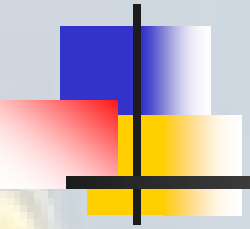
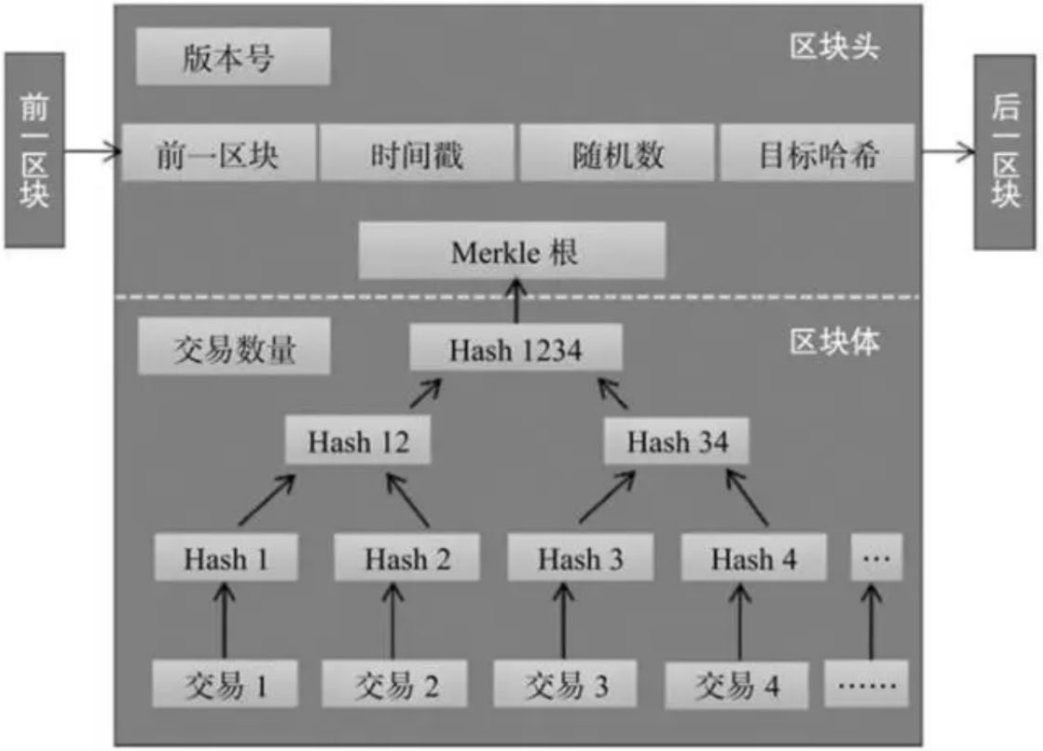
区块链基础与应用 2023



