1、 Blockchain——[区块链](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%8C%BA%E5%9D%97%E9%93%BE&zhida_source=entity)

区块链是分布式数据存储、点对点传输、[共识机制](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%85%B1%E8%AF%86%E6%9C%BA%E5%88%B6&zhida_source=entity)、加密算法等计算机技术的新型应用模式。是一个共享的分布式账本，其中交易通过附加块永久记录。

2、 Block——区块

在[比特币](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%AF%94%E7%89%B9%E5%B8%81&zhida_source=entity)网络中，数据会以文件的形式被永久记录，我们称这些文件为区块。一个区块是一些或所有最新[比特币交易](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%AF%94%E7%89%B9%E5%B8%81%E4%BA%A4%E6%98%93&zhida_source=entity)的记录集，且未被其他先前的区块记录。

3、 Node—一节点

由区块链网络的參与者操作的分类帐的副本。

4、去中心化

[去中心化](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=2&q=%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96&zhida_source=entity)是一种现象或结构，必须在拥有众多节点的系统中或在拥有众多个体的群中才能出现或存在。节点与节点之间的影响，会通过网络而形成[非线性因果关系](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E9%9D%9E%E7%BA%BF%E6%80%A7%E5%9B%A0%E6%9E%9C%E5%85%B3%E7%B3%BB&zhida_source=entity)。

5、 Pow—工作量证明

Proofof Work，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。

6、函数加密

与[同态加密](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%90%8C%E6%80%81%E5%8A%A0%E5%AF%86&zhida_source=entity)相关的一个问题是函数加密。同态加密保护的是数据本身，而[函数加密](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=3&q=%E5%87%BD%E6%95%B0%E5%8A%A0%E5%AF%86&zhida_source=entity)顾名思义保护的是处理函数本身，即让第三方看不到处理过程的前提下，对数据进行处理。

该问题已被证明是不存在对多个通用函数的任意多 key 的方案，目前仅能做到对某个特定函数的一个 key 的方案。

7、 PoS—权益证明

Proofof Stake，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。

8、[智能合约](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%99%BA%E8%83%BD%E5%90%88%E7%BA%A6&zhida_source=entity)

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

9、时间戳

时间戳是指字符串或编码信息用于辨识记录下来的时间日期。国际标淮为 ISO 8601。

10、[图灵完备](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%9B%BE%E7%81%B5%E5%AE%8C%E5%A4%87&zhida_source=entity)

图灵完成是指机器执行任何其他可编程计算机能够执行计算的能力。

11、 Dapp——[去中心化应用](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96%E5%BA%94%E7%94%A8&zhida_source=entity)

是一种开源的应用程序，自动运行，将其数据存储在区块链上，以密码令牌的形式激励，并以显示有价值证明的协议进行操作。

12、 DAO——[去中心化自治组织](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96%E8%87%AA%E6%B2%BB%E7%BB%84%E7%BB%87&zhida_source=entity)

可以认为是在没有任何人为干预的情况下运行的公司，并将一切形式的控制交给一套不可破坏的[业务规则](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E4%B8%9A%E5%8A%A1%E8%A7%84%E5%88%99&zhida_source=entity)。

13、 Privatekey——[私钥](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E7%A7%81%E9%92%A5&zhida_source=entity)

私钥是一串数据，它是允许您访问特定钱包中的令牌。它们作为密码，除了地址的所有者之外，都被隐藏。

14、 PublicKey—[公钥](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%85%AC%E9%92%A5&zhida_source=entity)

是和私钥成对出现的，公钥可以算出币的地址，因此可以作为拥有这个币地址的凭证。

15、 矿工

尝试创建区块并将其添加到区块链上的计算设备或者软件。在一个区块链网络中，当一个新的有效区块被创建时，系统一般会自动给子区块创建者（矿工）一定数量的代币，作为奖励。

16、[公有链](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%85%AC%E6%9C%89%E9%93%BE&zhida_source=entity)

完全开放的区块链，是指任何人都可读取的、任何人都能发送交易且交易能获得有效确认的、全世界的人都可以参与系统维护工作，任何人都可以通过交易或挖矿读取和写入数据。

17、[私有链](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E7%A7%81%E6%9C%89%E9%93%BE&zhida_source=entity)

写入权限仅面向某个组织或者特定少数对象的区块链。读取权限可以对外开放，或者进行任意程度地限制。

18、 [联盟链](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E8%81%94%E7%9B%9F%E9%93%BE&zhida_source=entity)

共识机制由指定若干机构共同控制的区块链。

19、主链

主链一词源于主网（，相对干测试网），即正式上线的、独立的区块链网络.

20、側链

楔入式侧链技术(pegged sidlechains），它将实现比特币和其他[数字资产](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%95%B0%E5%AD%97%E8%B5%84%E4%BA%A7&zhida_source=entity)在多个区块链间的转移，这就意味着用户们在使用他们己有资产的情况下，就可以访问新的加密货币系统。

21、[跨链技术](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E8%B7%A8%E9%93%BE%E6%8A%80%E6%9C%AF&zhida_source=entity)

跨链技术可以理解为连接各区块链的桥樂，其主要应用是实现各区块链之间的原子交易、资产转换，区块链内部信息互通，或解决 Oracle 的问题等。

22、硬分叉

区块链发生永久性分歧，在新共识规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会发生。

23、[软分叉](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E8%BD%AF%E5%88%86%E5%8F%89&zhida_source=entity)

当新共识规则发布后，没有升级的节点会因为不知道新共识规则下，而生产不合法的区块，就会产生临时性分叉。

24、 Hash—[哈希值](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%93%88%E5%B8%8C%E5%80%BC&zhida_source=entity)

一般翻译做"散列"，也有直接音译为"哈希"的。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。

25、 区块头

区块头里面存储着区块的头信息，包含上一个区块的哈希值（PreHash），本区块体的哈希值（Hash），以及时间戳（TimeStamp）等等。

26、 [中本聪](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E4%B8%AD%E6%9C%AC%E8%81%AA&zhida_source=entity)

自称日裔美国人，日本媒体常译为[中本哲史](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E4%B8%AD%E6%9C%AC%E5%93%B2%E5%8F%B2&zhida_source=entity)，此人是比特币协议及其相关软件Bitcoin-Qt的创造者，但真实身份未知。

27、 加密货币

加密货币是数字货币（或称[虚拟货币](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E8%99%9A%E6%8B%9F%E8%B4%A7%E5%B8%81&zhida_source=entity)）的一种。是一种使用密码学原理来确保交易安全及控制交易单位创造的交易媒介。

28、 Oracles

Oracle通过向智能合约提供数据，它现实世界和区块链之间的桥梁。

29、 DPoS——授权权益证明

Delegate Proof of Stake ，类似于董事会投票。以EOS来说，它引入了见证人的概念，持股者投票选出一定数量的见证人，每个见证人按序有两秒的权限时间生成区块，若见证人在给定的[时间片](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%97%B6%E9%97%B4%E7%89%87&zhida_source=entity)不能生成区块，区块生成权限交给下一个时间段对应的见证人。

30、 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形成共识，初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由该俱乐部51%的会员投票通过。共识遵循这些核心成员的“51%权利”，外部人员则没有影响力。由于该俱乐部由中心化开始，它将一直是中心化的，而如果它开始腐化，股东们什么也做不了。与[bitcoin](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=bitcoin&zhida_source=entity)及Peercoin一样，瑞波系统将股东们与其投票权隔开，因此它比其他系统更中心化。

31、 PoB——焚烧证明

Proof of Burn，通过焚烧自己手中的代币来表决谁拥有对网络的领导地位的承诺。焚烧代币的数量越多，能获得网络领导地位的概率越高。

32、 PBFT——[拜占庭容错算法](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%8B%9C%E5%8D%A0%E5%BA%AD%E5%AE%B9%E9%94%99%E7%AE%97%E6%B3%95&zhida_source=entity)

