1。比特币概述

区块链中的数据是可搜索的，不可篡改的。实现主要依靠大量的设计：数字签名和共识机制。

区块链技术是比特币的基础，比特币是区块链技术的第一个成熟应用。。区块链是指通过去中心化和不信任来集体维护可靠数据库的技术方案。

比特币的区块链其实是一个账本，里面有很多账单，账单是块，账本是区块链。

比特币体系中没有单一货币。只有交易单，每个人都有自己的账户ID。每笔交易都会以交易单的形式记录在账单上，货币价值附在交易单上。可以通过跟踪所有参与的交易表来计算余额。

这个账本以特殊的形式记录了比特币从诞生到现在的所有交易记录。账单的每一页都只记录了10分钟内比特币在全球的所有交易信息，所以每隔10分钟，所有新交易订单的数据都会汇集在一起，创建一个区块。并且每个新创建的块都会有一个指向前一个块的指针，越来越多的块连接在一起形成区块链。

区块链巧妙地结合了两种基于哈希值(函数算法)的数据结构：第一次结构是区块的哈希链。每个块都有一个块头，块头上有一个指向前一个块的散列指针。第二种数据结构是树状数据结构(Meckeltree)，它排列和存储块中所有事务的哈希值。这样，你可以通过树中的路径在块中快速搜索到一个需要的事务数据。

每页账单只记录10分钟内比特币在全球的交易信息。每10分钟会产生一个新的账单，所以账单会随着时间的推移而增加。每个人，每笔交易，将记录在一页账单上。这个记录过程是由比特币系统通过网络自动完成的。目前比特币世界已经运营了10多年，账单大概有53万页。账单放在世界上唯一的总账里，网络里每个用户都有一本。议案是一个阻碍。总分类账是区块链。

2。如何交易

比特币是通过签署交易单来完成的。比如B想用它买C&#039的产品。具体交易流程如下：

a从某地取得10条比特币记录并在Tx0.a转给B，在Tx1.b转给C，在Tx2记录。每张交易单都是双向记录的，类似于会计上的复式记账法。

来源，记录此次转账的资金来源。有两个主题：最后一个交易表单的ID(最后一个交

易表单的全文哈希值)和最后一个发送者的数字签名。

去向，记录本次转出资金的去向。，主要包括三个科目：转账金额、收款人&#039；的公钥和发送者&#039；的数字签名(加密接收方生成的哈希值&#039；资金来源交易表单的公钥)。

在接收到Tx2之后，每个节点执行以下验证：

1。找到Tx1交易单

2。获得B公钥

3。用B公钥

4解密Tx2数字签名。通过比较哈希来验证

。

验证得出两个结论：1.b确实从A处得到10个比特币(Tx1有A&#039s签名)

2.b确实有10个比特币，B要给c10个比特币(Tx2有B&#039；s数字签名)

。

交易真实性得到有效验证，交易欺诈被杜绝。

3。如何记账

每一笔交易都是以交易单的形式广播到整个比特币网络，网络上的每一个节点都在接收全网的所有交易单。，把它们放在一个本地临时账单(block)中，这样用户就参与维护账单。

会有一个谁的账单为准的问题。每个节点&#039；的上线时间不同，网络传输情况不同，收到的交易清单也可能不同。如何明辨是非，就是记账权的分配问题。目前记账权的分配机制有POW(工作证明)和POS(利害关系证明)三种。、DPOS(委托股权证明)等。比特币采用POW，越来越多其他数字货币采用POS和DPOS，或者混合机制。

共识机制	优势	缺点
PoW	实现简单，不需要过度复杂代码。 容易控制哈希值正确性。 系统可以承受大量节点。	消耗非常多的能源。 共识时间长。
PoS	资源消耗少	更多的安全问题。 实现较复杂。
DPoS	资源消耗少。 共识时间短。 吞吐量高	中间步骤较多，容易产生安全漏洞。 拥有高权益的参与者可投票使自己成为一名验证者
PBFT	可脱离币的存在 共识效率高	有 1/3 或以上记账人停止工作后，系统将无法提供服务。
dPoW	节能 安全性高 添加价值到其它区块链，无需付出 Bitcoin（或是其它任何安全链）交易的代价	只有使用 PoW 或 PoS 的区块链，才能采用这种共识算法 “公证员激活”模式下，必须校准不同节点（公证员或正常节点）的哈希率
dBFT	快速；可扩展	可能存在多个根链
PoET	参与代价低，去中心化。 易于验证领导者是通过合法选举产生的。	必须要使用特定的硬件； 不适用于公有区块链
LibraBFT	具有三分之一的容错性，防止双花攻击 吞吐量高 稳定性较强	星形拓扑结构通信中间节点被攻击可能造成全网瘫痪

比特币采用POW工作负载证明机制，实际上是计算能力的比拼。

这种机制的隐含逻辑是，努力工作的会计大概应该是诚实可信的，这个会计被称为比特币中的矿工。为了通过工作量证书获得记账权，需要做以下工作：

1。收听全网广播，通过与本地账本对比，拒绝一些不合理的交易指令，在本地账单中记录合理的新交易指令；2.计算一个随机数x。，连接X和本地账本计算一个哈希值；[XY002][XY001]3。哈希值的前几位需要为0(位数的调整会影响计算)，这样的随机数很难计算，需要最后计算(挖掘过程)；

4。一旦计算出符合要求的随机数，将立即广播到全网，全网其他节点将使用其符合要求的本地票据计算验证哈希值。校验通过后，对账将基于节点的账单。。记账节点将获得比特币奖励；5.对账完成后，将举行新一轮随机数计算比赛(挖矿比赛)继续争夺记账权。

另外，POS权益的证明就是权益的争夺。，按持有货币的金额和时间支付利息；而

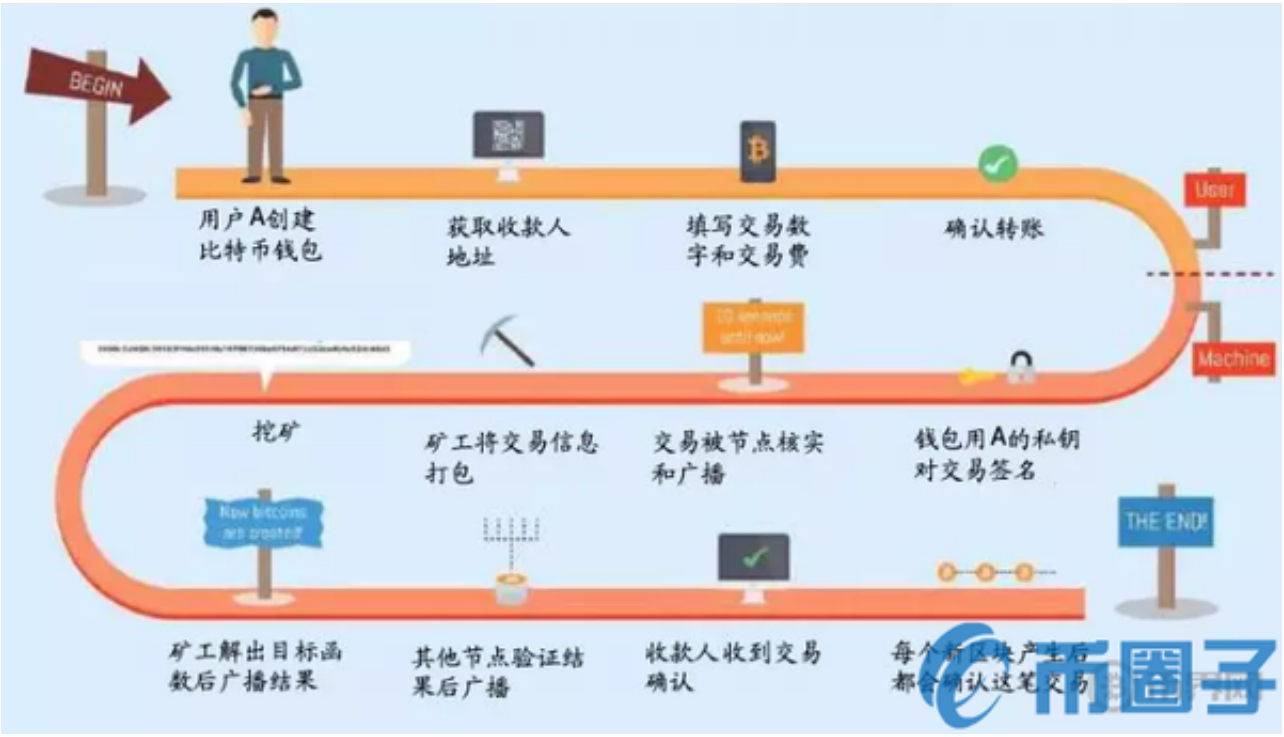
DPOS则是一种份额授权认证机制，实现电子民主，选择信任节点，成为受托者，保证通信安全。

4。如何形成链条

传统票据的页码是连续的数字。，而区块链法案的页码是一个很长的随机数密码(hash值，由Hash算法生成)前十位为0

在区块链法案中，需要指定上一页的页码才能将块按顺序排列。。每个区块都是&quot已连接&quot通过使用锁箱签名来处理下一个块。块头中该块的哈希值相当于该页票据的页码，父块的哈希值相当于上一页的页码。&quot的具体数值页码&quot使用&quot文本&quot作为自变量。，由哈希函数生成的随机字符串。为了争夺记账权，网络中的计算机节点必须随机生成一个&quot页码的前十位为0&quot，这是一个极其罕见的事件，所以整个区块链网络大约需要10分钟。，以便计算机节点可以找到这样一个&quot密码&quot符合要求的

。一旦找到，这个计算机节点就获得记帐的权利，它生成的新帐单(块)将被更新到网络中的所有计算机节点。。账单(块)通过上一页的页码(父块的哈希值)找到父块，自动链接成为总账(区块链)。



全网公认最长链。如果有人需要篡改数据，链条就会分叉。为了让别人认可这个假链，他必须用个人理论来维护这个链，直到长度大于真链。由于工作量证明机制单

个节点的计算能力必须超过全网计算能力的51%，才能超过真实的链长。随着系统的增长和节点的广泛分布，这几乎是不可能实现的。