Summary

苏 明

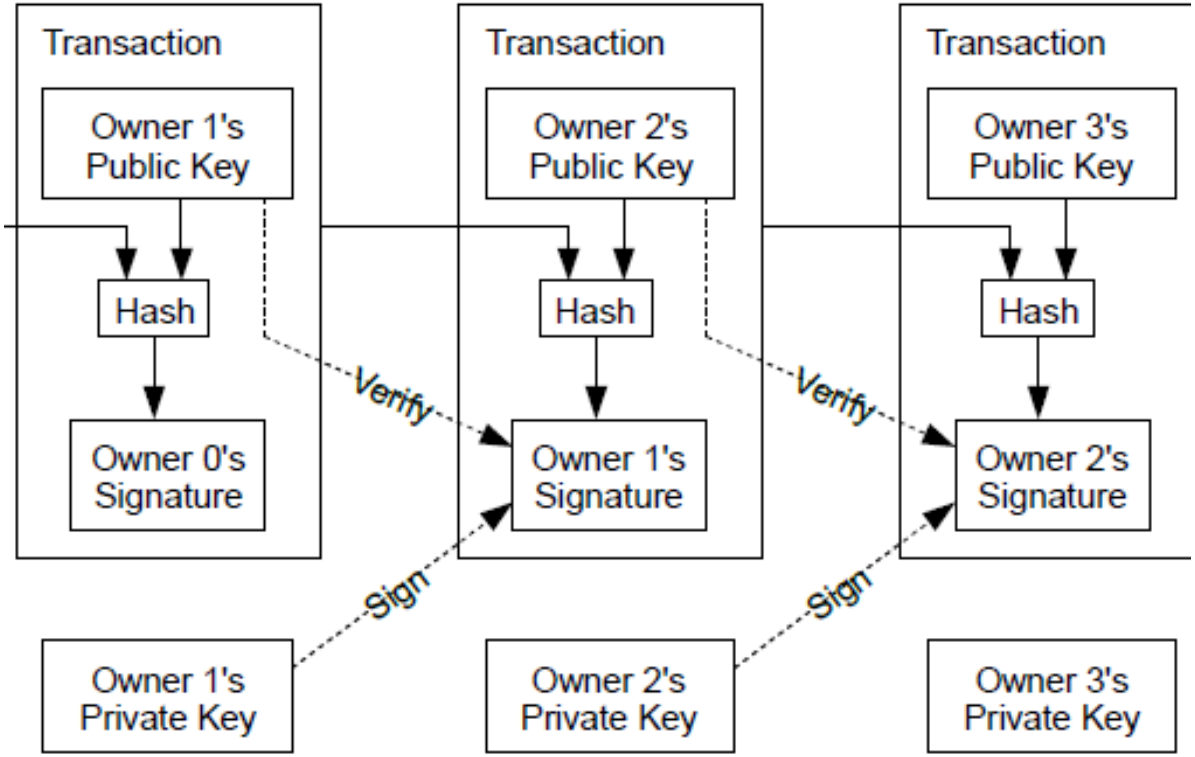
区块链的组织结构



数据项	描述	长度
Version	区块版本号	4字节
HashPreBlock	前一区块的Hash值256位	32字节
HashMerkleRoot	块交易记录的MerkleRoot节点的hash	32字节
Time	时间戳	4字节
Bits	压缩格式当前	4字节
Nonce随机数	从0开始的32位数	4字节

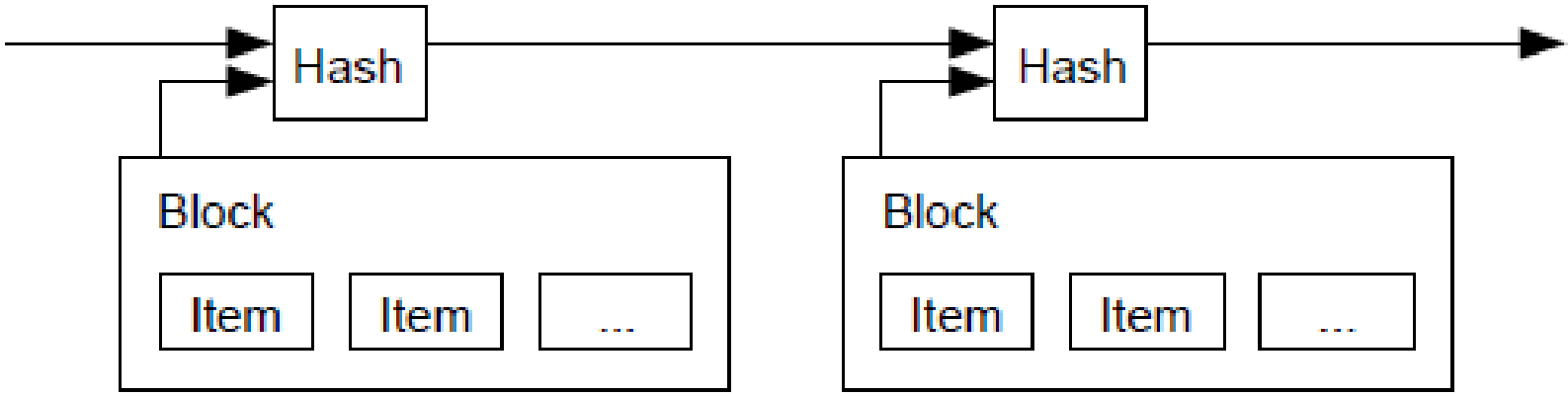
BlockChains & Bitcoin (1/9)

