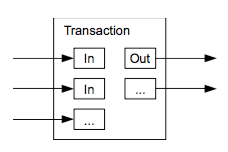
前言

现阶段最热门的技术是什么，你肯定或多或少的听说过区块链。区块链技术被认为是继蒸汽机、电力、互联网之后，下一代颠覆性的核心技术。 全球著名的新经济学家和商业策略大师Don Tapscott在TED演讲《对未来产生影响最大的科技》中也肯定了区块链技术可能带来的变革。

区块链的火爆，离不开比特币的加持。比特币从2008年由中本聪发表的一片关于p2p去中心化的电子货币论文开始，到目前为止比特币的交易过程一直很安全，基本没有出现过错误，所以作为比特币底层的区块链技术才被大家重视起来。所以说区块链是一种技术，而比特币是目前为止使用这种技术最成功的一个应用。

区块链是什么

维基百科对区块链的定义是：区块链是用分布式数据库识别、传播和记载信息的智能化对等网络, 也称为价值互联网。

百度百科中的定义是：区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。

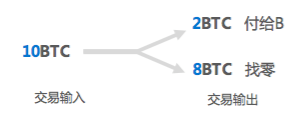
总结来说，区块链是通过特殊的密码学技术加密，去中心化、分布式记录的公开通明的交易记录总账，解决的是市场经济中最核心的“信任”问题，由人的信任变成机器信任。

它有如下几个非常显著的特点：1.去中心化；2.可追溯；3.不可篡改。下面以比特币交易为例，印证以上区块链的几个特点。

比特币交易简单地说，交易指把比特币从一个地址转到另一个地址。更准确地说，一笔“交易”指一个经过签名运算的，表达价值转移的数据结构。

比特币的交易形式有下面三种：

1.最常见的交易形式是从一个地址到另一个地址的简单支付，这种交易也常常包含给支付者的“找零”；



2.另一种常见的交易形式是集合多个输入到一个输出的模式；

3.最后一种是将一个输入分配给多个输出，即多个接收者的交易。

从上面三种交易形式，我们可以看到一个交易可以包含多个输入输出

比特币每次交易都需要签名与验证。

签名：

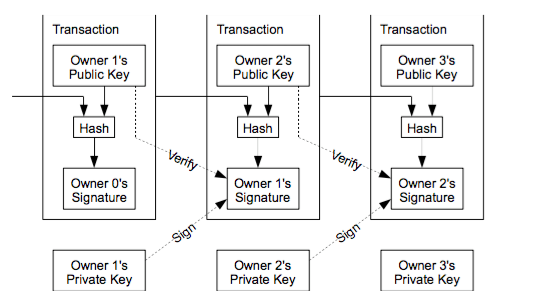
这笔交易的公钥并hash变成160长度；

上一笔交易的hash；

用他们生成一个哈希值h;

