区块链简介

Heyang Zhou

Dec 8, 2018

目录

- 两大区块链系统：比特币和以太坊
- 区块链 & 密码学
- 区块链 & 共识
- 区块链 & P2P 网络

比特币和以太坊

什么是区块链?

- 区块链 = 分布式账本 = 去中心化数据库?
- 保证事务及其局部或全局顺序在全网所有正确节点间的一致性

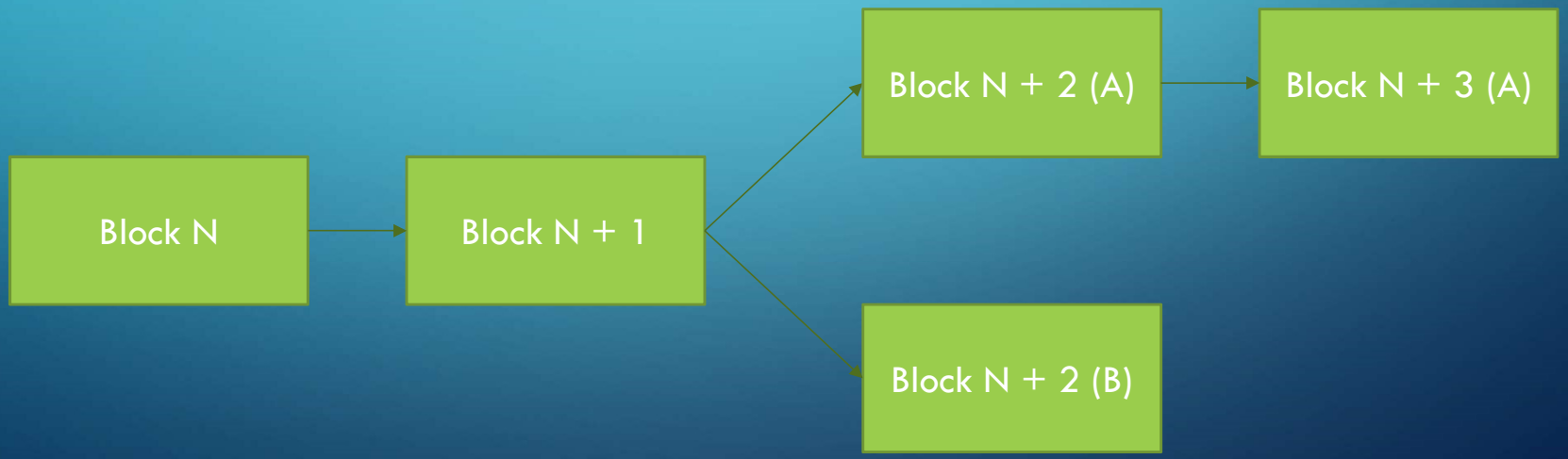
最早的区块链应用：比特币

- 比特币以区块形式组织交易
- 什么是区块?
- 区块 = 区块头 + 原始交易

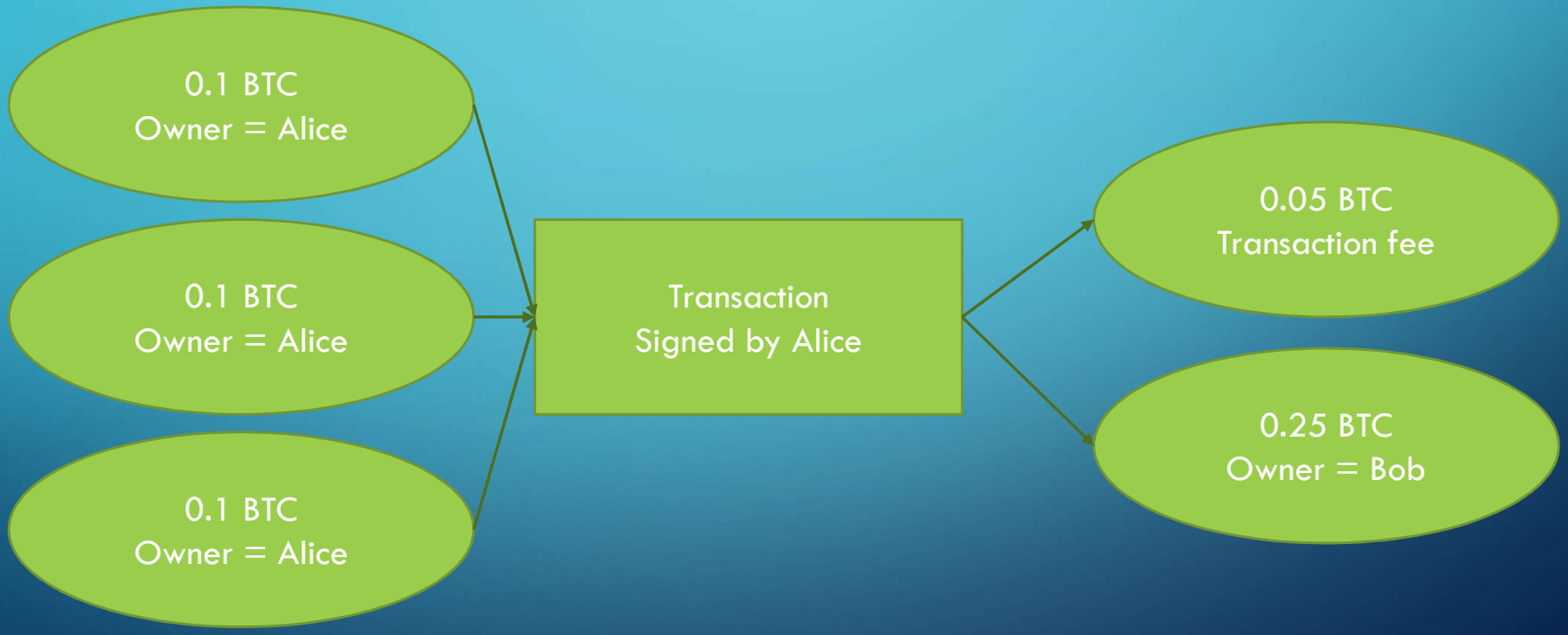
字节数	字段名称	数据类型
4	版本	int32_t
32	上一个区块头的 Hash	char[32]
32	Merkle 树根节点 Hash	char[32]
4	区块生成时间	uint32_t
4	目标难度	uint32_t
4	随机数	uint32_t

区块是怎样生成的

- 比特币的共识机制：工作量证明 (Proof-of-Work, PoW)
- 最长链原则



交易模型：UTXO


0.1 BTC
Owner = Alice
0.1 BTC
Owner = Alice
0.1 BTC
Owner = Alice
Transaction
Signed by Alice
0.05 BTC
Transaction fee
0.25 BTC
Owner = Bob

从比特币到以太坊

- 与比特币采用 UTXO 机制处理交易不同，以太坊采用了显式的 RSM (Replicated State Machine) 模型，并引入了账户的概念。
- 每笔交易相当于对相关账户的状态执行一次操作
- RSM 模型使有状态的智能合约变得可能

