密码学在计算上是不可行的：一个过程被称为在计算上是不可行的。如果有人想对完成一个过程感兴趣，那就要花不切实际的长时间去做(比如几十亿年)。通常2的80次幂的计算步长被认为是计算不可行性的下限。哈希：哈希函数(或哈希算法)是将文档(如数据块或文件)处理成看起来完全随机的数据块(通常为32字节)的过程。从中可以将无意义的数据还原成文档，最重要的表现就是哈希特定文档的结果总是一样的。此外，极其重要的是，在计算上不可能找到两个具有相同散列的文件。正常情况下即使改变文件的一个字母也会完全打乱散列；例如，SHA3哈希的&quot

星期六&quot是

。

c38BBC8e93c09F6ed3Fe39b5135da91ad1a99d397ef16948606CDCBD14929F9d、而星期二的SHA3散列是

b4013c0eed56d5a0b448b02EC1d10DD18C1b3832068FBBDC65b98fa9b14b6DBF。散列值经常被用

用于以下目的：为无法伪造的特定文件创建的全球一致的标识符。加密：与密钥相同(如

c85ef7d79691Fe79573B1a7064c19C1a9819EBDBD1FAAab1a8AEC9234438AAF4)，以及文档的处理(明文)。。加密将产生一个输出(密文)，它可以是&quot解密&quot由其他拥有密钥的人还原为原始明文，但是对于没有密钥的人来说，这是令人费解的并且在计算上是不可行的。公钥加密：一种特殊的加密，有同时生成两个密钥(通常称为私钥和公钥)的过程，这样用一个密钥加密一个文档后，就可以用另一个密钥解密。一般顾名思义，个人公开自己的公钥，自己保留私钥。。数字签名(Digitalsignature):数字签名算法是一个过程，用户可以使用私钥为文档生成一个称为签名的短数据串，这样任何拥有相应公钥、签名和文档的人都可以验证(1)文档是&quot署名&quot特定私钥的所有者。(2)文件自签署后未被更改。请注意，这与传统签名不同，传统签名中，签名后可以涂抹多余的字，这是无法区分的；数字签名后对文档的任何更改都将使签名无效。。区块链地址：地址本质上是属于特定用户的公钥的表示；例如，与上面给出的私钥相关联的地址是CD2a3d9f938e13CD947EC05ABC7Fe734df8d826。注意在实践中，从技术上讲，地址是一个公钥的哈希值，但为了简单起见，最好忽略这种差异。交易：交易是授权一些与区块链相关的特定操作的文档。在一种货币中，主要的交易类型是向他人发送货币单位或代币；在其他系统中，如域名注册、制定和完成报价、订立合同等也是有效的交易

类型。块：块是包含零个或多个事务的数据包，前一个块的哈希值(&quot父块&quot)，以及可选的其他数据。。除了开头的&quot创世纪街区&quot，每个块都包含其父块的哈希值。整组数据块被称为区块链，包含网络中的所有交易历史。注意，一些基于区块链的加密货币使用了单词&quot总帐&quot而不是区块链。。两者的含义大致相同，虽然在系统中使用了术语&quot总帐&quot，每个块通常包括每个帐户当前状态的所有副本(如货币余额、部分履行的合同、注册)，并允许用户丢弃过时的历史数据。。Genesisblock:Genesisblock是指区块链中的第一个块，用于初始化相应的加密货币。账户：账户是总分类账中的一个记录，按其地址索引，总分类账包含关于账户状态的完整数据。在货币体系中，这包括货币平衡。，也许是未完成的交易订单；在其他情况下，更复杂的关系可以存储在帐户中。随机数：一个块中一个无意义的值，为了满足工作证明的条件而努力调整。挖矿：挖矿是一个重复的总交易，搭积木，尝试不同的随机数。直到找到一个能满足工作证明条件的随机数的过程。如果一个矿工运气好，产生了一个有效的区块，他将获得一定数量的硬币(区块中的总交易成本)作为奖励。所有的矿工开始尝试创造新的区块。这个新块包含作为父块的最新块的散列。陈旧块：对于同一个父块，已经创建了另一个块，然后再创建；旧的街区通常会被丢弃，这是对能源的浪费。幽灵：幽灵是一种协议。通过这种协议，块不仅可以包含它们的父块的散列值，还可以包含散列该父块的父块的其他子块(称为第三块)的陈旧块。这确保了陈旧块仍然有助于区块链的安全，并缓解了大矿工在快速区块链中具有优势的问题。因为它们可以立即知道自己的块，所以不太可能产生陈旧的块。叔块：父块的父块的子块，但不是它自己的父块，或者更一般地说，是一个祖先的子块，但不是它自己的祖先。如果A是B的叔叔块，那么B是A的侄子块。。分叉：同时生成指向同一个父块的两个块，有的矿工看到一个块，有的矿工看到另一个块的情况。这导致了两种区块链的同时增长。一般来说，当一个链条中的矿工走运时，这个链条就会增长。所有的矿工都会转向那个链条，从数学上来说，他们几乎会在四个街区内结束自己。硬分叉：当比特币协议规则发生变化时，旧节点拒绝接受新节点创建的块。违反规则的块将被忽略，矿工将遵循他们的规则集。在他们最后一次看到的街区之后创造一个街区。软分叉：当比特币协议的规则发生变化时，旧节点不会意识到规则不同，它们会遵循变化后的规则集，继续接受新节点创建的块。矿工们可能会发现，他们根本没有理解。、或经验证的块。双重支出：这是一种故意的分歧。当一个有大量挖掘能力的用户发送交易购买产品，收到产品后，再进行一次交易，向自己发送等量的币。攻击者创建一个块。该块与包含原始事务的块处于同一级别，但它包含第二个事务而不是原始事务，并且在该分支上开始挖掘。如果攻击者有50%以上的挖矿能力，那么双倍的代价最终可以保证在任何格挡深度都能成功。。如果低于50%，有部分成功的可能。但是它通常在2-5深度处具有唯一显著的可能性。因此，在大多数加密货币交易所、赌博网站和金融服务中，需要等待六个区块被产生(也称为&quot六个确认&quot)才接受付款。。BIP:比特币改进提案(bitcoinImprovementProposals