Practical Byzantine Fault Toleran，采用“许可投票、少数服从多数”来选举领导者并进行记账的共识机制，该共识机制允许拜占庭容错，允许强监督节点参与，具备[权限分级](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%9D%83%E9%99%90%E5%88%86%E7%BA%A7&zhida_source=entity)能力，性能更高，耗能更低，而且每轮记账都会由全网节点共同选举领导者，允许33%的节点作恶，容错率为33%。实用拜占庭容错特别适合联盟链的应用场景。

33、 Byzantinefailures——[拜占庭将军问题](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%8B%9C%E5%8D%A0%E5%BA%AD%E5%B0%86%E5%86%9B%E9%97%AE%E9%A2%98&zhida_source=entity)

拜占庭将军问题是由[莱斯利·兰伯特](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E8%8E%B1%E6%96%AF%E5%88%A9%C2%B7%E5%85%B0%E4%BC%AF%E7%89%B9&zhida_source=entity)提出的点对点通信中的基本问题。含义是在存在消息丢失的不可靠信道上试图通过消息传递的方式达到一致性是不可能的。因此对一致性的研究一般假设信道是可靠的，或不存在本问题。

34、 51%攻击

当一个单一个体或者一个组超过一半的计算能力时，这个个体或组就可以控制整个加密货币网络，如果他们有一些恶意的想法，他们就有可能发出一些冲突的交易来损坏整个网络。

35、 DistributedLedger——[分布式账本](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=2&q=%E5%88%86%E5%B8%83%E5%BC%8F%E8%B4%A6%E6%9C%AC&zhida_source=entity)

数据通过分布式节点网络进行存储。分布式账本不是必须具有自己的货币，它可能会被许可和私有。

36、DistributedNetwork——[分布式网络](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%88%86%E5%B8%83%E5%BC%8F%E7%BD%91%E7%BB%9C&zhida_source=entity)

理能力和数据分布在节点上而不是拥有集中式[数据中心](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E6%95%B0%E6%8D%AE%E4%B8%AD%E5%BF%83&zhida_source=entity)的一种网络。

37、预言机

预言机是一种可信任的实体，它通过签名引入关于外部世界状态的信息，从而允许确定的智能合约对不确定的外部世界作出反应。预言机具有不可篡改、服务稳定、可审计等特点，并具有经济激励机制以保证运行的动力。

38、[零知识证明](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E9%9B%B6%E7%9F%A5%E8%AF%86%E8%AF%81%E6%98%8E&zhida_source=entity)

零知识证明由S.Goldwasser、S.Micali及C.Rackoff在20世纪80年代初提出的。它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。

39、AES——[高级加密标准](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86&zhida_source=entity)

密码学中的高级加密标准（Advanced Encryption Standard，AES），又称Rijndael[加密法](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%8A%A0%E5%AF%86%E6%B3%95&zhida_source=entity)，是美国联邦政府采用的一种区块加密标准。

40、Wallet——钱包

一个包含私钥的文件。它通常包含一个软件客户端，允许访问查看和创建钱包所设计的特定块链的交易。

41、冷钱包

通俗来说[冷钱包](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=2&q=%E5%86%B7%E9%92%B1%E5%8C%85&zhida_source=entity)就是将数字货币进行离线下储存的钱包，玩家在一台离线的钱包上面生成数字货币地址和私钥，再将其保存起来。而冷钱包是在不需要任何网络的情况下进行数字货币的储存，因此黑客是无法进入钱包获得私钥的。

42、SPV——[轻钱包](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E8%BD%BB%E9%92%B1%E5%8C%85&zhida_source=entity)

轻钱包依赖比特币网络上其他全节点，仅同步与自己相关的数据，基本可以实现去中心化。

43、全节点

全节点是拥有完整区块链账本的节点，全节点需要占用内存同步所有的区块链数据，能够独立校验区块链上的所有交易并实时更新数据，主要负责区块链的交易的广播和验证。

44、超级账本

超级账本（hyperledger）是Linux基金会于2015年发起的推进区块链数字技术和交易验证的开源项目。通过创建通用的[分布式账本技术](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%88%86%E5%B8%83%E5%BC%8F%E8%B4%A6%E6%9C%AC%E6%8A%80%E6%9C%AF&zhida_source=entity)，协助组织扩展、建立行业专属应用程序、平台和硬件系统来支持成员各自的交易业务。

45、[闪电网络](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E9%97%AA%E7%94%B5%E7%BD%91%E7%BB%9C&zhida_source=entity)

闪电网络的目的是实现安全地进行链下交易，其本质上是使用了哈希时间锁定智能合约来安全地进行0确认交易的一种机制，通过设置巧妙的“智能合约”，使得用户在闪电网络上进行未确认的交易和黄金一样安全。

46、P2P——[对等网络](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%AF%B9%E7%AD%89%E7%BD%91%E7%BB%9C&zhida_source=entity)

即对等计算机网络，是一种在对等者（Peer）之间分配任务和工作负载的[分布式应用](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%88%86%E5%B8%83%E5%BC%8F%E5%BA%94%E7%94%A8&zhida_source=entity)架构，是对等计算模型在应用层形成的一种组网或网络形式。

47、Mining——挖矿

挖矿是获取比特币的勘探方式的昵称。利用电脑硬件计算出币的位置并获取的过程称之为挖矿。

48、矿池

是一个全自动的挖矿平台，使得矿工们能够贡献各自的算力一起挖矿以创建区块，获得区块奖励，并根据算力贡献比例分配利润（即矿机接入矿池—提供算力—获得收益）。

49、哈希率

假设挖矿是解一道方程题，而且只有把每个整数代入才能算出来，那么哈希率就是每秒处理数据的速度。

50、Hashtree——[哈希树](https://zhida.zhihu.com/search?content_id=212606998&content_type=Article&match_order=1&q=%E5%93%88%E5%B8%8C%E6%A0%91&zhida_source=entity)

哈希树是一种树形数据结构，每个叶节点均以数据块的哈希作为标签，而非叶节点则以其子节点标签的加密哈希作为标签。

51、SHA256

SHA-256是比特币一些列数字货币使用的[加密算法](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95&zhida_source=entity)。然而，它使用了大量的[计算能力](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E8%AE%A1%E7%AE%97%E8%83%BD%E5%8A%9B&zhida_source=entity)和处理时间，迫使矿工组建采矿池以获取收益。

52、Kyc

KYC是Know Your Customer的缩写，意思是了解你的客户，在国际《反洗钱法》条例中，要求各组织要对自己的客户作出全面的了解，以预测和发现商业行为中的不合理之处和潜在违法行为。

53、交易（Transaction）

一次操作，导致账本状态的一次改变，如添加一条记录。

54、链（Chain）

由一个个区块按照发生顺序串联而成，是整个状态变化的日志记录。

55、[私人货币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E7%A7%81%E4%BA%BA%E8%B4%A7%E5%B8%81&zhida_source=entity)

中国最大的私人货币就是腾讯Q币，Q币在腾讯的[生态圈](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E7%94%9F%E6%80%81%E5%9C%88&zhida_source=entity)里面可以使用，你可以用人民币去买[Q币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=3&q=Q%E5%B8%81&zhida_source=entity)，但是你不能用Q币去换人民币，这本身就是一个私人货币，是某个商圈币。

56、[数字货币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=2&q=%E6%95%B0%E5%AD%97%E8%B4%A7%E5%B8%81&zhida_source=entity)

私人货币和数字货币的区别就在于，私人货币是一个中心化的机构做背书，数字货币没有中心化的机构来做信用背书，靠数学算法。

57、[创世区块](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%88%9B%E4%B8%96%E5%8C%BA%E5%9D%97&zhida_source=entity)