智能合约 / DApps

- 一种特殊的账户
- 普通账户受所有者的私钥控制，而智能合约受其自身代码控制
- 智能合约语言：EVM(Solidity), WebAssembly


区块链 & 密码学

区块链中广泛使用的密码学技术

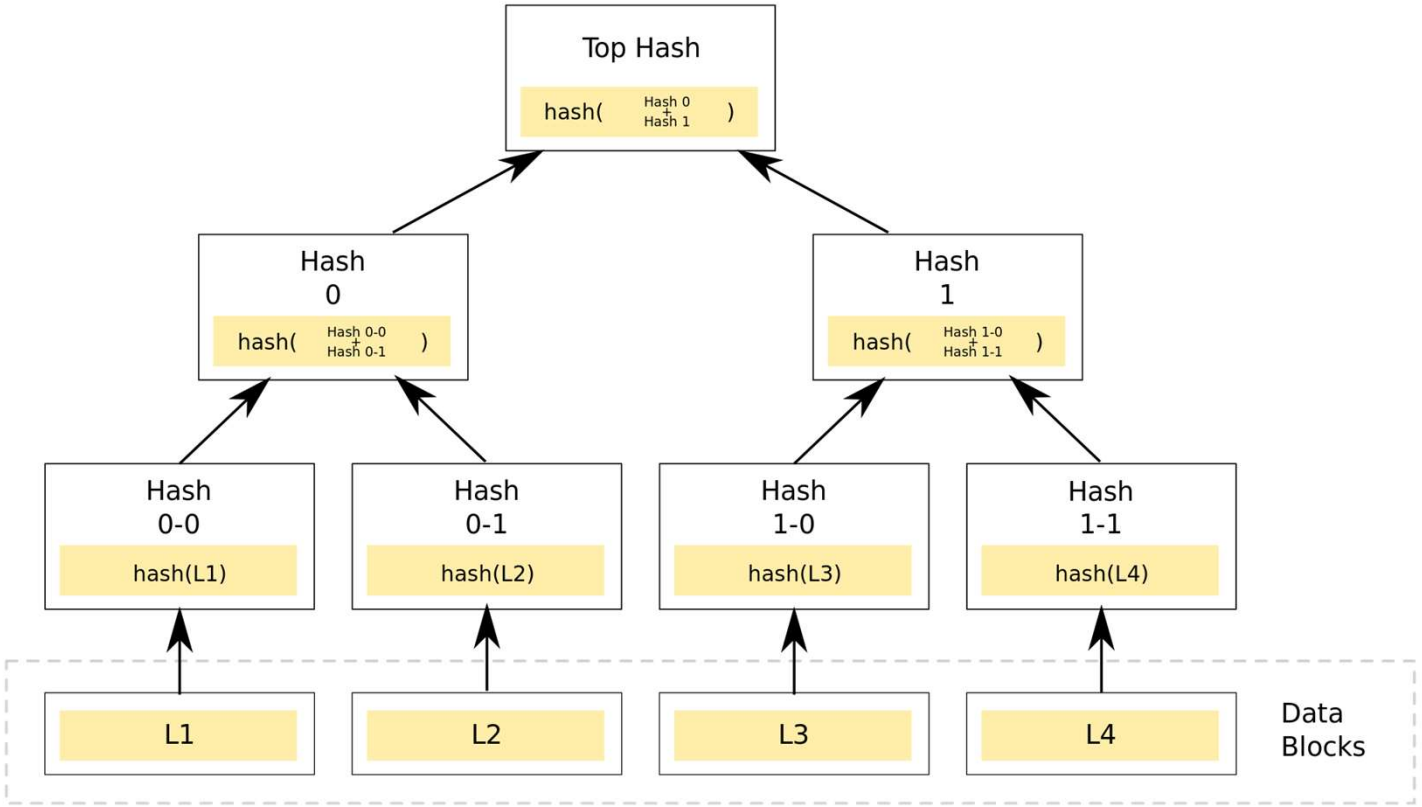
- Hashing
- 数字签名
- Merkle 树

账户所有者怎样证明一笔交易是自己发送的?


{
"tag": "transfer",
"nonce": 42,
"payload": {
"recipient": "6a635dadf06d891eb7359d540f8da08c7ca72955a9670e23401d708e2d0398ee",
"amount": 100
}
}
Hash: SHA512
86ea37082ebdb7ae1d9f9fa43a15aa85998edacbbe7ee284d746edf95c59422e
c661956e33b30822ba2f69b66b17b5f2aa995b3b0e06fca2252e7dcbf0f80ee3
Sign: Ed25519
???

