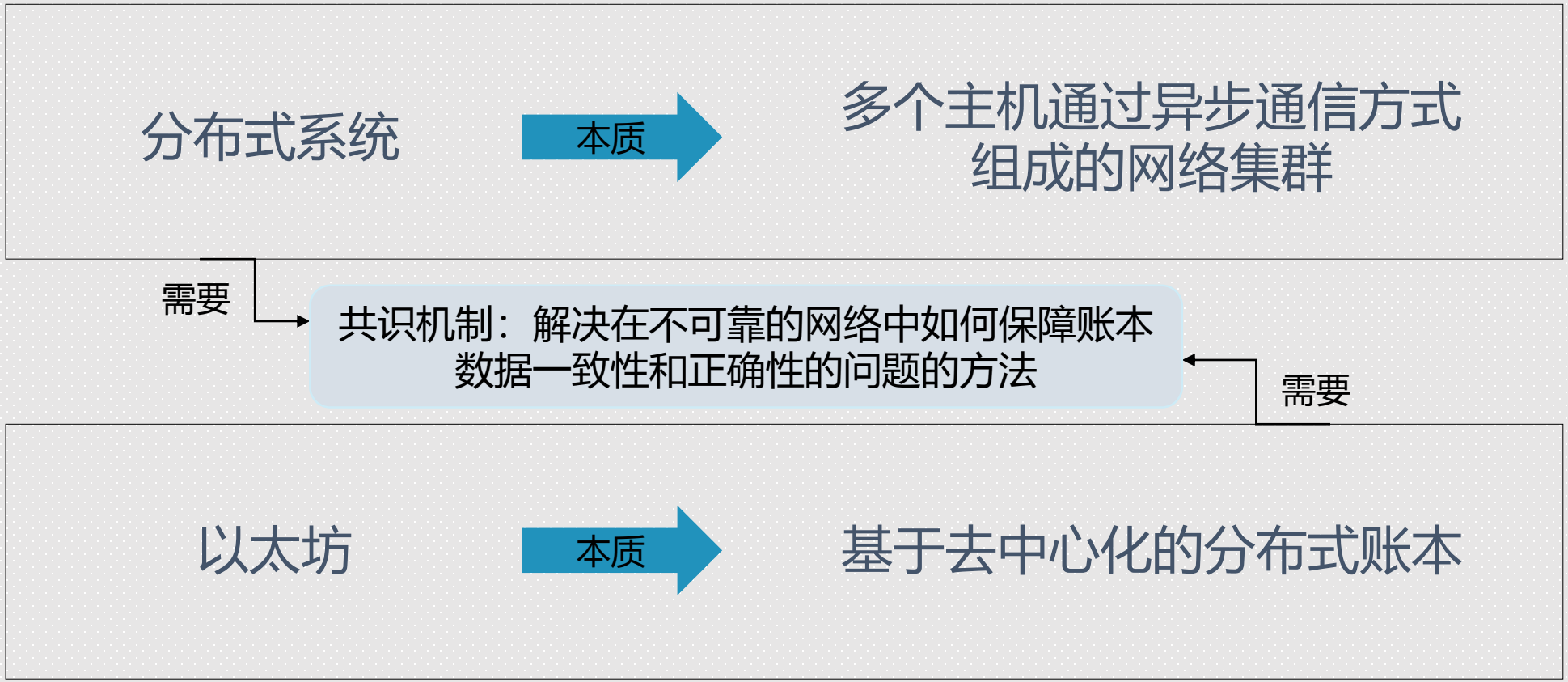
4.5 以太坊的共识机制与挖矿

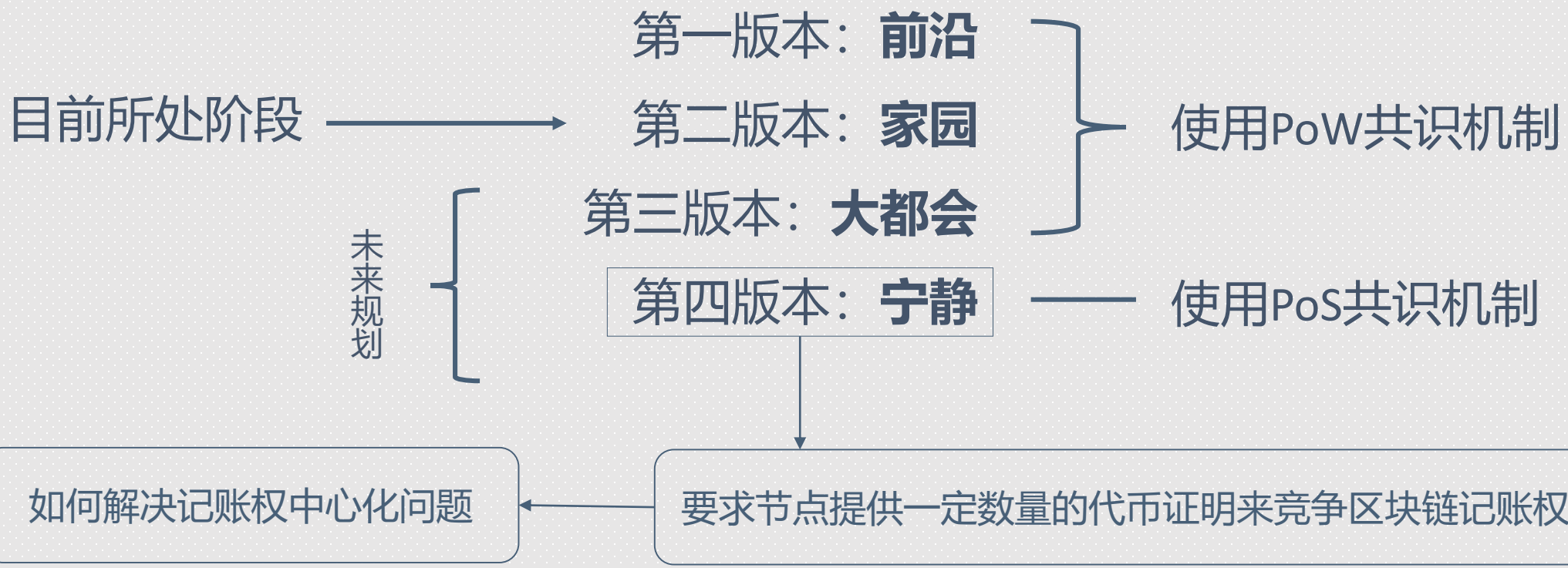
01 共识机制在以太坊中的价值

分布式系统、以太坊与共识机制



02 以太坊共识机制的版本

目前，以太坊的共识机制有四个版本。



03 如何解决记账权中心化问题

一种解决办法是根据你持有货币的量和时间来竞争记账权。

持有货币量		持有时间		币龄
100	x	30天	=	3000

↓

发现一个PoS区块=币龄清空为0

↓

清空365币龄=从区块中获得0.05个币的利息

04 Casper共识协议

Casper：基于保证金的经济激励共识协议

协议中的节点，作为“**锁定保证金的验证人**”，必须先缴纳保证金才可以参与出块和共识。

Casper共识协议通过**对这些保证金的直接控制**来约束验证人的行为。具体来说就是，如果一个验证人作出了任何Casper认为“无效”的事情，他的**保证金将被罚没，出块和参与共识的权利也会被取消。**

保证金的引入解决了经典PoS协议中做坏事代价很低的问题。

05 以太坊挖矿原理

