**区块链解密：构建基于信用的下一代互联网**

互联网领域最知名的“预言家”凯文·凯利在《失控》一书中指出，未来世界的趋势是去中心化的。亚当•斯密的“看不见的手”就是对市场去中心化本质的一个很好的概括。两点之间直线最短，人们之间沟通的最好方式也是直接沟通，无论从哪个角度切入，去中心化的市场本质都是无可辩驳的。

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。

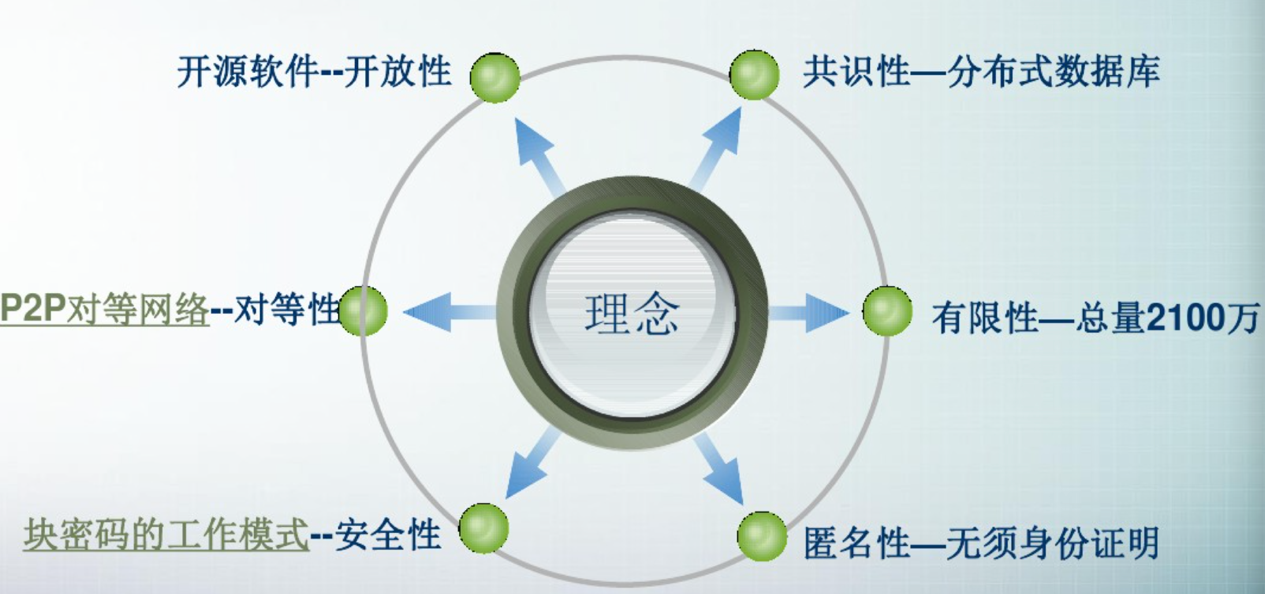
# 第1章 区块链：前世今生

## 比特币

### 产生背景

比特币（BitCoin）的概念最初由中本聪在2008年发表的论文《比特币：一种点对点的电子现金系统》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。

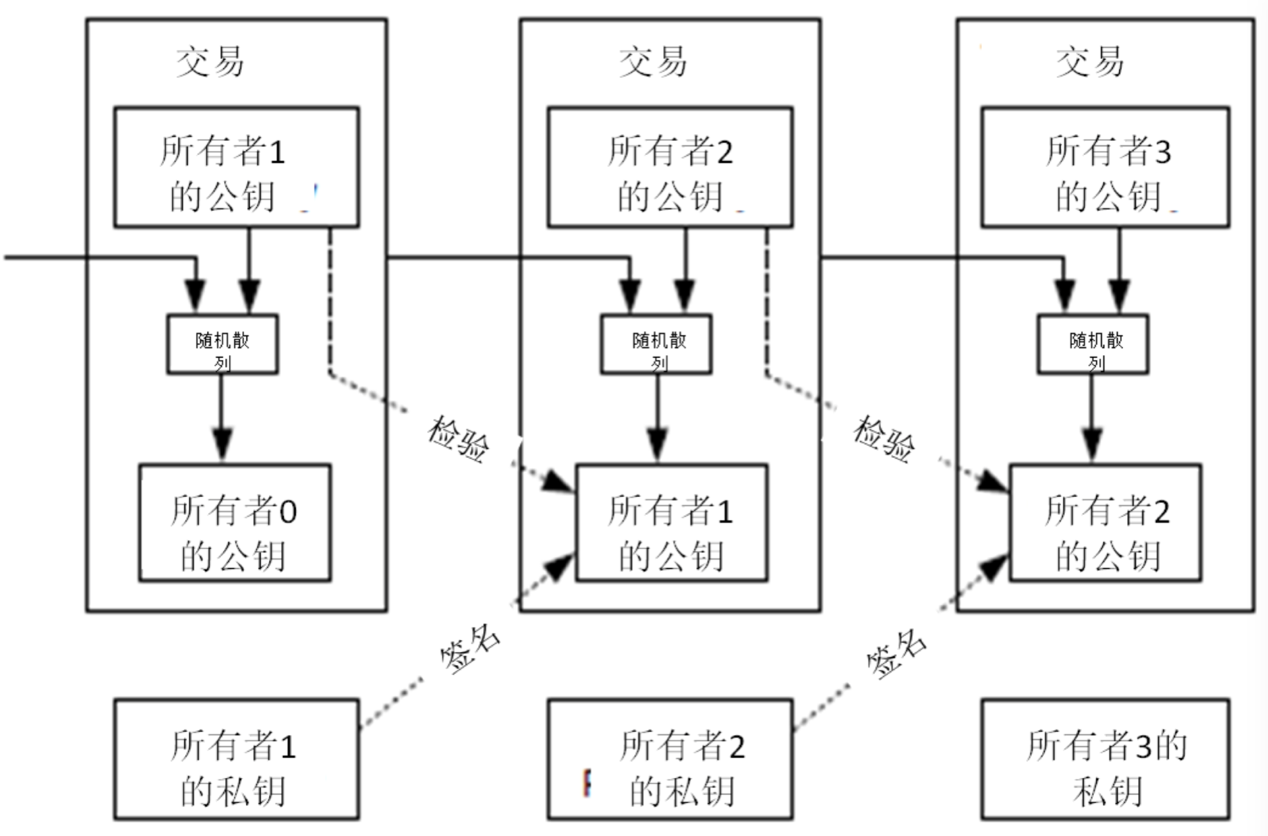
与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的[分布式数据库](http://baike.baidu.com/view/68389.htm)来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节[安全性](http://baike.baidu.com/view/421194.htm)。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。比特币与其他[虚拟货币](http://baike.baidu.com/view/16260.htm)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。



### 技术原理

#### 1交易

我们定义，一枚电子货币是这样的一串数字签名：每一位所有者通过对前一次交易和下一位拥有者的公钥(Public key) 签署一个随机散列的数字签名，并将这个签名附加在这枚电子货币的末尾，电子货币就发送给了下一位所有者。而收款人通过对签名进行检验，就能够验证该链条的所有者。

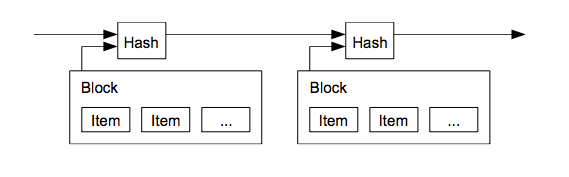


该过程的问题在于，收款人将难以检验，之前的某位所有者是否对这枚电子货币进行了双重支付。通常的解决方案，就是引入信得过的第三方权威，或者类似于造币厂的机构，来对每一笔交易进行检验，以防止双重支付。在每一笔交易结束后，这枚电子货币就要被造币厂回收，而造币厂将发行一枚新的电子货币；而只有造币厂直接发行的电子货币才算作有效，这样就能够防止双重支付。可是该解决方案的问题在于，整个货币系统的命运完全依赖于运作造币厂的公司，因为每一笔交易都要经过该造币厂的确认，而该造币厂就好比是一家银行。

我们需要收款人有某种方法，能够确保之前的所有者没有对更早发生的交易实施签名。从逻辑上看，为了达到目的，实际上我们需要关注的只是于本交易之前发生的交易,而不需要关注这笔交易发生之后是否会有双重支付的尝试。为了确保某一次交易是不存在的，那么唯一的方法就是获悉之前发生过的所有交易。在造币厂模型里面，造币厂获悉所有的交易，并且决定了交易完成的先后顺序。如果想要在电子系统中排除第三方中介机构，那么交易信息就应当被公开宣布，我们需要整个系统内的所有参与者，都有唯一公认的历史交易序列。收款人需要确保在交易期间绝大多数的节点都认同该交易是首次出现。

#### 2时间戳服务器

比特币本质是构造了一个永不停息、无坚不摧的时间戳系统。时间戳服务器通过对以区块形式存在的一组数据实施随机散列而加上时间戳，并将该随机散列进行广播，就像在新闻或世界性新闻组网络的发帖一样。显然，该时间戳能够证实特定数据必然于某特定时刻是的确存在的，因为只有在该时刻存在了才能获取相应的随机散列值。每个时间戳应当将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的一个时间戳进行增强，这样就形成了一个链条。



#### 3双花问题

加密数字货币和其他数字资产一样，如同可以将一个文件以附件形式保存并发送任意多次，具有无限可复制性的缺陷。如果没有一个中心化的机构，我们无法确认一笔数字现金或资产是否已经被花掉或提取。为了解决“双花”问题，可以信赖的第三方需要保留交易总帐从而保证每笔现金或资产只被花费或提取过一次。在区块链中，每一个区块都包含了上一个区块的哈希值，从创始区块开始连接到当前区块从而形成块链。每一个区块都要确保按照时间顺序在上个区块之后产生，否则前一个区块的哈希值是未知的。同时，由于区块链中所有交易都要进行对外广播，所以只有当包含在最新区块中的所有交易都是独一无二且之前从未发生过，其他节点才会认可该区块。因此在区块链中，“双花”变的非常困难。

#### 4拜占庭将军问题

拜占庭将军问题是一个共识问题，核心描述是军中可能有叛徒，却要保证进攻一致，由此引申到计算领域，发展成了一种容错理论。随着比特币的出现和兴起，这个著名问题又重入大众视野。

关于拜占庭将军问题，一个简易的非正式描述如下: 拜占庭帝国想要进攻一个强大的敌人，为此派出了10 支军队去包围这个敌人。这个敌人虽不比拜占庭帝国, 但也足以抵御5支常规拜占庭军队的同时袭击。基于一些原因，这10支军队不能集合在一起单点突破，必须在分开的包围状态下同时攻击。他们任一支军队单独进攻都毫无胜算，除非有至少6支军队同时袭击才能攻下敌国。他们分散在敌国的四周，依靠通信兵相互通信来协商进攻意向及进攻时间。困扰这些将军的问题是，他们不确定他们中是否有叛徒,叛徒可能擅自变更进攻意向或者进攻时间。在这种状态下，拜占庭将军们能否找到一种分布式的协议来让他们能够远程协商，从而赢取战斗？这就是著名的拜占庭将军问题。

