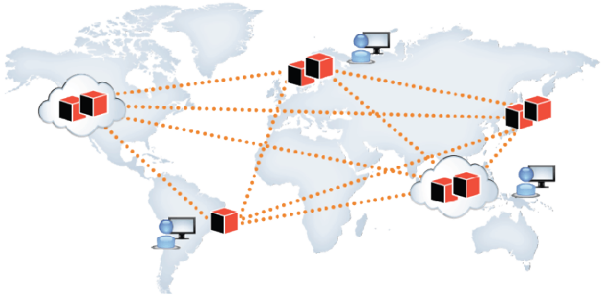
区块链本质

2018年2月8日 16:17

一、区块链的本质

区块链是什么？一句话，它是一种特殊的分布式数据库。



首先，区块链的主要作用是储存信息。任何需要保存的信息，都可以写入区块链，也可以从里面读取，所以它是数据库。

其次，任何人都可以架设服务器，加入区块链网络，成为一个节点。区块链的世界里面，没有中心节点，每个节点都是平等的，都保存着整个数据库。你可以向任何一个节点，写入/读取数据，因为所有节点最后都会同步，保证区块链一致。

二、区块链的最大特点

分布式数据库并非新发明，市场上早有此类产品。但是，区块链有一个革命性特点。

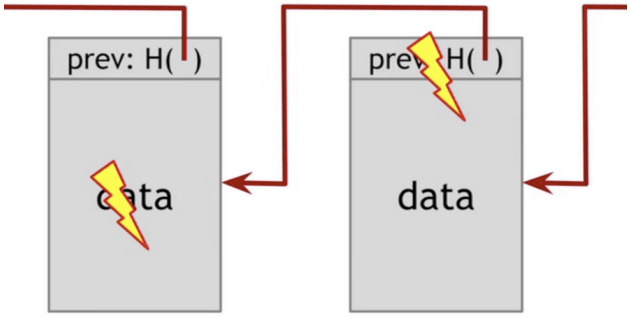
区块链没有管理员，它是彻底无中心的。其他的数据库都有管理员，但是区块链没有。如果有人想对区块链添加审核，也实现不了，因为它的设计目标就是防止出现居于中心地位的管理当局。

正是因为无法管理，区块链才能做到无法被控制。否则一旦大公司大集团控制了管理权，他们就会控制整个平台，其他使用者就都必须听命于他们了。

但是，没有了管理员，人人都可以往里面写入数据，怎么才能保证数据是可信的呢？被坏人改了怎么办？请接着往下读，这就是区块链奇妙的地方。

三、区块

区块链由一个个区块（block）组成。区块很像数据库的记录，每次写入数据，就是创建一个区块。



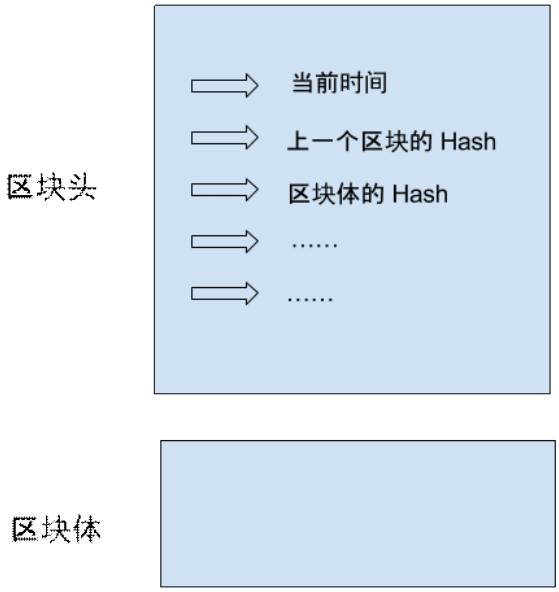
每个区块包含两个部分。

- 区块头（Head）：记录当前区块的元信息
- 区块体（Body）：实际数据

区块头包含了当前区块的多项元信息。

- 生成时间
- 实际数据（即区块体）的 Hash
- 上一个区块的 Hash
- ...

