Blockchain.
- Blockchain provides a **reliable** infrastructure that guarantees at least 2 out of the 3 properties of CIA triad: integrity and availability.

Integrity

By the use of symmetric/asymmetric cryptography (e.g., digital signature, hash pointer, Merkle tree) the integrity of the data is guaranteed.

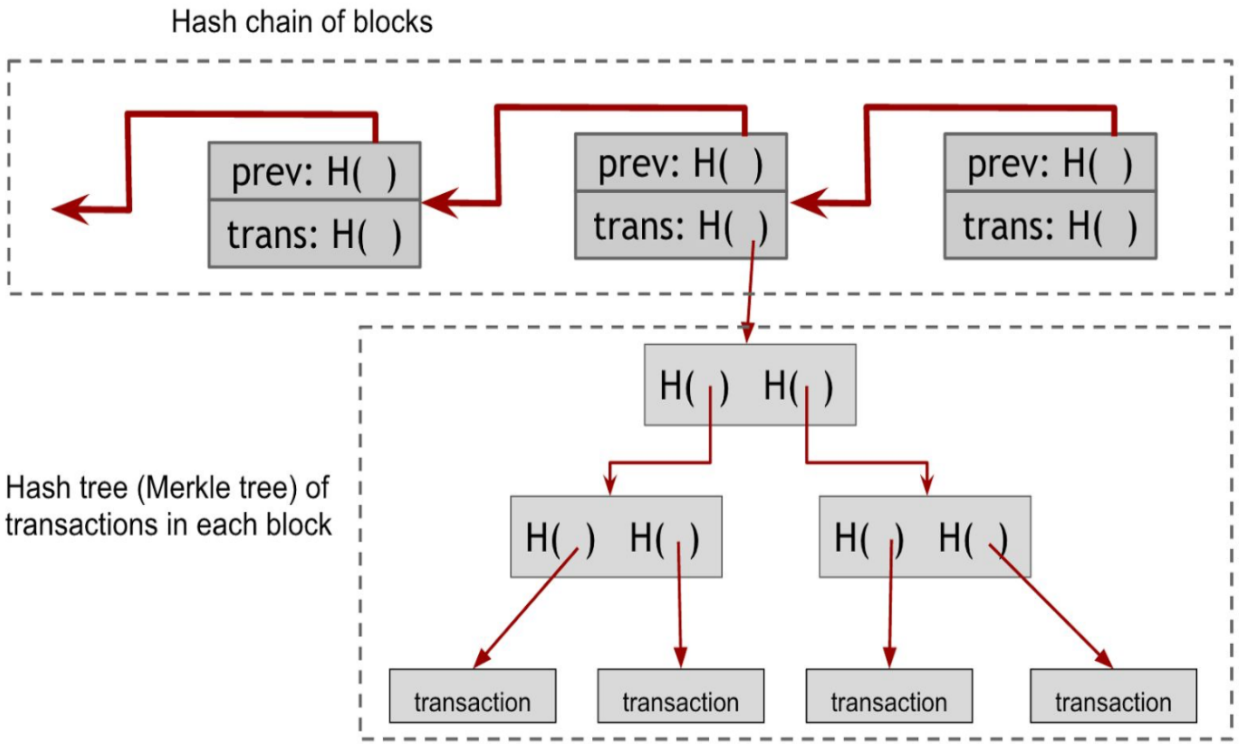
Availability

As a decentralized network, there is no single point of failure.

Confidentiality

It seems that some implementations could provide it as well (e.g. ZCash).

Simplified Bitcoin Blockchain



Basic Components for Bitcoin Blockchain

- Cryptographic hash functions: SHA-256
- Hash pointer
- Merkle tree
- Digital signature: ECDSA
- Public-key as identities

Requirements for Hash Functions in Bitcoin Blockchain

For hash function H,

- **Collision-resistance.** It is infeasible to find two values x, y such that $x \neq y$ and $H(x) = H(y)$.
- **Hiding.** When a secret value r is chosen from a probability distribution that has high min-entropy, then it is infeasible to find x for given $H(r\|x)$.
- **Puzzle friendliness.** For every possible n-bit output value y it is infeasible to find x such that $H(k\|x) = y$ in time significantly less than 2^n if k is chosen from a distribution with high min-entropy.

Application of Puzzle Friendliness

Search Puzzle

A search puzzle consists of

- a hash function H
- a value, id (which we call the puzzle-ID), chosen from a high min-entropy distribution
- and a target set Y

A solution to this puzzle is a value x such that

$$H(id \| x) \in Y$$

- It is a basic idea of block consensus/mining in bitcoin blockchain: Find a nonce *nonce* such that

$$H(nonce \| prev\_hash \| Tx \| Tx \| Tx \| \ldots \| Tx) < target.$$

Hash Pointer

- A hash pointer is a pointer to where data is stored together with a cryptographic hash of the information.

