常见共识机制简介

共识机制的分类

竞争 vs **非竞争**

竞争的共识机制

- 典型代表：
  - POW；
  - POS；
- 特点：
  - 出块间隔随机性；
  - 易分叉，区块树长度竞争；
  - 效率低；
  - 难以攻击；
- 常见场景：
  - 公有链，注重公平

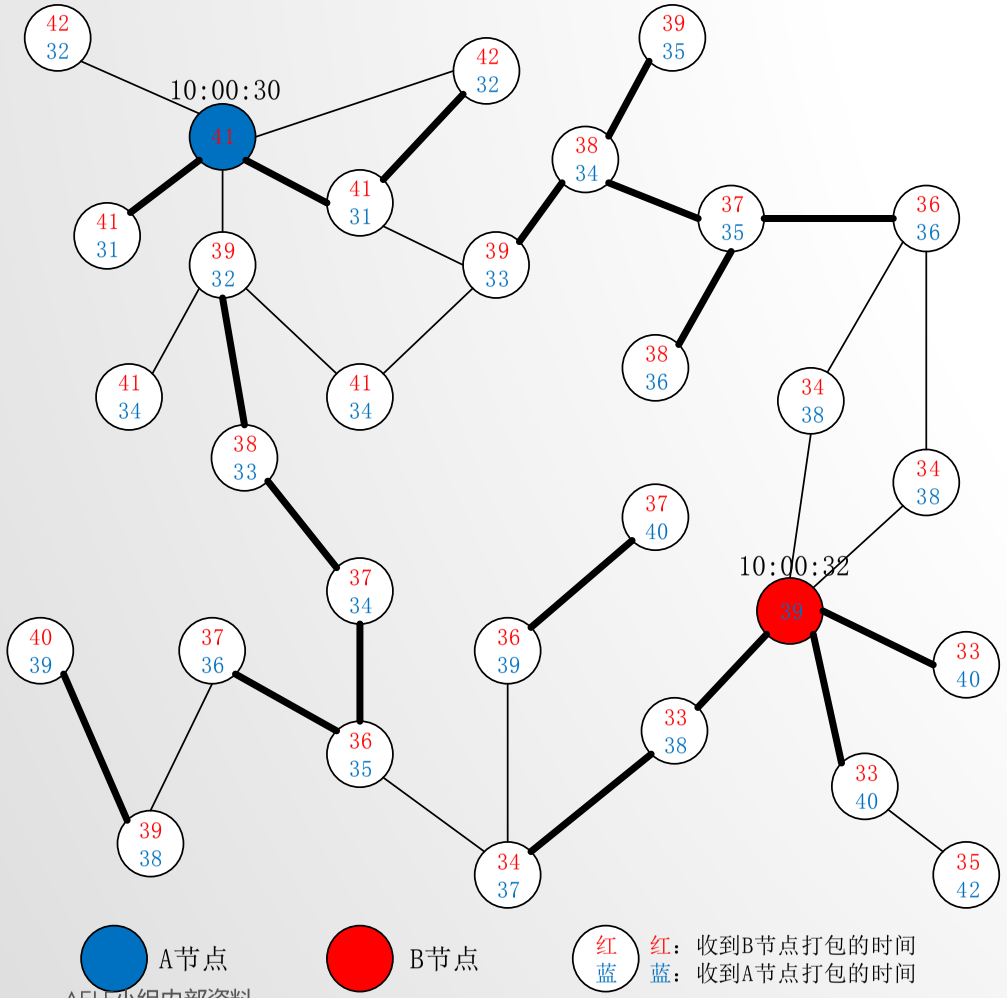
出块时间的随机性

Height	Time	Hash
500752 (Main Chain)	2017-12-24 00:00:11	000000000000000000064e429dfcfa3990922774f394604255ebb1622265915a0
500753 (Main Chain)	2017-12-24 00:03:00	000000000000000000377836caea3b829e2fc57e4511c803762247dd390fa5c9
500754 (Main Chain)	2017-12-24 00:08:19	000000000000000000003781d587f14d4b2669b27b2e82bbb79fd514b36e863b83
500755 (Main Chain)	2017-12-24 00:16:05	000000000000000000005070574eaddf7861be12b075b6936f22265f4004432bab
500756 (Main Chain)	2017-12-24 00:55:43	000000000000000000007d63c0697c2a0fe227a89f95f495bf050dea7635771e11
500757 (Main Chain)	2017-12-24 00:58:00	000000000000000000082757747cd7650c768b60ee6a77770ea374f6cf6d4f94a
500758 (Main Chain)	2017-12-24 00:59:01	000000000000000000440ecc4445a912a29420a4956cb369f4f04e59bd800695
500759 (Main Chain)	2017-12-24 01:01:55	000000000000000000095a8f6cb4b4885ec079dc38e01db4cf17c35d956f86470
500760 (Main Chain)	2017-12-24 01:07:49	000000000000000000026cbc2aacbb090198a93c21fd56af8ed8363bea74e9bfa
500761 (Main Chain)	2017-12-24 01:17:07	000000000000000000036c90c761f9be35ab4939a63482291e07412543de5bc3
500762 (Main Chain)	2017-12-24 01:20:11	000000000000000000088a45dd588aab53b4a359896c67ccb446714e2e9e0d2ea
500763 (Main Chain)	2017-12-24 01:37:15	000000000000000000868c6df4e74a2c00d98e4d0f5770a07ac4aec3621b2ad5
500764 (Main Chain)	2017-12-24 01:39:51	000000000000000000089cd345243bedc29b0eb31d7c06f4d61473ba20358dae4
500765 (Main Chain)	2017-12-24 01:56:08	000000000000000000002ed9996203f41987dac6dd0f64de44aba007863bc98392
500766 (Main Chain)	2017-12-24 02:00:32	000000000000000000002ab03b7a6ab1988451738aa16dd0d5f82e7492ca8c8860
500767 (Main Chain)	2017-12-24 02:01:17	000000000000000000002c126b0bcca806a9d1dfed9492b02464bc71d1aa406191
500768 (Main Chain)	2017-12-24 02:32:40	000000000000000000038e2a887e62ff4e8d75daf4fe317182062c674d8418070

40 min

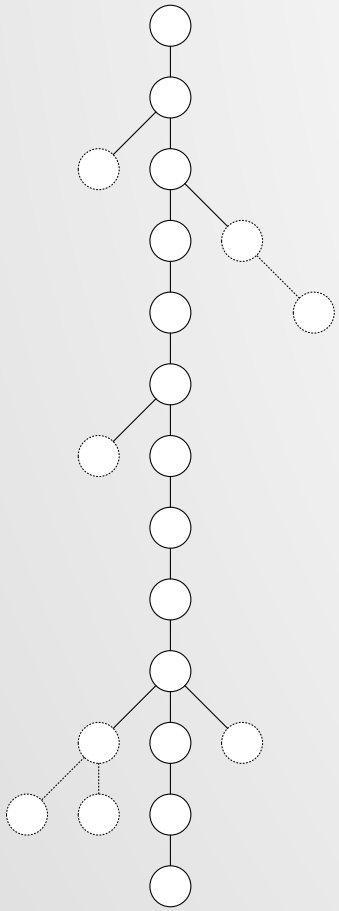
1 min

区块长度竞争:节点无法获知一个区块生成的精确时间



- 用一个简单的模型举例
- 假设高速网络传输一个区块需要1秒，低速网络需要2秒
- 假设A节点在10:00:30生成了一个区块，B节点在10:00:32生成了一个区块
- 受网络影响，每个节点收到这两个区块的时间均不同
- 节点无法判断这两个区块生成的时间先后

区块长度竞争:节点维护一个区块树



- 节点需要维护一个区块树，因为每一个收到的区块都是潜在的主链区块
- 最长的链为主链
- 每收到一个区块后，加入现有的区块树，重新比较各条链的长度，“胜出”的设为主链
- 这种方式低效、高成本
- 存在不确定性，现有主链有被“推翻”的可能性

POW

```
blockHeader {
        nVersion,
        prevBlockHash,
        mrkl_root,
        nTime,
        nBits,
        nNonce
}
```

Hash(blockHeader) < GetTarget (nBits)

POS

```
blockHeader {
        nVersion,
        prevBlockHash,
        mrkl_root,
        nTime,
        nBits,
        nNonce
}
blockSignature
```

blockSignature = UTXO.privkey.sign(blockHeader)

CoinAge = UTXO.amout * UTXO.confirmation

CoinWeight = UTXO.amout

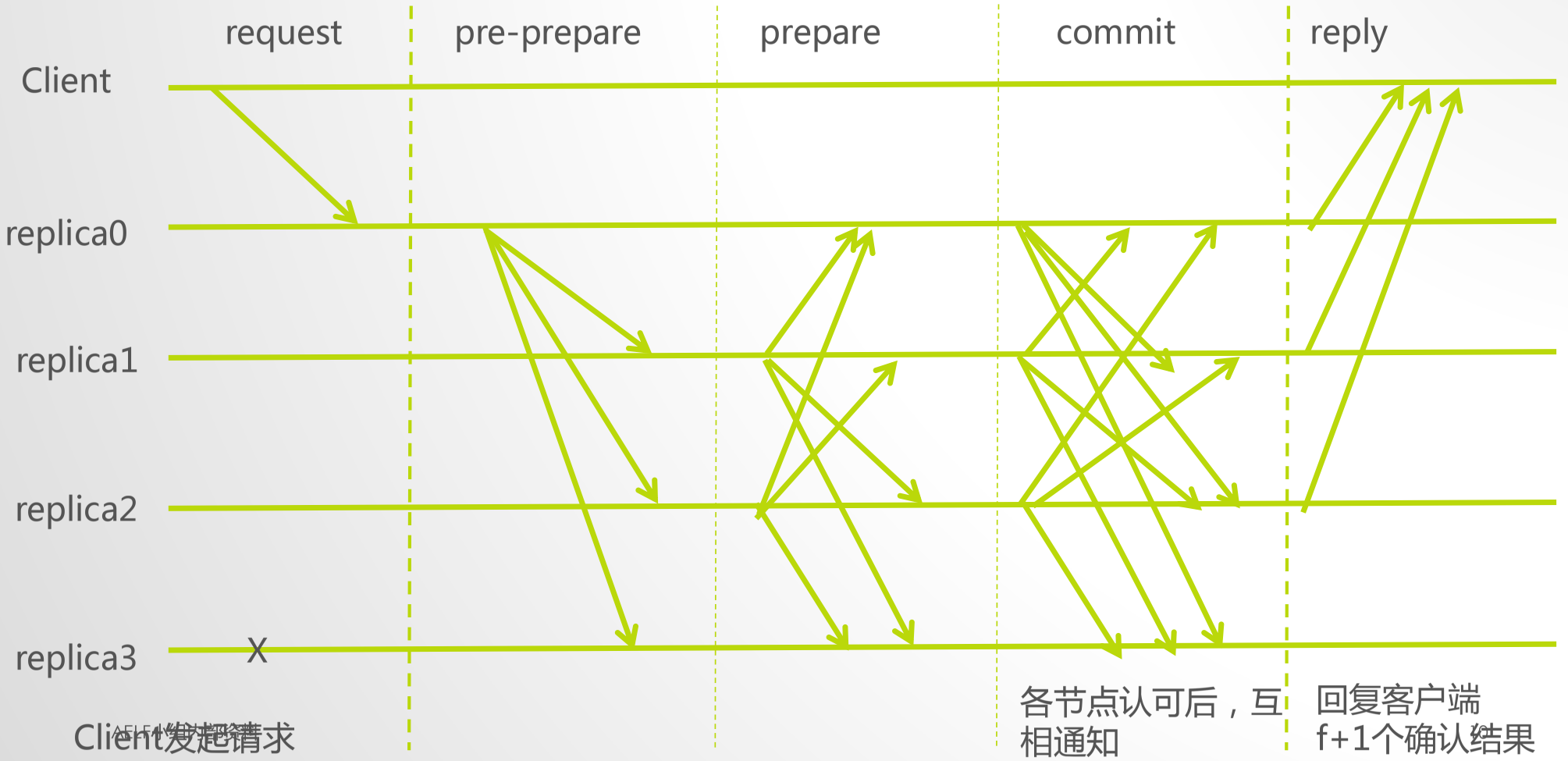
Hash(blockHeader) < GetTarget (nBits) * CoinAge

Hash(blockHeader) < GetTarget (nBits) * CoinWeight

非竞争的共识机制

- 典型代表：
  - PBFT
  - RAFT，KAFKA
  - DPOS*
- 特点：
  - 出块时间一致性；
  - 交叉检查，少数服从多数；
  - 效率高；
  - 容易女巫攻击
- 常见场景：
  - 私有链，联盟链

PBFT


request
pre-prepare
prepare
commit
reply
Client
replica0
replica1
replica2
replica3
X
Client发起请求
各节点认可后，互相通知
回复客户端
f+1个确认结果

DPOS

- DPOS节点通过股权投票产生
  - 解决女巫攻击与中心服务器问题
- DPOS节点间按照约定的顺序打包
  - 解决效率问题