**1、地址（Addresses）**

加密数字货币地址，用于在网络上接收和发送事务。地址是一个字母数字字符串，但也可以表示为可扫描的 QR 码。

**2、协议分类账（Agreement ledger）**

是由两方或多方用来协商和达成协议的分布式分类账。

**3、比特币的替代品或着山寨版（Altcoin，Bitcoin alternative）**

目前，大多数 Altcoin 都是比特币的分叉，通常比特币区块链的工作量证明（POW）算法有一些细微变化。最出名的 Altcoin 是莱特币，莱特币引入了原始比特币协议的变化，例如减少块生成时间，增加最大货币数量和不同的哈希算法。

**4、认证分类账（Attestation Ledgers）**

提供持久的协议，承诺或声明记录，提供证据（证明）这些协议，承诺或陈述是人为作出的。

**5、专用集成电路（ASIC）**

是专门设计用于执行单个任务的硅芯片。在比特币中，它们被设计为处理 SHA-256 散列问题以挖掘新的比特币。

**6、比特币（Bitcoin）**

是一个众所周知的加密货币，基于 POW 区块链。是在全球对等网络上运行的第一个去中心化开放源代码的加密货币，不需要中间商和集中式发行商。

**7、区块（Block）**

是在区块链网络上承载永久记录的数据的数据包。

**8、区块链（Blockchain）**

是一种分布式分类账，由不可更改的数字化记录的数据组成，称为数据块（更像是将数据整理成一张纸）。然后使用加密签名将每个块“链接”到下一个块。这允许块链像分类帐一样使用，具有适当权限的任何人可以共享和访问。

**9、区块资源管理器（Block Explorer）**

是一种用来查看区块上的所有交易（过去和当前）在线工具。它们提供有用的信息，如网络哈希率和交易增长率。

**10、分组密码（Block cipher）**

是一种对文本进行加密（以产生密文）的方法，其中密码密钥和算法一次作为一组应用于数据块，而不是一次一个 bit。

**11、块高度（Block height）**

是指块链中连接在一起的块的数量。例如，高度 0 即是第一块，也就是所谓的成因块。

**12、块奖励（Block reward）**

给予已成功散列一个事务块的矿工。块奖励可以是硬币和交易费用的混合，取决于所讨论的加密货币使用的策略，以及所有的硬币是否已经被成功开采。比特币网络的当前块奖励是每个块有 25 个比特币。

**13、中央分类帐（Central ledger）**

是指由中央机构维护的分类帐。

**14、链式链接（Chain linking）**

是将两个区块链彼此连接的过程，从而允许在链之间进行交易。这将允许像比特币这样的区块链与其他侧链进行沟通，允许它们之间的资产交换。

**15、密码（cipher）**

是用于信息加密或解密的算法。在通用语言中，“密码”也被用来指代加密消息，也被称为“代码”（code）。

**16、确认（Confirmation）**

意味着区块链交易已经被网络验证。这是在 POW 系统（比如比特币）中所谓挖掘的过程发生的。一旦交易被确认，不能被撤销或双重消费。交易的确认越多，执行双重支出攻击就越困难。

**17、共识流程（Consensus Process）**

是一组对等点，负责维护分布式账本的使用，以达到分类账内容的共识。

**18、一个联盟区块链（Consortium blockchain）**

是一个共识过程由一组预先选定的节点控制的区块链；例如，可以想象一个由15 个金融机构组成的联盟，每个联盟都运行一个节点，其中必须有十个成员在每个块上签字，才能使该块有效。阅读区块链的权利可能是公开的，也可能仅限于参与者。还有一些混合路由，例如块的根哈希值与 API 一起公开，允许公众成员进行有限数量的查询，并获得区块链状态某些部分的密码证明。这些区块链可能被认为是“半分布式的”。

**19、密码分析（Cryptoanalysis）**

是研究获得加密信息的含义的方法，而不需要访问通常需要的秘密信息。

**20、加密数字货币（Cryptocurrency）**

是基于数学的数字货币形式，其中使用加密技术来调节货币单位的生成并验证资金的转移。此外，加密货币独立于中央银行运作。

**21、加密哈希函数（Cryptographic Hash Function）**

密码哈希产生从可变大小交易输入固定大小和唯一哈希值。 SHA-256 计算算法是加密散列的一个例子。

**22、去中心化应用程序（Dapp）**

是一种开源的应用程序，自动运行，将其[数据存储](https://cloud.tencent.com/product/cdcs?from=20067&from_column=20067)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。

**23、密码使用法（Cryptography）**

是指加密和解密信息的过程。

**24、分散的自治组织（一个DAO）**

可以被认为是一个没有任何人的参与下运行的公司，在一套不可变的商业规则的控制之下。

**25、DAO（去中心化自治组织）**

是建立在以太坊上的一个风险投资基金，它引发了一次软/硬分叉。去中心化自治组织可以被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。

