2017年是比特币爆发的一年。在跳水了这么多年之后，比特币的价格突然从1000美元左右飙升到了近2万美元。有多少人变成了&quot密码学货币交易专家&quot。

赶上好的时候真的可以发大财，但是醒醒吧，盛宴结束了。

-2013年10月-2018年10月比特币价格走势图(来源：coinmarketcap.com)-

虽然主要原因人&#039；肾上腺素激增的是迅速上升的市值。但这波热潮最初是由技术掀起的。区块链技术还是有很大潜力的。现在是商业开发者，企业家和个人爱好者热情上车的时候了。但是，除了热血澎湃之外，我们首先要提高对区块链技术的认识。

遗憾的是，目前关于区块链技术的文章要么涉及太多复杂的专业术语，要么过于肤浅，缺乏深度。这两种类型的文章都不方便读者清楚地理解文章的内容。我们做什么呢建议你从下面这篇文章开始。只需要10分钟你可以理解为什么区块链技术如此具有颠覆性。它&#039；这次花钱还是值得的。祝你阅读愉快。

首先，区块链是一种电子数据的存储方式。数据以块的形式存在。假设有许多存储数字化数据的块。

这些块都是链接在一起的，这就赋予了它们内部数据的不变性。当一个数据块被链接到这个链时，它的内部数据就不能再被改变。

一旦块被添加到链中，其中的数据对任何人都是公开可见的。。这项技术具有非凡的创新意义，可以用来记录几乎所有我们能想到的数据(例如，产权、身份、余额、病历等。)，而且没有被篡改的风险。假设我买了一套房子，把产权证上传到区块链。我可以证明当时我享有这个房产的所有权。

这些信息一旦上线，谁也改不了(嗯，还是有办法改的。这里有一本进阶读物，建议你以后再看)。

因此，区块链是一种存储数据并确保数据不被篡改的方法。

听起来不错，但随之而来的问题是：我们是如何实现这项技术的？嗯，让我们&#039；让我们以比特币区块链为例。。比特币区块链是现存最古老的区块链。在比特币区块链上，每个区块的大小约为1MB。截止到截稿时，该链中已经累积了525，000个块，链中存储的数据总量约为525，000MB。。(校对注：其实离525,000M

B还远着呢，因为早期很多块都没有填满1MB。另外，截止到今天(2019年4月24日[XY002][XY001]，已经累计57.3万块，总数据量约250GB。。)

比特币区块链只存储比特币的交易数据。它就像一个巨大的交易记录库，可以追溯到第一笔比特币交易。在本文中，我们假设有一个存储交易数据的区块链，就像比特币区块链一样。

假设有三个块存储事务数据(如图1所示)。

这三个区块内都存有一些交易数据。它&#039；没什么特别的。它&#039；就像三个独立的word文档，描述交易的内容和余额的变化。文档1将从第一笔交易开始按时间顺序记录，直到数据量达到1MB，后续交易将记录在文档2中。直到数据量达到1MB，以此类推。这些文档是数据块。它们一个接一个地连接在一起。为此，每个块将根据其内部数据串生成一个特殊的(数字)签名。如果该块中的数据有任何变化，即使只改变一个数，这个块的签名也会改变。这是如何实现的？详细内容请阅读步骤3中的哈希运算部分。

(校对注：如上所述，实际情况中并不是所有的块都接近块大小的上限。实际的数据大小取决于打包区块并链接区块的矿工在区块中记录了多少事务，他们不会等到有1MB的事务数据才开始工作。实际情况见下文)

假设block1中记录了两笔交易。，分别是事务1和事务2。这两个事务的总数据量达到了1MB(其实一个块中的事务更多)。将根据该块中的数据串生成签名。假设这个签名是&quotX32&quot。如下图所示：

