比特币的信用基础区块链技术是一种巨大的技术突破，这种以P2P为基础的去中心化的新体系，它革新了互联网与金融产业，现在的比特币行业，只想当于1994年左右的互联网，还处于基础建议阶段，但未来十年，区块链有可能取代互联网。

# 第1章 区块链：前世今生

## 比特币

比特币（BitCoin）的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及建构其上的[P2P](http://baike.baidu.com/view/3280.htm)网络。比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的[分布式数据库](http://baike.baidu.com/view/68389.htm)来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节[安全性](http://baike.baidu.com/view/421194.htm)。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。比特币与其他[虚拟货币](http://baike.baidu.com/view/16260.htm)最大的不同，是其总数量非常有限，具有极强的稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个。

### 产生原理

从比特币的本质说起，比特币的本质其实就是一堆复杂算法所生成的特解。特解是指[方程组](http://baike.baidu.com/view/314172.htm)所能得到无限个（其实比特币是有限个）解中的一组。而每一个特解都能解开方程并且是唯一的。[8]  以人民币来比喻的话，比特币就是人民币的序列号，你知道了某张钞票上的序列号，你就拥有了这张钞票。而挖矿的过程就是通过庞大的计算量不断的去寻求这个方程组的特解，这个方程组被设计成了只有 2100 万个特解，所以比特币的上限就是 2100 万。

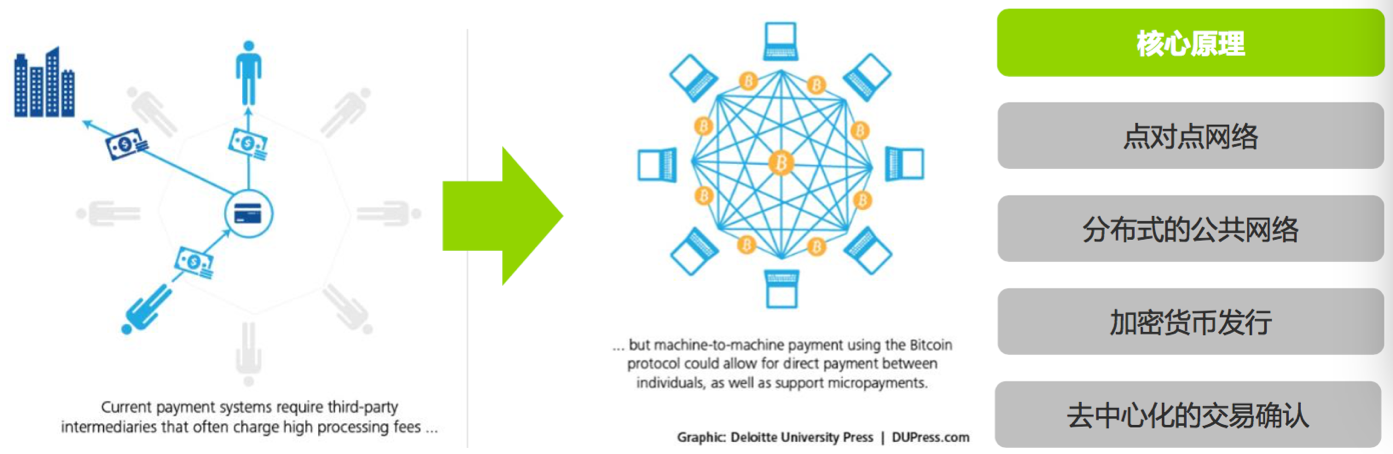
要挖掘比特币可以下载专用的比特币运算工具，然后注册各种合作网站，把注册来的用户名和密码填入计算程序中，再点击运算就正式开始。完成Bitcoin客户端安装后，可以直接获得一个Bitcoin地址，当别人付钱的时候，只需要自己把地址贴给别人，就能通过同样的客户端进行付款。在安装好比特币客户端后，它将会分配一个私有[密钥](http://baike.baidu.com/view/934.htm)和一个[公开密钥](http://baike.baidu.com/view/1145160.htm)。需要备份你包含私有密钥的钱包数据，才能保证财产不丢失。如果不幸完全格式化硬盘，个人的比特币将会完全丢失。

## 1.2 区块链是虾米？

说到区块链，大家自然会想到**比特币**。比特币是一种由开源的P2P软体产生的数字货币。比特币的概念最初由中本聪在2008年提出，与大多数货币不同的是，比特币不依赖于特定的中央发行机构，而是使用遍布整个P2P网络节点的去中心化的数据库来记录货币的交易，并使用密码学的设计来确保货币流通各个环节安全性。

那么**何为区块链**？区块链是一种去中心化的可信数据库，提供了一套安全稳定，透明，可审计且高效的记录交易以及数据信息交互方式。

* 高度安全，不可篡改的分布式账簿
* 存在于互联网，向所有用户公开
* 帮助人与人，物与物之间实现点对点的交易和互换
* 无需第三方的介入即可完成价值的交换



然而**区块链能干什么？**区块链可以存储数据，也可以运行应用程序。目前区块链技术主要应用在存在性证明、智能合约、物联网、身份验证、预测市场、资产交易、文件存储等领域。随着区块链技术的快速演变，新的性能在不断结合创造更有效的应用解决方案。



