A Review on Consensus Algorithm for Distributed P2P Network of Blockchain

Final Report of Operating System

Reporter：廖家鴻 0786009　Date：June 19, 2019

List of Studied Articles

[1] Mingxiao, Du, et al. "A review on consensus algorithm of blockchain." 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, 2017.

[2] Zheng, Zibin, et al. "An overview of blockchain technology: Architecture, consensus, and future trends." 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, 2017.

[3] Yuan, Yong, and Fei-Yue Wang. "Towards blockchain-based intelligent transportation systems." 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2016.

[4] Liu, Mengting, et al. "Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach." IEEE Transactions on Industrial Informatics (2019).

[5] Chenli, Changhao, et al. "Energy-recycling Blockchain with Proof-of-Deep-Learning. " arXiv preprint arXiv:1902.03912 (2019).

大綱 Outline

01 Distributed P2P Network

02 Consensus Protocol

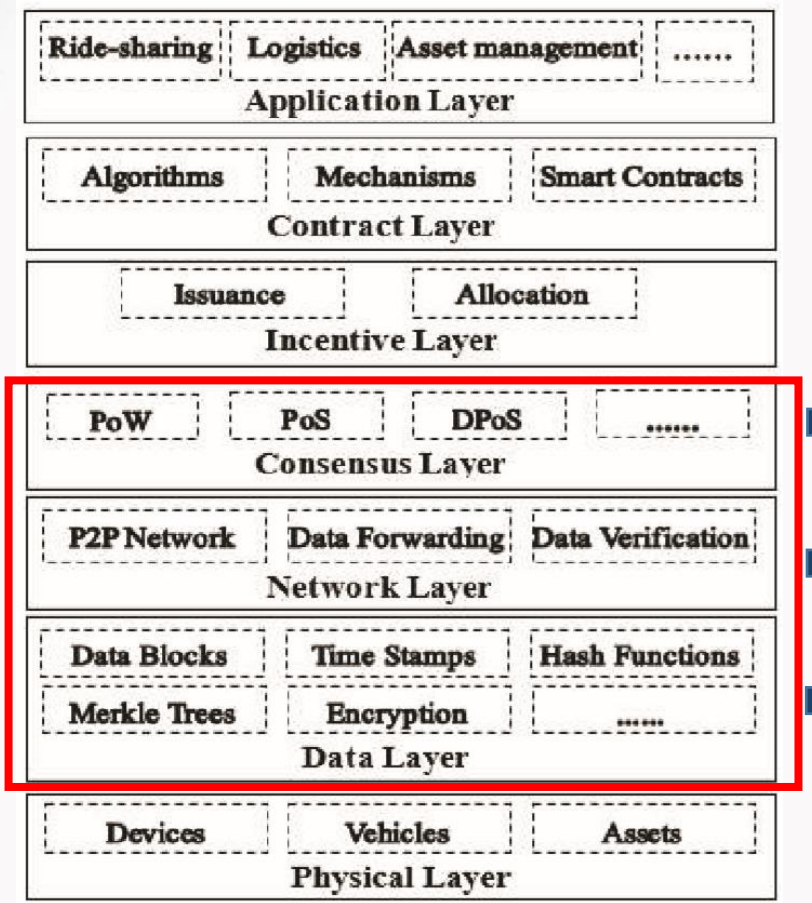
03 The 51% Attack

04 Comparisons of Different Consensus Algorithms

05 Conclusions

Blockchain Architecture and Distributed P2P Network

Blockchain Architecture

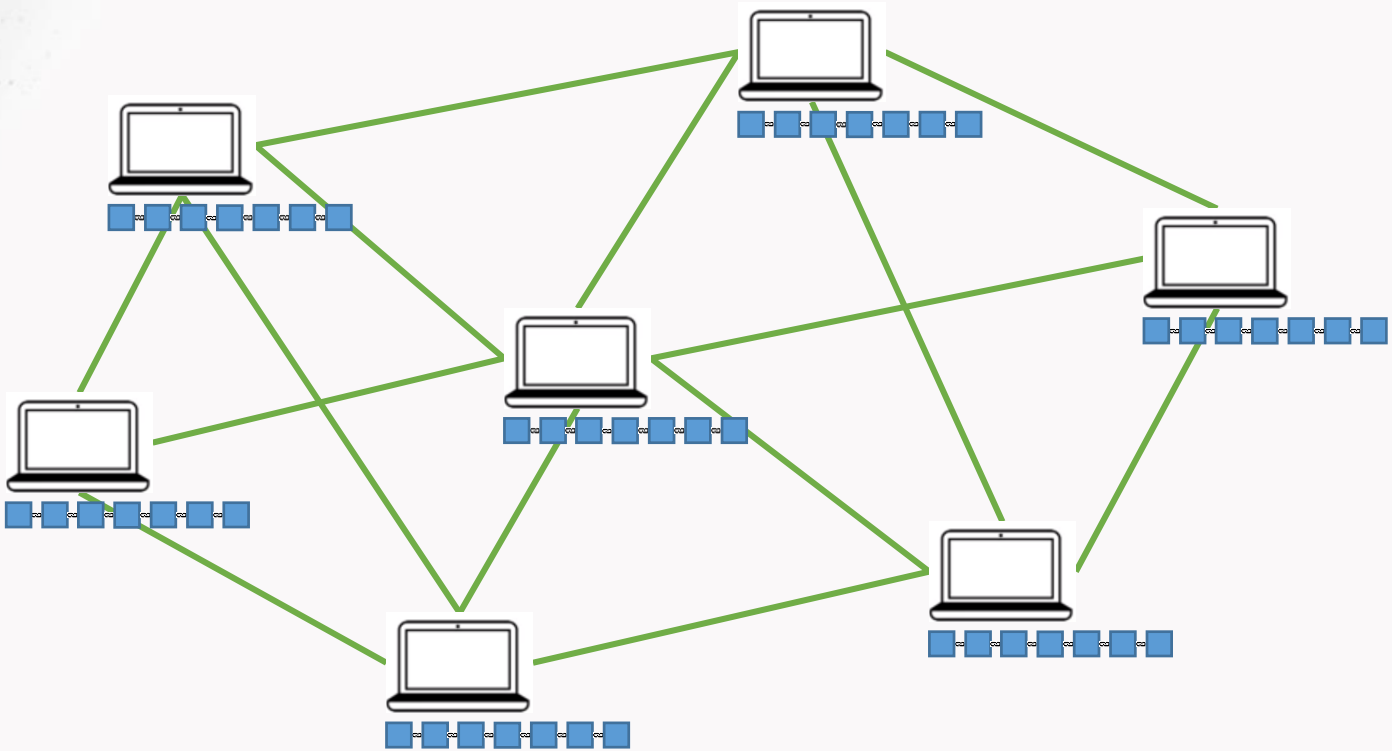


→ Fault tolerance and security?

