蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN

区块链的不可篡改性

- 蚂蚁链《区块链系统开发与应用》A认证系列课程

课程目标

- 了解区块链技术的不可篡改特征
- 了解链块式结构与默克尔树结构

课程目录

01 不可篡改

为什么区块链上的数据不可篡改

不可篡改的核心技术保证

为什么需要不可篡改

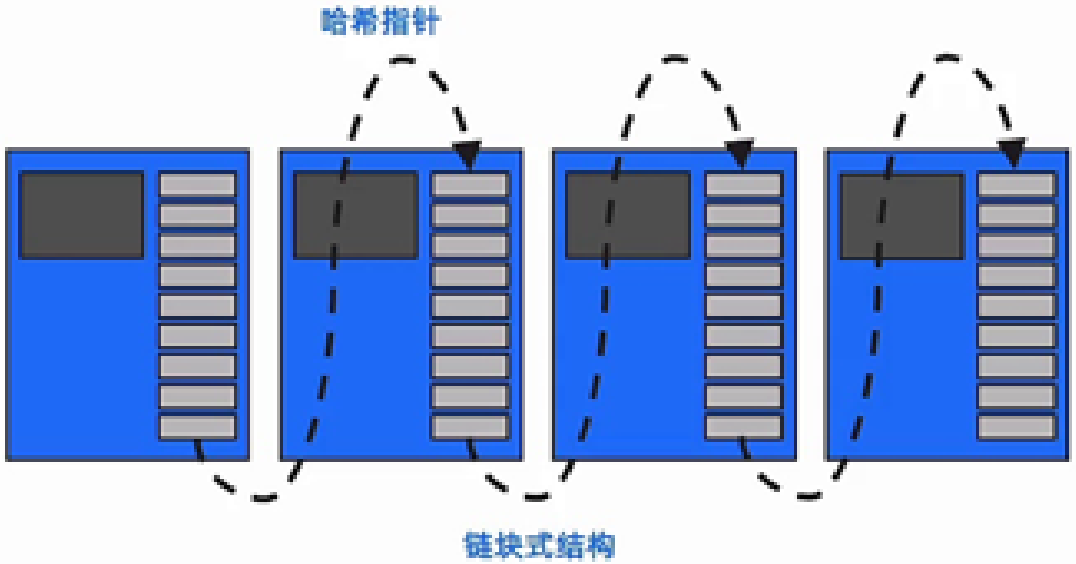
不可篡改的必要性

1.区块链要在开放的网络中实现一个可信的账本，数据安全是第一要求；

2. 数据安全的要素就是账本**不可损坏**和**不可篡改。**

不可篡改的技术实现

1. 分布式多点记账（P2P）保障账本安全、不可篡改的第一个手段；
2. 链块式结构 来保障账本安全、不可篡改的第二个手段。
3. 链块式结构 实现的关键点是哈希函数。