## 1.3 POW VS POS

POW（Proof of Work，工作证明）是指获得多少货币，取决于你挖矿贡献的工作量，电脑性能越好，分给你的矿就会越多。POS（Proof of Stake，股权证明）根据你持有货币的量和时间进行利息分配的制度，在POS模式下，你的“挖矿”收益正比于你的币龄，而与电脑的计算性能无关。POW、POS孰优孰劣？关于这个话题的讨论持久不息，也许基于两种设计理念的密码学货币将长期共存。

### 1.3.1 POW

为了在点对点的基础上构建一组分散化的时间戳服务器,仅仅像报纸或世界性新闻网络组 一样工作是不够的,我们还需要一个类似于亚当·柏克(Adam Back)提出的哈希现金(Hashcash) 6。在进行随机散列运算时,工作量证明机制引入了对某一个特定值的扫描工作,比方说 SHA-256 下,随机散列值以一个或多个 0 开始。那么随着 0 的数目的上升, 找到这个解所需要的工作量 将呈指数增长,但是检验结果仅需要一次随机散列运算。

我们在区块中补增一个随机数(Nonce),这个随机数要使得该给定区块的随机散列值出现 了所需的那么多个 0。我们通过反复尝试来找到这个随机数,找到为止。这样我们就构建了一 个工作量证明机制。只要该 CPU 耗费的工作量能够满足该工作量证明机制,那么除非重新完 成相当的工作量,该区块的信息就不可更改。由于之后的区块是链接在该区块之后的,所以想 要更改该区块中的信息,就还需要重新完成之后所有区块的全部工作量。

同时,该工作量证明机制还解决了在集体投票表决时,谁是大多数的问题。如果决定大多

数的方式是基于IP地址的,一IP地址一票,那么如果有人拥有分配大量IP地址的权力,则该机 制就被破坏了。而工作量证明机制的本质则是一CPU一票。“大多数”的决定表达为最长的链, 因为最长的链包含了最大的工作量。如果大多数的CPU为诚实的节点控制,那么诚实的链条 将以最快的速度延长,并超越其他的竞争链条。如果想要对业已出现的区块进行修改,攻击者 必须重新完成该区块的工作量外加该区块之后所有区块的工作量,并最终赶上和超越诚实节点 的工作量。我们将在后文证明,设想一个较慢的攻击者试图赶上随后的区块,那么其成功概率 将呈指数化递减。

另一个问题是,硬件的运算速度在高速增长,且节点参与网络的程度会有所起伏。为了解 决这个问题,工作量证明的难度(the proof-of-work difficulty)将采用移动平均目标的方法来确定, 即令难度指向令每小时生成区块的速度为某一预设的平均数。如果区块生成的速度过快,那么 难度就会提高。

### 1.3.2 POS

POS就是“股权证明”,Proof of stake，即直接证明你持有的份额。除了混合性的PPC之外，真正的POS币是没有挖矿过程的，也就是在创世区块内就写明了股权证明，之后的股权证明只能转让，不能挖矿。

在现实世界中股权证明很普遍，最简单的就是股票。股票是用来记录股权的证明，同时代表着投票权和收益权。股票被创造出来以后，除了增发外，不能增加股权数量，要获得股票只能转让。

在纯POS体系中，如NXT，没有挖矿过程，初始的股权分配已经固定，之后只是股权在交易者之中流转，非常类似于现实世界的股票。股权从创世区块中流出，被交易者买卖而逐渐分散化。