→ Distributed immutable ledger

→ How mining works?

Distributed P2P Network

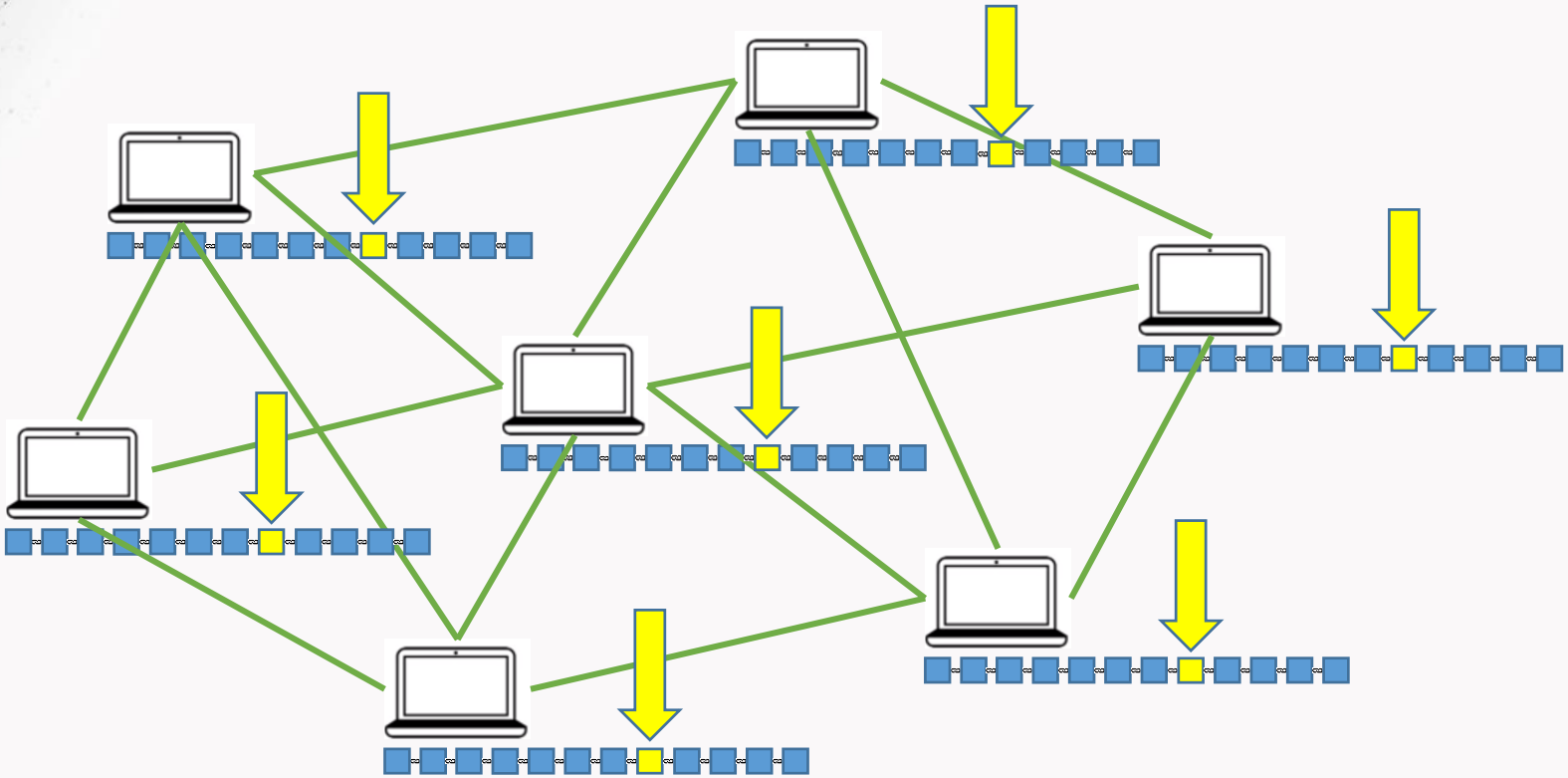


Although anybody can change the block information if they like or need, there are only seven computers in our example.