这里，你需要理解什么叫hash，这是理解区块链必需的。



所谓 Hash 就是计算机可以对任意内容，计算出一个长度相同的特征值。区块链的 Hash 长度是256位，这就是说，不管原始内容是什么，最后都会计算出一个256位的二进制数字。而且可以保证，只要原始内容不同，对应的 Hash 一定是不同的。

举例来说，字符串123的 Hash 是a8fdc205a9f19cc1c7507a60c4f01b13d11d7fd0（十六进制），转成二进制就是256位，而且只有123能得到这个 Hash。

因此，就有两个重要的推论。

- 推论1：每个区块的 Hash 都是不一样的，可以通过 Hash 标识区块。
- 推论2：如果区块的内容变了，它的 Hash 一定会改变。

四、 Hash 的不可修改性

区块与 Hash 是一一对应的，每个区块的 Hash 都是针对"区块头"（Head）计算的。

Hash = SHA256(区块头)

上面就是区块 Hash 的计算公式，Hash 由区块头唯一决定，SHA256是区块链的 Hash 算法。

前面说过，区块头包含很多内容，其中有当前区块体的 Hash（注意是"区块体"的 Hash，而不是整个区块），还有上一个区块的 Hash。这意味着，如果当前区块的内容变了，或者上一个区块的 Hash 变了，一定会引起当前区块的 Hash 改变。

这一点对区块链有重大意义。如果有人修改了一个区块，该区块的 Hash 就变了。为了让后面的区块还能连到它，该人必须同时修改后面所有的区块，否则被改掉的区块就脱离区块链了。由于后面要提到的原因，Hash 的计算很耗时，同时修改多个区块几乎不可能发生，除非有人掌握了全网51%以上的计算能力。

正是通过这种联动机制，区块链保证了自身的可靠性，数据一旦写入，就无法被篡改。这就像历史一样，发生了就是发生了，从此再无法改变。

每个区块都连着上一个区块，这也是"区块链"这个名字的由来。

五、采矿

由于必须保证节点之间的同步，所以新区块的添加速度不能太快。试想一下，你刚刚同步了一个区块，准备基于它生成下一个区块，但这时别的节点又有新区块生成，你不得不放弃做了一半的计算，再次去同步。因为每个区块的后面，只能跟着一个区块，你永远只能在最新区块的后面，生成下一个区块。所以，你别无选择，一听到信号，就必须立刻同步。

所以，区块链的发明者中本聪（这是假名，真实身份至今未知）故意让添加新区块，变得很困难。他的设计是，平均每10分钟，全网才能生成一个新区块，一小时也就六个。

这种产出速度不是通过命令达成的，而是故意设置了海量的计算。也就是说，只有通过极其大量的计算，才能得到当前区块的有效 Hash，从而把新区块添加到区块链。由于计算量太大，所以快不起来。

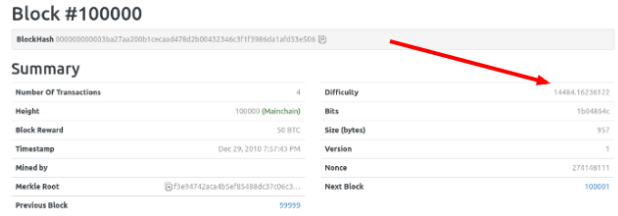
这个过程就叫做采矿（mining），因为计算有效 Hash 的难度，好比在全世界的沙子里面，找到一粒符合条件的沙子。计算 Hash 的机器就叫做矿机，操作矿机的人就叫做矿工。

六、难度系数

读到这里，你可能会有一个疑问，人们都说采矿很难，可是采矿不就是用计算机算出一个 Hash 吗，这正是计算机的强项啊，怎么会变得很难，迟迟算不出来呢？

原来不是任意一个 Hash 都可以，只有满足条件的 Hash 才会被区块链接受。这个条件特别苛刻，使得绝大部分 Hash 都不满足要求，必须重算。

原来，区块头包含一个难度系数（difficulty），这个值决定了计算 Hash 的难度。举例来说，第100000个区块的难度系数是 14484.16236122。



区块链协议规定，使用一个常量除以难度系数，可以得到目标值（target）。显然，难度系数越大，目标值就越小。

```
target = targetmax / difficulty
```

```
targetmax = 0x00000000FFFF0000000000000000000000000000000000000000000000000000
difficulty = 14484.162361
```

Hash 的有效性跟目标值密切相关，只有小于目标值的 Hash 才是有效的，否则 Hash 无效，必须重算。由于目标值非常小，Hash 小于该值的机会极其渺茫，可能计算10亿次，才算中一次。这就是采矿如此之慢的根本原因。

区块头里面还有一个 Nonce 值，记录了 Hash 重算的次数。第 100000 个区块的 Nonce 值是274148111，即计算了 2.74 亿次，才得到了一个有效的 Hash，该区块才能加入区块链。