## 1.4 分叉问题

|  |
| --- |
| 因为区块链是去中心化的数据结构，所以不同副本之间不能总是保持一致。区块有可能在不同时间到达不同节点，导致节点有不同的区块链视角。解决的办法是，每一个节点总是选择并尝试延长代表累计了最大工作量证明的区块链，也就是最长的或最大累计难度的链。节点通过将记录在每个区块中的难度加总起来，得到建立这个链所要付出的工作量证明的总量。只要所有的节点选择最长累计难度的区块链，整个比特币网络最终会收敛到一致的状态。分叉即在不同区块链间发生的临时差异，当更多的区块添加到了某个分叉中，这个问题便会迎刃而解。  在下面的图例中，我们可以了解网络中发生分叉的过程。图例代表简单的全球比特币网络，在真实的情况下，比特币网络的拓扑结构不是基于地理位置组织起来的。相反，在同一个网络中相互连接的节点，可能在地理位置上相距遥远，我们采用基于地理的拓扑是为了更加简洁地描述分叉。在真实比特币网络里，节点间的距离按“跳”而不是按照真实位置来衡量。为了便于描述，不同的区块被标示为不同的颜色，传播这些区块的节点网络也被标上颜色。  在第一张图（图8-2）中，网络有一个统一的区块链视角，以蓝色区块为主链的“顶点”。    图8-2 形象化的区块链分叉事件——分叉之前  当有两个候选区块同时想要延长最长区块链时，分叉事件就会发生。正常情况下，分叉发生在两名矿工在较短的时间内，各自都算得了工作量证明解的时候。两个矿工在各自的候选区块一发现解，便立即传播自己的“获胜”区块到网络中，先是传播给邻近的节点而后传播到整个网络。每个收到有效区块的节点都会将其并入并延长区块链。如果该节点在随后又收到了另一个候选区块，而这个区块又拥有同样父区块，那么节点会将这个区块连接到候选链上。其结果是，一些节点收到了一个候选区块，而另一些节点收到了另一个候选区块，这时两个不同版本的区块链就出现了。  在图8-3中，我们看到两个矿工几乎同时挖到了两个不同的区块。这两个区块是顶点区块——蓝色区块的子区块，可以延长这个区块链。为了便于跟踪这个分叉事件，我们设定有一个被标记为红色的、来自加拿大的区块，还有一个被标记为绿色的、来自澳大利亚的区块。    图8-3 形象化的区块链分叉事件：同时发现两个区块  假设有这样一种情况，一个在加拿大的矿工发现了“红色”区块的工作量证明解，在“蓝色”的父区块上延长了块链。几乎同一时刻，一个澳大利亚的矿工找到了“绿色”区块的解，也延长了“蓝色”区块。那么现在我们就有了两个区块：一个是源于加拿大的“红色”区块；另一个是源于澳大利亚的“绿色”。这两个区块都是有效的，均包含有效的工作量证明解并延长同一个父区块。这个两个区块可能包含了几乎相同的交易，只是在交易的排序上有些许不同。  当这个两个区块传播时，一些节点首先收到“红色”区块，一些节点收到“绿色”区块。如图8-4所示，比特币网络上的节点对于区块链的顶点产生了分歧，一派以红色区块为顶点，而另一派以绿色区块为顶点。    图8-4 形象化的区块链分叉事件：两个区块的传播将网络分裂了  从那时起，比特币网络中邻近（网络拓扑上的邻近，而非地理上的）加拿大的节点会首先收到“红色”区块，并建立一个最大累计难度的区块，“红色”区块为这个链的最后一个区块（蓝色-红色），同时忽略晚一些到达的“绿色”区块。相比之下，离澳大利亚更近的节点会判定“绿色”区块胜出，并以它为最后一个区块来延长区块链（蓝色-绿色），忽略晚几秒到达的“红色”区块。那些首先收到“红色”区块的节点，会即刻以这个区块为父区块来产生新的候选区块，并尝试寻找这个候选区块的工作量证明解。同样地，接受“绿色”区块的节点会以这个区块为链的顶点开始生成新块，延长这个链。  分叉问题几乎总是在一个区块内就被解决了。网络中的一部分算力专注于“红色”区块为父区块，在其之上建立新的区块；另一部分算力则专注在“绿色”区块上。即便算力在这两个阵营中平均分配，也总有一个阵营抢在另一个阵营前发现工作量证明解并将其传播出去。在这个例子中我们可以打个比方，假如工作在“绿色”区块上的矿工找到了一个“粉色”区块延长了区块链(蓝色-绿色-粉色)，他们会立刻传播这个新区块，整个网络会都会认为这个区块是有效的，如图8-5所示。    图8-5 形象化的区块链分叉事件：新区块延长了分支  所有在上一轮选择“绿色”区块为胜出者的节点会直接将这条链延长一个区块。然而，那些选择“红色”区块为胜出者的节点现在会看到两个链：“蓝色-绿色-粉色”和“蓝色-红色”。如图8-6所示，这些节点会根据结果将“蓝色-绿色-粉色”这条链设置为主链，将“蓝色-红色”这条链设置为备用链。这些节点接纳了新的更长的链，被迫改变了原有对区块链的观点，这就叫做链的重新共识。因为“红”区块做为父区块已经不在最长链上，导致了他们的候选区块已经成为了“孤块”，所以现在任何原本想要在“蓝色-红色”链上延长区块链的矿工都会停下来。全网将“蓝色-绿色-粉色”这条链识别为主链，“粉色”区块为这条链的最后一个区块。全部矿工立刻将他们产生的候选区块的父区块切换为“粉色”，来延长“蓝色-绿色-粉色”这条链。    图8-6 形象化的区块链分叉事件：全网在最长链上重新共识  从理论上来说，两个区块的分叉是有可能的，这种情况发生在因先前分叉而相互对立起来的矿工，又几乎同时发现了两个不同区块的解。然而，这种情况发生的几率是很低的。单区块分叉每周都会发生，而双块分叉则非常罕见。  比特币将区块间隔设计为10分钟，是在更快速的交易确认和更低的分叉概率间作出的妥协。更短的区块产生间隔会让交易清算更快地完成，也会导致更加频繁地区块链分叉。与之相对地，更长的间隔会减少分叉数量，却会导致更长的清算时间。 |
| 1.5 共识攻击 |
| 比特币的共识机制指的是，被矿工（或矿池）试图使用自己的算力实行欺骗或破坏的难度很大，至少理论上是这样。就像我们前面讲的，比特币的共识机制依赖于这样一个前提，那就是绝大多数的矿工，出于自己利益最大化的考虑，都会通过诚实地挖矿来维持整个比特币系统。然而，当一个或者一群拥有了整个系统中大量算力的矿工出现之后，他们就可以通过攻击比特币的共识机制来达到破坏比特币网络的安全性和可靠性的目的。  值得注意的是，共识攻击只能影响整个区块链未来的共识，或者说，最多能影响不久的过去几个区块的共识（最多影响过去10个块）。而且随着时间的推移，整个比特币块链被篡改的可能性越来越低。理论上，一个区块链分叉可以变得很长，但实际上，要想实现一个非常长的区块链分叉需要的算力非常非常大，随着整个比特币区块链逐渐增长，过去的区块基本可以认为是无法被分叉篡改的。同时，共识攻击也不会影响用户的私钥以及加密算法（[ECDSA](http://8btc.com/article-140-1.html)）。共识攻击也不能从其他的钱包那里偷到比特币、不签名地支付比特币、重新分配比特币、改变过去的交易或者改变比特币持有纪录。