CS 7172
Parallel and Distributed Computation

Distributed Consensus

Kun Suo

Computer Science, Kennesaw State University

https://kevinsuo.github.io/

Outline

- Computer networks, primarily from an application perspective
- Protocol layering
- Client-server architecture
- End-to-end principle
- TCP
- Socket programming

Revisit Distributed Election

- Distributed election is to select a master node from multiple nodes

- Every node has the right to elect and to be elected

- Most election methods use a majority strategy: a node can only become the master node if it has the approval of most nodes

Revisit Distributed Election

- Distributed election is an example of distributed consensus

- Every node follows the same rule (the majority strategy) to elect and be elected

- Every node gets involved and the results can be trusted

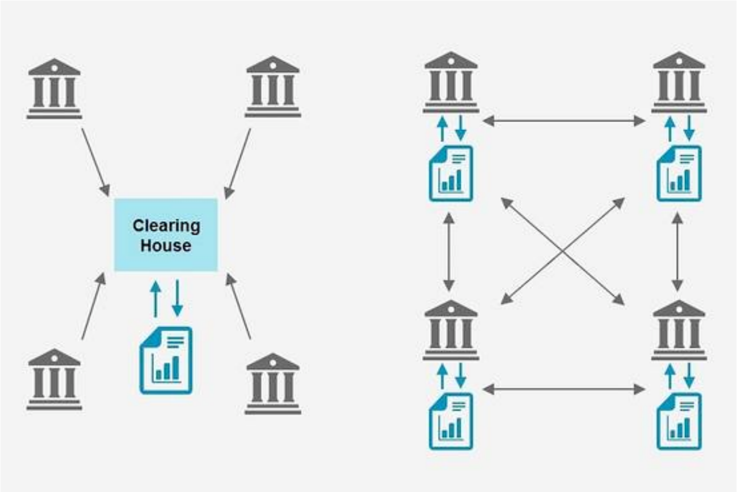
Another Example of Distributed Consensus: distributed accounting

- Centralized accounting:
  - E.g., suppose only one bank exists in U.S.

- Potential problems:
  - The master node is very easy for accounting fraud
  - The master node could be performance bottlenecks
  - Low reliability, e.g., master node fails

Another Example of Distributed Consensus: distributed accounting

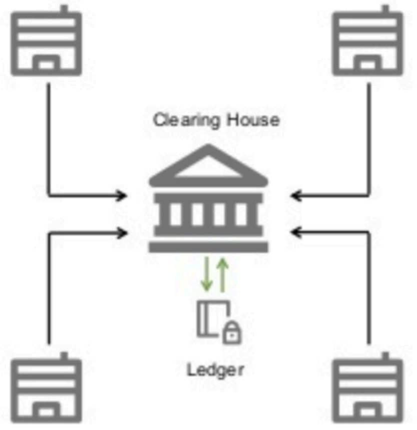
- Distributed accounting:
  - No centralized node
  - Any server that sees one transaction can record this transaction



- Potential benefits:
  - Results are trusted and accurate
  - System is strong and has high reliability

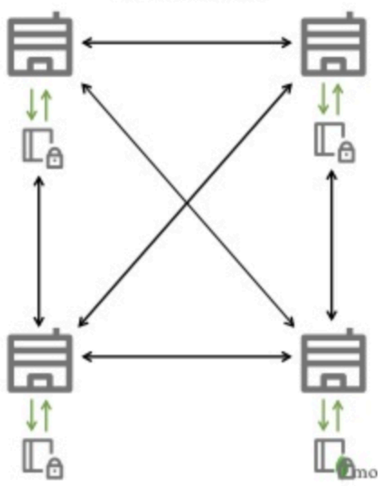
What is Distributed Consensus?

- Example:
  - 5 servers located at Georgia, Florida, Texas, California and New York
  - User A in GA send $100 to user B in TX
  - Traditional solution:
    - A – 100 and B + 100
    - Keep the record at centralized server



What is Distributed Consensus?

- Example:
  - 5 servers located at Georgia, Florida, Texas, California and New York
  - User A in GA send $100 to user B in TX
  - Distributed solution:
    - How to keep the data consistent in each server



Distributed consensus is the process of making all nodes agree on a certain state when multiple nodes can operate or record independently.

Difference between Consistency and Consensus

- Consistency: the data or status presented to the outside is consistent after a series of operations among multiple nodes in a distributed system

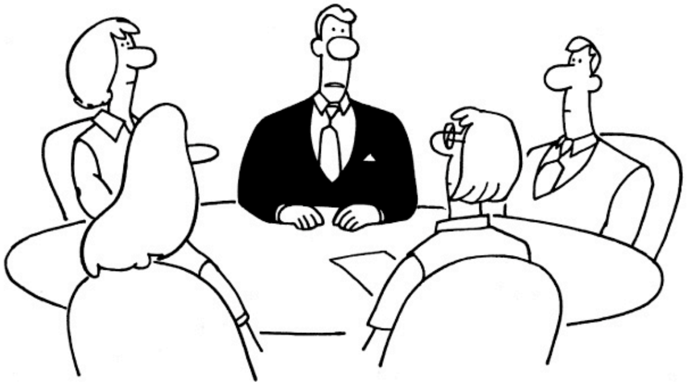
- Consistency refers to the results

- Consensus: the process that multiple nodes in a distributed system reach an agreement.

- Consensus refers to the process

How to Achieve Distributed Consensus?

- Distributed consensus is the process of making all nodes agree on a certain state when multiple nodes can operate or record independently.

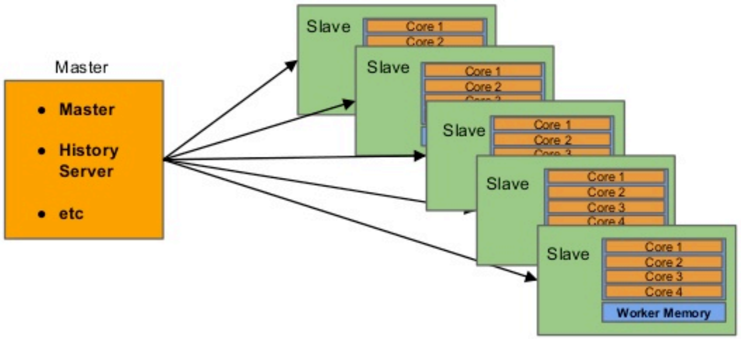


"Whew! That was close! We almost decided something!"

- Solution:
  - PoW (Proof-of-Work)
  - PoS (Proof-of-Stake)
  - DPoS (Delegated Proof of Stake)

1. PoW (Proof-of-Work)

- In distributed election, only one node in the same round of elections could be the master node



- In distributed accounting, for one transaction, only one node can obtain the ***accounting right***, and then reaches ***an agreement*** with other nodes for the accounting results

- Two key points in distributed accounting :
  - Accounting right
  - Agreement

1. PoW (Proof-of-Work)

- PoW algorithm is a mechanism that competes for accounting rights based on the computing power of each node.

- Whoever has stronger computing power will be more likely to obtain accounting rights.

