蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

Avalanche和Algorand算法

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

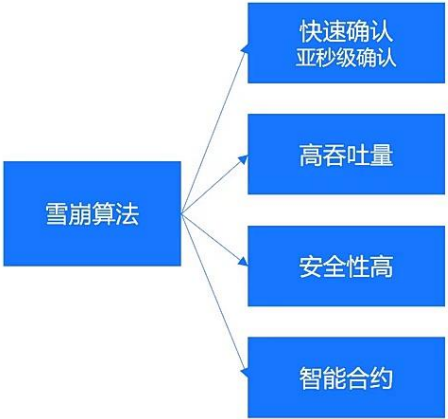
课程目标

- 了解Avalanche算法
- 了解Algorand算法

01 Avalanche概述

Avalanche简介

- 《Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies》
- 亚秒级共识、高吞吐量、高安全性、全智能合约研发生态
- Avalanche 是共识算法的重大突破和创新。将传统分布式一致算法与经典区块链共识机制的设计思想结合。



Avalanche核心约定

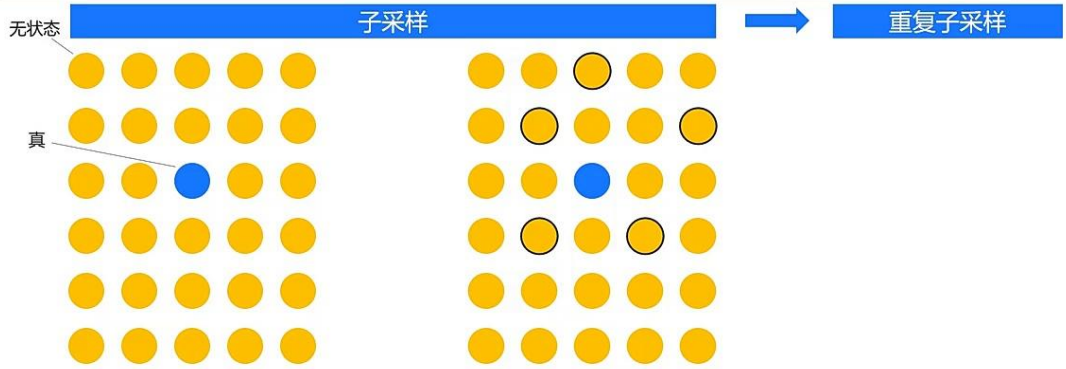
算法提出了一组『拜占庭容错』协议（简称『共识家族 Consensus family**』）。**
『共识家族』对诚实节点（Correct nodes**）和恶意节点（Byzanting nodes）的**
行为作了提前约定。如下：

- 诚实节点之间绝不会提交彼此有冲突的业务，而恶意节点也无法制造与诚实节点的冲突。
- 恶意节点可以制造许多彼此冲突的业务提交，而诚实节点只会接受其中一个提交。

Avalanche共识过程-第一阶段 · Slush

Avalanche 共识的发展经历了四个阶段，每个阶段（共识家族协议）都在前一个基础上进行了升级。

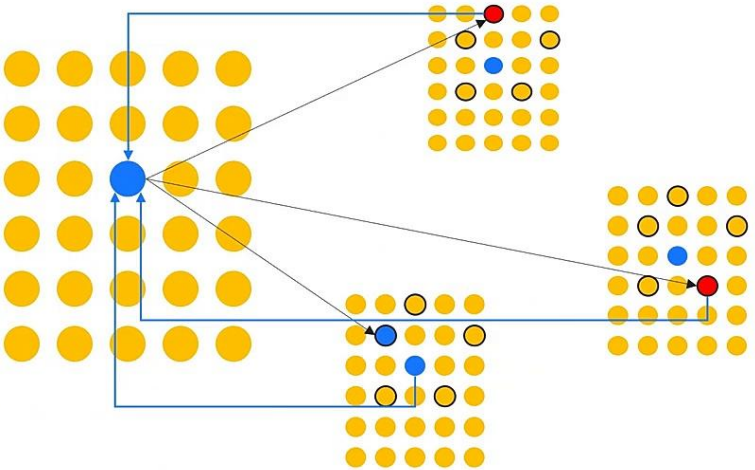
Slush 协议规定每个节点都有三种状态，即无状态、真和假，分别用黄色、蓝色和红色表示。