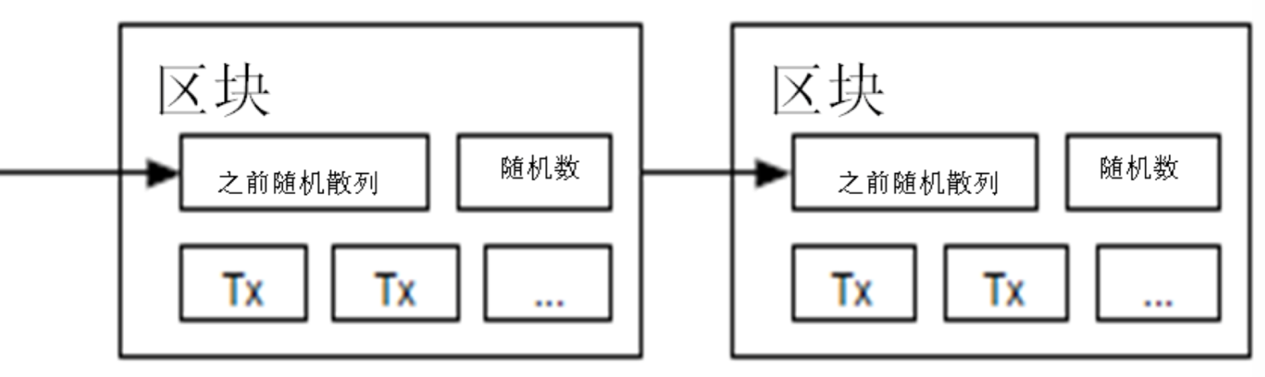
如果每支军队向其他九支军队派出一名信使，那么就是十支军队每个派出了九名信使，也就是在任何一个时间又总计90次的传输，并且每支军队分别收到九个信息，可能每一封都写着不同的进攻时间。除此以外，部分军队会答应超过一个的攻击时间，故意背叛发起人，所以他们将重新广播超过一条的信息链。这个系统迅速变质成不可信的信息和攻击时间相互矛盾的纠结体。

比特币通过对这个系统做出一个简单的修改解决了这个问题，它为发送信息加入了成本，这降低了信息传递的速率，并加入了一个随机元素以保证在一个时间只有一支军队可以进行广播。它加入的成本是“工作量证明”，并且它是基于计算一个随机哈希算法的。

#### 5工作量证明

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。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，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，并找到为止。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。

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。

#### 6网络

运行该网络的步骤如下:

（1）新的交易向全网进行广播;

（2） 每一个节点都将收到的交易信息纳入一个区块中;

（3）每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明;   （4）当一个节点找到了一个工作量证明，它就向全网进行广播;

（5）当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的,其他节点才认同 该区块的有效性;

（6）其他节点表示他们接受该区块,而表示接受的方法，则是在跟随该区块的末尾，制造新的区块以延长该链条，而将被接受区块的随机散列值视为先于新区块的随机散列值。

节点始终都将最长的链条视为正确的链条，并持续工作和延长它。如果有两个节点同时广播不同版本的新区块，那么其他节点在接收到该区块的时间上将存在先后差别。当此情形，他们将在率先收到的区块基础上进行工作，但也会保留另外一个链条，以防后者变成最长的链条。该僵局的打破要等到下一个工作量证明被发现，而其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。

所谓“新的交易要广播”，实际上不需要抵达全部的节点。只要交易信息能够抵达足够多的节点，那么他们将很快被整合进一个区块中。而区块的广播对被丢弃的信息是具有容错能力的。如果一个节点没有收到某特定区块，那么该节点将会发现自己缺失了某个区块，也就可以提出自己下载该区块的请求。

#### 7激励

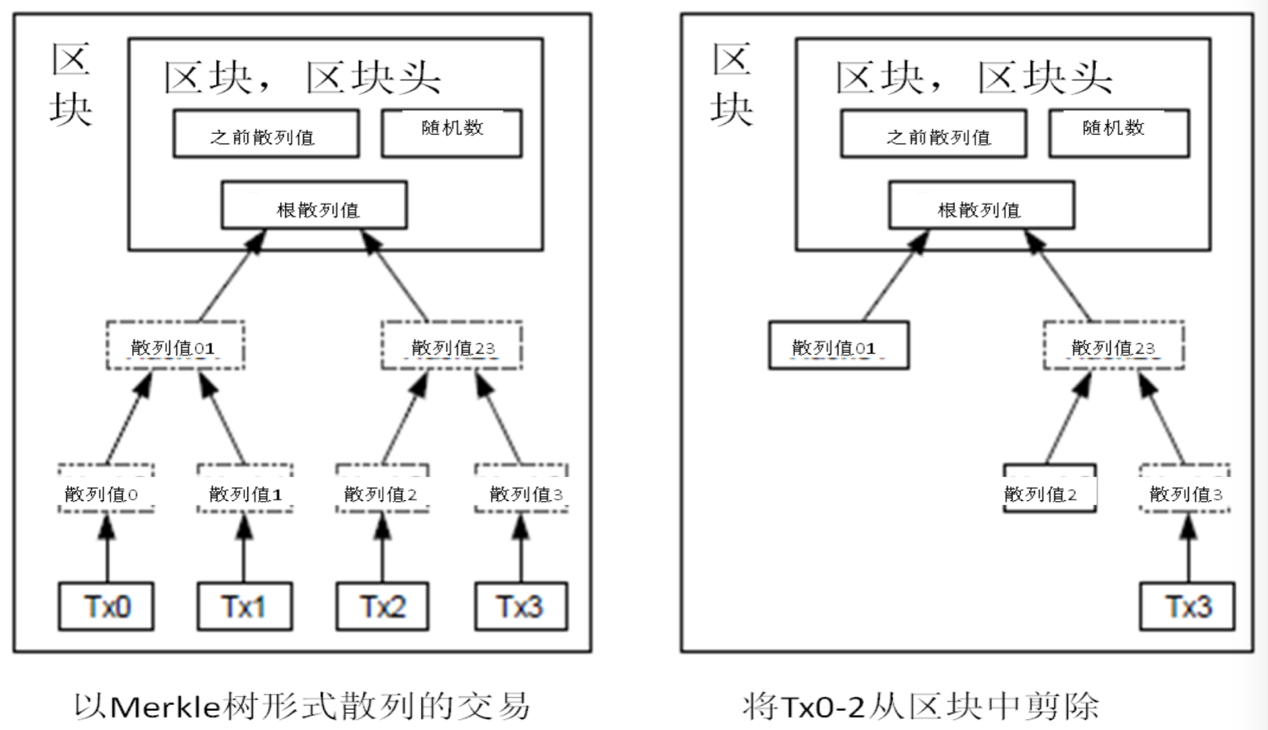
我们约定如此：每个区块的第一笔交易进行特殊化处理，该交易产生一枚由该区块创造者拥有的新的电子货币。这样就增加了节点支持该网络的激励，并在没有中央集权机构发行货币的情况下，提供了一种将电子货币分配到流通领域的一种方法。这种将一定数量新货币持续增添到货币系统中的方法，非常类似于耗费资源去挖掘金矿并将黄金注入到流通领域。此时， CPU的时间和电力消耗就是消耗的资源。

另外一个激励的来源则是交易费。如果某笔交易的输出值小于输入值，那么差额就是交易费，该交易费将被增加到该区块的激励中。只要既定数量的电子货币已经进入流通，那么激励机制就可以逐渐转换为完全依靠交易费，那么本货币系统就能够免于通货膨胀。

激励系统也有助于鼓励节点保持诚实。如果有一个贪婪的攻击者能够调集比所有诚实节点加起来还要多的CPU计算力，那么他就面临一个选择：要么将其用于诚实工作产生新的电子货币，或者将其用于进行二次支付攻击。那么他就会发现，按照规则行事、诚实工作是更有利可图的。因为该等规则使得他能够拥有更多的电子货币，而不是破坏这个系统使得其自身财富的有效性受损。

#### 8回收硬盘空间

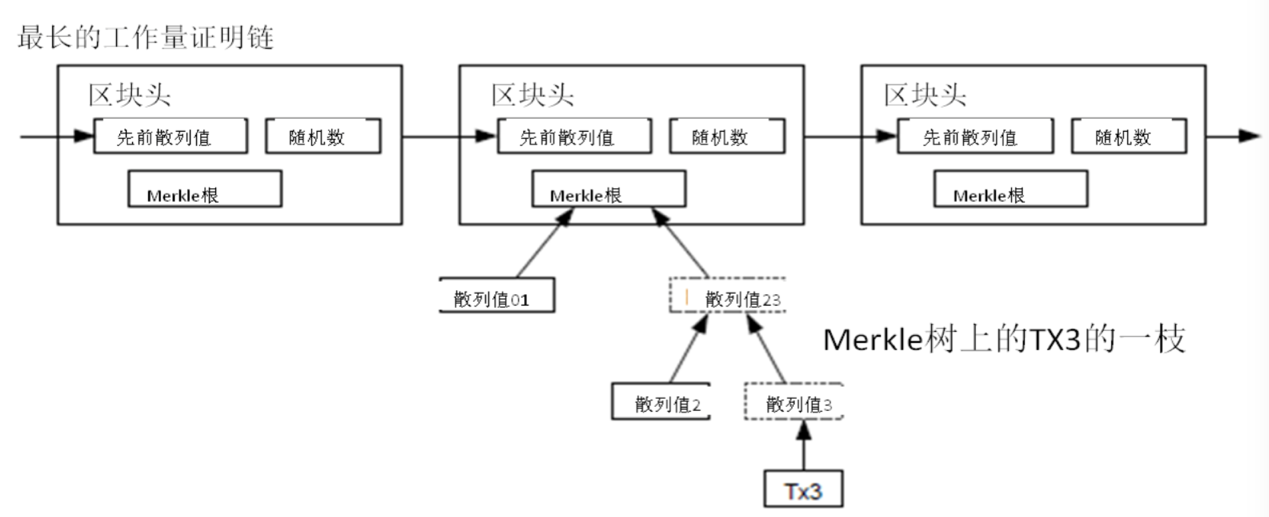
如果最近的交易已经被纳入了足够多的区块之中，那么就可以丢弃该交易之前的数据，以回收硬盘空间。为了同时确保不损害区块的随机散列值,交易信息被随机散列时,被构建成一种梅克尔树(Merkle tree) 的形态，使得只有根被纳入了区块的随机散列值。通过将该树的分支拔除的方法，老区块就能被压缩。而内部的随机散列值是不必保存的。



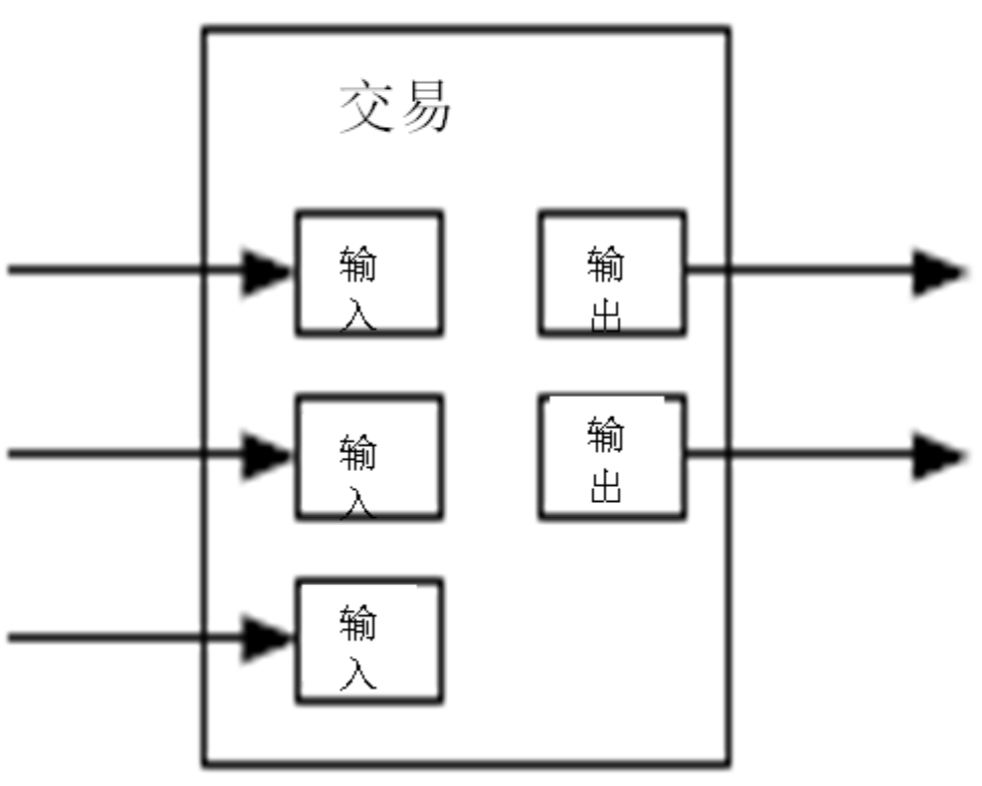
不含交易信息的区块头(Block header)大小仅有80字节。如果我们设定区块生成的速率 为每10分钟一个,那么每一年产生的数据位4.2MB。(80 bytes \* 6 \* 24 \* 365 = 4.2MB)。2008年，PC系统通常的内存容量为2GB,按照摩尔定律的预言,即使将全部的区块头存储于内存 之中都不是问题。