创世区块指区块链上的第一个区块，用来初始化相应的加密货币。

58、账户

帐户是在总账中的记录，由它的地址来索引，总账包含有关该帐户的状态的完整的数据。在一个货币系统里，这包含了货币余额，或许未完成的的交易订单;在其它情况下更复杂的关系可以被存储到账户内。

59、比特币地址

地址用于接收比特币，功能类似银行的存款账号，但不需要实名登记。若只公开地址不必担心里面的比特币被盗走，也没有任何身份信息，也可以离线产生。比特币的地址是由用户的[公开密钥](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5&zhida_source=entity)经过 SHA-256 散列运算后，再通过 RIPEMD-160 散列运算而得，其长度固定为 160 个[比特](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=6&q=%E6%AF%94%E7%89%B9&zhida_source=entity)(bits)，通常会利用 Base-58 将之编码成一串由英文字母和数字所组成的字符串，以方便显示或散布，其特征是皆以“1”或者“3”开头，区分大小写，但不包括“IlO0”等字符，“1”开头的地址长26~34位，“3”开头的地址长34位，例如

"1DwunA9otZZQyhkVvkLJ8DV1tuSwMF7r3v"，地址也可编码成快速反应[矩阵码](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E7%9F%A9%E9%98%B5%E7%A0%81&zhida_source=entity)(QR-Code)的形式让移动设备能够便捷地读取复制 。比特币客户端可以离线生成比特币地址 。一个人可以生成并拥有许多比特币地址，并用在不同的交易上，而且除非自己揭露，否则外人无法看出其中的关系。

60、钱包地址

如果我们把ETH钱包简单比作成银行卡账户的话，那么ETH钱包地址就可以看成是银行卡账号。不同的是，ETH地址是可以不存储在网络上的，更是可以独立于你的钱包而存在的。

61、钱包

以不同的协议又分为比特币钱包、以太坊钱包、EOS钱包等。

62、算力

为了挖到矿，参与处理区块的用户端往往需要付出大量的时间和计算力。算力一般以每秒进行多少次[hash](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=hash&zhida_source=entity)计算为单位，记为h/s。矿工能获得记账的权力，就能获得 比特币新发行出的奖励 ，这其实取决于其的算力 。获得奖励的概率等于他所掌握的算 力占全网算力的百分比 。[哈希碰撞](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%93%88%E5%B8%8C%E7%A2%B0%E6%92%9E&zhida_source=entity)是哈希算法的一种称呼，哈希算法是一种密码学数学算法 。每秒能做多少次哈希碰撞，就是其 " 算力 " 的代表，目前主流的矿机为10T左右的计算量级，即一台矿机就能每秒做至少10的13次方哈希碰撞，我们可以说，这一台10T的矿机就有10T的算力。一个矿工所掌握的矿机占比特 币全网的总算力的百分比是多少， 就代表TA在这10分钟记账竞争中能够获胜的概率就是多少 。

63、挖矿

挖矿是反复总计交易，构建区块，并尝试不同的随机数，直到找到一个随机数可以符合工作证明的条件的过程。如果一个矿工走运并产生一个有效的区块的话，会被授予的一定数量的币（区块中的交易全部费用）作为奖励。而且所有的矿工开始尝试创建新的区块，这个新区块 包含作为父块的最新的区块的[散列](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=3&q=%E6%95%A3%E5%88%97&zhida_source=entity)。

64、分叉

指向同一个父块的2个[区块](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=13&q=%E5%8C%BA%E5%9D%97&zhida_source=entity)被同时生成的情况，某些部分的矿工看到其中一个区块，其他的矿工则看到另外一个区块。这导致2种区块链同时增长。通常来说，随着在一个链上的矿工得到幸运并且那条链增长的话，所有的矿工都会转到那条链上，数学上分几乎会在4个区块内完结自己。

65、 EcoBall生态球

EcoBall生态球是一个全新的、开放兼容的多链并行区块链[操作系统](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F&zhida_source=entity)，它结合区块链账簿简单明了和DAG快速确认的优点，有效解决比特币和[以太坊](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=2&q=%E4%BB%A5%E5%A4%AA%E5%9D%8A&zhida_source=entity)等系统的体积快速膨胀问题，并力图建立一个可真正商业化的区块链生态系统。

66、比特币/ Bitcoin / BTC

一种点对点的[去中心化](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96&zhida_source=entity)加密货币 Bitcoin （比特币）的概念是由[中本聪](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E4%B8%AD%E6%9C%AC%E8%81%AA&zhida_source=entity)（化名）于 2009 年 1 月 3 日提出，是一种点对点 的、去中心化、全球通用、无[排他性](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%8E%92%E4%BB%96%E6%80%A7&zhida_source=entity)、不需第三方机构或个人，基于区块链作为支付技 术的加密货币，比特币不依赖中央机构发行，而是通过工作量证明[共识机制](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%85%B1%E8%AF%86%E6%9C%BA%E5%88%B6&zhida_source=entity)在区块链中 完成，也就是俗称“挖矿”。比特币使用整个 P2P 网络节点的[分布式数据库](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%88%86%E5%B8%83%E5%BC%8F%E6%95%B0%E6%8D%AE%E5%BA%93&zhida_source=entity)来确认、验 证及记录货币的交易 ; 比特币发行总量 2100 万枚，预计于 2140 年（编者注：2040 年的 说法有误）发行完毕，目前市面上流通量超过 80% 。

67、NFT

NFT是Non-Fungible Token的缩写，中文称为「[非同质化代币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E9%9D%9E%E5%90%8C%E8%B4%A8%E5%8C%96%E4%BB%A3%E5%B8%81&zhida_source=entity)」，通常是指[开发者](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%BC%80%E5%8F%91%E8%80%85&zhida_source=entity)在以太坊平台上根据ERC721标准/协议所发行的代币，它的特性为不可分割、不可替代、独一无二的，简单来说，采用ERC721标准/协议而发行的代币就叫做NFT。

68、GameFI：GameFi=NFT+DeFi+游戏

GameFi即Game Finance，将[去中心化金融](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96%E9%87%91%E8%9E%8D&zhida_source=entity)以游戏方式呈现。Defi提供底端逻辑，游戏提供方式载体，NFT承担游戏内的装备、道具。

69、DeFi

DeFi是decentralized finance（分布式金融）一词的缩写，通常是指基于以太坊的数字资产和金融智能合约，协议以及[分布式应用程序](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%88%86%E5%B8%83%E5%BC%8F%E5%BA%94%E7%94%A8%E7%A8%8B%E5%BA%8F&zhida_source=entity)（DApps）。简单来说，它是建立在区块链上的金融软件。

SocialFi：socialFi的定义是社交化金融，顾名思义socialFi即是socialFi和Finance的结合体。当前socialFi板块的[龙头币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E9%BE%99%E5%A4%B4%E5%B8%81&zhida_source=entity)只有ENJ。所以socialFi不是[币种](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%B8%81%E7%A7%8D&zhida_source=entity)

70、Gas Fee

矿工费（Gas Fee）就是用于转账激励矿工的费用，即支付给矿工的手续费，当你在以太坊区块链上进行转账时，矿工要把你的交易打包并放上区块链，才能使交易完成，在这过程中会消耗区块链的运算资源，所以要支付费用。

71、ICO

ICO(是Initial Coin Offering缩写)，首次币发行，源自股票市场的[首次公开发行](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E9%A6%96%E6%AC%A1%E5%85%AC%E5%BC%80%E5%8F%91%E8%A1%8C&zhida_source=entity)(IPO)概念，是区块链项目首次发行代币，募集比特币、以太坊等通用数字货币的行为。

中心化[交易所](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E4%BA%A4%E6%98%93%E6%89%80&zhida_source=entity):中心化交易所中，用户将数字资产存进交易所，由交易所集中保管和控制。当用户进行交易时，会向交易所提交交易指令，由交易所进行交易撮合，并将成交后结果告知用户。除了充提币以外，整个交易过程全部是在交易所的服务器中完成，与区块链没有交互。