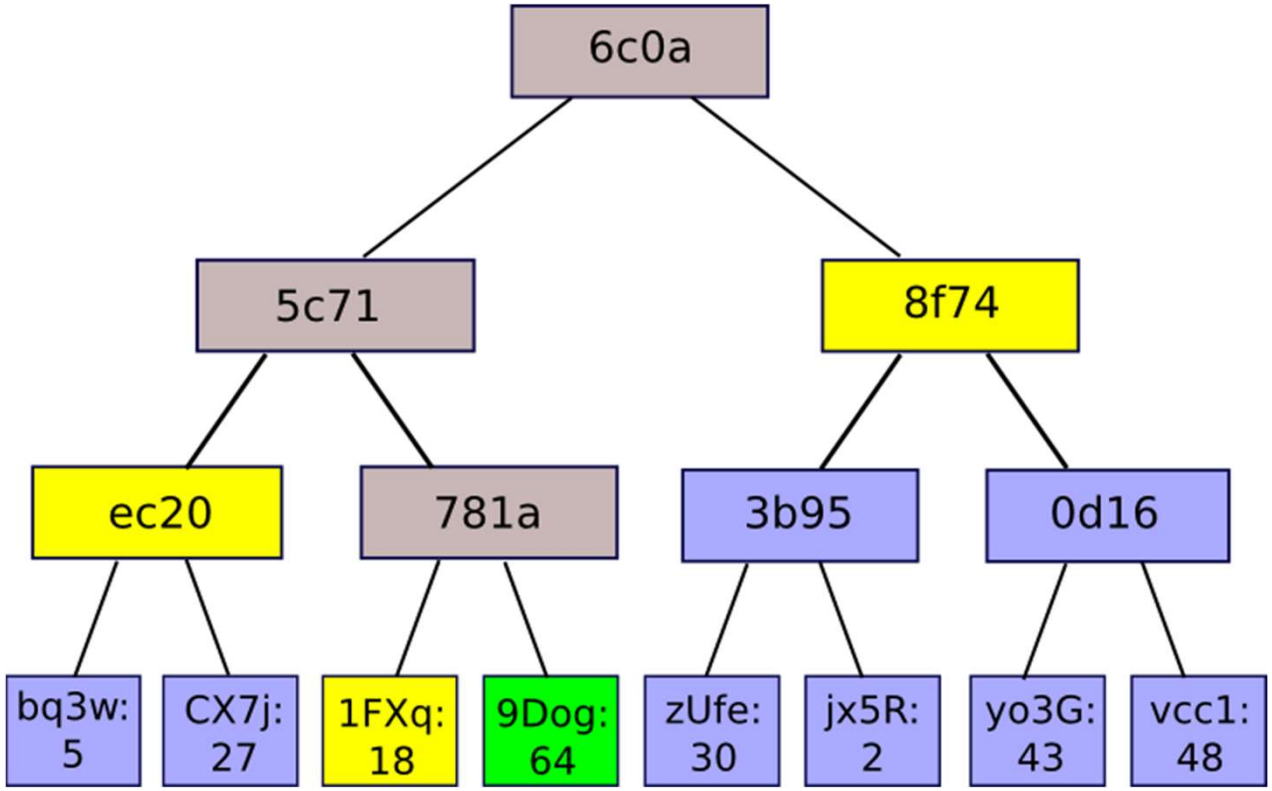
Merkle 树

分布式环境下高效的数据验证机制



Merkle 树的一个应用：SPV

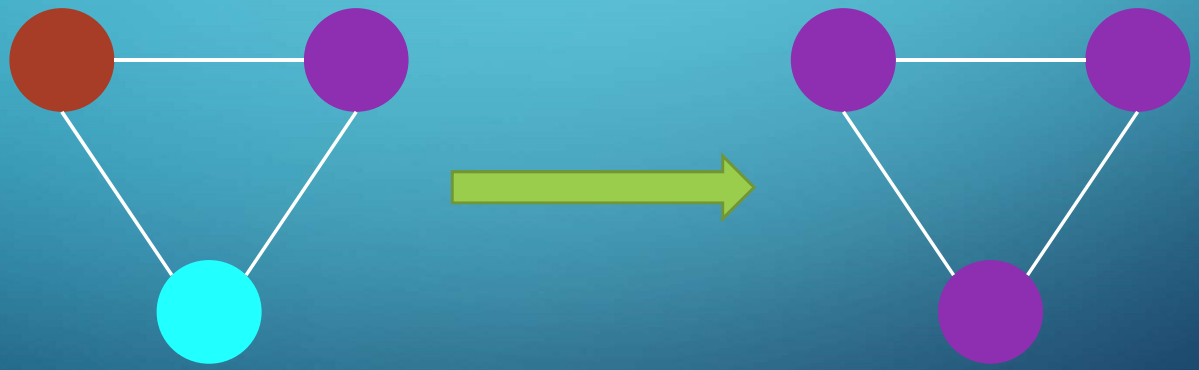
- SPV = Simplified Payment Verification
- 完整的区块链数据需要大量存储空间（Bitcoin: ~180GB as of Q3 2018）
- 轻量节点可以只保存区块头并要求为待验证的交易提供 Merkle 证明