- 交易(Transaction)



BlockChains & Bitcoin (2/9)

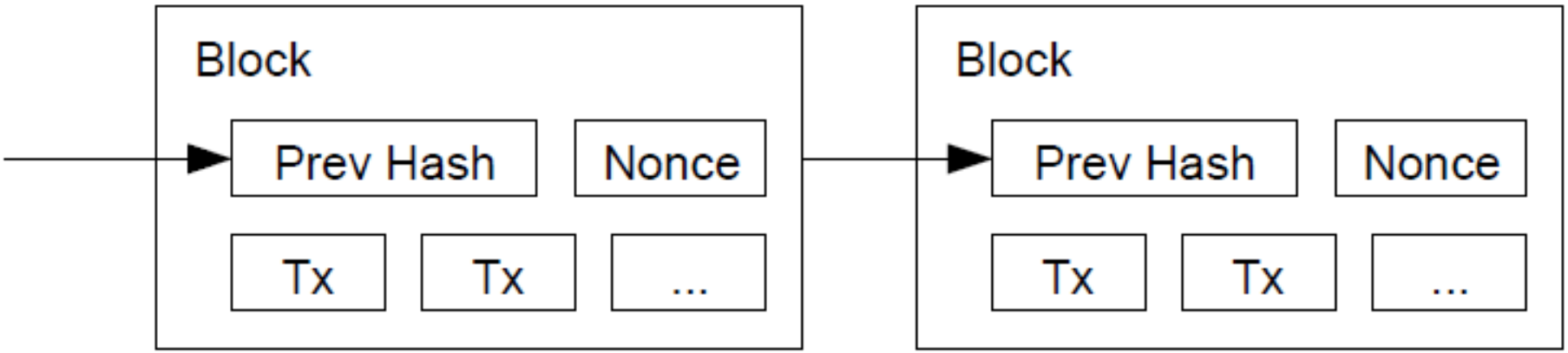
- 时间标签服务 (Timestamp Server)



时间对于整个比特币系统是很重要的。解决Double-spending的核心在于确认这笔交易在之前未发起过，因此如何在没有第三方的情况下明确时间顺序的先后成为重要问题。

BlockChains & Bitcoin (3/9)

- 工作量证明(Proof-of-Work)