72、去中心化交易所

去中心化交易所中，资金在用户钱包地址或者交易智能合约中，由用户完全控制。用户发起交易时，交易所执行智能合约来完成交易，资产划转在链上完成。交易记录链上可查，公开透明。

73、去中心化钱包

相对于私钥掌握在第三方服务商手中的中心化钱包（交易所），[去中心化钱包](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=2&q=%E5%8E%BB%E4%B8%AD%E5%BF%83%E5%8C%96%E9%92%B1%E5%8C%85&zhida_source=entity)的私钥则由用户自己保存，资产存储在区块链上，用户是真正的数字货币的持有者，钱包只是帮助用户管理链上资产和读取区块链数据的一个工具，所以也就无法控制、窃取、转移你的资产。

因此去中心化的钱包很难被黑客集中攻击，用户也不必担心钱包服务商的自我窃取或者跑路，因为只要创建钱包的时候自己把私钥保管好，您的资产依然在链上，换个钱包一样可以显示出来的。

注意：去中心化钱包一旦丢失、被盗，在没有备份私钥或助记词的情况下是无法找回的，因此一定要安全、正确的备份您的私钥。

74、以太坊/ Ethereum / 以太币/ Ether / ETH

下一代智能合约和去中心化应用平台 Ethereum （以太坊）是一种开源的、[图灵完备](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%9B%BE%E7%81%B5%E5%AE%8C%E5%A4%87&zhida_source=entity)的、智能合约公有区块链，基于区块链 账本用于合约的处理和执行，使得任何人都能够创建合约和去中心化应用，并在其中自有定义所有权规则、交易方式和状态[转换函数](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E8%BD%AC%E6%8D%A2%E5%87%BD%E6%95%B0&zhida_source=entity)。Ethereum 由 Vitalik Buterin （绰号 “ V 神”）所创立并于 2014 年 7 月进行 ICO。以太坊内置名为 Ether （[以太币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=2&q=%E4%BB%A5%E5%A4%AA%E5%B8%81&zhida_source=entity)）的加密货币。

75、（瑞波）/ Ripple / 瑞波币/ XRP

点对点的去中心化资产传输网络 Ripple 是一个去中心化的资产传输网络，用于解决[金融机构](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E9%87%91%E8%9E%8D%E6%9C%BA%E6%9E%84&zhida_source=entity)以及用户间的资产转换和 信任问题。XRP （[瑞波币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=2&q=%E7%91%9E%E6%B3%A2%E5%B8%81&zhida_source=entity)）是 Ripple 网络流通的[基础货币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%9F%BA%E7%A1%80%E8%B4%A7%E5%B8%81&zhida_source=entity)，任何人均可以创建 Ripple 账户并通过 Ripple 支付网络转账任意一种货币，包括美元、欧元、人民币、日元或 者比特币，交易确认在几秒以内完成且[交易费](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E4%BA%A4%E6%98%93%E8%B4%B9&zhida_source=entity)用几乎为零。瑞波币的最大发行量为 1000 亿枚并随着交易的增多而逐渐减少，瑞波币的运营公司为 Ripple Labs，其前身为 OpenCoin 。

76、比特现金/ Bitcoin Cash / BCH

比特币的大区块分叉币 Bitcoin Cash（比特现金）是比特币硬分叉产生的分叉币，比特现金修改比特币的代码， 通过将区块大小调整到 8M 以解决扩容问题并且移除 Segwit （隔离见证）。比特现金于 2017 年 8 月 1 日 UTC 时间 12:37 从比特币区块高度 478558 开始分叉。

77、[莱特币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E8%8E%B1%E7%89%B9%E5%B8%81&zhida_source=entity)/ Litecoin / LTC

最早的第一代加密货币竞争币之一 Litecoin （莱特币）是最早的竞争币之一，于 2011 年从比特币衍生出来并在技术上具 有相同的实现原理，其创新点有两个：其一，使用 Scrypt 作为工作量[证明算法](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E8%AF%81%E6%98%8E%E7%AE%97%E6%B3%95&zhida_source=entity)，使得莱特币在普通计算机上更易于挖掘；其二，莱特币网路大约每 2.5 分钟处理一个区块， 使得莱特币网络具有更快的交易确认速度。2017 年 6 月莱特币闪电网络上线。

78、[卡尔达诺](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%8D%A1%E5%B0%94%E8%BE%BE%E8%AF%BA&zhida_source=entity)/ Cardano / 艾达币/ ADA

第一个由研究为主导的完全开源的区块链[技术平台](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%8A%80%E6%9C%AF%E5%B9%B3%E5%8F%B0&zhida_source=entity) Cardano （卡尔达诺）是全球首创可以证明公平性、安全性，完全透明且不能作弊的、 完全开源的分散型游戏平台，特点是完全没有被运营商支配的民主平台。卡尔达诺的目 标是构建一个分层次的、集成加密货币（如比特币、莱特币）和智能合约（如以太坊、 EOS）的区块链生态系统。卡尔达诺运用独立的 SDK 系统，个人技术者可以参与游戏 开发，并产生游戏竞争以提高游戏的质数，以解决当前赌场、线上赌场的大部分缺陷。 ADA（艾达币）是 2017 年初公开的 Cardano 项目的加密货币，可用于发送和接收数字 资金；作为卡尔达诺的中心货币，如需要参与 Cardano 的游戏必须持有艾达币并通过 对战赢取艾达币。Cardano 项目发起于 2015 年，名称来自于 16 世纪的意大利[数学家](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%95%B0%E5%AD%A6%E5%AE%B6&zhida_source=entity) Gerolamo Cardano ，Cardano 是医生、[占星术士](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%8D%A0%E6%98%9F%E6%9C%AF%E5%A3%AB&zhida_source=entity)、哲学家同时也是个赌徒，他运用占星 术预言自己的死期并据说于同一日自杀。Ada 则是以 19 世纪英国贵族 Ada levea 命名， 她被称为人类史上的第一位程序员。

79、恒星币/ Stellar Lumens / XLM

数字货币与[法定货币](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%B3%95%E5%AE%9A%E8%B4%A7%E5%B8%81&zhida_source=entity)之间传输的去中心化网

关 Stellar Lumens （恒星币）是由电驴创始人以及前 Ripple 创始人 Jed McCaleb 因管理 层分歧而发起的加密货币项目，是基于 Ripple 代码修改创建的恒星支付网络中的基础 加密货币，用于搭建一个数字货币与法定货币之间传输的去中心化网关，使得数字资产 可以在银行、支付机构和个人之间快速、稳定、极低成本地转移。恒星币供应量为 1000 亿枚，其中 95% 将用于免费发放。

80、（小蚁股）/ NEO

非盈利的社区化的区块链项目 NEO（小蚁股（曾用名））是一个非盈利的社区化的 区块链项目，是利用区块链技术和数字身份进行资产数字化，利用智能合约对数字资 产进行自动化管理，实现“[智能经济](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%99%BA%E8%83%BD%E7%BB%8F%E6%B5%8E&zhida_source=entity)”的一种分布式网络。NEO 于 2014 年正式立项， 2015 年 6 月在 Github 上实时开源。NEO 总发行量 1 亿枚并在创世区块中一次性创设， 并实行双代币机制，另一代币为 GAS （小蚁币（曾用名））。

81、区块链技术（Block Chain）

是指通过去中心化的方式集体维护一个可靠数据库的[技术方案](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%8A%80%E6%9C%AF%E6%96%B9%E6%A1%88&zhida_source=entity)。该技术方案主要让区块（Block）通过密码学方法相关联起来，每个[数据块](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%95%B0%E6%8D%AE%E5%9D%97&zhida_source=entity)包含了一定时间内的系统全部数据信息，并且生成[数字签名](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D&zhida_source=entity)以验证信息的有效性并链接到下一个数据块形成一条主链（Chain）。