七、难度系数的动态调节

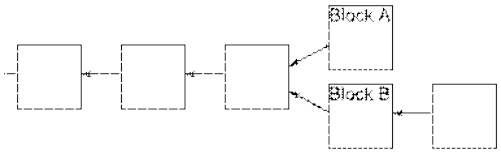
就算采矿很难，但也没法保证，正好十分钟产出一个区块，有时一分钟就算出来了，有时几个小时可能也没结果。总体来看，随着硬件设备的提升，以及矿机的数量增长，计算速度一定会越来越快。

为了将产出速率恒定在十分钟，中本聪还设计了难度系数的动态调节机制。他规定，难度系数每两周（2016个区块）调整一次。如果这两周里面，区块的平均生成速度是9分钟，就意味着比法定速度快了10%，因此难度系数就要调高10%；如果平均生成速度是11分钟，就意味着比法定速度慢了10%，因此难度系数就要调低10%。

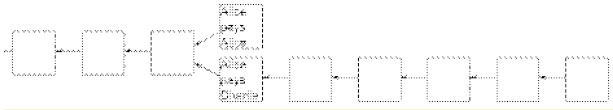
难度系数越调越高（目标值越来越小），导致了采矿越来越难。

八、区块链的分叉

即使区块链是可靠的，现在还有一个问题没有解决：如果两个人同时向区块链写入数据，也就是说，同时有两个区块加入，因为它们都连着前一个区块，就形成了分叉。这时应该采纳哪一个区块呢？



现在的规则是，新节点总是采用最长的那条区块链。如果区块链有分叉，将看哪个分支在分叉点后面，先达到6个新区块（称为"六次确认"）。按照10分钟一个区块计算，一小时就可以确认。



由于新区块的生成速度由计算能力决定，所以这条规则就是说，拥有大多数计算能力的那条分支，就是正宗的比特链。

九、总结

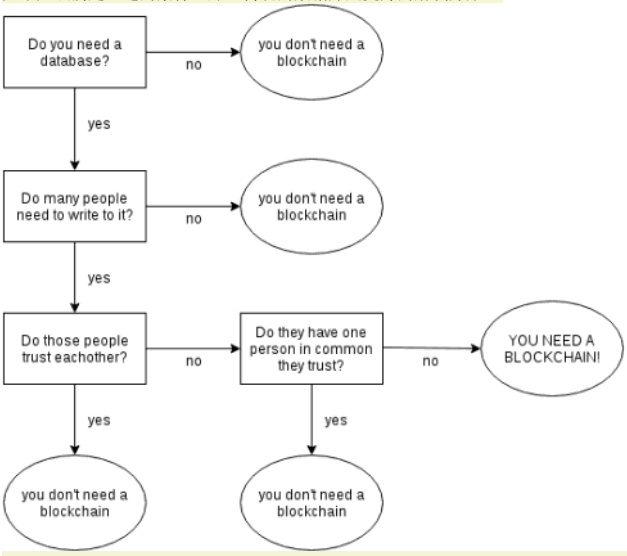
区块链作为无人管理的分布式数据库，从2009年开始已经运行了8年，没有出现大的问题。这证明它是可行的。

但是，为了保证数据的可靠性，区块链也有自己的代价。一是效率，数据写入区块链，最少要等待十分钟，所有节点都同步数据，则需要更多的时间；二是能耗，区块的生成需要矿工进行无数无意义的计算，这是非常耗费能源的。

因此，区块链的适用场景，其实非常有限。

1. 不存在所有成员都信任的管理当局
2. 写入的数据不要求实时使用
3. 挖矿的收益能够弥补本身的成本

如果无法满足上述的条件，那么传统的数据库是更好的解决方案。



目前，区块链最大的应用场景（可能也是唯一的应用场景），就是以比特币为代表的加密货币。

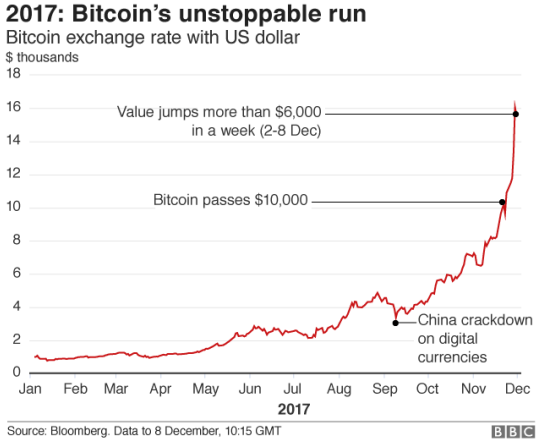
比特币

2018年2月8日　16:18

比特币（bitcoin）诞生于2008年的一篇论文。

一个署名为中本聪的人，提出了革命性的构想：让我们创造一种不受政府或其他任何人控制的货币！这个想法堪称疯狂：一串数字，背后没有任何资产支持，也没有任何人负责，你把它当作钱付给对方，怎么会有人愿意接受？