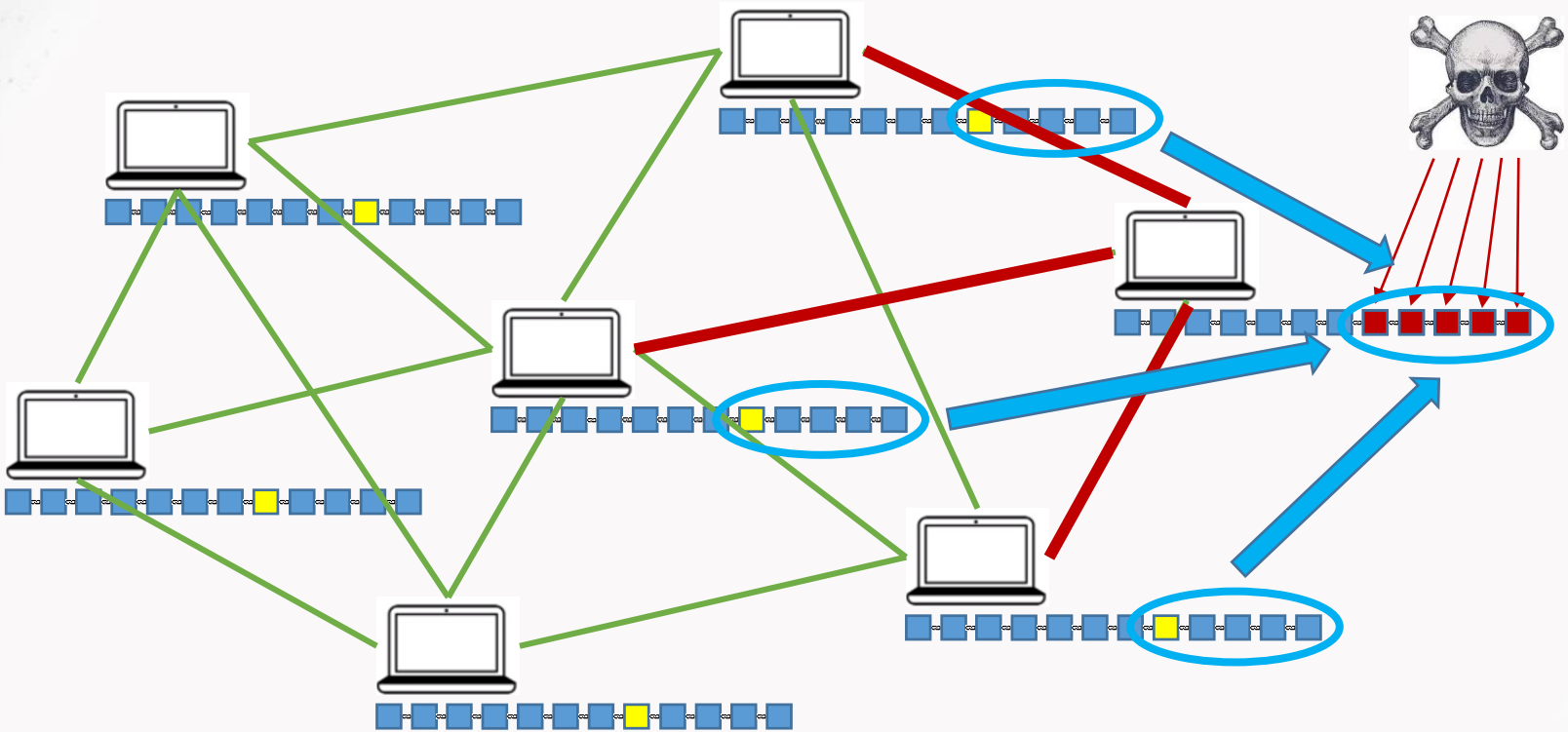
Actually there are thousands and thousands of computers interconnected, updating the chain, the valid ledger will eventually have one version through majority consensus.

Well, the Blockchain is copied across all the computers and forms distributed ledger.

Distributed P2P Network



Distributed P2P Network: Malicious Attack

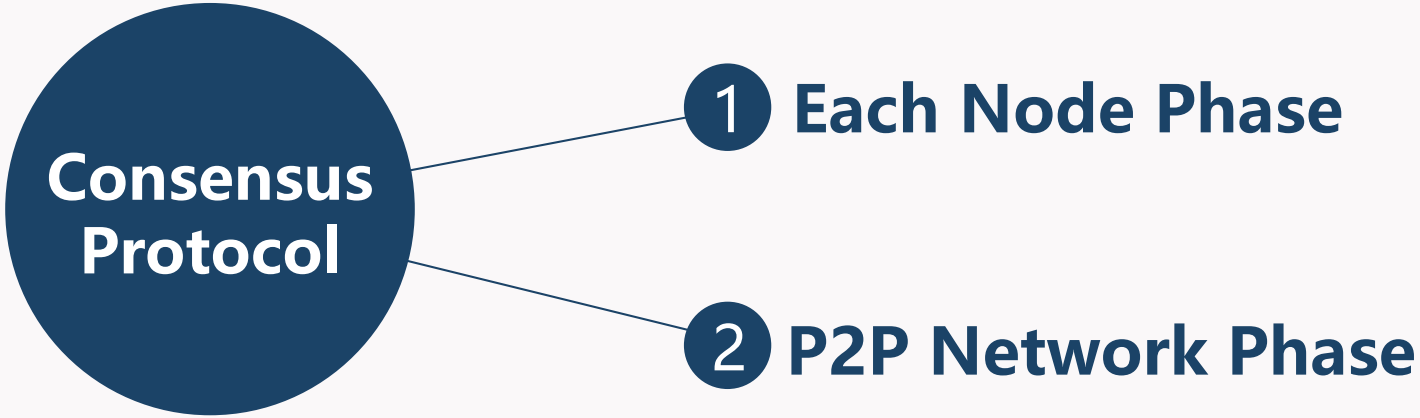


OK, that is the operation of distributed p2p network for blockchain.

02
PART

Consensus Protocol: Proof-of-Work (PoW)

Consensus Protocol: Proof-of-work (PoW)



PoW: Each Node Phase

Miner A

Block: #123	Nonce: 63
Prev. Hash: 000042f05976436ca9fd	
New Hash:	

Block Header

Data: Transaction A
Transaction C
Transaction G

Block Body

Miner B

Block: #123	Nonce: 129
Prev. Hash: 000042f05976436ca9fd	
New Hash:	