#### 9简化的支付确认

在不运行完整网络节点的情况下,也能够对支付进行检验。一个用户需要保留最长的工作量证明链条的区块头的拷贝,它可以不断向网络发起询问,直到它确信自己拥有最长的链条, 并能够通过 merkle 的分支通向它被加上时间戳并纳入区块的那次交易。节点想要自行检验该交易的有效性原本是不可能的,但通过追溯到链条的某个位置,它就能看到某个节点曾经接受 过它,并且于其后追加的区块也进一步证明全网曾经接受了它。



当此情形,只要诚实的节点控制了网络,检验机制就是可靠的。但是,当全网被一个计算 力占优的攻击者攻击时,将变得较为脆弱。因为网络节点能够自行确认交易的有效性,只要攻 击者能够持续地保持计算力优势,简化的机制会被攻击者焊接的(fabricated)交易欺骗。那 么一个可行的策略就是,只要他们发现了一个无效的区块,就立刻发出警报,收到警报的用户 将立刻开始下载被警告有问题的区块或交易的完整信息,以便对信息的不一致进行判定。对于 日常会发生大量收付的商业机构,可能仍会希望运行他们自己的完整节点,以保持较大的独立 完全性和检验的快速性。

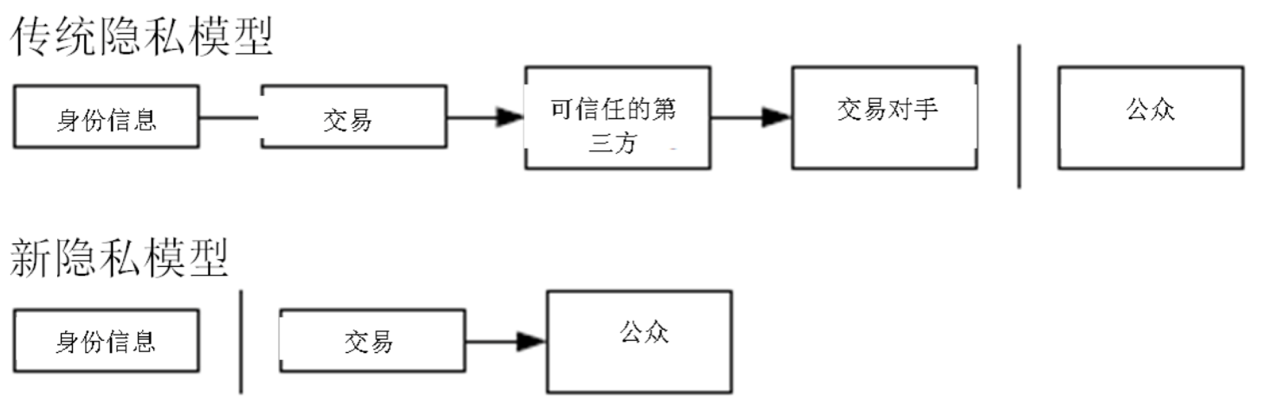


#### 10价值的组合与分割

虽然可以单个单个地对电子货币进行处理，但是对于每一枚电子货币单独发起一次交易将是一种笨拙的办法。为了使得价值易于组合与分割，交易被设计为可以纳入多个输入和输出。一般而言是某次价值较大的前次交易构成的单一输入，或者由某几个价值较小的前次交易共同构成的并行输入，但是输出最多只有两个：一个用于支付，另一个用于找零。

需要指出的是，虽然一笔交易依赖于之前的多笔交易、这些交易又各自依赖于多笔交易，但是这并不存在任何问题。因为这个工作机制并不需要展开检验之前发生的所有交易历史。

#### 11隐私



传统的造币厂模型为交易的参与者提供了一定程度的隐私保护，因为试图向可信任的第三方索取交易信息是严格受限的。但是如果将交易信息向全网进行广播，就意味着这样的方法失效了。但是隐私依然可以得到保护：将公钥保持为匿名。公众得知的信息仅仅是有某个人将一定数量的货币发所给了另外一个人，但是难以将该交易同某个特定的人联系在一起，也就是说，公众难以确信，这些人究竟是谁。这同股票交易所发布的信息是类似的，每一手股票买卖发生的时间、交易量是记录在案且可供查询的，但是交易双方的身份信息却不予透露。

作为额外的预防措施，使用者可以让每次交易都生成一个新的地址，以确保这些交易不被追溯到一个共同的所有者。不过由于存在并行输入，一定程度上的追溯还是不可避免的，因为并行输入暗示这些货币都属于同一个所有者。此时的风险在于，如果某个人的某一个公钥被确认属于他，那么就可以追溯出此人的其它很多交易。

### 特点

比特币特征如下：

1、去中心化：比特币是第一种分布式的虚拟货币，整个网络由用户构成，没有中央银行。去中心化是比特币安全与自由的保证。

2、全世界流通：比特币可以在任意一台接入互联网的电脑上管理。不管身处何方，任何人都可以挖掘、购买、出售或收取比特币。

3、专属所有权：操控比特币需要私钥，它可以被隔离保存在任何存储介质。除了用户自己之外无人可以获取。

4、低交易费用：可以免费汇出比特币，但最终对每笔交易将收取约1比特分的交易费以确保交易更快执行。

5、无隐藏成本：作为由A到B的支付手段，比特币没有繁琐的额度与手续限制。知道对方比特币地址就可以进行支付。

6、跨平台挖掘：用户可以在众多平台上发掘不同硬件的计算能力。

**比特币优点如下：**

1、完全去处中心化，没有发行机构，也就不可能操纵发行数量。其发行与流通，是通过开源的p2p算法实现。

2、匿名、免税、免监管。

3、健壮性。比特币完全依赖p2p网络，无发行中心，所以外部无法关闭它。比特币价格可能波动、崩盘，多国政府可能宣布它非法，但比特币和比特币庞大的p2p网络不会消失。

4、无国界、跨境。跨国汇款，会经过层层外汇管制机构，而且交易记录会被多方记录在案。但如果用比特币交易，直接输入数字地址，点一下鼠标，等待p2p网络确认交易后，大量资金就过去了。不经过任何管控机构，也不会留下任何跨境交易记录。

5、山寨者难于生存。由于比特币算法是完全开源的，谁都可以下载到源码，修改些参数，重新编译下，就能创造一种新的p2p货币。但这些山寨货币很脆弱，极易遭到51%攻击。任何个人或组织，只要控制一种p2p货币网络51%的运算能力，就可以随意操纵交易、币值，这会对p2p货币构成毁灭性打击。很多山寨币，就是死在了这一环节上。而比特币网络已经足够健壮，想要控制比特币网络51%的运算力，所需要的cpu/gpu数量将是一个天文数字。

**比特币的缺点如下：**

1、交易平台的脆弱性。比特币网络很健壮，但比特币交易平台很脆弱。交易平台通常是一个网站，而网站会遭到黑客攻击，或者遭到主管部门的关闭。

2、交易确认时间长。比特币钱包初次安装时，会消耗大量时间下载历史交易数据块。而比特币交易时，为了确认数据准确性，会消耗一些时间，与p2p网络进行交互，得到全网确认后，交易才算完成。

3、价格波动极大。由于大量炒家介入，导致比特币兑换现金的价格如过山车一般起伏。使得比特币更适合投机，而不是匿名交易。

4、大众对原理不理解，以及传统金融从业人员的抵制。活跃网民了解p2p网络的原理，知道比特币无法人为操纵和控制。但大众并不理解，很多人甚至无法分清比特币和Q币的区别。“没有发行者”是比特币的优点，但在传统金融从业人员看来，“没有发行者”的货币毫无价值。

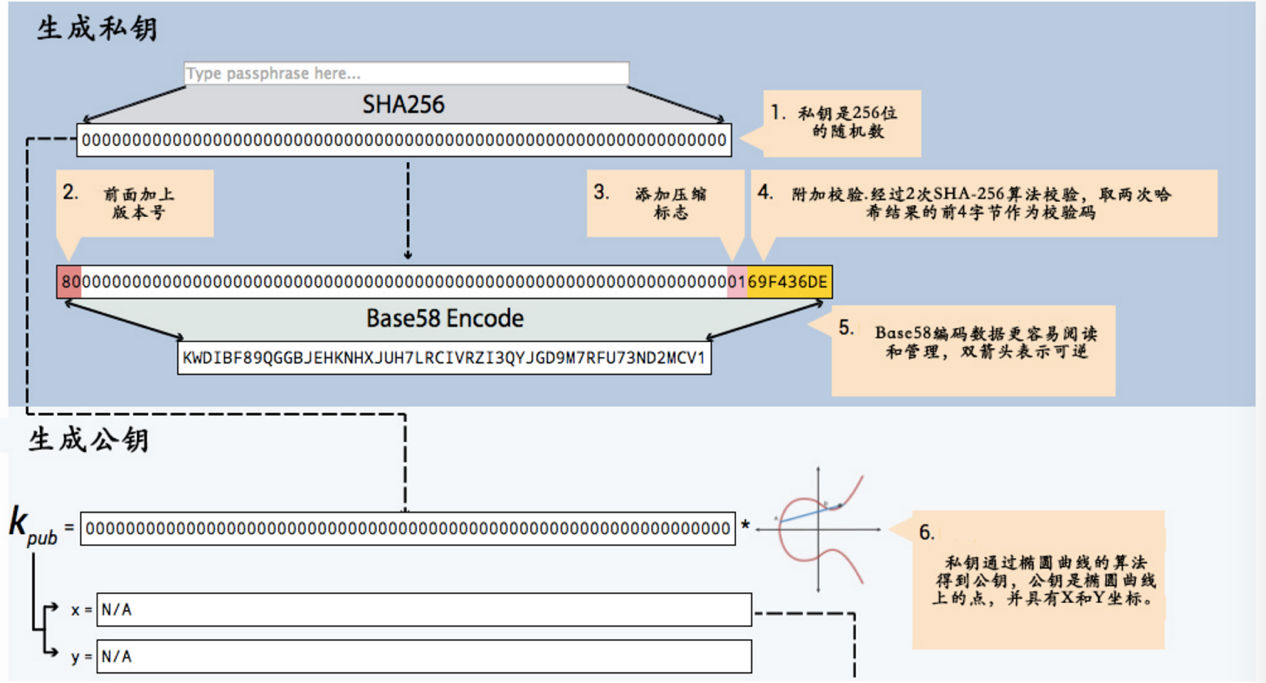
### 重要概念

#### 1比特币地址、私钥、公钥

地址：是为了人们交换方便而弄出来的一个方案，因为公钥太长了(130字符串或66字符串)。地址长度为25字节，转为base58编码后，为34或35个字符。base58是类似base64的编码，但去掉了易引起视觉混淆的字符，又在地址末尾添加了4个字节校验位，保障在人们交换个别字符错误时，也能够因地址校验失败而制止了误操作。

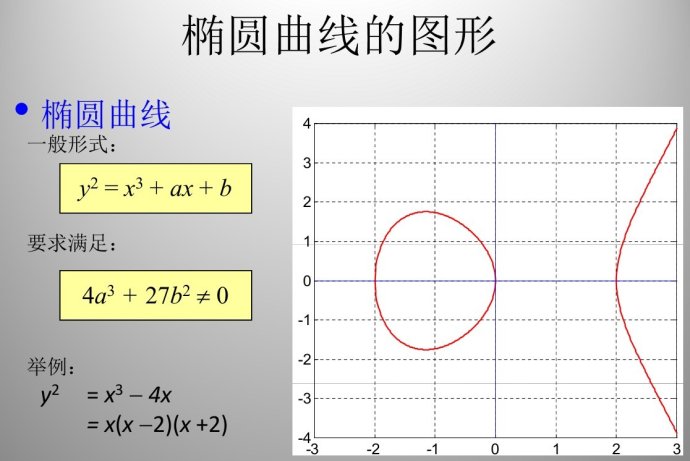
私钥：非公开，拥有者需安全保管。通常是由随机算法生成的，说白了，就是一个巨大的随机整数，256位、32字节。大小介于1 ~ 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4141之间的数，都可以认为是一个合法的私钥。于是，除了随机方法外，采用特定算法由固定的输入，得到32字节输出的算法就可以成为得到私钥的方法。

