Consensus Algorithms for Blockchain

Junsu Lim, Gwangjin Wi

Information and Communication Engineering
DGIST

Contents

Introduction

- Consensus is a fundamental problem in blockchain.
- With the advent of blockchain technology, a renewed interest has arisen in developing distributed consensus algorithms suitable for blockchain networks.

- Blockchain is a distributed system that relies upon a consensus algorithm, ensuring the *safety and *liveness of the blockchain network.
  - *Safety: nothing wrong happens.
  - *Liveness: the protocol can make progress even if the network conditions are not ideal.

Introduction

- A fundamental requirement in a consensus algorithm is that it must be fault-tolerant.
  - *fault-tolerant: it must be able to tolerate a number of failures in a network and should continue to work even in the presence of faults.

- Assumption:

➢ Blockchain is an asynchronous system; there is no upper bound on the communication and processor delays.

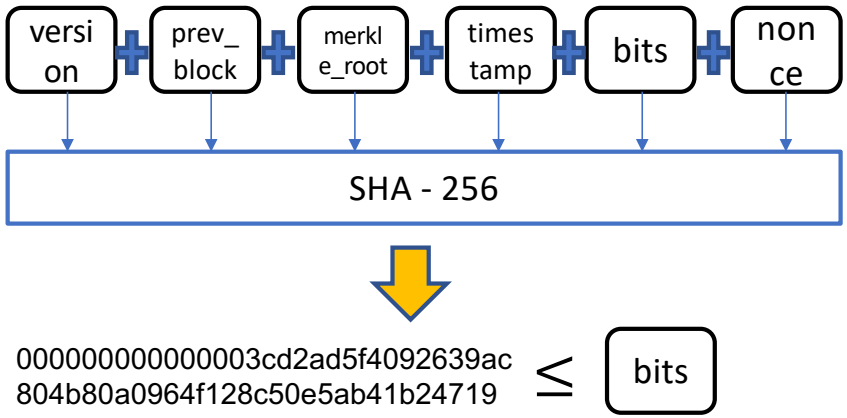
➢ Asynchronous systems are designed to run on asynchronous networks without any timing assumptions.

➢ Asynchronous systems are characterized by the unpredictability of message transfer delays and processing delays(the input load is unpredictable.)

Proof of Work (PoW)

- Basic algorithm
  - Proof-of-work is the process of obtaining a valid hash value to maintain the blockchain.
  - A valid hash value ≤ Difficulty

구분	이름	크기	설명
헤더 (80 bytes)	version	4 bytes	프로토콜 버전
	prev_block	32 bytes	이전 블록의 해시값
	merkle_root	32 bytes	거래 목록으로부터 생성된 머클 트리의 루트 해시값
	timestamp	4 bytes	블록이 생성된 대략적인 시각
	bits	4 bytes	작업증명 알고리즘의 난이도 목표
	nonce	4 bytes	작업증명 성공시 사용된 무작위 난수값



Proof of Work (PoW)

- Basic algorithm
  - Pseudo code of PoW

```
Alg ( version, prev_block, merkle_root, timestamp, bits, nonce  )

1. for nonce = 1 to 2^32
2.   m = version + prev_block + merkle_root + time stamp + bits + nonce
3.   U = SHA256HashFunction ( SHA256HashFunction( m ) )
4.   if U < bits
5.     return nonce
```

Proof of Work (PoW)

- Performance analysis
  - T_b^{PoW} : the average time to generate a new block in PoW
  - $U \leq \frac{1}{D} \leq 1$, U : the value obtained by hash operation, D is the target difficulty
  - $P\{T \leq t\} = P\{N \leq rt\} = 1 - P\{N > rt\} = 1 - \left(1 - \frac{1}{D}\right)^{rt} = 1 - \exp(\log\left(1 - \frac{1}{d}\right) rt)$
  - Assuming $1 - \frac{1}{D} \ll 1, \quad \log\left(1 - \frac{1}{D}\right) \cong -\frac{1}{D}, P\{T \leq t\} \cong 1 - \exp(-\frac{1}{D} rt)$
  - T follows an exponential distribution with mean $\frac{r_i}{D}$
  - The expected mining time for miner i is $E\left[T_{m_i}\right] = \frac{D}{r_i}$
  - With n miners, $T_b^{PoW} = \min\left\{T_{m_1}, T_{m_2}, \ \ldots\ , \ T_{m_n}\right\} = \frac{D}{\sum_{i=1}^{n} r_i}$

Proof of Work (PoW)

- Performance analysis
  - Properties of exponential distribution (memoryless)

$$P\{\text{minimum}(X_1, \ldots, X_n) > x\} = P\{X_i > x \text{ for each } i = 1, \ldots, n\}$$

$$= P(X_1 > t) \ldots P(X_n > t) = \prod_{i=1}^{n} P\{X_i > x\} \qquad \text{(by independence)}$$

$$= e^{-\lambda_1 t} \ldots e^{-\lambda_n t} = \prod_{i=1}^{n} e^{-\mu_i x}$$

$$= e^{-(\lambda_1 + \ldots + \lambda_n)t} = \exp\left\{-\left(\sum_{i=1}^{n} \mu_i\right) x\right\}$$