Data: Transaction B
Transaction D
Transaction F

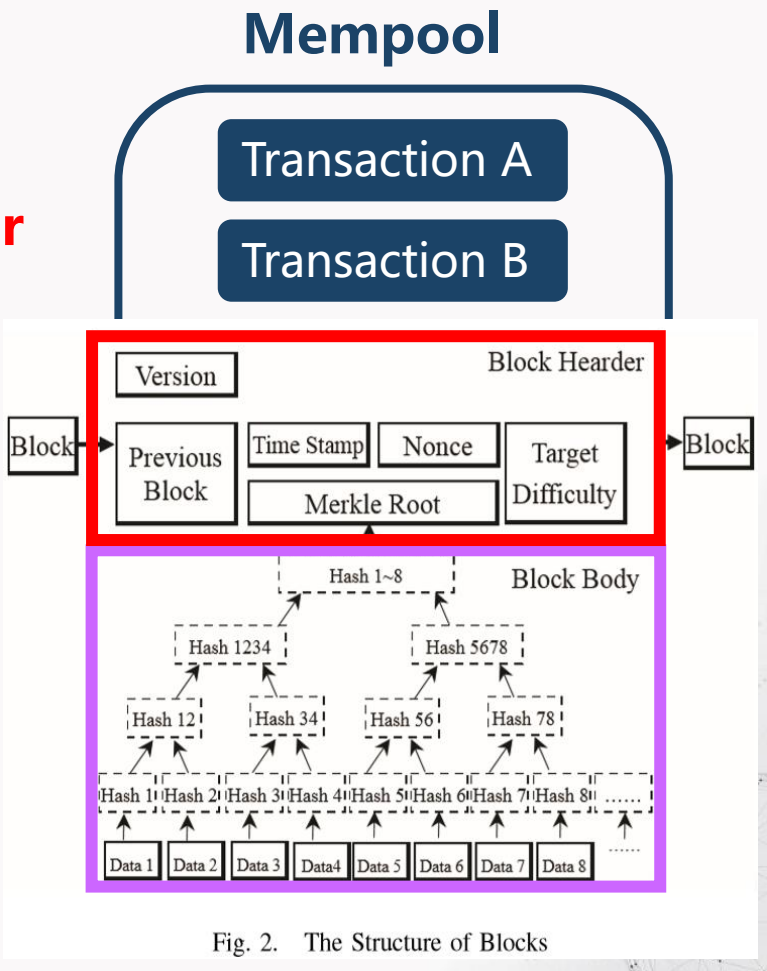


Fig. 2. The Structure of Blocks

PoW: How Mining Works

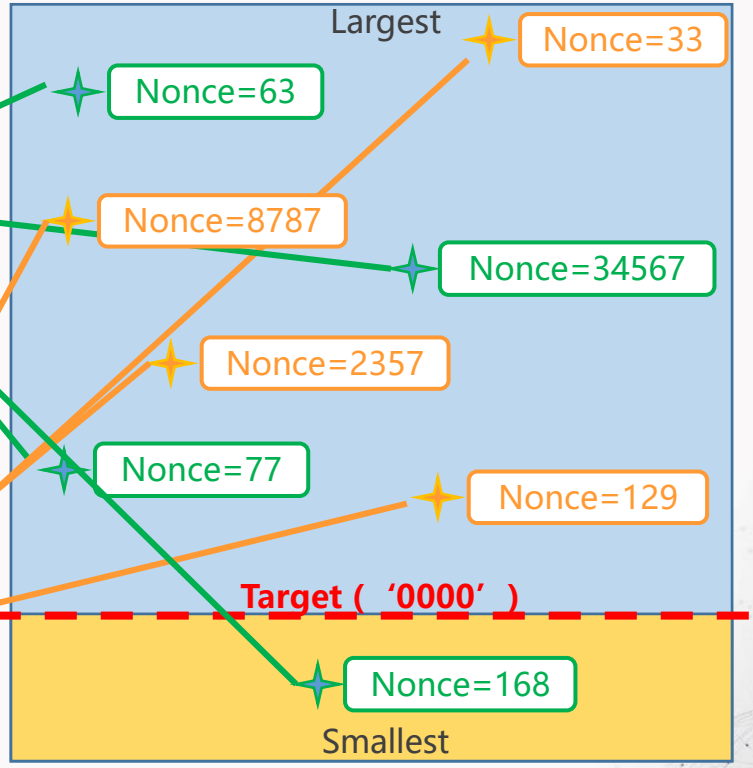
Solve Cryptographic Puzzle
-All Possible Hashes-

Miner A

Block: #123	Nonce: [illegible]
Prev. Hash: 000042f05976436ca9fd	
New Hash: 0000[illegible]	
Data: Transaction A Transaction C Transaction G	