但是，狂想居然变成了现实。随后的几年，在全世界无数爱好者的支持下，比特币网络运行起来了，越来越多的人和资本参与，星星之火，终成燎原。刚刚过去的2017年，比特币迎来了爆发式的增长，从年初的1000美元，最高涨到了2万美元，全世界都为之震动，上到政府，下到普通百姓都在关注。事实就是比特币已经并将继续改变世界。



新闻媒体往往只关注它的火爆表现，忽视或者无法回答一些基本的问题。

- 比特币的原理是什么？
- 为什么这个无人管理的体系可以成功运作？
- 比特币交易的流程是怎么回事？
- 它与区块链又是什么关系？

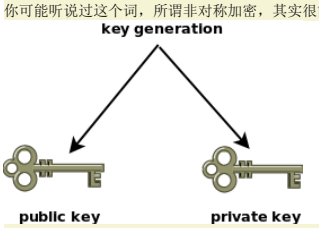
下面，我尝试回答这些问题，希望帮助大家理解比特币。抛开技术细节，还是很容易解释的。

有一点说明，本文只讨论技术问题，不涉及如何投资比特币，更不会预测价格走势。事实上，我也不知道，如果我知道怎么发财，可能就不会在这里写博客了。

一、非对称加密

首先，理解比特币，必须理解非对称加密。

你可能听说过这个词，所谓非对称加密，其实很简单，就是加密和解密需要两把钥匙：一把公钥和一把私钥。



公钥是公开的，任何人都可以获取。私钥是保密的，只有拥有者才能使用。他人使用你的公钥加密信息，然后发送给你，你用私钥解密，取出信息。反过来，你也可以用私钥加密信息，别人用你的公钥解开，从而证明这个信息确实是你发出的，且未被篡改，这叫做数字签名

现在请设想，**如果公钥加密的不是普通的信息，而是加密了一笔钱，发送给你，这会怎样？**

首先，你能解开加密包，取出里面的钱，因为私钥在你手里。其次，别人偷不走这笔钱，因为他们没有你的私钥。因此，支付可以成功。

这就是比特币（以及其他数字货币）的原理：非对称加密保证了支付的可靠性。

由于支付的钱必须通过私钥取出，所以你是谁并不重要，重要的是谁拥有私钥。只有拥有了私钥，才能取出支付给你的钱。（事实上，真实的交易流程稍有不同，私钥保证的不是取出支付给你的钱，而是保证只有你能把这些属于你的钱支付出去，详见后文。）

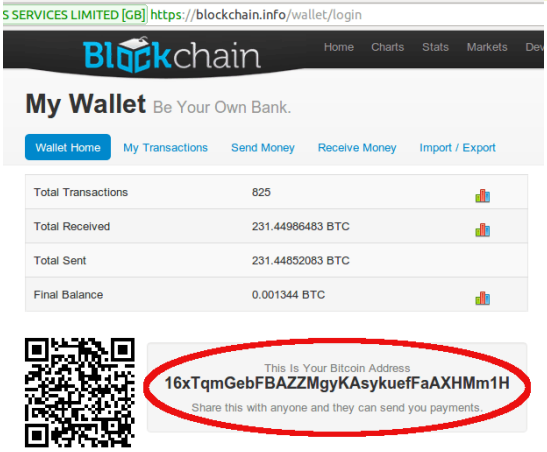
二、比特币钱包

对于比特币来说，钱不是支付给个人的，而是支付给某一把私钥。这就是交易匿名性的根本原因，因为没有人知道，那些私钥背后的主人是谁。

所以，**比特币交易的第一件事，就是你必须拥有自己的公钥和私钥。**

你去网上那些比特币交易所开户，它们会让你首先生成一个比特币钱包（wallet）。**这个钱包不是用来存放比特币，而是存放你的公钥和私钥。**软件会帮你生成这两把钥匙，然后放在钱包里面。