请记住即使存储在block1中的数据改变了一个数字，也会得到一个完全不同的签名！只要将块1的签名添加到块2，块1的数据就可以与块2相关联。。块1的签名也包含在块2的数据串中，所以这个签名和块2中的其他数据一样，成为块2的签名的数据基础。如下图所示：

正是这些签名将区块链接在了一起，形成一个区块链。现在添加block3，整个链条如下图所示：

现在假设块1中的数据已经被改变。例如，达米安和乔治之间的交易被更改了。达米安寄给乔治500个比特币，而不是100个。。由于块1中的数据串已经改变，其签

名也相应地改变。更改数据后，块1的签名不再是&quotX32&quot但是&quotW10&quot，如下图所示：

。

-请访问R/区块链查看更多关于区块链的科普知识-

结果新签名&quotW10&quot块1的与旧签名&quotX32&quot添加到块2的数据串中。。块1和块2之间的链接断开。该链中的其他用户将知道块1中的数据已被更改。为了保持区块链的不变性，其他用户将拒绝同步已更改的交易信息。原始交易记录(即达米安向乔治发送100BTC)保持不变，整个链条保持完整。这意味着如果您想要篡改交易而不显示痕迹，块2的数据串中的块1的旧签名必须用新签名替换。然而，一旦块2中的数据串改变，块2的签名也将改变。假设块2的签名从&quot9BZ&quot到&quotPP4&quot。。然后2块和3块的联系就断了！

区块链上的区块对所有人都是可见的。因此，如果篡改者真的想篡改交易而不露出任何痕迹，就必须保证所有被篡改的块仍然是连通的(否则，人们很容易发现哪个块没有与其他块连通，进而判断该块被更改过)。换句话说要改变一个块，必须为所有后续块计算新的签名。可以认为这几乎是不可能的，但是要理解为什么，请看下文。

所以，让&#039；下面以区块1为例再画一个示意图。假设在块1中只记录了一笔交易。也就是说，多马将100个BTC送给大卫。需要从该数据串中生成签名。在区块链上，该签名由加密哈希函数生成。。加密哈希函数是一个极其复杂的数学公式：将任意数据串作为输入值代入公式，即可得到唯一的64位输出值。例如，你可以用单词&quot京乐铃&quot到这个哈希函数中(哈希函数有很多种。，这只是一个例子)，输出是：

只要这个输入中的一个字符发生变化，包括改变大小写或者添加空格和标点符号，就会得到完全不同的输出。。如果您在此输入后添加一个句点，它将变成&quot京乐贝尔。"输出变成：

如果去掉句点，我们仍然可以得到和以前一样的输入：

对于同一个加密哈希函数，同样的输入一定会得到同样的输出，不同的输入一定会得到不同的输出。比特币区块链使用哈希函数为区块生成签名。将块中的数据作为输入，输出是块的签名。。让&#039；让我们看一下只有一个交易的块1的示意图(托马斯向大卫发送100个BTC)。

假设块1中的数据串如下：

块1Thomas-100David100

将这个数据串输入hash函数，得到的输出(签名)如下：

。

该签名将被添加到块2。假设大卫现在向吉米转账100BTC，这笔交易打包到区块2。然后就是如下图所示：

区块 2 的数据串如下所示：

将这个数据串输入hash函数，输出(签名)如下：

这是block2的签名。每个块将通过这个加密散列函数生成一个数字签名。哈希函数有很多种。比特币区块链使用SHA-256哈希算法。

但是，(以上措施显然不够)如果有人想篡改一个块中的数据，ta可以在篡改后生成一个新的签名，插入下一个块中，然后逐块生成新的签名。这些被修改的块仍然形成一个链，所以其他的可以&#039；我看不出数据被修改了。如何防止这种情况？

答案是，区块链只接受满足特定要求的哈希值(签名)。这是第四阶段介绍的采矿。

并非所有签名都符合要求。《区块链议定书》将预先确定一些要求。比如在比特币区块链上，只能上传数字签名连续零对应的区块。例如，只有当数字签名以不少于10个连续的零开始时。可以缠绕相应的块。