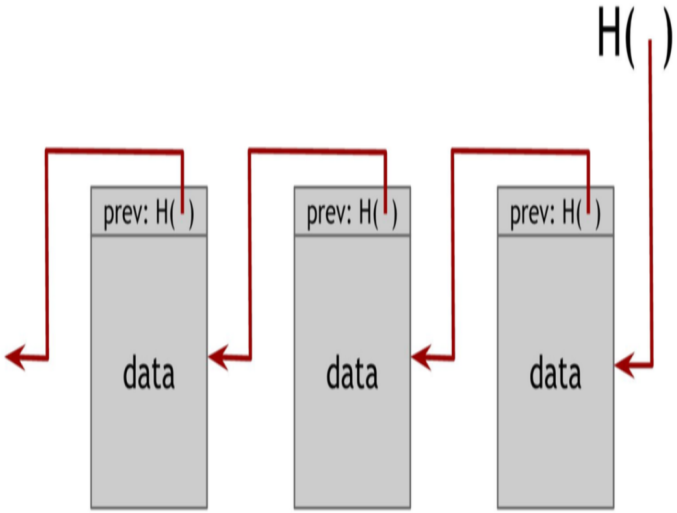


Figure: Hash Pointer in Blockchain

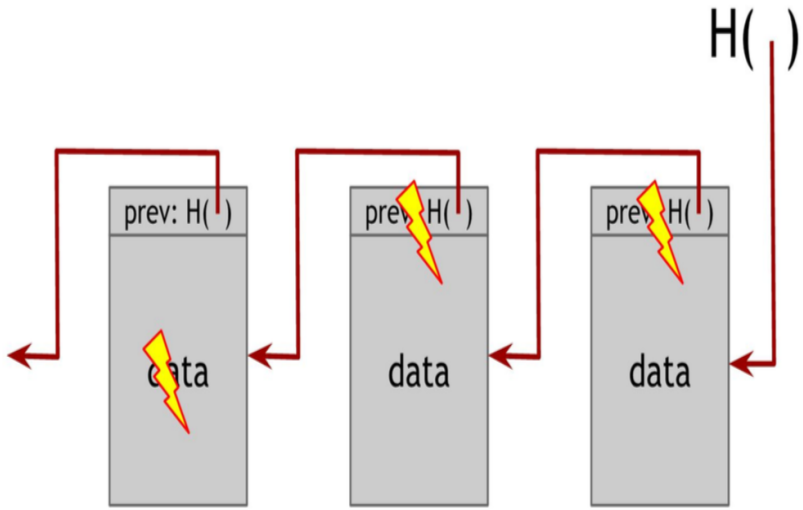
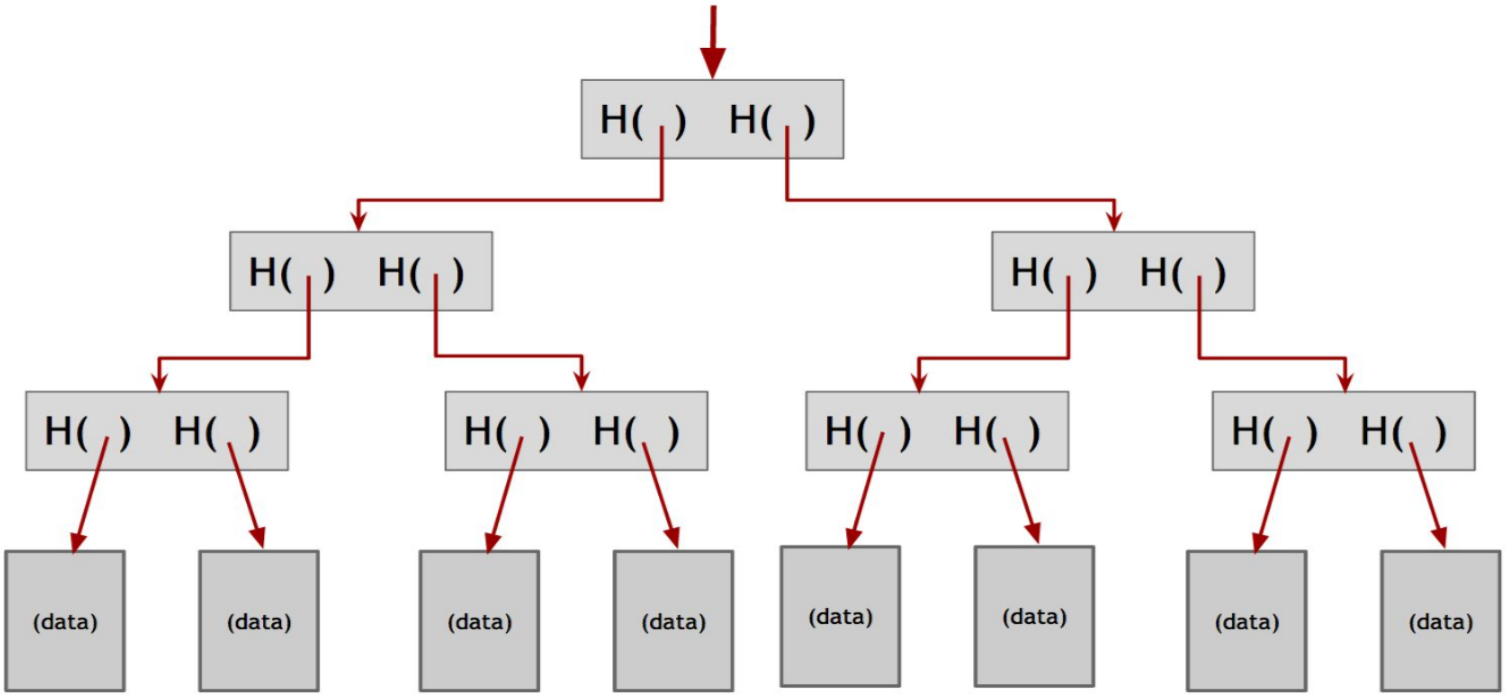