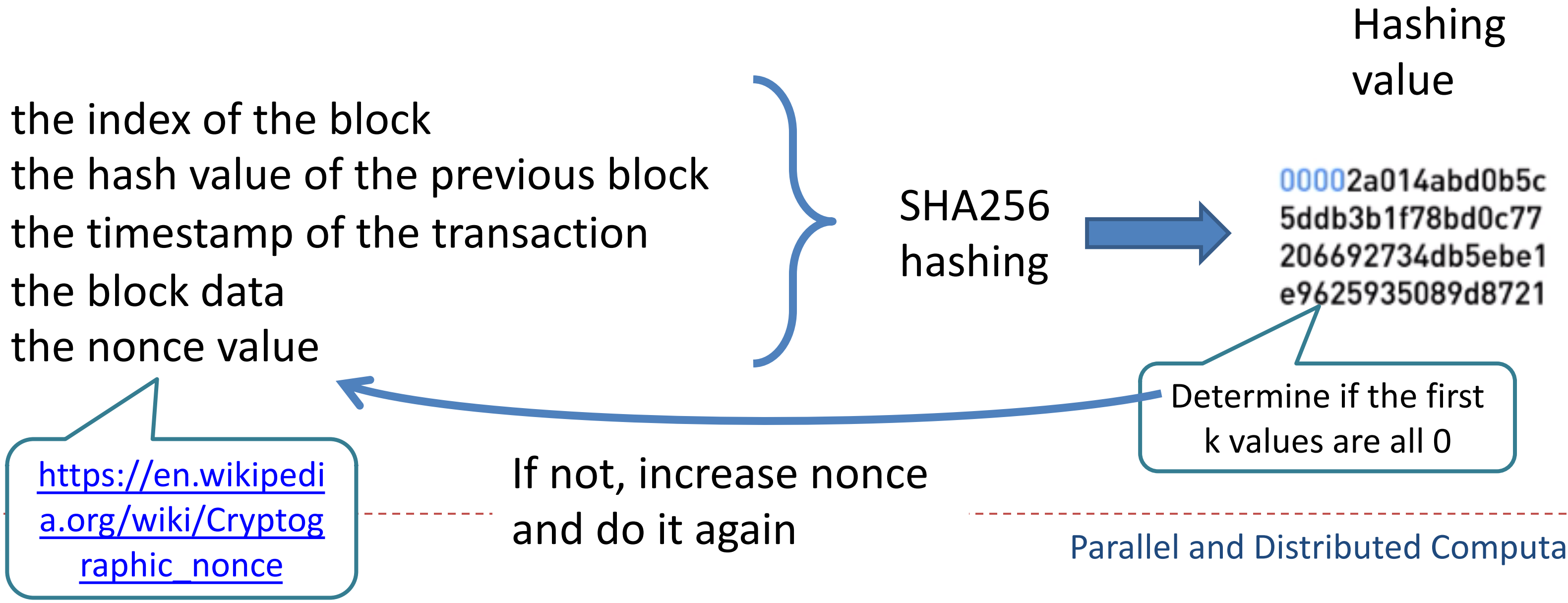
VS

VS

1. PoW (Proof-of-Work)

- How to measure the computing power?
  - Every node has to solve a problem
  - Whoever solves it first has the most computing power

- What is the problem?



the index of the block
the hash value of the previous block
the timestamp of the transaction
the block data
the nonce value

SHA256 hashing

Hashing value

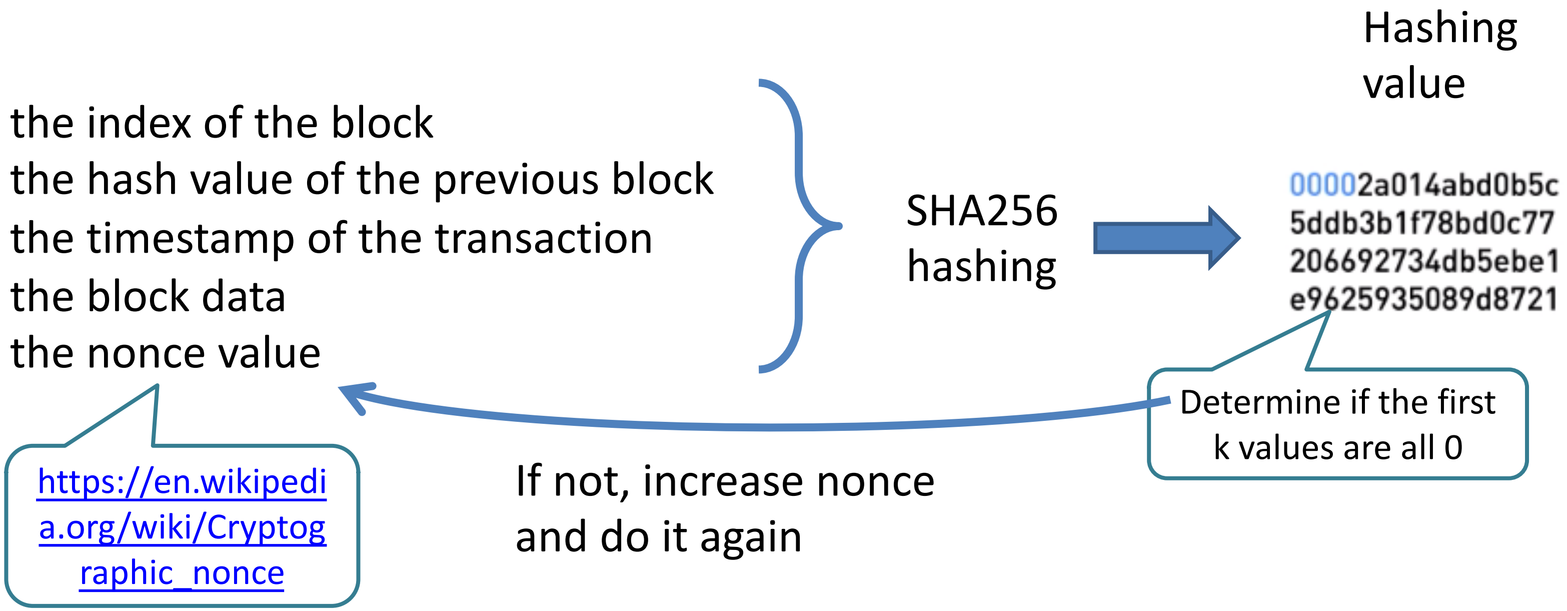
00002a014abd0b5c
5ddb3b1f78bd0c77
206692734db5ebe1
e9625935089d8721

Determine if the first k values are all 0

If not, increase nonce and do it again

https://en.wikipedia.org/wiki/Cryptographic_nonce

1. PoW (Proof-of-Work)



Hashing value

the index of the block
the hash value of the previous block
the timestamp of the transaction
the block data
the nonce value

SHA256 hashing

00002a014abd0b5c
5ddb3b1f78bd0c77
206692734db5ebe1
e9625935089d8721

Determine if the first k values are all 0

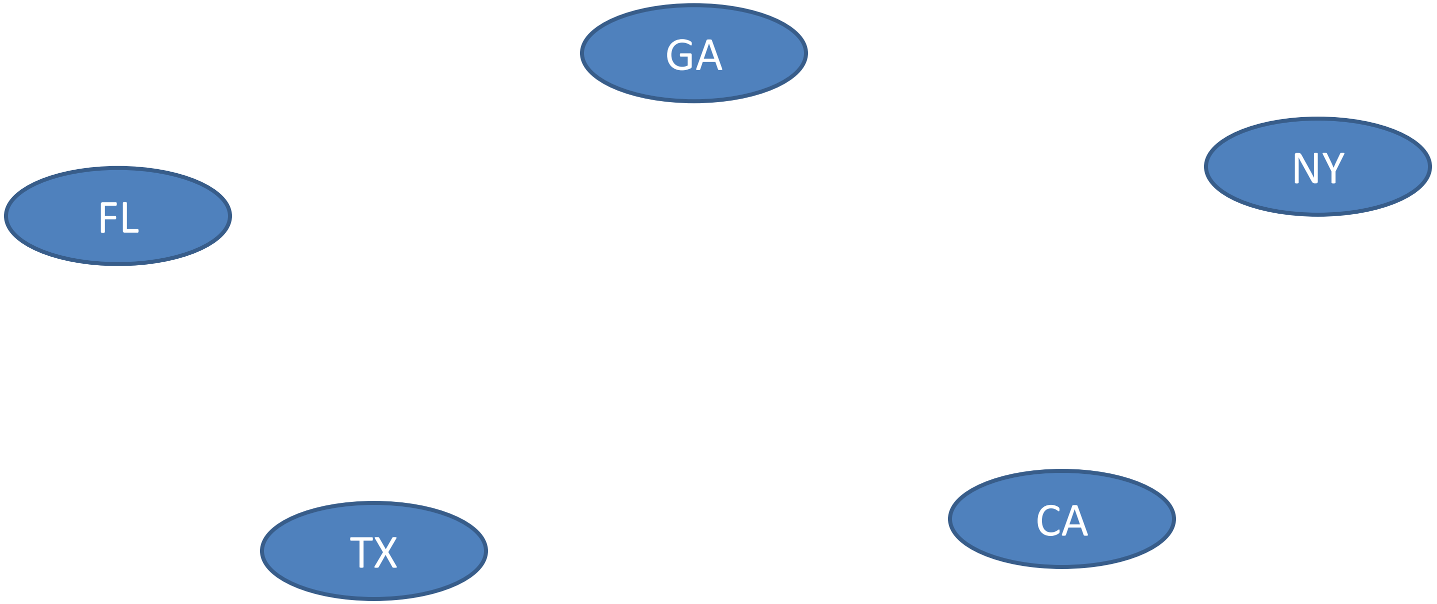
If not, increase nonce and do it again

https://en.wikipedia.org/wiki/Cryptographic_nonce

- Whoever solves it first can get the accounting rights
- After the node gets the right, it updates the transaction and make an agreement with other nodes to make it effective