公钥：公钥与私钥是相对应的，一把私钥可以推出唯一的公钥，但公钥却无法推导出私钥。公钥有两种形式：压缩与非压缩。早期比特币均使用非压缩公钥，现大部分客户端已默认使用压缩公钥。这个貌似是比特币系统一个长得像feature的bug，早期人少活多代码写得不够精细，openssl库的文档又不足够好，导致Satoshi以为必须使用非压缩的完整公钥，后来大家发现其实公钥的左右两个32字节是有关联的，左侧(X)可以推出右侧(Y)的平方值，有左侧(X)就可以了。现在系统里两种方式共存，应该会一直共存下去。两种公钥的首个字节为标识位，压缩为33字节，非压缩为65字节。以0×04开头为非压缩，0×02/0×03开头为压缩公钥，0×02/0×03的选取由右侧Y开方后的奇偶决定。压缩形式可以减小Tx/Block的体积，每个Tx Input减少32字节。



#### 2椭圆曲线数字签名算法

椭圆曲线数字签名算法（[ECDSA](http://8btc.com/article-140-1.html)）是使用[椭圆曲线密码（ECC）](http://8btc.com/article-138-1.html)对数字签名算法（DSA）的模拟。ECDSA于1999年成为ANSI标准，并于2000年成为IEEE和NIST标准。它在1998年既已为ISO所接受，并且包含它的其他一些标准亦在ISO的考虑之中。与普通的离散对数问题（discrete logarithm problem  DLP）和大数分解问题（integer factorization problem  IFP）不同，椭圆曲线离散对数问题（elliptic curve discrete logarithm problem  ECDLP）没有亚指数时间的解决方法。因此椭圆曲线密码的单位比特强度要高于其他公钥体制。



数字签名算法（DSA）在联邦信息处理标准FIPS中有详细论述，称为数字签名标准。它的安全性基于素域上的离散对数问题。椭圆曲线密码（[ECC](http://8btc.com/article-138-1.html)）由Neal Koblitz和Victor Miller于1985年发明。它可以看作是椭圆曲线对先前基于离散对数问题（DLP）的密码系统的模拟，只是群元素由素域中的元素数换为有限域上的椭圆曲线上的点。椭圆曲线密码体制的安全性基于椭圆曲线离散对数问题（ECDLP）的难解性。椭圆曲线离散对数问题远难于离散对数问题，椭圆曲线密码系统的单位比特强度要远高于传统的离散对数系统。因此在使用较短的密钥的情况下，ECC可以达到于DL系统相同的安全级别。这带来的好处就是计算参数更小，密钥更短，运算速度更快，签名也更加短小。因此椭圆曲线密码尤其适用于处理能力、存储空间、带宽及功耗受限的场合

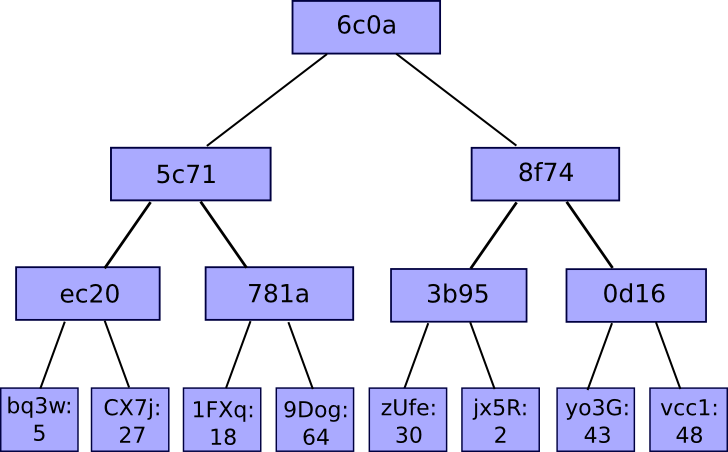
ECDSA是椭圆曲线对DSA的模拟。ECDSA首先由Scott和Vanstone在1992年为了响应NIST对数字签名标准（DSS）的要求而提出。ECDSA于1998年作为ISO标准被采纳，在1999年作为ANSI标准被采纳，并于2000年成为IEEE和FIPS标准。包含它的其他一些标准亦在ISO的考虑之中。

#### 3梅克尔树

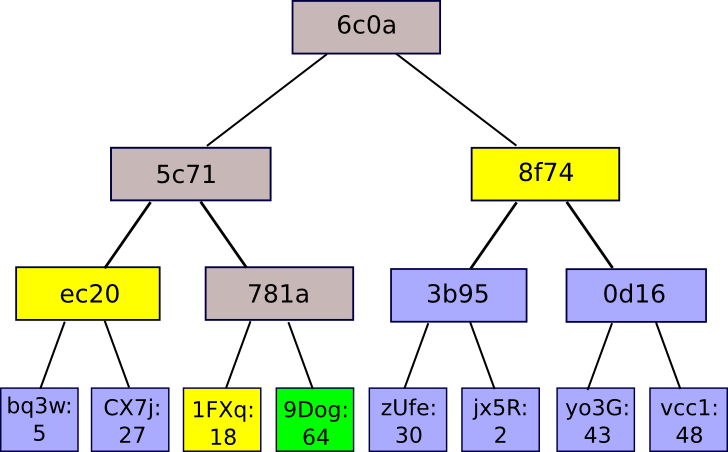
梅克尔树（Merkle trees）是区块链的基本组成部分。虽说从理论上来讲，没有梅克尔树的区块链当然也是可能的，你只需创建直接包含每一笔交易的巨大区块头（block header）就可以实现，但这样做无疑会带来可扩展性方面的挑战，从长远发展来看，可能最后将只有那些最强大的计算机，才可以运行这些无需受信的区块链。

梅克尔树，是哈希大量聚集数据“块”（chunk）的一种方式，它依赖于将这些数据“块”分裂成较小单位（bucket）的数据块，每一个bucket块仅包含几个数据“块”，然后取每个bucket单位数据块再次进行哈希，重复同样的过程，直至剩余的哈希总数仅变为1，即根哈希（root hash）。

梅克尔树最为常见和最简单的形式，是二叉梅克尔树（binary Mekle tree），其中一bucket单位的数据块总是包含了两个相邻的块或哈希，其描述如下：

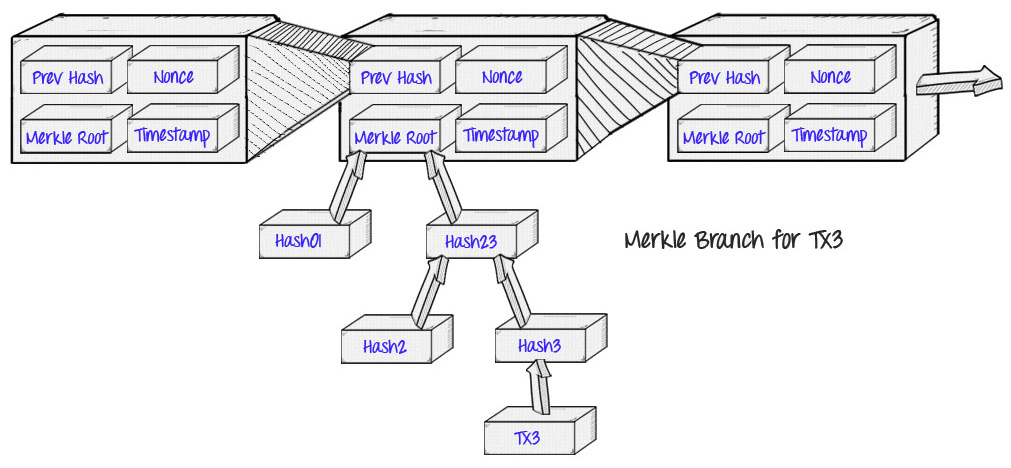


那么，这种奇怪的哈希算法有什么好处么？为什么不直接将这些数据块串接成一个单独的大块，用常规的哈希算法进行呢？答案在于，它允许了一个整齐的机制，我们称之为梅克尔证明（Merkle proofs）：



一个梅克尔证明包含了一个数据块，这颗梅克尔树的根哈希，以及包含了所有沿数据块到根路径哈希的“分支”。有人认为，这种证明可以验证哈希的过程，至少是对分支而言。应用也很简单：假设有一个大数据库，而该数据库的全部内容都存储在梅克尔树中，并且这颗梅克尔树的根是公开并且可信的（例如，它是由足够多个受信方进行数字签名过的，或者它有很多的工作量证明）。那么，假如一位用户想在数据库中进行一次键值查找（比如：“请告诉我，位置在85273的对象”），那他就可以询问梅克尔证明，并接受到一个正确的验证证明，他收到的值，实际上是数据库在85273位置的特定根。它允许了一种机制，既可以验证少量的数据，例如一个哈希，也可以验证大型的数据库（可能扩至无限）。

梅克尔证据的原始应用是[比特币](http://www.tuiunion.com/tuilink/redirect/8/?domain=www.btckan.com" \o "我要去比特币交易" \t "_black)系统，比特币区块链使用了梅克尔证明，为的是将交易存储在每一个区块中：



而这样做的好处，也就是中本聪描述到的“简化支付验证”（SPV）的概念:而不是下载每一笔交易以及每一个区块，一个“轻客户端”（light client）可以仅下载链的区块头，数据块大小为80字节，每个区块中仅包含五项内容：上一区块头的哈希值、时间戳、挖矿难度值、工作量证明随机数、包含该区块交易的梅克尔树的根哈希。

如果一个轻客户端希望确定一笔交易的状态，它可以简单地要求一个梅克尔证明，显示出一个在梅克尔树特定的交易，其根是在主链（main chain，非分叉链）上的区块头。

它会让我们走得很远，但比特币的轻客户确实有其局限性。一个特别的限制是，它们虽然可以证明包含的交易，但无法证明任何当前的状态（例如：数字资产的持有，名称注册，金融合约的状态等）。你现在拥有了多少个比特币？一个[比特币](http://www.tuiunion.com/tuilink/redirect/8/?domain=www.btckan.com)轻客户端，可以使用一种协议，它涉及查询多个节点，并相信其中至少会有一个节点会通知你，关于你的地址中任何特定的交易支出，而这可以让你实现更多的应用。但对于其他更为复杂的应用而言，这些远远是不够的。一笔交易影响的确切性质，取决于之前的几笔交易，而这些交易本身则依赖于更为前面的交易，所以最终你可以验证整个链上的每一笔交易。

https://blog.ethereum.org/2015/11/15/merkling-in-ethereum/

#### 4哈希现金

比特币使用一种名叫“哈希现金”（hashcash）的工作量证明算法，这种算法的出现早过比特币，最初创造这种算法的目的，只是使之成为反DOS攻击的工具。哈希现金的灵感来自于这样一个想法，即一些数学结果难于发现而易于校验。一个众所周知的例子是因数分解一个大的数字（尤其是因数较少的数字）。将数字相乘来获得它们的积的代价是低廉的，但首先找到那些因数的代价却要高得多。

对交互式协商来说，因数分解足以胜任。比如，希望客户端能象征性地为其付出代价方能访问在线资源。这个时候可以定义协议，首先服务器向客户端发送一个消息，说“只要您能因数分解这个数，我将让您得到这个资源”。没有诚意的客户端将无法得到我的资源，只有那些能够证明自己有足够的兴趣、付出一些CPU周期来回答这个协商的才能得到这个资源。

不过，有一些资源无法很方便地进行交互式协商。比如电子邮件反垃圾或者支付交易，怎么才能避免邮箱不被垃圾邮件所占据?“我并不介意陌生人给我写信，但是，我希望他们能以稍微认真的态度，亲自通过对我有价值的邮件与我取得联系。至少，我不希望他们是垃圾邮件制造者，那些人向我和上百万的其他人发送包含同样消息的邮件，期望我们中的某些人能购买某种产品或者落入一个骗局。”而对于电子货币，内容的复制几乎是没有代价的，如何保证电子货币（内容）没有被交易（发送）多次?这和反垃圾邮件是同样的问题。