**26、解密（Decryption）**

是将密文变成纯文本的过程。

**27、加密（Encryption）**

是将明文消息（明文）转换成数据流（密文）的过程，使其看起来像一个无意义的随机的比特序列。

**28、双重支付（Double Spending）**

当花费一笔钱多于一次支付限额时，就会发生双重支付。

**29、以太（Ether）**

是以太坊区块链的原生代币，它用于支付交易费用、矿工奖励和网络上的其他服务。

**30、以太坊（Ethereum）**

是一个基于[区块链技术](https://cloud.tencent.com/product/blockchain-catalog?from=20067&from_column=20067)的开放式软件平台，支持开发人员撰写智能合约，构建和部署分散式应用程序。

**31、以太坊经典（Ethereum Classic）**

是现有加密数字货币的分拆，经过硬分叉后的以太坊。

**32、以太坊虚拟机（EVM）**

是以太坊区块链上的帐户可以包含代码的编程语言。每次向该帐户发送消息时，都会执行与帐户关联的 EVM 代码，且可以读取/写入存储并自行发送消息。

**33、数字商品（Digital commodity）**

是一种稀缺的，可电子转让的，无形的，具有市场价值的虚拟商品。

**34、**[**数字身份**](https://cloud.tencent.com/product/tdid?from=20067&from_column=20067)**（Digital identity）**

是由个人组织或电子设备在网络空间中采用或声明的在线的网络身份。

**35、分布式账本（Distributed ledger）**

是分布在多个站点，国家或机构中的一种数据库。记录一个接一个地存储在连续分类账中。分布式账本数据可以通过“许可”或“不许可”来控制谁可以查看它。

**36、分布式网络（Distributed Network）**

处理能力和数据分布在节点上而不是拥有集中式数据中心的一种网络。

**37、容易程度（Difficulty）**

是指成功挖掘交易信息的数据块的容易程度。

**38、难度（Difficulty）**

在“POW”挖掘中，验证区块链网络中的区块是非常困难的。在比特币网络中，采矿难度调整为每隔 2016 个块进行验，这是为了保持块验证时间在十分钟。

**39、双倍支出（Double spend）**

是比特币网络中的一种情况，即有人试图同时向两个不同的收款人发送比特币交易。但是，一旦比特币交易得到确认，就几乎不可能将花费翻倍。特定交易的确认越多，双倍花费比特币就越难。

**40、菲亚特货币（Fiat currency）**

是指政府宣布为履行财务义务而有效的任何货币（如美元或欧元）。

**41、分叉（Fork）**

是通过在网络的不同部分同时创建两个区块来创建一个正在进行的区块链替代版本。这会创建两个平行的区块链，其中一个是获胜区块链。

**42、创世区块（Genesis Block）**

区块链的第一个区块。

**43、气体（Gas）**

是一个与计算步骤大致相当的测量法（以太坊）。每笔交易都需要包括一个 Gas 限制和一个愿意为每个 Gas 支付的费用；矿工可以选择进行交易和收费。每个操作都有一个 Gas 支出；对于大多数操作来说，支出范围在 3-10，虽然一些昂贵的操作花费高达 700，但一般这种情况下，交易本身花费高达 21000。

**44、减半（Halving）**

比特币的供应有限，这使得它们成为稀缺的数字商品。将要发行的比特币总量为 2100 万。每块产生的比特币数量每四年下降 50%。这就是所谓的“减半”，最后的减半将在 2140 年完成。

**45、硬分叉（Hardfork）**

是对区块链协议的改变，使先前无效的块/交易有效，因此要求所有用户升级其客户端。

**46、Hashcash**

是一个用于限制垃圾邮件和拒绝服务攻击的 POW 系统，最近以其在比特币（和其他加密货币）中的使用而成为挖掘算法的一部分。

**47、哈希（Hash）**

也叫做散列函数，是指把任意长度的输入变换成固定长度的输出，该输出就是哈希值（散列值）。哈希值是一段数据唯一且极其紧凑的数值表示形式。如果散列一段明文而且哪怕只更改一个字母，随后的哈希都将产生不同的值。要找到哈希值相同的两个不同的输入，在计算上是不可能的。HASH 算法是密码学的基础，比较常用的有 MD5 和 SHA，不可逆和无冲突是其重要性质。不可逆是指：知道 A 的 HASH 值，无法求出 A；无冲突是指：知道 A，无法求出一个 B， 使 A 与 B 的 HASH 值相同。