1、挖矿流程

以太坊当前的共识机制是PoW，使用的算法是Ethash，它是Dagger-Hashimoto算法的改良版本。挖矿的流程大概如下：

（1）对于每一个块，首先计算一个种子，该种子只和当前块的信息有关，然后根据种子生成一个32M的随机数据集（Cache）。

（2）根据随机数据集Cache生成一个1GB大小的数据集合DAG(有向非循环图)，它是一个完整的搜索空间，挖矿的过程就是从DAG中随机选择元素(类似于比特币挖矿中查找合适Nonce)再进行哈希运算，可以从Cache快速计算DAG指定位置的元素，进而哈希验证。

在这要求对Cache和DAG进行周期性更新，每1000个块更新一次，并且规定DAG的大小随着时间推移线性增长，从1G开始，每年大约增长7G左右。

06 以太坊挖矿原理

2、挖矿步骤

第一步：生成一个钱包

（钱包可以通过本地钱包软件或交易平台等方式获取）

第二步：拥有一台电脑并把电脑调成挖矿最高效的状态

（以太坊挖矿主要是使用显卡，它决定了挖矿的速度；主板和电源则在很大程度上决定了矿机运行的稳定程度）

第三步：下载挖矿软件并开始挖矿

（目前主流的挖矿软件是Claymore-Dual-Miner）