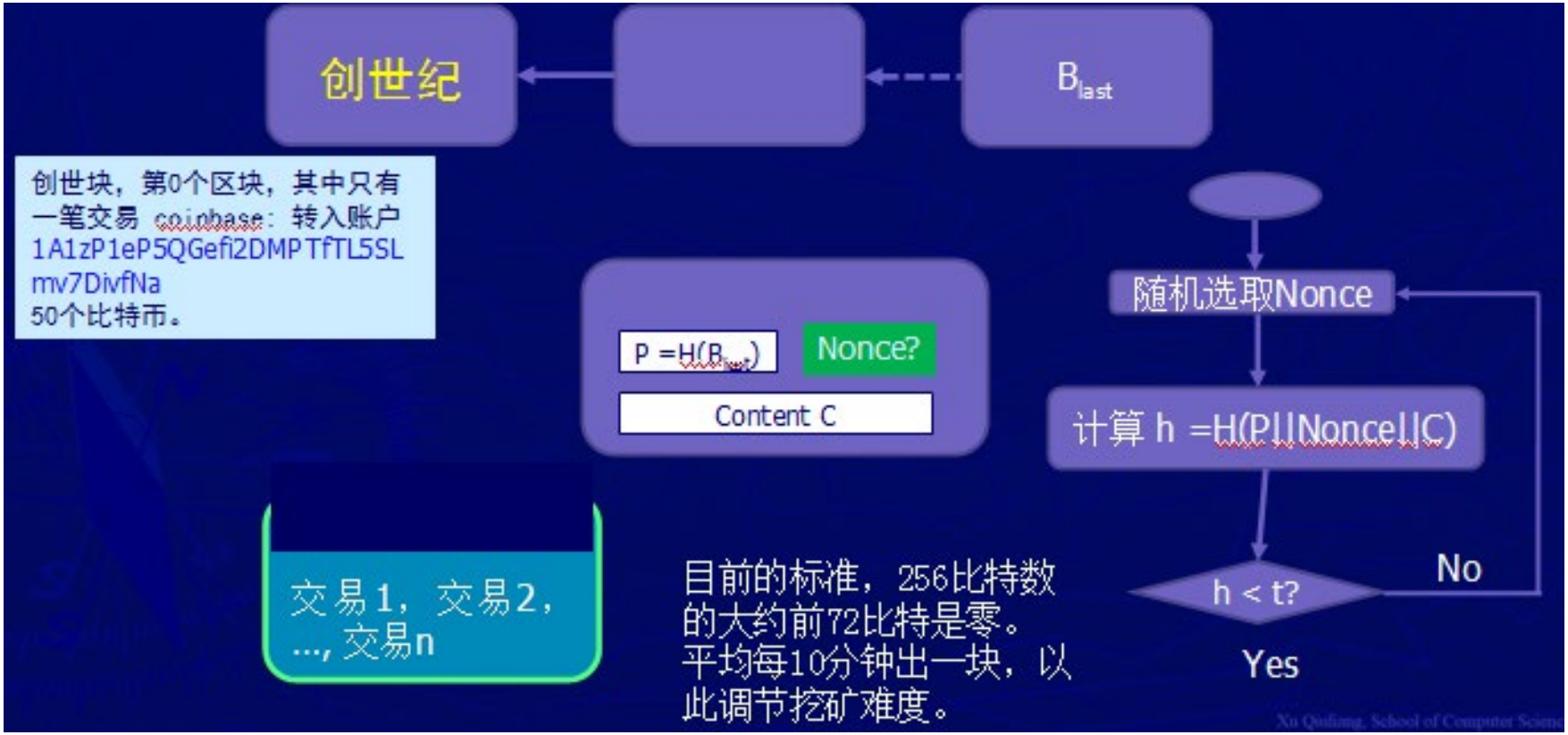


实现工作量证明的方式：逐次修改区块中的nonce直到**满足要求**的区块哈希值产生。

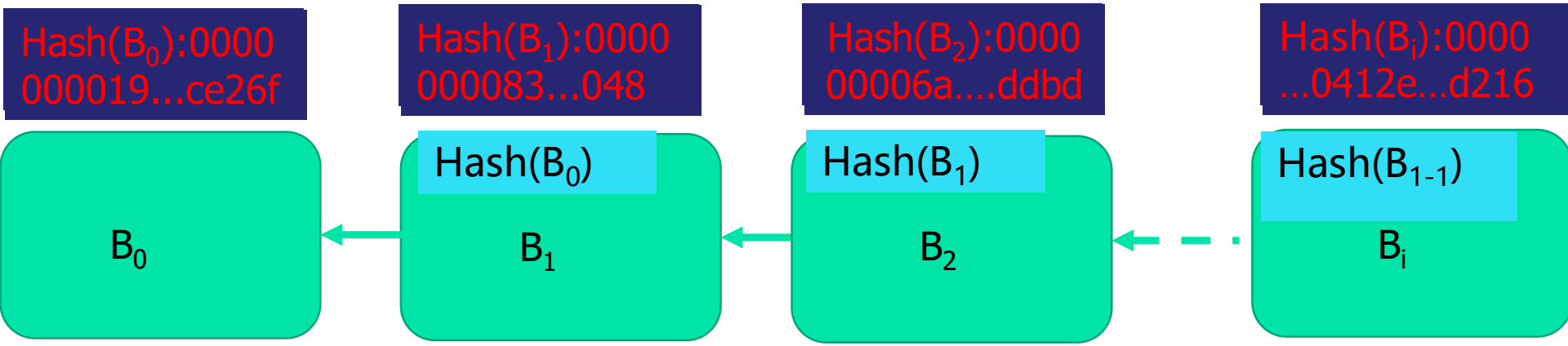
BlockChains & Bitcoin (4/9)