共识攻击能够造成的唯一影响是影响最近的区块（最多10个）并且通过拒绝服务来影响未来区块的生成。  共识攻击的一个典型场景就是“51%攻击”。想象这么一个场景，一群矿工控制了整个比特币网络51％的算力，他们联合起来打算攻击整个比特币系统。由于这群矿工可以生成绝大多数的块，他们就可以通过故意制造块链分叉来实现“双重支付”或者通过拒绝服务的方式来阻止特定的交易或者攻击特定的钱包地址。区块链分叉/双重支付攻击指的是攻击者通过不承认最近的某个交易，并在这个交易之前重构新的块，从而生成新的分叉，继而实现双重支付。有了充足算力的保证，一个攻击者可以一次性篡改最近的6个或者更多的区块，从而使得这些区块包含的本应无法篡改的交易消失。值得注意的是，双重支付只能在攻击者拥有的钱包所发生的交易上进行，因为只有钱包的拥有者才能生成一个合法的签名用于双重支付交易。攻击者只能在自己的交易上进行双重支付攻击，但当这笔交易对应的是不可逆转的购买行为的时候，这种攻击就是有利可图的。  让我们看一个“51%攻击”的实际案例吧。在第1章我们讲到，Alice 和 Bob 之间使用比特币完成了一杯咖啡的交易。咖啡店老板 Bob 愿意在 Alice 给自己的转账交易确认数为零的时候就向其提供咖啡，这是因为这种小额交易遭遇“51%攻击”的风险和顾客购物的即时性（Alice 能立即拿到咖啡）比起来，显得微不足道。这就和大部分的咖啡店对低于25美元的信用卡消费不会费时费力地向顾客索要签名是一样的，因为和顾客有可能撤销这笔信用卡支付的风险比起来，向用户索要信用卡签名的成本更高。相应的，使用比特币支付的大额交易被双重支付的风险就高得多了，因为买家（攻击者）可以通过在全网广播一个和真实交易的UTXO一样的伪造交易，以达到取消真实交易的目的。双重支付可以有两种方式：要么是在交易被确认之前，要么攻击者通过块链分叉来完成。进行51%攻击的人，可以取消在旧分叉上的交易记录，然后在新分叉上重新生成一个同样金额的交易，从而实现双重支付。  再举个例子：攻击者Mallory在Carol的画廊买了描绘伟大的[中本聪](http://8btc.com/article-25-1.html)的三联组画，Mallory通过转账价值25万美金的比特币与Carol进行交易。在等到一个而不是六个交易确认之后，Carol放心地将这幅组画包好，交给了Mallory。这时，Mallory的一个同伙，一个拥有大量算力的矿池的人Paul，在这笔交易写进区块链的时候，开始了51%攻击。首先，Paul利用自己矿池的算力重新计算包含这笔交易的块，并且在新块里将原来的交易替换成了另外一笔交易（比如直接转给了Mallory的另一个钱包而不是Carol的），从而实现了“双重支付”。这笔“双重支付”交易使用了跟原有交易一致的UTXO，但收款人被替换成了Mallory的钱包地址。然后，Paul利用矿池在伪造的块的基础上，又计算出一个更新的块，这样，包含这笔“双重支付”交易的块链比原有的块链高出了一个块。到此，高度更高的分叉区块链取代了原有的区块链，“双重支付”交易取代了原来给Carol的交易，Carol既没有收到价值25万美金的比特币，原本拥有的三幅价值连城的画也被Mallory白白拿走了。在整个过程中，Paul矿池里的其他矿工可能自始至终都没有觉察到这笔“双重支付”交易有什么异样，因为挖矿程序都是自动在运行，并且不会时时监控每一个区块中的每一笔交易。  为了避免这类攻击，售卖大宗商品的商家应该在交易得到全网的6个确认之后再交付商品。或者，商家应该使用第三方的多方签名的账户进行交易，并且也要等到交易账户获得全网多个确认之后再交付商品。一条交易的确认数越多，越难被攻击者通过51%攻击篡改。对于大宗商品的交易，即使在付款24小时之后再发货，对买卖双方来说使用比特币支付也是方便并且有效率的。而24小时之后，这笔交易的全网确认数将达到至少144个（能有效降低被51%攻击的可能性）。  共识攻击中除了“双重支付”攻击，还有一种攻击场景就是拒绝对某个特定的比特币地址提供服务。一个拥有了系统中绝大多数算力的攻击者，可以轻易地忽略某一笔特定的交易。如果这笔交易存在于另一个矿工所产生的区块中，该攻击者可以故意分叉，然后重新产生这个区块，并且把想忽略的交易从这个区块中移除。这种攻击造成的结果就是，只要这名攻击者拥有系统中的绝大多数算力，那么他就可以持续地干预某一个或某一批特定钱包地址产生的所有交易，从而达到拒绝为这些地址服务的目的。  需要注意的是，51%攻击并不是像它的命名里说的那样，攻击者需要至少51%的算力才能发起，实际上，即使其拥有不到51%的系统算力，依然可以尝试发起这种攻击。之所以命名为51％攻击，只是因为在攻击者的算力达到51%这个阈值的时候，其发起的攻击尝试几乎肯定会成功。本质上来看，共识攻击，就像是系统中所有矿工的算力被分成了两组，一组为诚实算力，一组为攻击者算力，两组人都在争先恐后地计算块链上的新块，只是攻击者算力算出来的是精心构造的、包含或者剔除了某些交易的块。因此，攻击者拥有的算力越少，在这场决逐中获胜的可能性就越小。从另一个角度讲，一个攻击者拥有的算力越多，其故意创造的分叉块链就可能越长，可能被篡改的最近的块或者或者受其控制的未来的块就会越多。一些安全研究组织利用统计模型得出的结论是，算力达到全网的30%就足以发动51%攻击了。  全网算力的急剧增长已经使得比特币系统不再可能被某一个矿工攻击，因为一个矿工已经不可能占据全网哪怕的1%算力。但是中心化控制的矿池则引入了矿池操作者出于利益而施行攻击的风险。矿池操作者控制了候选块的生成，同时也控制哪些交易会被放到新生成的块中。这样一来，矿池操作者就拥有了剔除特定交易或者双重支付的权力。如果这种权利被矿池操作者以微妙而有节制的方式滥用的话，那么矿池操作者就可以在不为人知的情况下发动共识攻击并获益。  但是，并不是所有的攻击者都是为了利益。一个可能的场景就是，攻击者仅仅是为了破坏整个比特币系统而发动攻击，而不是为了利益。这种意在破坏比特币系统的攻击者需要巨大的投入和精心的计划，因此可以想象，这种攻击很有可能来自政府资助的组织。同样的，这类攻击者或许也会购买矿机，运营矿池，通过滥用矿池操作者的上述权力来施行拒绝服务等共识攻击。但是，随着比特币网络的算力呈几何级数快速增长，上述这些理论上可行的攻击场景，实际操作起来已经越来越困难。近期比特币系统的一些升级，比如旨在进一步将挖矿控制去中心化的P2Pool挖矿协议，也都正在让这些理论上可行的攻击变得越来越困难。  毫无疑问，一次严重的共识攻击事件势必会降低人们对比特币系统的信心，进而可能导致比特币价格的跳水。然而，比特币系统和相关软件也一直在持续改进，所以比特币社区也势必会对任何一次共识攻击快速做出响应，以使整个比特币系统比以往更加稳健和可靠。 |

