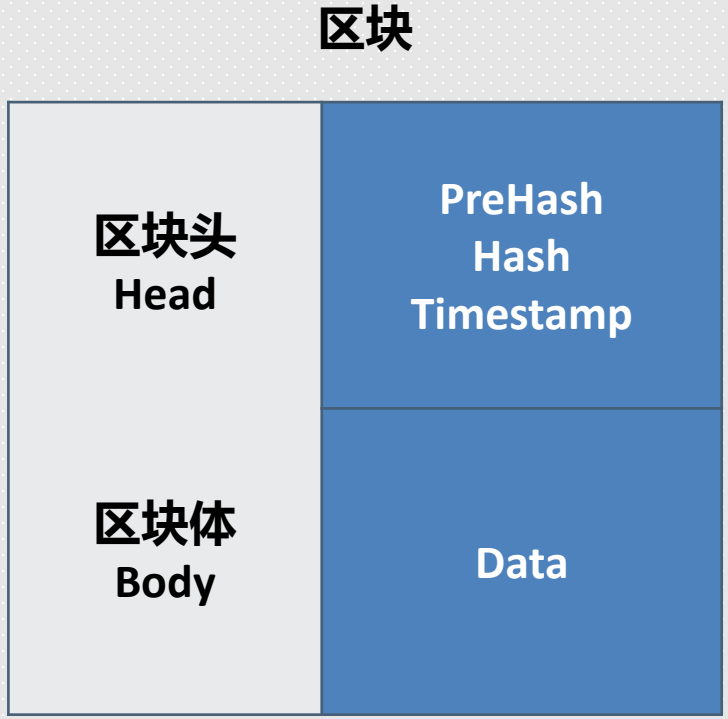
2.7 区块高度，51%攻击，矿池与算力

01 区块

区块，是一种被包含在公开账簿（区块链）里的聚合了交易信息的容器数据结构。

它是构成区块链的基本单元，由包含元数据的**区块头**和包含交易数据的**区块体**构成。

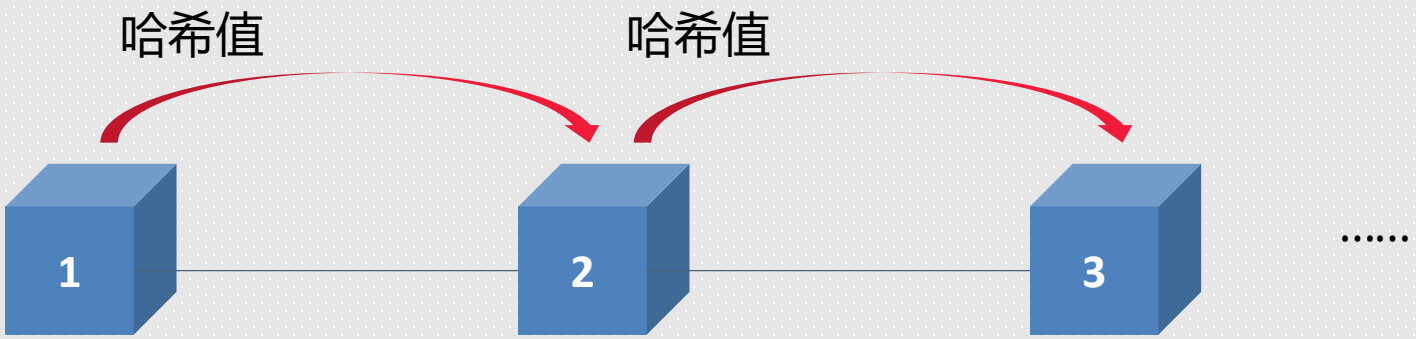
区块主体：记录交易信息



02 区块头

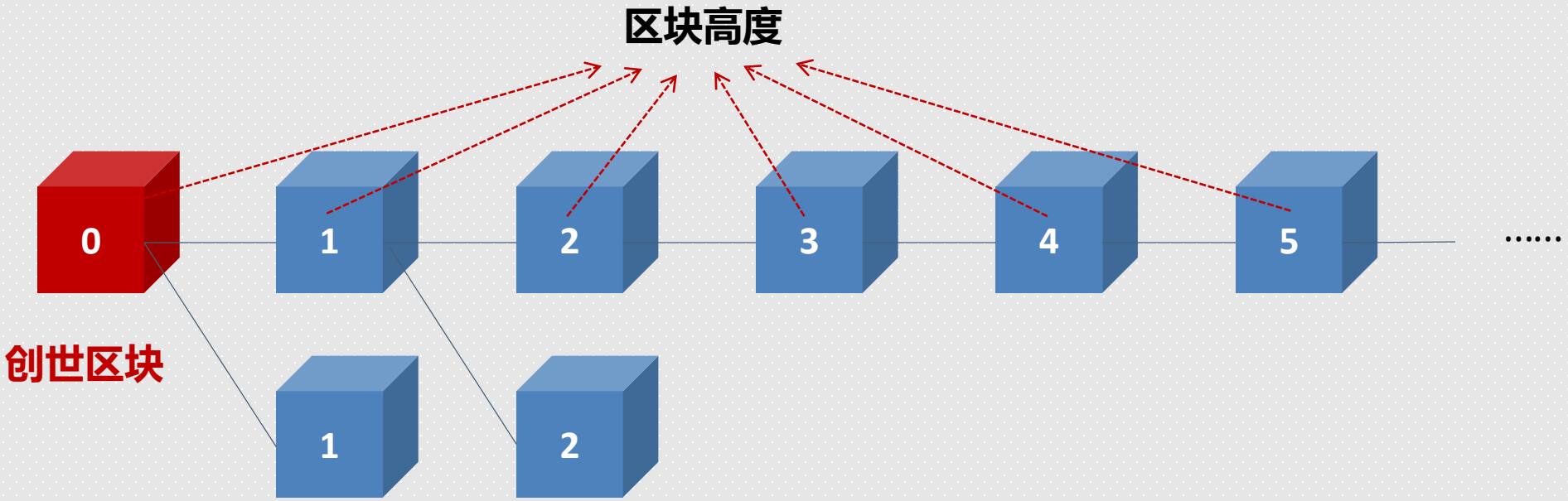
区块头结构表

大小	字段	描述
4字节	版本	版本号，用于跟踪软件/协议的更新
32字节	父区块哈希值	引用区块链中父区块的哈希值
32字节	Merkle根	该区块中交易的merkle树根的哈希值
4字节	时间戳	该区块产生的近似时间（精确到秒的Unix时间戳）
4字节	难度目标	该区块工作量证明算法的难度目标
4字节	Nonce	用于工作量证明算法的计数器



03 区块高度

区块高度是用来标识一个区块在区块链中位置的一个概念。



区块高度并不能唯一标识一个区块。

04 算力

算力，也叫哈希率，是用来衡量进行哈希运算的能力的指标，或者说进行一次哈希计算所需要使用的时间。如果说网络达到了10T hash/s（10T哈希每秒）的哈希率时，就意味着它可以每秒进行10万亿次计算。

哈希碰撞：解出随机哈希值不断尝试的过程。

一个挖矿机每秒钟能做这种碰撞的次数，代表其算力。

矿工进行挖矿所使用的机器越先进，算力就会越高。