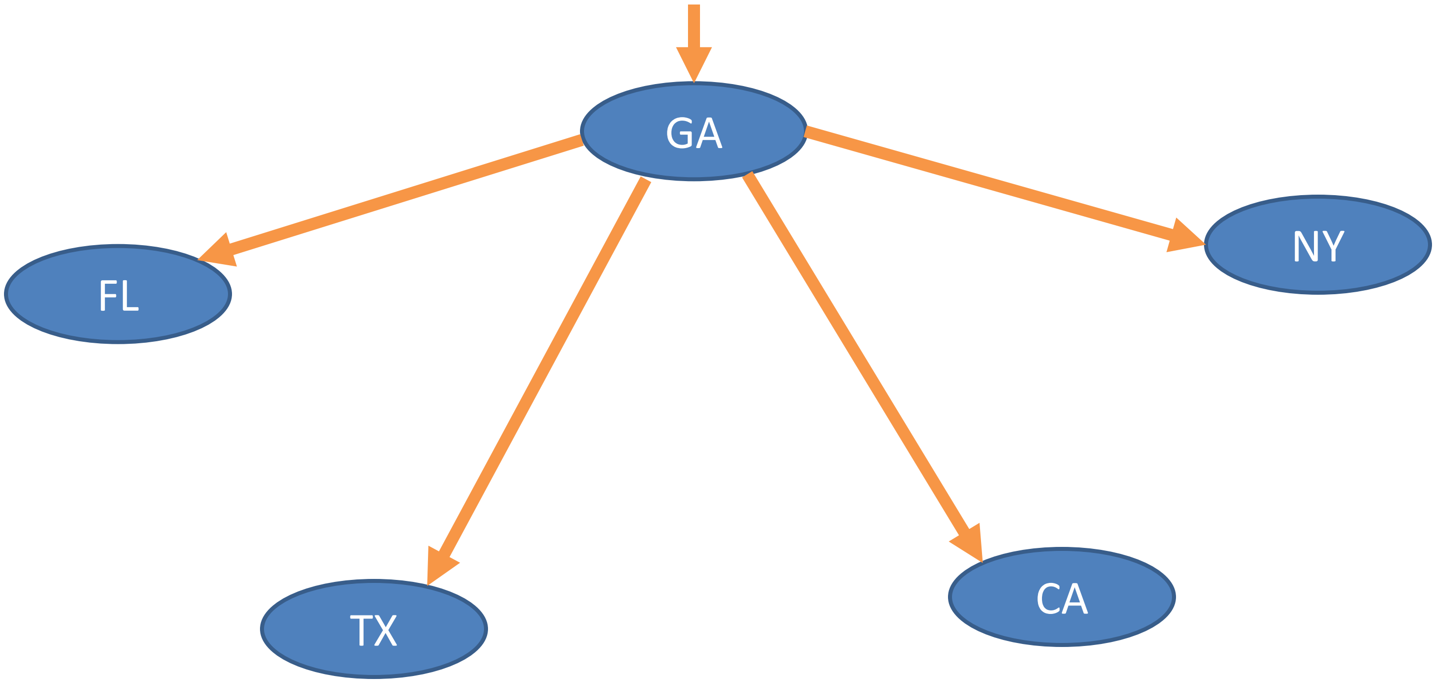
1. PoW (Proof-of-Work)

- Example:
  - 5 servers located at Georgia, Florida, Texas, California and New York
  - User A in GA send $100 to user B in TX



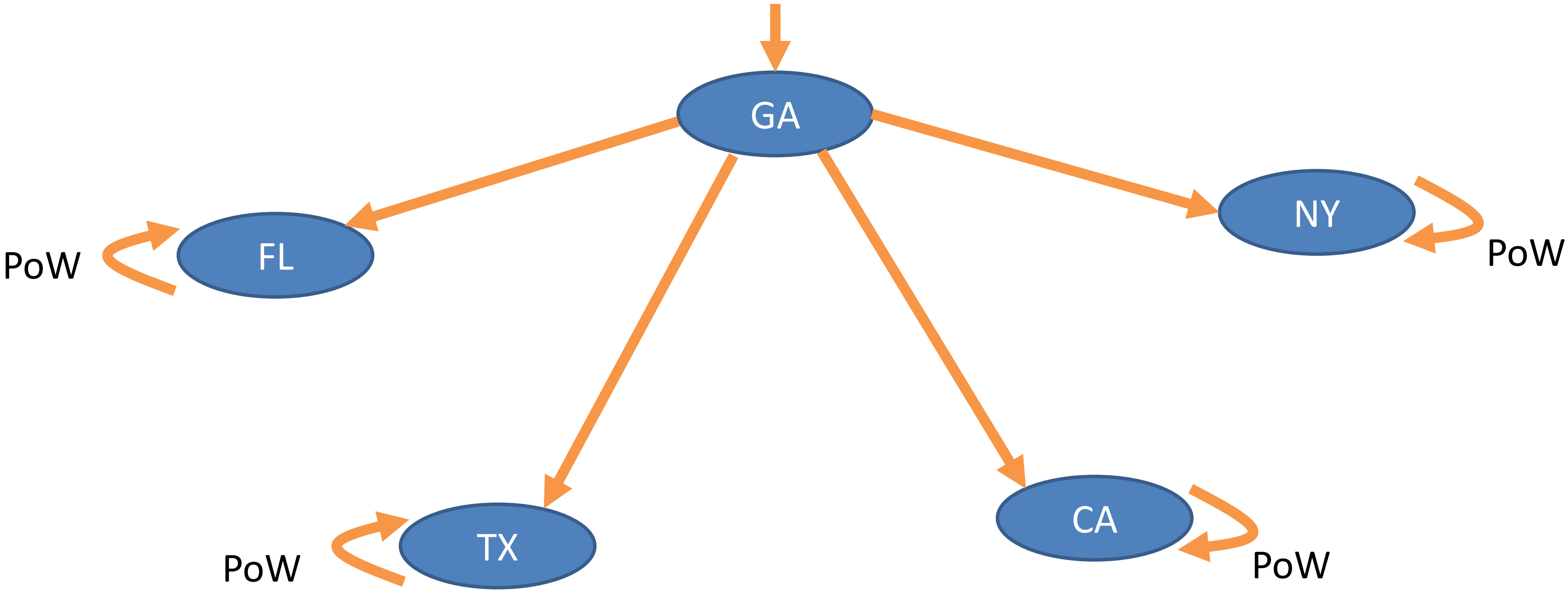
1. PoW (Proof-of-Work)

- Step 1: Generate new transactions, broadcast to the entire network, and require accounting for transactions