根据协议，公钥的长度是512位。这个长度不太方便传播，因此协议又规定，要为公钥生成一个160位的指纹。所谓指纹，就是一个比较短的、易于传播的哈希值。160位是二进制，写成十六进制，大约是26到35个字符，比如1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2。这个字符串就叫做钱包的地址，它是唯一的，即每个钱包的地址肯定都是不一样的。



你向别人收钱时，只要告诉对方你的钱包地址即可，对方向这个地址付款。由于你是这个地址的拥有者，所以你会收到这笔钱。

由于你是否拥有某个钱包地址，是由私钥证明的（具体的证明方法稍后介绍），所以一定要保护好私钥。这是极其重要的，如果你的私钥被偷了，你的比特币也就等于没了，因为他人可以冒用你的身份了，把钱包里面的钱都转走。

同样的，你向他人支付比特币，千万不能写错他人的钱包地址，否则你的比特币就支付到了另一个不同的人了。

三、交易过程

下面，我把整个流程串起来，看看比特币如何完成一笔交易。

一笔交易就是一个地址的比特币，转移到另一个地址。由于比特币的交易记录全部都是公开的，哪个地址拥有多少比特币，都是可以查到的。因此，支付方是否拥有足够的比特币，完成这笔交易，这是可以轻易验证的。

问题出在怎么防止其他人，冒用你的名义申报交易。举例来说，有人申报了一笔交易：地址 A 向地址 B 支付10个比特币。我怎么知道这个申报是真的，申报人就是地址 A 的主人？

比特币协议规定，申报交易的时候，除了交易金额，转出比特币的一方还必须提供以下数据。

- 上一笔交易的 Hash（你从哪里得到这些比特币）
- 本次交易双方的地址
- 支付方的公钥
- 支付方的私钥生成的数字签名

验证这笔交易是否属实，需要三步。

第一步，找到上一笔交易，确认支付方的比特币来源。

第二步，算出支付方公钥的指纹，确认与支付方的地址一致，从而保证公钥属实。

第三步，使用公钥去解开数字签名，保证私钥属实。

经过上面三步，就可以认定这笔交易是真实的。

四、交易确认与区块链

确认交易的真实性以后，交易还不算完成。**交易数据必须写入数据库，才算成立，对方才能真正收到钱。**

比特币使用的是一种特殊的数据库，叫做区块链（blockchain），本文只讨论交易如何写入区块链。

首先，所有的交易数据都会传送到矿工那里。矿工负责把这些交易写入区块链。

根据比特币协议，一个区块的大小最大是 1MB，而一笔交易大概是500字节左右，因此一个区块最多可以包含2000多笔交易。矿工负责把这2000多笔交易打包在一起，组成一个区块，然后计算这个区块的 Hash。

Number[2]	Hash[2]	Time[2]	Transactions[2]	Total BTC[2]	Size (kB)[2]
356987	141a6f95b2...	2015-05-18 13:28:14	1714	17353.00313324	749.227
356986	13cff723ec...	2015-05-18 13:11:53	2114	23805.24520712	749.204
356985	1128aa2601...	2015-05-18 12:27:49	594	6119.90095486	392.306
356984	140b0f27b9...	2015-05-18 12:20:14	1087	7849.33374079	544.102
356983	d1ea5bc1c7...	2015-05-18 12:08:01	830	7799.27270534	455.006
356982	76634b52be...	2015-05-18 11:58:42	221	1706.08443753	152.745
356981	ab5a643167...	2015-05-18 11:57:28	756	7245.57902445	372.38
356980	b780d34ab0...	2015-05-18 11:46:36	383	4623.1382688	430.319
356979	110a166e82...	2015-05-18 11:41:08	2276	19539.64880577	999.931

计算 Hash 的过程叫做采矿，这需要大量的计算。矿工之间也在竞争，谁先算出 Hash，谁就能第一个添加新区块进入区块链，从而享受这个区块的全部收益，而其他矿工将一无所获。

一笔交易一旦写入了区块链，就无法反悔了。这里需要建立一个观念：**比特币不存放在钱包或其他别的地方，而是只存在于区块链上面。**区块链记载了你参与的每一笔交易，你得到过多少比特币，你又支付了多少比特币，

因此可以算出来你拥有多少资产。

五、矿工的收益

交易的确认离不开矿工。为什么有人愿意做矿工呢？

比特币协议规定，挖到新区块的矿工将获得奖励，一开始（2008年）是50个比特币，然后每4年减半，目前（2018年）是12.5个比特币。这也是比特币的供给增加机制，流通中新增的比特币都是这样诞生的。