82、哈希散列(Hash)

是密码学里的经典技术，把任意长度的输入通过哈西算法，变换成固定长度的由字母和数字组成的输出。

83、数字签名（Digital Signature）

[数字签名算法](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D%E7%AE%97%E6%B3%95&zhida_source=entity)是一种用户可以用私钥为文档产生一段叫做签名的短字符串数据的处理，以至于任何拥有相应公钥，签名和文档的人可以验证（1）该文件是由特定的私钥的拥有者“签名”的，（2）该文档在签名后没有被改变过。请注意，这不同于传统的签名，在传统签名上你可以在签名后涂抹多余的文字，而且这样做无法被分辨;在数字签名后任何对文档的改变会使签名无效。

84、[公钥加密](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%85%AC%E9%92%A5%E5%8A%A0%E5%AF%86&zhida_source=entity)

一种特殊的加密，具有在同一时间生成两个密钥的处理（通常称为私钥和公钥），使得利用一个钥匙对文档进行加密后，可以用另外一个钥匙进行解密。一般地，正如其名字所建议的，个人发布他们的公钥，并给自己保留私钥。

85、确认

当一项交易被区块收录时，我们可以说它有一次确认。矿工们在此区块之后每再产生一个区块，此项交易的确认数就再加一。当确认数达到六及以上时，通常认为这笔交易比较安全并难以逆转。

86、搬砖

一种生动而幽默的说法，学名套利。所谓搬砖，就是指当不同的[比特币交易](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%AF%94%E7%89%B9%E5%B8%81%E4%BA%A4%E6%98%93&zhida_source=entity)平台存在着价差时，“搬砖工”发现这一情况，在价低的平台买入比特币，再到价高的平台卖出比特币，从而赚取低风险差价的一种投机行为。

87、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](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E7%94%B5%E5%AD%90%E8%B4%A7%E5%B8%81&zhida_source=entity)已经进入流通，那么比特币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。

88、[半衰期](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%8D%8A%E8%A1%B0%E6%9C%9F&zhida_source=entity)

这个针对比特币产生的一个概念，即为矿工每验证一个区块即可得到的奖励。从最开始的50BTC，每四年减半，目前是12.5BTC,已经历过2次半衰（50BTC–>25BTC–>12.5BTC）。

89、PKI体系

在[非对称加密](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E9%9D%9E%E5%AF%B9%E7%A7%B0%E5%8A%A0%E5%AF%86&zhida_source=entity)中，公钥则可以通过证书机制来进行保护，PKI（Public Key Infrastructure）是建立在公私钥基础上实现安全可靠传递消息和身份确认的一个通用框架，PKI框架包含CA\RA、证书数据库三个重要组件，CA（Certification Authority）：负责证书的颁发和作废，接收来自 RA 的请求，是最核心的部分，RA（Registration Authority）：对用户身份进行验证，校验数据合法性，负责登记，审核过了就发给CA，证书数据库：存放证书，一般采用 LDAP [目录服务](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E7%9B%AE%E5%BD%95%E6%9C%8D%E5%8A%A1&zhida_source=entity)，标准格式采用 X.500 系列。

90、UTXO

Unspent Transaction Outputs是未花费的交易输出，它是比特币交易生成及验证的一个核心概念。交易构成了一组链式结构，所有合法的比特币交易都可以追溯到前向一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。所有的未花费的输出即整个比特币网络的UTXO。比特币规定每一笔新的交易的输入必须是某笔交易未花费的输出，每一笔输入同时也需要上一笔输出所对应的私钥进行签名，并且每个比特币的节点都会存储当前整个区块链上的UTXO，整个网络上的节点通过UTXO及签名算法来验证新交易的合法性。这样，节点不需要追溯历史就可以验证新交易的合法性。

91、找零地址（Change Address）

在使用比特币或者类似的加密货币的时候，我们经常会听到找零地址的概念。找零地址是指：发送金额大于接受金额产生的零钱所去到的地址。和我们一般理解的概念不一样，比特币及比特币的类似货币基于UTXO模型来交易。

简单来说，假设一个地址有10个比特币，那么这10个比特币应该是某个或者某些交易导致的，我们假设以前某个人一次性向这个地址里转入了10个比特币，这个交易称为a，现在我想通过这个地址向另外一个地址发送5个比特币，称之为b交易，那么我需要消耗掉a里所有的比特币，也就是10个。但是我还有5个比特币，这剩下的5个比特币我需要再指定一个地址转入（不考虑手续费），这个地址就是找零地址。（这个地址也可以是原地址，这样原地址还是会有5个比特币）

92、交易拼车

当你从交易所或者一些托管钱包提币出来的时候，经常会发现这笔交易中的发出方或者接收方很多，这是由于这笔交易是一个拼车交易。

在上面说的UTXO模型中，你其实应该已经发现了，b交易其实有两个输出方，一个是我需要转到的地址，一个是找零地址。其实每笔交易的输入也可以是多个，输出也可以是多个，交易所或者钱包把同一时间的提现需求在一笔交易中通过不同输出的方式完成，可以有效降低矿工费。

93、[图灵机](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%9B%BE%E7%81%B5%E6%9C%BA&zhida_source=entity)（英语：Turing machine）

又称确定型图灵机，是英国数学家艾伦·图灵于1936年提出的一种抽象计算模型，其更抽象的意义为一种[数学逻辑](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%95%B0%E5%AD%A6%E9%80%BB%E8%BE%91&zhida_source=entity)机，可以看作等价于任何有限逻辑数学过程的终极强大逻辑机器。

所谓的图灵机就是指一个抽象的机器，它有一条无限长的纸带，纸带分成了一个一个的小方格，每个方格有不同的颜色。有一个机器头在纸带上移来移去。机器头有一组内部状态，还有一些固定的程序。在每个时刻，机器头都要从当前纸带上读入一个方格信息，然后结合自己的内部状态查找程序表，根据程序输出信息到纸带方格上，并转换自己的内部状态，然后进行移动。

94、区块链盲（Blockchain-blindness）

UTXO看不到区块链的数据，例如随机数和上一个区块的哈希。这一缺陷剥夺了[脚本语言](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E8%84%9A%E6%9C%AC%E8%AF%AD%E8%A8%80&zhida_source=entity)所拥有的基于随机性的[潜在价值](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%BD%9C%E5%9C%A8%E4%BB%B7%E5%80%BC&zhida_source=entity)，严重地限制了博彩等其它领域应用。

95、[图灵测试](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%9B%BE%E7%81%B5%E6%B5%8B%E8%AF%95&zhida_source=entity)

1945年到1948年，图灵在国家[物理实验室](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E7%89%A9%E7%90%86%E5%AE%9E%E9%AA%8C%E5%AE%A4&zhida_source=entity)负责自动计算引擎（ACE）的研究工作。1949年，他成为[曼彻斯特](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%9B%BC%E5%BD%BB%E6%96%AF%E7%89%B9&zhida_source=entity)大学计算机实验室的副主任，负责最早的真正的计算机---曼彻斯特一号的软件工作。在这段时间，他继续作一些比较抽象的研究，如“计算机械和智能”。图灵在对人工智能的研究中，提出了一个叫做图灵测试（Turing test）的实验，尝试定出一个决定机器是否有感觉的标准。

1952年，图灵写了一个[国际象棋](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%9B%BD%E9%99%85%E8%B1%A1%E6%A3%8B&zhida_source=entity)程序。可是，当时没有一台计算机有足够的运算能力去执行这个程序，他就模仿计算机，每走一步要用半小时。他与一位同事下了一盘，结果程序输了。

后来美国新墨西哥州[洛斯阿拉莫斯国家实验室](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%B4%9B%E6%96%AF%E9%98%BF%E6%8B%89%E8%8E%AB%E6%96%AF%E5%9B%BD%E5%AE%B6%E5%AE%9E%E9%AA%8C%E5%AE%A4&zhida_source=entity)的研究组根据图灵的理论，在ENIAC上设计出世界上第一个电脑程序的国际象棋－洛斯阿拉莫斯国际象棋。

