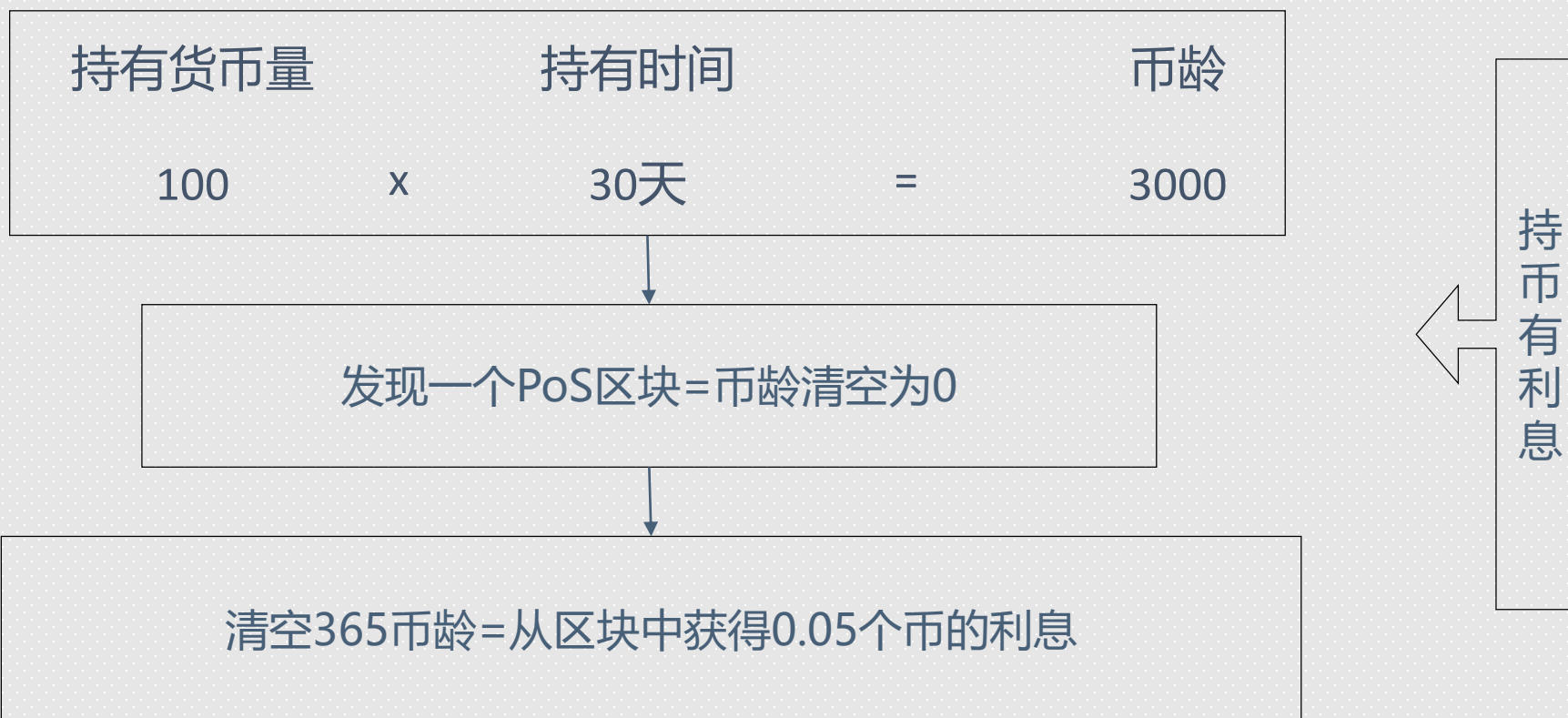


4.8 EOS的共识算法

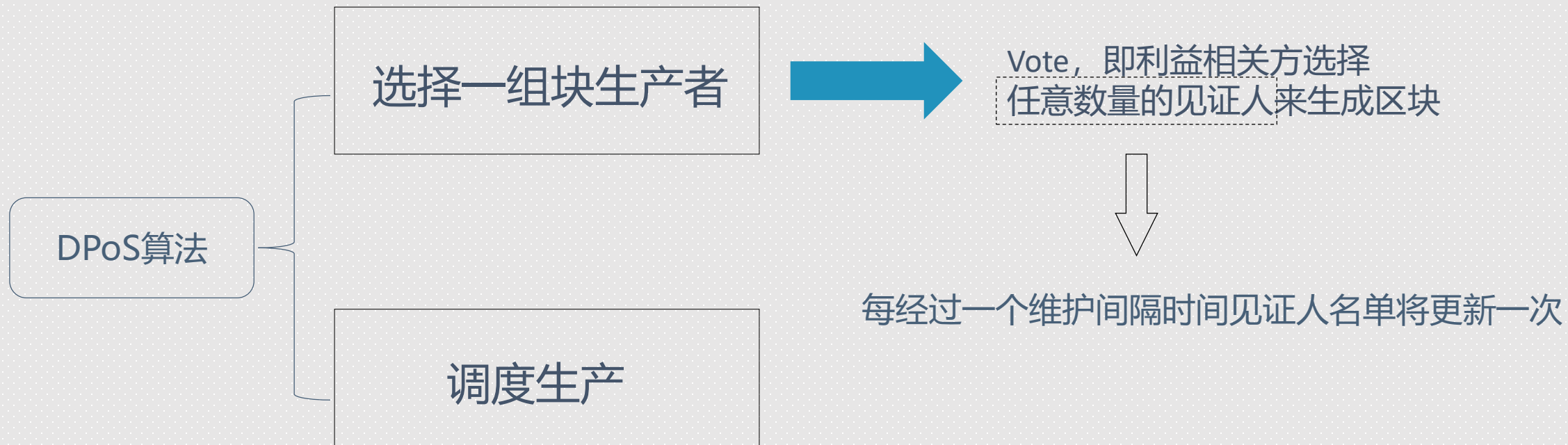
1、设计理念

- 2012年，开发者Sunny King首次提出PoS权益证明概念。
- 只有打开钱包客户端程序，才能发现PoS区块和获得利息。
(人们必须经常打开钱包客户端)
- 即使拥有全球51%的算力，也未必能够进行51%攻击
(51%攻击的难度再次增大)
- 持有越多，获得越多

