EDU

CSDN学院　IT实战派

比特币和区块链的相关技术细节

区块链的共识算法

讲师：康烁

本节目标

1. 理解中本聪共识算法
2. 理解POS共识算法
3. 了解无利益攻击
4. 理解DPOS共识算法

中本聪共识（POW）

POW：通过算法生成的一组数据，难于生成而易于验证

比特币使用的Hashcash proof of work这样的POW算法。由Adam Back发明，用于防止垃圾邮件和拒绝服务攻击。

Hashcach proofs of work被中本聪用于比特币的挖矿。

挖矿的过程是选择一个节点作为区块产生者。

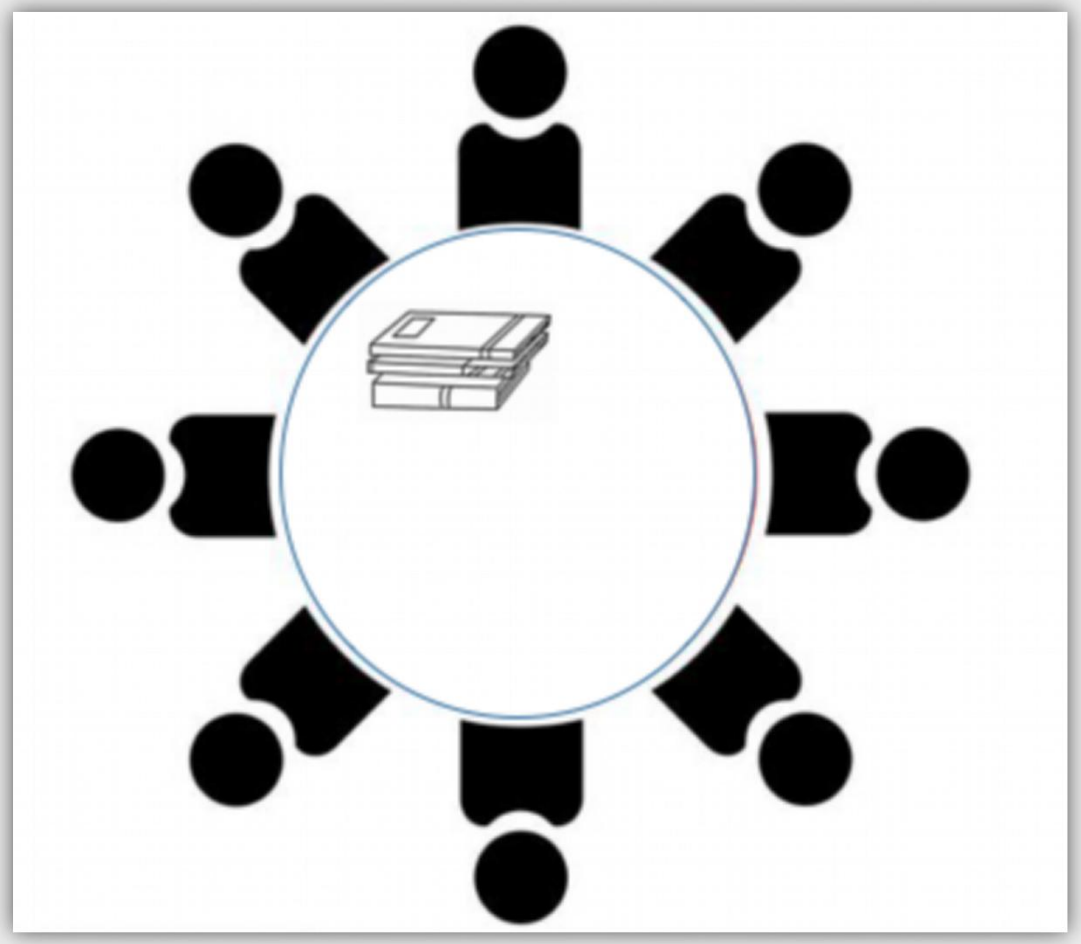
POS共识

POS：最早由一个网名为“QuantumMechanic”的网友在比特币论坛中提出。其核心思想为

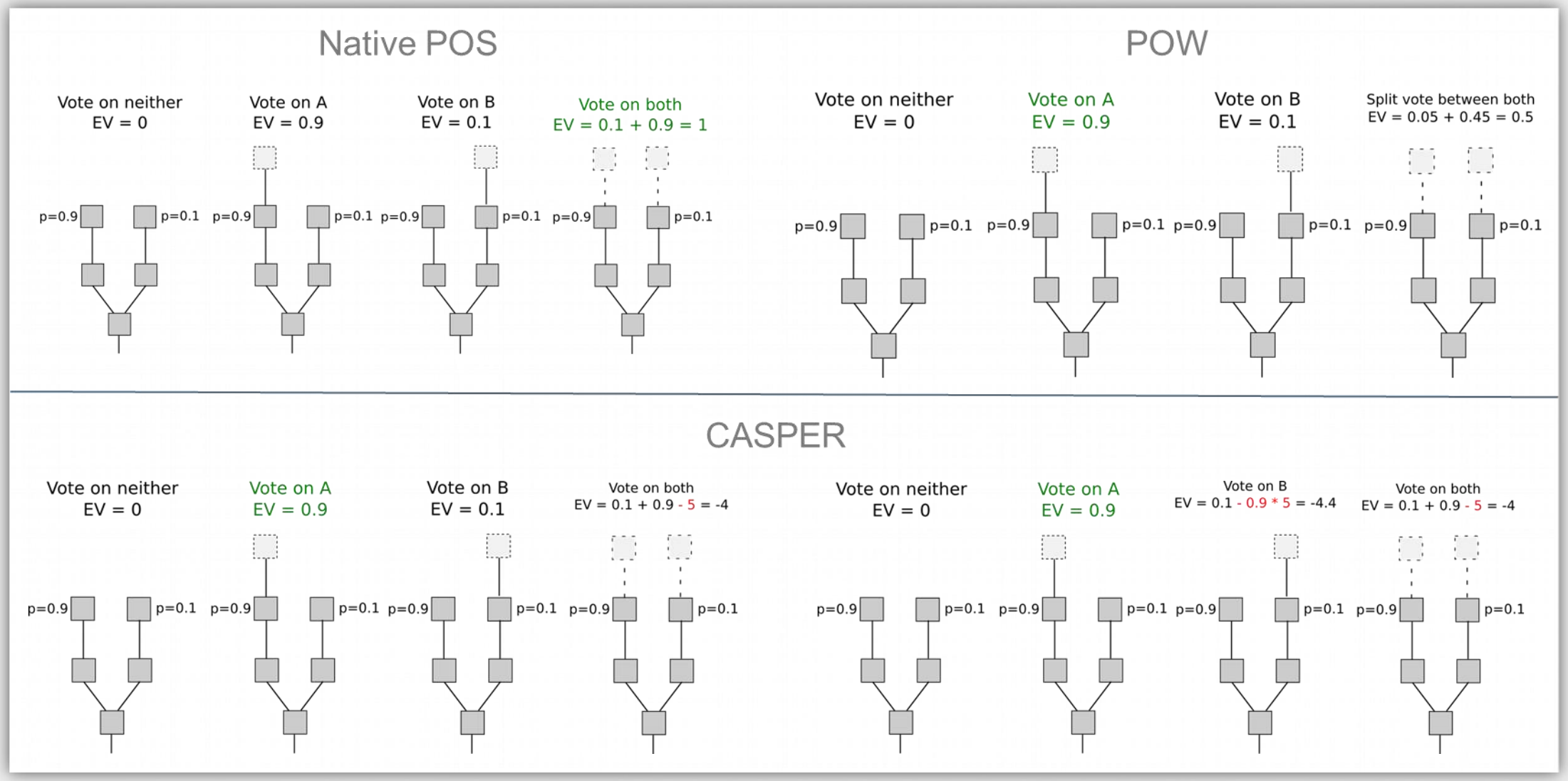
https://bitcointalk.org/index.php?topic=27787.0

https://en.bitcoin.it/wiki/Proof_of_Stake

Native POS的面临的问题：nothing_to_stake



CASPER VS Native POS VS POW



DPOS：Delegated Proof of Stake

1. DPOS由BM提出：由代币持有者选择见证人节点，由一组见证人通过round-robin的方式轮流产生区块
2. DPOS对Nothing_to_stake的应对方案：让生产者被淘汰，"Miners" are now generally public, known individuals rather than anonymous individuals.
3. https://bitsharestalk.org/index.php?topic=18720.0

不同共识算法的观点

1. POW共识算法目前最有效
2. POS共识算法经过了长时间的探索还在发展中
3. DPOS共识算法是一种接近于中心化的解决方案

总结

1. P2P网络和数字签名
2. 哈希函数的原理
3. 哈希指针的原理和作用
4. 比特币的账户和交易
5. 共识算法和区块链

布置作业

- 必做内容：
- 了解区块链中各种共识机制的不同之处

EDU

CSDN学院　IT实战派