你可能看出来了，每4年奖励减半，那么到了2140年，矿工将得不到任何奖励，比特币的数量也将停止增加。这时，矿工的收益就完全依靠交易手续费了。

所谓交易手续费，就是矿工可以从每笔交易抽成，具体的金额由支付方自愿决定。你完全可以一毛不拔，一分钱也不给矿工，但是那样的话，你的交易就会没人处理，迟迟无法写入区块链，得到确认。矿工们总是优先处理手续费最高的交易。

目前由于交易数量猛增，手续费已经水涨船高，一个区块2000多笔交易的手续费总额可以达到3～10个比特币。如果你的手续费给低了，很可能过了一个星期，交易还没确认。

一个区块的奖励金12.5个比特币，再加上手续费，收益是相当可观的。按照目前的价格，可以达到100万～200万人民币。想想看，运气好的话，几分钟就能挖到一个区块，拿到这样一大笔钱，怪不得人们对挖矿趋之若鹜。

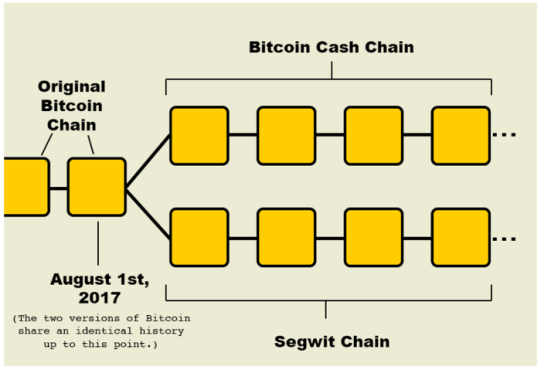
六、区块的扩容

，比特币协议规定，平均10分钟诞生一个区块。区块的大小只有 1MB，最多只能包含2000多笔交易。也就是说，比特币网络每10分钟，最多只能处理2000多笔交易，换算一下，就是处理速度为3～5笔/秒。

全世界的比特币交易这么多，可是区块链每秒最多只能处理5笔，这已经成为制约比特币发展的一个瓶颈。

很早就有人呼吁，改革比特币协议，提升处理速度。这件事在2017年8月有了一点眉目，当时区块链发生了一次分叉，诞生了一个新协议，称为 Bitcoin Cash（简称 BCH）。这种新货币其他方面都与比特币一致，就是每个区块的大小从 1MB 增加到了 8MB，因此处理速度提升了8倍，手续费也低得多。该协议是对原有区块链的分叉，因此当时持有比特币的人，等于一人获赠了一份同样数量的 BCH。

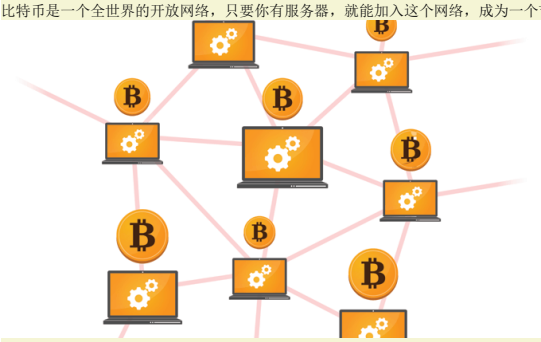
DIAGRAM OF THE BITCOIN CASH FORK



BCH 等于创造了一种新货币，还有人提议，原始比特币的区块大小提升到 2MB，。这个建议原定于2017年11月实施，但是最后一刻由于缺乏共识，就被取消了，目前还在讨论中。

七、点对点网络

比特币是一个全世界的开放网络，只要你有服务器，就能加入这个网络，成为一个节点。每个节点都包含了整个区块链（目前大概 100多 GB），并且节点之间时刻不停地在同步信息。



当你发生了一笔支付，你所在的节点就会把这笔交易告诉另一个节点，直至传遍整个网络。矿工从网上收集各种新发生的交易，将它们打包写入区块链。一旦写入成功， 矿工所在节点的区块链，就成为最新版本，其他节点都会来复制新增的区块，保证全网的区块链都是一致的。