**48、哈希率（Hashrate）**

是比特币矿工在给定的时间段(通常是一秒)内可执行的哈希值。

**49、首次代币发行（ICO）**

是一种事件，指新的加密数字货币从总体基础币出售高级代币以换取前期资本。 ICO 经常被用于新的加密数字货币的开发者来筹集资金。

**50、分类账（Ledger）**

是一个仅追加记录的存储器，记录是不可变的，可能比财务记录拥有更多的一般信息。

**51、莱特币（Litecoin）**

是基于 Scrypt 工作量证明网络的点对点加密货币。有时被称为比特币黄金中的白银。

**52、挖矿（Mining）**

是验证交易并将其添加到区块链的过程。这个使用计算硬件解决密码问题的过程也触发了加密货币的发行。

**53、矿池（Mining Pool）**

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）。这使得矿工能够获得持续稳定的收入，而不是小概率的一次性获得一个区块产生的比特币奖励。

**54、多重签名（Multi-Signature）**

地址允许多方要求多个密钥授权交易。在创建地址时同意所需的签名数量。多重签名地址对盗窃具有更大的抵抗力。

**55、节点（Node）**

是连接到区块链网络的任何计算机。

**56、Oracles（数据库）**

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。

**57、完整节点（Full node）**

是完全实施区块链的所有规则的节点。

**58、点对点（P2P）**

是指在高度互连的网络中至少两方之间发生的去中心化交互。 P2P 参与者通过一个中介点直接处理彼此。

**59、公用地址（Public Address）**

公共地址是公钥的密码哈希值。它们作为可以在任何地方发布的电子邮件地址，与私钥不同。

**60、被许可的分类帐（Permissioned ledger）**

是行动者必须有权访问的分类帐。被许可的分类帐可能有一个或多个所有者。当添加新记录时，分类账的完整性将通过有限的共识流程进行检查。这是由信任的行动者（例如政府部门或银行）执行的，举个例子——未被许可的分类账使用的共识形成过程会使得维持一个共享记录要简单得多。

**61、被许可的区块链（Permissioned blockchain）**

提供了高度可验证的数据集，因为共识流程创建了数字签名，各方都可以看到。

**62、私钥（Private key）**

是一串数据，表明您可以访问特定钱包中的比特币。私钥可以被认为是一个密码;私钥绝不能透露给任何人，因为密钥允许你通过加密签名从你的比特币钱包里支付比特币。

**63、权威证明（Proof of Authority）**

是私人区块链中的一种共识机制，它基本上为一个客户（或特定数量的客户）提供一个特定的私人密钥，使得区块链中的所有区块都成为可能。

**64、权益证明（Proof of Stake）**

是工作量证明系统的替代方案，在这种系统中，您使用加密货币的现有股份（您持有货币的数量）来计算您可以挖掘的货币数量。

**65、工作量证明（Proof of Work）**

是一个将挖掘能力与计算能力联系起来的系统。块必须被散列，这本身就是一个简单的计算过程，但是在散列过程中增加了一个额外的变量，使其变得更加困难。当一个块被成功散列时，散列必须花费一些时间和计算量。因此，散列块被认为是工作量的证明。

**66、协议（Protocol）**

是描述如何传输或交换数据的正式规则集，特别是在整个网络中。

**67、Ripple**

是建立在分布式账本上的支付网络，可以用来转账任何货币。该网络由支付节点和由当局运营的网关组成。付款是使用一系列的借条进行的，网络基于信任关系。

**68、Scrypt**

是 SHA-256 工作系统的一个替代证明，旨在对 CPU 和 GPU 矿工特别友好，然而对 ASIC 矿工没有什么优势。

**69、SHA 256**

是用作比特币工作证明系统基础的密码函数。

**70、智能合约（Smart contract）**

是其条款以计算机语言记录而非法定语言的合约。智能合约可以由计算系统自动执行，例如合适的分布式账本系统。

**71、软分叉（Softfork）**

是对比特币协议的一个修改，其中只有以前有效的块/事务被无效。由于旧节点会将新块识别为有效，所以软分叉是向后兼容的。这种分叉只需要大量矿工来升级执行新规则。

**72、流密码（Stream ciphers）**

是一种对文本（密文）进行加密的方法，其中密码密钥和算法一次一bit地应用于数据流中的每个二进制数字。

**73、代币（Token）**

是可以被获取的东西的数字身份。

**74、无代币分类帐（Tokenless ledger）**

是指不需要本地货币操作的分布式分类帐。

**75、交易区块（Transaction block）**

是比特币网络上的交易集合，集合成一个块，然后可以将其散列并添加到区块链中。

**76、交易费用（Transaction fees）**

是对通过比特币网络发送的一些交易征收的小额费用。交易费用授予那些成功散列包含相关交易的块的矿工。

**77、分类账（Unpermissioned ledgers）**

像比特币这样的未经许可的分类账没有单一的所有者——事实上，它们不能被拥有。未经许可的分类帐的目的是允许任何人向分类帐提供数据，并为拥有分类账的每个人提供相同的副本。

**78、图灵完备（Turing Complete）**

图灵完备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。一个例子是Ethereum虚拟机（EVM）。

**79、钱包（Wallet）**

是一个包含私钥集合的文件。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。

**80、51% 攻击（51% Attack）**

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。

-