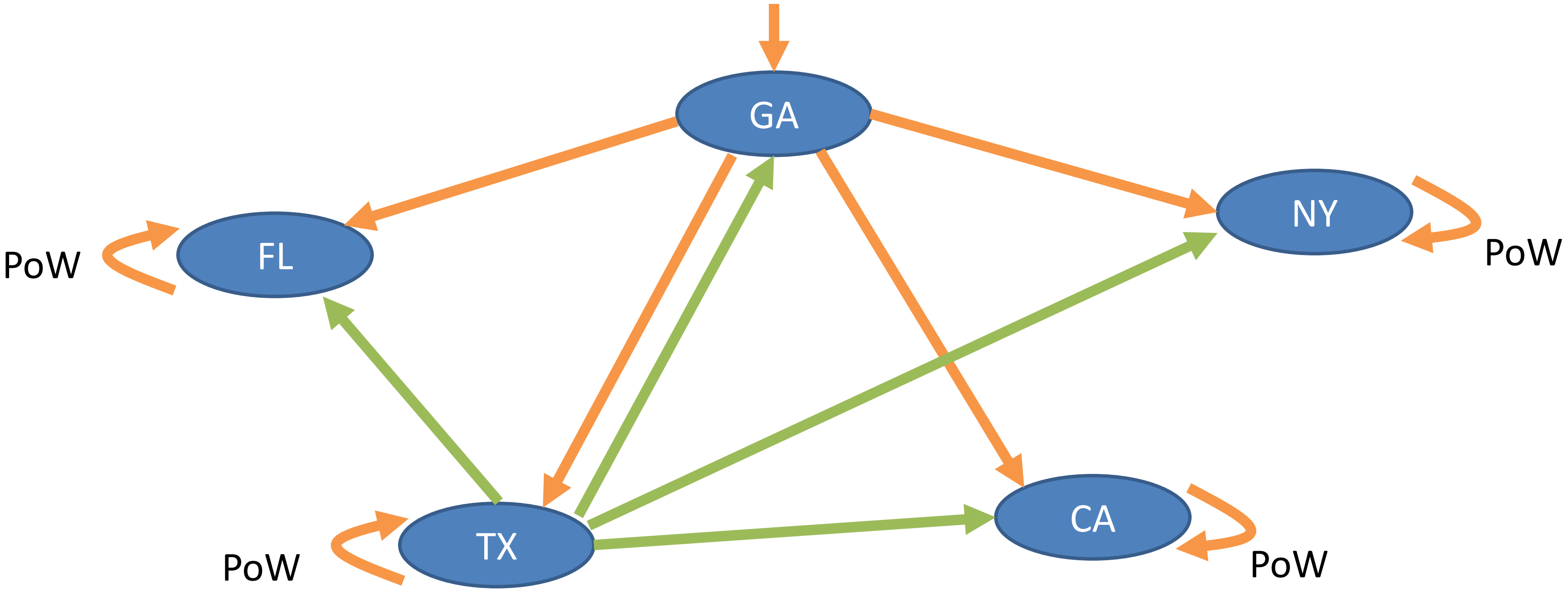
1. PoW (Proof-of-Work)

- Step 2: After each node receives this request, it puts the received transaction information into a block. Each node uses the PoW algorithm to calculate the hash value of the block and gets a proof of computing power.



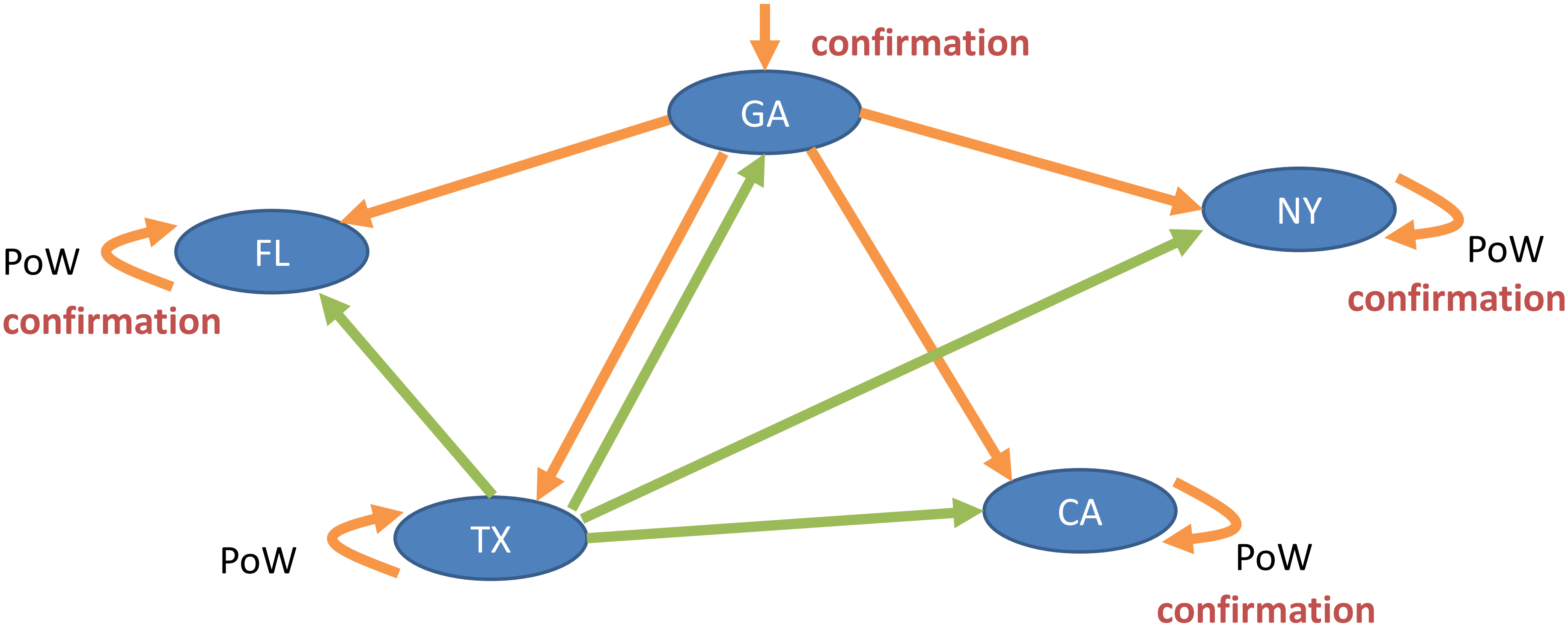
1. PoW (Proof-of-Work)

- Step 3: If node TX gets a proof of work, it broadcasts to the whole network. If the transaction contained in the block is valid and have not existed before, other nodes will recognize the validity of the block.



1. PoW (Proof-of-Work)

- Step 4: When other nodes receive the broadcast and confirm its validity, they will accept the new block and put it at the end of blockchain.



1. PoW (Proof-of-Work)

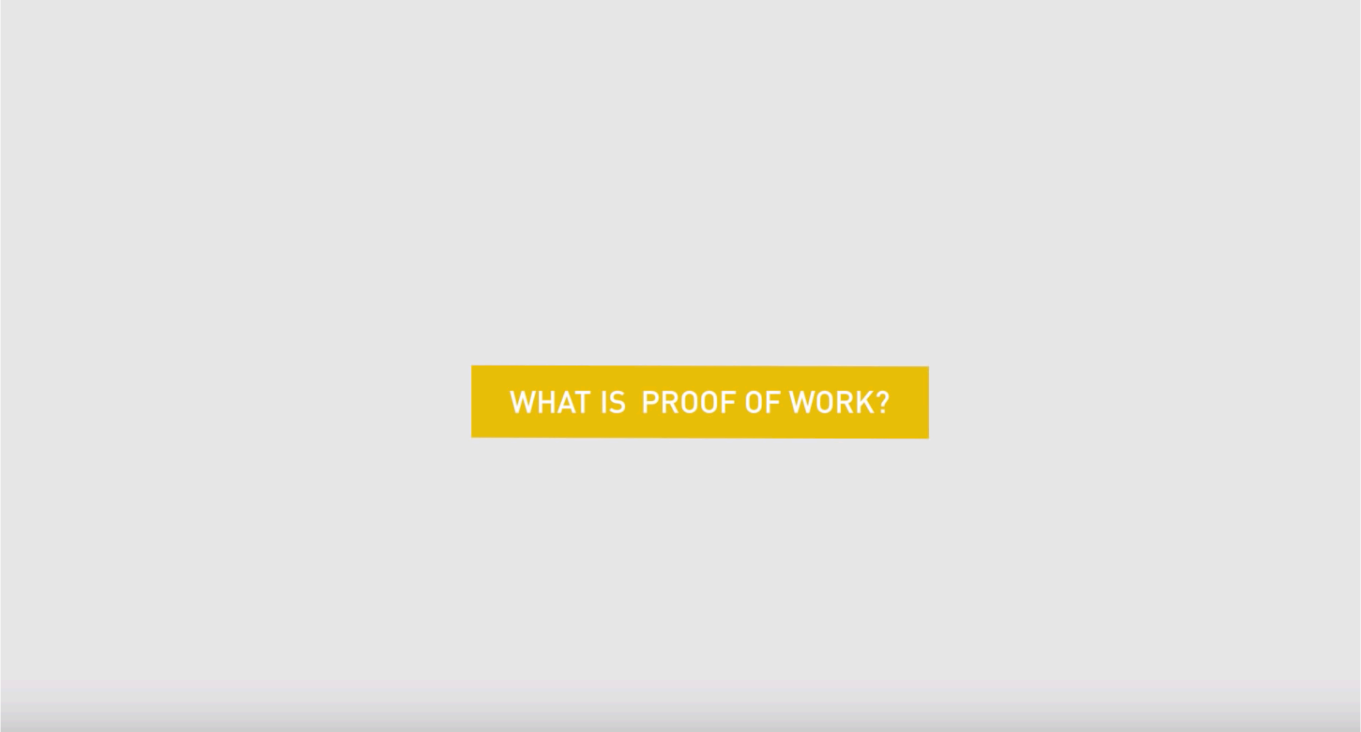
- Advantages:
  - Simple
  - Good fairness
  - High reliability, e.g., to break this system, you have to own 51% of the entire computing power of the entire system