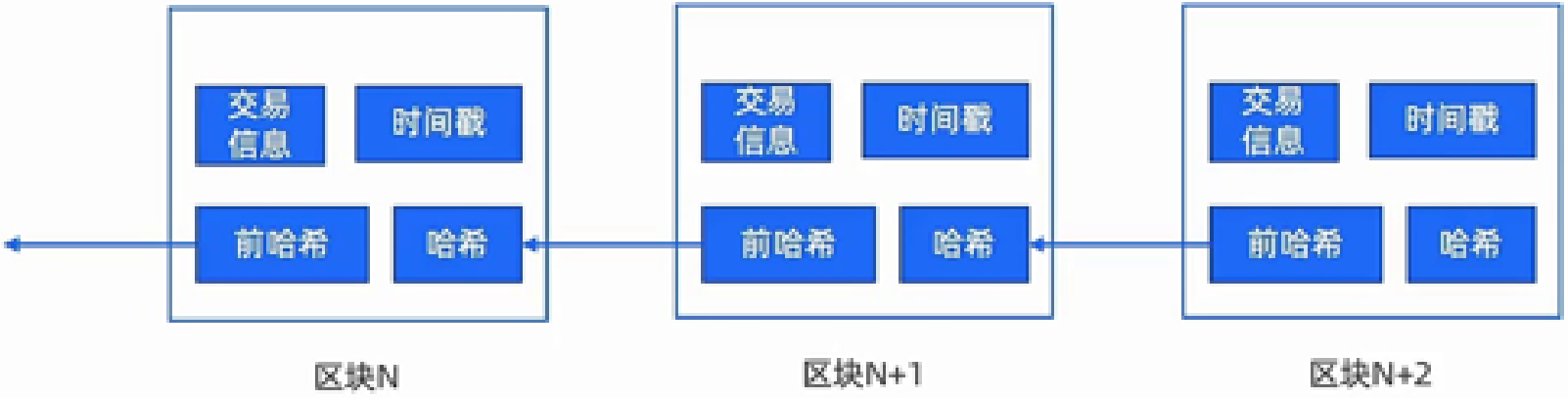


不可篡改的核心技术保证·哈希函数概念

1. 哈希函数一般翻译做散列、杂凑，或音译为哈希，是把任意长度的输入通过散列算法变换成固定长度的输出，该输出就是散列值。
2. 哈希函数是防碰撞的。

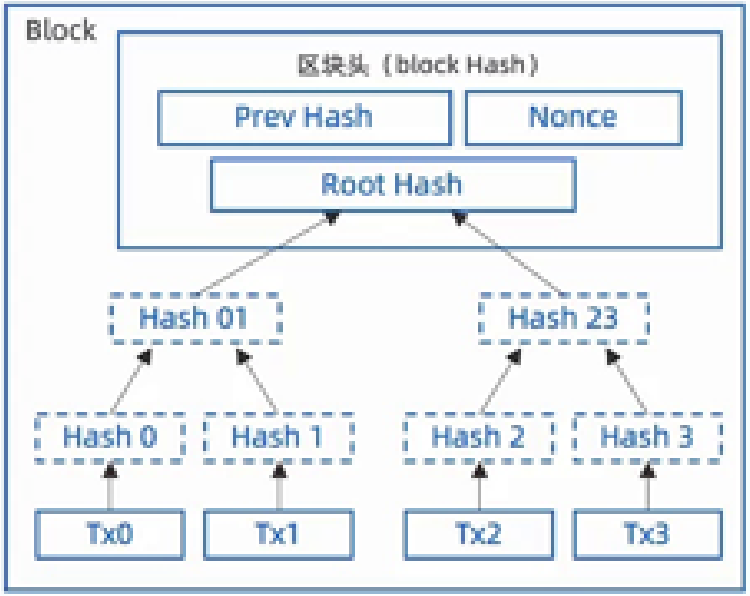
不可篡改的核心技术保证·哈希指针组成的链块式结构

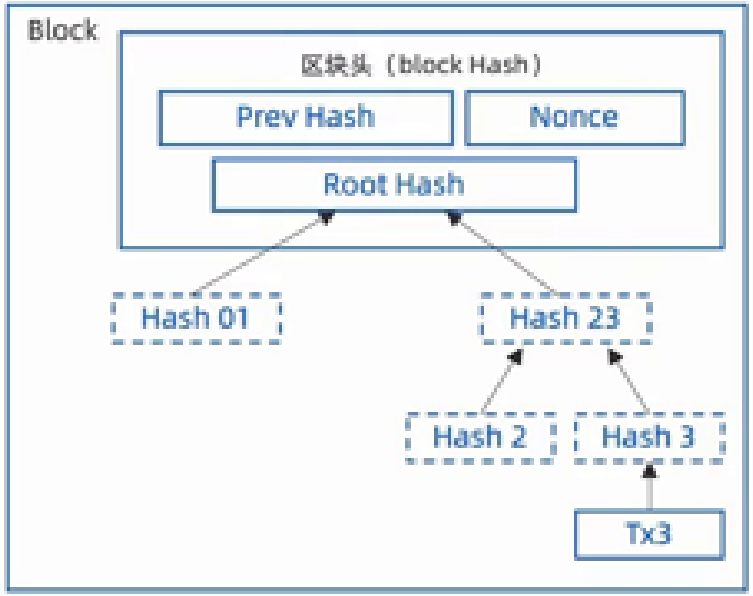
- 简单理解的话，可认为区块内包含**时间戳**、**交易信息**、**前块哈希**和**当前块哈希**。
- 后一个块内始终记录**前一块**的哈希值，通过后块始终可以找到其前块。



不可篡改的核心技术保证·默克尔树助力防篡改

- 一个区块分为**区块头**和**区块体**两部分。
- 区块哈希值由**前块哈希值**、**Nonce**（随机值）、**默克尔树根**、**时间戳**作为输入项计算获得，这些信息都记录在区块头中。





02 总结

总结

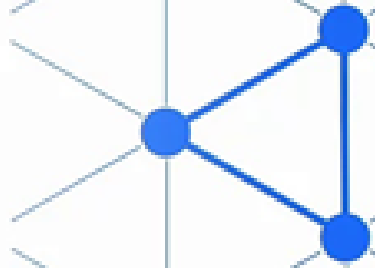
■ 不可篡改

- 可信账本必然要求不可篡改
- 区块链通过技术手段保证不可篡改

■ 不可篡改的技术实现

- P2P网络分布式记账
- 基于哈希函数的链块式结构
- 默克尔树

谢 谢



蚂蚁集团 ANT GROUP | 蚂蚁链 ANTCHAIN