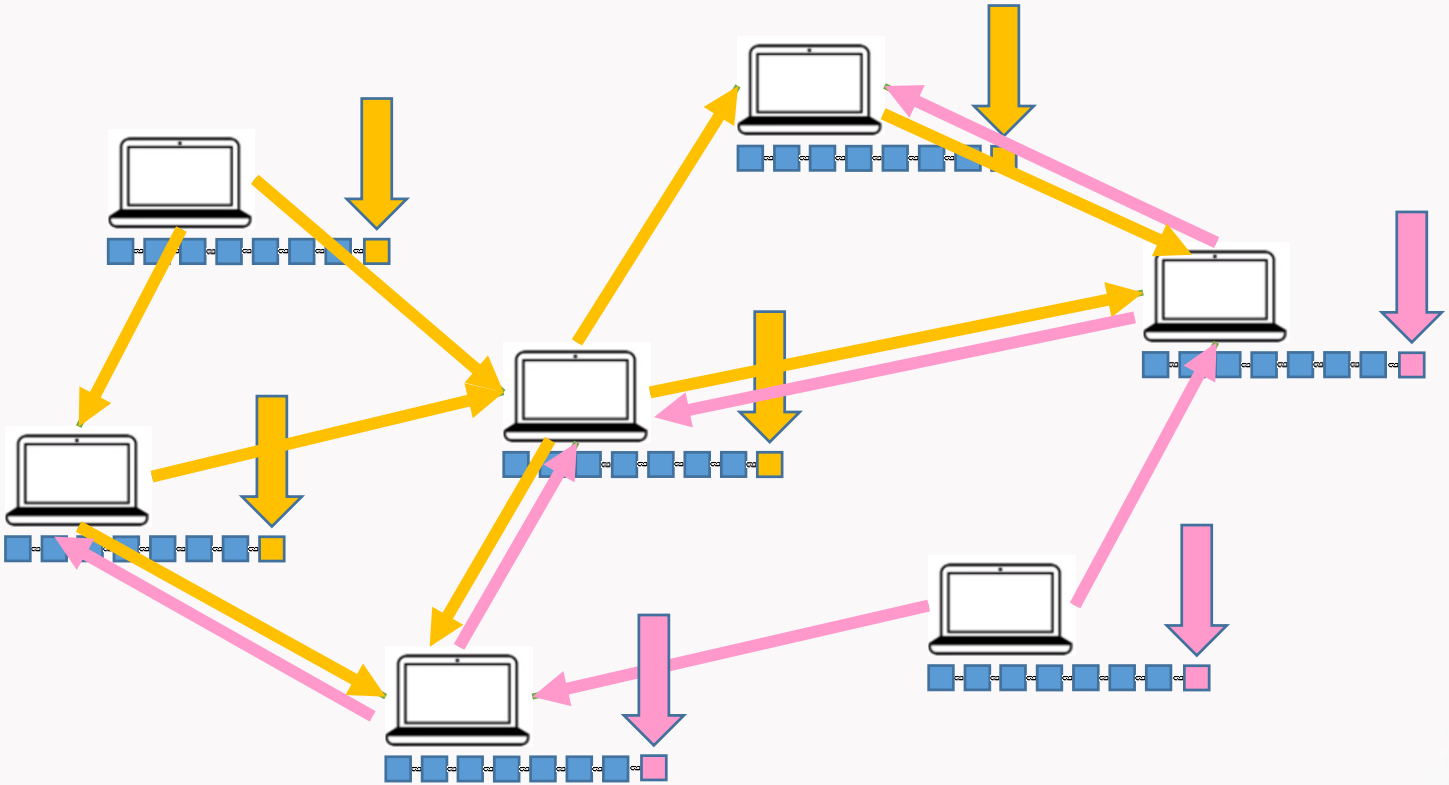
Miner B

Block: #123	Nonce: [illegible]
Prev. Hash: 000042f05976436ca9fd	
New Hash: [illegible]	
Data: Transaction B Transaction D Transaction F	

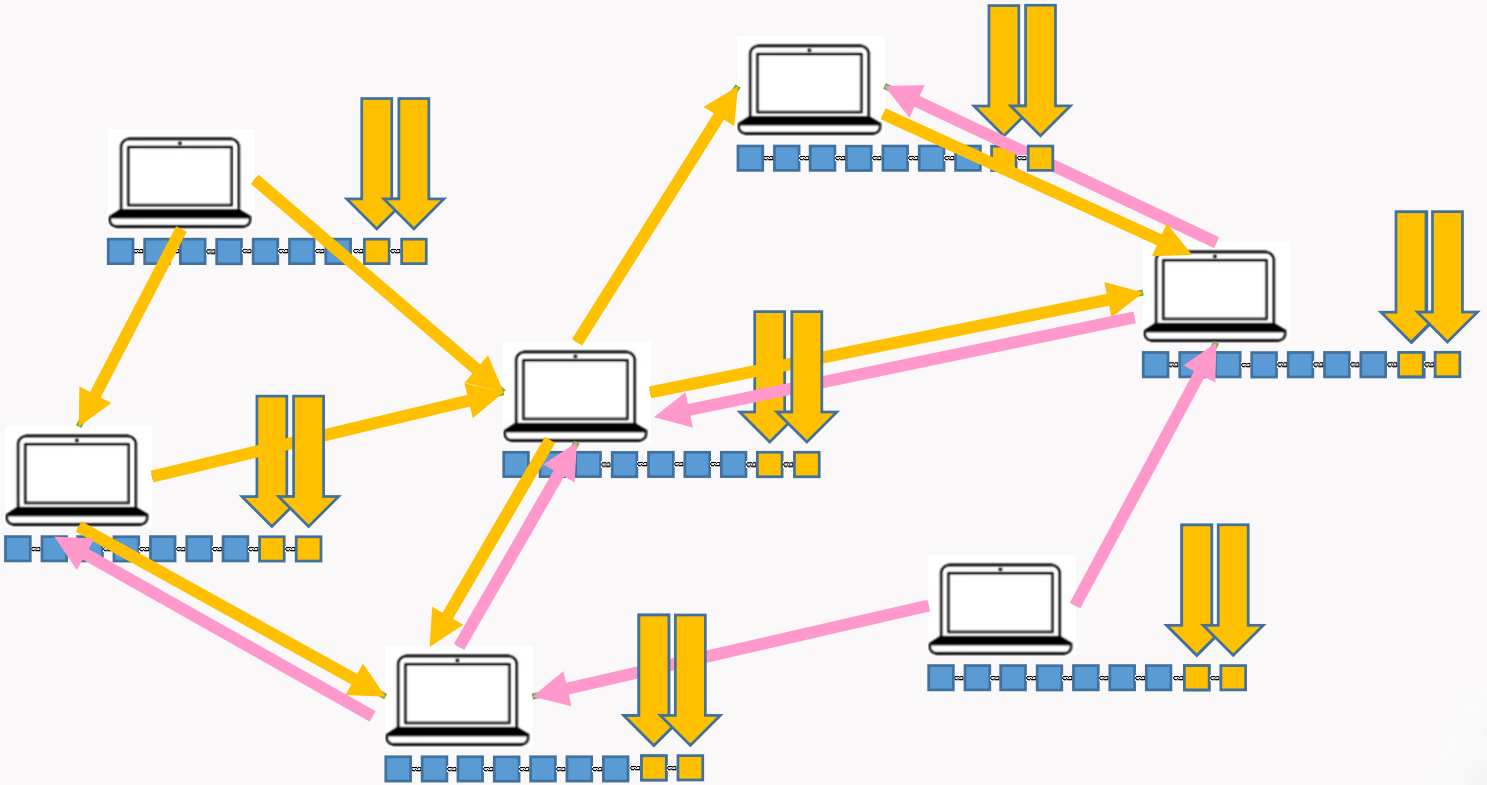


Tip: Express Target with leading zeros,
Such as '0000'