区块链 & 共识

什么是共识?

- 在一个分布式系统的不同节点之间对一个值达成一致的机制

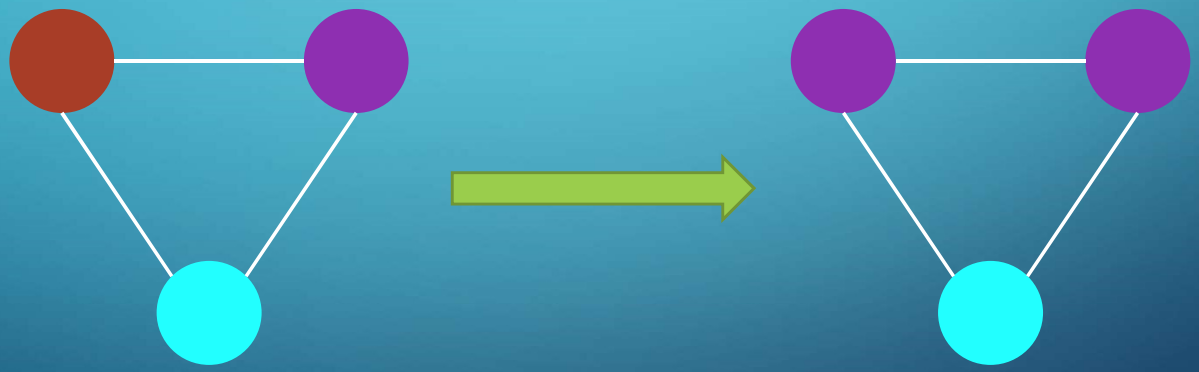


共识要解决的问题

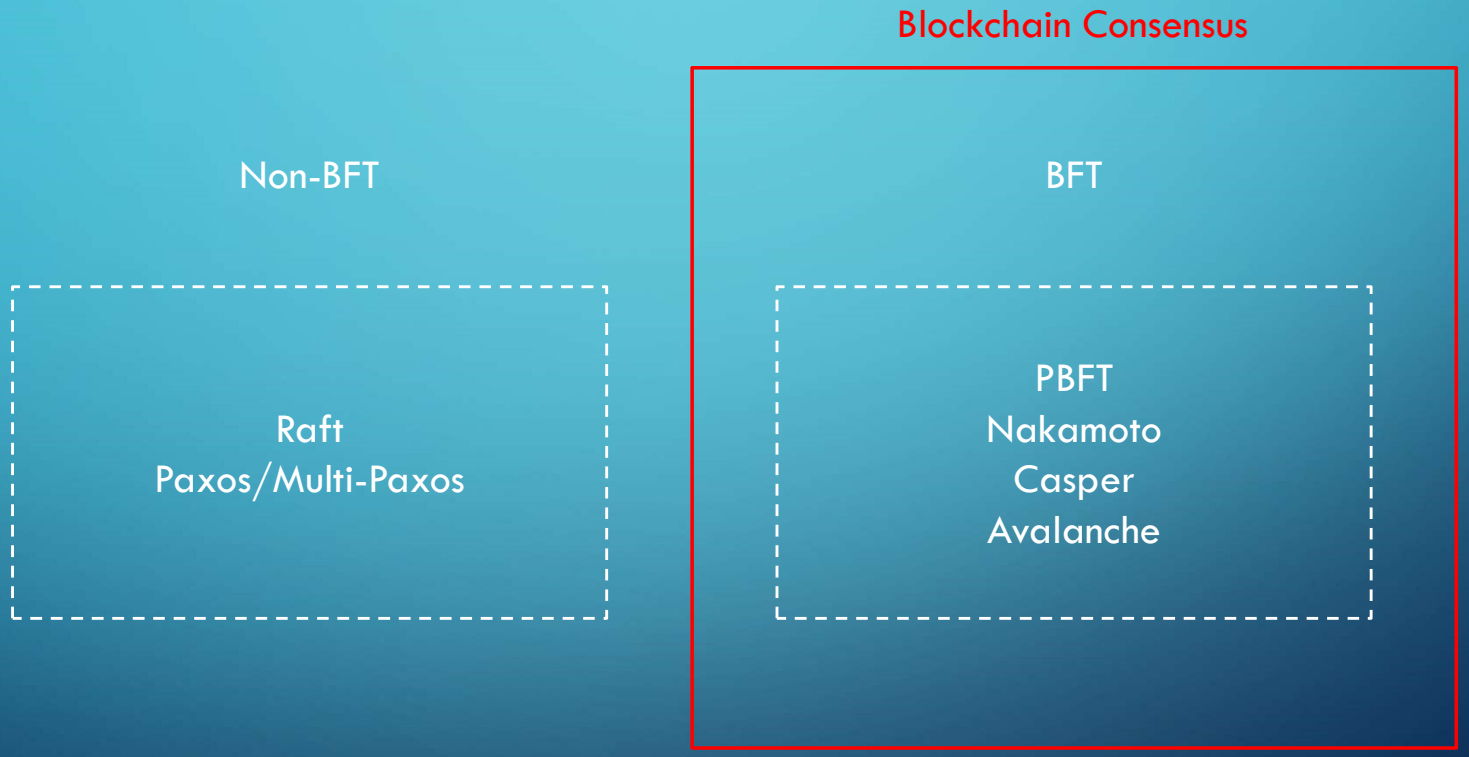
- 当有多个互相冲突的事务“同时”产生时，如何确保所有正确节点只执行其中相同的一个事务？（一致性 / Consistency）
- 如果网络中的部分节点出现错误，如何使其余节点不受影响？（可用性 / Availability）
- 当网络发生分区（通信失败）时，优先保证一致性还是可用性？（分区容错 / Partition Tolerence）
- 当网络中存在恶意节点时，如何确保正确节点仍然能够正确决策？（拜占庭容错 / Byzantine Fault Tolerence (BFT)）
- 已经被执行的事务，什么情况下会被回退？（终结性 / Finality）