## 1.6 区块链形态

### 1.6.1 公有链

比特币区块链即是一种典型的公有链。比特币的区块链作为一种公开账本，具有人人皆可参与的特性。也就是说任何人都可以发起一笔交易，任何人也都可以参与验证交易，任何人也都可以同时读取区块链上的所有信息。不仅是比特币区块链，其他各类山寨币由于基本模仿了比特币的架构，以建立一种支付验证体系为目的，因此也基本都属于公有链的范畴。在以太坊创始人Vitalik Buterin（2015）的定义中，公有链的特性被定义为任何人都可参与到共识机制中的区块链组织架构，即任何人都可以参与到决定一个新的区块是否被加入到链上，不论是以工作量证明的方式还是以持有量证明（Proof-of-Stake）参与其中。

由于比特币区块链形成最早，同时比特币持有人、验证节点、矿工广泛分布于全球，因此在800多p的全网算力支持下，比特币区块链即成为了所有公有链中最为强健、最为安全的代表。

### 1.6.2 私有链

正是由于比特币区块链作为公用链具有以上的局限性，导致了当前大多数金融巨头所热衷的区块链技术研究并不以比特币区块链或者公有链为开发目标。然而虽然广泛被认为除了公有链以外的各种尝试均被称为私有链，但事实上私有链也被分为了两种细分类型，分别为财团链或者半管制私有链，以及纯私有链或全管制私有链。

财团链指的是共识机制的参与需经历提前的筛选，并非所有人都可对链上的区块进行验证。举例来说，一个由15个金融机构组成的财团，设置了规则，要求超过10个以上的金融机构签署过的区块才能够被认证上链，对已上链的区块验证可以是公开的，也可以是对特点参与者进行限制性开放的，但除了金融机构组成的财团内部以外的节点是不能参与共识机制的认证的。