1. PoW (Proof-of-Work)

- Disadvantages:
  - Requires the entire network to participate the calculation, which increases the calculation amount of each node
  - If the problem is too difficult, it will lead to long calculation time and high resource consumption
  - If the topic is too simple, it will cause many nodes to obtain the accounting right at the same time and introduce too many conflicts.
  - Long cycle to achieve consensus, low efficiency, and high resource consumption

1. PoW (Proof-of-Work)

- https://youtu.be/3EUAcxhuoU4



WHAT IS PROOF OF WORK?

2. PoS (Proof-of-Stake)

- Key idea: using ***equity (wealth or age)*** instead of computing power to determine the accounting right

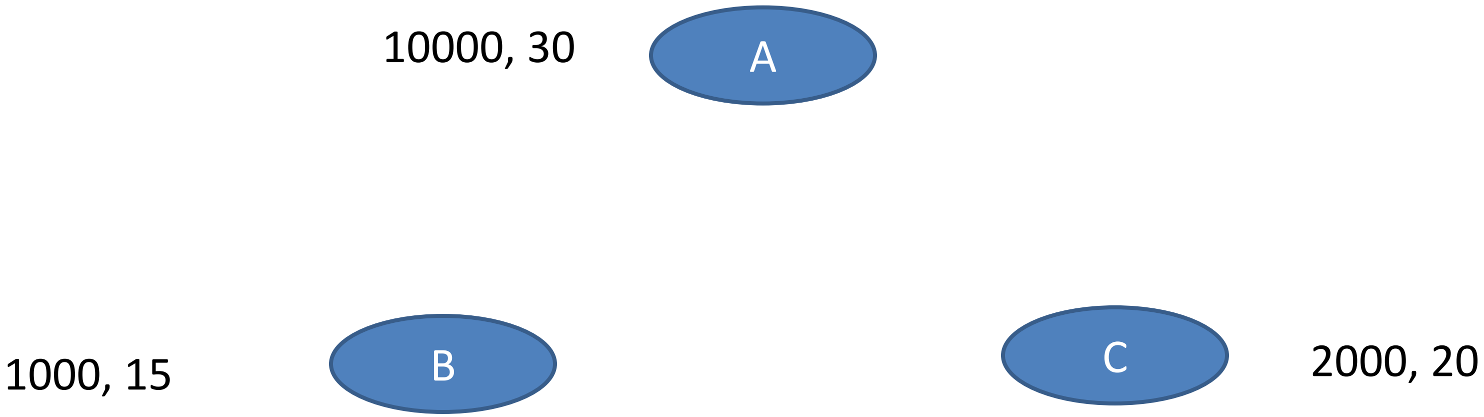
- Whoever has more equities will be more likely to obtain accounting rights.

2. PoS (Proof-of-Stake)

- Equity (wealth or age) example:
  - If you hold 100 coins for a total of 50 days, then your coin age is 5000
  - If you find a PoS block, your coin age will be reduced by 365. For every 365 coin age reduction, you can get 0.05 coin interest from the block (as 5% annual interest rate)
  - Equity = coins * ages * 5% / 365

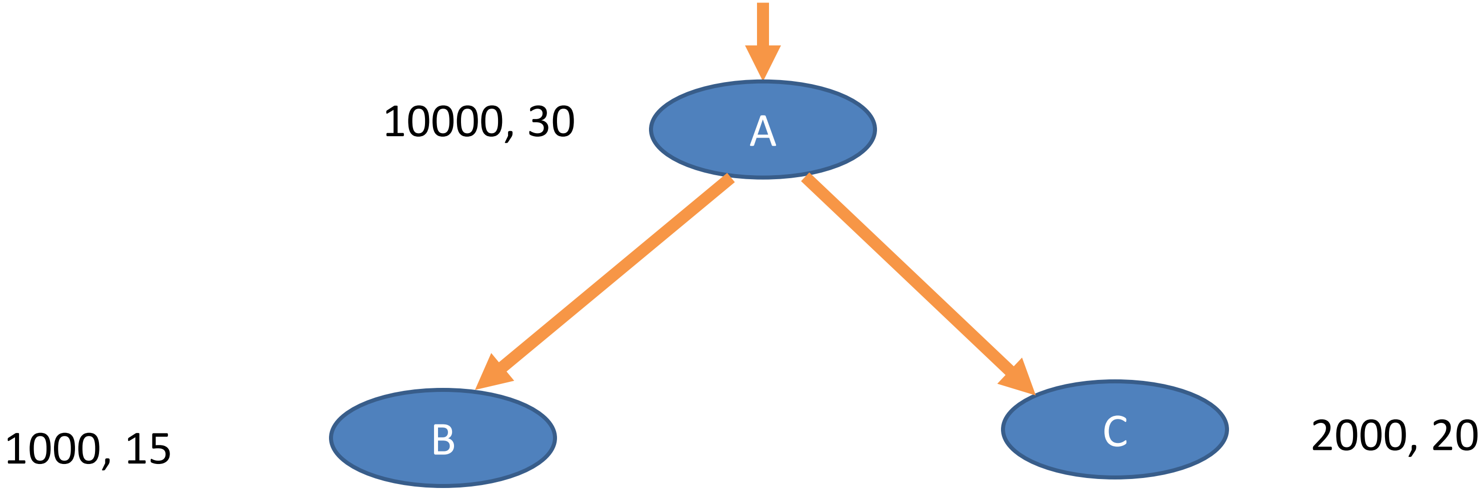
2. PoS (Proof-of-Stake)

- Example:
  - A network containing 3 nodes: A, B, C
  - A: 10000 coins, 30 days; B: 1000 coins, 15 days; C: 2000 coins, 20 days.