最后，你所在的节点也拿到了最新的区块链，从而得知你早先的那笔交易，已经写在里面了，至此交易确认成功。

八、还有一个问题

写到这里，我就介绍完了比特币的基本知识，希望你已经明白了比特币是怎么回事。但是还有一个根本的问题，我没有回答：比特币的本质到底是什么？

说到底，比特币只是区块链的一条记录，是凭空生成的，为什么可以当钱用？举例来说，矿工获得12.5个比特币的奖励，其实就是区块链有一个记录："xxx地址获得12.5个比特币"。正是这行记录，导致该矿工获得了大笔金钱。如果区块链突然增加了一条记录，记载你的地址获得了1000个比特币，你就真的会有1000个比特币。这到底是为什么？

比特币为啥可以相信

2018年2月8日 16:19

很多人都在问，加密货币（cryptocurrency）的时代，真的来临了吗？将来会不会人类不再使用美元、人民币，改用加密货币？那么多品种，我应该使用哪一种币？要不要现在就去投资一些？

这些问题的答案，我也想知道，就花了很多时间查阅资料、研究协议。下面就是我对这个问题的思考。阅读之前，如果你已经了解区块链和比特币，那很好；如果不了解，也没关系，本文不涉及技术，只讨论最基本的原理。

一、钱是什么？

我们都知道，人民币是钱，美元是钱，金银财宝是钱。我问一个问题，它们为什么能成为钱？

你可能回答，因为它们有价值，或者是价值的代表。但是，有价值的东西多了，为什么只有这些品种成为了钱？

答案很容易想到，因为人们普遍相信（认同）它们的价值，其他东西的价值难以得到普通认同，无法成为钱。比如，邮票的价值就没有普遍的认同，除了集邮爱好者，其他地方都不能当钱用。一般来说，认同的人越多，这种钱的通用性就越高。

我曾经去俄罗斯旅行，当地货币是卢布。可是，一旦离开俄国，没人相信它的购买力，所以卢布离开俄国就没用了。相反，全世界人民都相信美元的价值，所以全世界都能用。我用美元付账的时候，我发现那些俄国人都很满意。

所以，**钱的本质，或者说货币的本质，就是它的可信性。**它必须使人们相信，它是有价值的，然后才能成为钱，才能被收藏和支付。

二、可信性

为什么钱必须是可信的？因为对方必须相信它的价值，否则你没法支付出去。那么，接下来的问题就是，可信的东西是否就是钱？

我的回答是 Yes。**一样东西能否成为钱，只取决于人们是否相信它的价值，至于它是不是真的有价值，根本不重要。**

如果马云在一张纸条上写"这张纸条价值10000元"，下面签了他的名，并且附上防伪标记。你说这纸条是钱吗？我跟你保证，这就是钱，你用来支付，人们都会接受，马云等同于发行了一种新的纸币。

比特币也是如此，它是什么，其实不太重要。重要的是，它必须保证自己是可信的，这样才能让足够的人相信它的价值，然后才能成为钱。

三、比特币的可信性

比特币要解决的核心问题，就是创造一种可信的数字凭证。由于这种凭证可信，所以能够当做货币。

比特币的技术基础是加密学，因为只有加密学才能保证它的可信性。一旦加密被破解，它就没法当作货币了。这也是这一类数字凭证被称为"加密货币"的原因。

技术人员对比特币感兴趣，还有一个重要原因。任何需要可靠的数字凭证的场合，也许都可以用到这种技术。

四、比特币的特点

比特币有三个特点，就是因为做到了这三点，所以它可信，能够当作钱。

首先，它不会被（轻易）偷走。或者反过来说，它使得你无法去偷别人，你只能花你自己的钱。因为必须要有别人的私钥，才能取出他的钱。正常情况下，你拿不到别人的私钥。

其次，它无法伪造。每一个比特币都能追溯来源，而所有比特币都来源于矿工获得的奖励。矿工只有新建区块，才能获得奖励，这是很难的事情，所以无法伪造比特币。

最后，它无法大批生成。原因跟上一条一样，比特币的发行速度是稳定的，现在每10分钟新增12.5个，然后每四年减半，最终停止增长。因此不会像纸币那样，政府滥发导致通货膨胀。

五、比特币有实体吗？

由于后面要提到的原因，比特币不可能拥有实体，没法做到"从口袋里掏出一个币"这种场景，交易都必须通过互联网完成。

你可能会说，钱都有实体，怎么可能存在无形的钱呢？答案正好相反，**钱就应该是无形的，那些实体的钱其实是对物质材料的浪费，由于技术不够发达，不得不做成实体。**

我小时候买东西，都必须用现金，否则没法证明，自己拥有购买力。只有通过实体的钱，才能保证对方确实收到了钱。如果银行业发达，就不用现金了，可以使用银行卡。支付的时候，对方抄一下银行卡号码，查询银行"这个账户有钱吗"。银行回答有钱，OK，成交。