In the Blockchain Context

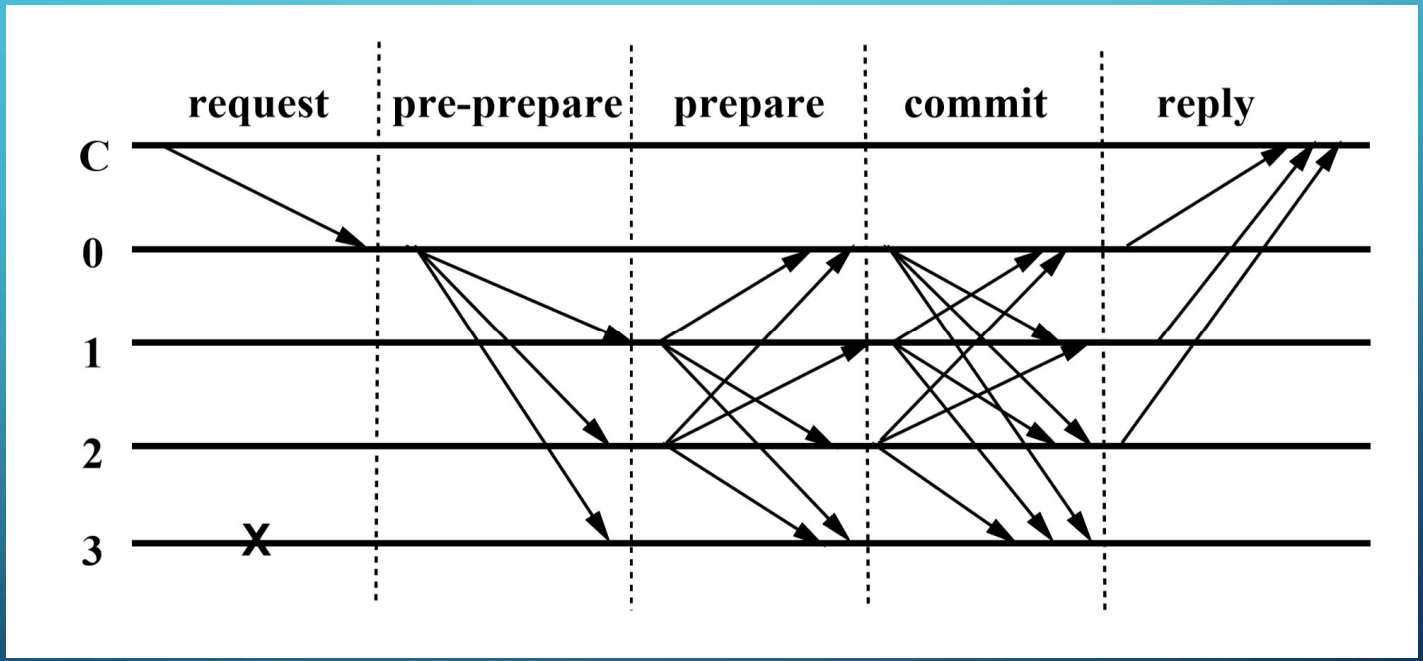
- 全网节点最终状态不一致可导致双花（Double Spending）攻击



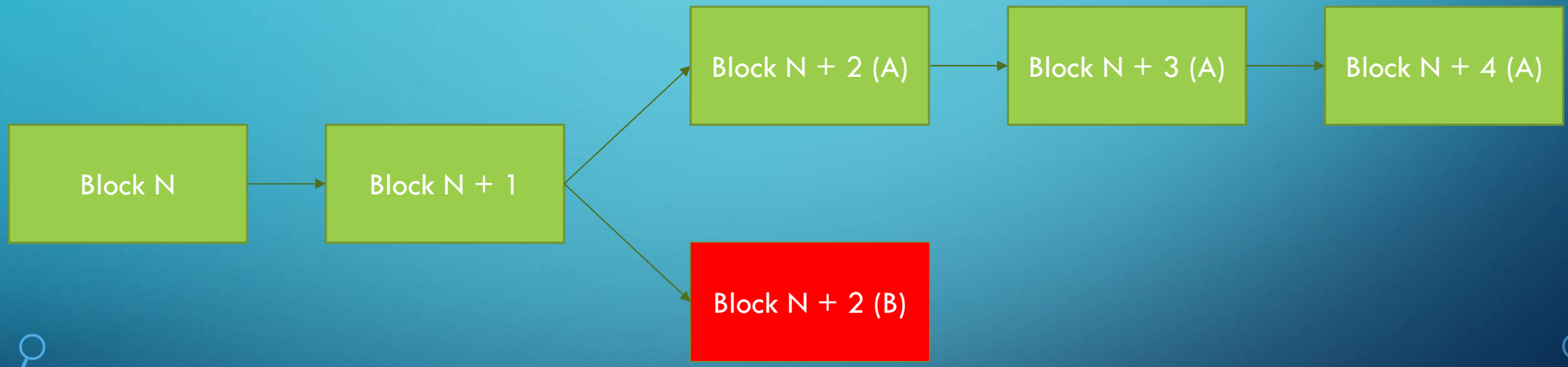
常见的共识机制


Blockchain Consensus
Non-BFT
Raft
Paxos/Multi-Paxos
BFT
PBFT
Nakamoto
Casper
Avalanche