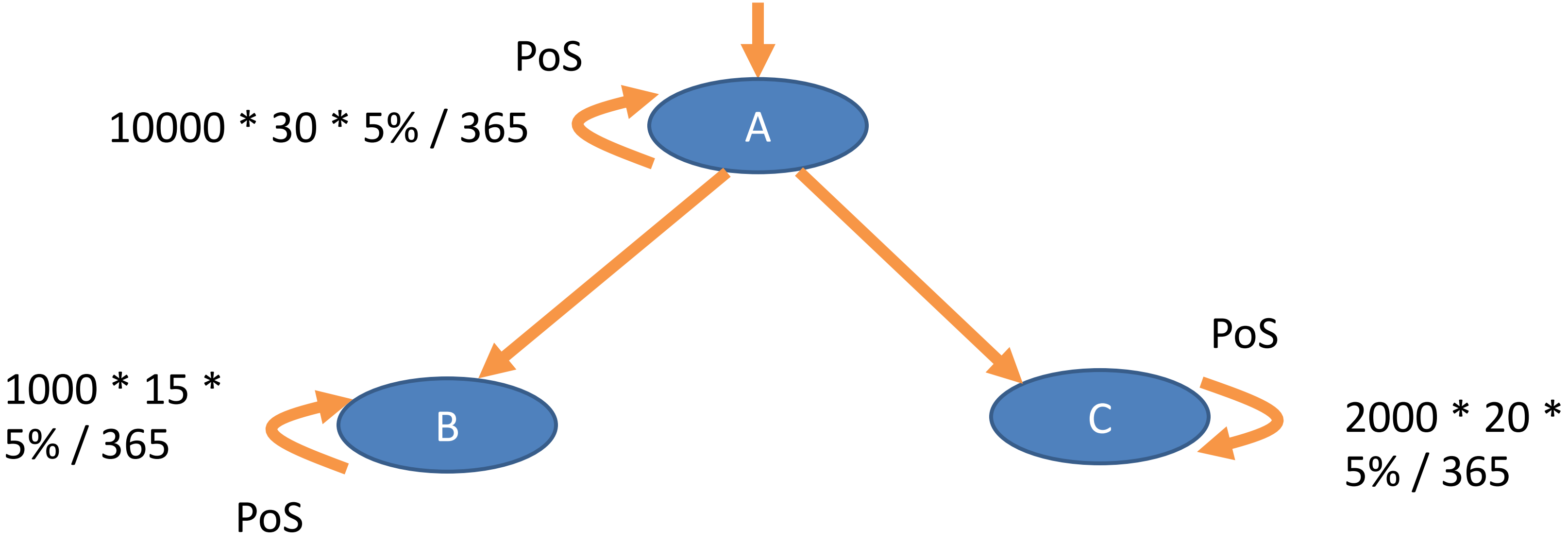
2. PoS (Proof-of-Stake)

- Step 1: Generate new transactions, broadcast to the entire network, and require accounting for transactions



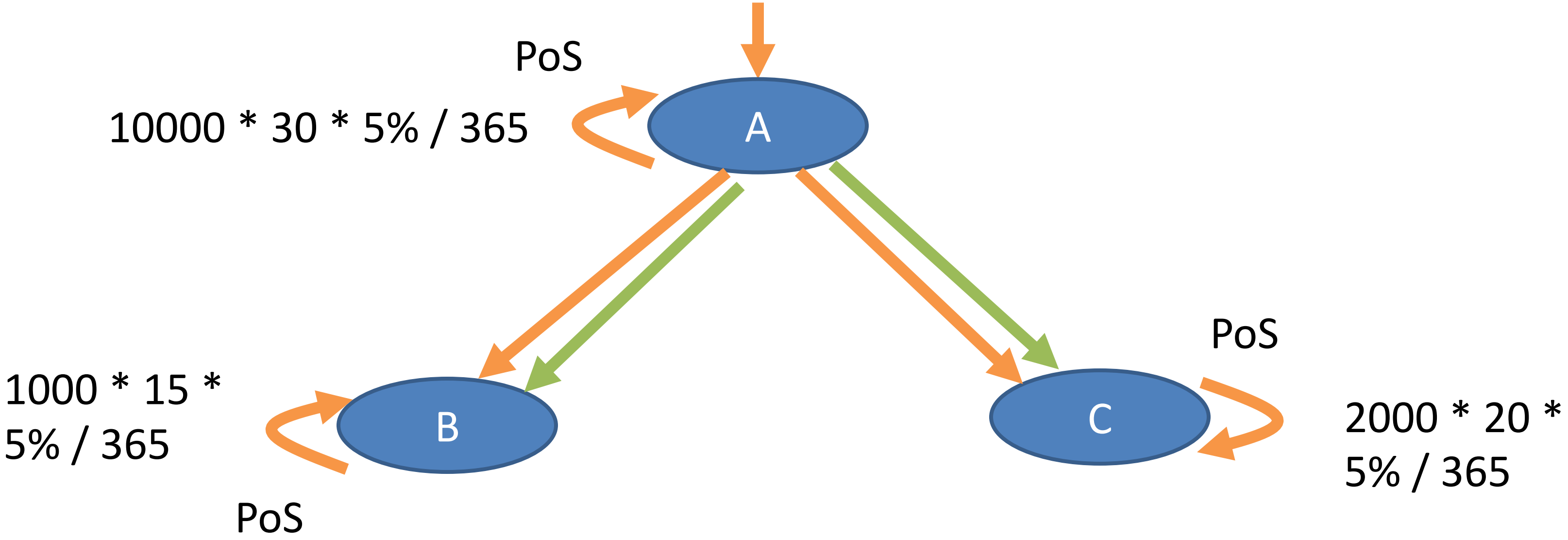
2. PoS (Proof-of-Stake)

- Step 2: After each node receives this request, it puts the received transaction information into a block. Each node uses the PoS algorithm to calculate the hash value of the block and gets a proof of equity.



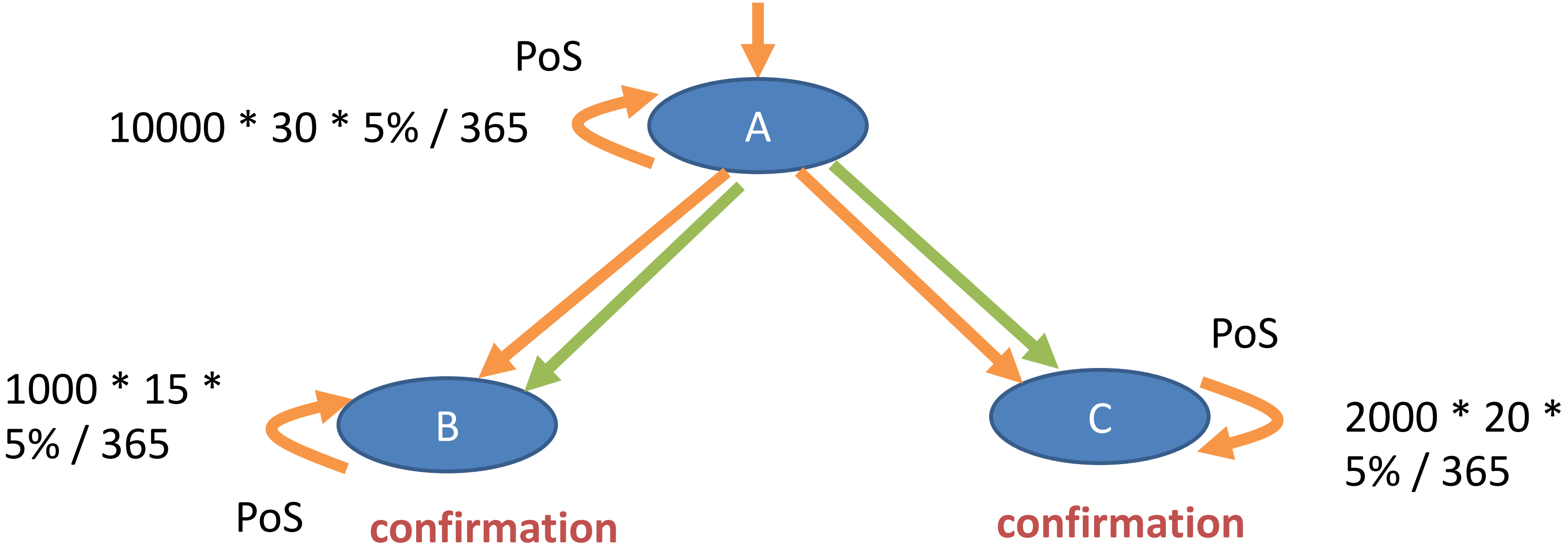
2. PoS (Proof-of-Stake)

- Step 3: A gets a proof of equity; it broadcasts to the whole network. If the transaction contained in the block is valid and have not existed before, other nodes will recognize the validity of the block.