05 矿池

矿池（Mining Pool），为了将少量算力合并联合运作所建立的网站。

06 51%攻击

51%攻击（Majority Attack），就是说在整个网络中有人的算力超过了全网的50%。那么他就可以尝试对区块链的状态进行修改，进行反向交易，实现双花。

“信任危机”

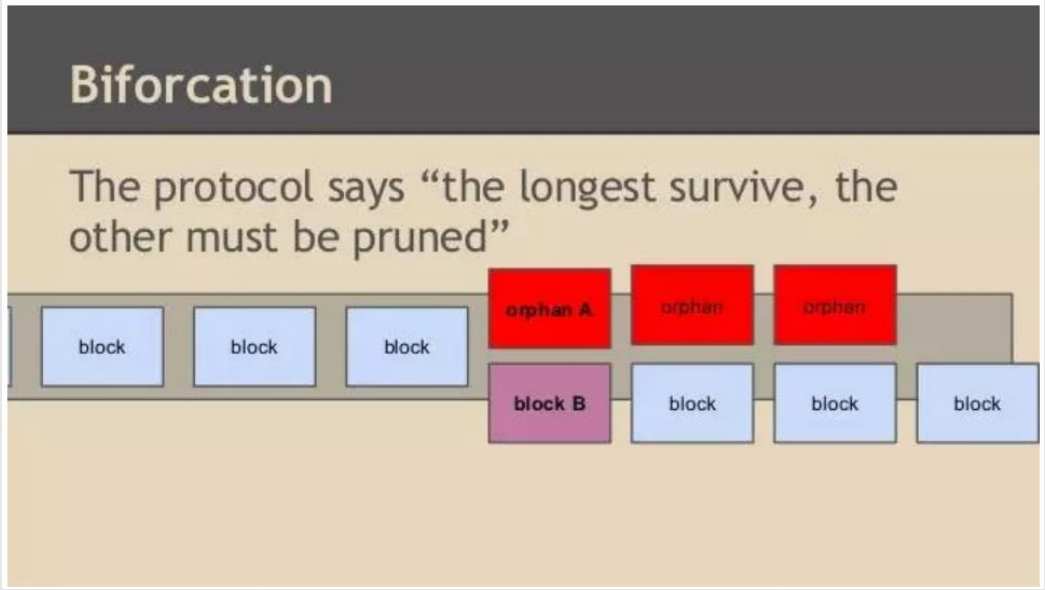
07 51%攻击

我们设想，Alice现在控制了比特币网络上51%以上的算力，在控制算力的期间，她把一定数量的比特币发给自己在交易所的钱包，这条分支我们命名为分支A。同时，她又把这些比特币发给另一个自己控制的钱包，这条分支我们命名为分支B。分支A上的交易被确认后，她立马卖掉这些比特币，成功套现。

这时候，分支A成为主链。然后，Alice在分支B上进行挖矿，因为她控制了全网50%以上的算力，所以有很大的几率获得记账权，于是很快，分支B的长度就超过了分支A的长度，那么分支B就会成为主链，分支A上的交易就会被回滚。所谓回滚，指的是程序或数据处理错误，将程序或数据恢复到上一次正确状态的行为。

08 51%攻击

这时候，由于交易回滚，分支A恢复到Alice发起第一笔交易之前的状态，所以她之前换成现金的那些比特币又回到了自己手里。于是这些比特币就成为了交易所的损失。最后，Alice把这些比特币发到自己的另一个钱包。就这样，她凭借51%以上的算力控制，实现了同一笔token的“双花”。



09 51%攻击

51%攻击怎么才会发生呢?

- 某个矿池的算力过大
- 有无限的资本

51%攻击悖论