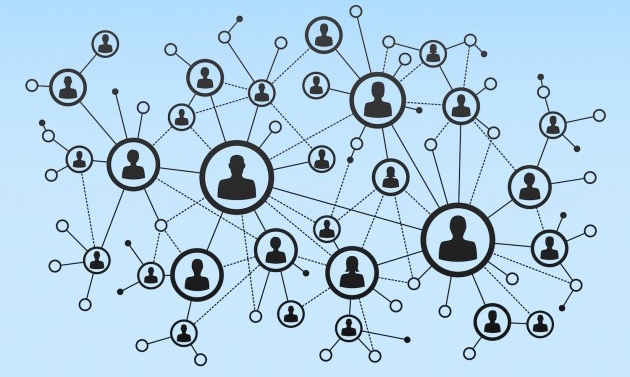
纯私有链则是整个区块链的共识机制、验证、读取等行为均被严格限制在一个范围以内，其作用与企业数据库管理、内部审计等相似，仅对特定主体内部开放，并不以任何形式对外公开。

# 第2章 通往区块链之路

## 2.1 区块链互联网

传统的互联网是一个“中心——去中心——中心”的结构，但本质是一个中心化结构;而区块链是一个“去中心-中心-去中心”的结构，更接近于自然的智慧。区块链技术宣告了互联网从传递信息的信息互联网向转移价值的价值互联网进化。

## 2.2 管理的一种新模式



随着希腊债务危机的显露，以及资本管制对希腊人民的压迫，比特币再一次回到了主流的焦点。ATM机前那长龙似的排队，不禁让人联想起塞浦路斯的危机，再一次地，比特币似乎为人们提供了一个安全的避风港。

虽然很多人所关注的，只是比特币的价格波动以及潜在采用人群的增加，货币只是其改变游戏规则技术的第一个应用。区块链的核心，是针对寡头所控制的，对希腊人民严厉的财政紧缩政策，而提供一个备选管理模式。

六年时间的存在，公众对这项技术的认识已经得到了长足的发展。现在，大多数意识到这种突破性技术的人都已经明白，区块链是一个总账，然而，它不仅仅是简单地作为货币交易的记账系统而已。

其核心，是作为一个平台，可以在无需中介方的情况下，允许人们在几乎任何事情上达成协议。它提供了一个基础，让基于协商一致原则的社会契约论成为可能。

当这一技术的白皮书在2008年出世，其匿名创造者中本聪就曾指出，这是一种针对信任基础模式存在的内在缺陷，而发明的一种解决方案。Roger Ver，又名“比特币耶稣”，他是比特币创业公司天使投资人，最近他对希腊财政危机发表了评论，指出了现有政府单向的契约形式容易犯错的性质：

比特币通过算法自我调节，消除了合约对方的风险，而传统法律和监管工具在一些事件中已被证明是无效的，例如汇丰银行洗钱案以及整个巨大的银行业印钱与操纵市场的问题。这项发明的核心是分布式信任机制，并通过一种名为工作量证明（POW）的机制来实现。

工作量证明

安德烈亚斯·安东诺普洛斯(Andreas Antonopoulos），区块链技术和比特币专家，在他的[共识算法](http://www.iamsatoshi.com/consensus-algorithms-blockchain-technology-and-bitcoin/)演讲中，他描述了工作量证明如何由特定的加密散列函数，一系列动态调整并创造规模经济的博弈论均衡系统组成。

工作量证明机制在保证整个系统的安全性中，扮演了一个至关重要的作用。Adam Back，Hashcash的发明者，对比特币的基本原理提供了帮助，他指出了这个系统是如何从工作量证明机制以及共识中构建出计算机的不可撤销性。

这意味着，没有人可以对已做过的工作进行撤销处理。也没有人可以对此进行伪造以及重新分配，矿工作为比特币生态系统中的心脏，他们必须通过宝贵的资源来执行哈希操作，如果他们按规则行事，他们将获得报酬，反之，他们将失去报酬。

这使得区块链具有了强大的抵抗性，还拥有了耐操纵性，它预防了政府通过诸如量化宽松措施所造成的恶性通货膨胀。

经济激励的神来之笔

那是什么在激励着这个自治组织系统？以及最重要的，其会计责任的力量又从何而来？比特币没有一个中央计划者。从某种意义上来说，中本聪的匿名体现了技术的精髓，这项技术实际上并不存在指纹。这项数学发明的中心点，是一个至关重要的经济诱因，可以让矿工自发地去维护这个总账，使得它去中心化并且不可更改。

这种激励结构表现在现有比特币网络背后，其内置的数字稀缺性。它由现实主义以及人的自我利益诚实的评估组成。

当我们没有考虑我们的自私会带来什么时，历史给予了我们各种证据。原子弹、奴隶制、大屠杀和种族灭绝，这些黑暗的回忆，提醒了我们人性固有的残忍与暴力。

“区块链创造了激励，能够让参与者诚实地工作，其规则将一视同仁。”

当自利原则不被承认，他们将很快逃离自觉。当人们开始自我否认自己的人性，便可以轻易地获得优势。他们变得贪得无厌，这推动人们去追求权力，创造不诚实的系统，其中反社会势力会攻击网络，接管经济，破坏国家主权以及人民的意志。

