蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

区块链共识算法演进

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

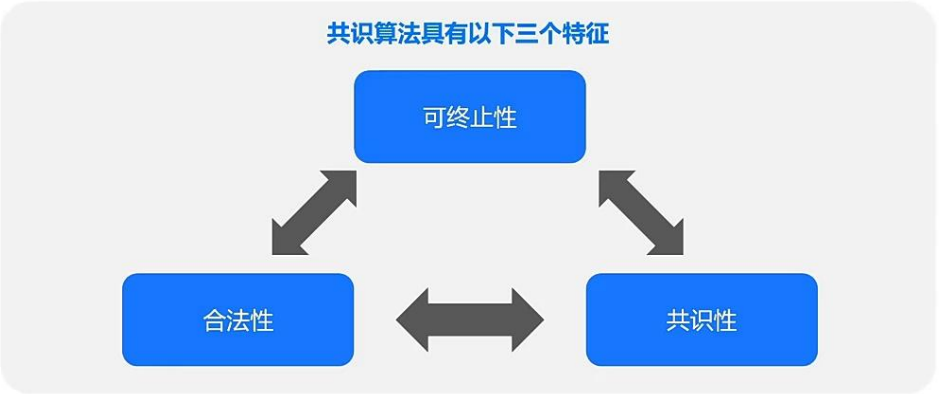
- 了解密码学共识算法演进过程

01 区块链共识算法演进

共识算法概述

工业和信息化部人才交流中心发布的《区块链产业人才岗位能力要求》对共识算法的定义是：

区块链系统中各分布节点对事务或状态的验证、记录、修改等行为达成一致确认的方法。



区块链共识算法的演进-一至三阶段

区块链共识算法演进大致可以分为五个阶段。

1959年

《主观概率的共识: 平衡-互惠方法》

首次以一致性问题为研究对象

1982年

正式提出拜占庭容错类算法

解决了网络存在恶意节点时如何达成一致的过程和算法。

少数服从多数的原则

1989年

提出Paxos算法开创非拜占庭容错类算法

解决了存在网络故障时如何达成一致的过程和算法。

少数服从多数的原则

区块链共识算法的演进-四至五阶段

2008 年10 月

中本聪发表论文开启区块链共识算法研究

提出POW共识算法。
解决了扩容问题，支持节点随时加入与离开。

少数服从多数+工作量证明

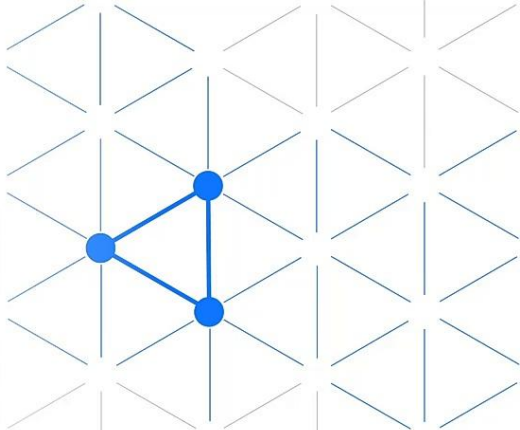
2008 年之后

学者们在共识算法领域的研究如雨后春笋般涌现，先后提出PoS、DPoS、Raft 等一系列新的共识算法。

总结

- **共识算法就是用来保证分布式系统一致性的方法。**
- **区块链共识算法演进过程的里程碑算法**
  - 拜占庭算法、Paxos算法、中本聪算法

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN