区块链技术与应用

第十六讲 共识计算与激励机制

主讲人：赵其刚

唯一和确定的数据库系统

- 对数据库中的任何一个数据项在符合规则的条件下进行修改

结果

非对称密钥体制

哈希计算

P2P通信

确保分布式节点数据一致性的共识计算与激励机制

比特币

- 奠定了区块链的技术框架

共识机制

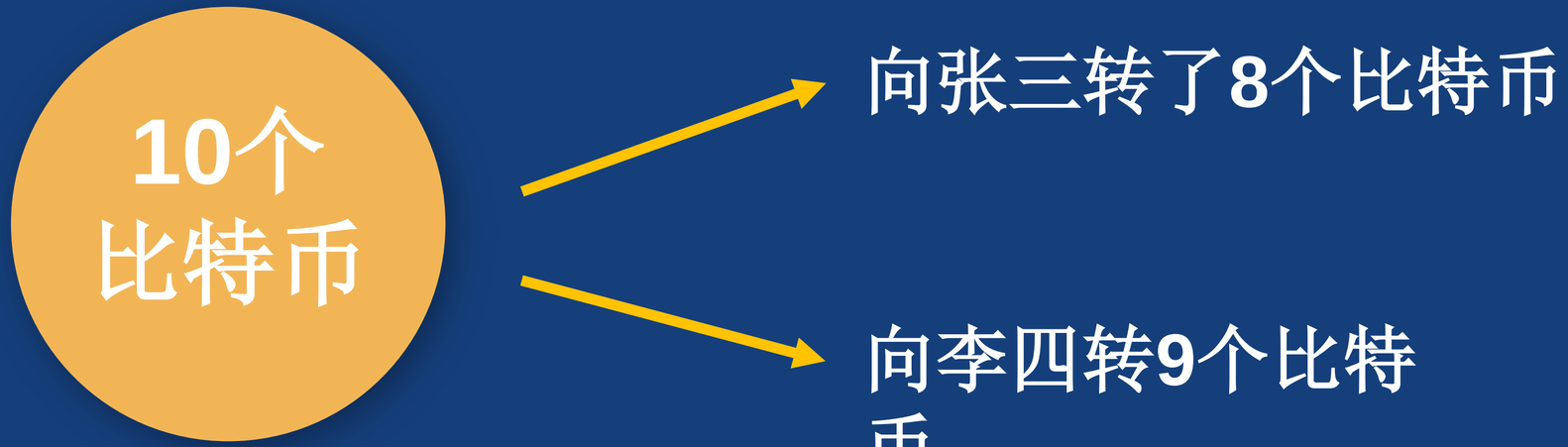
“双花”

“自私挖矿”

共识机制

“双花”

- 指用户同一笔款项多处花费



共识机制

“自私挖矿”

- 指每一个节点都希望能由自己来封装区块

- 是可以获得区块封装的奖励
- 若能由单一节点控制区块封装，实际上就具备了主宰区块中的交易序列的可能

共识机制

“自私挖矿”

- 指每一个节点都希望能由自己来封装区块

为了公平性并避免单一节点作弊，我们就需要一套公平的机制来选择某一时刻的“矿工”来将网络中交易序列封装为区块，并确保所封装区块是合乎网络的规则的。

共识机制

创始区块

按时间顺序将先后在网络中所产生的交易序列
封装为一个个按序号编列和封装的区块

共识机制

共识机制的核心

如何公平、公正、合理地生成区块、确认区块，并纳入网络中统一的区块链序列中

工作量证明（POW = Proof of Work）

比特币　以太坊

由于比特币与以太坊在区块链网络中的巨大影响力，
因而POW可以说是最著名的共识机制

工作量证明（POW = Proof of Work）

所有区块封装者

投入算力

- CPU、GPU或专用算力芯片

随机数计算竞赛

- 随机数与待封装区块组成的数据体的哈希值满足某个条件

工作量证明（POW = Proof of Work）

所有区块封装者

- 随机数与待封装区块组成的数据体的哈希值满足某个条件

可以凭借找到的这个随机数进行区块封装，并将封装的区块向网络中的其它节点广播，其它的节点获得该区块后，将按照区块的生成规则对所收到的区块进行合规性验证，当符合规则时，就会将该区块纳入本地区块链中，否则丢弃该区块。

工作量证明（POW = Proof of Work）

缺点

1. 由于必须进行随机数计算，需要花费相应时间，出块时间较长，因此TPS很低；

2. 能源浪费，为了计算这个随机数，进行算力计算，需要消耗大量电力能源。

权益证明机制（POS）

新区块

“币权”交易

- 交易会按照预先设定的比例把一些币发送给矿工本身

权益证明机制（POS）

每个节点拥有代币的比例和时间

依据算法等比例地降低节点的挖矿难度

加快了寻找随机数的速度

权益证明机制（POS）

可以缩短达成共识所需的时间

本质上仍然需要网络中的节点进行挖矿运算

股份授权证明机制（DPOS）

它在尝试解决传统的POW机制和POS机制问题的同时，还能通过实施科技式的民主抵消中心化所带来的负面效应。

内置的实时股权人投票系统

股份授权证明机制（DPOS）

依赖于一定数量的代表，而非全体用户

- 全体节点投票选举出一定数量的节点代表，由他们来代理全体节点确认区块、维持系统有序运行

全体节点

- 具有随时罢免和任命代表的权力

股份授权证明机制（DPOS）

全体节点可以通过投票让现任节点代表失去代表资格，重新选举新的代表，实现实时的民主。

股份授权证明机制

- 可以大大缩小参与验证和记账节点的数量，从而达到秒级的共识验证。

验证池（POA机制）

验证池基于传统的分布式一致性技术建立，并辅之以数据验证机制，是目前区块链中广泛使用的一种共识机制。

验证池（POA机制）

不需要依赖代币

可以实现秒级共识验证

能够实现的分布式程度不如PoW机制

实用拜占庭（PBFT机制）

准备阶段（Prepare）

- 每个节点接收到交易列表后，根据排序模拟执行这些交易。
- 所有交易执行完后，基于交易结果计算新区块的哈希摘要，并向全网广播，如1->023，2->013，3因为宕机无法广播。

实用拜占庭（PBFT机制）

执行阶段（Commit）

- 如果一个节点收到的2f个其它节点发来的摘要都和自己相等，就向全网广播一条执行消息（f为可容忍的拜占庭节点数）

回应阶段（Reply）

- 如果一个节点收到2f+1条commit消息，即可提交新区块及其交易到本地的区块链和状态数据库。

实用拜占庭（PBFT机制）

1 安全性

即是否可以防止二次支付、自私挖矿等攻击，是否有良好的容错能力。

安全问题

- 如何防止和检测二次支付行为

实用拜占庭（PBFT机制）

2 扩展性

即是否支持网络节点扩展。扩展性是区块链设计要考虑的关键因素之一。

实用拜占庭（PBFT机制）

3 性能效率

即从交易达成共识被记录在区块链中至被最终确认的时间延迟，也可以理解为系统每秒可处理确认的交易数量。

性能效率问题

实用拜占庭（PBFT机制）

4 资源消耗

即在达成共识的过程中，系统所要耗费的计算资源大小，包括CPU、内存等。

- 计算资源
- 网络通信资源

激励机制

共识机制

- 主要解决区块链中如何生成一致性的区块的问题

公链系统

激励机制

公链系统

如何确保网络能够有稳定甚至不断扩大的算力？

激励机制

激励机制

- 对完成区块封装的矿工进行区块链原生代币增发奖励；
- 获得所封装区块中用户所支付的交易费。

激励机制

基本原理

在区块链中置入代币，并通过让代币具有交易价值，使矿工对区块封装获得代币奖励具有热情。

总结

1 对P2P分布式网络架构的区块链而言

- 防止“双花”与“自私挖矿”

从而保证网络中数据的一致性是一个特别重要的课题，区块链主要是通过共识机制来确保的。

总结

2 区块链的共识机制的实质：

是如何设计一种机制在P2P网络环境下，生成一个按时间顺序排列的区块链，更直接的说就是如何生成、验证和编列每一个区块。

总结

3 根据生成区块产生的机制、算法的不同，区块链共识机制共包括有**POW\POS\DPOS\POA\PBTF**等。

4 **激励机制**是公链系统中激励自由进出的矿工持续为网络提供算力，同时确保网络安全的的一个机制。