Figure: Tamper-Evident Log

Merkle Tree

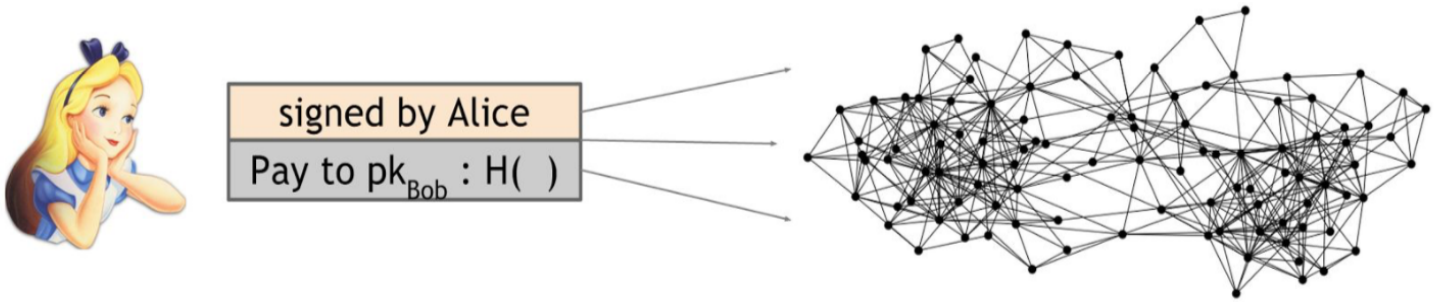
- Invented by Ralph Merkle
- A binary tree with hash pointer



- It provides membership/non-membership proofs.

How does Blockchain Work? - Transaction Work-Flow

1. Clients create and sign transactions (Tx) using their private keys, then they broadcast Tx to the network.



2. Network nodes (miners) receive transactions and store them in the so called mempool.

3. Miners prioritize transactions based on fees, validate and put them in a block.

4. Once successfully created and verified by the network, the block is finally appended to the chain.

How does Blockchain Work? - Consensus/Mining

"It is all about consensus!"

- Blockchain concept is in continuous evolution and new protocols are continuously created to improve the current flaws.
- Earliest implementations (which includes Bitcoin and Ethereum) are using a system called *Proof of Work* (PoW) to validate the transactions.
- Validation is required in order to append a new block of transactions to the chain; preventing things such as double spend.

Concensus/Mining (Cont.)

- The process of block validation is known as mining.
- Lately a new system called *Proof of Stake* (PoS) was developed to address PoW flaws.
- Nodes are motivated to maintain the network with an incentive coming from transaction fees and block rewards.
- Hence, consensus is achieved though these systems (PoW/PoS).

Proof of Work: The Bitcoin case

Block creation (mining)

Participants of a Blockchain network put computational resources to validate transactions by solving the so called cryptographic puzzles.