Proof of Work (PoW)

- Performance analysis
  - Worst-case
  - Best-case
    - O(1) : when the first selected nonce value satisfies the condition
  - Average-case
    - With n miners, $T_b^{PoW} = \min\{T_{m_1}, T_{m_2}, \ \dots\ , \ T_{m_n}\} = \frac{D}{\sum_{i=1}^{n} r_i}$
    - O($\frac{D}{H}$) : H is defined as the hash power of all miners

Proof of Work (PoW)

- Recent research
  - StrongChain: Transparent and Collaborative Proof-of-Work Consensus, In 28th {USENIX} Security Symposium
  - Drawbacks of Bitcoin
    - Strong competition between miners resulted in a high reward variance
    - Because of Bitcoin's deflation, it indicate that Bitcoin may be unsustainable
  - Solution
    - In the StrongChain's design, they employ weak solutions
    - Weak solution's finders are rewarded independently

Proof of Stake (PoS)

- Basic algorithm
  - Similar with PoW, PoS is the process of obtaining a valid hash value to maintain the blockchain
  - A valid hash value $\leq$ Difficulty * bal * t

    bal : denotes the balance of miner in the system

    t : denotes the lifetime of bal from the last winning time to current time
  - Unlike PoW, it is easy to find such values, and the difficulty is determined by own staking

Proof of Stake (PoS)

- Basic algorithm
  - Pseudo code of PoS

```
Alg ( version, prev_block, merkle_root, timestamp, bits, nonce  )

1. for nonce = 1 to 2^32
2.   m = version + prev_block + merkle_root + time stamp + bits + nonce
3.   U = SHA256HashFunction ( SHA256HashFunction( m ) )
4.   if U < bits * balance * lifetime
5.     return nonce
```

Proof of Stake (PoS)

- Performance analysis
  - T_b^{PoS} : the average time to generate a new block in PoS
  - $U \leq \frac{bal*t}{D} \leq 1$, U : the value obtained by hash operation, D is the target difficulty
  - $P\{T \leq t\} = P\{N \leq rt\} = 1 - P\{N > rt\} = 1 - \left(1 - \frac{bal*t}{D}\right)^{rt} = 1 - \exp(\log\left(1 - \frac{bal*t}{D}\right) rt)$
  - Assuming $1 - \frac{bal*t}{D} \ll 1$, $\log\left(1 - \frac{bal*t}{D}\right) \cong -\frac{bal*t}{D}$, $P\{T \leq t\} \cong 1 - \exp(-\frac{bal*t}{D} rt)$
  - T follows an exponential distribution with mean $\frac{r_i*bal_i*t_i}{D}$
  - The expected mining time for miner i is $E[T_{m_i}] = \frac{D}{r_i*bal_i*t_i}$
  - With n miners, $T_b^{PoS} = \min\{T_{m_1}, T_{m_2}, \ldots, T_{m_n}\} = \frac{D}{\sum_{i=1}^{n} r_i*bal_i*t_i}$

Proof of Stake (PoS)

- Performance analysis
  - Worst-case
  - Best-case
    - O(1) : when the first selected nonce value satisfies the condition
  - Average-case
    - With n miners, $T_b^{PoS} = \min\{T_{m_1}, T_{m_2}, \ \dots, \ T_{m_n}\} = \frac{D}{\sum_{i=1}^{n} r_i * bal_i * t_i}$
    - O($\frac{D}{H}$) : H is defined as the hash power of all miners

Proof of Stake (PoS)

- Recent research
  - Ouroboros: A Provably Secure Proof-of-Stake Blockchain
    - The white paper of Cardano ADA
  - Drawbacks of PoS
    - Stake-Grinding Attack
  - Solution
    - Coin Tossing protocol
    - Making all network members participate in random variable generation

Delegated Proof of Stake (DPoS)

- Basic algorithm
  - DPoS system is maintained by an election system for choosing nodes that verify blocks.
- Voting
  - In DPoS consensus, users can either directly vote or give their voting power to another entity to vote on their behalf.
  - witness: These are responsible for validating transactions and creating blocks and are in return awarded associated fees(On average 21-101 witnesses)

Delegated Proof of Stake (DPoS)

- Basic algorithm
- A round in a DPoS blockchain with N block witnesses follows a round-robin order as follows:
  - N block witnesses get elected from the pool of witness' candidates.
  - The kth block witness signs the kth block.
  - A block is finalized when it is voted on by $\left(\frac{2}{3}+1\right)$of block witnesses. In the case of two chains, the longest chain rule is followed. Block added, it could not be reversed.