PBFT (Practical Byzantine Fault Tolerence)

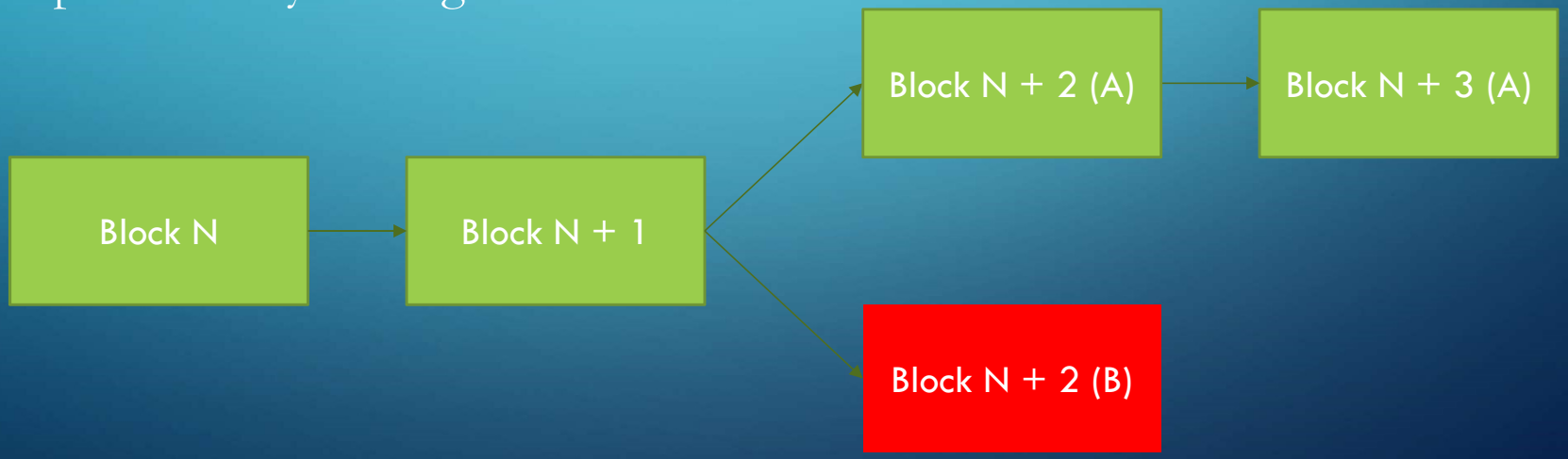


中本聪共识



Casper: 以太坊的新共识机制

- From PoW to PoS
- 早期 PoS 机制的问题：Nothing at stake
- Casper: Vote by betting



从链到 DAG: 并行交易处理

- 区块“链”的问题：单一的链结构使共识和交易处理无法并行化
- DAG（有向无环图）结构的“区块链”：交易并行化 + 局部顺序一致
- 未解决的问题：有状态的智能合约?

```
1:  procedure onQuery(v, col')
2:      if col = ⊥ then col := col'
3:      respond(v, col)
4:  procedure slushLoop(u, col_0 ∈ {R, B, ⊥})
5:      col := col_0 // initialize with a color
6:      for r ∈ {1 ... m} do
7:          // if ⊥, skip until onQuery sets the color
8:          if col = ⊥ then continue
9:          // randomly sample from the known nodes
10:         K := sample(N\u, k)
11:         P := [query(v, col)   for v ∈ K]
12:         for col' ∈ {R, B} do
13:             if P.count(col') ≥ α · k then
14:                 col := col'
15:     accept(col)
```

Avalanche: Metastability

Demo of the Avalanche family protocols


区块链 & P2P 网络

P2P 在区块链系统中的作用

- 分布式账本需要在全网所有节点之间保持一致
- 这一过程必须是去中心化的
- 怎样设计网络结构和协议，使交易处理尽可能安全、高效?

DHT（分布式哈希表）

- 键-值查询
- 在区块链中的应用：节点发现
- Kademlia & S/Kademlia