然而，根据第三部分，对应于每个数据串的散列值是唯一的。如果数据块的签名(哈希值)以少于10个零开头会怎样？为了获得合格的分组签名，需要反复改变输入数据串。直到你能生成一个以10个连续的零开始的签名。但是，因为事务数据和元数据(块号、时间戳等。)需要保持不变(否则，意义会变)，在每个块中加入特定长度的可以改变的数据。。当你想在链上添加一个块的时候，人们可以不断地改变这个数据块，直到找到一个合格的签名，然后确定这个数据块的具体值。该数据是块的随机数。Nonce不是预先确定的数据。，而是根据实际需要找到的一系列完全随机的数(注：图中所示的其他数据可以由任意字符组成，nonce只能由数字组成)。

总结一下。该块包含：1)交易数据；2)前一个块的签名；3)现时.这种反复更改nonce、散列块数据并找到合格签名的过程称为挖掘，这就是矿工所做的事情。矿工投入大量电力。，转化为计算能力，不断代入nonce进行哈希运算，直到找到合格的签名(输出)。挖掘者的计算能力越强，哈希运算的速度就越快，首先找到合格签名的可能性就越高。这是一个试错的过程，如下图所示：

-注意：nonce必须是一个数字(具体请阅读r/BlockchainSchool上的解释)-

区块链网络上的任何用户都可以通过下载并启动挖矿软件参与挖矿。事实上，这是使用他们的硬件计算能力来计算块的随机数。以比特币区块链上的#521477区块为例：

-从区块链浏览器blockchain.com-

可以看出，这个块的hash值(签名)和前一个块的hash值都是以相同数量的0开头的。找到这样的哈希值并不容易。需要很大的计算能力和时间，或者运气爆棚。

是的，有时候幸运的矿工可以在几分钟内计算出合格的签名，而且几乎不需要计算能力。523034号地块是一个极其罕见的例子。

一个没什么计算能力的小矿工很快找到了一个合格的签名，其他矿工的计算能力加起来是他的7万亿倍。相比之下，赢得强力球彩票头奖的概率是2.92亿分之一。而这个幸运儿挖到矿的概率是一等奖的1/24000。唐&#039；不要低估这些零。这一节的重点是很难找到合格的签名。

如三阶所述，改变一个区块会导致其签名改变。与后续块的记录不匹配，因此断开了与后续块的链接。为了使网络中的其他参与者接受这个改变的块，有必要将其与后面的块重新链接。也就是说，如果一个块的签名发生变化，它后面的所有块的签名都会发生变化。为了让别人觉得这是一个一致的链条。你还记得什么吗？

如第四节所述，签名必须符合要求！虽然改变所有块的签名似乎是可行的，但这需要大量的成本和时间，因此被认为是不可能的。原因如下：

假设一个矿工恶意篡改了某个区块中的交易，然后根据哈希运算为这个区块及其后面的所有区块生成一个新的签名，使得网络中的其他参与者可以接受被篡改的交易。问题是网络中的其他矿工也在不断地为原始链上的新块计算签名。随着新块上线，邪恶矿工不得不重新计算这些块的签名。他必须确保所有块都链接在一起，包括

不断添加到链中的新块。。除非这个矿工的计算能力比全网其他人都强，否则永远赶不上其他矿工。

(校对注：这段话的实际意思是，只要矿工们在他们所见过的最长的区块链里挖掘，所有的计算能力都会随着时间的推移自然地汇聚到一条主链上。攻击者只有创建一个比当前主链更长的链，才能成功更改所有人都认可的交易记录。这个总是以最长的链为主链(有效链)的原理就是所谓的&quot最长链规则&quot，这是中本聪共识(中本聪共识机制)的一部分。此外，并非所有区块链都采纳了中本聪共识。)