通过私念与贪欲的核算，用奖励来鼓励他们在透明开放的网络中良好地表现，区块链为参与者创造了一个诚信工作的激励，这种规则将一视同仁。

通过这种方式，该系统可以更有效地减轻人类潜在破坏的风险性。

分布式会计责任（Distributed accountability）

比特币网络通过自愿原则以及由共识规则而实现的自我调节，促进了真正的主权在民的实现。

这项创新所形成的，是社会责任的一种新形式。不同于传统的管理模型代表，其中，检查与平衡系统是通过第三方来行使。在比特币的共识模式下，会计责任将是直接分配，并由整个网络的所有参与者共同行使。

这就消除了单点故障的问题，提供了比现有系统更好的安全性。随着区块链的透明性，那些喜欢不劳而获的人将无处可去，也无处可避。

目前，通过这项技术来加强政治会计责任，已经有了创造性的举措。伦敦市长候选人乔治·加洛韦（George Galloway）呼吁伦敦采用基于区块链技术的记账系统，为伦敦市民的金融活动提供充分的透明度。

据RT财经节目主持人Max Keiser报道，加洛韦还创建了一个市长链项目（ The Mayor's Chain Project ），打算将伦敦城的年度预算放到区块链中，让公民们来共同审计。

比特币协议，它是分布式管理的蓝图。它是一项真正的发明，无法被撤销。当全球合法性危机加深，紧缩政策继续时，破产的银行忙着自救，对冲基金们则通过篡改帐本来避开这一问题。

比特币可能无法在此刻拯救希腊，但是其核心技术，为那些想要引入替代中心化机构强制信任模式，并进入基于分布式民主网络社会的人们，提供了一种真正可行的工具。

## 2.3 三体与区块链

春节期间阅读了《三体》这本小说，这部小说的作者刘慈欣2015年获得了全球科幻小说的最高奖“雨果奖”。这本小说的原创性，是对人性的丑恶有非常深刻的认识，人类有太多的欺诈、伪善，主要是以文革为背景写的，文革期间的人与人之间的斗争处处可见，甚至于现在一些热播电视剧，像《甄嬛传》，《琅琊榜》大量的都是勾心斗角，好像中华文明这样的东西太多，不断循环，跳脱不出原有的限定模式。《三体》这本小说是说“三体人”的思想是完全透明的，互相之间交流完全无障碍。人类完全不能理解，说一个思想全透明的社会会产生怎样的政治和文化呢？难道你们没有计谋和伪装？三体人就回答说：“计谋和伪装是什么？”刘慈欣虚构出这样的三体人社会，比人类文明发达许多，到地球上来把地球人打得大败！显然作者的愿望是：人类如果不克服自己的弱点的话，将无法真正上升到一个更高的文明。

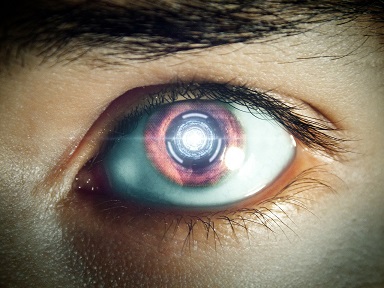


回到区块链技术本身，区块链是去中心化的，不可篡改的分布式帐簿；区块链网络中的每个节点是透明的，无法自行伪造；其思想与三体世界呈现的精神不谋而合。**然而区块链能让地球人变成三体人吗？**完全有可能，我们可以应用脑机接口技术，将来人脑思考的信息，通过计算机可以直接读取出来；同时利用区块链分布式公正技术，建立一个透明的、没有伪装的、没有欺诈的智能决策过程；另外，区块链本身的共识主动性就是一个群体智能的概念，是指在一个共识群体中，个体单独行动的机制。在主动共识性的机制作用下，这个群体无需中枢控制系统，群体内部成员间也无需直接交流信息，个体为了实现自己的利益单独地、连续地相互修正和自我更新，从而逐步完善自己的生态环境，实现整体的利益最大化。

## 2.4 人工智能与区块链

人工智能和区块链？这听起来好像一首很奇妙的歌曲，不过如果你认真的思考一下，也未尝不可，能否让区块链来为我们创造一个新的世界?我们会不会在不久的将来生活在这样的一个世界里：机器人战警可以替代血肉之躯的警察担负起危险的行动任务。在这个区块链创造的世界里，将由人类来制定他们的法规规范，也就是说人类可以通过区块链的技术在特定的环境下来打开或关闭机器人的特定行动。

**区块链上的人工智能**  
  
1955年，约翰麦卡锡创造了“人工智能”这一术语。从那时起，人类一直在孜孜不倦地进行研究，试图创造一个完美的真正的智能机器人。也许是人类试图想更加接近机器的渴望所驱使。或者他们有和我相同的想法，在试图尝试那些复杂的足以模仿人类思维的挑战。再或者他们试图创造出一个他们最最关心和心爱的人儿，这无疑是值得他们去为之努力奋斗的一件事。总之，不管是什么原因驱使他们去发明创造智能机器人，智能机器人都越来越可能会有实现的那一天。  
   