2. PoS (Proof-of-Stake)

- Step 4: When other nodes receive the broadcast and confirm its validity, they will accept the new block and put it at the end of blockchain.



2. PoS (Proof-of-Stake)

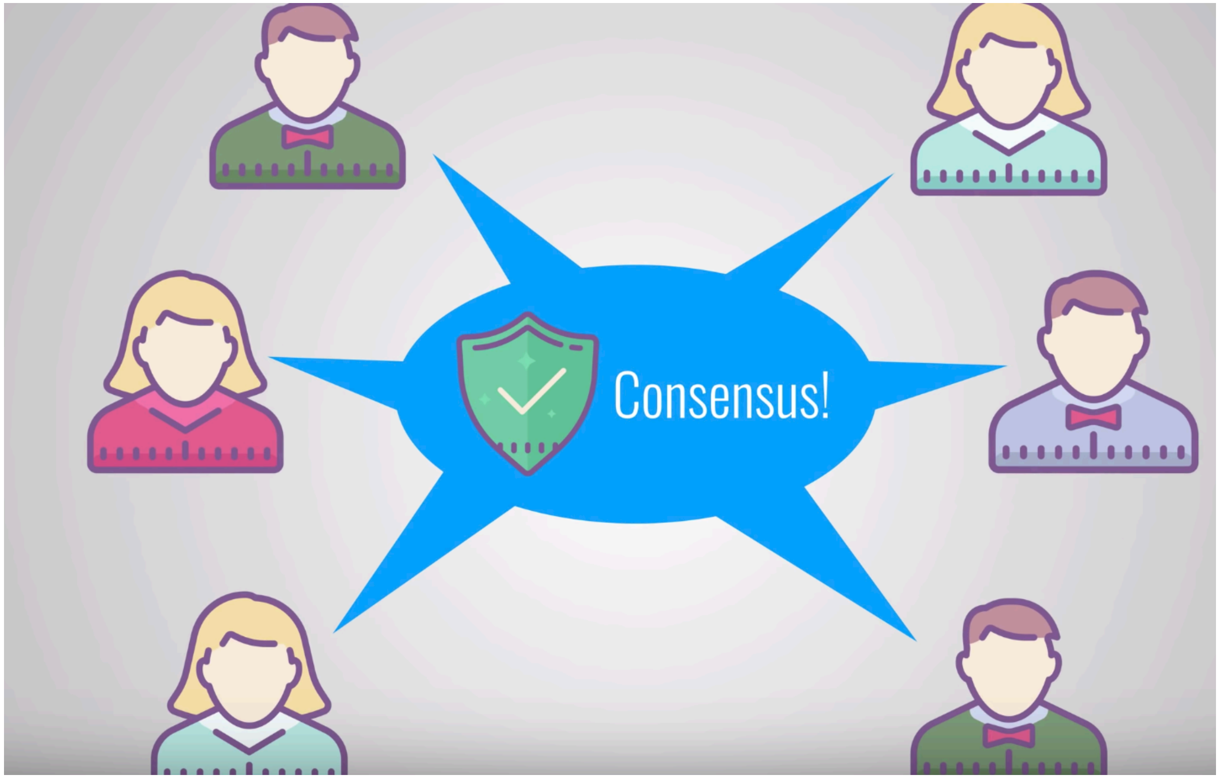
- Advantages:
  - Does not need to consume a lot of computing and power to ensure the security of the blockchain network
  - Reduced time required to reach consensus

2. PoS (Proof-of-Stake)

- Disadvantages:
  - The more or the longer the coin is held, the easier it will be for the node to get the accounting right, while the nodes holding less coins will have little chance.
  - Unfairness and monopoly happens
  - Unbalanced network

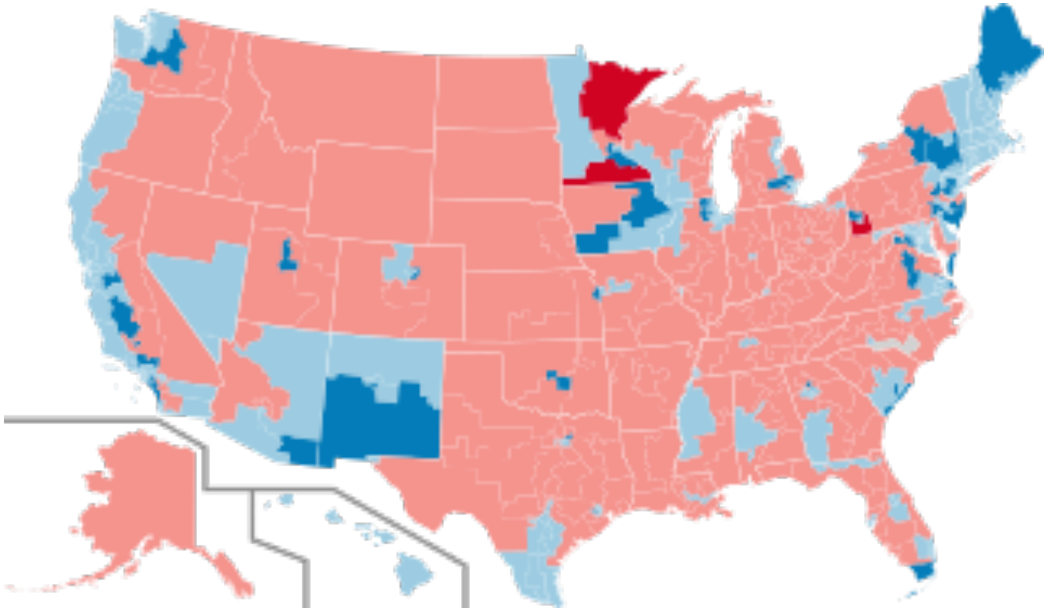
2. PoS (Proof-of-Stake)

- https://youtu.be/M3EFi_POhps



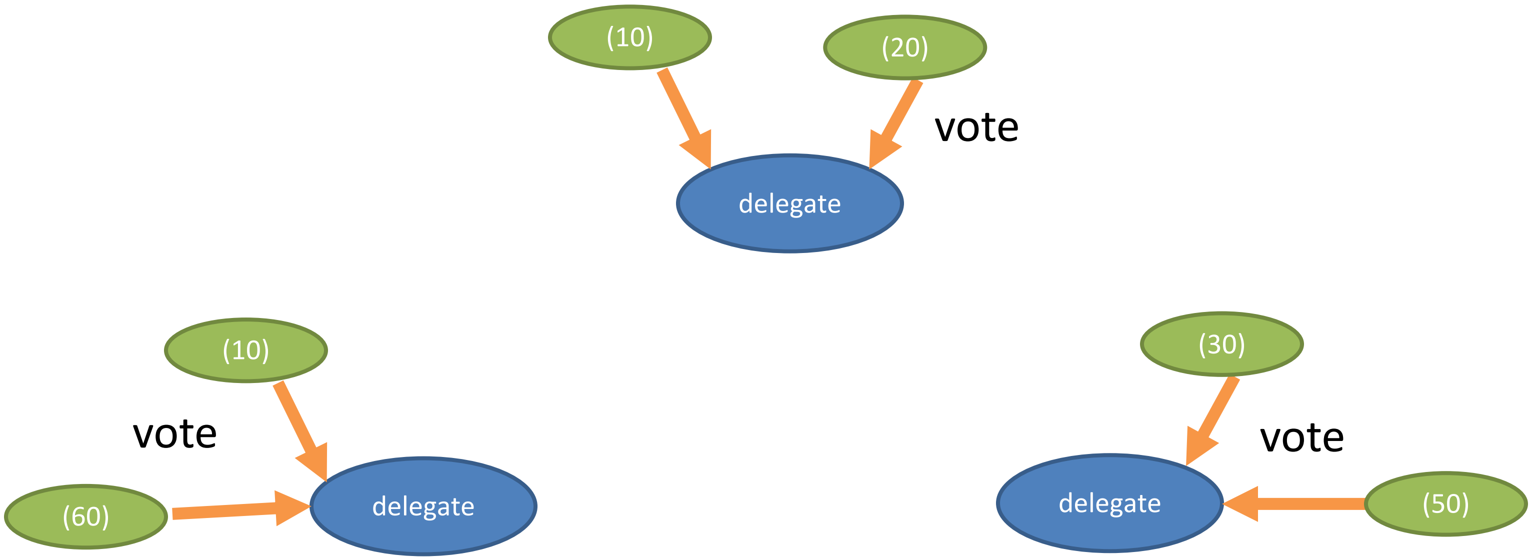
3. DPoS (Delegated Proof of Stake)