PoW: P2P Network Phase



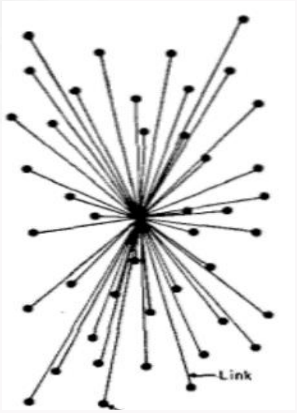
PoW: P2P Network Phase



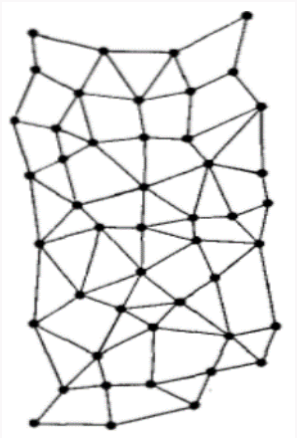
orphaned block

The 51% Attack

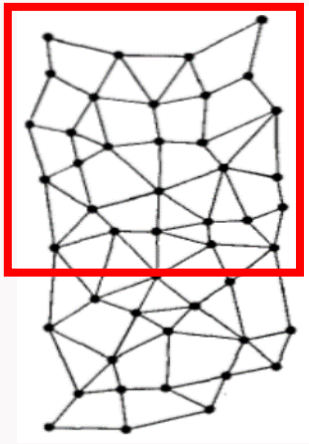
Security Issue of Blockchain P2P Network



In this centralized network, the hacker would have succeeded and it would have taken away that million dollar property.



But in distributed p2p networks, the hacker will not succeed because all of the peers are all synchronized very constantly.



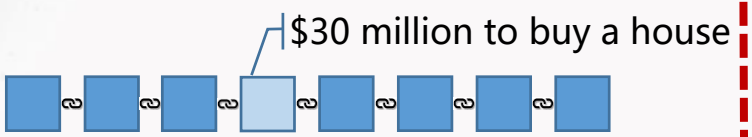
The hacker should have to attack more than **50%** of the blockchains at the same time.

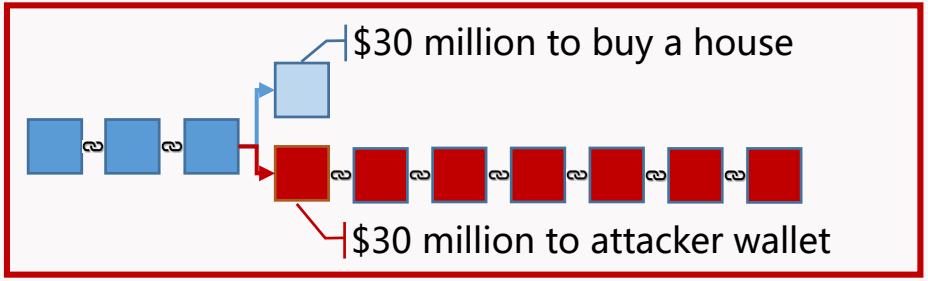
This is almost impossible to achieve this malicious attack.

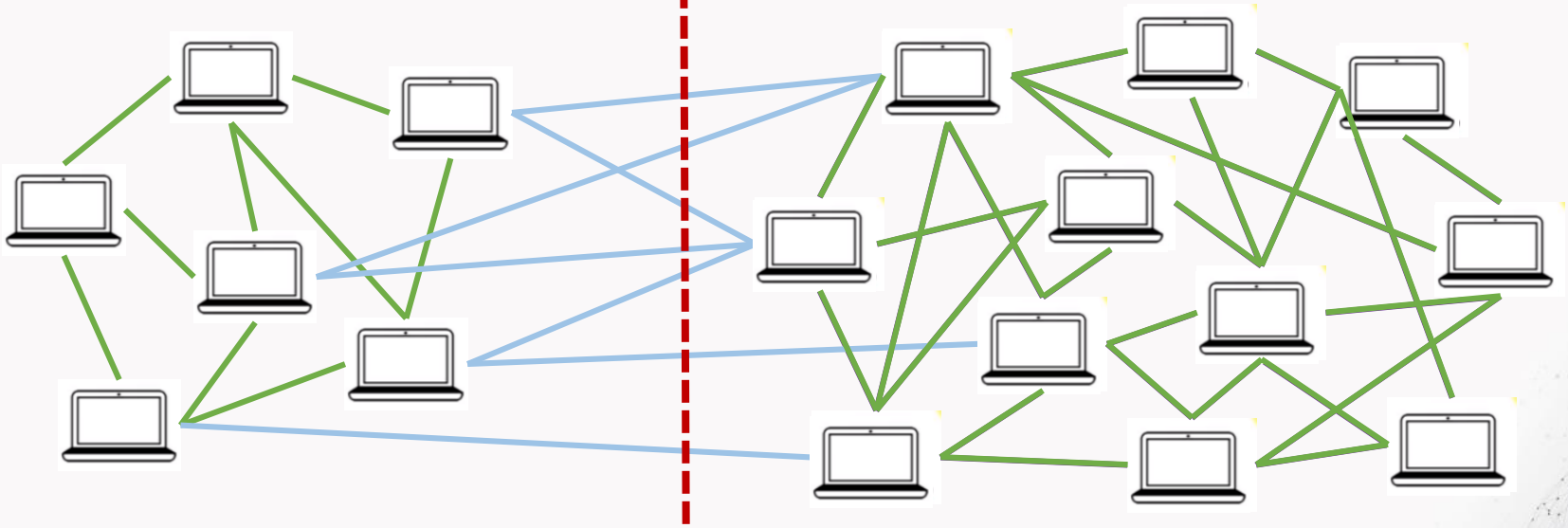
However, the **"51% attack"** does not means the 51% nodes.

Instead, what we talk is **51% hash rate** (computing power).