哈希现金的解决方法就是：在电子邮件的消息头中，增加一个hashcash戳记（hashcash stamp）散列值；该散列中包含收件人地址、发送时间、salt值。该散列值特别之处在于它至少前20位必须是0才是一个合法的hashcash戳记。为了得到合法的散列值，发送者必须经过许多次尝试（改变salt值）才能获得。一旦生成戳记，不希望每一个给我发送邮件的垃圾邮件制造者都能重复使用它。所以，hashcash戳记要带一个日期，这样可以指定时间更早的戳记是非法的。另外哈希现金的接收端要实现一个重复支付数据库，用来记录戳记的历史信息。

http://8btc.com/article-2008-1.html

#### 5 51%攻击

一提到对比特币的攻击，大部分人想到的就是51%攻击。51%攻击是指掌握了比特币全网的51%算力之后，用这些算力来重新计算已经确认过的区块，使区块链产生分叉并且获得利益的行为。

他能够：

（1）修改自己的交易记录，并进行双重支付

（2）阻止区块确认部分或者全部交易

（3）阻止部分或全部矿工开采到任何有效的区块

但是他无法做到：

（1）修改其他人的交易记录

（2）阻止交易被发出去（交易会被发出，只是显示0个确认而已）

（3）改变每个区块产生的比特币数量

（4）凭空产生比特币

（5）把不属于他的比特币发送给自己或其他人

假如掌握了整个网络51%的算力，则可以计算出一个这样的区块链，包含我发送所有的比特币到我的私人账户上这个交易信息。这个区块链的长度为10，但是我不向网络广播；同时，我把所有的比特币在交易市场换成美元并提取出来，而且这笔交易记录在正常的那个区块链中。当我的美元提取正在进行中的时候，那个正常的区块链的长度是9，而我的区块链长度是10。现在我向网络广播出去，然后观察，网络会确认我的区块链是正确的。但是美元已经被我提取了，损失的是交易市场。

比特币发动51%攻击具体方法如下：

准备工作：

（1）既然是51%攻击，就必须首先掌握足够的算力，无论是控制矿池，还是利用其它计算资源，总之必须使你的算力领先与现在网络总算力，领先的幅度越大，成功的可能性越高；

（2）拿到足够的BTC作为筹码，无论是自己挖到的，还是从任何渠道买的，都可以；

攻击步骤：

（1）将手中的BTC充值各大交易所，然后卖掉，提现;或者也可以直接卖给某人或某一群人;

（2）运用手中的算力，从自己对外付款交易之前的区块开始，忽略自己所有对外的付款交易，重新构造后面的区块，利用算力优势与全网赛跑，当最终创建的区块长度超过原主分支区块，成为新的主分支，至此攻击完成。

攻击结果： 由于撤销了所有对外付款交易，等于收回来所有已卖掉的比特币。

过去几年比特币网络的算力悄无声息的增长到了无比之大，这大大增加了比特币成功的可能性。在依赖密码学的数字货币领域，先发优秀是非常明显的。所以51%攻击对于比特币来说并不是一个什么大问题（早在2013年7月，比特币全网算力已经达到世界前500强超级计算机算力之和的20倍），即使有政府集全国之力秘密造出一台超级计算机，用来击溃比特币来挽救自己的货币发行体系，它会发现使用该能力进行挖矿便可垄断比特币的发行权，其收益远大于击溃比特币，动机也就不复存在了。

#### 6冷钱包

一直以来，比特币行业的安全深受诟病，尤其2014年3月曾是世界最大比特币交易平台的Mt.Gox遗失总计65万枚比特币，2015年2月14日比特儿存钱罐丢失总额为7170BTC。比特币的理想是构建一种金融社交网络，实现人类的金融民主。时至今日，比特币的基础技术架构仍有很大的提升空间。比特币交易平台、在线钱包等如何安全的保存大量比特币是整个行业面临的重要问题。比特币的安全是基于比特币的核心加密算法和私钥的安全保存。密码学界认为比特币的密码学基础(SHA256和EDSA)在目前的解密技术能力下，是绝对安全的，比特币安全的主要问题就在于私钥的保存，所以业界通常采用冷钱包（绝对不接触互联网的钱包）来保存大量比特币.

什么是冷储存?

比特币钱包的冷储存（Cold storage）是指将钱包离线保存的一种方法。具体来说，玩家在一台离线的电脑上生成比特币地址和私钥，并将其妥善保存起来。以后挖矿或者在交易平台得到的比特币都可以发到这个离线生成的比特币地址上面。由这台离线电脑生成的私钥永远不在其它在线终端或者网络上出现。

为什么要使用冷储存?

使用比特币钱包冷储存技术主要是出于安全上的考量。举两个例子：

1、某比特币超级大户想保证他的比特币钱包绝对安全，即使在电脑被黑客入侵的情况下，黑客依然得不到比特币私钥。这样，这位大户就必须使用冷储存技术，他离线生成几对比特币地址和私钥，作为冷储存钱包，以后所有需要储存的比特币都发到这些地址上面。这样初步就保证了比特币的安全。

2、某比特币交易平台每天有庞大的比特币用户群，用户在平台上存有数以万计的比特币。为了保证这些比特币的安全，交易平台的管理人员便每天定时将主机服务器上所储存的比特币放入冷储存钱包中。而只在服务器上存有少量的比特币，来应付正常的提现请求，这样就算黑客入侵了交易平台主机也无法得到用户所储存的比特币。

如何进行冷储存？

( 一 ) 私钥产生和备份

1.在完全离线的电脑上生成10000个私钥和对应的地址。

2.在完全离线电脑上对私钥进行AES加密。

3.删除原始私钥。

4.AES密码由两个分属异地的人掌握。

5.把之前加密后的私钥和明文地址生成二维码加密文档。

6.通过二维码扫描完全离线电脑生成地址文档，用于日常使用，每次热钱包往冷钱包汇币，必须使用一个未使用过的地址，每个地址不可重复使用。

( 二 ) 线上往冷钱包打币

1.从地址文档中取相应地址，根据安全级别，每个地址汇不超过1000B。

2.每个地址被使用一次后就不可再使用。

( 三 ) 从冷钱包取币

1.把私钥密文通过二维码扫描放入完全离线电脑。

2.掌握AES密码的人在完全离线电脑上进行解密，获得私钥明文。

3. 通过二维码扫描把私钥明文导入另一台完全离线电脑。

4.在另一台完全离线电脑上进行签名交易，并把签名后的交易通过二维码或U盘同步至有网络的电脑广播交易。

#### 7闪电网络

比特币闪电网络（Bitcoin Ligtning Network）是一项针对比特币的设计改进，它可以让用户以去中心化的方式进行小额支付。通过在用户间增补哈希化时间锁合约（hashed timelock contracts）来解决比特币规模问题和立即支付问题。目前，该项目面临的首要问题是“软分叉”，即修改比特币协议，无效化之前的区块和交易，同时就节点依然可以识别新的有效区块。

与当今的金融系统相比，Visa在标准的节假日每秒处理4.5万笔交易，通常的一个营业日则为数亿次交易，然而比特币现在每秒约能支持7笔交易，同时还会受到区块链大小的限制。要想实现每秒4.5万笔交易，比特币必须进行离线处理。

闪电网络的工作原理可能听起来比较复杂，本质的工作原理非常类似于这个例子：假设所有的比特币交易能够在一个开放的论坛（比特币公共账）中探讨，闪电网络在特定时间段内可以让各方进入到一个密闭的房间（此段时间进行赊账交易），同时在合约时间结束时，在将那些交易广播到比特币网络上，这样可以保证区块链上保存最小化的信息，比特币闪电网络与现行的金融系统解决该问题的方式极为类似。

http://www.8btc.com/amiko-pay

#### 8多重签名

一般来说一个比特币地址对应一个私钥，动用这个地址中的资金需要私钥的掌握者发起签名才行。而多重签名地址，可以有三个相关联的私钥，你需要其中的两个才能完成一笔转账。实际上，你也可以设置成1/3，5/5，6/11，但是最常见的是2/3的组合。

多重签名托管工作原理如下：当Alice想要发送20元钱给Bob购买一个产品时，首先Alice挑选一个相互信任的仲裁员，我们叫他Martin，然后通过Alice，Bob，Martin三方多重签名来发送20元钱。Bob看到付款后，确认订单，邮寄商品。当Alice收到商品之后，她可以创建一个20元的多重签名给Bob，来完成这一笔转账。然后，Bob再对其进行签名，这样就完成了转账。另外，Bob可能会选择不发送产品，在这种情况下，他创建并签署20元的退款交易发送给Alice，让Alice可以签名并发布。那么，如果Bob声称已经发货，但是Alice拒绝付款呢？Alice和Bob就会联系Martin，让他来决定谁对谁错。Martin赞成哪一方，他就创建一笔给自己1元和对方19元的交易，并由对方提供签名，从而完成转账。

这种多重支付的方法需要一个中介机构来收取费用，那么它和Paypal相比好在哪里？首先，它是自愿的。在某些情况下，当你从一个有信誉的大公司购买东西，或者当你汇款给一个信任的账户时，中介机构是不需要的，普通的A转账给B就好了。其次，该系统是可以调整的。有时候，某些转账的仲裁员需要非常专业的知识才能够胜任。比如，你购买虚拟商品的时候，仲裁员最好就选择虚拟商品平台上的专业人士。在其他的时候，你可能就需要一个一般的仲裁员就够了，因为专业仲裁员的收费比较高。而且，市场上会产生专门的仲裁公司。通过多重签名技术，你可以每单交易轻松地选择不同的仲裁员，或者不需要仲裁员，这样就0手续费。

[http://bitcoinmagazine.com/11108/multisig-future-bitcoin/#](http://bitcoinmagazine.com/11108/multisig-future-bitcoin/)

#### 9合并挖矿

比特币工作量证明机制是指在矿工挖矿时，给区块补增一个随机数，并作随机哈希运算，使得给定区块的哈希值开头含有一定数量的零。一个简单的例子：

对短语“message”（不含引号）进行SHA256哈希算法加密，你会得到：

ab530a13e45914982b79f9b7e3fba994cfd1f3fb22f71cea1afbf02b460c6d1d

现在开始加入数据，直到你得到一个以0开头的哈希：

1message daad0bc80059253928621a10365de153e335a18f03b9dc7e7e25897fb791f023

2message 6532f42bd1d6ccd00f47c133c3ca1a0fc852598e67c62eb31adab8ceb3aaa680

...