Delegated Proof of Stake (DPoS)

- Performance analysis
  - Worst-case
  - Best-case
    - When a specific i-node is elected at one time and receives more than $\frac{2}{3}$ of the votes for the proposed block at once.
  - Average-case(Using exponential distribution)
    - a = time it takes for a specific i-node to be elected: $P(X > a) = \int_a^\infty \lambda e^{-\lambda t} dt$, $\lambda = average\ voting\ time$
    - b = Time it takes to receive more than $\frac{2}{3}$ votes: $P(X > b) = \int_b^\infty \lambda e^{-\lambda t} dt$, $\lambda = average\ voting\ time$
    - O($\int_a^\infty \lambda e^{-\lambda t} dt$ + $\int_b^\infty \lambda e^{-\lambda t} dt$)

Delegated Proof of Stake (DPoS)

- Advantages
  - DPoS blockchains have good protection from double-spending.
  - DPoS is more democratic and financially inclusive due to lesser staking amount required by a user/node.
  - DPoS doesn’t require lots of power to run network, which makes it more sustainable.

- Disadvantages
  - Effective operation and decision making of network requires delegators to be well informed and appoint honest witnesses.
  - Limited number of witnesses can lead to centralization of network.

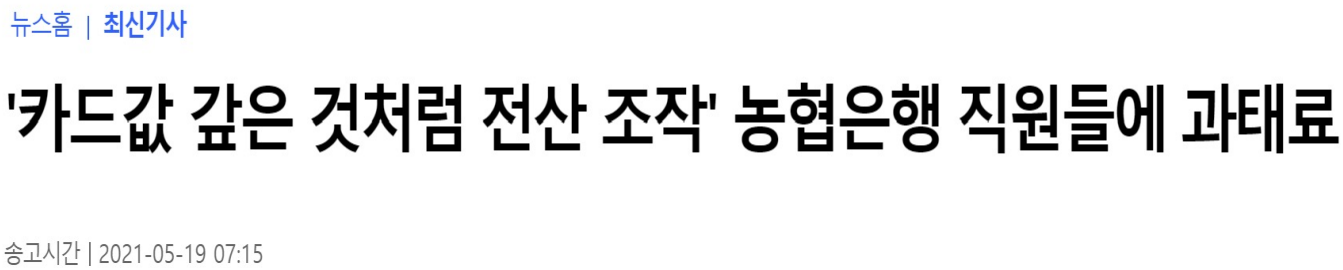
Delegated Proof of Stake (DPoS)

- Recent research

- Let's decentralize using technology other than blockchain
- Representatively,
  - IOTA(using tangle algorithm)
  - ➢ Tangle is an algorithm that removes the block itself to overcome the limitations of the existing blockchain and works so that a new transaction confirms two previous transactions.
  - Hedera Hashgraph(using hashgraph)
  - ➢ Hashgraph is an algorithm that works to deliver gossip to other unspecified nodes rather than a linked list method to overcome the limitations of the existing blockchain.

Conclusion

- The consensus algorithm supports decentralization, a key element in constructing a blockchain.
- Still, poor performance compared to EMV (Europay, MasterCard, Visa) and environmental problems. If so, should we use blockchain to decentralize it?
- The following consensus algorithm is developed to ensure low energy consumption, anonymity, exclusion of centralization, and high TPS (Transaction per second).


뉴스홈 | 최신기사

'카드값 갚은 것처럼 전산 조작' 농협은행 직원들에 과태료

송고시간 | 2021-05-19 07:15

Reference

- Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2020). Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks, 6(4), 480-485.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *www.bitcoin.org*, *23*(4), 552–557.
- Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). Ouroboros: A provably secure proof-of-stake blockchain protocol. In Annual International Cryptology Conference (pp. 357-388). Springer, Cham.
- Szalachowski, P., Reijsbergen, D., Homoliak, I., & Sun, S. (2019). Strongchain: Transparent and collaborative proof-of-work consensus. In 28th {USENIX} Security Symposium ({USENIX} Security 19) (pp. 819-836).
- I. Bashir, Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more, 3rd Edition. Birmingham, England: Packt Publishing, (2020), p.139-181.
- Proof of Stake versus Proof of Work, white paper, and Version 1.0. URL : https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf
- *Frontjang.info*. [Online]. Available: https://frontjang.info/entry/지수분포와-망각성질. [Accessed: 22-May-2021]
- “Delegated proof of stake (DPoS) - GeeksforGeeks,” *Geeksforgeeks.org*, 17-Aug-2020. [Online]. Available: https://www.geeksforgeeks.org/delegated-proof-of-stake/. [Accessed: 22-May-2021]
- ″해시그래프,” *Hash.kr*. [Online]. Available: http://wiki.hash.kr/index.php/%ED%95%B4%EC%8B%9C%EA%B7%B8%EB%9E%98%ED%94%84. [Accessed: 22-May-2021].
- ″탱글 - 해시넷,” *Hash.kr*. [Online]. Available: http://wiki.hash.kr/index.php/%ED%83%B1%EA%B8%80. [Accessed: 22-May-2021].