- 系统参数
  - 选取一个hash函数 H() = SHA256(SHA256())
  - 取一个门限值 t = 00000000FF…FF/d = 2^{224}/d.
  - 选取一个签名体制 EC-DSA
- 交易
  - 建立一个签名算法(sk, pk),
  - A = RIPEMD160(SHA256(pk))便形成一个账户。
  - 交易: (A, 2, B, sig_{skA}(A, 2, B),pk_A)

BlockChains & Bitcoin (5/9)

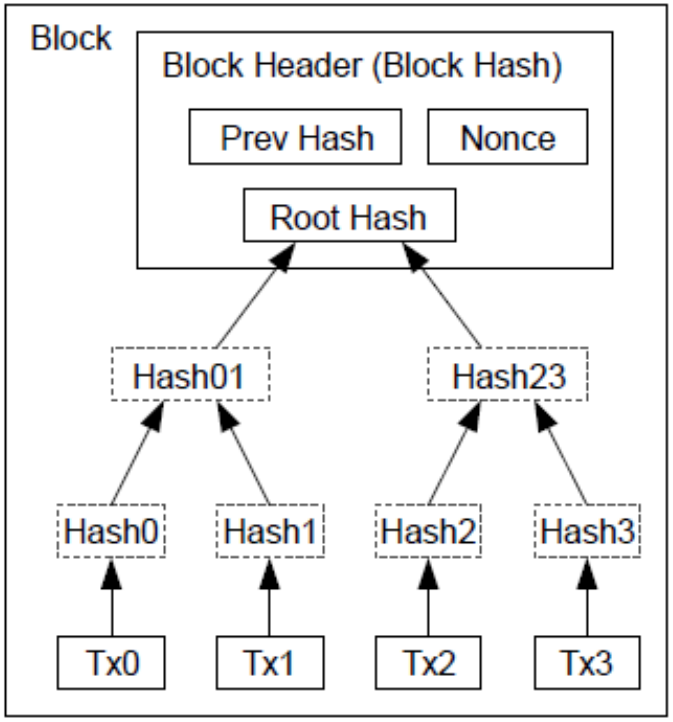


BlockChains & Bitcoin (6/9)

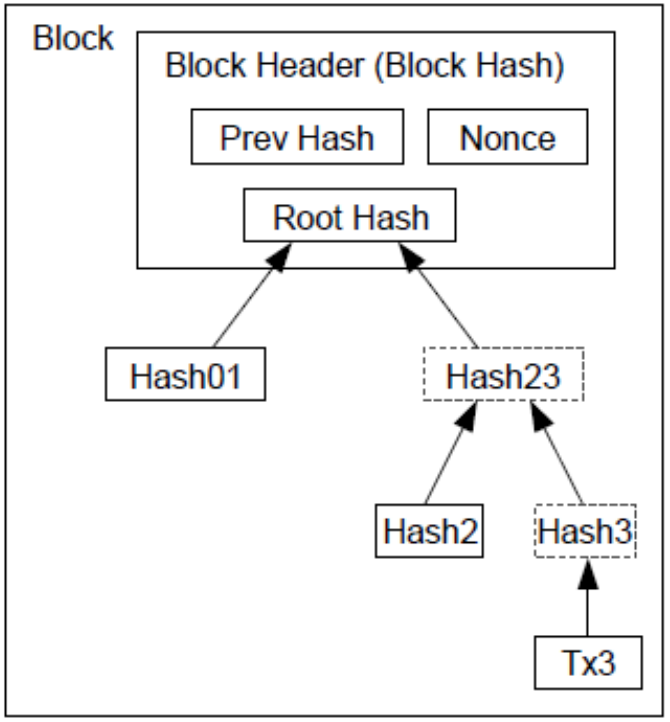


BlockChains & Bitcoin (7/9)