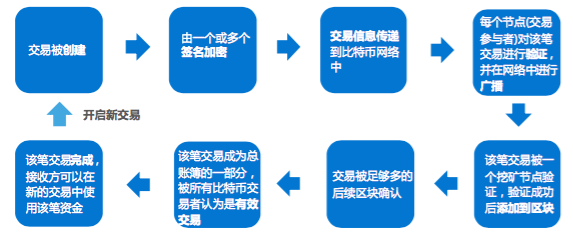
在用上一笔交易的私钥对哈希值h进行签名S

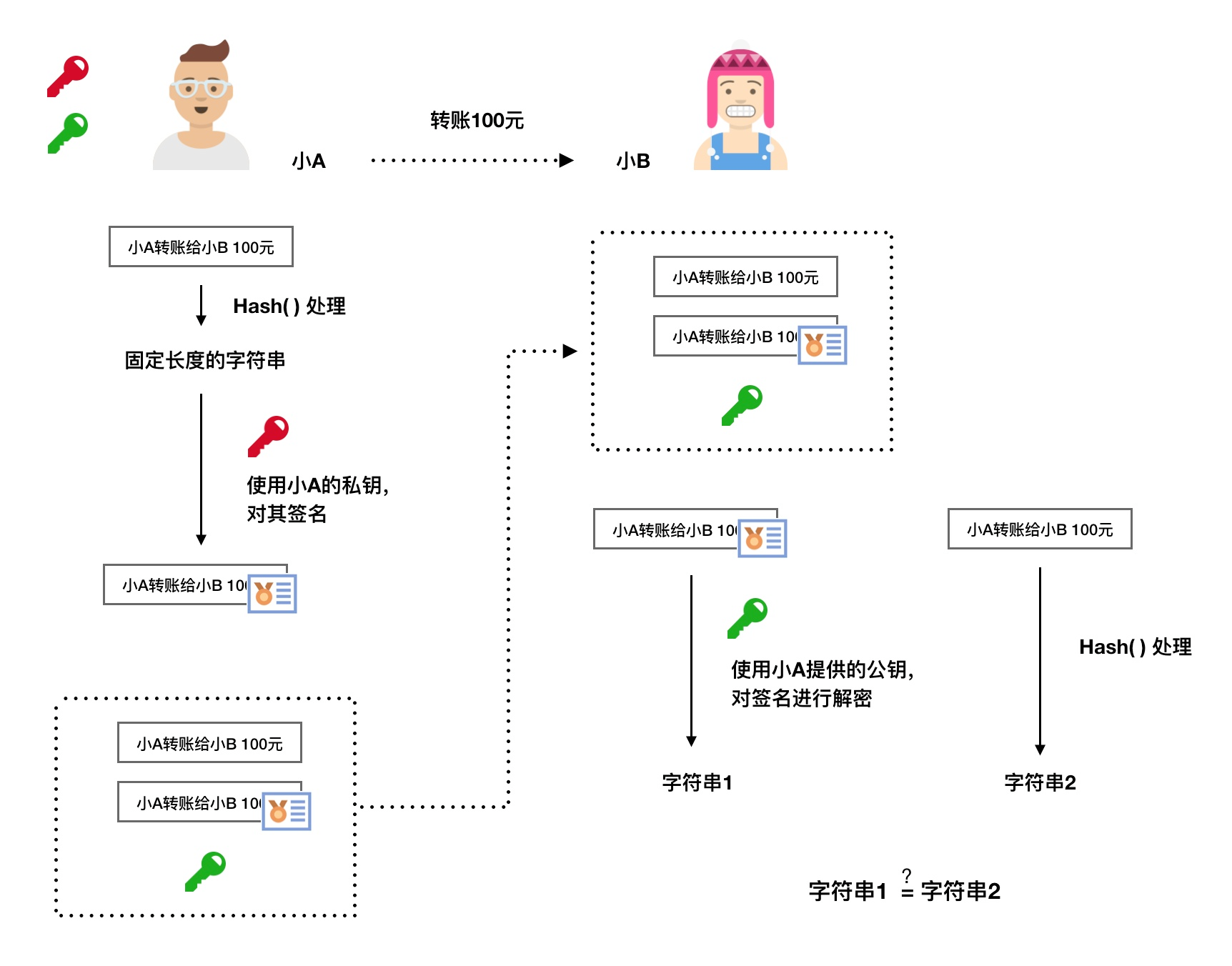
验证：

通过上一次的交易得到公钥，对签名S解密得到x；

用本次交易的公钥和前一次的交易数据进行哈希运算，得到哈希值y，如果x=y，验证成功。

从上图中的交易过程我们可以看到，交易过程只涉及到A、B两人，没有中间人。以我们熟悉的淘宝网购过程为例，交易流程是：你将钱打给支付宝－支付宝收款后通知卖家发货－卖家发货－你确认收货－支付宝把钱打给卖家。本来是买家与卖家之间交易，却需要第三方支付宝介入。而比特币交易过程就是一个去中心化的交易过程。

比特币每次交易都需要网络上的节点来验证是否合理，验证通过后会在网络中进行广播，交易需要矿工打包到区块并被足够多的后续区块确认，这次交易才算完成。

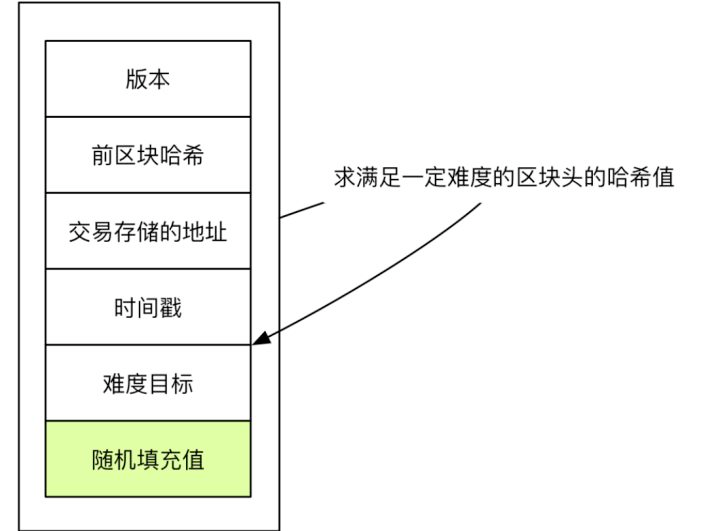
矿工打包区块的过程就是工作量大小证明，也就是常说的比特币挖矿。

工作量大小是通过计算符合某一个标准的比特币区块头的哈希散列值来体现的。区块头通常包含前一个区块的哈希散列值、Merkle根、时间戳、难度目标、以及一个填充的随机值。试图争夺记账权的节点称为挖矿节点，挖矿过程就是求出一个能够填充本区块头的随机值，让区块头的哈希散列值符合某一个标准。

挖矿的过程就是找到x使得

SHA256(SHA256(version + prev\_hash + merkle\_root + time + bits + x)) < TARGET

需要以下参数：

1.block的版本version

2.上一个block的hash值：prev\_hash

3.需要写入的交易记录的hash树的值：merkle\_root

4.更新时间：ntime

5.当前难度：nbits

一旦你找到了x，你就可以广播一个新的区块，其他节点会验证你的区块是否合法。一旦被接受，你就可以得到一笔比特币挖矿奖励。

从上面的区块打包过程，我们可以看到每次交易都需要上个区块的哈希值，这就使得数据可追溯，数据可追溯，网络中的节点就可以通过历史记录验证该笔交易是否有能力去履行，比如验证该笔交易发送者金额是否足够，这使得交易不可伪造。

同时这种区块链这种结构也保证了交易信息的不可篡改。如果某区块被篡改，那么之后的每一个区块都将被改变。因此试图篡改数据的人必须同时入侵至少全球参与记录51%的节点并篡改数据。从技术上来讲,这几乎是不可能的。

从区块链的数据结构，我们知道了区块链如何具备了去中心化、可追溯、不可篡改的特性。

区块链的行业应用

1.去中心化。应用于传统的中心化场景中，替代原本由中介或中心机构处理的交易流程。主要应用行业：银行、证券等

2.信息可追溯。区块中包含了创世块以来所有的交易信息，信息完备公开透明，数据追踪和防伪。主要应用场景：食品安全、信息脱媒

3.分布式记录存储。区块链中每个参与记录和存储数据信息的节点具有相同的权利,不 存在中心节点,因此在受到攻击的时候,也可以保持数据库的正常 运转。应用场景:物联网、智慧交通、供应链等

4.智能合约。 区块链中每笔交易信息基于可编程原理,内嵌了脚本概念,使得基 于区块链技术的价值交换活动升级成为可编程“智能合约”模式。

应用场景:各类合约 、版权保护