2、利息计算

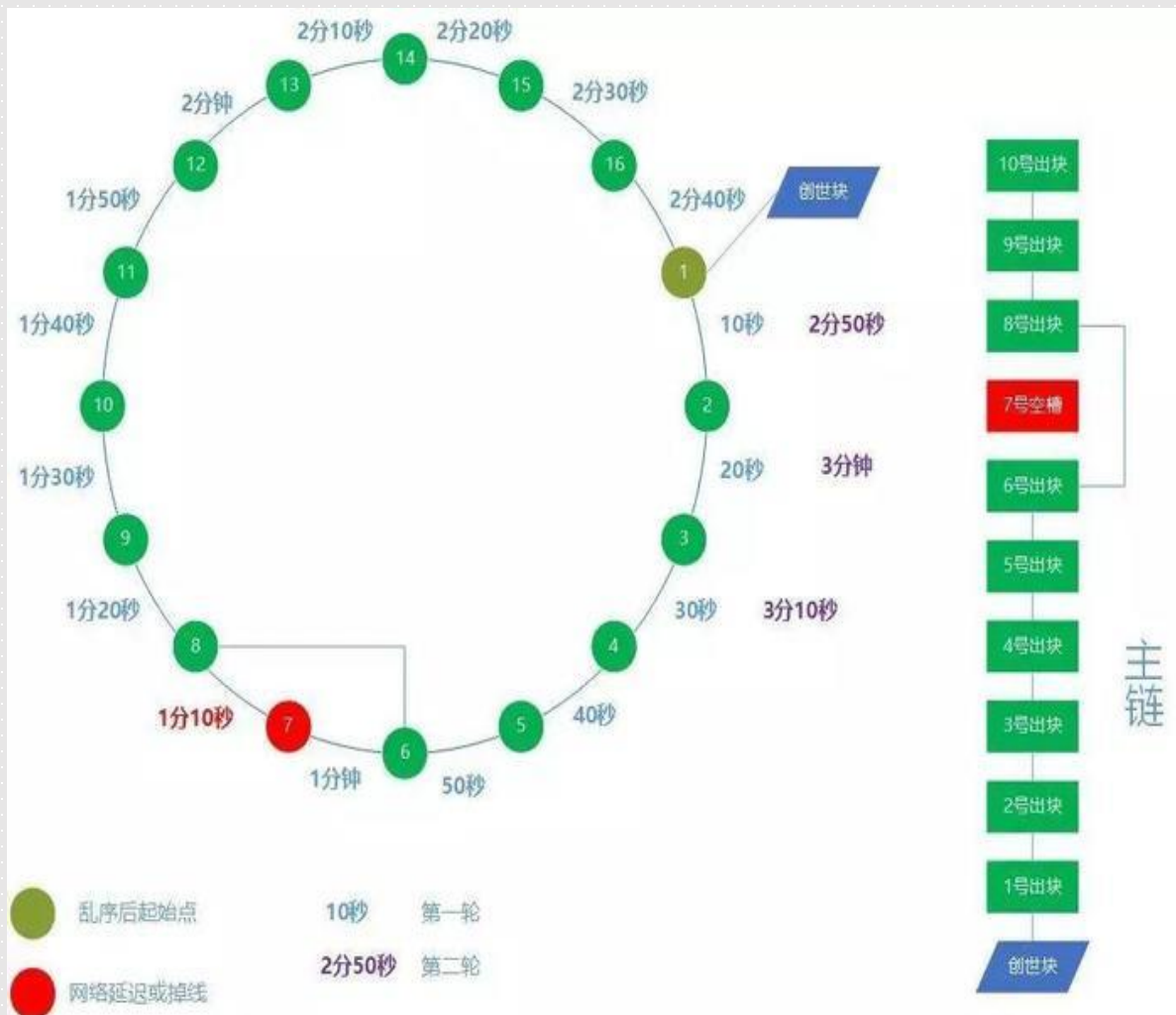


目前所有共识协议中**最快、最有效、最分散、最灵活**的共识模式



04

DPoS——洗牌过程



选出N个见证人



对选出的人排序，形成一个圈



1号见证人开始铸块



2号见证人铸第二个区块



.....以此类推，轮流出块

- **1、成为代表：**在网络上注册公钥，得到分配的32位标识符。
 - 标识符会被每笔交易数据的“头部”引用。
- **2、授权选票：**在钱包参数设置窗口中选择一个或更多代表，并将其分级。设定后，用户所做的每笔交易将把选票从“输入代表”转移至“输出代表”。
- **3、保持代表诚实：**钱包的状态指示器，告知用户他们的代表表现如何。一旦代表错过太多区块或签发了一个无效区块，钱包将在更多交易进行前要求用户选出新的代表。
- **4、抵抗攻击：**前100名代表获得的权力相同，无法通过获得超过1%的选票将权力集中到一个单一代表手中，因此需依次对每一位代表进行攻击；且代表的标识是公钥而非IP地址，减轻了定向攻击威胁