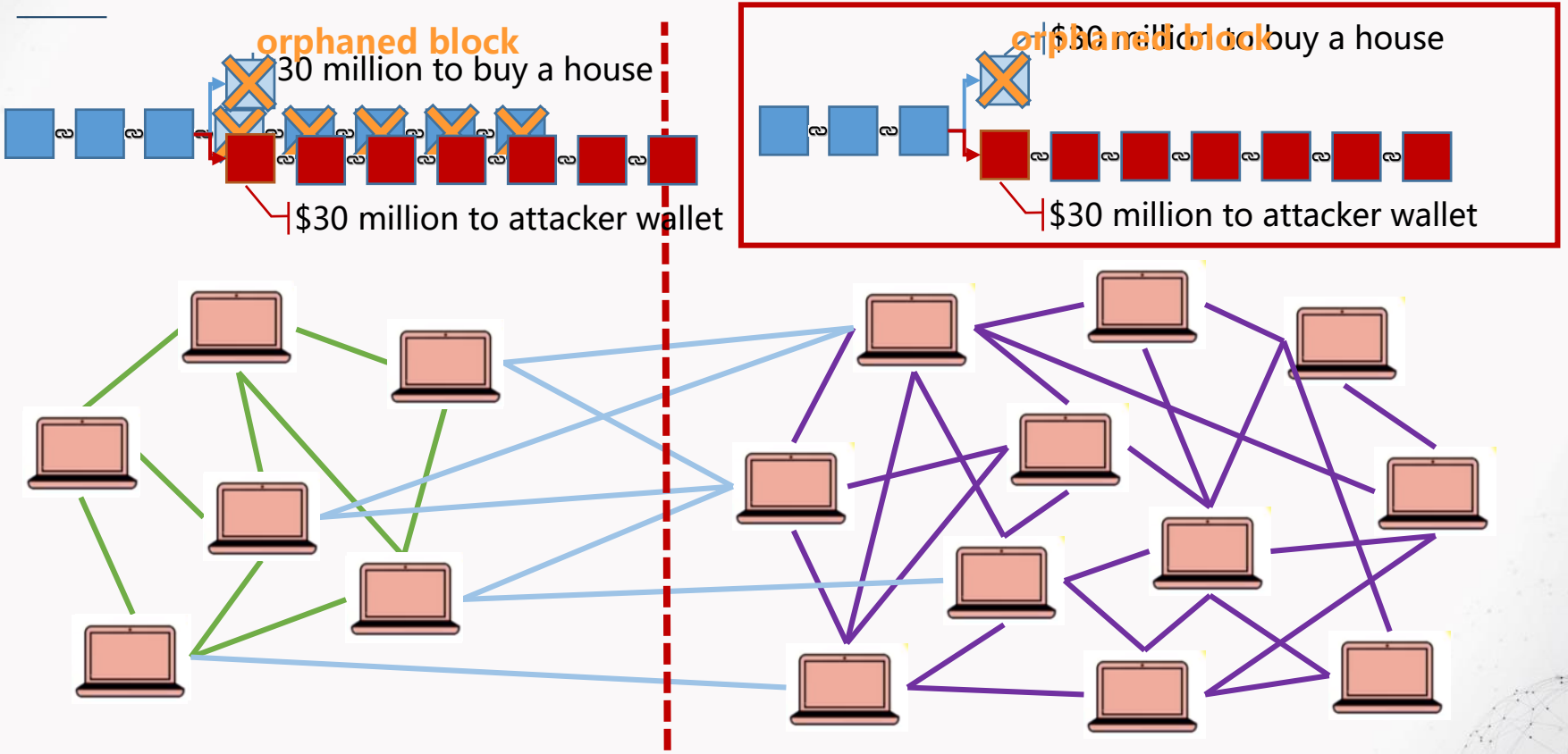
How does the 51% Attack works?







How does the 51% Attack works?



Hash Power and Double Spending

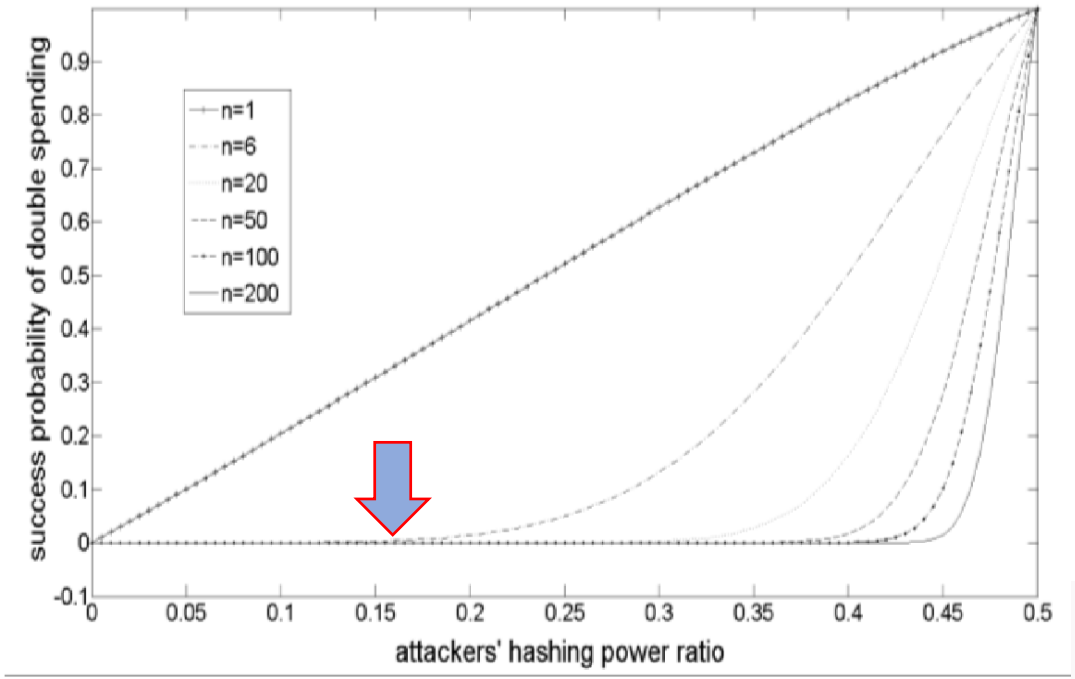
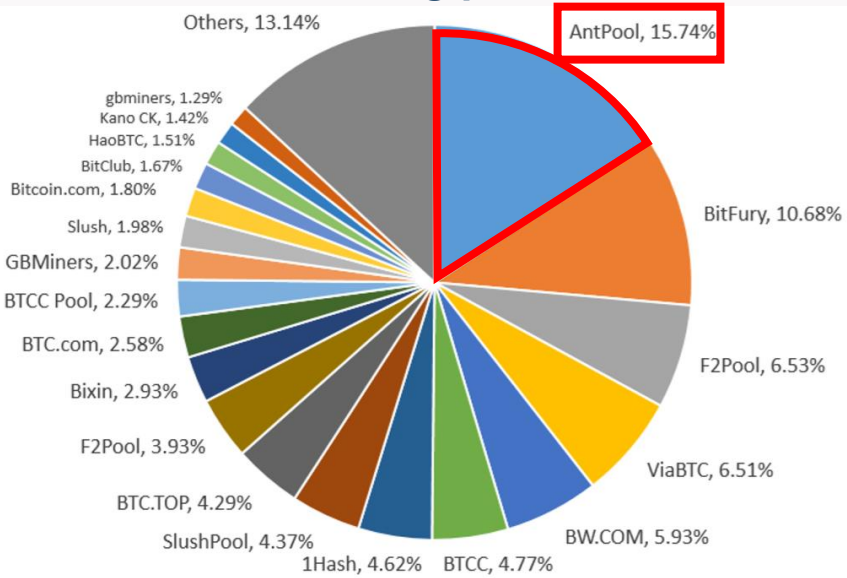