96、缺少[图灵完备性](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%9B%BE%E7%81%B5%E5%AE%8C%E5%A4%87%E6%80%A7&zhida_source=entity)

这就是说，尽管比特币脚本语言可以支持多种计算，但是它不能支持所有的计算。最主要的缺失是循环语句。不支持循环语句的目的是避免交易确认时出现无限循环。理论上，对于脚本程序员来说，这是可以克服的障碍，因为任何循环都可以用多次重复if 语句的方式来模拟，但是这样做会导致脚本空间利用上的低效率，例如，实施一个替代的[椭圆曲线](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%A4%AD%E5%9C%86%E6%9B%B2%E7%BA%BF&zhida_source=entity)签名算法可能将需要256次重复的乘法，而每次都需要单独编码。

97、价值盲（Value-blindness）

UTXO脚本不能为账户的取款额度提供精细的的控制。例如，预言机合约（oracle contract）的一个强大应用是[对冲合约](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%AF%B9%E5%86%B2%E5%90%88%E7%BA%A6&zhida_source=entity)，A和B各自向对冲合约中发送价值1000美元的比特币，30天以后，脚本向A发送价值1000美元的比特币，向B发送剩余的比特币。虽然实现对冲合约需要一个预言机（oracle）决定一比特币值多少美元，但是与现在完全中心化的解决方案相比，这一机制已经在减少信任和基础设施方面有了巨大的进步。然而，因为UTXO是不可分割的，为实现此合约，唯一的方法是非常低效地采用许多有不同面值的UTXO（例如对应于最大为30的每个k，有一个2^k的UTXO)并使预言机挑出正确的UTXO发送给A和B。

98、缺少状态

UTXO只能是已花费或者未花费状态，这就没有给需要任何其它内部状态的多阶段合约或者脚本留出生存空间。这使得实现多阶段[期权合约](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E6%9C%9F%E6%9D%83%E5%90%88%E7%BA%A6&zhida_source=entity)、去中心化的交换要约或者两阶段加密承诺协议（对确保计算奖励非常必要）非常困难。这也意味着UTXO只能用于建立简单的、一次性的合约，而不是例如去中心化组织这样的有着更加复杂的状态的合约，使得元协议难以实现。二元状态与价值盲结合在一起意味着另一个重要的应用-取款限额-是不可能实现的。

99、[同态加密](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E5%90%8C%E6%80%81%E5%8A%A0%E5%AF%86&zhida_source=entity)

同态加密（Homomorphic Encryption）是一种特殊的加密方法，允许对密文进行处理得到仍然是加密的结果，即对密文直接进行处理，跟对明文进行处理再加密，得到的结果相同。从代数的角度讲，即同态性。

如果定义一个运算符 $$\triangle{}$$，对加密算法 E 和 解密算法 D，满足：

$$ E(X\triangle{}Y) = E(X)\triangle{} E(Y)

$$ 则意味着对于该运算满足同态性。

同态性在代数上包括：加法同态、乘法同态、减法同态和除法同态。同时满足加法同态和乘法同态，则意味着是 代数同态，即 全同态。同时满足四种同态性，则被称为 算数同态。

同态加密的问题最早是由 Ron Rivest、Leonard Adleman 和 Michael L. Dertouzos 在 1978 年提出，但 第一个“全同态”的算法 到 2009 年才被克雷格·金特里（Craig Gentry）证明。

仅满足加法同态的算法包括 Paillier 和 Benaloh 算法；仅满足乘法同态的算法包括 RSA 和 ElGamal 算法。

同态加密在[云时代](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E4%BA%91%E6%97%B6%E4%BB%A3&zhida_source=entity)的意义十分重大。目前，从安全角度讲，用户还不敢将敏感信息直接放到第三方云上进行处理。如果有了比较实用的同态加密技术，则大家就可以放心的使用各种[云服务](https://zhida.zhihu.com/search?content_id=212654672&content_type=Article&match_order=1&q=%E4%BA%91%E6%9C%8D%E5%8A%A1&zhida_source=entity)了。

遗憾的是，目前已知的同态加密技术需要消耗大量的计算时间，还远达不到实用的水平。

100、P2SH脚本

输出脚本由支付者创建，他们（钱花出去之后）不怎么关心他们消费的比特聪的长期安全或者对别人是否有用。

收款人则关心输出脚本指定的条件。如果收款人愿意，他们可以请求支付者使用某种特定脚本。遗憾的是，定制的脚本没有短小的比特币地址方便，也不像P2PKH的公钥哈希方案( P2PKHpubkey hashes)那样容易保护。

为了解决这些问题，“支付到脚本哈希”（P2SH）交易在2012年被创建，它让支付者创建一个输出脚本，里边包含另一个脚本的哈希，另一个脚本称为“认领脚本”

101、“幽灵“协议（"Greedy Heaviest Observed Subtree" (GHOST) protocol）

是由Yonatan Sompolinsky 和 Aviv Zohar在2013年12月引入的创新。[幽灵协议](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%B9%BD%E7%81%B5%E5%8D%8F%E8%AE%AE&zhida_source=entity)提出的动机是当前快速确认的块链因为区块的高作废率而受到低安全性困扰；因为区块需要花一定时间（设为t）扩散至全网，如果矿工A挖出了一个区块然后矿工B碰巧在A的区块扩散至B之前挖出了另外一个区块，[矿工](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=3&q=%E7%9F%BF%E5%B7%A5&zhida_source=entity)B的区块就会作废并且没有对[网络安全](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8&zhida_source=entity)作出贡献。此外，这里还有中心化问题：如果A是一个拥有全网30%算力的矿池而B拥有10%的算力，A将面临70%的时间都在产生作废区块的风险而B在90%的时间里都在产生作废区块。因此，如果作废率高，A将简单地因为更高的算力份额而更有效率，综合这两个因素，区块产生速度快的块链很可能导致一个矿池拥有实际上能够控制挖矿过程的算力份额。

102、[默克尔树](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E9%BB%98%E5%85%8B%E5%B0%94%E6%A0%91&zhida_source=entity)

默克尔树是一种二叉树，由一组[叶节点](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%8F%B6%E8%8A%82%E7%82%B9&zhida_source=entity)、一组中间节点和一个根节点构成。最下面的大量的叶节点包含基础数据，每个中间节点是它的两个子节点的[哈希](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%93%88%E5%B8%8C&zhida_source=entity)，根节点也是由它的两个子节点的哈希，代表了默克尔树的顶部。默克尔树的目的是允许区块的数据可以零散地传送：节点可以从一个源下载区块头，从另外的源下载与其有关的树的其它部分，而依然能够确认所有的数据都是正确的。之所以如此是因为哈希向上的扩散：如果一个恶意用户尝试在树的下部加入一个伪造的交易，所引起的改动将导致树的上层节点的改动，以及更上层节点的改动，最终导致根节点的改动以及区块哈希的改动，这样协议就会将其记录为一个完全不同的区块（几乎可以肯定是带着不正确的工作量证明的）。

103、共识机制

区块链从本质上而言是一种[分布式账本技术](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%88%86%E5%B8%83%E5%BC%8F%E8%B4%A6%E6%9C%AC%E6%8A%80%E6%9C%AF&zhida_source=entity)。传统的账本，通常会以[数据库](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%95%B0%E6%8D%AE%E5%BA%93&zhida_source=entity)的形式，集中存储在银行或公司的[服务器节点](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%9C%8D%E5%8A%A1%E5%99%A8%E8%8A%82%E7%82%B9&zhida_source=entity)上。而在区块链的网络中，每个节点都会保有一份完整的账本，且所有节点的账本内容完全一致。每个节点都可以根据自己本地的账本去查找交易，也可以往账本中添加交易。