的简称)，比特币等区块链产品，是指比特币社区成员提交的一系列改进比特币的提

案。例如BIP0021是一个改进比特币统一资源标识符(URI)方案的提案。比特币：&quot比特币&quot既可以指这种虚拟货币单位，也可以指比特币网络或网络节点使用的比特币软件。确认：当交易包含在块中时。我们可以说它被证实了一次。矿工在这个区块之后每生产一个区块，这个交易的确认号就加一。当确认次数达到6次以上时，一般认为交易相对安全，不易逆转。。难度：全网会调变量&quot难度&quot控制生成工作量证书所需的计算能力。难度目标：使全网计算能力每10分钟生成一个区块所需的难度值为难度目标。。难度调整：BTC全网每生成2106块后，会根据之前2106块的计算力来调整难度。矿工&#039；手续费：交易发起者通常会向矿商支付一笔费用。网络处理交易的费用。大多数交易需要矿工&#039；0.5毫比特币的费用。。哈希：二进制数据的数字指纹。矿工：矿工是指通过反复重复哈希运算生成工作负载证书的网络节点。网络：比特币网络是由若干节点组成的P2P网络，用来广播交易信息和数据块。。奖励：每个新区块都有一定数量的新造比特币奖励出工作量证书的矿工。在这个阶段，每块有25个比特币的奖励。私钥：用于解锁相应(钱包)地址的字符串。比如5j76SF8l5JTtze96r66SF8CKa9y44wdpjmwcxr3tzlH3IBVpxh。交易：简单来说，交易是指将比特币从一个地址转移到另一个地址。更准确地说A&quot交易&quot指的是一种数据结构，它被签名并表示值的传递。每个&quot交易&quot是通过比特币网络传输的，由矿工收集&#039；节点并打包成块，永久保存在区块链的某个地方。钱包：钱包是指保存比特币地址和私钥的软件。你可以用它来接受、发送和存储你的比特币。SPV客户端(或称轻客户端):只下载一小部分区块链的客户端，让智能手机、笔记本电脑等低功耗或低存储硬件的用户也能维持几乎相同的安全保障。这是有时选择性下载的状态的一小部分，在区块链验证和维护期间，它不需要花费兆字节的带宽或千兆字节的存储空间。楔形侧链技术(挂钩

sidechains):它将实现比特币和其他数字资产在多个区块链之间的转移，这意味着用户可以在使用现有资产的同时访问新的加密货币系统。。工作证明(Proof-of-Work):一种共识机制，由一方(通常指参考方)提出计算结果，众所周知这种结果很难计算，但很容易验证。通过验证这一结果任何人都可以确认该引用已经执行了一定量的计算工作来产生这个结果。利害关系证明：

一种共识机制，在这种机制中，矿工需要创建一个&quot货币权利&quot创建块时的事务。集市会按照设定的比例给矿工自己发一些硬币，类似利息。DPOS:[XY002][XY001]一种共识机制，允许每个持有资金的人投票选出整个系统资源的代表。，获得票数最多的101名代表获得交易包计算权，系统给予相应奖励。它是一个并发的分布式区块链。"分布式&quot意味着区块链被细分为多个组件，这些组件连接成一个统一的整体。，而不需要一次全部计算(而比特币区块链需要它)。"并发&quot意味着此分支使不同的进程能够并行运行，而不会相互干扰。罗朗：是查因&#039；的原生智能合约语言(或编程语言)。一种基于进程演算的反射式高级进程编程语言，允许以高效、安全的方式并行执行进程，并在低级智能合约的基础上组合高