- DPoS is similar as U.S. House
- Votes selects representatives to make a decision



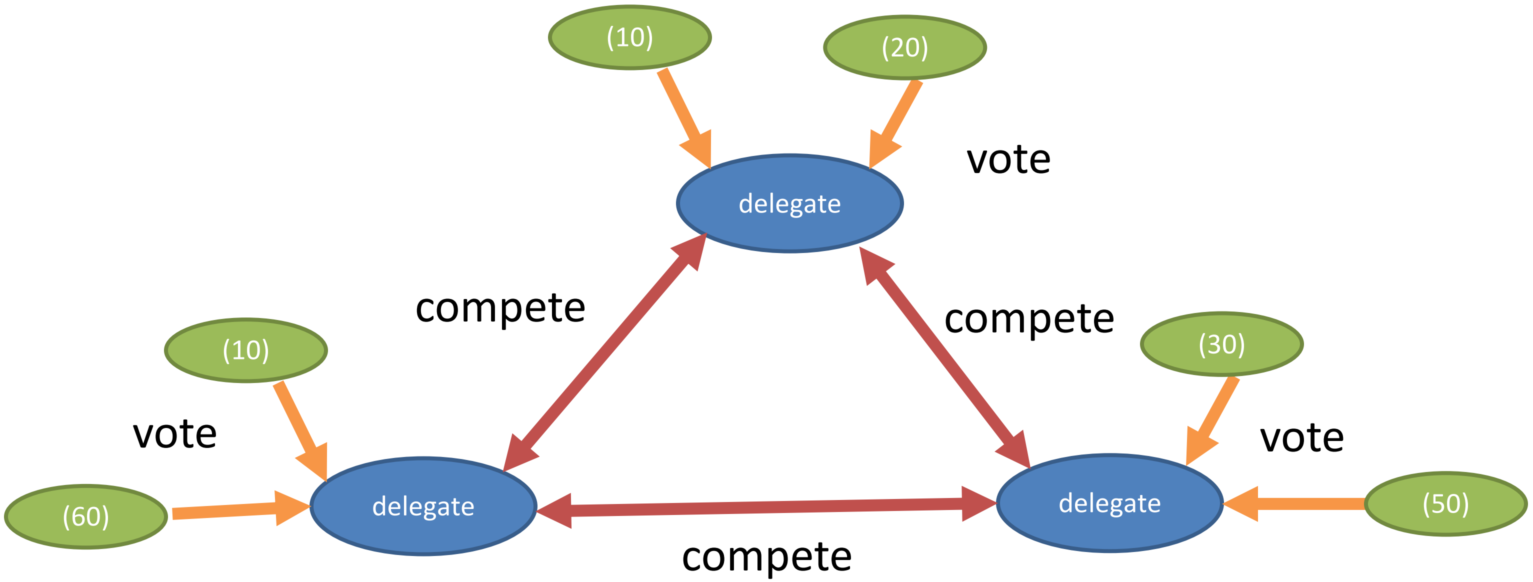
3. DPoS (Delegated Proof of Stake)

- User votes for delegates to compete for the accounting right
- Every user has different voting power. For instance, suppose the total stock share is 1000, the user holding 10 shares has 1/100 voting power



3. DPoS (Delegated Proof of Stake)

- After the delegates are elected, they compete for the accounting right based on their computing power



3. DPoS (Delegated Proof of Stake)

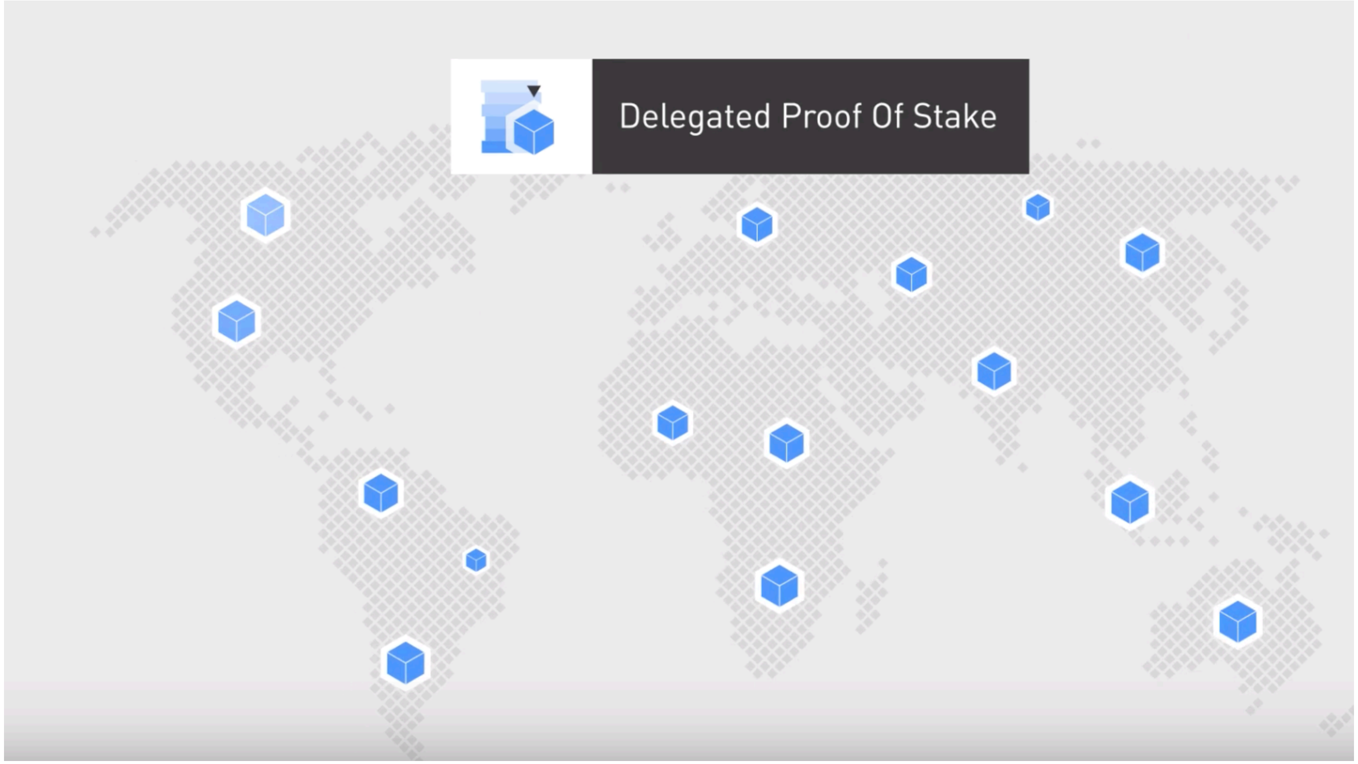
- Advantages:
  - Several more trustworthy delegates elected by voters competes the accounting right, which reduces all nodes participating in competition, making less communications, shorter consensus time, less energy consumption and faster agreement speed
  - Over a period, new delegates will be elected to avoid fraud and monopoly

3. DPoS (Delegated Proof of Stake)

- Disadvantages:
  - Less fairness: DPoS users with small stakes can decide that their vote doesn't matter in comparison with votes of bigger stakeholders
  - Low reliability for delegate nodes: once the node fails, it leads to potential security risks

3. DPoS (Delegated Proof of Stake)

- https://youtu.be/OVKAOwzAwHI



Comparison

	PoW	PoS	DPoS
Computing consumption	High	Medium	Low
Structure	Distributed	Distributed	Distributed but having some centers
Performance (throughput)	PoW < PoS < DPoS		
Transaction cost	High	Low	Low
Application platform	Bitcoin	Ethereum	Bitshares