也许不久后的一天，智能机器人将像和我们一起生活的兄弟姐妹们一样，伴随我们一起成长，我们不会觉得他有什么特别的。就好比人们不会因为有一个不同种族的哥哥或姐姐而想的太多。爱会让人变得理智和理性，因为人总是会追寻快乐幸福的，这都是同样的道理。人工智能机器人也会在不久的将来成为我们这个社会不可或缺的一部分。  
   
我们如何实现让他们可以拥有比我们更高的智力，而又有谁可以知道他们会不会成为下一个终结者？毕竟，人，有血有肉的人类，在过去的历史岁月里是劣迹斑斑的，战争，强奸，谋杀，盗窃…但我们也有爱，欢笑，和互助友善等美好的感情。智能机器人是不是也会和我们人类一样，他们中的一些人会不会也呈现出一些病态特征，而另一些则满怀了爱，关怀，像人类一样的拥有复杂的感情？  
   
在区块链上依靠投票的方式创建创造一套更加完善的法律系统，这可能是有助于人类构建一套适用于机器人的法律体系的办法，当然前提是要遵循原来的法律。新的以区块链为基础构建的政府体系将给予机器人们应得的权利，与此同时，和我们一起朝夕共处的人工智能机器人也将受到和我们同样的法律规范的制约。通过植入区块链技术到每个个体中，从而确保每个人工智能机器人可以严格遵循法律规范的制约。当一则新的法律条款出炉，而我们还不太了解的时候，甚至他们还会告诉我们什么是可以做的而什么是不可以做的。  
   
基于区块链的政府，人工智能机器人可以胜任众多新的工作岗位，比如：创造更多的智能机器人，就像我们现在建造房屋和设备一样。当然他们还可以胜任教师，教授，或是消防员，警察，或其他领域的公共服务岗位。通过和区块链政府的直接对接，他们会非常适合担任法官，律师，当然，还有政客。



《电影》人工智能

**可以挽救生命的区块链解决方案**  
  
我先来描述一个场景。假如一个人犯了罪，然后他从犯罪现场驾车急速逃离现场，警察及时发现了这起事件，并驾驶警车超速把他的车逼停。而这时警察可能不知道犯罪分子手里还有一把枪。警察走近犯罪嫌疑人的车，并要求他出示证件。然后警察转身回到巡逻车来查询验证证件，这时犯罪嫌疑人朝警察的背部开枪了。这位警察有亲爱妻子和孩子，但是他们以后将再也不能看到他了，他们唯有为他哀悼，并且在之后的岁月里相依为命的活下去。与此同时，罪犯却逃到了另一个国家，并在那里长期的隐匿起来，在他被逮捕前没有人知道他犯下的滔天罪行。  
   
那么，如果换成人工智能机器人警察呢。  
   
同一犯罪场景，但这一次的警察是一个智能机器人。机器人警察拿到罪犯的证件，然后回到他的警车。如果这时罪犯对他开枪，由于机器人警察的身体是被防弹材料保护起来的，所以子弹不会让他受到伤害。为什么人类的警察不穿盔甲呢，那是因为它相当的笨重，而这可能会让他的动作变得迟缓。而大多数时候，警察是不会遭遇到枪击事件的，所以没有理由让他们成年累月的穿着一套笨重的盔甲工作。机器人就不同了，可以在设计之初就让他身上覆盖一层防护材料。即便是便宜又笨重的材料，比如加厚的钢板也不在话下，当然有些身体部位也可使用于轻质的纤维或其他材料。如此一来，在遭遇同样情况的时候，警察就不会因为犯罪分子的子弹而殉职了，机器人警察将会变得勇猛异常甚至所向无敌。  
   
可能还有另一种情况，机器人警察被犯罪分子使用爆破手段或在没有任何盔甲防护的情况下被枪击，或者被以别的形式的犯罪手段而摧毁。这种情况下，机器人警察将不再向控制中心发送定时的信号，这时，整个警察网络将及时知道他遇到麻烦了。而他最后发送给控制中心的信号将包含他发射信号时所在GPS坐标位置和正在执行的指令。而就近的警察可以很容易找到他，发现他被摧毁的现场，而另外的警察将继续追捕犯罪分子。另外，发给中心的信号也可以包含更多的信息，比如被追踪的汽车车牌或其他有用信息，这样可以让别的警察了解他追踪的对象是谁。而与此同时，一个新的机器人将被制造出来，用来取代那个被摧毁的机器人警察。  
   
现在该向你提几个小问题了!你认为未来的世界里，智能机器人和区块链技术会扮演什么角色？你想不想生活在一个由大多数人制定规则的世界里？你想不想生活在一个机器人可以拯救许多生命的世界里？你认为区块链政府体系是否靠谱，它能帮助我们约束机器人的行为吗？   
 －－－－  
原文：https://www.cryptocoinsnews.com/ai-blockchain-dystopian-utopian-future/

## 2.5 从O2O到区块链

# 第3章 区块链应用场景

## 3.1 存在性证明

## 3.2 智能合约

## 3.3 物联网

## 3.4 身份验证

## 3.5 预测市场

## 3.6 资产交易

## 3.7 电子商务

## 3.8 文件存储

## 3.9 数据库