这样就带来了一个问题，如果所有节点同时一起写入账本数据，那么肯定数据会不一致。因此需要一种机制来保证区块链中的每一区块只能由一个节点来负责写入，并且让所有其他节点一致认同这次写入。如何选出写入账本数据的节点，这就是共识机制。

104、PBFT

实用[拜占庭](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%8B%9C%E5%8D%A0%E5%BA%AD&zhida_source=entity)容错协议（PBFT，Practical Byzantine Fault Tolerance）是Miguel Castro (卡斯特罗)和Barbara Liskov（利[斯科夫](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%96%AF%E7%A7%91%E5%A4%AB&zhida_source=entity)）在1999年提出来的，解决了原始拜占庭容错算法（即上文中的口头协议）效率不高的问题，将[算法复杂度](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E7%AE%97%E6%B3%95%E5%A4%8D%E6%9D%82%E5%BA%A6&zhida_source=entity)由指数级降低到多项式级，使得[拜占庭容错算法](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=2&q=%E6%8B%9C%E5%8D%A0%E5%BA%AD%E5%AE%B9%E9%94%99%E7%AE%97%E6%B3%95&zhida_source=entity)在实际系统应用中变得可行。

PBFT算法的结论是n>=3f+1 n是系统中的总节点数，f是允许出现故障的[节点数](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=2&q=%E8%8A%82%E7%82%B9%E6%95%B0&zhida_source=entity)。换句话说，如果这个系统允许出现f个故障，那么这个系统必须包括n个节点，才能解决故障。这和上文口头协议的结论一样，或者这么说，PBFT是优化了口头协议机制的效率，但是结论并未改变。

105、Ethereum

由于ASIC矿机被大量运用在[比特币](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%AF%94%E7%89%B9%E5%B8%81&zhida_source=entity)的挖矿过程中，所以如果出现其他基于hash运算达到共识的区块链，则很容易受到原本服务于比特币的ASIC矿机攻击。因此Ethereum在设计其PoW[共识算法](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%85%B1%E8%AF%86%E7%AE%97%E6%B3%95&zhida_source=entity)的时候，就意识到应该让算法在普通的个人电脑上运行更有优势，从而避免被ASIC进行攻击。

106、Delegated Methods

以上的PoW和PoS的挖矿过程，是全网所有节点共同参与的，每一时刻都有成千上万个节点同时去争取产出下一个block，因此会时有发生区块链分叉（fork）的问题。即同一时刻，两个节点同时产出了next block，但由于网络时延的问题，block产出的时候两个节点并不知道有其他节点已经产出了另一个block，因此这两个block都被发布到了网络中。[5]中对分叉的问题有详细的描述，可以进行参考。

正是由于分叉的存在，block的产出时间间隔不能太短。各区块链通过动态调整的挖矿难度，将block时间间隔稳定在自己期望的水平。例如最初比特币的间隔是10分钟，后续的[以太坊](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E4%BB%A5%E5%A4%AA%E5%9D%8A&zhida_source=entity)是15秒左右。如果时间间隔进一步调短（即降低挖矿难度），分叉问题就会大量显现，不利于共识的达成和系统的稳定。

107、冷存储

该术语指的是离线保存比特币。当比特币的私钥被创建，同时将该私钥存储在安全的离线环境时，就实现了冷存储。冷存储对于任何比特币持有者来说是重要的。在线计算机在黑客面前是脆弱的，不应该被用于存储大量的比特币。

108、染色币

比特币2.0[开源协议](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%BC%80%E6%BA%90%E5%8D%8F%E8%AE%AE&zhida_source=entity)允许开发者在比特币区块链之上，利用它的超越货币的功能创建[数字资产](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%95%B0%E5%AD%97%E8%B5%84%E4%BA%A7&zhida_source=entity)。

109、共识

当网络中的许多节点，通常是大部分节点，都拥有相同的本地验证的最长区块时，称为共识。不要与共识规则混淆。

110、难度

整个网络会通过调整“难度”这个变量来控制生成工作量证明所需要的计算力。

111、难度重定

全网中每新增2016个区块，全网难度将重新计算，该新难度值将依据前2016个区块的[哈希算力](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%93%88%E5%B8%8C%E7%AE%97%E5%8A%9B&zhida_source=entity)而定。

112、难度目标

使整个网络的计算力大致每10分钟产生一个区块所需要的难度数值即为难度目标。

113、[双重支付](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%8F%8C%E9%87%8D%E6%94%AF%E4%BB%98&zhida_source=entity)

双重支付是成功支付了1次以上的情况。比特币通过对添加到区块中的每笔交易进行验证来防止双重支付，确保交易的输入没有被支付过。

114、ECDSA

[椭圆曲线数字签名算法](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%A4%AD%E5%9C%86%E6%9B%B2%E7%BA%BF%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D%E7%AE%97%E6%B3%95&zhida_source=entity)（ECDSA）是比特币使用的加密算法，以确保资金只能被其正确拥有者支付。

115、超额随机数

随着难度增加，矿工通常在循环便利4亿次随机数值后仍未找到区块。因为coinbase脚本可以存储2到100字节的数据，矿工开始使用这个存储空间作为超额nonce空间，允许他们利用一个更大范围的区块头[哈希值](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%93%88%E5%B8%8C%E5%80%BC&zhida_source=entity)来寻找有效的区块。

116、创世块

[创世区块](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%88%9B%E4%B8%96%E5%8C%BA%E5%9D%97&zhida_source=entity)指区块链上的第一个区块，用来初始化相应的加密货币。

117、硬件钱包

硬件钱包是一种特殊的比特币钱包，硬件钱包可以将用户的私钥存储在安全的硬件设备中。

118、哈希锁

哈希锁是限制一个输出花费的限制对象，其作用一直持续到指定数据片段公开透露。哈希锁有一个有用的属性，那就是一旦任意一个哈希锁被公开打开，其他任何安全使用相同密钥的哈希锁也可以被打开。这使得可能创建多个被同意哈希锁限制的输出，这些支出将在同一时间被花费。

119、HD协议

层级确定性（HD）密钥创建和传输协议（BIP32），该协议允许按层级方式从父密钥创建子密钥。

120、HD钱包

使用创建层次确定的钥匙和BIP32传输协议的钱包。

121、HD钱包种子

HD钱包种子或根种子是一个用于为HD钱包生成主私钥和主链码所需种子的潜在简短数值。

122、哈希时间锁定合约

哈希时间锁定合约（HTLC）是一类支付方式，其使用哈希锁和[时间锁](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=3&q=%E6%97%B6%E9%97%B4%E9%94%81&zhida_source=entity)来锁定交易。解锁需要接收方提供通过加密支付证明承认在截止日期之前收到了支付，或者接收方丧失了认领支付的能力，此时支付金额将返回给支付方。

123、KYC

充分了解你的账户（KYC，Know yourcustomer）是一个商业过程，用于认证和验证顾客的身份信息。也指银行对这些活动的监管。

124、LevelDB

LevelDB是一个开源的硬盘键值对数据库。LevelDB是一个用于持久性绑定多个平台的轻量级、单用途的库。

125、锁定时间

锁定时间（技术上来说是nLockTime）是交易的一部分，其表明该交易被添加至区块链中的最早时间或区块。

126、[交易池](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E4%BA%A4%E6%98%93%E6%B1%A0&zhida_source=entity)

比特币内存池是区块中所有交易数据的集合，这些交易已经被比特币节点验证，但为被确认。

127、随机数

随机数是比特币区块中一个32位（4字节）的字段，在设定了该值后，才能计算区块的哈希值，其哈希值是以多个0开头的。区块中的其他字段值是不变的，因为他们有确定的含义。

