Second Assignment

Name： 余韦藩 **ID：** 2020285102

1. Compare consensus mechanisms such as Paxos, Raft, PBFT, PoS, DPoS, Algorand (VRF), DAG, and Hashgraph.

Answer:

1. First, I will compare the following consensus mechanisms Paxos, Raft, PBFT, PoS, DPoS, Algorand, DAG and Hashgraph in the aspect of the application environment, complexity, maximum fault tolerance as shown in the following figure.

	Paxos	Raft	PBFT	PoS
Application environment	private blockchain	private blockchain	consortium blockchain	public blockchain
Complexity	-	O(n)	$O(n^2)$	-
maximum fault tolerance	2f+1<=N	2f+1<=N	3f+1<=N	2f+1<=N
	DPoS	Algorand	DAG	Hashgraph
Application environment	public blockchain	public blockchain	public blockchain	private blockchain
Complexity	-	-	-	-
maximum fault tolerance	2f+1<=N	3f+1<=N	-	3f+1<=N
Advantage				
Disadvantage				

2. Next, we state the advantage and disadvantage of the DAG.

DAG:

Advantage: (1)Fast transaction speed (2)Strong expansibility

Disadvantage: (1)Uncontrollable transaction duration (2)Strong consistency is not supported

3. We compare the BFT and PoS (DPoS) in detail. BFT and PoS (DPoS) are consensus in distributed peer-to-peer networks. There are several

differences between the two.

(1) From the perspective of the scale of nodes involved in consensus:

In a network composed of n nodes, the time complexity required for BFT algorithms to complete a round of consensus is O (n^2), so the scale of the network is limited. At the beginning of the consensus process, the "master node" needs to be selected from the nodes to issue a proposal. Therefore, a trusted node identity list needs to be maintained, which has low scalability. Large scale networks usually adopt federal Byzantine protocol or proxy voting consensus, with a high degree of centralization.

In the network with PoS or DPoS consensus, all nodes compete for accounting rights according to certain resources they own, which can achieve a lower degree of centralization and relatively high scalability in theory.

(2) From the perspective of selecting a account-keeping(记账) node:

The BFT consensus is to replace the "master node" in turn and issue the block proposal. All nodes directly vote on the block, which is called reaching a consensus directly. There is no accounting node in strict sense. PoS or DPoS consensus selects accounting nodes through fixed rules, determines the content of blocks by accounting nodes, and then selects possible branching chains through certain rules, which is called indirect consensus.

(3) In the perspective of the finality of the consensus:

BFT consensus will not be restructured or bifurcated after blocks are recorded in the blockchain history. Even without malicious nodes, PoS or DPoS consensus is likely to bifurcate. It is necessary to reach consensus on the chain through certain rules. PoS or DPoS consensus usually requires certain block confirmation, sacrificing transaction efficiency to ensure decentralized consensus consistency.

(4) From the perspective of the incentive layer of consensus:

BFT consensus has no mining process, and there can be no incentive mechanism. However, PoS or DPoS consensus requires an incentive mechanism to constrain accounting nodes from breaking the blockchain, and increase the cost of malicious nodes launching attacks.

(5) From the perspective of the actual performance of the network:

BFT consensus is a direct consensus, so the response time (the time from broadcast to confirmation of a transaction) is fast and the transaction carrying capacity is high. PoS or DPoS consensus, due to the limitations of objective block capacity, block output speed and network communication delay, can only sacrifice transaction carrying capacity and response time to ensure network security. Compared with BFT, PoS or DPoS has the advantages of scalability and decentralization.

2. Briefly describe the concepts and principles of smart contracts and contract accounts.

Answer: (1) Smart contracts is a computer program that runs on a distributed ledger with preset rules. When the network reaches up to its set status and condition, the smart contracts will response to the distributed nodes with corresponding action according to the preset rules. Smart contracts apply to complete information exchange, value transfer, and asset management.

(2) Contract accounts is a separate account that forms the methods of interaction between various Ethereum smart contracts and contract stakeholders. A contract account is prepared to find out the cost of the contract and to know the profit or loss made on the contract. Through contract account, other similar contracts can be undertaken on the basis of the current contract.

3. What is the blockchain CAP principle and the triangular impossibility.

Answer: (1) CAP principle: In a distributed system (a collection of interconnected nodes that share data), you can only have two of the following three guarantees across a write/read pair: decentralization, scalability, and security. In other words, one of them must be sacrificed.

(2) The triangular impossibility: In a distributed system, you can only have two of the following three guarantees across a write/read pair: consistency, availability, and partition tolerance. In other words, one of them must be sacrificed.

4. Briefly describe the principles of stablecoins.

Answer: Stablecoins is a kind of a digital currency with stable value, which are linked to certain stable assets, such as gold, dollar, etc so that the unit price of the currency also represents a certain purchasing power. While they have some similar characteristics of Bitcoin, they will not rise and fall its value dramatically like Bitcoin. These advantage makes stablecoins more suitable for value storage, exchange medium and unit of account.