EDU

CSDN学院　IT实战派

以太坊基础

以太坊的性能解决方案

讲师：康烁

本节目标

1. 以太坊的性能瓶颈
2. 以太坊的性能瓶颈的解决思路

以太坊性能瓶颈

以太坊交易速度为每秒7笔（7TPS）

性能公式：

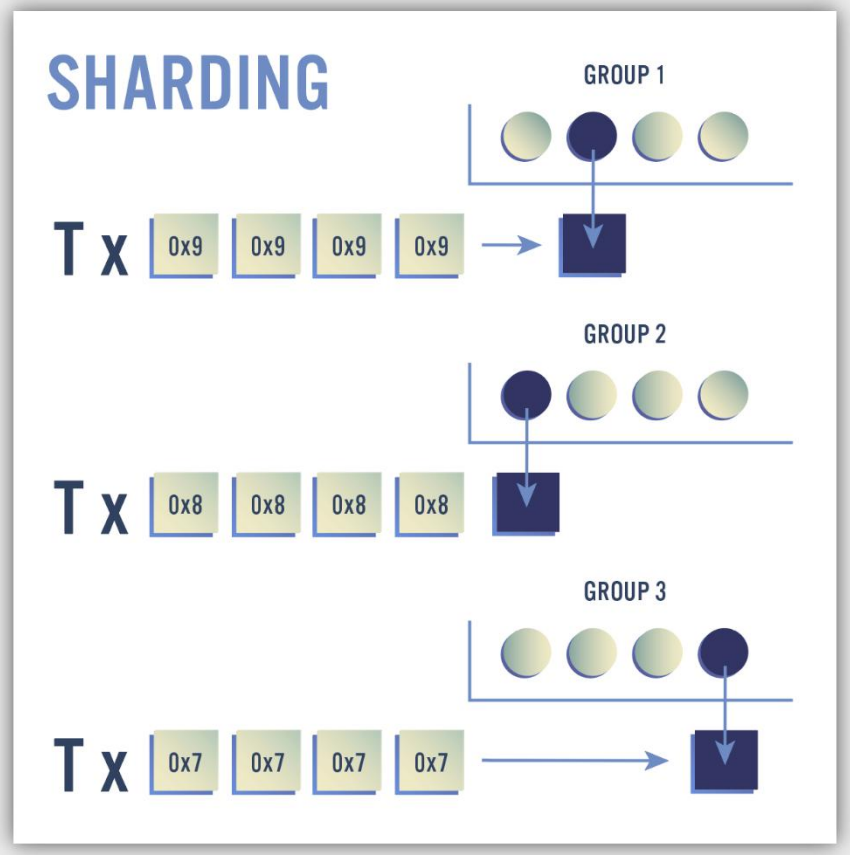
TPS = concurrency * blocksize / block_gen_internal

结论：

- concurrency -> 分片
- 加大块大小 （blocksize）
- 加快块产生速度(减小block_gen_internal) -> 改进共识算法

