主题：区块链中的每一个节点不需要保存完整账本（全节点），只需要保存一个区块的信息

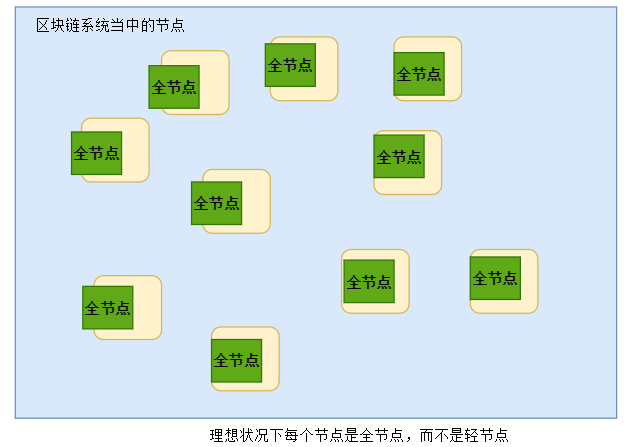
区块链现在存在的问题：体积问题

体积问题：区块链对数据备份的要求对存储空间提出挑战。区块链要求在一笔交易达成后向全网发出广播，系统内的每一个节点都要进行数据备份。以比特币为例，自创世区块至今的区块数据已经超过60GB，并且区块链数据量还在不断增加，这将给比特币核心客户端的运行带来很大的挑战

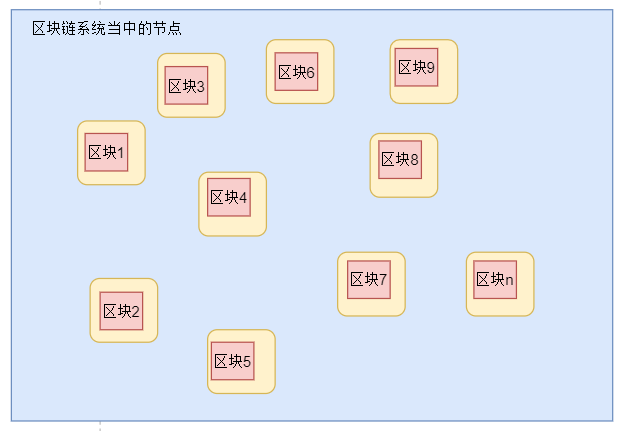
解决这个问题的想法：运用bittorrent技术，每一个节点仅仅只保存一个区块的信息

具体分析

（1）在区块链当中，每一个节点应该保存有一份实时更新的账本，保存了完整账本的节点叫做全节点。而一个完整账本的保存非常占内存，并且账本规模会越来越大



（2）这时，我们可以让每一个节点并不保存完整的账本，而知识保存整个区块链系统的其中一个区块



（3）那么我们该如何进行记账呢？和别人发生交易的时候知道对方真的拥有这么多余额？

答案是：运用bittorrent技术。下面我们将整个问题简化。

为了容易理解，我们引入四个人A，B，C，D。目前整个区块链只有4个区块

A：持有区块1（创世区块）。这个区块记录了有关用户B的交易（无论是支出还是获得金钱）

B：持有区块2

C：持有区块3。这个区块记录了有关用户B的交易（无论是支出还是获得金钱）

D：持有区块4

这时候，如果有用户D想要与B产生交易，让B支出20元，但怎么知道B真的拥有20元呢？

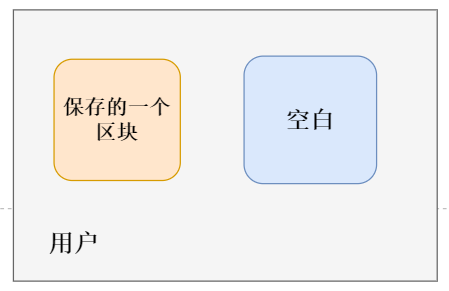
这时，用户D就要检索区块链系统的每一个区块，检索与B交易有关的区块。

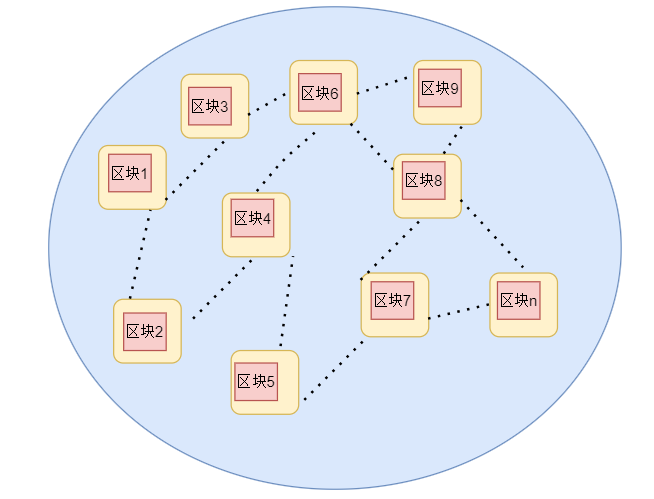
过程：D与A交换区块，发现区块1记录了与用户B有关的交易，然后将该笔交易记录在本地的内存中

D与B交换区块，没发现，不做记录

D与C交换区块，发现区块3记录了与用户B有关的交易，然后将该笔交易记录在本地的内存中

一切检索完毕，记录了与B有关的一切交易，得知B是否真的有20元，然后可以进行交易了





（4）

在步骤（3）中存在的疑问有：

1. 你如何保证遍历完了整个账本（区块1，区块2，区块3。。。。。。当前区块）

答案：首先我们需要得知当前有多少个区块。当矿工打包好了一个区块之后，向全网广播这个新区块的同时，也告诉全网这是第几个区块。

然后，每一个区块头中增加一个新的属性，用来标识这是第几个区块

用户遍历区块的时候，记录已经遍历过的区块的编号，当每一个编号都遍历完之后，说明我们遍历完了整个账本。

遍历过程如果遇到了相同的编号，则跳过此区块的遍历，否则遍历此区块。

1. 为了得知某用户的交易记录，要遍历每一个区块的每一笔交易，这效率不高而且浪费资源，这该怎么办？

答案：每一个区块头中增加一个属性，用于记录该区块中的交易来源。

比如：甲和乙交易，甲账户定位是中国广西，乙账户定位是是日本东京。那么我们编写一个表（像每一本书的ISBN号一样），中国的编号是123，日本的456。广西是a，东京是a。那么中国广西就是123-a，日本东京是456-a。记录于区块头。

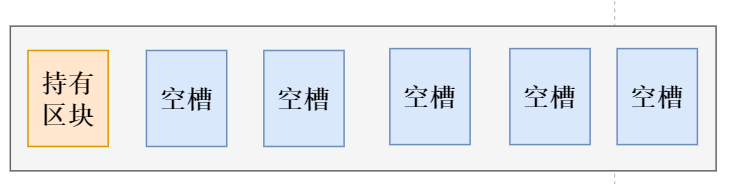
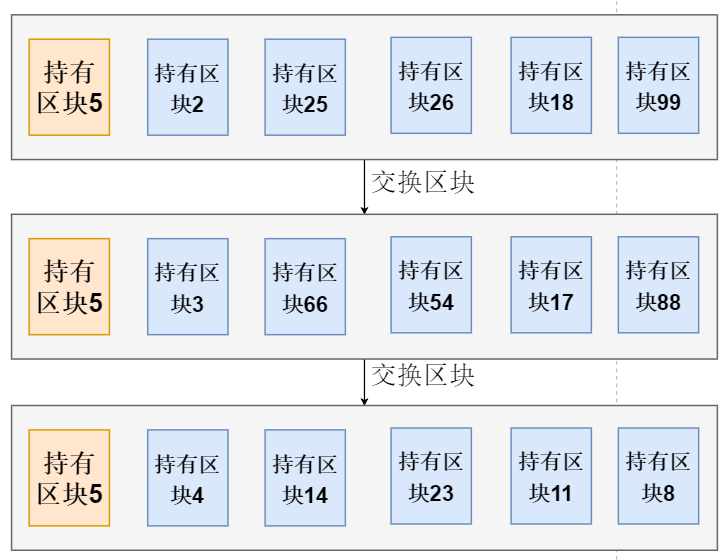
进行交易的时候，根据交易双方的编号去区块头查看是否有相应编号，如果有则遍历区块，否则不去遍历区块。

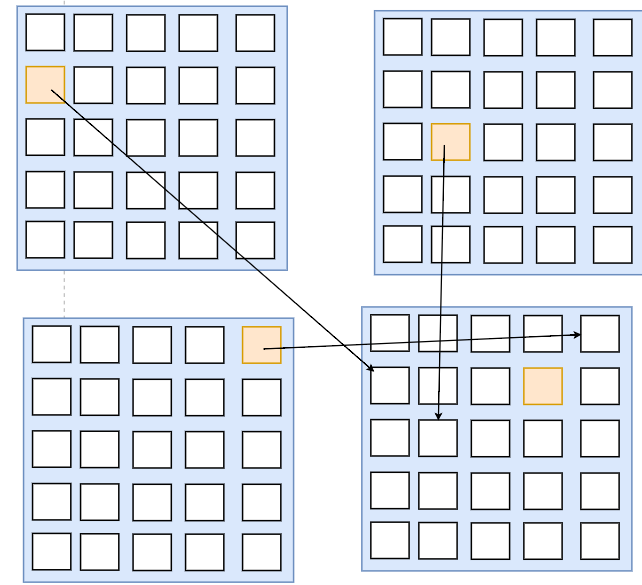
1. 比如比特币系统中，目前有60万个区块，这么多个区块，越到后面的遍历，重复遍历到之前遍历过的区块的可能性越大，想要找到没有遍历过的区块的可能性就越小。当区块数目到达100亿甚至更多的时候，该怎么办呢？

答案：用户持有一个区块，剩余比如5个槽位用于交换获得其他区块。每从其他节点下载获得一个区块并且遍历后（如果需要的话），就删除此区块，继续交换，遍历……重复此操作，直到遍历完所需n个区块。

因为bittorrent技术可以保证我们飞速的从其他节点获取想要的资源（比如我们是区块2，缺区块1、3、4、5、6，那么就可以从全网中搜集）。

这里的bittorrent技术是变种的，因为我们一共6个槽位（持有区块不变，5个空槽不断的交换区块，遍历，删除，交换，遍历，删除……），如图





由于全网是有很多节点的，当节点数目特别庞大的时候（假设当前60万个区块，参与区块链系统的节点有14亿用户，那么每一个节点被重复备份的数量也会非常大）。我们假设此时缺少区块3没有验证，那么根据bittorrent技术进行全网搜寻（此过程本身就很快），找到了目标节点，他持有区块3，就进行下载交换。

1. 我们的目标是：每一个节点（用户）不保存完整账本而减少节点（用户）的数据体积。

做法：每一个节点保存一个区块

我们可以通过下载区块来验证用户的余额。因为节点数目庞大，根据bittorrent技术，那么下载速度也会非常的快，以至于只需几毫秒的的时间，瞬间完成下载完整账本而验证了用户的余额。

【5】

【6】

（5）