51message 0985e57510d017b177867168642543ab4f143333ad63782680e812251ab3141e

51次运算后得到第一个有效的哈希。只要“51message”一发送，接收器可以迅速通过哈希运算来验证它是否符合要求。被添加的那部分数据（本例中的51），被称作随机数（nonce），关键在于该随机数可以是任何信息。

假设你在同时挖A币与B币，现在你有部分区块数据来自A币，部分区块数据来自B币，而且一个母随机数不断改变直到你找到一个区块。一旦你找到一个块，它就是一个对A币、B币两者同时有效的块链（假设两者的挖矿难度相等）。例如：

同时哈希以下数据：[A币区块数据|B币区块数据|公随机数]

当一个块被发现：

对A币广播区块>> [A币区块数据] +随机数= B币区块数据+母随机数]

对B币广播区块>> [B币区块数据] +随机数= A币区块数据+母随机数]

只要你愿意，你可以制造任意多的链。Slush矿池2011年就已经合并挖比特币与域名币（Namecoin）。

合并挖矿的好处有：1）同时为两个区块链贡献哈希计算力，有助于提高两个区块链的安全性。2）挖矿的回报更高，消耗相同的电力的情况下，同时采两种货币，如果你不喜欢域名币，可以把它卖掉换成比特币。

#### 10彩色币

通过仔细跟踪一些特定比特币的来龙去脉，可以将它们与其他的比特币区分开来，这些特定比特币就叫作彩色币（Colored bitcoins）。它们具有一些特殊的属性，比如支持代理或聚集点，从而具有与比特币面值无关的价值。彩色币可以用作替代货币、商品证书、智能财产以及其他金融工具，如股票和债券等。

比特币的P2P支付结算系统已经安全建立，可以实现可靠的近乎免费的转账，比特币网络（协议）本身是安全、稳定的，但比特币生态的服务提供商比如汇率市场却被黑客攻击多次，这损害了比特币的声誉和交易价值。有没有一种办法可以利用安全可靠的比特币自身协议，来创建分布式的汇兑交易呢？

BitcoinX就是这样一个基于比特币的开放标准协议，就像HTTP和BitTorrent，用来规范互联网的价值交易。基于BitcoinX协议，你不旦可以在分布式、安全的云平台上持有比特币，还可以持有黄金、欧元、美元或各种证券资产。这意味着人们可以使用金融工具自由交易，如果某个节点G持有黄金，另一个节点E持有欧元，他们可以一种安全、透明、直接的方式相互兑换，而不需要第三方的介入。

BitcoinX的设计思想是将比特币网络（技术）与货币价值分割开来，并使用比特币网络技术来明晰交易来路以避免重复消费。通过创世转账来建立一个新货币（即彩色币），创世转账是一定量的比特币转账，这些比特币金额将用来赋予所有这种新货币的价值。这一定量比特币发送到的那个地址就是新货币的起源地址，它将控制新货币的初始分配。

彩色币客户端就是通过一种特殊的方法来计算资金平衡的轻量级客户端。

首先，我们发现所有的转账最后一个地址就是客户端地址，我们抓取区块链，查看这些转账是否是来自创世转账。

如果是，我们对交易金额乘以初始分割率，这样我们得到用户余额：

初始分割：0.00001BTC = 1 彩币（假设）

彩色币客户端是分布式的，然后围绕特定的创世转账创建一个社区，这就创造了一个独立的与比特币网络无关的“彩色币”生态，这个小的经济生态的波动建立在对比特币的基础设施的利用之上。

由于彩色币也是普通比特币，故它们也可以使用比特币网络，从一个地址传送到另一个地址。

因为我们有办法识别彩色币，所以它们相当于稀有货币，因此它们的价值取决于用户对这种稀有货币的需求，而与比特币价值无关。

彩色币怎样进行初始分配呢？在货币创世时，彩色币起源地址拥有该币的总体价值。在分配结束时，所有的货币价值将从起源地址转移到每个客户端。

在实际应用中，彩色币拥有者将不会知道货币总量有多少，此外，拥有者也不必知道想参与他的经济的人有哪些。在这种情形下，他可以建立一个邀请系统，每一个新的客户端都可以邀请其他客户端加入。实现这种技术还有很长的路要走，比如社交网络身份验证、社交图谱搜索、担保系统、短信验证、独特的IP地址、物理识别等，这些方法可最大量减少在初次分配中的欺诈。

## 区块链

### 1.2.1区块链是什么？

区块链是一种去中心化的、不可篡改的可信的分布式账簿，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。

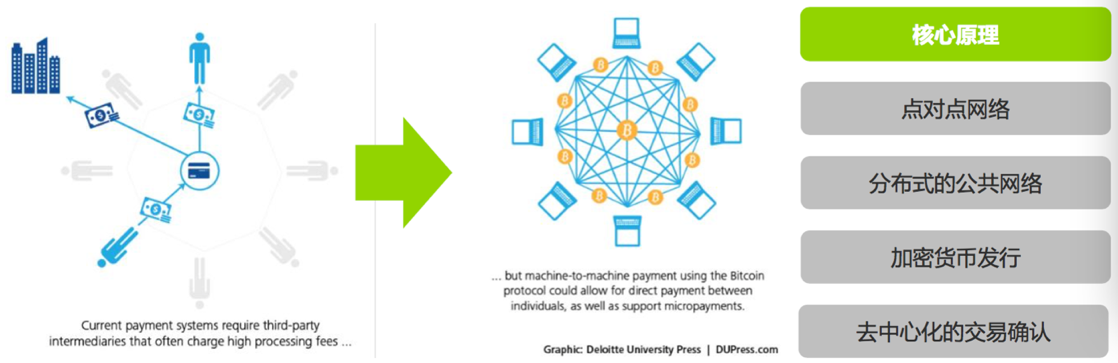
区块链的特点如下：

（1）高度安全，不可篡改的分布式账簿

（2）存在于互联网，向所有用户公开

（3）帮助人与人，物与物之间实现点对点的交易和互换

（4）无需第三方的介入即可完成价值的交换



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。



### 1.2.2区块链历史

#### 1重要里程碑

2008年：化名为中本聪的人发表了论文《比特币：一种点对点的电子现金系统(Bitcoin: A Peer-to-Peer Electronic Cash System)》，首次提出区块链的概念。

2009年：比特币开始在一个开源的区块链上运行，这是人类历史上的第一个区块链，比特币是区块链的首个应用。

2012年：瑞波(Ripple)系统发布，利用数字货币和区块链进行跨国转账。

2013年：9月，美卡币(MEC)区块链发生断裂，数据更新中断1天后，发布新版本，重新接回一条区块链，艰难复活。

2014年：4月，奥斯汀·希尔(Austin Hill)和亚当·贝克(Adam Back)披露，开始在比特币区块链的基础上打造侧链(sidechain)；5月，Storj宣布将采用区块链技术为客户提供去中心化的存储服务；6月，搜索引擎DuckDuckGo接入区块链查询；8月，Coinbase收购区块链信息浏览服务商Blockr.io，区块链API服务提供商Chain获950万美元A轮投资；10月，Tilecoin团队发布首个集成区块链技术的物联网实验设备。

　　2015年：大量银行和传统金融机构开始测试区块链技术，包括在内部系统上使用比特币区块链系统和瑞波币系统。

#### 2应用发展历史

Melanie Swan在其著作《BLUEPRINT FOR A NEW ECONOMY》中将区块链的应用范围划分成三个层面，分别称其为区块链1.0、2.0和3.0。

（1）区块链1.0：可编程货币

区块链技术伴随比特币的产生而产生，其最初应用范围完全聚集在数字货币上。[比特币](http://www.tuiunion.com/tuilink/redirect/8/?domain=www.btckan.com)的出现第一次让区块链进入大众视野，而后产生了莱特币、以太币、狗狗币等“山寨”数字货币。可编程货币的出现，使得价值在互联网中直接流通成为了可能。区块链构建了一种全新的去中心化的数字支付系统，随时随地的货币交易、毫无障碍的跨国支付以及低成本运营的去中心化体系都让这个系统变得魅力无穷。这样一种新兴数字货币的出现，强烈地冲击了传统金融体系。

（2）区块链2.0：可编程金融

 受到数字货币的影响，人们开始将区块链技术的应用范围扩展到其他金融领域。基于区块链技术可编程的特点，人们尝试将“智能合约”的理念加入区块链中，形成了可编程金融。有了合约系统的支撑，区块链的应用范围开始从单一的货币领域扩大到涉及合约功能的其他金融领域。彩色币、比特股、以太坊、合约币等新概念的出现，让区块链技术得以在包括股票、清算、私募股权等众多金融领域崭露头角。目前，许多金融机构都开始研究区块链技术并尝试将其运用于现实，现有的传统金融体系正在被颠覆。

（3）区块链3.0：可编程社会

随着区块链技术的进一步发展，其“去中心化”功能及“数据防伪”功能在其他领域逐步受到重视。人们开始认识到，区块链的应用也许不仅局限在金融领域，而是可以扩展到任何有需求的领域中去。于是，在金融领域之外，区块链技术又陆续被应用到了公证、仲裁、审计、域名、物流、医疗、邮件、鉴证、投票等其他领域中来，应用范围扩大到了整个社会。在这一应用阶段，人们试图用区块链来颠覆互联网的最底层协议，并试图将区块链技术运用到物联网中，让整个社会进入智能互联网时代，形成一个可编程的社会。

借鉴Melanie Swan的思路，区分了区块链1.0、2.0和3.0，但其实这三个层面并非区块链技术发展程度上的变化，而仅仅是应用范围的逐步扩展。区块链技术本身在所有的应用中均有体现，发挥了各自领域应有的作用。

### 1.2.3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。 |

### 1.2.4区块链形态

数字货币、虚拟货币的圈子里永远不乏吵，比特币社区中为了扩容问题吵得不可开交，将区块链技术从中脱离开来后，关于使用何种类型的区块链，公有链和私有链孰优孰劣的争执，一时也甚嚣尘上。这里我们就来好好地来场华山论剑，看看到底谁是“链中之王”。

实际上，我们要对比的区块链形态有三种：公有链、联盟链、私有链。联盟链介于公有链和私有链之间，实质上仍属于私有链的范畴，因此公有链的支持者对另外两者态度一致的反对。在他们眼里，这就是Permissionless VS Permissioned。

我们先来介绍下这三种部署方式不同的区块链：

公有链：任何人都能读取区块链信息，发送交易并能被确认，参与共识过程的区块链。是真正意义上的去中心化分布式区块链，比特币区块链即是公共链最好代表。

联盟链：根据一定特征所设定的节点能参与、交易，共识过程受预选节点控制的区块链。被认为是“部分去中心化”或“多中心化”的区块链，R3组成的银行区块链联盟要构建的就是典型的联盟链。

私有链：写入权限仅在一个组织手里，读取权限可能被限制的区块链。私有链没有去中心化特点，但具有分布式特点。私有链对公司政府内部的审计测试、以及银行机构内的交易结算有很大价值。

下表所示的是不同区块链的主要差异。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 去中心化程度 | 权限和范围 | 经济奖励 |
| 公有链 | 完全去中心化 | 全球范围可以访问、交易 | 个人从中可获得的经济奖励，与对共识过程作出的贡献成正比。 |
| 联盟链 | 部分去中心化 | 读取、交易权限可设定 | 未知 |
| 私有链 | 中心化 | 写入权限仅在一个组织手里，读取权限可能被限制 | 不需要奖励，可能没有虚拟货币。 |

可以看出，联盟链和私有链相比公有链中心化程度不断提高，权限则越收越紧。和完全开放、无许可必要的的比特币公共链不同，联盟链和私有链在信息公开程度和中心控制力度方面有所限制，这些限制可以帮助区块链满足不同类型的应用需求。

公有链和私有链在其他方面也有着共同的优点。尽管随着范围的缩小，有人怀疑私有链的安全性，但两者基于共识机制来保证的系统安全性仍然十分可信；区块链的不可篡改性和可追溯性特点在公有链和私有链上都有体现。

下面来分析下公有链和私有链的优缺点：

公有链的优势：

开放

成功经验

潜力

理想乡

开放：

如互联网一样。不设限的读取、交易权限，面向全球开放，

互联网已经告诉了我们，突破性的技术通常都是建立在一个公平竞争的开放协议层中，任何人都可以对其进行创新。网络的开放性让一切皆有可能。历史表明，开放的技术总是能够战胜封闭式花园的做法，是共识合并孤岛，而非孤岛自成大陆。

开放还从另一面维护了系统的安全性。如此大规模的公有链可有效抵御双花攻击。以比特币为例，当前情况下要进行双花攻击的资金总额在50亿美金以上，因此，从经济角度说，任何的攻击收益都低于这个数额，且攻击收益随着比特币算力的增长而越来越低，攻击没有任何意义。

成功的经验：

以比特币为例，今年是比特币的第八年，八年来这场“人类历史上最大的社会经济实验”并没有崩溃，没有双花，没有宕机，没有一笔交易出错。这足以证明公共区块链的稳定。在银行业看来，无间断运行的特性正是比特币区块链中最具参考价值的因素之一。有了这些基于比特币的开发工作，加上比特币区块链自身也存在后续变革，以吸收新兴区块链优点，同时改进自己的不足的可能，公共区块链基础设施将变得更加可靠和可扩展。

潜力：

在隐私、扩展性，交易速度等方面，公有链还有很大潜力可挖。

公共区块链的隐私将通过使用“零知识证明”得到进一步提升：零知识证明，指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明实质上是一种涉及两方或更多方的协议，即两方或更多方完成一项任务所需采取的一系列步骤。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。除了声明的有效性，这个验证方法并不会透露出其他的信息。