- Block creation consists in finding a nonce (number) for the block that satisfies a property of the block's hash (a number of leading zeros) known as difficulty.
- This is a trial and error procedure (a kind of brute-force).
- The first node that finds a successful solution announces it to the network.
- The rest of the nodes can easily verify that the solution (and hence the block) is valid.
- If a node acts dishonestly, the rest of nodes will discard the block.

Proof of Work: The Bitcoin case

How?

- Taking the solution (nonce) into the block and computing block's hash (SHA-256) must result in a hash with a leading number of zeroes.

$$H(nonce \| prev\_hash \| Tx \| Tx \| Tx \| \ldots \| Tx) < target.$$

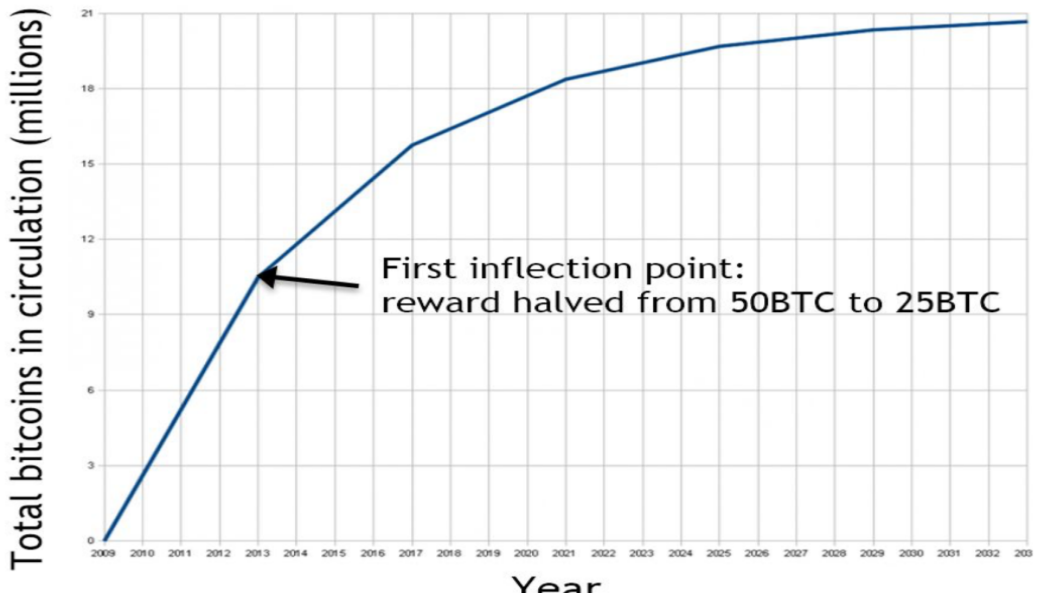
- This is easy to verify for any node.

Drawbacks

- Huge energy consumption.
- Susceptible to a 51% attack.
- Democratization of the network (hardware, electricity price,...)

Incentive I: The Bitcoin Case

- Block reward
  - The node that creates a block gets to include a special transaction in that block, called coin-creation transaction.
  - The value of block reward was initially set to 50 BTC.
  - It actually halves every 210,000 blocks.



  - The minor can get a block reward after 6 subsequent blocks.

Incentive II: The Bitcoin Case

- Transaction fees
  - The creator of any transaction can choose to make the total value of the transaction outputs less than the total value of its inputs.
  - The amount of the transaction fees can bring the priority over other transactions to add into the block.
- Minor profits if (mining reward)$>$ (mining cost) where
  - mining reward $=$ block reward $+$ transactions fees
  - mining cost $=$ hardware cost $+$ operating costs (electricity, cooling, etc.)

Proof of Stake

Given the aforementioned problems that PoW presents, the new Proof of Stake (PoS) model was developed.

Block creation (forging)

Participants of the network stake an amount of currency they hold (a kind of deposit) to be able to forge and send a block to the network.

- The next block creator (called forger) will be chosen randomly following certain criteria.
- The forger verifies transactions, forges a new block and sends it to the network.
- As in PoW, new block is added to the chain and forger (minor) receives transaction fees (and its stake back).
- If the forger acts dishonestly, the rest of nodes will discard the block and forger will lose the stake.

Advantage of Proof of Stake

Pros

- A way more energy efficient: there are no computational resources required.
- More democratization and hence decentralization.
- Security: Purchasing more than half of the coins is likely more costly than acquiring 51% of PoW hashing power.

Several proposals have been presented, studied and even implemented but PoS still faces some challenges that must be addressed.

References

[NBF+16] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016. (Most pictures in these slides come from this reference.)

[LLS18] 이경현, 이임영, 신상욱 역, 비트코인과 암호화폐 기술, 한티미디어, 2018.