- 空间存储回收(Reclaiming Disk Space)



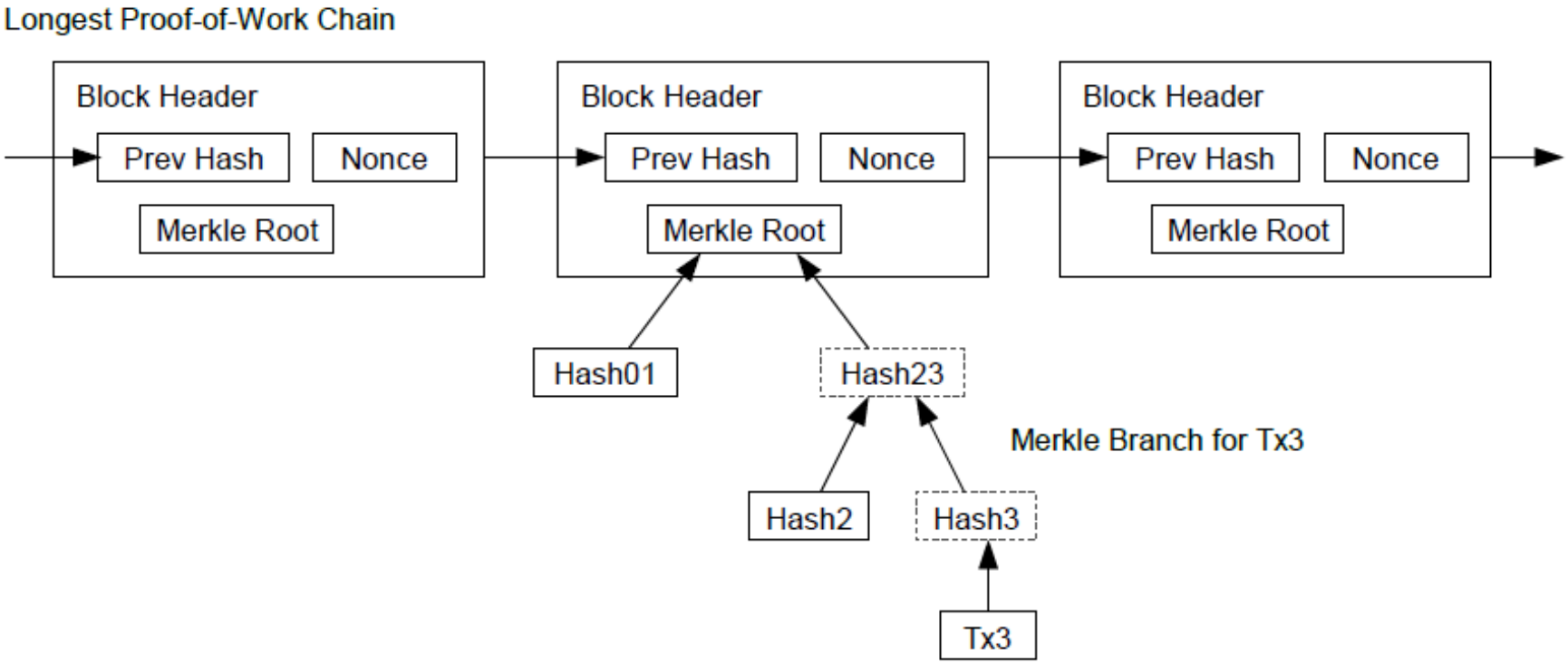
Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