在未来，在公共区块链上构建私有业务也是有可能的，就好比现在能通过网络来构建安全的电子商务交易一样。

随着未来区块链上智能合约的发展，区块链的扩展性将会有质的提升，届时公有链将会成为全球范围内的下一个互联互通的网络。

理想乡：

公有链完全公开、不受控制，并通过加密经济来保证网络安全，这是很多追求自由的人心中的乌托邦。有人会嘲笑追求完全去中心化的信徒们，但公有链的确给了美梦成真的机会。因此它也会吸引那些不满足当下监管和中心化的金融市场，或者缺乏相关服务的人群和爱好者。

公有链的劣势：

分化严重

影响节点

匿名问题

隐私问题

去中心化社区分化严重：

矿池算力占全网算力比例的不断上升，使得比特币的共识机制蒙上了阴影。区块扩容的方案也几乎使比特币社区分裂，这一规则更改的过程也让许多人明白所谓去中心化的比特币，在重大议题上还是需要参考核心开发者和算力大的矿池，这就偏离了去中心化的初衷。

影响节点：

公有链在存储容量和能耗上对各个节点影响很大。

由于区块链需要所有节点备份整个账本，公有链的大范围此时便成了绊脚石。区块链本身存储效率偏低且检索效率不高，全网的交易数据的增加以及今后智能合约的执行，会增加对节点内存和存储空间的压力。这会对面向大众的公有链的发展有影响，当然这也是私有链需要解决的问题。

确认时间长和能量消耗大是PoW带来的两个问题。尤其是因为全球网络广播，公有链的交易确认时间，一般情况下会比私有网络更长。此外为了实现共识而产生的大量能耗，也削弱了公有链降低成本方面的优势。上交所专家朱立曾在评价区块链在金融交易层面的前景时说，公有链的应用方面，区块链的低吞吐量、高时延可能将长期存在，无法支撑海量的证券交易、信用卡转账等实际金融业务规模。

匿名带来的问题：

完全匿名会带来监管的问题，成为滋生犯罪的温床。因为隐蔽性强、不可追踪的特点，比特币往往和外汇转移、恐怖组织融资、逃税等有紧密联系。这种联系也让各国监管层对其颇为警惕。例如，匿名性强的比特币能够在被称为“暗网”的网络集市上进行敲诈勒索，购买毒品和雇佣杀手等行为，著名暗网黑市“丝绸之路”大多交易都用比特币支付，难以追查，留下了监管的黑洞。

匿名也有可能对反洗钱带来很大的挑战，区块链去中心化性质并不符合传统监管模式。因此公有链难以作为金融机构的解决方案，原因就是像比特币区块链这样的公共区块链，是不可能在发行链下资产方面既具有免审查性又具有法律权威性。

隐私问题：

与匿名问题相对的是隐私问题，尽管每个节点背后的身份是匿名的，但是节点与节点之间的交易是全网公开并广播的。这就带来一个问题，当匿名问题被解决后，交易双方的记录就完全暴露在全世界的眼中，这很难令人接受。这意味着区块链上一个智能合约中的非参与者可以囤积或者卖掉某一资产，因为他们获得了智能合约上公开的信息。

此外，交易信息的公开也会影响金融交易，失去了信息不对称的优势将大大削弱金融机构的盈利能力。在华尔街的银行家眼中，真正“去中心化”的清算模式，将会让他们失去在“信息不对称”情况下所带来的优势，也随之失去“左手倒右手”的赚钱能力。

私有链的优势

前景广阔

博采众长

减少威胁

灵活

前景广阔：

区块链给建立一个成本很低且能够防止篡改的公共数据库提供了完美的解决方案。

区块链作为金融机构结算、追溯等问题的解决方案，发展很有前景，甚至会有颠覆性的影响。

基于区块链的支付系统更快、更安全、性价比更高。通过区块链，我们同样可以加强监督，提高透明度。

而在金融机构等需要权限设置的场合，私有链能更好的契合金融界人士的痛点。在公证、审计、物联网甚至投票等方面，私有链都可以给出解决方案。

博采众长：

私有链仍能保留着区块链真实性和部分去中心化的特性，并且在此基础上可以创造出访问权限控制更为严格，修改甚至是读取权限仅限于少数用户的系统。兼有去中心化和中心化的特点。

减少被攻击的威胁：

由于存在权限设定和准入机制，区块链的节点基本可以确保无害，相对透明的熟人圈减少了作假和攻击区块链的可能性，权限控制也能减少风险。

不同于公有链的全网公开，私有链参与者即便拥有整套加密账簿，通过加密私钥也只能浏览与其相关的交易并确保安全——所有交易会以加密形式登陆，包括时间、日期、参与者等。交易一旦入账，不可被删除、撤销或修改。

灵活：

针对不同的应用场景，不同的私有链可以灵活调节自身。读取权限，交易权限和验证权限可根据需要修改，已应对隐私、追溯、管理的问题；各个节点可以自定义定制，由于接入节点少可适当加大区块链对节点的负担，以提高可拓展性和安全性；经济激励机制在有些场合可以省略，挖矿机制也可以被其他方法取代以减少能耗，提高效益。

私有链的劣势：

封闭

银行界创新能力令人怀疑

信任问题

丧失核心特性

封闭：

从不同节点间不同权限的角度看，历史选择了各节点平等的互联网，每个节点权限不一致很容易招致反感。从私有链覆盖的范围看，互联网的规律是共识合并孤岛，而不是孤岛自成大陆。私有链单独自成体系会引起互联网的抵制。

“大公司们迫切地追求不需要比特币的区块链，这像极了1994年：离开了互联网，我们能够上网么？”

——马克·安德森（Marc Andreessen），著名的风险投资家，早期Web浏览器Mosaic的发明者

银行自身创新能力：

垄断的机构、企业不思进取，疏于改革，转身缓慢是很多人看衰的地方。除了创新动力不足外，金融界在对自身改革上也有着先天不足，一方面金融监管和银行间合作困难，另一方面银行创新速度慢，无法迅速整合资源。

私有链的技术障碍，例如隐私问题，只有通过所有参与者的高度协作才能解决。不过，在高度竞争的金融市场，要实现这一点并不容易。

尽管银行可能会尽量朝着区块链技术发展，但是他们会发现传统信息传递系统对结算策略执行所需的信息保密性，高吞吐量和可靠传输的要求还是可以满足的，这时他们就可能缺乏了运用区块链创新的动力。考虑到不断拖延的时间表以及各种艰巨的障碍，可能会存在这样的风险：银行会对区块链失去兴趣，并决定追求一些没那么耀眼的技术，或者继续固步自封。

信任问题：

当参与区块链的节点输减少，节点身份被预置，节点权限不一，很多人就会担忧私有链的诚实问题。是否会存在联合起来控制私有链，影响区块链的信任程度的可能性？

尽管区块链被视作“信任的机器”，但一旦它的成员中出现一个控制率非常高的团体，或一组串通勾结的团体，区块链就会开始有问题。因此很有可能仍需要引入传统的信任\监管机制，这将会大大削弱区块链的效率。

此外，规模较小的私有链很难证明没有“隐藏的可替代区块链”的存在，难以抵御双花攻击。

丧失核心特性：

区块链的核心特性是去中心化、去中介化、无须信任系统、不可篡改性和加密安全性。当参与范围，权限大小被控制限定，随意更改区块链的规则，以上的几个特性是否依旧存在就要打上一个问号了。学界甚至有专家将私有链看作“共享式数据库一个令人困惑的别名而已”。

主导私有链取代公有链这一进程的主要是金融界。区块链技术及其复杂，也极富争议性。包括被德勤认为最具颠覆性意义的区块链支付应用，也被认为可能威胁银行的地位。因此德勤提出，各银行间应加强合作，共同应对这个挑战，转向区块链技术尚未深入的领域。比如第一个区块链金融财团联盟R3 CEV，现在已有数十家金融巨头，合作紧密，积极推动区块链在银行界内的运用。R3正在着手为区块链技术在银行业中的使用创建区块链代码、制定行业标准和协议，并称将在一年内启动其区块链项目，银行可以通过使用这种通用共享账本技术，大幅减少协调成本。

2月初，央行行长周小川接受财新专访时，也对区块链表明了理性务实的开放性态度。

将区块链技术从比特币中分离出来后，金融界人士迫切希望能将其运用到自身环境中，而对比特币界所期待的去中心化、自由货币的乌托邦并不在乎。全国人大常委、财经委副主任吴晓灵，就在中国互联网金融协会举办的首次培训会上表示，央行提到的数字货币和现在基于区块链的数字货币不完全一样，后者是无中心的，而央行的是有中心的，“尽管用的是同样的信息技术，但发行、运作的原理不一样，这方面还有很多问题、很多工作需要我们去探讨”。今年年初，英国政府发布了一份名为《分布式账本技术：超越区块链》的报告，提到英国政府计划开发一个为政府管理提供服务的“中心化”的分布式账本系统，而非“去中心化”。这意味着英国政府并未接受区块链技术的去中心化。

中国和英国同时在区块链的中心化问题上发声，表明央行、政府、法定货币等方面是不会运用去中心化的区块链的。

中心化与去中心化，新旧金融体系之间的博弈，这都是争论缘起的原因。

有一个有趣的现象，国外的比特币从业者，或是计算机科学家大多反对联盟链和私有链，而金融界人士支持比特币的人居多。可以说两方都是某种程度上的既得利益者，比特币从业者在比特币，也就是公有链上投注了大量心力，公有链向私有链的转变必然会影响他们的利益；金融界人士也不希望坐视公有链领导的去中心化、去中介化革了银行、交易所等的命，因此提早在区块链上布局，希望借此新技术维持金融机构的领导地位。

理性的声音：

除去两派人士的论战的喧嚣，业界还是存在冷静的声音呼吁大家理性看待这一问题。其中的代表就是以太坊的创始人VItalik Buterin和《经济学人》杂志。

Vitalik Buterin是以太坊的创始人，以太坊于2015年7月上线以来的迅速崛起，是基于区块链技术上进行智能合约应用开启无限可能性的代表案例。作为另类区块链中的优秀改进，以太坊致力于打造一个提供超强图灵完备脚本语言的优秀底层协议。在该协议的基础上，用户可以创建任意的高级智能合约、众筹协议、货币、投票、公司管理或其他去中心化应用。

尽管年纪轻轻，Vitalik Buterin的观点却十分有前瞻性，他很早就看到了比特币和基于比特币区块链改良的币在实现多样化功能上的困局，因此希望在底层布局，建立一个用于实现区块链广泛应用的协议。以太坊这一平台的建立，正是他将区块链领域的资源团结整合起来的方法。在2014年的最后一天，他在自己的博文《在孤岛上》这样写道：

“即便数字货币社区的人们不会全都团结起来站在“比特币”的旗帜下，有一点还是值得争论的，那就是我们需要以某种方式团结在一起，努力建立一个更加统一的生态系统。“

“对生活，对数字货币界以及等等事情来说，如果比特币不足以强大到成为一个切实可行的支柱，那我们为什么不建立一个更好的以及更加可升级的分布式系统来替代它，并且在新的系统上重建每一样东西？”

——Vitalik Buterin

《纽约时报》的文章将以太坊看作一种可与比特币匹敌的虚拟货币，但Vitalik Buterin的初衷并不是再造一个比特币，智能合约和对搭建私有链的支持才是以太坊的核心竞争力。2015年8月份，他在博客上也专门写到了对公有链和私有链的看法。不同于其他非金融界的区块链圈内人，他没有一棒子把私有链打死，而是很客观的通过分析需求来分析两种区块链的存在意义。

“任何事物从任何角度分析，讲都是一个成本效益分析。如果用户们想要专门用来执行特定功能的特定网络，那么网络将会为此而存在，如果用户想要一个执行通用目的的高效网络，它同样会存在。”

“金融机构对这种系统有着很大的兴趣，这也导致了部分人的激烈反对，他们认为这样的发展，是违背了去中心化的本质，这是那些守旧落伍的中间商们孤注一掷的行为（或者说只是简单地提出了一个非比特币的错误应用）。然而，对那些仅仅是因为想更好造福人类，或者只是继续寻求为客户提供更优质服务的人们而言，公共和私有区块链有什么实际差别呢？”