但是，互联网使得实体的银行卡也不需要了。如果存在一个开放的中央记账系统，任何人都可以查询，你把钱划到老板的账户，老板查询一下，发现收到了，交易自动成交，整个过程都是无形的，还需要什么银行卡呢？

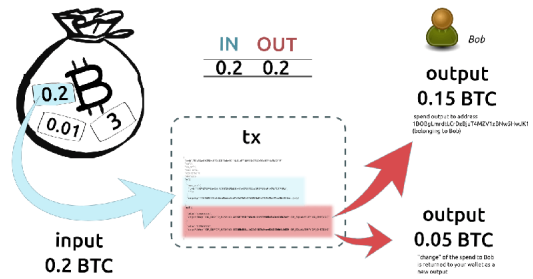
这个中央记账系统已经实现了，就叫做区块链。

六、区块链的作用

区块链就是一个数据库，记载了所有的交易，用作中央记账系统。

每笔交易的核心，就是一句话，比如"张三向李四转移了1个比特币"。为了证明这句话可信，张三为它加上了数字签名。任何人都可以用张三的公钥，证明这确实是张三本人的行为。另一方面，其他人无法伪造张三的数字签名，所以不可能伪造这笔交易。

矿工们收到这句话，首先验证数字签名的可信性，然后验证张三确实拥有这些比特币（每一笔交易都有上一笔交易的编号，用来查询比特币的来源）。验证通过以后，就着手把这句话写入区块链了。一旦写入区块链，所有人就都可以查询到，因此这笔比特币就被认为，从张三转移到了李四。



区块链的作用就是把这句话永久保存下来了，让任何人都可以查看，并且任何人（包括张三本人在内）都无法再修改了。

货币是什么？其实就是这句话。这一句话就完成了一次支付。我们平时用人民币支付，其实只是用纸币表达这条信息。如果每个人都可以实时写入/读取中央记账系统（区块链），那么完全可以不携带货币。

七、双重支出

前面说过，交易不可能被伪造。但是，由于每一笔交易都是一串二进制信号，因此可能被复制。举例来说，"张三向李四转移了1个比特币"这句话，可能被其他人复制，也可能被张三自己复制，提交到区块链。

如果这句话被两次写入区块链，就意味着张三可以把同一笔钱花掉两次。但是，第二次写入的时候，查询区块链可以发现张三已经把这笔钱花掉了，从而认定这是不合法的交易，不能写入区块链。因此，复制交易是不可能的。

比较麻烦的是另一种情况，就是张三把同一笔钱付给两个人。他先向区块链提交一个交易"张三向李四转移了1个比特币"，然后又提交了另一个交易"张三向王五转移了1个比特币"。这两个交易都可能被认为是真实的交易，从而进入区块链。因此，必须有办法防止出现这种情况。

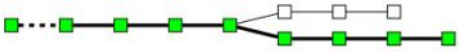
情况一：同一个矿工收到了这两个交易。那么他会察觉到，它们不可能同时成立，因此选择其中的一笔写入区块链。

情况二：矿工 A 收到了第一笔交易，矿工 B 收到了第二笔交易，他们各自都会认定这是合法的交易，分别把这两笔交易写入了两个区块，这时区块链就出现了分叉。

(a) Initial state of the blockchain in which all transactions are considered as valid.

(b) Honest nodes continue extending the valid chain by putting yellow blocks, while the attacker secretly starts mining a fraudulent branch.

(c) The attacker succeeds in making the fraudulent branch longer than the honest one.



(d) The attacker's branch is published and is now considered the valid one.

比特币协议规定，分叉点之后最先达到6个区块的那个分支，被认定为正式的区块链，其他分支都将被放弃。由于区块的生成速度由计算能力决定，所以到底哪一笔交易最后会被写入区块链，完全由它所在的分支能吸引多少计算能力决定。**隐藏的逻辑是，如果大多数人（计算能力）选择相信某一笔交易，那么它就应该是真的。**

综上所述，双重支出不可能发生。因为中央记账系统总有办法发现，你把同一笔钱花了两遍。但是，这也说明了比特币的一个代价，就是交易不能实时确认，必须等待至少一个小时。