128、离线交易

离线交易是区块链外的价值转移。当在链交易（通常简单来说就是一个交易）修改区块链并依赖区块来决定它的有效性时，离线交易则依赖其他方法来来记录和验证该交易。

129、操作码

操作码来源于比特币[脚本语言](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E8%84%9A%E6%9C%AC%E8%AF%AD%E8%A8%80&zhida_source=entity)，通过操作码可以在公钥脚本或签名脚本中实现压入数据或执行函数的操作。

130、开放资产协议

开放资产协议是一个建立在比特币区块链纸上简单有效的协议。它允许用户创建资产的发行和传输。开放资产协议是颜色币概念的一个进化。

131、OP\_RETURN

一个用在OP\_RETURN交易中的一种输出操作码。不要与OP\_RETURN交易混淆。

132、OP\_RETURN交易

OP\_RETURN在比特币核心0.9.0中默认的一种被传播和挖出的[交易类型](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E4%BA%A4%E6%98%93%E7%B1%BB%E5%9E%8B&zhida_source=entity)，在随后的版本中添加任意数据至可证明的未花费公钥脚本中，全节点中无需将该脚本存储至他们的UTXO数据库中。不要与OP\_RETURN操作码混淆。

133、孤块

孤块由于父区块未被本地节点处理的区块，所以他们还不能被完全验证。

134、孤立交易

孤立交易是指那些因为缺少一个或多个输入交易而无法进入交易池的交易。

135、交易输出

交易输出（TxOut）是交易中的输出，交易输出中包含两个字段：1.输出值字段：用于传输0或更多聪；2.公钥脚本：用于确定这些聪需在满足什么条件的情况下才可花费。

136、P2PKH

支付到比特币地址的交易包含支付公钥哈希脚本（P2PKH）。由P2PKH脚本锁定的交易输出可以通过给出由相应私钥创建的公钥和数字签名来解锁（消费）。

137、P2SH

P2SH是一种强大的、新型的、且能大大简化复杂交易脚本的交易类型而引入。通过使用P2SH，详细描述花费输出条件的复杂脚本（赎回脚本）将不会出现在锁定脚本中。相反，只有赎回脚本哈希包含在锁定脚本中。

138、P2SH地址

P2SH地址是基于Base58 编码的一个含有20 个字节哈希的脚本。P2SH地址采用“5”前缀。这导致基于Base58 编码的地址以“3”开头。P2SH 地址隐藏了所有的复杂性，因此，运用其进行支付的人将不会看到脚本。

139、P2WPKH

P2WPKH签名包含了与P2PKH花费相同的信息。但是签名信息放置于见证字段，而不是签名脚本字段中。公钥脚本也被修改了。

140、P2WSH

P2WSH与P2SH的不同之处在于加密证据存放位置从脚本签名字段转变至见证字段，公钥脚本字段也被改变。

141、纸钱包

在大多数特定含义下，纸钱包是一个包含所有必要数据的文件，这些数据用于生成比特币私钥，形成密钥钱包。然而，人们通常使用该术语来表达以物理文件形式离线存储比特币的方式。第二个定义也包括纸密钥和[可赎回](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%8F%AF%E8%B5%8E%E5%9B%9E&zhida_source=entity)编码。

142、支付通道

[微支付](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%BE%AE%E6%94%AF%E4%BB%98&zhida_source=entity)通道和支付通道是 设计用于允许用户生成多个[比特币交易](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%AF%94%E7%89%B9%E5%B8%81%E4%BA%A4%E6%98%93&zhida_source=entity)，且无需提交所有交易至比特币区块链中。在一个典型的支付通道中，只有两个交易被添加至区块链中，但参与双方可以生成无限制或接近无限制数量的支付。

143、奖励

每一个新区块中都有一定量新创造的比特币用来奖励算出工作量证明的矿工。现阶段每一区块有12.5比特币的奖励。

144、RIPEMD-160

RIPEMD-160是一个160位的加密[哈希函数](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%93%88%E5%B8%8C%E5%87%BD%E6%95%B0&zhida_source=entity)。RIPEMD-160是RIPEMD的加强版，其哈希计算后的结果是160位哈希值。通过RIPEMD-160加密期望能实现在未来的10年或更长时间都是安全的。

145、脚本

比特币使用脚本系统来处理交易。脚本有着类Forth语言、简单、基于堆栈以及从左向右处理的特点。脚本故意限定为非[图灵完备](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%9B%BE%E7%81%B5%E5%AE%8C%E5%A4%87&zhida_source=entity)的，没有循环计算功能。

146、PubKey (公钥脚本)

脚本公钥或者公钥脚本是包含在交易输出中的脚本。该脚本设置了比特币花费需满足的条件。满足条件的数据可以由签名脚本提供。

147、Sig (签名脚本)

签名脚本是有支付端生成的数据，该数据几乎总是被用作满足公钥脚本的变量。

148、SHA

安全哈希是有NIST（国家标准技术研究所）发布的加密哈希函数族。

软分叉:软分叉是区块链中的一个短暂分叉，通常是由于矿工在不知道新共识规则的情况下，未对其使用节点进行升级而产生的。不要与分叉、硬分叉、软分叉或者Git分叉混淆。

149、SPV (简化支付验证)

简化支付验证是在无需下载所有区块的情况对特定交易进行验证的方法。该方法被用在一些比特币轻量级客户端中。

150、旧块

旧块是那些被成功挖出，但是没有包含在当前主链上的区块，很有可能是同一高度的其他区块优先扩展了区块链长度导致的。

时间锁:时间锁是一种阻碍类型，用于严格控制一些比特币只能在将来某个特定时间和区块才能被支出。时间锁在很多比特币合约中起到了显著的作用，包括支付通道和哈希时间锁合约。

151、环签名

环签名由 Rivest,shamir 和 Tauman 三位密码学家在 2001 年首次提出。环签名属于一种简化的[群签名](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E7%BE%A4%E7%AD%BE%E5%90%8D&zhida_source=entity)。

签名者首先选定一个临时的签名者集合,集合中包括签名者自身。然后签名者利用自己的私钥和签名集合中其他人的公钥就可以独立的产生签名,而无需他人的帮助。签名者集合中的其他成员可能并不知道自己被包含在其中。

152、[数字证书](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%95%B0%E5%AD%97%E8%AF%81%E4%B9%A6&zhida_source=entity)

数字证书用来证明某个公钥是谁的。

对于数字签名应用来说，很重要的一点就是公钥的分发。一旦公钥被人替换，则整个安全体系将被破坏掉。

怎么确保一个公钥确实是某个人的原始公钥？这就需要数字证书机制。顾名思义，数字证书就是像一个证书一样，证明信息和合法性。由证书[认证机构](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E8%AE%A4%E8%AF%81%E6%9C%BA%E6%9E%84&zhida_source=entity)（Certification Authority，CA）来签发。

数字证书内容可能包括版本、序列号、签名算法类型、签发者信息、有效期、被签发人、签发的[公开密钥](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5&zhida_source=entity)、CA 数字签名、其它信息等等。其中，最重要的包括 签发的公开密钥、CA 数字签名 两个信息。

因此，只要通过这个证书就能证明某个公钥是合法的，因为带有 CA 的数字签名。更进一步地，怎么证明CA 的签名合法不合法呢？类似的，CA 的数字签名合法不合法也是通过 CA 的证书来证明的。

主流[操作系统](https://zhida.zhihu.com/search?content_id=212692211&content_type=Article&match_order=1&q=%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F&zhida_source=entity)和浏览器里面会提前预置一些 CA 的证书（承认这些是合法的证书），然后所有基于他们认证的签名都会自然被认为合法。

原文链接：

[区块链150个专业名词解释（上） - 知乎](https://zhuanlan.zhihu.com/p/560134390)

[区块链150个专业名词解释（中） - 知乎](https://zhuanlan.zhihu.com/p/560349017)

[区块链专业名词解释150条（下） - 知乎](https://zhuanlan.zhihu.com/p/560517672)