他引用David Johnston（Dapps Fund Managing Director）的比喻来解释这种共存，“区块链就好像程序语言：他们彼此都有自己的特殊属性，并且从程序语言的历史上来看，很少有程序员能够虔诚的遵循唯一一种语言。我们会具体问题具体分析，使用最适合的方法。”

具体情况具体分析，因地制宜因势利导，这是Vitalik Buterin的观点。

《经济学人》对区块链的态度也不是非黑即白，2015年10月底，《经济学人》刊登了使区块链技术广为人知的封面文章《区块链，信任的机器》，明确将区块链技术从比特币“不好的名声”中抽离出来，提及了多项区块链在私有链方向的应用。

“这一创新，其承载的延伸意义已经远远超出了加密货币这个范畴。区块链让人们可以在没有一个中央权威机构的情况下，能够对互相协作彼此建立起信心。简单的说，它是一台创造信任的机器。”

“区块链是一个貌似平凡的过程，但是有潜力改变人们和企业之间互相协作的方式。比特币狂热分子已被纯粹的自由意志给迷住了，即数字货币能够超越任何央行的这种理想。真正的创新不是数字货币本身，而是铸造出它们的信任机器，而它的希望远远不仅如此。”

文章中提到“在一个分布式的系统里面，没有信任的地方，区块链就发挥作用了。”，这与Vitalik Buterin不同需求对应不同区块链类型的想法不谋而合，不拘泥于类型，而是专注于适应应用场景。

当然《经济学人》也不是一边倒的打压公有链（比特币），偏向私有链，在2016年3月份刊登的文章中，就表达了银行界对区块链技术过度狂热的担忧。

“在技术最终得到应用前，过高的期望会带来失望。”

即使区块链会深刻地改变社会，这个技术也必然需要经过时间的磨炼，需要不断地进行发展，需要探寻如何和现实世界相结合。现在的区块链技术，有些像是早起的互联网时代，现在来谈Web2.0或许为时尚早。《经济学人》这篇文章只不过再次提醒我们，我们经常会高估技术短期内产生的影响，而低估长期可能产生的影响。

我们认为，公有链和私有链并非是非黑即白的对立关系，关键还是要针对特定的应用场合的需求，选择合适类型的区块链。橘生淮南则为枳，强行推崇、推行单一的区块链体系只能无功而返，因地制宜才能解决问题。

随着区块链技术的快速发展，不排除以后公有链和私有链的界限会变得比较模糊。因为每个节点都可以有较为复杂的读写权限，也许有部分权限的节点会向所有人开放，而部分记账或者核心权限的节点只能向许可的节点开放，那就会不再是纯粹的公有链或者私有链。

目前国内外对区块链技术都处于初创和研究阶段，尽管有来自监管者的关注和积极讨论，但区块链到底如何应用仍是关切者的共同疑问。若是为区块链而区块链，反而因为过度设计，丧失了使用新技术的意义。

比特大陆联合创始人吴忌寒认为，目前市场的情绪是，总感觉很多问题可以通过区块链技术来得到解决，但是实施起来还是困难很大。主要的困难应该不是技术上的，还是其经济意义。中国的区块链应用必须找到能够为客户切实创造价值的应用场景才会成功。

对于公有链，对于一些全民参与的应用场合，例如医疗、公证、彩票等方面，就有它独特的优势。而像投票、民调、去中心化自治公司、组织等方面，还是需要政治环境发生改变，公众认可程度提高之后才能提上议事日程。同时在搭建公有链时也需要考虑到成本、可控性、实用程度等方面

实际上，公有链技术实现后能惠及的人群的想法，正是公有链发展最大的障碍。在行业外，区块链还不被人所熟知，人们很难完全将信任票投给这个解决信任问题的技术。

不被熟知的公有链的竞争对手是概念深入人心的中介们。事实上像房屋中介、UBER等中介（此处称UBER为中介不太恰当，可以理解为一种目录化的公司），基于互联网的发展，已经对自身进行了全面的改造，减少了费用，提高了方便程度，并且建立了评价机制，足以满足公众的需求，在人们心中树立了良好的口碑，那么公有链在这些方面就有些无可奈何。所以公有链在应用上很难立刻撼动中介行业中现有的几座大山，彻底的去中介化也很难实现。

同样，公众对完全去中心化并不感兴趣，对他们而言最重要的是便利。

以支付为例，支付宝之类的第三方支付短期内足以满足人们的需求，也许区块链建立的去中心化支付机制有些更好的地方，但这不足以使民众大规模地更换支付系统。

就如同互联网上千千万万个节点都是离散的，但最后人们还是需要门户网站、社交平台等中心将彼此相连。这样的观念无所谓对或错，只是现阶段不接纳完全去中心化，这需要时代的变迁，社会的发展。现今区块链的发展还将会是缓慢渐变的，由内而外的。量变引发质变，当人们逐渐改变了观念，那时就是公有链时机成熟，大放异彩的时代。

而私有链，由于范围小，可以率先在较小的圈子中进行实验，不需要得到全民的理解和认可，只需要参与者的认同。IT界、金融界、企业界中的有识之士意识到区块链的颠覆性意义后，便可以立即搭建私有链在行业中落地发展，这样更多的应用机会也促进了私有链的发展。

私有链的灵活性也使得它在实际落地的过程中较公有链占优势。根据不同的应用场合，所需特性不同，会需要定制化强的区块链服务，这样的市场中就需要有做BaaS（区块链即服务）的企业来提供个性化部署区块链的解决方案。区块链即服务”即把区块链当做一个基础设施，并在上面搭建各种满足普通用户需求的应用，我们的链将成为一个半开放的平台，不仅可以为企业级的B端客户进行服务，并且，可以帮助整个产业链上的品牌或商家进行供应链管理、产品追溯、以及嫁接在透明供应链平台上的商业智能合约应用。

综上所述，我们认为今后私有链的发展可能会领先公有链一步，会更早解决自身的不足，吸纳公有链的优点。而不同的私有链也会有针对不同应用场合，发展出自己的特色。链遍江湖，链链不同。

### 1.2.5共识机制

目前主流的共识机制有POW、POS、DPOS，还有瑞波和恒星的共识协议,以及以太坊的共识协议等。

#### 1工作量证明机制POW

工作量证明POW，就是我们所熟悉的挖矿，通过与或运算，计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储。

该机制的优点：完全去中心化，节点自由进出。其缺点也很明显，目前比特币已经吸引全球大部分的算力，其它再用工作量证明共识机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿也造成大量的资源浪费；共识达成的周期较长，不适合商业应用。

#### 2股权证明机制POS

股权证明POS（Proof of stake）就是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。

#### 3瑞波共识机制

瑞波共识算法，使一组节点能够基于特殊节点列表达成共识。初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由51%的该俱乐部会员投票通过。共识遵循这核心成员的51%权力，外部人员没有影响力。由于俱乐部由“中心化”开始，它将一直是“中心化”的。与比特币及点点币一样，瑞波系统将股东们与其投票权隔开，并因此比其他系统更中心化。

#### 4授权股权证明机制DPOS

股份授权证明机制DPOS（Delegate Proof of Stake）是一种新的保障加密货币网络安全的算法。它在尝试解决比特币采用的传统工作量证明机制以及点点币和NXT所采用的股份证明机制的问题的同时，还能通过实施科技式的民主以抵消中心化所带来的负面效应。

通过引入“受托人”这个角色，DPOS可以降低中心化所带来的负面影响。一共有101位受托人通过网络上的每个人经由每次交易投票产生，他们的工作是签署（生产）区块。通过去中心化的投票过程，DPOS能让网络比别的系统更加民主。与其要让我们完成在网络上信任所有人这个不可能完成的任务，不如让DPOS通过技术保护措施来确保那些代表网络来签署区块的人们（受托人）能够正确地工作。除此之外，在每个区块被签署之前，必须先验证前一个区块已经被受信任节点所签署。像DPOS这样的设计，实际上缩减了必须要等待相当数量的未授信节点进行验证后才能够确认交易的时间成本。

## 1.3应用前景

### 1.3.1金融领域

目前为止，金融领域是区块链技术介入最多，也是需求最大的一个领域。区块链技术的出现，让金融的去中心化成为了可能：金融领域对区块链的第一个需求是数字货币，特别是比特币的诞生。数字货币的成功发行大大刺激了传统银行业，银行、股权/有价证券交易所领域、保险领域也纷纷表现出了对区块链技术的强烈需求。由于金融领域与社会经济直接挂钩，因此其对区块链技术的探索也是走在时代最前沿的，技术需求会更快地转化为动力，加速区块链技术的应用落地。

### 1.3.2医疗领域

医疗行业中的许多资料都是非常私密的，对其阅读与管理权限的保护要求也十分苛刻。然而，目前中心化模式下的资料存储方式无法很好地保证资料的安全性，经常会造成病人隐私的泄露，而且一旦系统出现问题就会造成大规模的数据外泄。区块链的可编程、匿名性特征能更好的在去中心化的环境中保护病人的隐私，其应用前景非常广阔。

### 1.3.3公证领域

目前社会中的公证成本是非常高的，大多数公证均依赖于政府机关的信用来完成。这样的高成本、中心化方式使得如[知识](http://www.wanbizu.com/baike/)产权、房产等一系列需要公证的资产都未能得到很好的保护。区块链技术的去中心化特征能让数据资料通过数学信用背书的方式，在没有政府机关介入的情况下，完成自动化公证过程，且数据会永久保留并可随时追踪源头。因此，房产等政务资料管理与[知识](http://www.wanbizu.com/baike/)产权等非政务资料管理方面都已经对区块链技术表现出了强烈的需求。

### 1.3.4通信领域

通信领域最重要的是信息安全问题。区块链技术通过去中心化方式，完全改变了信息传输的渠道，由于网络中的每个人都能收到这份信息(但只有拥有私钥的人才能打开)，因此信息的拦截无从谈起，信息的跟踪也就无法实现。

### 1.3.5供应链领域

目前市场中的供应链系统并没有为货物提供一套完全可追踪的物流数据，许多物品的物流信息中途流失，为假冒伪劣产品的横行提供了机会。如果区块链技术能为供应链中的物流信息提供认证服务，那我们通过区块链数据库的源头追踪功能就可以很快地找到问题所在。这激发了供应链领域的强烈兴趣。

### 1.3.6域名领域

目前互联网中的域名是一种中心化结构的管理模式，ICANN作为协调机构来统一组织调配域名系统，再一层层分配给下面的域名承包商。从国家安全的角度来考虑，域名资源的去中心化是一种极大的需求。区块链技术的分布式结构能很好的管理域名资源而不需要一个统一调配机构，成为了满足这个需求的关键技术。

### 1.3.7投票领域

目前社会中的投票方式还很不完善。基于区块链技术的投票，可以在很好保护投票人身份的同时快速统计出结果，让整个投票体系能高效率、低成本的运行。目前纳斯达克已经正式试行区块链技术，未来来自投票领域的需求范围相信还会进一步扩大。

### 1.3.8其他领域

以上几个领域都是较早接触区块链技术并已开始取得初步探索成果的领域。现如今，随着区块链技术越来越广为人知，更多的领域开始意识到区块链技术的重要性，也逐渐展现了对这种全新技术的需求。物联网领域需要以太坊区块链的容错功能来确保安全和稳定，P2P借贷领域需要区块链的去中心化信任功能来建立一个公开透明的借贷市场，审计领域需要区块链的数据库功能来保证审计数据的真实性与可追踪性，拍卖领域需要区块链的数据公开透明功能来保证拍卖的正常进行，教育领域需要区块链的时间戳及数据库功能来帮助提供学历证书的认证，智能资产领域需要区块链的数据自动处理功能来帮助资产实现智能化、自动化，甚至游戏、彩票领域也需要区块链的数学功能来保证摇奖时的公正性。

区块链技术发展到今天，其应用需求已经从最初的数字货币扩展到社会领域的方方面面。区块链技术可以认为是一个人类在去信任环境下的大规模协作工具，它第一次使用纯技术的方式让互联网上的价值转移成为了可能。对区块链技术的需求，来自涉及到政治、经济、金融、社会(数字社会)、法律(计算法律学)、计算机、互联网、万维网WWW、物联网、人工智能、自动(无人)驾驶汽车、电子商务、中国制造2025、大数据、云计算等多个领域，而且部分领域已经有了一些落地的实践。