如今有数百万用户在比特币区块链上挖矿由此可以推断，一个恶意参与者或实体的计算能力不可能超过整个网络的剩余计算能力。这意味着网络中的其他参与者不可能接受对区块链的任何修改，从而实现区块链的不变性。数据一旦添加到区块链中，就无法修改。

只有一个例外，就是恶意参与者的计算能力真的超过了全网其他人计算能力的总和。理论上，在这种情况下，可以篡改区块链(即改变大家公认的历史记录)。这被称为51%攻击(我写了另一篇文章来解释这种情况)，许多区块链在过去遭受过这种攻击。

(校对注：到目前为止，遭受51%攻击的著名区块链有bitGold、Verge和以太坊经典。)

事实上，对比特币区块链发起51%的攻击所获得的收益，与高昂的攻击成本相差甚远。。为了获得足够的计算能力，不仅要承担硬件、散热设备、存储空间的成本，还要承担被千人指责的风险。更重要的是，它会对被攻击的区块链的生态系统造成极大的破坏，攻击的收益也会大幅贬值。。51%的攻击实际上是针对区块链上的其他用户。这也是为什么参与挖掘的用户越多，整个链条的安全性就越高。

恭喜你，你又进入第一关了！现在你应该明白为什么(大)区块链被认为是不可变的。但现在有一个非常重要的问题：如何防止矿工在区块链中添加伪造的交易数据？从技术上讲，它&#039；这是不可能的。区块链交易的详细解释可以在以下文章中找到。。

(校对注：只有私钥的拥有者才能在对应的地址消费资金，矿工不&#039；你不知道你的私钥，别人只能通过你的公钥来验证交易是否是你发起的。所以伪造交易是不可行的)

.区块链协议自动以最长链上的交易记录为标准，将这个链视为代表绝大多数参与者

的链。构建最长的链条需要消耗全网的大部分计算能力。被篡改的块是从最长的链上断开的，所以会被全网大部分节点自动拒绝。

在比特币区块链上，所有交易历史和钱包余额都是公开可见的(blockchain.info)。任何人都可以查看任何钱包的余额，或者从第一笔交易(2009年1月3日)开始的所有交易记录。。虽然任何人都可以查询钱包余额，但这些钱包的主人大多不为人知。举个例子，一个钱包里有69000个比特币，在我写这篇文章的时候大约值5亿美元。这个钱包在2015年4月用过一次。之后一直没有交易。

(校对注：其实这部分没有回答问题&quot谁决定规则&quot，但只是粗略地说明&quot按照现有的规则，这项技术可以实现&quot。公链治理是一个复杂的问题。这也超出了下一篇文章的范围。)

加密货币本质上是比特币的变种。大多数加密货币都是根据自己的区块链协议构建的，遵循与比特币不同的规则。比特币应该归类为货币。换句话说，它显然具有货币职能。门罗币也是一种具有相同功能的加密货币，但其区块链协议也增加了一些增强隐私的规则(使追踪交易更加困难)。

然而区块链发行的资产可以被赋予许多不同的用途，这是由发行人决定的。如此发行的资产通常称为&quot代币&quot。这些代币可以赋予其所有者一定的权利，比如赌博执照、社交媒体渠道、水电等等。。所有这些资产交易都在不同的区块链进行记录，并可以通过Coin&#039安。

代币其实是一种新型的互联网货币，可能会影响到一些行业，典型的例子就是股票市场。在将来公司股份等财产权可能会以代币的形式存储在区块链中。区块链不局限于以代币的形式表示物理价值，还可以安全记录病历、身份、历史记录、税务记录等数据。这就是区块链科技的伟大之处。更不用说区块链的另一个重要特征：权力下放。

以上是《区块链入门》的详细内容：区块链入门7步。更多关于7步入门区块链的信息，请关注dadaqq.coM其他相关文章(www.dadaqq.coM)！

本站提醒投资有风险，入市需谨慎。此内容不作为投资理财建议。