增加concurrency——以太坊分片方案

基本思想：把以太坊的节点进行分组，并把不同的交易分组，交给以太坊节点中的一组节点来确认。



文档：https://github.com/ethereum/sharding/blob/develop/docs/doc.md

加快块产生速度——改进共识算法：Algorand

来自MIT的CSAIL实验室，SOSP`17 ，

https://dl.acm.org/citation.cfm?id=3132757

核心技术：Verified Random Function

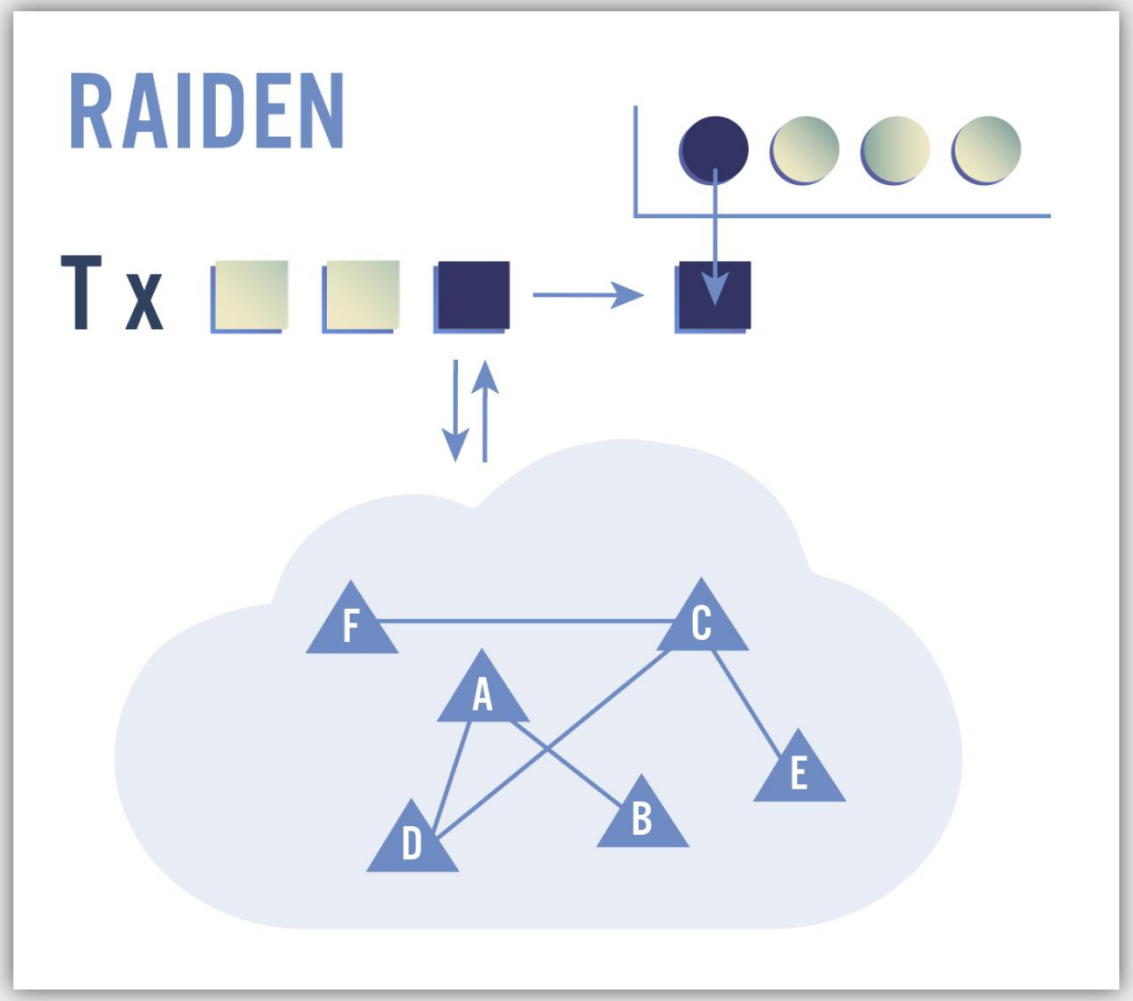
是一种POS的实现，用VRF随机选中一组用户来投票选举块生产者，被选中的用户能够在发送消息中包含他们被选中的证明

性能

通过在1000台虚拟机网络中测试，吞吐量是比特币的125倍，交易确认时间小于一分钟

链下状态通道

链下处理，相对比较容易且经过验证的方案。



链下状态通道应用示例（五子棋区块链应用）

- 示例：Alice和Bob下五子棋来对赌，每人都需要下注（红色为链上操作）
- 步骤0：在智能合约上部署五子棋智能合约，里面有下棋规则和输赢判断标准。并可以保存和转移玩家的押金
- 步骤1、Alice和Bob分别把押金放到以太坊智能合约上
- 步骤2、Alice把自己的公钥发给Bob和智能合约，Bob把自己的公钥发给Alice和智能合约
- 步骤3、Alice先走棋，把自己走棋落点和时间进行签名发给Bob
- 步骤4、Bob收到Alice经过签名的走棋步骤，然后再走一步，并且把走棋落点和时间签名发给Alice
- 步骤5、重复步骤3和4，直到Alice或者Bob某一方认为胜负已分
- 步骤6、Alice和Bob中的胜者把胜负结果，走棋的所有步骤打包签名，发给智能合约，要求获得赌金
- 步骤7、智能合约收到Alice或者Bob发来的下棋结果，等待一段时间的争议期，如果在争议期中没有人质疑，则赏金直接发给宣称获胜的胜者
- 步骤8、如果步骤7中另一方提交了不同的棋局，宣称有争议。则智能合约负责验证下棋步骤，对作弊者进行惩罚

总结

1. 以太坊是一个运行智能合约的全球计算机
2. 以太坊的性能瓶颈和几种解决思路

布置作业

- 必做内容：
- 分析以太坊的性能瓶颈

EDU

CSDN学院　IT实战派