Fig. 3. Relationship between hashing power ratio and double spending

Ratios of the mining pool of bitcoin



The biggest one is AntPool, which occupies 15.74% of whole hash power.

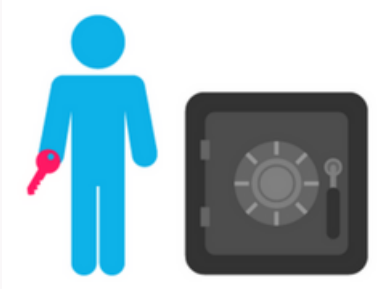
Therefore, bitcoin is still totally safe from double spending attack.

04
PART

Comparisons of Different Consensus Algorithms

Proof-of-work (PoW) vs Proof-of-stake (PoS)

PoW: Its core idea is to allocate the accounting rights and rewards through the hash power competition among the nodes.



PoS: The new block is chosen depending on miners' wealth, also defined as stake.

It is believed that people with more coins would be less likely to attack the network.

The stake is described by (coin*age).

For example:
Miner A has $1 in 20 days => 20 coin*age
Miner B has $2 in 40 days => 80 coin*age

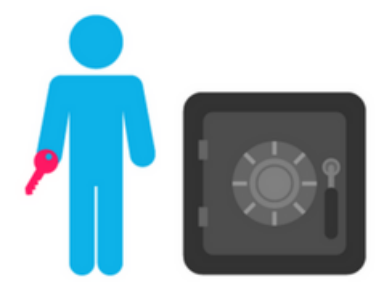
Difficulty Formula: hash < (coin*age)*target

=>The new block generating probability for B is 4 times than A.

Proof-of-work (PoW) vs Proof-of-stake (PoS)

Pros:
1) Widely tested and used from 2009
2) Easy to practice
3) Need relative cost to launch attack

Cons:
1) Waste of resource and energy
2) Slow transaction confirmation
3) Concentration of hash power



Pros:
1) Save energy and cost
2) Attack cost is extremely high
3) Stable network

Cons:
1) Poor fluidity
2) The rich get richer,
   the poor get poorer
3) "Nothing-at-the-stake" Attack

Comparison of Typical Consensus Algorithms

characteristics	consensus algorithms				
	PoW	*PoS*	*DPoS*	*PBFT*	*RAFT*
Byzantine fault tolerance	50%	50%	50%	33%	N/A
crash fault tolerance	50%	50%	50%	33%	50%
verification speed	>100s	<100s	<100s	<10s	<10s
throughput(TPS) (transaction per second)	<100	<1000	<1000	<2000	>10k
scalability	strong	strong	strong	weak	weak
Node identity	open	open	open	close	close
Energy saving	waste	partial	good	better	better

Practical Byzantine Fault Tolerance (PBFT):

PBFT was proposed to make original BFT more efficiently.

PBFT has a master sever to manage client request.

Delegated Proof-of-Stake (DPoS):

If PoS is direct democratic, DPoS can be viewed as representative democratic.

Stakeholder can elect different delegates at each round to generate and validate new block.

RAFT Algorithm:

RAFT has strong consistency, and is a highly available distributed protocol used in engineering.

RAFT achieves consensus via an elected leader. The leader is responsible for log replication to the followers.

Suitable Scenario for Each Consensus Algorithms

TABLE I: Comparisons among *public blockchain*, *consortium blockchain* (*permissioned blockchain*) and *private blockchain*

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned
Suggest algorithm	**PoW, PoS, DPoS…**	**PBFT, IBFT, DPoS, Ripple…**	**RAFT, PBFT, Paxos…**

Current blockchain systems are categorized into three types:
public, permissioned, and private chains.

About consensus determination,
All miner can take part in public chain.
Only selected node can take part in consortium chain.
Fully controlled by one organization for private chain.

Transactions in a public chain are visible and nearly impossible to be tampered, but it depends when it comes to private or consortium chain.

Famous consortium chain:
1)Hyperledger Fabric (IBM) uses PBFT
2)Quorom (JP Morgan) uses IBFT

05
PART

Conclusions

Conclusions

1) Blockchain use distributed p2p network to make the ledger immutable.

2) The so-called consensus is the idea that multiple nodes consistently agree on something, even in the case of partial node failure, network latency, and network segmentation.

3) The 51% attack means the 51% hash power, not 51% nodes.

4) A good consensus algorithm means efficiency, safety and convenience.

5) It is necessary to learn pros and cons of every consensus algorithms, and hybrid use possibility, reliability, etc. Therefore, the appropriate consensus is adopted according to the actual scenarios.

6) Consensus algorithm is the core technology of blockchain, but how to make the blockchain performance better in a particular scenario? It still needs further research.

THANKS