BlockChains & Bitcoin (8/9)

- 交易验证 (Simplified Payment)



BlockChains & Bitcoin (9/9)

诚实大多数原理

- 算力主要消耗在挖矿、区块链的生成、交易确认中
- 系统稳定性的缺省信任基础：算力掌握在大多数诚实的用户手中，出于自身利益的考虑，这些用户也愿意维护区块链系统
- 比特币51%攻击理论：**攻击者要创造一条新链条，然后长度超越旧链条，覆盖旧链条**。如果现在只有1次确认，被覆盖的概率稍高，而到了6次确认，被覆盖的概率下降为接近"0"。

教学内容-1

Chapter 1 密码学及加密货币概述

1.1 密码学哈希函数
1.2 哈希指针及数据结构
1.3 数字签名
1.4 公钥即身份
1.5 两种简单的加密货币

Chapter 2 比特币如何做到去中心化

2.1 中心化与去中心化
2.2 分布式共识
2.3 使用区块链达成没有身份的共识
2.4 奖励机制与工作量证明
2.5 总结

Chapter 3 比特币的运行机制

3.1 比特币的交易
3.2 比特币的脚本
3.3 比特币脚本的应用
3.4 比特币的区块
3.5 比特币网络
3.6 限制与优化

Chapter 4 如何存储和使用比特币

4.1 简单的本地存储
4.2 热存储与冷存储
4.3 密钥分存和密钥共享
4.4 在线钱包和交易所
4.5 支付服务
4.6 交易费
4.7 货币兑换市场

教学内容-2

Chapter 5 比特币挖矿

5.1 比特币矿工的任务
5.2 挖矿所需硬件
5.3 能源消耗和生态环保
5.4 矿池
5.5 挖矿的激励和策略

Chapter 6 比特币和匿名性

6.1 匿名的基础知识
6.2 如何对比特币去匿名化
6.3 混币
6.4 分布式混币
6.5 零币和零钞
零知识证明、zk-SNARK、Tonado cash

Chapter 8 其他挖矿算法

ASIC Ristant PoW, Scrypt, Primecoin, Permacoin,...

Chapter 10 另类币和加密货币生态系统

另类币的介绍;
不可分割的交叉链交换;
以太坊和智能合约;

Blockchains More

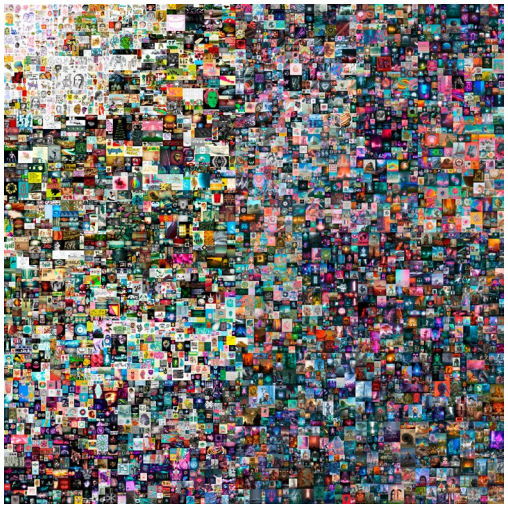
- (1) 区块链 1.0：没有任何的应用功能，以数字货币回报为主
- (2) 区块链 2.0：智能合约为上层应用开发提供基础设施支持
- (3) 区块链 3.0：对商业的颠覆在于其对生产关系的变革
- (4) 区块链 4.0：支持隐私计算

Blockchains More

Blockchains More

- NFT (Non-Fungible Token)

- Beeple的NFT画）（6937万美元）作 (Everydays：TheFirst5000Days



- 大火的NFT，防得住盗版防不住小偷？ --科技日报

Examination

- 判断题、
- 填空题、
- 解答题、
- 综合题、
- 难度题

涉及到算法，请写清楚逻辑结构(如伪码)，并解释

答疑 1.1 *计控楼450 15：00-16：00 PM*