级智能合约。，允许在正常验证的基础上进行更好的安全测试和模拟。SpecialK:分布式存储技术的一种方法，为程序员提供单一的领域特定语言和熟悉统一的API。通过API，他们可以访问分布在整个网络中的数据。数据分发时总是考虑到冗余性和敏感性，确保需要时随时随地可用，不需要时隐藏。零知识证明：证明者和验证者之间的交互证明者可以使验证者确信某个断言是正确的，而无需向验证者提供任何有用的信息。比特币的可替代性：无论你之前有过什么交易历史，包括可能参与毒品交易等。这与&quot原始硬币&quot刚挖出来的，完全可以同等替换。目前有交易所或其他服务公司跟踪用户账户中比特币的来源，一旦涉及犯罪就不受理。。环签名：因签名中的参数Ci(i=1，2，...，n)按照一定的规则首尾相连形成一个环而得名。实际上，实际签名者使用其他可能签名者的公钥生成一个带有断裂的环，然后使用私钥将断裂连接成一个完整的环。。任何验证者都可以通过使用环成员的公钥来验证环签名是否由可能的签名者生成。隔离见证：隔离见证，缩写为SW。当用户进行交易时，他们会将比特币发送到不同的地址。。在使用这些比特币时，其签名

(即见证)不会被记录为交易ID的一部分，而是单独处理。换句话说，交易ID完全由交易状态(即余额的进出)决定，不受见证部分的影响。。闪电

网络：一个可扩展的微支付通道网络。如果交易双方在区块链上预先有支付渠道，，可以多次、高频、双向滚动差实现微支付即时确认；如果双方之间没有直接的点对点支付通道，只要在网络中存在连接双方的由多个支付通道组成的支付路径。闪电网也可以利用这种支付路径实现双方资金的可靠转移。序列化：将数据结构转换成字节序列的过程。以太坊内部使用的编码格式称为递归长度前缀编码(RLP)。帕特丽夏夏树：一种数据结构它存储每个帐户的状态。通过从每个节点开始，然后将节点分成多达

16个组，然后散列每个组，然后继续散列散列结果，直到整个树具有最终&quot根哈希&quot。。该树具有重要的特征：(1)只有一个可能的树，所以每个数据集对应一个可能的根哈希；(2)易于更新、添加或删除树节点并生成新的根散列；(3)没有办法在不改变根散列的情况下修改树的任何部分。因此，如果根哈希包含在签名的文档或有效块中，签名或工作证明可以保证整个树(

4)并且任何人只能提供向下到特定节点的分支，可以加密该分支以证明具有确切内容的节点确实在树中。。帕特里斯夏树也被用来存储帐户，交易已被存储在第三块内部。你可以在这里看到更详细的说明。账户随机数：每个账户的交易次数。这可以防止重放攻击，在重放攻击中，一个事务从A向B发送20个硬币，并且可以被B一次又一次地重放。直到A的账户余额被持续榨干。EVM代码：以太坊虚拟机的代码，以太坊区块链可以包含的编程语言的代码。每次向该账户发送消息时，执行与该账户相关联的EVM码，并且该账户具有读/写存储和自身发送消息的能力。。消息

：A&quot虚拟交易&quot通过EVM电码从一个账户转到另一个账户。应该注意的是&quot交易&quot和&quot消息&quot在以太坊是不同的；术语&quot交易&quot以太坊中特指一串带有物理数字签名的数据。并且每个交易触发相关的消息，但是消息也可以通过EVM码发送，在这种情况下，它们从不被表示为任何数据。存储：包含在每个帐户中的键/值数据库，其中键和值都是32字节的字符串。，但可以用其他方式包含任何内容。外部拥有的帐户：由私钥控制的帐户。外部拥有的帐户不能包含EVM代码。合同：包含EVM代码并受其控制的帐户。除非被编译成EVM码，否则契约不能被私钥直接控制。一旦合同发出，就没有业主了。以太：以太坊网络内部基础的加密令牌。以太用于支付交易和以太坊交易的计算成本。气体：大致相当于计算步骤的测量。每笔交易都需要包括天然气限制。，并愿意为每一种气体付费；矿工可以选择是否包括交易和收集费用。如果由包括原始消息和任何可能被触发的子消息的交易生成的用于计算的gas的总量大于或等于gas的限制，则处理该交易。。除非交易仍然有效，费用仍然由矿工收取，否则，如果气体总量小于限额，将恢复所有更改。每个操作都有气体支出；对于大多数手术来说，费用是1个煤气，尽管一些昂贵的手术费用可能高达100个煤气。