- 某个节点收到交易后，该节点作为发起节点
- 假设该节点选择蓝色，即接受交易

- 随机选择 5 个节点，询问各节点的选择
- 根据少数服从多数原则，确定小样本的倾向

Avalanche共识过程-第一阶段-重复采样



Avalanche共识过程-第二阶段

Snowflake协议

在 Slush 的基础上对每一个节点增加了一个计数器（counter）。具体来说：

- 每个节点都有一个计数器；
- 每一轮子采样完成后，如果颜色与上一轮相同，则计数器加1；
- 每一轮子采样完成后，如果颜色不同，则计数器重置为0；
- 当计数器的值超过阈值 β 时，则接受该节点所倾向的颜色。

- 图示和第一阶段一样。走和第一阶段同样的网络传播过程。

Avalanche共识过程-第三、四阶段

第三阶段——Snowball协议

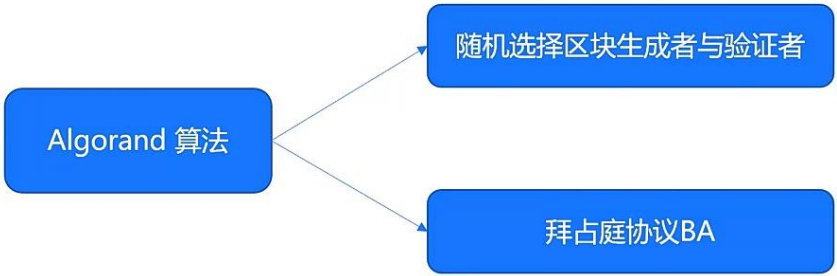
Snowball 在 Snowflake 原有计数器基础上增加了置信度（confidence），通过概率算法，减少随机扰动。

第四阶段——Avalanche协议

在 Snowball 的基础上添加有向无环图。一个 DAG 节点可以有多个父节点和多个子节点，而线性结构的节点只能有一个父节点和一个子节点。

Algorand共识算法

Algorand 利用 VRF 函数（可验证随机函数） 将区块产生者和投票者的选举随机化，让恶意节点难以攻击。



Algorand共识算法·随机选择区块生成者与验证者。

在第一轮种子是系统随机生成，但是后轮次中，种子是前一轮种子和轮数的VRF的随机结果。

凭证=VRF（种子+节点私玥签名+轮数）。

节点将区块与凭证广播，凭证出现概率小于某个值的节点成为验证者。

验证者中凭证值最小的数为领导者。

领导者广播的块将成为下一步验证的区块。

Algorand共识算法

拜占庭协议BA·一个两阶段投票机制

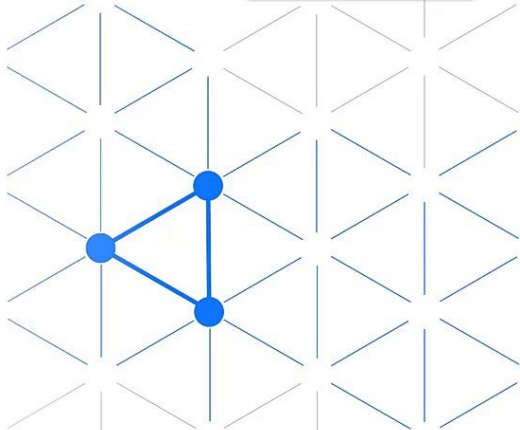
03 总结

总结

- **Avalanche协议**
  - 利用『朋友圈』散布消息，实现网络快速达成数据一致

- **Algorand 协议**
  - 让作恶者找不到投票人，使投票人放心地快速达成共识，向全网传播经过安全认证的区块

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN