易懂的比特币工作机理详解

姚勇（H3D, http://www.h3d.com.cn）

前言

原始论文：
中文版：《比特币：一种点对点的电子现金系统》
http://wenku.baidu.com/view/f26c8d916bec0975f465e236.html

英文版：《Bitcoin: A Peer-to-Peer Electronic Cash System》
http://wenku.baidu.com/view/2e3f91bb1a37f111f1855b50.html

网络上介绍比特币的文章。
1 https://en.bitcoin.it/wiki/Main_Page 很详细。
2 http://blog.codingnow.com/2011/05/bitcoin.html
3 http://zhiqiang.org/blog/it/technical-document-of-bitcoin.html
4 http://www.showmuch.com/a/20110530/233347.html
5 http://ivarptr.blogspot.com/2011/05/bitcoin_31.html
6 http://www.8btc.com

比特币技术的意义

比特币的技术意义在于，人类文明诞生之后，在没有暴力手段（国家法律警察/黑社会）维护下，人与人的交易从来就是不安全的。存在着各种尔虞我诈和骗局。直到 bitcoin 技术出现，才有了一个真正安全的手段，使得人与人直接交易是安全，无法反悔，无法抵赖的。

这个技术不基于信任和暴力，而基于算法。几乎无法作弊。

以下做详细介绍。介绍方法为，尽可能简化概念，用日常可对应的概念对照比特币技术概念。不会很精确，但保证概念正确。

一，比特币运行机理概述

本章介绍比特币世界的运行机理。比特币体系是由账簿(block)，交易单，钱（bitcoin），和交易(transactions)等几个概念组成。

1 账簿（BLOCK），账簿链，与交易单

1）账簿

比特币体系，不存在单独货币。只存在**账簿**（BLOCK）与**交易单。**每个人有自己的账户 ID。每一次交易，获得多少钱，花多少钱，全以**交易单**形式记录在一个全世界唯一的账簿上。账簿上会记录很多交易单。相当于银行交易底单。只要账簿上收支都记录清楚，这个世界不需要单独货币也可以做交易（等于大家都刷卡交易）。
如图：

账簿有很多本。每本账簿只记录比特币全世界 10 分钟内的交易信息。每 10 分钟一个新的账簿被产生（制造/创建）出来。所以账簿随时间流逝会不断增多。每个人每做一笔交易，某个账簿上就会记录这笔**交易单**。这个记录过程是比特币软件通过网络自动完成的（黑客很难伪造）。目前比特币世界存活了 4 年多，就有大概 24 万多本账簿了。（4 年*365 天*24*60 分钟/10 分钟 = 21 万本账簿）

2）账簿链

账簿本全局唯一。因为这个世界发生过的交易肯定是全局唯一的。记账记录也会是唯一的。所有账簿本是被一根链子串起来的（双向链表---**账簿链**）。每个账簿里，都记录着前一个账簿和后一个账簿的索引。知道任何一个账簿，都能顺藤摸瓜向前或者向后找到所有账簿。这也决定了账簿记录交易的前后关系。这等于是银行的对账底单。后面会说交易的前后关系对比特币体系是最核心最重要的事情。

如图：

比特币世界（以下简称“世界”），只有一套唯一的账簿（由于被串起来，也就是账簿链）。在每个用户 PC 上都保存一个备份。等于每个用户都保存一份这个世界从诞生起到当下所有交易的记录备份（全球所有用户的所有交易）。记录备份较大，比特币软件会有优化手段，这里不细说。

每个用户都备份所有交易记录，这就是比特币没有银行的机理，因为不需要一个中心来储存所有交易，每个人都必须要储存所有的。

3）交易单

交易单记录一笔交易的具体信息。比如付款人账号 ID，收款人账号 ID，付款金额，付款人签字，收款人公钥，等。

世界中，每隔差不多 10 分钟，就会有一个新的账簿本制造出来，添加到世界里（加到账簿链尾部）。有了新的账簿，这十分钟里发生的**交易单**，就都写到这个新产生的账簿中。查看账簿可以去这里：http://blockexplorer.com/，输入账簿（BLOCK）的序号，从 0 到 24 万，就可以看每个账簿里记录的交易单。 可以看到序号靠前的账簿（BLOCK）里都没有交易单。说明账簿产生前 10 分钟里没有交易（那时候大家还根本不知道这么个玩意儿）。

世界中，先临时记录下 10 分钟里的交易。然后用这些交易单，创建一个新账簿。把这些记录都放进去。之后这本账簿就封存作为底单。只提供查询用。每个用户账户有多少钱，都要从这些底单中推算出来。

2 钱（比特币/bitcoin）的由来---账簿创建（挖矿）

1）钱的由来

有账簿，可以记录交易。但是世界中总要有钱可花。初始时可以花的钱怎么来的？

世界中每个用户都可以创建账簿。**谁创建账簿，就给谁钱！**

一个账簿被创建后，这个账簿里初始就有钱。钱归创建者所有。所以每个账簿第一条**交易单**总是“世界给予创建者张三 50 元”。注意，比特币世界里没有独立的钱，只有交易单。钱都是通过交易单体现的。钱的产生都是从每个账簿第一条交易单来的。

账簿里初始有多少钱，根据世界中已经创建账簿的数量来定。世界刚开始，创建一个账簿有 50 元。产生到第 21 万个账簿之后，每个账簿里初始降低为 25 元。以此类推，第 42 万个账簿创建后，账簿里初始只有 12.5 元。 但随着账簿创建数量增多，账簿里初始钱减少。最后，比特币世界中只会有 2100 万元钱。钱初始全部是创建账簿的人所有。账簿可以不断创建下去，但是每个新账簿里初始的钱几乎为 0 了。（可花的钱数量恒定，很像通货紧缩的世界）。

这些创建账簿的人有钱之后，可以和其他**愿意**兑换的人兑换，做交易。比如买 PIZZA，或者和**愿意**用美元/人民币购买比特币的人换现金。

2）账簿创建/制造（挖矿）

世界先记录 10 分钟里发生的所有交易单。接着用这些交易单创建一个账簿。账簿里记录了这些交易单。

账簿创建后，成为记录全世界 10 分钟里发生交易的永久记录本。账簿属于这个世界。不属于创建者。但是里面的钱归创建者。

账簿制造很难。不能随意创建。极其消耗电脑时间。大家先理解为那是一个艰难的计算过程，和扔几亿个骰子差不多。要等到几亿个骰子的数字加起来刚刚符合要求。如果网络上一个用户扔出的骰子符合要求，还要和其他正在扔骰子的用户比较。看看谁扔的筛子更多。选出扔筛子最多的人制造的账簿。这要买很多 CPU/显卡来计算，要花电费。是个苦差事。创建一个账簿后，账簿里面的钱，是奖励这些创建账簿的人。也是这个世界钱的由来。账簿极难伪造，所以钱也很难造假。比现实世界造伪币难多了。

世界中，整个世界账簿每 10 分钟产生一个的速度不会改变。不管有多少试图创建账簿的用户在同时努力，每 10 分钟只会有一个新账簿被创建出来。这是算法决定的。算法具体的后面讲。创建出一个新的账簿，这个用户就发了一笔小财。每 10 分钟会有一个幸运儿。

现实世界中，人们需要买采矿机，挖掘矿石卖出得到钱。比特币世界里，人们需要买来强

力 PC 和显卡/ASIC 等，来创建账簿以得到钱。所以创建账簿这件事被形象地叫做“挖矿”。只不过不用去发现金矿位置。在比特币互联网数字世界里，2040 年前，只要有强力矿机，就能挖出矿（创建账簿），随即获得钱（不用卖矿）。

总得来讲，账簿是算出来的，钱也是凭空产生的。之所以有人**愿意**花现实世界的钱去购买，一定是有某种原因的。后面再讲。归根结底是必须有人**愿意**。比如类似炒股票，抄黄金。低价买高价卖。股票是纸，黄金是用处很小的金属。之所以有人**愿意**买，是因为卖得出去，能换成现实世界的物品或者货币。

提一句，挖矿到最后，账簿本身就没有比特币产出了。但是由于交易频繁，交易过程中可能因为交易数量和交易单分支过大，会产生一些交易费。这个交易费会直接给予交易单所在账簿的制造人。这么做是为了鼓励在 2100 万比特币挖完之后，依然有动力继续制造账簿。没有账簿就没有比特币交易体系。账簿必须不断制造下去。否则比特币体系就完蛋了。（没钱谁还挖矿，没矿这世界就坍塌，这真的不是个坑么？）

3 交易过程（TRANSACTION）

用一个例子说明比特币世界交易过程

比如，2012 年某一天，张三要给李四 10 元（单位是比特币）。用来够买李四的披萨饼。张三要做的事，是用比特币软件向全世界宣布，“我张三给李四 10 元了”。 于是比特币世界会生成一个交易单，向 P2P 全网广播，大致内容（不一定精确，但说明个意思）：

1 交易单 ID
2 资金来源---上个交易单 ID（张三的钱从哪里来的，比如王二），
3 王二对上一笔资金的签字（证明是王二给张三的）
4 资金去向---李四收款帐号，
5 数额---10 元，
附加张三的签字（每个用户都能够鉴别这是张三签的 10 元交易单，不能伪造）

之后此交易单记录在世界第 180000 本账簿上。 网络上每个用户都保存了这个交易记录。这就是交易全部过程。这个交易单世界每个用户可以查询。至于张三的名字，是以一串数字代替 。这样虽然可以查询交易单，但是不知道是现实世界中谁做的交易。每个用户在比特世界只是一串数字。用于大家匿名交易。

张三李四各用比特币软件查询自己的账户时，由于第 180000 本账簿上有一笔交易单，李四向全网求证这个交易是否属实，如果属实，李四头上就多了 10 元。张三的账户同理，会少了 10 元。

账户余额统计

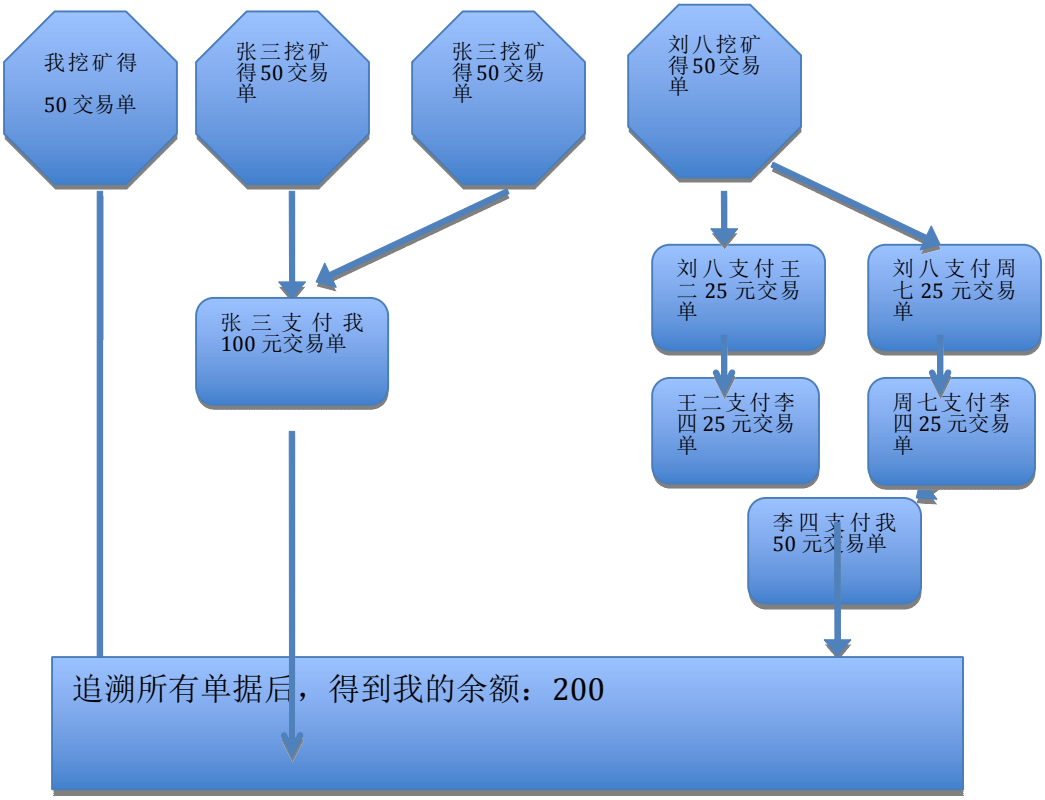
注意，交易单里缺少一个信息，就是张三账户有多少钱。世界中也没有银行储存张三账户有多少钱。那么如何辨别每个人账户有多少钱，是否能够支出那么多数额？ 下面讲解比特币世界如何统计一个用户的账户余额。

统计张三余额，就是统计张三的钱从哪里来，有多少。那只有 2 个可能。1，张三创建账簿

（挖矿）里初始给的钱；2，别人给张三的。从“上一个交易单 ID”可以很容易追溯张三户头的钱都从哪些交易里来。

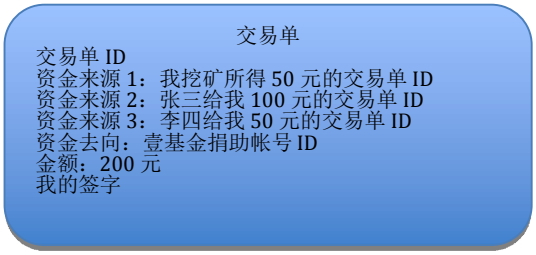
比如我账户有 200 元。来源分别是：1，创建账簿获得 50；2，张三给我 100 元；3，李四给我 50 元。 张三的 100 元是创建 2 个账簿获得。李四 50 元是王二和周七 2 人各给了李四 25. 王二和周七的钱也有来源，比如都由刘八分别给王二和周七各 25 元。刘八的 50 元是创建账簿所得。逐步追溯回去，每个人的钱来源都能统计清楚。那就得到了我账户的 200 元数目。

交易单关系如图（箭头是钱的走向，按箭头的反方向从下到上，是追溯的过程）：



最终大家钱的来源都会追溯到账簿创建时给予创建者的钱。毕竟钱只有“创建账簿”这么一个来源。钱在交易过程中被不断分割为不同数量，给向不同账户。钱在比特币世界中，所有的交易走向历史全部清清楚楚。每个人账户的钱也是靠交易单中的“资金来源”追溯出来。

我如果给出 200 元。我的交易单中就要注明这 200 元的 3 个资金来源（交易单 ID）：1)我创建账簿（挖矿）获得 50 元的交易单。2）张三给我 100 元的交易单 ID。3）李四给我 50 元的交易单 ID。
如图：



二，安全的保障

比特币体系最大的贡献和优点，是很好的解决了交易安全问题。 现实生活中，金子有假的，钞票有假的，支票有假的，信用卡有假的。但比特币交易单没假的。

银行和基金虽然没假的，但是银行利用国家暴力机器，强行逼迫被统治的劳动人民使用它发行的统一货币。从而达到彻底控制人民劳动所得，任意利用金融工具获得巨额利益。恣意增发货币导致通货膨胀，货币贬值，物价增高，人民劳动成果化为流水，房价高到无法负担，或者房市崩盘。人民居无定所。这都是由于某些金融机构，某些国家，某些集团，利用货币中央管理的特点，进行的正确或者错误的控制与操作导致。所以在安全交易的基础上，去中心化这个想法天生有一些令人神往的特点（是不是真的靠谱后面细说）。交易安全也是摒弃中央银行管理的基础。没有安全，一切无从谈起。

下面简单讲述一下比特币体系如何保障用户交易安全的机制。比特币安全机制涉及到非对称加密算法和数字签名，sha256 散列算法(hash），Hashcash 的工作量证明机制等。详细理解机理，需要仔细阅读这些技术文献。为了做到通俗易懂，本文把这些算法全部映射到现实中日常生活用到的概念。不保证精确，但保证概念正确。

比特币世界中，张三提交一笔交易，给李四付款 25 元。类似张三签一张支票给李四。要保证安全，需要确认几点： 1，交易确实是张三提交的；2，张三有 25 元；3，张三签署的支票这 25 元过去没有支付过给别人。以下逐一介绍。

1，sha256（散列/hash）含义

首先我们需要一个编码方法。给任意不同的数据（字符串，字母数字组合排列等，比如账簿内容，或者交易单内容），标记一个全世界唯一的标记（一个整数）。相同的数据，给予相同的标记。不同的数据(字母数字，以及排列顺序等)，一定给予不同的标记。

这个编码方法有个特点。对一个数据编码很容易。但是只有编码，无法反推出编码的数据。这个特点被广泛用于比特币机制。

sha256 散列的含义：可以理解为 sha256 是一个函数。任何一串数据，送入这个函数，都会得到一个整数。这个整数大小范围在 0 到 2^256 次方。也就是 256bit 长度的整数。相同的数据送入此函数，会得到相同的结果。数据不同，就会得到不同的结果。等于用一个 256bit 的数，给任意数据做编码。每个数据都有自己特定的编码。256bit 长度的这个整数非常巨大。比地球上所有沙子的颗粒还多。所以只要送入这个函数的数据稍有不同(字母数字，以及排列顺序等)，这个数据就会得到自己独一无二的 256bit 整数编码。

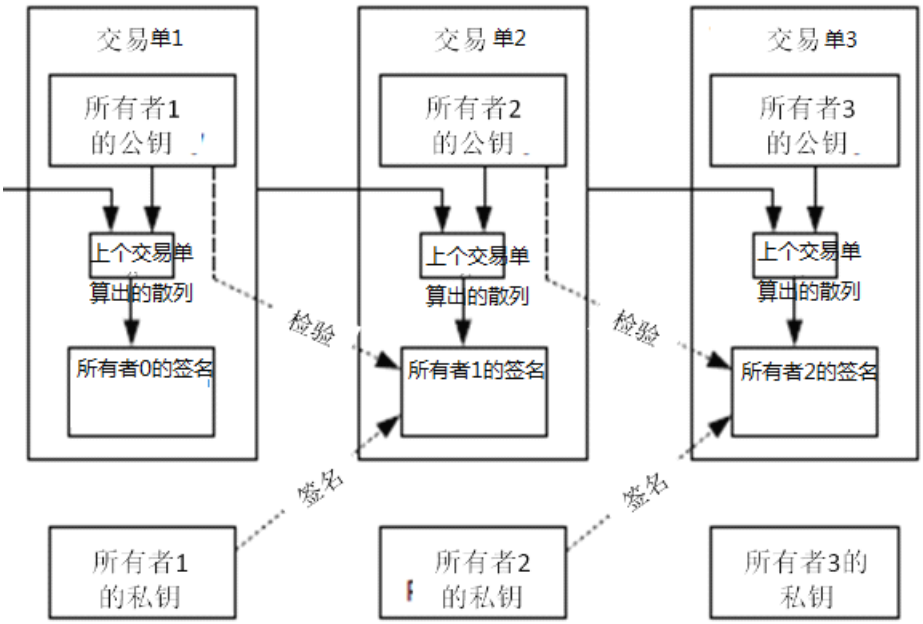
2，是否交易真实 ------ 数字签名

1）交易单签字

由于没有银行做保证中介，张三和李四是直接交易。现实生活中 2 个从未相识的人做交易，会极其不靠谱。因为没有实体货币，张三声称付款给李四后，完全可以不认帐。即便现实中，张三也可以用假币付款然后跑路。

比特币采取的方法是：让付款方用户在交易单上根据交易单内容来签字（数字签名）。并且让收款方有办法验证这个签字的真实性（不用法院和笔迹对比专家）。

如图所示，这是 3 个交易单，代表用户 0 给用户 1 支付钱款“交易单 1”，用户 1 给用户 2 支付“交易单 2”，用户 2 给用户 3 支付的“交易单 3”：



这个签名靠“非对称加密算法”，保证付款方签的字，没人能作假，并且付款方自己必须认帐。

2）数字签名大致描述

有必要简单介绍数字签名。

一个只有签名者自己知道的密码，作为密钥。签名者用这个密钥可以对任意数据加密。得到一个**数字签名**。 同时这个签字者对全世界公开一个“公钥”，意思即为公开的钥匙。其他人可以方便快速的用这个“公钥”解密签字，查看签字的解密后内容。如果有证据表明：解密签字后的内容，与加密者加密的内容相符，就能证明这个内容确实是加密者加密的。比如加密者用私钥加密了一个字符串，写着自己名字的签名。大家用公钥解开一看，便知道这个签名一定是加密者干的。

最重要的是，比特币交易单这个签名和交易内容严格相关。**一个人，用同样的私钥（印章/手印）签署不同内容的交易单，签出来的字也会不同**。这一点是计算机算法比按手印更优越的地方。所以一旦用户对一个交易单签字了，且被其他人验证，就有两样事情他无法抵赖：1，付款方签字付款了；2，付款方的资金来源（包括金额）

3）对交易单的签名和验证过程

签名：

1 付款人 A 首先制作一张交易单 T2。T2 要包括收款人 B 的“公钥”（一组数字）。

2 得到 A 资金来源的上一张交易单 T1 的数据。T1 代表 A 要支付这笔钱的来源，它必然是之前某个时刻由某人通过 T1 支付给 A 的（或者挖矿所得）。

3 利用 T1 的数据和 B 的公钥联合起来，求出一个 hash 数值 x。

4 A 用自己密钥对 x 进行加密。得到一个 A 的签名 s。

5 把这个 A 的签名 s 附加到交易单 T2。发给收款人 B。

验证：

B 为了验证这个签名。需要做以下事情：

1，得到付款人 A 的公钥，这是解密 A 签名 s 的钥匙。 付款人的公钥，会在此张交易单的上一张交易单 T1（资金来源交易单）里。 因为 A 要付款的这笔钱，一定是之前某个时刻，由某个人 X，通过交易单 T1 发给 A 的。 于是付款人 A 的公钥也会在上面。

2,收款人 B 解密 T2 上 A 的签名 s，得到 A 加密前的内容，是一个整数 x。

3，收款人 B 把 T1 交易单数据与 B 的公钥联合起来， 取 hash 值 y

4，检验 x 是否等于 y。如果等于，那么说明 T2 交易单有效。一定是 A 发出的，且资金来源 A 无法抵赖。因为资金来源是 T1 交易单中的支付内容数据（包括金额），已经被关联计算到 hash 值 y 中。A 既然对 y 加密 成为数字签名 s，而这个加密过程只有 A 自己能做，故而证明交易单 T2 是 A 签署支付的。

网络上没有人能签出一样的数字签名。而且如果这个世界上存在一个被你签名的交易单，说明你确实签过这个交易单，这个事实无从抵赖。类似现实生活的指纹画押。这都是算法保证的，不用怀疑。类似方法各大银行包括美国军方也在使用。

有交易单，上面有你的签字。证明你确实付款了，而且这个签字和交易金额直接相关。金额也无法抵赖。于是你账户的钱就会少。耍赖反悔是没用的。相当于卡已经刷了，你再也没有能力拿回你的钱。

你不能制作一个别人向你付款的交易单。因为只有付款的人才有能力签字。你没有对方的密钥（印章/手印等），无法签出一张别人向你付款的交易单。

另外如上图交易单关系图所示，每个一笔钱的走向是由一系列交易单链串起来的。交易单签名的时候，签出来的名字，不仅和一张交易单内容相关，而且还和这笔钱之前相关所有交易单的内容都相关(签字的形成，和前一个交易单的散列值相关）。这一个签字下去，就固化了一笔钱上所有交易单的内容，金额与之前的签字（签字也是交易单内容的一部分）。任何人可以很容易的验证和这笔钱相关交易单链中的所有签字。这意味着：要伪造或修改一个交易单，需要把一笔钱交易单链条中，被修改交易单后面所有交易单全部修改一遍。而交易单储存在全世界统一的账簿中。账簿又被所有用户备份。所以比特币世界，没有任何人能够修改交易单链中间的单据。

3，是否有足够的钱支付

前面的“交易单关系图”，说明了如何根据交易单内容的“资金来源”一项，最终回溯出一个账户的余额是否足够支付交易单款项。一个用户是否可以伪造自己的账户余额？并且签署一个交易单，支付出本来不存在的钱？

首先，伪造挖矿是极难的。后面细说。

其次，伪造某一个交易单。让交易单的“资金来源”指向一个金额很大的大款账户交易单。这需要伪造那个大款账户的签名。因为“资金来源”下面跟着是资金来源付款方的签名。这个签名必须和交易单内容对应上。每个用户私有签名别人无法模仿，这是算法保证的，所以做不到。

然后，篡改交易单，让交易单的“资金去向”是自己的小号，然后付款金额改得很大。根据交易单关系图，金额修改得再大也没用。因为软件要从这个账户交易单一直追溯到挖矿记录。你篡改的交易单金额，无法正常回溯，会识做非法支付。即便你篡改了自己的软件。当别人用正常软件回溯交易单（注意交易单是全世界统一的）时，依然会露馅。

4，是否重复支付 ------ 建立全局唯一交易记录

还有一种对交易单篡改的情况，没有列出。那就是复制交易单。修改其中一个交易单的收款人。从一个“资金来源”，重复向 2 个人付款。这就是“重复支付”。

举例：

A 挖矿所得 50 比特币后。A 给 B 支付 50 比特币换取 PIZZA。提交一个交易单“AB”。然后复制此交易单变为“AC”，改为 A 给 C 支付 50 比特币换取 50 美元。A 把“AB”和“AC”2 个交易单同时提交出去。

由于网络传输速度不同，B 先接到了付款交易单 AB。快递了 PIZZA。C 先接到了交易单“AC”，支付给 A 美元。由于交易单签名是合法的。只是由于 B 和 C 所处网络地点不同，无法全面了解 A 发出交易单的全部情况和顺序。导致 A 用 50 元的余额账户支付了 100 元。 所以这种由于没有中央服务器来决定交易时序的情况，就必须得到解决。

在银行的体系下，于比特币的付款类似在支票上签字。当我签字两张支票给 2 个收款人后，2 个收款人会去银行兑现。银行的交易记录中，2 人的兑现必然是分前后次序的。一个人用支票从我账户取钱时，另外一个人绝对不可能同时从我账户取钱（双重支付）。假如我账户只有 50 元。我签署了两张 50 元的支票。2 个收款人同时在 2 个银行网点兑现。银行的交易记录必然有一笔兑现交易在前，取走 50 元后，我账户余额为 0.第二个收款人无法再从我账户提取现金。假如银行允许同时支付，2 个用户同时兑现支票，他们俩人都会发现我账户有 50 元。于是同时提现.....比特币系统大家都是平等地位，没有银行之说，谁也说不清我是否为一笔钱签署了两张支票。即便需要把 2 张支票的交易向全网广播，由于网速问题，整个网络也无法判断哪笔支付在前。

禁止重复支付，是比特币技术要解决的核心问题。它的核心，就是在 P2P 网络体系下，**创建一套全世界统一且唯一的有前后次序的交易记录**。以保证一笔钱的交易没有重复支付的情况。下一章专门讲解。

三，P2P 中建立全世界统一交易记录的解决方案

1，统一交易记录的意义

有一套全世界唯一的交易记录，在一笔钱被支付时，就能够查出之前这笔钱有没有进行过支付。类似刷卡交易，卡上的钱一定是之前没有支付出去的。现实中，这是银行的统一交易单系统保证的。钱被按照次序依次支付。比特币的支付都是靠电子交易单，如果没有统一的交易记录和交易次序，交易单很容易复制后同时发送（修改支付对象）出去。等于同一笔钱支付了 2 次。这个非法行为在网速不同的 P2P 网络上很难判别。

2，统一交易记录的次序------时间戳机制（TimeStamps）

统一交易记录的核心数据，除了每笔交易内容，还有每笔交易的前后次序。只要有了全世界所有交易的前后次序。尤其是对于一笔钱支付的先后顺序。就能够防止一笔钱被支付两次。因为一笔钱被支付过后，不可能再重复地从同样的支付人账户中支付出去。

我们知道比特币世界有一套全局统一并且唯一的账簿本集合。每本账簿记录 10 分钟的交易。按照时间顺序，账簿依次排列。我们肯定不能用一段字符串标记时间，来判断账簿的前后关系。这种明文在没有中央节点服务器的体系下是行不通的。因为用户机器上的时间不可能都严格一致。

我们要做的只是把账簿数据产生的前后顺序用某种算法固定和记录下来，并且可以验证。

决定账簿前后关系的机制，采用了**时间戳机制（TimeStamps）**。

这里时间戳的意思是对数据产生的先后次序进行标记。这个标记很难人为修改。很容易被反复验证。在时间戳机制中，这个标记使用一个账簿数据的 hash。

如果我们使得每个账簿的内容，和前一个账簿内容相关，并且可以验证这一点。那么就可以说明账簿的前后关系。因为如果没有前一个账簿的内容去生成后面的账簿，后一个账簿内容一定是非法的。

举例说明：

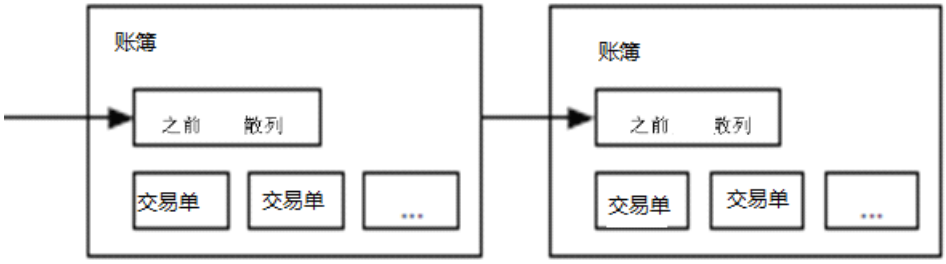
1，把账簿 A 的全部内容当成数据，计算一个散列数值 a。

2，把这个散列数值 a 放入下一个账簿 B 里。

3，验证账簿 A 一定产生于账簿 B 前一个：找到账簿 B 里的散列数值，姑且叫 x。 计算账簿 A 内容的散列 a 。 假如 x = a ，那么结论成立。

4，继续使用账簿 B 的全部内容生成一个散列数值，放入 C，依次类推，形成账簿链条。

如图：



形成这样的链条不用依据用户机器上的时间。只根据数据产生实际的先后关系。这样的链条一但形成，没有任何人能够修改账簿的前后关系。因为牵一发而动全身。要颠倒 2 个账簿的次序，就要重新计算改动账簿之后的所有账簿内容。再次提示，这是 P2P 网络，所有用户都备份同一份账簿链，修改所有用户机器上的备份数据是不可能的。哪怕修改 51%用户机器上的数据都不可能。 而验证数据产生的次序，概念上是要靠全网用户表决的。

3，统一交易记录的产生

1）综述

银行系统使用了大量人力物力，联合暴力国家机器，来保障中央服务器的安全，也就是产生和维护一份全球唯一的，反应交易事实和次序的交易单。

中央服务器带来的好处显而易见。互联网应用通常都基于 SERVER/CLIENT 模式。网站服务器，网络银行服务器，游戏服务器，域名服务器等。但弊病是一旦服务器被攻击，占领，那么整个服务体系全部沦陷崩溃。

P2P 网络没有中央节点。每个 PC 用户都是平等的。一套全世界统一的账簿，无法从一个中央服务器中产生。这是 P2P 网络最大的特点。

作为 P2P 体系，没有中央节点是其最明显优势。但维护一套全局唯一且值得信任，不会被攻击的数据，则没有简单易行的办法。而 P2P 节点都是平等的。全局统一交易记录只能由全部 P2P 的节点协作来产生。

假如这套交易记录能够被 P2P 上的邪恶节点进行伪造，改写。那就会导致比特币经济崩溃。所以必须靠算法解决。不让任何人轻易修改记录。

2）解决办法 ------ 全网节点协作产生

产生全局统一交易记录的解决的办法是：**全体用户一起协作产生**。

准确的说，是全网挖矿节点一起协作产生。

注意，“挖矿节点”，以后被简称为“节点”。

为了全体一起产生统一的交易记录和交易次序。需要每一笔交易都在全网广播。这样一来，一笔交易就可以由全体用户都来验证是否通过。这等于是全体用户做了银行。

比如今天我在全网喊“我给张三 100 元”，全世界人都知道了。大家一起协作，把这个交易记录到一个全局统一的交易记录账簿中。

到了明天我要抵赖不给张三钱，是不行的。同样，假如我给张三钱的时候如果同时喊“我这笔钱同时再给李四”，或者过了一天我又喊“我昨天的那笔钱 100 元再给张三一次”， 也是不行的。

原因是：我手里没有实际的钱币，钱都是写在交易单上，交易单由大家维护，全世界唯一，备份保存在所有用户机器上，扣钱的时候，张三会问全世界人是不是有这么一笔交易存在。这个时候，我要抵赖，只有通过强行修改这个世界上所有 P2P 节点上的交易单。显然这不可能。

也就是说，一个中央银行，变为了所有用户都维护一套中央银行数据。大家一起维护这个数据。随时更新。一起决定某个交易是不是合法。

要集体维护一个统一的交易记录不是一件容易的事情。这可以解释为什么这个世界要每 10 分钟创建一个账簿。为何账簿创建（挖矿）如此困难。为何 10 分钟内的交易单要打包到一个账簿。为何全局唯一的账簿要用一个链子串起来。

这些全都是因为要解决比特世界中交易的时序问题。以及防止这个机制被作弊者破坏。因为比特币交易是基于算法安全，而不是基于信任，法律，集权，强迫，惩罚等手段。

3）P2P 诚实用户节点创建账簿（交易记录）

由于交易单是全网络广播。每个用户都可以得到所有交易单。其实，只要一个诚实的用户，根据接收到交易单的次序，创建的交易单记录，就可以给大家作为全局统一的账簿。账簿作为对交易单的永久封存。

P2P 上不同的诚实节点，也许某一时刻收到的交易单的顺序不一样。但这没有关系。如果我有 100 块，先买 20 块的 PIZZA 还是先买 50 块的手表，都是花钱。只要我的钱足够，我的付款交易就有效。如果我先花掉一些钱，账户变空，又收到一些钱，再花掉这些钱。这就对交易的顺序记录有所要求。由于交易单都是可以回溯的，并且一笔钱相关的交易单也都串成一条链 。一个诚实节点只用等待所有交易单发送到自己机器上，进行记录便可。交易单本身就知道交易顺序(每个交易单都会记录这笔支付款的资金来源交易单索引)。

所以，创建账簿的问题，其实归结为：**如何判定一个制造账簿的用户是诚实的**。这就需要全网诚实节点协作了。

确认一个节点是诚实的之后，就采纳这个节点创建的账簿。作为全世界统一的账簿作为交易记录。每个比特币用户都复制一份这个账簿的数据到自己机器上。

4，诚实 P2P 挖矿节点判定

1）hashcash 的工作量证明

hashcash 机制大致描述如下（http://www.hashcash.org）：

如果希望判定一个人提供的的信息是本着正常使用，具备一定价值的。那么我们倾向认为提供这个信息的人，愿意为此付出一定工作量来证明他的诚实。假如有一种机制，能够容易的证明提供信息的人为此付出了一定工作量，那么此信息是可以接受，并被认为合理的。

比如，我收邮件的时候，做了一个规定：“把邮件内容数据，加入一个随机数，求一个 sha256 散列数值。这个散列值一共 256bit 。前 20bit 必须都为 0”.

这样，要给我发信的人，就必须反复尝试一个随机数，以保证邮件内容数据加上这个随机数，能够产生 sha256 的结果------前 20bit 都是 0.

如何产生出指定要求的整数？完全靠运气和 CPU 运算时间。这就是一个工作量。工作本身毫无意义。但是如果谁愿意付出这个工作量，就意味着他给我的邮件多半是有意义的。这就叫“工作量证明”。也就是意味着这个人很有可能是诚实的。

这个机制被广泛用于防止垃圾邮件等。因为群发垃圾邮件的人，不可能有那么多时间去给每个人算一个毫无意义的数字，浪费时间，降低发垃圾邮件的效率。

2）比特币的工作量证明

比特币系统最棒的做法产生于此：把工作量证明与建立全局统一交易记录结合起来

一个 P2P 用户节点如果要试图创建一个被全网认可的新账簿（挖矿节点），要花很大力气做一些毫无意义的运算（挖矿）。运算结果可以被所有人容易的证明他确实做了这些工作。得到结果的同时，他就创建了一个数据块，这个数据块里面可以放入一些经过这个用户节点检验的交易单。这些交易单有**严格的顺序**。由于他创建这个数据块花费了很大力气，所以多半他是诚实用户，这个数据块也许值得信任。里面的交易单的真实性也就值得信任。于是这个数据块就有可能作为账簿被全网接受。

这就是比特币最核心的工作机理：依靠“工作量证明”来创建存放交易单的账簿。

下面介绍比特币中如何进行“工作量证明”：

为了证明我是一个诚实的用户，我需要做一个数字游戏。 目的是猜出一个随机数。

游戏的规则是：

1，得到这个世界中已经创建好的账簿链中最后一个账簿，用这个账簿内容做数据，计算一个 hash 值

2，不断接收这个世界被广播出来，且没有被放入账簿链的交易单。检验这些交易单（根据交易单链信息和支付款项等信息），剔除掉不合理的（比如账户余额不足的支付）。

3，猜一个幸运随机数 n（比如从 0 一直到 999999.... ）

4，把 1-3 步骤得到的数据都组织起来成为一个数据 buffer，送入 sha256，得到一个 256bit 的散列值 x

5，检查 x 这个整数，前面若干 bit（比如 96bit）是否都是 0？如果是，这个 x 符合“工作量证明难度”么？ 如果符合，那么“工作量证明”游戏结束！

6，如果不是，从步骤 2 开始不断重复。假如这个时候收到了一个其他节点发来的新的账簿数据块。 还没有猜出满足要求的随机数，需要重新开始游戏。

“工作量证明难度”：有一个本地难度标准。这个标准是一个浮点数，可以换算为一个 256bit 的整数。算出的 sha256 散列值 x 必须小于这个难度数字。

这种重复性的计算往往要重复上亿次，才会得到一个幸运随机数。

游戏如果及时结束，我们就得到了一个幸运随机数 n ， 以及一组未放入世界统一账簿集里的交易单！ 这个随机数 n 代表了我为了证明我的诚实做出的努力。

到此为止，一个“工作量证明”结束。 我证明了我是个诚实的用户。

不过，一个用户最终被判定为诚实用户并且能够创建出账簿，还要靠另外一个 P2P 竞争机制。我们在下面“账簿的创建”中讲解。

5，账簿的创建，以及重复支付检验

得到幸运数字并不等于能够成功创建账簿。最终判定需要得到全网节点的认可。

1）全网账簿创建速度控制 ------ 10 分钟一个

前面说过，得到幸运随机数后，计算的 sha256 值要经过难度检测。看计算出的散列值是否小于某个“工作量证明难度值”。

比特币依靠这个难度数字，来进行全网账簿创建的速度调整。每过一段时间，节点都会检测新账簿的创建是否符合 10 分钟一个。 如果不符合，则调整这个难度数字，使得下一个账簿创建的时间或延长或缩短，让这个世界的账簿创建速度始终保持 10 分钟一个。

这个机制屏蔽了日益增快的硬件计算速度带来的影响。把摩尔定律闭之门外。

2）创建临时账簿，打包广播

当我得到了一个幸运随机数，意味着我只是获得了一个创建临时账簿的权利。我马上把以下数据打包成一个账簿数据块：

1，sha256 算出的 x，作为这个数据块 ID！这个 ID 前面几十 bit 全部是 0.

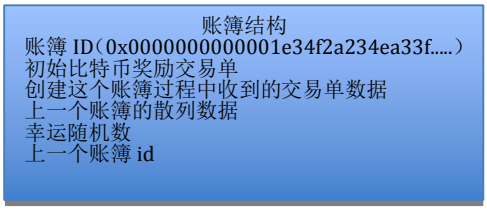
2，做游戏时收集到的所有经过我检验的交易单，

3，幸运随机数 n，

4，世界账簿链中最后一个账簿的 hash 值

5，账簿需要的其他信息

如图：



账簿数据块被我在全网广播。意思是：“大家看，我算出了一个幸运随机数，大家把我创建的账簿加入到世界统一账簿链中”

3）检测重复支付

当由节点创建出来的临时账簿在全网广播后，每个收到账簿的节点都要判断这个数据块中的交易单都是合法的。并且，根据已经创建的世界账簿链中交易单，逐一查找，以判断这个临时账簿内所有的交易单，在世界中已经发生的所有交易中从来没有出现过。这点很重要，判定是否

有**重复支付**，就在这个环节完成。

当所有节点检测一个临时账簿没有重复支出，交易单都合法后，节点会把收到的这个账簿，临时挂接到本地备份的世界账簿链的最后。

4）账簿链分支判断，最终创建账簿

在一个节点进行工作量证明的同时，全网其他希望创建账簿的挖矿节点（要知道创建账簿成功是会有钱的!），也在做同样的事情------不断接收网上广播的交易单，根据这些交易数据，计算出幸运随机数。然后打包成临时账簿，广播出来。

全网到处广播着被新创建出来的临时账簿。有时候一个节点会先后收到连接在同一个链尾部的多个新创建临时账簿。

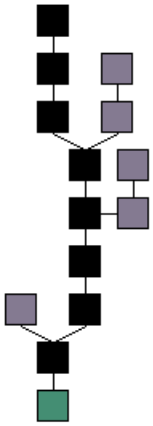
这时候，一个节点在本地会把自己维护的本地账簿链建立分支。比如一个节点先后收到 2 个临时账簿块。它们两个同位于世界账簿链的最后一个账簿链表的后面。 于是在本地数据的账簿链上，生成 2 个分支（两根链条）。之后此节点继续在先收到的账簿分支后面进行工作量证明的工作------利用先收到的临时账簿，进行创建下一个账簿的工作。

每个节点收到新建临时账簿的时间不同，在本地建立的账簿链分支也会不同。

当节点收到最长的工作链账簿时，会抛弃掉比较短的分支。转为在最长的链条上工作。

注意，这里所谓“最长的工作量”，是指计算难度最大的工作链。 计算难度由一个节点本地的难度系数控制。这个难度系数随着随机数计算速度而改变。每个账簿块里面会记录一个难度系数。

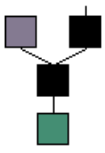
举例如图：



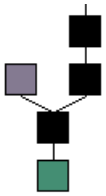
绿色为世界第一块创建的账簿（创世纪账簿）。 黑色方块为这个世界最长的账簿链。也是最终被全网所有用户确认为世界统一账簿。并在本地备份。 灰色的方块代表某个节点临时工作的本地账簿链分支。当某个分支收到新账簿而延长后，另外一条短的分支会被抛弃。里面的交易单会被拿出来检查，如果存在没有放入现存账簿的交易单，会继续用作新工作量证明的素材。

这条账簿链形成的步骤如下：

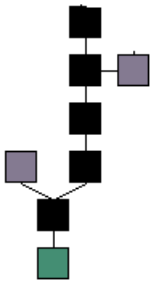
1，先后收到连接在同一个尾部的 2 个不同临时账簿，都以绿色上面的黑块作为前一个账簿。打分支



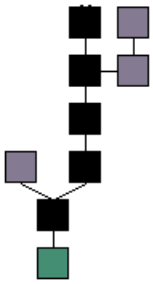
2，右边账簿收到了后续账簿，抛弃左边分支



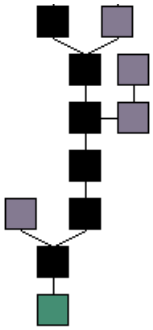
3，右边收到了连接在同一个尾部的 2 个不同临时账簿



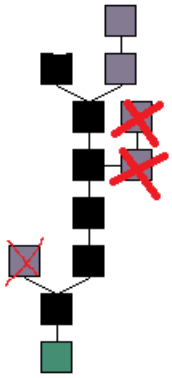
4，先收到了链接在右支路的账簿块



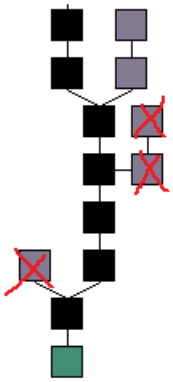
5，又收到了 2 个链接在左边支路的账簿块，这时 2 个分支还是一样长，都无法抛弃



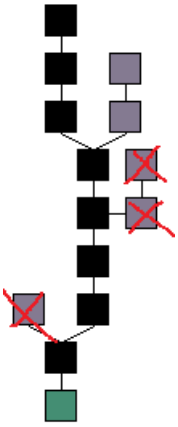
6，新支路上收到一块，彻底抛弃最右边的 2 个灰块



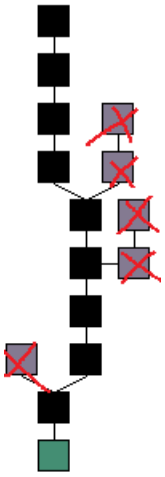
7，左路又收到一块



8，最终左路又收到一块，成为最长链，



9，假如左路继续收到账簿块链接，则右路彻底会被抛弃



临时账簿被不断创建，广播。当全网节点全部确认一个共同的难度总和最大的账簿链条，并开始在这个链条之后开始工作量证明，这个账簿链中的账簿，就被最终确认为世界统一账簿链。里面记录的交易单，就作为世界统一交易，被永久封存。

创建账簿的过程，也就是检测交易单正确性和顺序的过程，也是保存交易单的过程。同时它还是创建比特币的过程。创建账簿的机制是比特币的核心。

由于全网节点一起在不停的计算，创建新账簿。所以账簿链增长最长的分支，代表了全网用户做出的最大工作量证明(每一个黑快代表一个用户得到了一个工作量证明随机数)。凡是在这个最长链中的账簿，就被全网所有用户认为是最诚实，最可信的。

换句话说，是全网络诚实的节点一起工作，进行工作量证明的工作。并且全网还要一起来判别，哪个账簿工作在最长账簿链上，就代表了最诚实的账簿创建。

5）全网协作与竞争，每 10 分钟唯一的最诚实赢家

P2P 网络是个完全平等的网络。你可以挖矿创建账簿得到钱。我也可以。在同一时间，也许全球网络中有无数个账簿被创建出来。但是比特币世界依靠前面账簿创建的难度机制，以及最大工作量分支机制，限制了每 10 分钟只有一个账簿会被确认。因为账簿是全局唯一，每 10 分钟的交易单和交易单次序当然只能放入唯一的账簿中被大家承认。这就保证了全网统一的交易记录。

PC 电脑速度越来越快，计算那个幸运随机数的速度也越来越快。这个世界账簿的创建不能受到越来越快电脑硬件的影响。于是引入工作量难度机制，电脑越快，难度系数会被调整得越高。电脑计算出幸运随机数的速度就都慢下来了。

全网所有挖矿节点都在争相用“工作量证明“创建数据块。每十分钟只有一名幸运的用户从竞争中脱颖而出。这种竞争保证了全网不断增加的账簿链中，难度最大的分支代表工作量最大累计的证明。一个用户一秒钟内做了更多的 sha256 运算，说明他越诚恳，越诚实。于是他产生的账簿的难度系数可能越高，就越有可能添加到最长的账簿链分支上。最长分支代表了最大工作量证明，从而被全网节点认可。简单说，如果我算得快，在最长链上工作，增加这条链的难度总和就大，就越有可能竞争过其他对手。把自己工作的链变成最长。但我尽管算得比别人快，但我的账簿产生速度并不会很快。因为我计算难度大。所以还是很可能被其他节点抢先算出下一个账簿块。从而加到最长链上。

由于大家创建账簿块的速度差不多，而我创建账簿的难度系数大，所以在竞争中我会比较

有优势。

这就是靠协作与竞争，判断出最诚实，最卖力气的一些节点。它们创建出的账簿被全网确认账簿的几率就大。从而会得到更多的钱。

由于这些机制保证，所以伪造一个新账簿，从而为自己账号加钱，非常困难。因为你要作弊，就需要算出一个合法的账簿 ID。这个 ID 要得到全网承认，必须在 10 分钟内所有竞争对手中脱颖而出。想竞争过全网络的所有挖矿节点，你的计算能力必须要比他们加起来的计算量还要大！

6，交易确认过程

到此为止，介绍完全部比特币工作机理。下面描述一个完整的交易确认过程，交易单的确认，是靠账簿的不断创建和确认来进行。过程如下

1，新交易单广播到全 P2P 网络

2，挖矿节点收集所有的新有效交易单，放入一个新数据块

3，节点开始根据新数据块内容结合老数据块散列，计算一个符合要求的随机数，试图产生一个新的账簿 -------比特币工作量证明

4，如果一个节点找到了幸运随机数，表明创建了一个账簿。马上广播到其他节点

5，其他节点开始验证这个新账簿的有效性，检测账簿内的交易单都是新的，之前没有重复支付过。

6，如果其他节点验证此账簿有效（账簿链上账簿创建难度之和最大），则承认它。这个账簿算正式挂接到全局账簿链后。然后开始在此账簿后面继续创建新账簿

一个交易单，要想被最终确认。需要首先被放入一个新成功创建的账簿。然后，再经历几个（一般是 5 个）新账簿的创建后，这个交易单才被最终确认安全通过。表明支付成功。

因为往往世界账簿链被增加 6 个之后，账簿链被修改和作弊的可能性已经几乎降为 0 。这个时候确认交易成功是绝对可靠的。这么做背后的原理是，作弊者无法找到足以抗衡网络所有诚实节点计算能力的计算机集群，去强力计算持续在世界账簿链上增加 6 个假账簿。

一旦一个交易单被所有节点确认通过，再想修改和取消，几乎是不可能的。这保证了比特币体系的不可逆转性和不可更改性。

7，保证账簿合法性机制详解

1）P2P 所有网络用户监督交易，保存全局统一交易记录备份

交易用投票进行，而全体用户的交易记录和客户端无法同时被篡改。保证数据安全性。

其次，P2P 网络不接受非法交易。比如我伪造一个新交易单，挖矿所得 5000 元。 这种交易单，在 P2P 的其他网络用户客户端上，无法通过鉴定。也就无法支付我伪造的 5000 元。

2）时间戳保证交易顺序，无法修改账簿链

交易顺序的保障，制止了电子货币的重复支付。

利用时间戳机制，创建新账簿要包含一个”上个账簿数据散列值“，是为了把所有账簿创建都联系起来。新的账簿创建总是依赖于老的账簿数据。这个机制保证了这个世界的账簿是一环扣一环创建的。每一环的数据都决定了下一个账簿 ID 的产生。所以，即确定了账簿产生的顺序。也保证没有人能够孤立地改变其中一个账簿内交易单的数据而不被检查出来。

因为如果改变了账簿链中的一个账簿内交易单的数据。这个账簿的散列值就一定会变化。账簿散列值变化，一定会引起这个账簿之后创建的所有账簿的 ID 号发生变化！要改变这个作弊账簿之后所有账簿的 ID，我们都知道，不可能。因为全网用户机器上都有一个账簿链备份。

3）sha256 保证创建合法账簿极难，检验账簿合法性极其容易

创建一个有效账簿异常困难，但检查一个账簿是否有效非常简单快速，把一个账簿的当初创建时用到的数据送入 sha256 函数重新计算一次，必然得到此账簿的 ID。所以每次交易，每个用户都可以使用全世界统一的账簿链，通过里面的交易单，追溯钱的来龙去脉，彻底搞清历史交易清单。从而保证自己的交易安全。

4）非对称加密保证无法伪造别人支付给作弊者的交易单

无论我怎么修改交易单，或者新添加一张伪造交易单，我都无法伪造其他人的签名。也就无法从别人的账户偷来钱。

5）工作量证明机制，保证数量占优的诚实节点产生的统一交易记录内容与次序真实

前面的机制，把伪造挖矿，伪造他人支付，伪造非法交易单，伪造交易次序，重复支付等情况完全杜绝。

作弊的方式在比特比体系中，只有很少几种可能，比如改变刚刚发生的交易单，试图拿回刚支付出去的钱。也就是抹掉类似向全世界喊的“我支付给张三 1000 元”这样的交易。

要这么作弊，就要试图创建假的账簿和交易单。附加在已有账簿链的最后。然后在假账簿后面持续制造新的假账簿，以维持世界统一账簿链，不被诚实节点创建的账簿所冲掉（假账簿链分支难度和变为短分支，被丢弃）。这需要作弊的节点制造的账簿能够被全网判定为最长分支上的账簿。这需要比全网计算能力还要强的运算能力。或者掠夺诚实网络节点的一半以上成为作弊节点。

下面详细解释对交易单和账簿的作弊是如何被避免的。

做个假账簿也需要链接到世界账簿链最后，形成连续的假账簿链。比如我在第 240000 个账簿之后要产生一个假账簿，链接到已存在账簿链最后。假账簿里面删除掉我向世界喊的“我支付

给张三 1000 元”这个交易单。由于一个交易确定，需要在交易发生之后，世界上产生 6 个被全网认可的新账簿。所以我需要连续生成 6 个假账簿，里面不包含“我支付张三 1000”的交易单。

要这么做，我必须生成 6 一个难度系数很高的工作量证明随机数。然后把假账簿打包广播出去。其他诚实节点一定会产生含有“我支付张三 1000 元“交易单的账簿。我的 6 个假账簿必须在全网挖矿节点竞争中连续胜出。这需要我的账簿制作的难度系数比所有诚实节点产生账簿的难度系数之和都高。

之所以要比其他诚实节点制作账簿难度之和要高，是因为，我作弊生成假账簿的同时，全网都在共同协力生成新账簿。一个账簿要被认可，需要从 10 分钟内全网竞争中产生。

考虑极端情况，可能有的节点，在收到我广播的假账簿之前，就已经把其他诚实节点的账簿都串接到了账簿链上（由于网络延时，且诚实节点间没有竞争）。 这样，我的账簿制作难度必须比这些诚实账簿制作难度之和要大。这样才能在假账簿链分支的长度上领先诚实节点创建的分支。由于之后不能让任何一个含有“我支付张三 1000 元”的账簿出现在世界统一账簿链中。所以我需要再制作 5 个假账簿。继续保持我创建账簿的难度系数，比全网全部的诚实节点创建账簿的难度之和要大。

这需要比全网络所有节点总和还要大的计算能力。而代价只是我收回了刚刚 10 分钟内支付的几笔交易。这完全不现实，也不划算。

如果有了比全网节点计算力还强大的电脑，我应该持续做诚实节点挖矿，这个收益会比作弊要强。从动机上也避免了这种作弊发生。