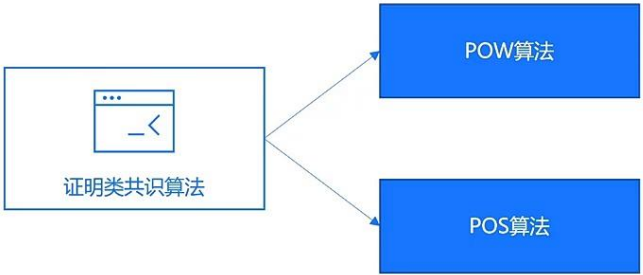
蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

证明类共识算法概述

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

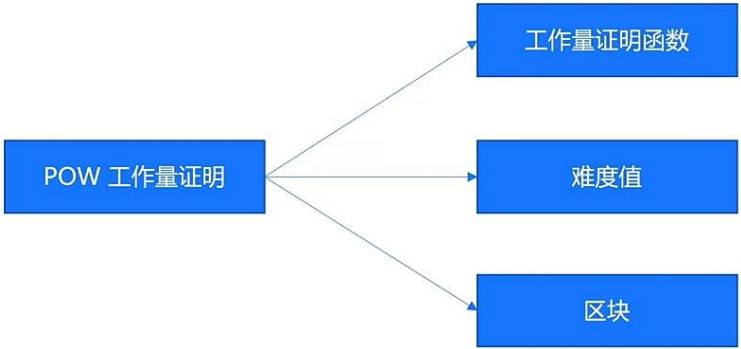
证明类共识算法概述

证明类共识被称为“Proof of X”类共识，即节点在每一轮共识过程中必须证明自己具有某种特定的能力，以获得记账权和奖励。



POW机制

POW 采用按劳分配的原则，将算力作为记账的主要指标，算力大的节点将有更多的机会在区块链上进行记账。



POW机制——记账策略

- 首先，客户端产生新的交易，向全网广播
- 第二，每个节点收到请求，将交易暂存于存储池中
- 第三，每个节点进行pow工作量证明
- 第四，当某个节点找到了证明，向全网广播
- 第五，当且仅当该区块的交易是有效的且在之前中未存在的，其他节点才认同该区块的有效性
- 第六，接受该区块且在该区块的末尾制造新的区块

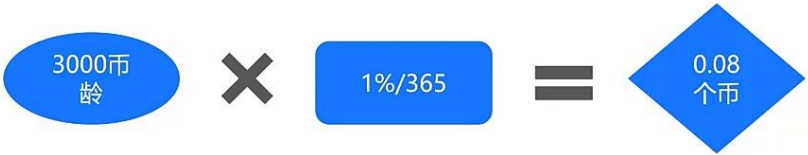
02 POS机制

PoS共识算法的基本概念

币龄，即持有货币的时间。这是POS机制难度值确定的核心

币龄计算举例：

利息，即在发现区块之后会根据一定的利率给付数字货币。



POS与POW共识算法比较

比较项	POW	POS
记账权获得	以算力竞争记账权利	以权益竞争记账权利
篡改难度	低	高
头部玩家	未能解决	未能解决

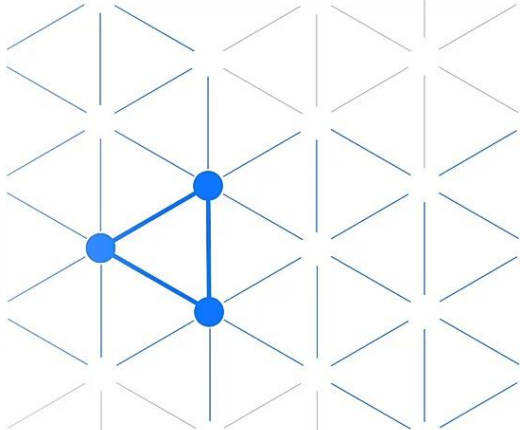
总结

- **证明类共识被称为“Proof of X”类共识，通过竞争的方式获得记账权，包括POW、POS等共识算法**

- **POW共识算法**
  - 主要基于算力实现记账权

- **POS共识算法**
  - 主要基于持有权益实现记账权

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN