区块链行业词典

维京研究院 & 甲子智库

2018年2月26日

维京资本
VIKING CAPITAL

甲子光年
JAZZYEAR

区块链行业词典

维京研究院 & 甲子智库

2018 年 2 月 26 日

顾问合作方：清华大学校友区块链协会、鲸准研究院、NEO GLOBAL CAPITAL、万向区块链实验室、SegmentFault、云象区块链、哈希世界、分布科技、边界智能、王逵、张宇文、田甲、李岩

媒体合作方：今日头条、百度百家、36 氪、品途商业评论、WeMedia、BlockMedia、31 区、新共识、BiaNews、三言财经

主编：Bobo Jin、甲小姐、程曼祺

责任编辑：曾元佐、何思谊　**编辑：**涂靖靖、邓璐、姚毅

校对：王洋、张筱璇、李凯悦、陈文汇

目录

区块链简介

2008 年，中本聪发表了《比特币：一种点对点的电子现金系统》白皮书，以区块链技术为核心，使得在线支付能够直接由一方发起并支付给另一方，中间不需要通过任何的金融机构。这份文件被视为区块链技术的开端。

简言之，区块链技术是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术，并不是一种单一的、全新的技术，而是多种现有技术整合的结果，包含“区块 + 链”的数据结构、分布式存储、加密算法、共识机制四大核心技术。

通俗地说，区块链相当于一个“串珠”的过程，就像向一条基于时间的射线上不断追加新的珠子，在链上不断新增新的区块；当然，“链”并非真实存在，只是基于密码学以及时间戳的原理在时间上凸显先后次序，而“区块”也不是直观上认为的珠子，而是拥有存储信息能力的网络事务数据包，数据包内可以包含转账交易数据、智能合约代码或执行数据等信息。

“分布式存储”则是指串珠并非仅仅由个人完成，而是一个公开的、透明的、无中心程序，由一个称作“共识机制”的方式决定“谁”有权力在线上“串珠”，通过游戏规则获得串珠权力的人则可以得到系统奖励的代币，这就是所谓的“挖矿”。也就是说，通过在区块链网上依据共识机制争夺记账权，成功的节点将得到记账权以及伴生的记账奖励和交易费用，如比特币就是通过工作量证明（Proof of Work）确定记账权，并向挖矿的节点提供比特币奖励。

在比特币或其他区块链网络中，其最根本的诉求是解决网络环境中价值交换时相互之间的信任问题，如在串珠后获得了新的代币，然而要通过串珠网络交易这些代币则会面临“如何交易”、“向谁交易”、“对方可以信任吗”这些问题，这也就是传统金融中介机构所解决的问题，通过银行可以进行借贷、通过证交所可以买卖股票、通过电商可以交易购买商品，通过中介机构可以在支付中介费的情况下使用服务，然而这样的操作是基于对中心结构或中介机构的信任，因为中介机构在事务处理中拥有管理员权限，技术上可以修改用户的数据。即便中介机构不作恶，其中心化处理模式仍然会存在单点故障风险，如果被黑客控制将会产生严重后果。

如果在“串珠网络”中交易代币，当发生对方没有向你汇款却声称已经汇款等意外情况时，在没有中介机构的情况下，你需要获得“串珠网络”中大多数人的认可保证这些信息是合法有效的，这就是“分布式存储结构”的好处。分布式存储结构允许所有节点都拥有一个总账本，避免“串珠网络”中某一个人随意对总账本进行改动，在无法信任他人的情况下，通过大多数人的共同利益确保任何交易节点的交易是合法的。

在解决“如何交易”、“跟谁交易”的问题后，马上就会面临到物理隔阂的问题，由于在交易过程中，你无法确信这笔代币会不会在途中某个地方被别人修改或是拦截，因此你

需要一个别人无法破解的密码锁，而某个聪明的科学家就设计出了一组十分复杂的密码锁并用在一个坚不可摧的保险箱中。

这种密码锁有两个密码：一个放钱用（公钥、地址）、一个收钱、支付用（私钥、密码）；任何人都可以通过公钥向密码箱放代币，但是只有私钥能够取走代币。私钥只有你自己拥有，这就是“非对称加密”；但是私钥非常难记，用户为了方便会通过钱包对私钥再次进行加密，并通过用户名密码来登录钱包获得私钥的支配使用权。

从本质上来说，公钥和私钥是非对称加密算法的产物，除了钱之外也可以用来传递信息，比如用自己私钥加密的信息传播出去，别人可以用你的公钥进行验证，从而确认这个信息是由你发出的。

因此，在一个大家一起建设并建立游戏规则的“串珠网络”，你只要有一个钥匙、一个密码柜就可以参加了。

1 基本概念

1.1 区块链定义

区块链/ Blockchain
区块链技术是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。

块链式数据结构/ Chained-Block Data Structure
一段时间内发生的事务处理以区块为单位进行存储，并以密码学算法将区块按时间先后顺序连接成链条的一种数据结构。

去信任/ Trustless
去信任表示用户不需要相信任何第三方。用户使用去信任的系统或技术处理交易时非常安全和顺畅，交易双方都可以安全地交易，而不需要依赖信任的第三方。

点对点/ Peer-to-Peer / P2P
通过允许单个节点与其他节点直接交互，无需通过中介机构，从而实现整个系统像有组织的集体一样运作的系统。

去中心化/ Decentralized
去中心化是区块链最基本的特征，指区块链不依赖于中心的管理节点，能够实现数据的分布式记录、存储和更新。

中本聪/ Satoshis Nakamoto
中本聪是比特币的发明人或发明组织，目前身份存疑。“中本聪”也可能仅仅是个化名。中本聪于 2008 年发表了一篇名为《比特币：一种点对点式的电子现金系统》（Bitcoin: A Peer-to-Peer Electronic Cash System）的论文，描述了一种被称为“比特币”的电子货币及其算法，被视为是区块链的第一个成功实践。

1.2 区块链特性

匿名性/ Anonymous
由于区块链各节点之间的数据交换遵循固定且预知的算法，因此区块链网络是无须信任的，可以基于地址而非个人身份进行数据交换。

自治性/ Autonomous
区块链采用基于协商一致的机制，使整个系统中的所有节点能在去信任的环境自由安全地交换数据、记录数据、更新数据，任何人为的干预都不起作用。

开放性/ Openness

区块链系统是开放的，任何节点都能够拥有全网的总账本，除了数据直接相关各方的私有信息通过非对称加密技术被加密外，区块链的数据对所有节点公开，因此整个系统信息高度透明。

可编程/ Programmable
分布式账本的数字性质意味着区块链交易可以关联到计算逻辑，并且本质上是可编程的。因此，用户可以设置自动触发节点之间交易的算法和规则。

可追溯/ Traceability
区块链通过区块数据结构存储了创世区块后的所有历史数据，区块链上的任一一条数据皆可通过链式结构追溯其本源。

不可篡改/ Tamper Proof
区块链的信息通过共识并添加至区块链后，就被所有节点共同记录，并通过密码学保证前后互相关联，篡改的难度与成本非常高。

集体维护/ Collectively Maintain
区块链系统是由其中所有具有维护功能的节点共同维护，所有节点都可以通过公开的接口查询区块链数据和开发相关应用。

无需许可/ Permissionless
无需许可表示所有节点都可以请求将任何交易添加到区块链中，但只有在所有用户都认为合法的情况下才可进行交易。

1.3 区块链类型

根据应用范围

公有链/ Public Blockchain
公有链的任何节点都是向任何人开放的，每个人都可以参与到这个区块链中的计算，而且任何人都可以下载获得完整区块链数据，即全部账本。

联盟链/ Consortium Blockchain
联盟链是指参与每个节点的权限都完全对等，各节点在不需要完全互信的情况下就可以实现数据的可信交换，联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入或退出网络。联盟链是一种公司与公司、组织与组织之间达成联盟的模式。

私有链/ Private Blockchain
在某些区块链的应用场景下，开发者并不希望任何人都可以参与这个系统，因此建立一种不对外公开、只有被许可的节点才可以参与并且查看所有数据的私有区块链，私有链一般适用于特定机构的内部数据管理与审计。

根据部署机制

主链/ 主网/ Main net
通常区块链，尤其是公有链都有主网和测试网。主网是区块链社区公认的可信区块链网络，其交易信息被全体成员所认可。有效的区块在经过区块链网络的共识后会被追加到主网的区块账本中。

测试链/ 测试网/ Testnet
测试链是对应主网具有相同功能，但主要目的用于测试的区块链。由于测试链是为了在不破坏主链的情况下尝试新想法而建立的，只作为测试用途，因此测试链上的测试币不具备交易价值。比特币的测试链已经历多次重置，以阻止将其测试币用作交易、投机用途的行为。

根据对接类型

侧链/ Side Chain
侧链是主链外的另一个区块链，锚定主链中的某一个节点，通过主链上的计算力来维护侧链的真实性，实现公共区块链上价值与其他账簿上价值在多个区块链间的转移。最具代表性的实现有 Blockstream。这种主链和侧链协同的区块链架构中的主链有时也被称为母链（Parent chain）。

互联链/ InterChains
针对特定领域的应用可能会形成各自垂直领域的区块链，互联链就是一种通过跨链技术连接不同区块链的基础设施：包括数据结构和通信协议，其本身通常也是区块链。各种不同的区块链通过互联链互联互通并形成更大的区块链生态。与互联网一样，互联链的建立将形成区块链的全球网络。

1.4 区块链层级结构

数据层/ Data Layer
数据层主要描述区块链的物理形式，是区块链上从创世区块起始的链式结构，包含了区块链的区块数据、链式结构以及区块上的随机数、时间戳、公私钥数据等，是整个区块链技术中最底层的数据结构。

网络层/ Network Layer
网络层主要通过 P2P 技术实现分布式网络的机制，网络层包括 P2P 组网机制、数据传播机制和数据验证机制，因此区块链本质上是一个 P2P 的网络，具备自动组网的机制，节点之间通过维护一个共同的区块链结构来保持通信。

共识层/ Consensus Layer
共识层主要包含共识算法以及共识机制，能让高度分散的节点在去中心化的区块链网络中高效地针对区块数据的有效性达成共识，是区块链的核心技术之一，也是区块链社群的治理机制。目前至少有数十种共识机制算法，包含工作量证明、权益证明、权益授权证明、燃烧证明、重要性证明等。

数据层、网络层、共识层是构建区块链技术的必要元素，缺少任何一层都不能称之为真正意义上的区块链技术。

激励层/ Actuator Layer
激励层主要包括经济激励的发行制度和分配制度，其功能是提供一定的激励措施，鼓励节点参与区块链中安全验证工作，并将经济因素纳入到区块链技术体系中，激励遵守规则参与记账的节点，并惩罚不遵守规则的节点。

合约层/ Contract Layer
合约层主要包括各种脚本、代码、算法机制及智能合约，是区块链可编程的基础。将代码嵌入区块链或是令牌中，实现可以自定义的智能合约，并在达到某个确定的约束条件的情况下，无需经由第三方就能够自动执行，是区块链去信任的基础。

应用层/ Application Layer
区块链的应用层封装了各种应用场景和案例，类似于电脑操作系统上的应用程序、互联网浏览器上的门户网站、搜寻引擎、电子商城或是手机端上的 APP，将区块链技术应用部署在如以太坊、EOS、QTUM 上并在现实生活场景中落地。未来的可编程金融和可编程社会也将会是搭建在应用层上。

激励层、合约层和应用层不是每个区块链应用的必要因素，一些区块链应用并不完整包含此三层结构。

2 区块链基本技术

2.1 区块数据

区块/ Block

区块是在区块链网络上承载交易数据的数据包，是一种被标记上时间戳和之前一个区块的哈希值的数据结构，区块经过网络的共识机制验证并确认区块中的交易。

父块/ Parent Block

父块是指区块的前一个区块，区块链通过在区块头记录区块以及父块的哈希值来在时间上排序。

区块头/ Block Header

记录当前区块的元信息，包含当前版本号、上一区块的哈希值、时间戳、随机数、Merkle Root 的哈希值等数据。此外，区块体的数据记录通过 Merkle Tree 的哈希过程生成唯一的 Merkle Root 记录于区块头。

区块体/ Block Body

记录一定时间内所生成的详细数据，包括当前区块经过验证的、区块创建过程中生成的所有交易记录或是其他信息，可以理解为账本的一种表现形式。

哈希值/ 散列值/ Hash Values / Hash Codes / Hash Sums / Hashes

哈希值通常用一个短的随机字母和数字组成的字符串来代表，是一组任意长度的输入信息通过哈希算法得到的“数据指纹”。因为计算机在底层机器码是采用二进制的模式，因此通过哈希算法得到的任意长度的二进制值映射为较短的固定长度的二进制值，即哈希值。此外，哈希值是一段数据唯一且极其紧凑的数值表示形式，如果通过哈希一段明文得到哈希值，哪怕只更改该段明文中的任意一个字母，随后得到的哈希值都将不同。

时间戳/ Timestamp

时间戳从区块生成的那一刻起就存在于区块之中，是用于标识交易时间的字符序列，具备唯一性，时间戳用以记录并表明存在的、完整的、可验证的数据，是每一次交易记录的认证。

随机数/ 一次性的随机数/ Nonce

Nonce 是指“只使用一次的随机数”，在挖矿中是一种用于挖掘加密货币的自动生成的、毫无意义的随机数，在解决数学难题的问题中被使用一次之后，如果不能解决该难题则该随机数就会被拒绝，而一个新的 Nonce 也会被测试出来并且直到问题解决，当问题解决时矿工就会得到加密货币作为奖励。在区块结构中，Nonce 是基于工作量证明所设计的随机数字，通过难度调整来增加或减少其计算时间；在信息安全中，Nonce 是一个在加密通信只能使用一次的数字；在认证协议中，Nonce 是一个随机或伪随机数，以避

免重放攻击。

梅克尔树/ Merkle Tree
梅克尔树（又叫哈希树）是一种二叉树，是一种高效和安全的组织数据的方法，被用来快速查询验证特定交易是否存在，由一个根节点、一组中间节点和一组叶节点组成。它使用哈希算法将大量的书面信息转换成一串独立的字母或数字。最底层的叶节点包含存储数据或其哈希值，每个中间节点是它的两个子节点内容的哈希值，根节点也是由它的两个子节点内容的哈希值组成。

区块容量/ Block Size
区块链的每个区块，都是用来承载某个时间段内的数据的，每个区块通过时间的先后顺序，使用密码学技术将其串联起来，形成一个完整的分布式数据库，区块容量代表了一个区块能容纳多少数据的能力。

未花费的交易输出/ Unspent Transaction Output / UTXO
未花费的交易输出是一个包含交易数据和执行代码的数据结构，可以理解为收到的但尚未花费的加密货币清单。比特币和其他加密货币在其区块链技术中使用 UTXO，以验证一个人是否拥有未使用的加密货币可用于支出。

2.2 链式结构

链/ Chain
链是由区块按照发生的时间顺序，通过区块的哈希值串联而成，是区块交易记录及状态变化的日志记录。

链下/ Off-chain
区块链系统从功能角度讲，是一个价值交换网络，链下是指不存储于区块链上的数据。

无代币区块链/ Token-Less Blockchain
即区块链并不通过代币进行价值交换，一般出现在不需要在节点之间转移价值并且仅在不同的已被信任方之间共享数据的情况下，如私有链。

创世区块/ Genesis Block
区块链中的第一个区块被称为“创世”区块。创世区块一般用于初始化，不带有交易信息。

区块高度/ Block Height
一个区块的高度是指在区块链中它和创世区块之间的块数。

分叉/ Fork
在区块链中，由矿工挖出区块并将其链接到主链上，一般来讲同一时间内只产生一个区

块，如果发生同一时间内有两个区块同时被生成的情况，就会在全网中出现两个长度相同、区块里的交易信息相同但矿工签名不同或者交易排序不同的区块链，这样的情况叫做分叉。

软分叉/ Soft Fork
指在区块链或去中心化网络中向前兼容的分叉。向前兼容意味着，当新共识规则发布后，在去中心化架构中节点不一定要升级到新的共识规则，因为软分叉的新规则仍旧符合老的规则，所以未升级的节点仍旧能接受新的规则。

硬分叉/ Hard Fork
指在区块链或去中心化网络中不向前兼容的分叉，硬分叉对加密货币使用的技术进行永久更改，这种变化使得所有的新数据块与原来的块不同，旧版本不会接受新版本创建的区块，要实现硬分叉所有用户都需要切换到新版本协议上。如果新的硬分叉失败，所有的用户将回到原始数据块。

幽灵协议/ GHOST Protocol
通过幽灵协议，区块可以包含不只是他们父块的哈希值，也包含其父块的父块的其他子块（被称为叔块）的陈腐区块的哈希值，这确保了陈腐区块仍然有助于区块链的安全性，并能够获得一定比例的区块奖励，减少了大型矿工在区块链上的中心化倾向问题。

孤块/ Orphan Block
孤块是一个被遗弃的数据块。因为很多节点都在维护区块链并同时创建多个区块，但是一次只能有一个被继续继承，而其它被遗弃的数据块就是孤块。

陈腐区块/ Stale Block
是父块的父块的“其他”子块，或更一般的说是祖先的其他子块，但不是自己的祖先，如果 A 是 B 的一个叔块，那 B 是 A 的侄块。

2.3 非对称加密

密码学/ Cryptography
密码学是数学和计算机科学的分支，同时其原理大量涉及信息论。密码学不只关注信息保密问题，还同时涉及信息完整性验证（消息验证码）、信息发布的不可抵赖性（数字签名）、以及在分布式计算中产生的来源于内部和外部的攻击的所有信息安全问题。

加密/ Cipher
加密是一系列使信息不可读的过程，它能使信息加密也能使信息加密后能够再次可读，在加密货币中使用的密码也使用由字母和数字组成的密钥，该密钥必须用于解密密码。

加密算法/ Encryption Algorithm

加密算法是一个函数，也可以视为是一把钥匙，通过使用一个加密钥匙，将原来的明文文件或数据转化成一串不可读的密文代码。加密流程是不可逆的，只有持有对应的解密钥匙才能将该加密信息解密成可阅读的明文。加密使得私密数据可以在低风险的情况下，通过公共网络进行传输，并保护数据不被第三方窃取、阅读。

非对称加密/ Asymmetric Cryptography

非对称加密是一种保证区块链安全的基础技术。该技术含有两个密钥：公钥和私钥，首先，系统按照某种密钥生成算法，将输入经过计算得出私钥，然后，采用另一个算法根据私钥生成公钥，公钥的生成过程不可逆。由于在现有的计算能力条件下难以通过公钥来穷举出私钥（即计算上不可行），因此可以认为是数据是安全的，从而能够保证区块链的数据安全。

同态加密/ Homomorphic Encryption

同态加密是一种特殊的加密方法，允许对密文根据特定的代数运算方式进行处理后得到的仍然是加密的结果，将其解密所得到的结果与对明文进行同样的运算结果是一样的。即“对密文直接进行处理”与“对明文进行处理后并加密”其结果是一样的，这项技术可以在加密的数据中进行诸如检索、比较等操作而无需对数据先进行解密，从根本上解决将数据委托给第三方时的保密问题。

公钥加密/ Asymmetric Cryptography / Public Key Cryptography

公钥加密是一种特殊的加密手段，具有在同一时间生成两个密钥的处理（私钥和公钥），每一个私钥都有一个相对应的公钥，从公钥不能推算出私钥，并且被用其中一个密钥加密了的数据，可以被另外一个相对应的密钥解密。这套系统使得节点可以先在网络中广播一个公钥给所有节点，然后所有节点就可以发送加密后的信息给该节点，而不需要预先交换密钥。

RSA 加密算法/ RSA Algorithm

RSA 公开密钥密码体制是使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。它通常是先生成一对 RSA 密钥，其中之一是保密密钥，由用户保存; 另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。

椭圆加密算法/ Elliptic Curve Cryptography / ECC

椭圆加密算法是一种公钥加密体制，最初由 Koblitz 和 Miller 两人于 1985 年提出，其数学基础是利用椭圆曲线上的有理点构成 Abel 加法群上椭圆离散对数的计算困难性。

明文/ Plaintext

在密码学中，明文是指传送方想要接收方获得的可读信息。明文经过加密所产生的信息被称为密文，而密文经过解密而还原得来的信息被称为明文。

密文/ Ciphertext

在密码学中，密文是明文经过加密算法所产生的。因为密文是一种除非使用恰当的算法进行解密，否则人类或计算机是不可以直接阅读理解的加密形态，可以理解为被加密的信息。

环签名/ Ring Signatures

因签名中参数 Ci（i=1,2,⋯,n）根据一定的规则首尾相接组成环状而得名。其实就是实际的签名者用其他可能签字者的公钥产生一个带有断口的环，然后用私钥将断口连成一个完整的环。任何验证人利用环成员的公钥都可以验证一个环签名是否由某个可能的签名人生成。

数字签名/ Digital Signatures

数字签名（又称公钥数字签名、电子签名）是一种类似写在纸上的签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法，在网络上可以使用数字签名来进行身份确认。数字签名是一个独一无二的数值，若公钥能通过验证，那我们就能确定对应的公钥的正确性，数字签名兼具可确认性和不可否认性。

多重签名/ Multi-Signatures

多重签名意味着在交易发生之前需要多个签名或批准。多重签名会增加加密货币的安全性，这样一个人就不能在未经他人同意的情况下把所有的数字货币都拿走。

数字证书/ Digital Certificate

数字证书是区块链中标识各个节点的身份信息的一串数字，用以证明公钥的归属以及内容信息的合法性，在区块链的非对称加密中，一旦通过中间人攻击将公钥替换后将会破坏区块链的安全体系，因此通过共识机制建立互相承认的数字证书机制，在不需要第三方的情况下识别数据的合法性。

哈希/ 散列/ Hash

哈希又称作“散列”，是一种数学计算机程序，它接收任何一组任意长度的输入信息，通过哈希算法变换成固定长度的数据指纹输出形式，如字母和数字的组合，该输出就是“哈希值”。哈希使存储和查找信息速度更快，因为哈希值通常更短所以更容易被找到。同时哈希能够对信息进行加密，一个好的哈希函数在输入域中很少出现哈希冲突，哈希一个特定文档的结果总是一样的，但找到具有相同哈希值的两个文件在计算上是计算上不可行的。

安全哈希算法/ Secure Hash Algorithm 256 / SHA 256

SHA 256 是 SHA 系列算法之一，由美国国安局设计、美国国家标准与技术研究院发布的一套哈希算法，由于其摘要长度为 256bits，故称 SHA 256。SHA 256 是保护数字信息的最安全的方法之一。

钥匙/ Key

钥匙是使隐藏的、不可读的信息可读的一串秘密字母和数字。

密钥/ Secret Key
密钥是用于加密或解密信息的一段参数，在非对称加密系统中，是通过利用公钥（账户）与私钥（密码）的配合而实现的。

公钥/ Public Key
公钥与私钥是通过一种算法得到的一个密钥对，公钥是密钥对中公开的部分，私钥则是非公开的部分，公钥通常用于加密会话密钥、验证数字签名，或加密可以用相应的私钥解密的数据。

私钥/ Private Key
公钥与私钥是通过一种算法得到的一个密钥对，公钥是密钥对中公开的部分，私钥则是非公开的部分，私钥是指与一个地址（地址是与私钥相对应的公钥的哈希值）相关联的一把密钥，是只有你自己才知道的一串字符，可用来操作账户里的加密货币。

零知识证明/ Zero-Knowledge Proof
证明者和验证者之间进行交互，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。

计算上不可行/ Computationally Feasible
密码算法依赖的原理是当前计算不可行的数学问题，而“计算不可行”是一个在时间及空间上相对而言的概念，计算上不可行即表示一个程序是可处理的但是需要一个长得不切实际的时间（如几十亿年）来处理的步骤。通常认为 2 的 80 次方个计算步骤是计算上不可行的下限。

暴力破解法/ Brute Force Attack / BFA
暴力破解法又名穷举法，是一种密码分析的方法，通过逐个推算猜测每一个可能解锁安全系统的密钥来获取信息的方法。

2.4 分布式存储

分布式存储/ Distributed Data Store / DDS
传统上的分布式存储本质上是一个中心化的系统，是将数据分散存储在多台独立的设备上，采用可扩展的系统结构、利用多台存储服务器分担存储负荷、利用位置服务器定位存储信息。而基于 P2P 网络的分布式存储是区块链的核心技术，是将数据存储于区块上并通过开放节点的存储空间建立的一种分布式数据库，解决传统分布式存储的问题。

P2P 存储/ Peer-to-Peer Storage / P2P Storage
P2P 存储是一种不存在中心化控制机制的存储技术。P2P 存储通过开放节点的存储空间，以提高网络的运作效率，解决传统分布式存储的服务器瓶颈、带宽而带来的访问不便等问题。

分布式/ Distributed
分布式是通过区块链的 P2P 技术实现，分布式是描述一个计算机系统具有在多台计算机上同时运行和维护的完整副本，没有任何人或组织来控制这个系统。

账本/ Ledger
账本是指包括区块链的数据结构、所有的交易信息和当前状态的数字记录。

分布式账本/ Distributed ledger Technology / DLT
分布式账本是指一种在网络成员之间共享、复制和同步的数据库，分布式账本在区块链中是一个通过共识机制建立的数字记录，区块链网络中的参与者可以获得一个唯一、真实账本的副本，因此难以对分布式账本进行篡改。更改记录的方式非常困难，技术非常安全。

节点/ Node
节点是区块链分布式系统中的网络节点，是通过网络连接的服务器、计算机、电话等，针对不同性质的区块链，成为节点的方式也会有所不同。以比特币为例，参与交易或挖矿即构成一个节点。

全节点/ 完整节点/ Full Node
全节点是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。

2.5 共识机制

共识机制/ Consensus
由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序不可能完全一致。因此区块链系统需要设计一种机制对在差不多时间内发生的事务的先后顺序进行共识，这种对一个时间窗口内的事务的先后顺序达成共识的算法被称为“共识机制”。

工作量证明/ Proof of Work / PoW
工作量证明简单理解就是一份证明，用来确认节点做过一定量的工作。监测工作的整个过程通常是极为低效的，而通过对工作的结果进行认证来证明完成了相应的工作量，则是一种非常高效的方式。比特币在区块的生成过程中使用了 PoW 机制，要得到合理的随机数求解数学难题需要经过大量尝试计算，通过查看记录和验证区块链信息的证明，就能知道是否完成了指定难度系数的工作量。

权益证明/ Proof of Stake / PoS
PoS 也称权益证明机制，类似于把资产存在银行里，银行会通过你持有数字资产的数量和时间给你分配相应的收益。采用 PoS 机制的加密货币资产，系统会根据节点的持币

数量和时间的乘积（币天数）给节点分配相应的权益。

权益授权证明/ Delegated Proof of Stake / DPoS

DPoS 是一种类似董事会的授权共识机制，该机制让每一个持币人对整个系统的节点进行投票，决定哪些节点可以被信任并代理他们进行验证和记账，同时生成少量的对应奖励。DPoS 大幅提高区块链的处理能力，并降低区块链的维护成本，从而使交易速度接近于中心化的结算系统。

燃烧证明/ Proof of Burn / PoB

燃烧证明是一种投资于全新的加密货币的方法：为了获得一种新的货币，你必须“烧掉”（摧毁）另一种货币，比如比特币。从理论上讲，这将使每一种新的加密货币价值相当于被摧毁的币的价值，但实际上你不能真的摧毁加密货币，系统需要你把它送到一个会减少它的总供应量的地方。

开发者证明/ Proof of Developer / PoD

开发者证明是一个真实的、活的软件开发人员创建了一种加密货币的证据。它用于启动新的加密货币，以防止匿名开发人员在不提供可行的加密货币的情况下收集和窃取资金。

重要性证明/ Proof of Important / PoI

重要性证明是根据交易量、活跃度等维度而不仅仅是根据工作量和币的数量来决定区块链的记账权力。

基于交易的权益证明机制/ Transaction as Proof of Stake / TaPOS

TaPOS 为股东们提供了一个长效机制来直接批准他们的代表的行为，平均而言，51% 的股东在 6 个月内会直接确认每个区块，取决于活跃流通的股份所占的比例，差不多 10% 的股东可以在几天内确认区块链。这种方式直接确认保障了网络的长期安全，并使所有的攻击尝试变得极度清晰易见。

瑞波共识机制/ Ripple Consensus

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。共识遵循核心成员 51% 权力规则，外部人员则没有影响力。

分布式共识/ Distributed Consensus

所有的节点必须定期更新彼此之间的不断复制的状况，通过专门的槽位来识别每一个更新。当所有节点更新了他们的分类账并放映的值相同时，就可达成共识，会将协商一致的声明具体化并发布至它们的分类账副本去。

验证池机制/ POOL

验证池机制是基于传统的分布式一致性技术和数据验证机制的结合，它使得在成熟的分

布式一致性算法（Pasox、Raft）基础上，不需要代币也能实现秒级共识验证。

51% 攻击/ 51% attack
51% 攻击，是指利用比特币以算力作为竞争条件的特点，凭借算力优势篡改或者撤销自己的付款交易。如果有人掌握了 50% 以上的算力，他能够比其他人更快地找到开采区块需要的那个随机数，因此他能够比其他人更快地创建区块。

双重支付/ 双重花费/ 双花/ Double Spending
双重支付是一个故意的分叉，是指具有大量计算能力的节点发送一个交易请求并购买资产，在收到资产后又做出另外一个交易将相同量的币发给自己。攻击者通过创造一个分叉区块，将原始交易及伪造交易放在该区块上并基于该分叉上开始挖矿。如果攻击者有超过 50%的计算能力，双重花费最终可以在保证在任何区块深度上成功；如果低于 50%则有部分可能性成功。

拜占庭将军问题/ Byzantine Generals Problem / BGP
拜占庭将军问题是指“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”。因此在系统中存在除了消息延迟或不可送达的故障以外的错误，包括消息被篡改、节点不按照协议进行处理等，将会潜在地会对系统造成针对性的破坏。

改进型实用拜占庭容错/ Practical Byzantine Fault Tolerance / PBFT
PBET 共识机制是少数服从多数，根据信息在分布式网络中节点间互相交换后各节点列出所有得到的信息，一个节点代表一票，选择大多数的结果作为解决办法。PBET 将容错量控制在全部节点数的 1/3，即如只要有超过 2/3 的正常节点，整个系统便可正常运作。

授权拜占庭容错算法/ Delegated Byzantine Fault Tolerance / dBFT
dBFT，是基于持有权益比例来选出专门的记账人（记账节点），然后记账人之间通过拜占庭容错算法（即少数服从多数的投票机制）来达成共识，决定动态参与节点。dBFT 可以容忍任何类型的错误，且专门的多个记账人使得每一个区块都有最终性、不会分叉。

联邦拜占庭协议/ Federated Byzantine Agreement / FBA
联邦拜占庭协议的主要特性是去中心化和任意行为容错，通过分布式的方法，达到法定人数或者节点足够的群体能达成共识，每一个节点不需要依赖相同的参与者就能决定信任的对象来完成共识。

3 区块链的衍生技术

3.1 主链扩容

分片/ Sharding

分片是区块容量的一种解决方案。通常情况下，每个节点和区块链网络都包含区块链的完整副本，分片是一种允许节点具有完整的区块链的部分副本的技术，以提高整体性能和稳定速度。

闪电网络/ Lightning Network

闪电网络是一种允许加密货币的交易即时发生和成本降低的技术，它使一般在比特币网络中需要等待区块确认的交易瞬间完成。闪电网络基于一个可扩展的微支付通道网络，通过序列到期可撤销合约 RSMC，使交易双方在区块链上的预先设置的支付通道进行的多次高频的双向交易瞬间完成。同时，它通过哈希时间锁定合约 HTLC 在没有直接点对点支付信道的交易双方之间连接一条由多个支付通道构成的支付路径，实现资金的转移。

雷电网络/ Raiden Network

雷电网络是一种以太坊链下扩容解决方案，它使得使用以太坊技术的加密货币能够即时和低成本交易。交易双方只要在链上存在交易信道，就能在链下根据被锁定的余额进行高频、双向的即时确认交易，将这样多个通道形成的支付路径构成“雷电网络”。

隔离见证/ Segregated Witness / SW

隔离见证是一种技术，通过把占用大量存储空间的区块的数字签名重新放置到不同的记录（也称为隔离），使每个区块能进行更多的交易，以达到扩容的目的。区块链上不仅记载了每笔转账的具体信息，还包括了每笔交易的数字签名以核实交易的合法性。矿工在打包区块的时候需要用数字签名来验证每笔交易，确认无误之后才会将该笔交易记录在区块里。但对于用户不需要验证信息，且每个比特币记录大小被限制在 1 兆字节（MB），每 10 分钟记录一次新的记录，所以通过隔离见证转移签名以扩大区块空间。

3.2 跨链协议

跨链技术/ Cross-Chain

跨链技术是实现区块链之间互联互通的技术，若对标互联网则可理解为“去中心化网络的结合”，区块链技术的特性使得跨链技术的落地，以及对于链外信息的获取都非常困难，早期跨链技术包括以 Interledger Protocal 和 BTC Relay 为代表，更多是关注资产的转移；现有跨链技术以 Aion、Kyber Network、Bletchley、Polkadot、Cosmos 主要着重的是跨链基础设施。“如果说共识机制是区块链的灵魂核心，那么对于区块链特别

是联盟链及私链来看，跨链技术就是实现价值网络的关键，它是把联盟链从分散单独的孤岛中拯救出来的良药，是区块链向外拓展和连接的桥梁。”——《连接不同区块链的跨链技术介绍》。

原子互换/ Atomic Swap
原子互换是一种正在开发中的去中心化、无需第三方的新技术，允许在不同类型的数字资产之间实现无需信任的点对点交易，任何一方在瞬间完成的点对点交易中都遵守协议，且之后若有一方退出，资金会在规定的时间返回各方账户。

见证人机制/ Notary Schemes
见证人模式是一种中心化的结构，通过选定一批见证人并在见证人之间采用拜占庭容错结构，监听目标链上的事件和状态并签名进行资产的转移，如 Ripple 的 Interledger Protocal 的早期版本。

侧链技术/ Sidechains
（参见前文）。

侧链协议/ Sidechain Protocol
侧链协议是一种实现双向锚定（Two-way Peg）的协议，通过侧链协议实现资产在主链和其它链之间互相转换，或是以独立的、隔离系统的形式，降低核心区块链上发生交易的次数。

楔入式侧链技术/ Pegged Sidechain
它将实现比特币和其他数字资产在多个区块链间的转移，这就意味着用户们在使用他们已有资产的情况下，可以访问新的加密货币系统。

中继技术/ Relays
中继技术是通过在两个链中加入一个数据结构，使得两个链可以通过该数据结构进行数据交互，并通过在一个链上调用数据结构的 API，实现监听并验证另一个链上的交易，而若该数据结构是一个链式结构，则具备侧链的形式并称作中继链。

哈希时间锁定合约/ Hashed TimeLock Contract / HTLC
哈希时间锁定合约包含哈希锁定（Hashlock）以及时间锁定（Timelock）两个部分，哈希时间锁定合约最典型的代表就是比特币的闪电网络，闪电网络提供一个可扩展的微支付通，用以提升链外的交易处理能力，使用哈希锁定将发起方的交易代币进行锁定，并通过时间锁定让接收方在某个约定的时刻前生成支付的密码学证明，并与先前约定的哈希值一致，则可完成交易。

3.3 其他技术

图灵完备/ Turing Complete
在可计算理论中，当一组数据操作的规则（一组指令集、编程语言或元胞自动机）满足任意数据按照一定的顺序可以计算出结果，则称为图灵完备。

混币服务/ Mixing Service
混币服务，就是用一种加密货币从其他人那里得到同样金额的加密货币。原理是分离交易中的输入和输出地址，目的是提高加密货币的隐私性和匿名性，使其更难追踪加密货币的用途以及它属于谁。

零币协议/ Zerocash Protocol
零币协议是一个发布于 2013 年的独立协议，原先目的是为了在混币技术、环签技术外增强加密货币的匿名性，零币协议使用零知识证明实现完全匿名，通过一个集合的托管池（Escrow Pool）删除交易的历史记录。零币协议有两个主要部分："铸币"使有交易记录的币匿名化并置于托管池；通过零知识证明创建一个没有交易记录的新币，并销毁托管池中的币。

CryptoNote 协议/ CryptoNote
CryptoNote 是一种应用协议，旨在实现加密货币的匿名性，于 2013 年 10 月发布，并可被用于多种加密货币中，如门罗币、百特币、Aeon、Fantomcoin 等。CryptoNote 通过使用分布式公共分类账，记录区块链上加密货币的交易和余额，但将发送方、接收方匿名化，并将交易金额模糊化。

缠结/ Tangle
Tangle 是 IOTA 项目创造的一种改革性的去区块化分布式账本，它是可扩展的、轻量级的，还能在无需任何费用的前提下进行价值转移。Tangle（缠结）是基于有向无环图（DAG）的机构，而不是像区块链的连链式架构，它能定期添加区块，从而实现更高的交替吞吐量和零交易手续费。

有向无环图/ Database Availability Group / DAG
DAG 指有向无环图，是常用于计算机领域的数据结构。DAG 具备独特的拓扑结构，经常被用于处理动态规划，导航中获得最短路径等场景中。在区块链领域，DAG 用来解决扩容性的问题，通过增加区块大小或者区块频率在网络中产生大量分叉，但是攻击者还是需要 51% 的算力才能进行攻击。

去中心化应用/ Decentralized Application / DApp
DApp 是一种在网络上公开运行的软件应用程序，这项技术是由许多人维护的，而不是由一个组织维护的，黑客不能改变应用程序的数据，除非他们能够访问几乎所有的网络计算机并在那里调整它。

去中心组织/ Decentralized Organization

去中心组织是一个没有中央领导，而是使用正式民主投票进程和共识主动性自我组织的结合来作为其基本操作原则的组织。

去中心化自治组织/ Decentralized Autonomous Organization / DAO

去中心化自治组织是一个通过编码为称为智能合约的计算机程序的规则运行的组织，由计算机网络支持的无中心组织并且没有单一的领导者，是一种自主的或者是自治的组织结构。

4 区块链的技术应用

区块链 1.0 / Blockchain 1.0

区块链 1.0 是以比特币、莱特币为代表的加密货币，具有支付、流通等货币职能。

区块链 2.0 / Blockchain 2.0

区块链 2.0 是以以太坊、瑞波币为代表的智能合约或理解为“可编程金融”，是对金融领域的使用场景和流程进行梳理、优化的应用。

区块链 3.0 / Blockchain 3.0

区块链 3.0 是区块链技术在社会领域下的应用场景实现，将区块链技术拓展到金融领域之外，为各种行业提供去中心化解决方案的“可编程社会”。

4.1 加密货币

数字货币/ Digital Currency

数字货币是一种不具备实体形式的、仅以数字形式存在的货币，在英语语境中与电子货币同义，而在中文语境下一般将电子货币解释为“电子化的法定货币”，即“电子化的人民币”并与数字货币区别开来。数字货币具备与实体货币相似的性质，但允许在互联网上即时地、无地理限制地转让。数字货币包含虚拟货币、加密货币、电子货币等概念。

加密货币/ Cryptocurrency

加密货币是基于密码学的、不具备物理形式的货币，是数字货币的表现形式之一，在区块链中是指“一种基于 P2P 网络、没有发行机构、总量基本确定、依据确定的发行制度和分配制度创建及交易、基于密码学及共识机制保证流通环节安全性的、具备一定编程性的数字货币。”，而各国对于加密货币的定义不一而足，我国央行将加密货币定义为一种“虚拟商品”不具备货币属性；而在美国则根据不同部门有不同的定义，如：财产、大宗商品、货币、虚拟货币等。

代币/ Token / Token Coin

代币与令牌的对应英文单字皆为 Token，在区块链领域中一般不加以区分，但两者在意思上具有些许区别；英文 Token 实际上既包含代币、令牌也包含代金券、证券、通证、纪念物等概念，准确来说代币的对应英文为 Token Coin，在区块链领域中与“支付令牌”具备相同的意义。代币可以定义为某种账户的余额，并且不仅仅局限于加密货币的范畴，广义而言包含 Q 币在内的虚拟货币皆属于代币的范畴。

非货币/ Noncurrency

非货币是指不具有货币的流通性质、价格衡量功能，因此并不能作为市场的支付工具，

并且需要依据其法律定义征收相应的税款，如增值税、资本利得税。

竞争币/ AltCoin
Altcoin 是 Bitcoin alternative 的缩写，竞争币一般指除了比特币外的所有加密货币的总称。

山寨币/ AltCoin
山寨币是竞争币、替代币的一种业内戏称，是指在比特币源码基础上进行修改创造出的加密货币。

4.2 智能合约

智能合约/ Smart Contract
智能合约最早在上世纪末就被提出，但直到近年随着区块链技术的发展逐步被社会大所熟悉，智能合约的概念具备承诺、协议、数字形式三大要素，因此能够将区块链的应用范围扩展至金融行业交易、支付、结算和清算的各个环节。智能合约是指当一个预先编好的条件被触发时，智能合约会立即执行相应的合同条款，其工作原理类似于计算机程序的 if-then 语句。

以太坊/ Ethereum
Ethereum（以太坊）是一个平台和一种编程语言，使开发人员能够建立和发布下一代分布式应用。Ethereum 可以用来编程，分散、担保和交易任何事物，投票，域名，金融交易所，众筹，公司管理，合同和大部分的协议、知识产权，还有得益于硬件集成的智能资产。

EVM 代码
以太坊虚拟机代码，以太坊的区块链可以包含的编程语言的代码。与帐户相关联的 EVM 代码在每次消息被发到这个账户的时候被执行，并且具有读/写存储和自身发送消息的能力。

合约/ Contract
一个包含并且受 EVM 的代码控制的账户。合约不能通过私钥直接进行控制，除非被编译成 EVM 代码，一旦合约被发行就没有所有者。

令牌/ 通证/ Token
计算机术语中“令牌”一词有两个意思: 对用户进行授权的小工具，或是认证用户身份的固定字符串；在加密货币中令牌是数字价值的一个单位，是内置可编程潜力的代币，除了具备经济属性外，同时在也可用以构建软件，并可能通过技术实现集代币、身份识别、荣誉标识、确权工具、资产量化指标、系统通行证和系统保护于一身的工具。如 OMG 和 EOS 是建立在 Ethereum 令牌上的加密货币。根据瑞士金融市场监督管理局

（FINMA）在 2018 年 2 月提出的定义，令牌主要分为支付令牌、功能令牌、资产令牌三种，并且可能存在混合形式：

1. **支付令牌/ Payment Tokens**
   “支付令牌与加密货币是同义词，并没有其他功能或链接其他开发项目的功能，令牌在某些情况下可能只会开发必要的功能，并在一段时间内成为支付手段。”如比特币、狗狗币、莱特币等第一代加密货币以及达世币、门罗币等以支付、结算为主要功能的令牌。

2. **功能令牌/ Utility Tokens**
   “功能令牌是旨在为应用程序或服务提供数字访问的令牌。”如瑞波币、艾达币、恒星币、小蚁股等内嵌代码，并具备使用场景或潜在使用场景的令牌。

3. **资产令牌/ Asset Tokens**
   “资产令牌代表资产，例如参与真实实体收益，公司股份或收益权益，或者获得股息或利息支付的权利。就其经济功能而言，令牌类似于股票，债券或衍生品。”如 BitShares 上的 PDA 令牌或是 DigixDAO 上的 DGX 令牌，在现实世界中具备对应的资产。

令牌化/ Tokenize
令牌化是将现实世界中的有价物转化为数字价值的过程。在未来有可能通过区块链技术实现将线下资产标记出来，并将单一资产进行分割、令牌化（如将一间房子分成 1000 份在市场上流通）。没有区块链技术的协助就无法建立标记，对于单一资产的部分进行交易时不可能的是不可能的。由于这些代币是在区块链上交换的，所以数据是公开的、几乎不可能作弊。

4.3 主要代币

比特币/ Bitcoin / BTC
Bitcoin（比特币）的概念是由中本聪（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、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%。

1. **Megabitcoin / MBTC**
   Megabitcoin 缩写为 MBTC，是 100 万个比特币。

2. **比特分/ Bitcent / cBTC**
   比特分又被称作 cBTC，一枚比特币的价值是 10^2 比特分。

3. **毫比特/ Millibitcoin / mBTC**
   毫比特又被称作 mBTC，一枚比特币的价值是 10^3 毫比特。

4. **微比特/ Microbitcoin / BTC**
   微比特又被称作 uBTC，一枚比特币的价值是 10^6 微比特。

5. **聪/ Satoshi**
   Satoshi 是比特币中最小的数量单位，表示十亿分之一比特币或 0.000000001 比特币，这个单位是由比特币的创造者 Satoshi Nakamoto 所命名的，Satoshi Nakamoto 是 2009 年创造比特币的一个不知名的人或者一群人。

6. **维珍比特币/ Virgin Bitcoin**
   Virgin Bitcoin 是由一台正在挖掘的计算机建立的全新的比特币。挖矿是记录和验证被称为区块链的数字记录上的信息的计算机过程。在比特币和其他加密货币中，挖矿需要通过计算机相互竞争来解决复杂的数学问题。

7. **比特币改进提议/ Bitcoin Improvement Proposals / BIPs**
   由于比特币是一个去中心化的公有链，因此全世界的开发者都有权对网络的开发做出贡献，比特币改进协议是一种向比特币社区提供信息的设计文档，是开发者用于描述为比特币网络带来的新功能、信息、流程或环境。根据 BIP 目的和指南（BIP Purpose and Guidelines）分为三种比特币改进协议形式：标准类 BIP、信息类 BIP、过程类 BIP。

以太币/ Ether / ETH

Ethereum （以太坊）是一种开源的、图灵完备的、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。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）的加密货币。

1. **瓦斯/ Gas**
   瓦斯是用于支付给在电脑上记录交易和其他行为的以太币，可以理解成比特币中的交易费用。瓦斯的计算方法是用瓦斯价格（一小部分的以太币）乘以瓦斯限值，如果瓦斯的量不够，任务就会失败，这也意味着更多瓦斯也就意味着电脑完成得速度越快。

2. **瓦斯限值/ Gas Limit**
   以太坊用瓦斯限值取代区块容量限制，瓦斯限值是用来衡量以太坊的瓦斯总量，

以此可以用来决定单个区块中能打包多少笔交易。在进行操作时必须确保足够的瓦斯限值，否则交易将不能顺利完成。

3. **瓦斯价格/ Gas Price**
   瓦斯价格是非常少量的以太币，它乘以瓦斯限值的就是瓦斯，用来人们记录交易和做其他软件操作的费用。

4. **Ether**
   Ether 即一单位以太币。

5. **Milliether / Finney**
   Milliether 又被称作 Finney，一枚以太币的价值是 10^3 Milliether。

6. **Microether / Szabo**
   Microether 又被称作 Szabo，一枚以太币的价值是 10^6 Microether。

7. **GWei / Shannon**
   GWei 又被称作 Shannon，一枚以太币的价值是 10^9 GWei。

8. **Mwei / Lovelace**
   MWei 又被称作 Lovelace，一枚以太币的价值是 10^{12} MWei。

9. **Kwei / Babbage**
   KWei 又被称作 Babbage，一枚以太币的价值是 10^{15} KWei。

10. **Wei**
    Wei 是以太币的最小单位，一枚以太币的价值是 10^{18} Wei。

瑞波币/ Ripple / XRP

Ripple 是一个去中心化的资产传输网络，用于解决金融机构以及用户间的资产转换和信任问题。XRP （瑞波币）是 Ripple 网络流通的基础货币，任何人均可以创建 Ripple 账户并通过 Ripple 支付网络可以转账任意一种货币，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。

比特现金/ Bitcoin Cash / BCH

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。

莱特币/ Litecoin / LTC

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，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。

5 数字货币交易

5.1 账户

账户/ Account

账户是在总账中的一份记录，通过地址在总账中索引，总账包含有关该账户的状态的完整的数据。在一个加密货币系统中，该数据则包含了加密货币余额、未完成的交易订单等情况。

账户随机数/ Random Number

每个账号的交易计数，通过账户随机数可以防止重放攻击。例如，A 给 B 发送 20 个币，B 重放一遍又一遍，直到抽干 A 的账户余额。

地址/ Address / Addy

地址通过一系列密码算法推算形成，本质上是属于特定用户的公钥的哈希值，地址用于在网络上交易时接收和发送数据，由一连串字母和数字的字符串组成，但也可以表示为可扫描的二维码。

虚拟地址/ Virtual Address

虚拟地址是一串公开可用的字母和数字，并且以一组定制的字母和数字开始。虚拟地址允许接收，保存和发送加密货币。

虚荣地址/ Vanity Address

虚荣地址是指通过哈希函数计算随机产生特定的字符串，由于无法通过逆向计算哈希函数，因此只能不停地重复生成密钥，直到密钥中包含希望出现的字符串，而这样的密钥地址称为虚荣地址。

虚荣地址挖矿/ Vanity-Mining

虚荣地址挖矿即通过计算机重复产生基于哈希函数的秘钥地址，直到通过大量的计算得到密钥中出现所期待的字符串的过程，其通过大量并行计算寻找特定字符串与加密货币挖矿寻找特定数学解在某种程度上相似。

虚荣池/ Vanity Pool

虚荣池是一个虚荣地址生成池，这种服务允许用户将他们的虚拟地址生成需求外包给第三方矿工，而不用担心会危及他们的安全。

5.2 挖矿

与挖矿相关词汇

挖矿/ Mining

挖矿是指利用电脑硬件计算、记录和验证被称为区块链的数字记录信息的过程。矿工通过挖矿求解数学难题从而获得创建新区块的记账权以及区块的比特币奖励，由于其工作原理与矿物开采十分相似，故称之为挖矿。目前最常见的方式是通过 PoW 工作量证明共识机制，第一个解决复杂数学问题的计算机将得到一个新的可记录区块链上信息的块，同时得到新的比特币。

矿工/ Miner

在区块链网络中，矿工是指通过不断进行哈希运算来求解数学难题并产生工作量证明的各网络节点，通过算力来验证、确认交易并防止双重支付。

矿池/ Mining Pool

矿池是一个完全节点，矿池是通过一种将少量算力合并联合运作的方法，整合区块链网络中的零散算力，并在所有成员中共享奖励。在全网算力提升到了一定程度后，单个设备难以在比特币网络上获取比特币网络提供的区块奖励，变成了纯粹 0 和 1 的概率事件，而通过加入矿池集合网络中较大比例的算力，远比单独获取区块奖励的几率更大。

矿场/ 挖矿基地/ Mining Farm

矿场与矿池是两个区分概念，矿场是指地理上集中的矿机分布形式。基于比特币全网的算力水平不断上升，单个设备难以获得比特币的区块奖励，因此通过大规模挖矿、商业化运作的模式，将大量的矿机集中到挖矿成本较低的地方进行的规模化挖矿。矿场的主要成本来自于硬件成本以及电力成本。

随机数/一次性的随机数/ Nonce

（参见前文）。

目标值/ The Target

目标值是指挖矿时，数学难题的哈希值的阈值。矿工只能通过在该目标值范围内求得正确的随机数以得到该区块的记账权及区块奖励。当全网算力提升时，该目标值就会根据难度调整而降低并增加求数学解的难度。

瞬时挖矿/ Instamine

瞬时挖矿指一种新的加密货币在发行后很短的时间内，能很容易被获得的过程。瞬时挖矿的目的是在早期积累大量可用的货币供应，以在后期出售获取高利润。

挖矿难度/ Mining Difficulty

挖矿难度是衡量将信息记录到被称为区块链的数字记录上的难度。在工作量证明中，为

了使得区块产生的速度（也即数学难题的解答速度）维持在大约每十分钟一个，产生的新区块的挖矿难度会定期调整，每隔 2016 个区块（即两周），挖矿难度就会被重新计算，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。

难度目标/ Difficulty Targets
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。难度目标由区块链网路根据过去两周的计算结果，自动重新计算未来两周的难度目标。难度目标由区块中的 SHA 256 Hash 值所决定，通过控制区块标头（Block Header）SHA 256 Hash 值应恰好落在可控范围目标区间之内来增加或减少难度目标。

难度调整/ Difficulty Retargeting
比特币网络每产生 2016 个区块（两周）后，会根据之前 2016 个区块的计算时间以及算力进行数学难题的难度调整，通过将数学解的阈值提高或降低来减少或增加难度，使每个区块的计算时间维持在大约 10 分钟的范围。

与矿机相关词汇

矿机/ Mining Rig
矿机是一种用于加密货币挖矿的计算机，一般配备专业的挖矿芯片，因而耗电量较大。矿机是用来记录被称为区块链的数字记录信息的计算机，通过在区块链网络上的共识机制（一般指 PoW）争夺区块链的记账权，得到求解区块的加密货币奖励以及交易费用，因为挖矿通常需要大量的计算机能力，所以这种专用的计算机是为了挖矿而设计的。矿机一般可分为：ASIC 矿机、GPU 矿机、CDN 矿机、云矿机。

中央处理器/ Central Processing Unit / CPU
中央处理器是计算机的主要设备之一，其功能是解释计算机指令以及处理计算机软件中的数据，与内部存储器、输入及输出设备成为现代电脑的三大部件；CPU 作为通用性计算单元，结构中包含分支预测单元、寄存单元等对于挖矿并无帮助的模块，同时 CPU 并不擅长并行运算（即重复性的工作），因此并不适合用作挖矿。

图形处理单元/ Graphical Processing Unit / GPU
图形处理单元，通常称为显卡，是一种专门在个人电脑、工作站、游戏机和一些移动设备（如平板电脑、智能手机等）上图像运算工作的微处理器。因显卡含有较多的移位寄存器及支持更大量的并行运算，相比 CPU 会更适用于某些数字货币的挖矿。

专用集成电路/ Application-Specific Integrated Circuit / ASIC
专用集成电路（ASIC）是一种为专门目的而设计的集成电路，是指应特定用户要求和特定电子系统的需要而设计、制造的集成电路。在加密货币的应用上，通过牺牲通用计算的能力换取执行特定任务的高效率，ASIC 被使用来帮助记录区块链上的交易，在挖

矿能力方面远优于 GPU。

与算力相关词汇

算力/ 哈希率/ Hashrate
算力是计算机能够完成一个数学程序的速度，譬如接收任何一组信息，并将其转换成字母和一定长度的数字的速度就称为算力。在比特币“挖矿”中，对于数学难题的求解需要找到相应的数学解，而对于任意一个给定范围内的 Hash 值，其求解只能通过自动生成的随机数，因此一个挖矿机每秒能做多少次求解过程就是算力的代表，其单位为 Hash/s。

1. **千哈希/秒/ Kilo-hashes per Second / KH/s**
   KH/s 是千哈希/秒的缩写，即 10^3 hashes/s。

2. **百万哈希/秒/ Mega-hashes per Second / MH/s**
   MH/s 是百万哈希/秒的缩写，即 10^6 hashes/s。

3. **十亿哈希/秒/ Tera-hashes per Second / TH/s**
   TH/s 是十亿哈希/秒的缩写，即 10^9 hashes/s。

4. **万亿哈希/秒/ Giga-hashes per Second / GH/s**
   GH/s 是万亿哈希/秒的缩写，即 10^{12} hashes/s。

5. **千万亿哈希/秒/ Peta-hashes per Second / PH/s**
   PH/s 是千万亿哈希/秒的缩写，即 10^{15} hashes/s。

6. **十亿兆哈希/秒/ Exa-hashes per Second / EH/s**
   EH/s 是 10^{18} 哈希/秒，截止至 2018 年 1 月，比特币全网算力约为 20EH/s。

7. **10^{21} 哈希/秒/ Zetta-hashes per Second / ZH/s**
   ZH/s 是 10^{21} 哈希/秒的缩写。

8. **10^{24} 哈希/秒/ Yotta-hashes per Second / YH/s**
   YH/s 是 10^{24} 哈希/秒的缩写。

与区块奖励相关词汇

区块奖励/ Block Reward
区块奖励是矿工通过算力解决相关数学难题并创建新区块后所获得的奖励，区块奖励根据不同加密货币而有所不同。以比特币为例，比特币以一个确定的但不断衰减的速率被

挖出来，大约每十分钟产生一个新区块，每一个新区块都伴随着一定数量从无到有的全新比特币；每开采 210000 个区块其奖励减半，其周期为四年。从比特币发明最初的 50 个比特币/区块到 2016 年后的 12.5 个比特币/区块，并会在 2040 年达到总数接近 2100 万个比特币，在那之后新的区块不再包含比特币奖励，矿工的收益全部来自交易费。

奖励减半/ Halving

奖励减半是指开采比特币的回报以一个确定的但不断衰减的机制在每 210000 个区块被挖出来后减半。在加密货币中，挖矿是用来记录和验证被称为区块的数字记录的信息。每当解决了一个数学难题后，就会创建一个新区块并将其添加到区块链中，新的加密货币奖励将会在区块链网络确认后交给解决该数学难题的计算机。

5.3 交易

与交易相关词汇

交易/ Transaction / TX

在区块链中一笔交易是一个数字记录，通过区块链网络将交易数据在全网范围中广播，通告加密货币的所有权发生转移，并通过共识机制在全网中进行确认及验证，使得该笔交易变得不可逆并防止篡改。在普通货币里主要的交易类型是发送的货币单位或代币给别人；而在如域名注册等其他系统中，作出并完成报价、订立合约的行为也是有效的交易类型。

验证/ Verification

验证是对于交易的一种确认，通过区块链网络中节点的共识机制，将交易数据在区块链网络广播并由其他节点确认，即验证该笔交易的合法性。

可互换性/ Fungible

可互换是指两种以上商品或是资产可以互换交易，可互换性是指两种以上商品或是资产拥有相互替代的性质。也就是说，在普通交易不影响市场价值的前提下，两种商品具备相互流通的功能，如币币交易中的 BTC、ETH、USDT 等主流加密货币通常用于其他加密货币的计价，因此与其他货币在具备可互换性。

法币交易

即通过法定货币购买，出售或交易数字资产。

币币交易

即通过加密货币购买，出售或交易数字资产。

污点/ Taint

污点指一个账户中被标注为来自于不被信任的渠道的加密货币的百分比。污点常用来测

量使用者的数字钱包中有多少加密货币与失窃货币、假币或者与负面、非法活动相关，由此产生的新数据也会继承源数据“是否被污染”的属性。

重放攻击/ 重播攻击/ 回放攻击/ Replay Attacks
重放攻击在区块链中不同于传统意义，是指“一条链上的交易在另一条链上也往往是合法的”，即在链分叉时，地址和私钥生产的算法相同，交易格式也完全相同，因此在一条链上的交易在另一条链上很可能是完全合法的，也即你在分叉区块中进行的一笔交易很可能在分叉链中皆为合法，即为“重放”。

与过程相关词汇

交易费用/ 矿工费/ Transaction Fee
交易费用，亦称为“区块链费用”、“矿工费”，是在用户进行加密货币交易时收取的交易费用，用以奖励矿工对比特币网络的维护。由于矿工通过向网络提供算力以验证发送和接收的数据是否正确，并将这些信息存储在被称为区块链的记录中，由于这些交易每分钟发生很多次，因此较高的费用会激励这些人先验证并记录交易。

小额交易/ Microtransaction
小额交易是指价值量很少的购买或交易。

尘埃交易/ Dust Transactions
用少量的加密货币在区块链网络中进行购买、出售等交易行为，一般认为当交易费用高于 1/3 交易价值时，即可称作“Dust”或尘埃交易，目前而言，尘埃交易是指交易价值低于 546 satoshis 比特币（即 0.000000546 BTC）的交易。

保证金交易/ Margin Trading
保证金交易是通过使用保证金采取杠杆交易的交易方式，保证金交易允许投资者在支付杠杆资金利息费用的同时控制并使用比自己实际拥有更多的资产，是一种高风险的市场操作行为，因此在金融领域中已将其纳入监管范围进行穿透监管。

交易广播/ Transaction Broadcast
将交易信息在区块链网络中“广播”，并由节点验证即确认的过程。

交易确认/ Confirmation
交易确认表示该笔交易被区块链网络所记录并确认，当交易发生时，记录该笔交易的区块将进行第一次确认，并在该区块之后的链上的每一个区块进行再次确认；当确认数达到六个及以上时，通常认为这笔交易比较安全并难以篡改。

交易零确认/ 0 确认/ Zero Confirmation
比特币交易的拥堵情况随着并发交易数量的增加而增加，许多矿池会对内存池中的交易

按照手续费高低排列，优先处理高手续交易，其理想情况是高手续费交易先解决，低手续费交易后解决。然而在实际的市场应用中，由于新的交易不断出现，低手续费交易可能永远得不到处理，长时间甚至永久处于 0 确认状态。

未确认交易/ Unconfirmed Transactions
交易数据处于未确认的状态，即交易数据在全网广播后，节点会不断从交易池中选择交易数据进行记录（一般根据交易手续费进行排序），并试图将数据记录在区块上，而未确认交易是指该笔交易尚未被记录在区块链上。

零确认交易/ Zero Confirmation Transaction
零确认交易是指，交易卖家不等待该笔交易被区块链网络节点确认，即交付出售的东西。零确认交易是一种信任的标志，卖方必须相信买方在该笔交易被区块链中的其他节点记录前不会再尝试将其持有的加密货币再花在其他地方。

5.4 市场

与指标相关词汇

波动性/ Volatility
波动性被广泛用来测量资产的风险性，与潜在收益率的范围及其发生的可能性有关，是衡量资产价格在一段时间内可能发生变动的大小；与股市相比，加密货币交易市场具有更大的波动性，因此加密货币的市场价格在一天之内可能会发生极大的变化。

供应量/ Circulating Supply
供应量是市场参与者持有的流通的加密货币总量，能够通过市场进行购买、出售以及交易，而被锁定、被保留或者不能被出售和流通的加密货币则不在供应量的范畴以内。

总供给/ Total Supply
总供给量是当前可用的加密货币的总量，是指市场中当前存在的所有的流通或非流通加密货币的总量，而被销毁的币则不在总供给的范畴以内。销毁币是将加密货币发送到一个不可靠地址的行为，是不可逆的。

最大供应量/ Max Supply
最大供应量是指加密货币的最大数量，如：比特币的最大供应量约为 2100 万枚、瑞波币的最大供应量约为 1000 亿枚，而不同的加密货币则有不同的数量上限，如 EOS 没有最大供应量，所以其货币数量将持续增长。

登月/ Mooning
登月是指一种加密货币的价格大幅上升的情况，夸张地说就是价格达到天空以及月亮的高度。

投资回报率/ Return on Investment / ROI

投资回报率（ROI）=（税前年利润/投资总额）*100%。是指企业从一项投资性商业活动的投资中得到的经济回报，是衡量一个企业盈利状况所使用的比率，也是衡量一个企业经营效果和效率的一项综合性的指标。

与操作相关词汇

套利/ Arbitrage

套利是指在两个不同的市场中，以有利的价格同时买进并卖出或者同时卖出并买进，同种或本质相同的证券、商品或是资产以赚取价差的行为。通常发生于某种实物资产或金融资产拥有两个价格的情况，通过套利获取低风险的收益。

做空/ Shorting

做空是指预期未来行情将会下跌，将手中借入的股票或是资产按当前价格卖出，待行情下跌后买进再归还并将差额保留为利润。

杠杆/ Leverage

杠杆是一种常见的金融交易制度，通过保证金制度借入资产进行投资，在可交易金额被放大的同时增加投资者的投资能力、放大投资的结果；但也使投资者获得的收益和承担的风险加大，无论最终的结果是收益还是损失，都会以一个固定的比例增加。

Shilling

Shilling 意味着欺骗尽可能多的人，让他们认为该加密货币是有价值的，并且借由价格上涨卖出并赚取利润。

低吸高抛/ Pump and Dump

指少数具有影响力的投资机构或是投资人低价购入加密货币，接着在报纸文章、电视媒体或互联网吹捧他们手中的加密货币使价格上涨并在高位时卖出获利。

拉抬价格/ Pumping

散布虚假的信息吹捧股票以拉抬股价叫做 Pumping。

高价抛售/ Dumping

在股价上涨后卖出手中持股获利叫做 Dumping，卖出持股时使股价下跌，并造成其他投资者利益受损。

大反转/ Flippening

大反转是指竞争币（Altcoin）或其他加密货币对于比特币进行一种替代，成为市值更高、流通更频繁、在区块链中更为重要、更有价值的转变。比特币是第一个主要的加密货币，并且大多数的加密货币的价格和技术都被与比特币相比较；目前而言，可能发生

大反转并取代比特币市场地位的加密货币有以太币、瑞波币。

鲸鱼/ Whales
鲸鱼是指在二级市场中持有大量数字货币、股票、权证的人或组织，因为他们具有大量买入或是卖出的能力，能够通过二级市场操作大大影响当前的市场价格，造成市场价格较大的波动，故称作鲸鱼。

5.5 工具

与钱包客户端相关词汇

完整客户端/ Client
完整的钱包客户端能够存储所有的交易历史记录，功能完备。

轻量客户端/ 轻钱包/ Lightweight Client / SPV Wallet
轻量级的钱包客户端不保存交易副本，通过简易付款验证技术实现，交易需要向其他节点查询。

简易付款验证/ Simplified Payment Verification / SPV
简易付款验证（SPV）是一种客户端的替代解决方案，用这种方案可以实现轻量级的钱包客户端，在客户端无需下载和管理整个数字记录，就可以确认自己的加密货币交易已经被正确记录。

在线客户端/ Online Client
在区块链交易中。通过网页模式来浏览第三方服务器提供的服务，并藉由加密的私钥实现加密货币的交易。

与钱包类型相关词汇

钱包/ Wallet
加密货币钱包形式多样，使用者可以通过钱包检查、储存、花费其持有的加密货币资产。

冷钱包/ Cold Wallet
冷钱包是一种脱离网络连接的离线钱包，将私钥、交易数据存储于冷钱包将免疫网络黑客、木马病毒的袭击，并且避免出现丢币、盗币的情形。冷钱包是加密货币存储的最安全方式，但也不是绝对安全的，硬件损坏、丢失都可能造成加密货币的损失，因此需要做好密钥的备份。

离线钱包/ Offline Wallet

即冷钱包。

热钱包/ Hot Wallet

热钱包是一种网络连接的在线钱包，其原理是将私钥加密后存储在服务器上，当需要使用时再从服务器上下载下来并在浏览器端进行解密；由于联网的原因，个人的电子设备有可能被黑客植入木马用以盗取钱包文件、记录钱包的口令或是破解加密私钥，而钱包服务器也并非完全安全。总体而言，热钱包由于不受客户端限制，易用性强。

在线钱包/ Online Wallet

即热钱包。

核心钱包/ Core Wallet

钱包是与记录网络（区块链）交互的软件，可以让用户接收、存储和发送加密货币。而核心钱包则包含整个区块链的记录，用户不仅可以接收、存储和发送加密货币外，还可以在上面进行编程。比特币交易被保存在数字记录中，被称为区块链，区块链由全球数千人维护，这个数字记录每天都在增长，并在 2016 年超过 100 千兆字节。

软件钱包/ Software Wallet

软件钱包是一个计算机程序设计的设备，具备排他性用以保护加密货币。钱包是与记录网络（区块链）交互的软件，可以让用户接收、存储和发送加密货币。

硬件钱包/ Hardware Wallet

硬件钱包是专门处理比特币的智能设备，通过硬件接口将加密货币的私钥存储于硬件设备中，用以保护加密货币免受网络黑客攻击，与离线钱包的概念较为相似。

本地钱包/ Local Wallet

本地钱包是指将私钥、交易数据存储于本地端，如电脑、手机或是其他本地设备中；是指密钥的存储位置，其概念独立于在线钱包、离线钱包。

纸钱包/ Paper Wallet

纸钱包是转移加密货币的一种方法，是将比特币交易所需要的公钥和私钥信息以纸质化的形式保存，只要进入到「纸钱包工具（Paper Wallet Tool）」页面，就能生成一组钱包地址，收到的人在支持的网站上输入纸上的密钥信息后就可以领取，通常纸钱包上还会印上二维码，用户通过扫描二维码能够直接将加密货币转移到钱包中快速交易。

分层确定性钱包/ HD 钱包/ Hierarchical Deterministic Wallet / HD Wallet

分层确定性钱包是指通过创建一个父公钥生成所有的子公钥，并将主私钥以纸钱包的方式备份、离线存放在本地端，在安全、记账、备份、权限控制等方面相较于传统钱包具有优势。

与数据存储相关词汇

冷存储/ Cold Storage
冷存储是指加密货币“离线化”的过程，相当于将加密货币存储于保险箱，通过容量大、性能要求不高、成本低廉的永久存储介质来集中存储冷数据，其目的在于保证其安全性和可靠性。目前加密货币的冷存储方式主要有三种：

1. 使用硬件钱包。
2. 打印软件钱包中的二维码，并将其储存于安全的地方。
3. 将软件钱包中的文件存储于 USB 中，并将其储存于安全的地方。

离线存储/ Offline Storage
即冷存储，实际上离线存储还是需要上线，并将其存储地址传送给在线存储。

热存储/ Hot Storage
热存储是指加密货币“在线化”的过程，相当于将加密货币存储于钱包，通过保持联网上线将需要被计算节点频繁访问的数据放在网上以就近计算，其目的在于保证高频使用的数据的方便获取。

在线存储/ Online Storage
即热存储。

5.6 发行

发行/ Emission
“发行”也被称为发行曲线、发行率和发行时间，是创建和发布新的加密货币的速度。许多加密货币都设置了定期创建定额加密货币的机制，可以通过发行率来衡量；有些加密货币会限制货币被创建的总量，即最大供应量。

空投/ Airdrop
空投实际上是一个有特定市场或是既有的项目将其本身的代币按照某一规则进行派发的行为过程，当一个新的加密货币被创建出来，获取用户群的一个方法就是空投。

水龙头/ Faucet
水龙头是提供少量、免费的新型加密货币的网站或应用程序，以帮助提高人们持有加密货币的意识。比特币水龙头是一种全新的免费获取比特币的体验站点，此类网站在国外十分流行，只需要输入简单的验证码，就可以在固定的时间段免费获得一定比例比特币。

首次赏金发行/ Initial Bounty Offering / IBO

首次赏金发行是在一段时间内公开并发行一个新的加密货币，通过这个过程，加密货币将被公开分发给花费时间及能力协助加密货币社区创建的人群，是一种在项目早期的激励方式，与 ICO 不同的是，IBO 不是一个买与卖的过程，而是一种精神投入。

与发行数额相关词汇

软顶/ Soft Cap

软顶是加密货币从初次币发行（ICO）投资者处获得的最低金额。ICO 是在有限时间内，将新的加密货币公开、直接销售给人们。如果 ICO 没有达到软顶金额，资金将按照原路径被退还给投资者。

硬顶/ Hard Cap

硬顶是投资者从首次币发行中获得的最大金额。

隐顶/ Hidden Cap

Hidden cap 是加密货币在其初始发行（ICO）中可以从投资者那里获得的金额的未知限制。Hidden cap 的情况和限值是由开发团队创建的，目的是防止富有的投资者投入大量资金，使小额投资者有机会把他们的钱投资到一种新的加密货币中。

与发行轮次相关词汇

众筹/ Crowdfunding

众筹是由发起人、跟投人以及平台构成。具有低门槛、多样性、依靠大众力量、注重创意的特征，是指一种向不特定公众募资，以支持发起人或组织的特定目的行为。

基石轮/ 种子轮/ Seed Round

基石轮是区块链项目的早期投资，团队提出了产品的想法但没有实际的产品，需要启动资金使产品落地，是项目启动后的第一轮融资，相当于风险投资领域的种子轮概念。

天使轮/ Angel Round

天使轮即通过天使投资人获得融资，项目启动后的第一轮融资，融资额度高于种子轮，约在数百万元人民币左右。

私募轮/ PE Round

私募轮广义上包含种子轮、天使轮以及 ICO 发行前的各个轮次融资，私募轮只对特定机构或投资人发行，并且无需对外公开。

公募轮/ Public Offering

公募轮在区块链中一般是指 ICO 阶段，ICO 阶段一般持续数十天，并且分为数个融资

轮次给予不同折扣，并根据融资规模设置硬顶及软顶。

首次公开发行/ Initial Public Offering / IPO

首次公开发行是指一家企业或股份有限公司将股份通过证券交易所，首次向公众出售并筹集资金的行为。

首次币发行/ Initial Coin Offering / ICO

首次币发行是区块链项目首次发行代币以募集比特币、以太币等通用加密货币的行为。ICO 可类比股票市场的 IPO 概念，是为加密货币或者数字货币募集资金的一种广泛形式，参与者看重的是项目发展的潜在投资价值，其本质是一种产品众筹。

首次矿机发行/ Initial Miner Offering / IMO

首次矿机发行与 ICO 和 IFO 具有明显的不同，ICO 和 IFO 是在已有加密货币的前提下使用矿机挖矿，而 IMO 则是使用区块链中的共识机制发行，通过发行一种专用矿机，通过该种矿机挖矿来产生新的加密货币以规避监管。

首次分叉发行/ Initial Fork Offering / IFO

首次分叉发行与首次币发行不同，首次分叉发行通常是建立在主流加密货币的基础上进行分叉，通过分叉前持有主流加密货币即可获得数量相等的对应分叉的分叉币，即另一种虚拟货币。IFO 技术人员采用技术手段对比特币等主流加密货币分叉，开发的分叉币会按比例相应分配给比特币持有人，并且在交易流通中获得价值，部分也会通过数字资产交易所进行交易流通。

与 ICO 相关词汇

天使投资/ Angel Investment

天使投资属于权益资本投资，是指个人将资金投入在具有技术或独特想法的原创项目或小型初创企业或团队，进行一次性的前期投资。

风险投资/ Venture Capital

风险投资也是权益资本投资的一种，指金融机构对新兴发展的、有巨大潜力的创业团队或者企业的高风险投资行为。风险投资的产品关注的是产品和技术的市场潜力和社会价值，看重其长期价值，公司在步入正轨以及项目有一定的成熟度后，风险投资会提高公司的估值。

私募机构/ Private Equity

私募机构是面对少数机构投资者以非公开的形式发行证券、募集资金的机构。私募机构的销售和赎回业务都是通过基金管理人与特定的投资者协商的形式进行。

代投/ Delegated Investment

随着央行七部委在 2017 年 9 月 4 日颁行《关于防范代币发行融资风险的公告》，将 ICO 定义为非法集资行为后，部分国内人士将自己的数字资产交由“代投”人员进行加密货币投资，由于代投属于非法集资范畴并且交易相对隐秘，因此成为虚假项目、诈骗项目滋生的温床。

传销组织/ MLM Organizations

传销组织是以一个虚假的项目或公司作为噱头，煽动人们参加的非法组织。在传销组织中，管理者根据每个人发展的新成员的数量支付报酬，新成员加入组织时需缴纳一定的费用才能获取入会资格。传销组织的日常活动就是洗脑和煽动新成员加入。

与白皮书相关词汇

白皮书/ White Paper

白皮书是解释加密货币中使用的目的和技术的文档，通常一个加密货币通过使用白皮书帮助人们了解它所提供的内容，同时也是投资人了解一个项目的重要信息渠道，因此一个清晰而简单的白皮书是一个新的加密货币的好兆头。

摘要/ Abstract

摘要在加密货币技术文件中很常见，通常放在开头部分用来简要描述整个文件。

路线图/ Roadmap

路线图是一个有预计完成日期的计划，显示了一个组织想要达到的长期目标，查看路线图有助于解组织希望向客户提供什么以及想要成为什么。

概念证明/ Proof of Concept / POC

概念证明是对某些想法的一个较短而不完整的实现，以证明其可行性。概念证明通常被认为是一个有里程碑意义的实作的原型，在区块链中是预发布版的另一个称呼。

6 风险与监管

6.1 投资风险

Cryptojacking
黑客在受害者的计算机上安装病毒程序，在受害者不知情的情况下下秘密挖掘加密货币。

黑客攻击/ Hacking
黑客攻击是指以未经授权或未经批准的方式强行用计算机恶意操作另一台计算机或其计算机系统的过程。

丝绸之路/ Silk Road
丝绸之路是一个非法的网站，营业于 2011 年至 2013 年 10 月，允许人们使用比特币等加密货币买卖非法产品和服务，如毒品、武器、身体部位和刺客等。

庞氏骗局/ Ponzi Scheme
庞氏骗局是以查尔斯 • 庞齐的名字命名的，他是一名伪造概念企业的人，他向投资者承诺在 45 天内将 50% 的钱返还给投资者，或者在 90 天内 100% 返还。他没有使用他们的钱来建立一个企业，而是用新投资者的资金用来偿还原始投资者，同时查尔斯把一部分投资收入囊中。这种把新投资者的钱用来偿还原始投资者的非法行为，被称为庞氏骗局，其表现形式为在没有具体生产经营的前提下对资金进行“拆东墙补西墙”。

分散式阻断服务攻击/ Distributed Denial-of-Service Attacks / DDoS
DDoS 是一种对网站或其他在线服务的计算机进行攻击，导致服务减速或关闭，阻止真实用户接受服务。DDoS 是由一台计算机获得对许多其他计算机的控制而引起的，这些计算机是用户所不知道的，攻击并将计算机引向在线服务，因为成千上万的计算机试图与一个在线服务连接，所以它变得不堪重负，最终导致不能为用户提供服务。

6.2 政策监管

法令/ Fiat
当权者的官方命令、声明或特定政策，即政权机关所颁布的命令、指示、决定等的总称。

法币/ 法定货币/ Fiat Currency
法定货币是政府宣称有价值的货币，例如美元就是一种法定货币。法定货币本身没有任何价值，也不代表任何有价值的东西，但是法定货币保持其价值，因为本质上它代表公众对政府和银行的信心和信任。

反洗钱/ Anti Money Laundering / AML
反洗钱，是指为了预防通过各种方式掩饰、隐瞒毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私犯罪、贪污贿赂犯罪、破坏金融管理秩序犯罪等犯罪所得及其收益的来源和性质的洗钱活动，是一系列旨在防止将非法收入转化为合法收入、维护市场经济秩序的政策及法律体系。

受监管/ Regulated
受监管表示按照当地或受约束的国际规则去控制或管理某些事情或领域。

无监管/ Unregulated
无监管表示一些不按规则管理和控制的东西，如目前的加密货币仍然不受许多政府管制。

KYC 规则/ Know Your Customer / KYC
KYC 法则要求金融机构实行账户实名制，了解账户的实际控制人和交易的实际收益人，同时要求对客户的身份、常住地址或企业所从事的业务进行充分的了解，并采取相应的措施。

7 民间用语

佛系买币

指持币后不关心加密货币价格走势，无论加密货币资产价格跌到什么程度，都不会减持手中的加密货币的行为。

炒币

为获取高额利润，反复买卖加密货币的行为。

梭哈/ All-In / Show Hand

原本是赌博牌局游戏中的名词，指将手中的全部可用筹码一次性押出；引申为将资金全用来购买加密货币的行为，具有“赌一把”的含义。

腰斩

指加密货币的价格下跌后相对于先前最高价位只有一半的水平。

割肉

指在加密货币价格下跌时减持的止损行为。提前设立好止损价位，防止更大的损失，是短线投资者应灵活运用的方法，新股民使用可防止深度套牢。

爱西欧

ICO 的拟声词，指首次币发行，是用区块链把使用权和加密货币合二为一，来为开发、维护、交换相关产品或者服务的项目进行融资的方式。

PPT 融资

当一个项目进行首次币发行时，需要发布 ICO 白皮书来披露项目情况、发行的代币数量、筹集资金的用途等信息。白皮书通常以 PDF、PPT 等文件格式发布在项目官网或相关专业网站上，“白皮书”在 ICO 中的作用就和招股说明书在 IPO 中的作用类似，但由于 ICO 项目极大程度地依赖于白皮书是否制作精良，因此被称之为“PPT 融资”。

韭菜

指不了解市场情况的散户。因为散户不了解市场情况且容易受到投资情绪左右，容易高位买入、低价卖出，而当一部分人亏损离场后又会有新生力量进入，就像韭菜一样割一茬很快又长一茬。

割韭菜

指庄家低位买入，炒高币价等散户进来后高价卖出获利，再砸盘砸到低位重复以上套路。而散户就像韭菜一样，割完又有新的一批入场。

空气币

空气币指没有任何技术依托的 ICO 代币，通过传销机构吹捧而号称有广大远景，但实际上不可行或是无法兑现。与国外相比，国内的 ICO 项目伴随着诸多“空气币”骗局。

传销币

传销币采用拉人头的方式获利，和开启项目后投资者获币不同，传销币成本不清，而且可能长期超发以满足新的受害者持币的心理。传销币完全抄袭别人的开源代码来搭建程序，且项目方长期不更新代码也不公布项目进度。

币圈/ Coin Community

“币圈”指的是专注于炒币，甚至发行自己的加密货币进行筹资（即代币众筹）的人群，业内俗称“币圈”。

链圈/ Chain Community

“链圈”指的是专注于区块链的研发、应用或区块链底层协议的人群。

矿圈/ Mine Community

“矿圈”指的是专注于“挖矿”的“矿工”人群。

矿难/ Mine Disaster

虚拟货币矿难指的是当挖掘成本（主要是矿机和电费）高于市场价时，继续挖矿也无法赚取虚拟货币收益。“矿难”时，大量挖矿玩家停止挖矿，而前期购买的显卡等硬件可能会以较低的价格出售，因此虚拟货币的矿难会极大地缓解显卡缺货的局面。

糖果/ Candy

加密货币在项目起步时都需要推广，常见的推广方式之一就是“发糖果”，即免费向用户发放一定数量虚拟币，这些免费的虚拟币被用户们称之为“糖果”。

“Hello World”

学习一个新的编程语言，一个最重要的仪式就是写出一个能输出 Hello World 的程序。而在币圈是指微拍创始人胡震生做的区块链项目 Showcoin （秀币）在 ICO 后，其代码库只有一句“Hello World”。

亿元披萨

2010 年，佛州程序员 Laszlo Hanyecz 用 10000 个比特币成功支付 2 个披萨，这是比特币历史上的第一次商业交易。以比特币后来最高超过 10 万人民币的价格来计算，当时 1 个披萨价值约为 5 亿元人民币。

泡菜溢价/ Kimchi Premium

韩国民众热衷于投资加密货币，当地的加密货币价格相对于其他国家和地区的高溢价被称为“泡菜溢价”。

类固醇以太坊/ Ethereum on Steroids

“类固醇以太坊”是 EOS 的戏称，EOS 区块链是完全可编程的，消除交易费用并能够每秒处理数百万次交易。

8 加密货币 TOP100

注：以下内容根据 2018 年 1 月 15 日 CoinMarketCap 的加密货币市值排名编写。

001. 比特币/ Bitcoin / BTC

——一种点对点的去中心化加密货币

Bitcoin （比特币）的概念是由中本聪（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、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%。

002. 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。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）的加密货币。

003.（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，用于解决金融机构以及用户间的资产转换和信任问题。XRP （瑞波币）是 Ripple 网络流通的基础货币，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。

004. 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。

005. 莱特币/ 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，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。

006. 卡尔达诺/ 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

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 Gerolamo Cardano，Cardano 是医生、占星术士、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。

007. 恒星币/ Stellar Lumens / XLM

——数字货币与法定货币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。

008.（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”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））。

009.Enterprise Operation System / EOS

——下一代可扩展的商用 *DApps* 操作系统

EOS 是一种全新的基于区块链智能合约平台，旨在为高性能分布式应用提供底层区块链平台服务，提供帐户、身份验证、数据库、异步通信以及在数以百计的 CPU 或群集上的程序调度。EOS 的项目目标是实现一个支撑分布式应用程序的区块链架构，并在横向和纵向都高度模块化的区块链操作系统，并提供各种必要的功能和超高的处理能力让开发者可以将注意力集中在业务层，实现分布式应用的性能拓展并最终达到支持每秒

执行数百万笔交易，同时普通用户在执行智能合约时无需支付使用费用。

010. 埃欧塔/ Internet of Things Association / IOTA

——*去中心化物联网加密货币平台*

IOTA（埃欧塔）专注于解决机器与机器（M2M）间的交易问题，是物联网面临的基础设施挑战的解决方案，通过实现机器与机器间无交易费的支付来构建未来机器经济的蓝图。基于新型的分布式账本——Tangle （缠结），克服现有区块链设计中的低效性，具有零传输费用、无限扩展、数据安全等特性并能够成为任何 P2P 交易结算的支柱。IOTA 目前的主要功能是无需手续费的微支付、安全的数据转移以及数据锚定，具有良好的扩展性和分区容错特性。

011. 达世币/ Dash / DASH

——*基于比特币的专注于保护隐私的匿名币*

Dash （达世币）是一款支持即时交易并以保护用户隐私为目的的加密货币，基于比特币，特有的双层网络能使其更全面地进行测试和更新。达世币通过独创的去中心化网络服务器“主节点”混淆交易实现匿名，使得交易无法被追踪查询，用户可以使用达世币进行安全的在线即时支付，商户则可以在店内（如网店、应用商店等）添加由全球用户所建立的开源支付平台。

012. 新经币/ New Economy Movement / NEM / XEM

——*基于区块链技术的“新的经济引擎”*

XEM （新经币）的创始者是 BitcoinTalk.org 论坛的 UtopianFuture，受到 NXT （未来币）启发并在未来币的基础上进行改进形成新经币。新经币于 2015 年发布，是一个基于 Java 编写的新型加密货币，采用基于 POI （重要性证明）的同步解决方案。新经币自最初的股权分配起就被设定为平等发布，决定重要性的关键在于节点在网络中的活跃度以及交易的对象，而非持有币的多寡或是算力的高低。新经币据称是第一个在块链层面实现多重签名的加密货币。

013. 门罗币/ Monero / XMR

——*基于 CryptoNote 的专注于保护隐私的匿名币*

Monero（门罗币）基于 CryptoNote 协议于 2014 年创建，致力于隐私保护的新一代虚拟货币，规避了比特币的设计缺陷，使得门罗币更加隐私、去中心化、可扩展，而在协议层的 RingCT （环形加密技术）使得门罗币成为目前唯一能隐藏交易发起者、接收者、交易金额和交易 IP 的加密货币。

014. 应用链/ Lisk / LSK

——*基于 JS 的去中心化应用平台*

Lisk（应用链）是一种基于 JavaScript 的高度可扩展公有链，可以在 Lisk 平台上编写 DApps，而不需学习相对复杂的区块链编程语言。开发者可以通过官方提供的 SDK，使用 JavaScript 语言在 Lisk 平台内开发自己的 DApps，让开发者可以快速在区块链上

建立自己的应用。

015. 以太经典/ Ethereum Classic / ETC

——以太坊因 *DAO* 失窃案的产生的分叉币

Ethereum Classic（以太经典）是以太坊项目针对 The DAO 资金问题，开发团队在征询社区意见执行硬分叉后，未遵从或未升级的以太坊区块分支，保留了原有以太坊的代码规则和特色。以太经典的宗旨是“延续一个去审查制度的以太坊”、“为反对硬分叉的人提供选择空间”。

016. 波场币/ Tron /TRX

——基于区块链的全球自由内容娱乐体系

Tron （波场）是基于区块链的开源去中心化内容娱乐协议，致力于利用区块链与分布式存储技术，构建一个全球范围内的自由内容娱乐体系，让每个用户自由发布、存储、拥有数据，并通过去中心化的自治形式，以数字资产发行、流通、交易方式决定内容的分发、订阅、推送，赋能内容创造者并形成去中心化的内容娱乐生态。

017. 量子链/ Qtum / QTUM

——价值传输协议及去中心化应用平台

Qtum （量子链）是面向移动端的基础链，致力于开发比特币和以太坊之外的第三种区块链生态系统，并拓展区块链技术的应用及技术边界，是首个基于 UTXO 模型的 PoS 智能合约平台，可以实现和比特币生态、以太坊生态的兼容性。在量子链系统中，可以通过价值传输协议来实现价值转移，并根据此协议构建一个支持多个行业（金融、物联网、供应链、社交游戏等）的去中心化的应用开发平台，并通过移动端的战略，促进区块链技术的产品化和提高区块链行业的易用性，使普通网络用户能感受到区块链技术的价值。

018. 唯链/ VeChain / VEN

——基于区块链的全球账本型信息交互协作云平台

VeChain （唯链）是一个基于区块技术的全球账本型信息交互协作云平台，唯链通过 API 与应用层对接，把现实世界中的人、事或物数字化，实现信息的互通互联。通过基于行业实际应用的智能合约，实现不同场景下的协同和价值转移，从而将现实的商业世界映射到区块链上。唯链以 Baas 的形式为企业级用户提供商品资产管理、追踪溯源、防伪校验、新型供应链管理等服务。

019. 泰达币/ Tether / USDT

——利用比特币区块链交易的法币代币

USDT（泰达币）是一个由著名交易所 Bitfinex 发起和由全球多家交易所支持的 USD 电子代币，按照银行实际持有的法币量进行发行，市场价值与美元按照 1:1 锚定。USDT 基于比特币网络上的一个资产代币，允许用户在全球范围内像使用比特币一样在区块链上进行即时的存储与转账。

020. 比特黄金/ 比特币黄金/ Bitcoin Gold / BTG

——*利于 GPU 挖矿的比特币分叉币*

Bitcoin Gold （比特黄金）是由香港挖矿公司 Lightning ASIC 主导，于 2017 年 10 月在块高度 491406，通过改变挖矿算法 Equihash 以利于 GPU 挖矿而分叉出现的新加密货币，将保留比特币的交易历史，总发行数量为 2100 万并且有 10 万枚预挖 BTG。

021.ICON / ICX

——*基于社会团体的去中心化公有链平台*

ICON 是一个由韩国团队组建的去中心化项目，是类似于以太坊的公有链平台，主要面对银行、证券、保险、医院、大学、政府机构等各种独立的社会团体，让公共机构加入社区（community），社区内部是单独自治的区块链，并通过区块链跨链技术连接而形成去中心化网络，ICON 提供多样化的去中心化应用，包括区块链身份认证、支付和交易等服务。

022.OmiseGO / OMG

——*去中心化交易和支付平台*

OmiseGO 基于以太坊区块链，目标是搭建一个具备去中心化交易、流动性提供机制、清算信息网络和资产支持的区块链网关，帮助用户“摆脱银行的枷锁”。OmiseGO 使用协议代币机制来创建权益证明区块链，以便在参与者之间实现市场活动。和几乎所有其他去中心化交易平台不同，该分布式网络在无需可信任的币的前提下，允许不同区块链间直接进行去中心化交易。该项目的目标群体是东南亚国家总人口中，73% 尚未使用或无法使用正规金融服务的人（无银行账户者），以及 27% 目前使用正规金融服务的人（使用银行者）。

023. 大零币/ Zcash / ZEC

——*无须信任的去中心化交易与支付服务*

Zcash （大零币）是首个采用零知识证明的透明和匿名性共存的区块链系统，它可提供完全的支付保密性，同时仍能够使用公有链维护一个去中心化网络。与比特币不同之处在于，Zcash 交易自动隐藏区块链上所有交易的发送者、接受者及数额，只有拥有查看密钥的人才能看到交易的内容。用户拥有完全的控制权，他们可自行选择是否允许其他人查看密钥。

024. 源石币/ Nano / (RaiBlocks) / XRB

——*零交易手续费的分布式加密货币*

Nano（源石币）是一种基于区块点阵结构（BlockLattice）的新型加密货币，其中每个账户都有自己的区块链，提供近乎瞬时的交易速度和无限的可扩展性，允许账户异步地更新到网络的其余部分，从而以极小的资源开销获得快速的交易确认。交易记录帐户余额而不是交易金额，使得系统可以在不牺牲安全性的情况下进行大幅度的数据库修剪。

025.Steemit / STEEM

——去中心化的社交媒体平台

Steemit 是一个去中心化的社交媒体平台，通过加密货币奖励支持社区建设和社交互动的区块链数据库。Steemit 是第一个尝试精确地、透明地对无数个对其社区做出主观性贡献的个体做出奖励的社交媒体平台，用户可以通过在平台上发布文章、图片、评论或是投票后，根据算法来确定所贡献的价值，得到一种系统奖励代币 Steem。

026. 币安币/ Binance Coin / BNB

——币安发行的用以抵扣交易手续费的代币

Binance Coin（币安币）是由 Binance （币安）发行的代币，基于以太坊发行的 ERC 20 标准代币，其发行总量恒定为 2 亿个并保证永不增发。币安币可以用来优惠抵扣币安的交易手续费，同时币安会通过定期回购的方式使币安币增值。

027. 百特币/ 字节币/ Bytecoin / BCN

——基于 *CryptoNote* 技术的匿名加密货币

Bytecoin （百特币）于 2012 年 7 月发布，是第一个基于 CryptoNote 技术并通过无法跟踪、绝对匿名的交易提供切实可行的匿名货币方案，算法和比特币一样采用 SHA 256，就像一个字节等于 8 个比特一样，百特币总量是比特币的八倍，即 1.68 亿枚。

028.Populous / PPT

——基于区块链的票据金融交易系统

Populous 是一个基于区块链的全球 P2P 票据金融交易系统，采用 XBRL 数据，使用信用评分和破产公式（内含如 Altman Z-score 技术）对潜在目标借款人进行深入的信用风险分析，将区块链的去信任、透明性、安全性和速度与专有的智能合约相结合，直接与票据销售商和贷方进行交易而无需借助第三方，投资者和票据卖家可以使用 Populous 的区块链技术在世界各地交易大量不同的票据。同时 Populous 还使用 K-means 聚类分析等方法，找到需要发票或汇票融资的借款人，提供有针对性的营销解决方案。

029.Stratis / STRAT

——企业级区块链应用开发工具

Stratis 是一个简化的、灵活可定制的区块链开发平台，提供区块链即服务（BaaS）解决方案，Stratis 可以让任何人在几分钟内创建并管理区块链，同时可以定制用户自己的侧链；让希望进行区块链开发的企业，可以简单快捷地在平台上进行开发、测试和部署应用程序。

030.Verge / XVG

——基于比特币技术的匿名币

Verge 是基于比特币技术的开源、匿名加密货币，专为注重隐私的用户而设计，采用多重匿名中心网络（如 TOR、i2P）实现隐私保护及快速交易，平均交易确认时间缩短到 5 秒，易于大规模采用，并使用五种不同的算法挖矿，为矿工提供公平的加密货币分配方式。

031. 云储币/ Siacoin / SC

——基于区块链的去中心化的云存储平台

Sia 是基于区块链的去中心化的云存储平台，通过编码技术、加密技术和区块链，Sia 网络中节点之间互相租用存储空间，而不是向中心化的存储空间提供者租用，既具备传统的云储存功能，同时又解决了传统的云储存存在的安全隐私问题。Sia 将文件分割、加密后通过形成合约分发到分布式网络存储，储存文件的主机不能翻阅其所存储的文件，用户通过私钥来管理数据，主机则可以通过提交证明得到奖励。Sia 相比于传统的云存储平台更快、更便宜、更可靠，而且即使在系统大面积瘫痪的情况下文件也能够不受损坏。

032. 狗狗币/ Dogecoin / DOGE

——起源于网络草根文化的第一代加密货币竞争币

Dogecoin （狗狗币）是基于比特币的源码、采用莱特币 Scrypt 算法并以日本柴犬作为符号的一款竞争币，于 2013 年年底发布，狗狗币起初只是创始人 Billy Markus 用于证明、同时作为比特币的改进示范而创立的加密货币，但发布之后由于价格便宜而在加密货币社区中作为小费的通货而流行。狗狗币是目前国际上用户数仅次于比特币的第二大虚拟货币，交易确认时间为 1 分钟，其飞快的出块速度以及发行总量是为了鼓励用户交易。

033.Status / SNT

——基于区块链的开源通讯平台

Status 是一个开源的通讯平台和支持以太坊的去中心化应用的移动浏览器。Status 是第一个完全基于点对点技术构建的移动以太坊客户端，在为 DApps 开发人员提供一个灵活的平台的同时，最大限度地提高日常中以太坊公有链的使用频率。Status 代币是其网络上的一种功能性网络代币。

034.R 链/ RChain / RHOC

——可并行的去中心化区块链

Rchain（R 链）是一个开源的商业级区块链解决方案，Rchain 合作组织基于一种形式化验证的、去中心化的、并行计算模型来开发一个可并发的、可组合的、可无限伸缩的区块链，在这个技术平台上可以建立一系列的解决方案，包括金融服务、货币化内容传递网络、市场治理解决方案、DAOs 以及 RChain 自己的去中心化社交平台。任何人都可以在 Rchain 上创建私有或联盟的区块链网络，且这些网络都拥有每秒 40000 笔交易的吞吐能力。与 EOS 不同的是，Rchain 的交易吞吐能力随着节点的增加而无限扩展。

035. 比特股/ BitShares / BTS

——点对点的多态数字资产交易系统

BitShares （比特股）是基于石墨烯技术的去中心化交易系统，结合了去中心化的全球支付系统、去中心化的数字货币交易所、去中心化的证券交易所系统，比特股网络中创

造了一种多态数字资产（Polymorphic Digital Asset, PDA）的金融产品，能够跟踪黄金、白银、美元或其他货币的价值，并让持有者获得红利的同时避免所有的交易对手风险。

036.MakerDAO / MKR

——以太坊上的去中心化自治组织和智能合约系统

MakerDAO 是一个基于以太坊区块链的去中心化自治组织，是运行贷券信贷系统的基础设施，为此系统的每一个用户提供有限的违约担保并收取保费作为回报。Dai（贷券币，Dai Bond Coin）贷券币是 MakerDAO 的第一个产品，用以寻求最小代价实现一个对法币稳定的数字资产代币，MakerDAO 利用抵押及价格反馈制度使 Dai 稳定在 1 美元。MKR 是 MakerDAO 系统的管理型代币和效用代币，用来支付借 Dai 的稳定费用以及参与管理系统。与 Dai 稳定货币不同，由于其独特的供给机制和在 MakerDAO 上的作用，MKR 的价值和整个系统的表现息息相关。

037. 波币/ Waves / WAVES

——以太坊上的去中心化自治组织和智能合约系统

Waves（波币）是一个多功能的去中心化定制代币平台，用于自定义资产及代币的发行、转账和交易，用户可以方便安全地在上面发行、存储、管理、交易、分析数字资产，Waves 团队以大规模市场应用和易用性为目标，致力于将区块链技术的便利性和去中心化优点应用到众筹、证券交易和法定货币转账领域。发布之时，Waves 将提供一个全功能的去中心化众筹平台，并提供一个轻量级的 Chrome 插件，运行完整区块链的全节点将会运行在一个单独的软件模块中，用户体验完全接近于中心化的交易、银行体验，使用户在浏览器中就能体验到一键安装程序和全功能去中心化的交易、众筹平台。

038.Veritaseum / VERI

——智能契约

Veritaseum 是一个智能合约，采用点对点的自主分布式网络，使资本市场脱离经纪人、银行、交易所，并可以实现跨链、支持自定义配置，让非专业人员在无需第三方的情况下，可以快速创建、配置、直接输入和管理智能合约。

039.Aeternity / Æternity / AE

——重塑智能合约底层协议的下一代区块链网络

Aeternity 是基础链，致力于解决目前比特币及以太坊所面临的可扩展性、隐私保护、交易速度上的固有缺点。Aeternity 的智能合约是仅仅存在于状态通道中的功能选项，用户仅在侧链上进行互动，只有在意见不一致的时候，代码、智能合约才会涉及到区块链，整个模式就像一个具有自我裁决能力的数字法庭。Aeternity 具有三项特性：状态通道、PoS+PoW 的共识机制、去中心化的预言机。AE 是 Aeternity 的代币，也是 Aeternity 网络使用的记账单位。

040.Augur / REP

——*去中心化的市场预测平台*

Augur 是建立在以太坊平台上的去中心化市场预测平台。用户可以利用 Augur 为自己感兴趣的主题创建一个预测市场，并提供初始流动性，普通用户则可以根据自己的信息和判断在 Augur 上预测、买卖事件的股票。当事件发生以后，如果预测正确并持有正确结果的股票，每股将获得 1 美元奖励，从而收益将是 1 美元减去当初的买入成本。

041. 沃尔顿链/ WaltonChain / WTC

——*结合区块链及物联网的商业生态链*

WaltonChain（沃尔顿链）将区块链技术与 RFID 技术结合，致力于推进区块链技术由互联网向物联网贯通，实现价值物联网、打造现有商业的全新生态。沃尔顿链的目的是搭建一条底层的商业生态公有链，商家可以根据自己的需求建立各式各样的子链。这条商业生态链的主要特征是所有的数据真实可信、可溯源、数据完全共享、信息完全透明、带有时间戳。Walton 团队提出四个阶段性规划，由底层基础平台建立，逐步扩散至零售、物流，最终整合产品生产厂家，实现商业生态纵深的全覆盖。

042. 科莫多币/ Komodo / KMD

——*端对端的安全和匿名货币付款解决方案*

Komodo（科莫多）是一个使用 ZCash 零知识证明来提供 100% 的匿名交易、通过比特币的算力来保证安全，并且以隐私保护为中心的加密货币。使用由 Komodo 团队开发的新的共识机制：延时工作量证明，Komodo 块可以使用比特币区块链进行公证。KMD 是通过基于 Equihash 的 PoW 协议发布的，新的块信息被发送到预先投票的公证人节点，这些节点通过创建自定义事务在 BTC 区块链上插入 Komodo 块信息。

043. 超级现金/ HCash /（红烧肉）/ Hshare / HSR

——*区块链与 DAG 系统的双重侧链*

Hshare（HSR）是 Hcash 发行的代币，该代币基于 UTXO 模型的稳定区块链系统进行开发。而在 Hcash 主链上线之后，可以与 Hcash 进行 1:1 兑换。Hcash（超级现金）旨在建立一个新的底层技术平台用以链接各种不同的区块链技术，从而让基于信任的价值在不同的区块链系统中自由流通。

044.Decred / DCR

——*致力于社区治理机制改进的数字货币*

Decred 是一种开放、渐进和自筹资金的平台系统，将一个基于社区的治理系统整合到其中。其核心是 PoW+PoS 混合工作量证明共识机制，其目的是在 PoW 矿工和 PoS 选民之间取得平衡, 所有 PoW 产出的块都必须经过 PoS 的验证才能成为合法的块，以创造一个更强大的共识概念。一般而言，运作基础设施的矿工拥有相当大的影响力，而用户影响力则相对微弱，Decred 则允许用户无需拥有昂贵的挖矿硬件就能直接参与此项目而发挥其影响力，杜绝了去中心化项目的算力垄断现象以及治理机制问题。

045. 归零币/ ZClassic / ZCL

——删除慢启动和创始人奖励的 *Zcash* 分叉币

ZClassic （归零币）是 Zcash （大零币）的分叉币，Zcash 是一种采用零知识证明算法的透明和匿名性共存的新型加密数字资产，采用 EquiHash 算法和 PoW 的方式构建适合普通电脑挖矿的分发机制。而 ZClassic 的操作与 Zcash 完全相同，但是将 Zcash 中的慢启动和 20% 创始人的奖励删除。

046.0x 协议/ 0xProject / 0x / ZRX

——基于区块链的去中心化交易所协议

0xProject （0x 协议）是基于以太坊的点对点交易的开源协议，以促进以太坊区块链中 ERC20 代币的去信任和低摩擦交易，该协议旨在作为开放标准和通用模块，推动具有交易功能去中心化应用（DApps）之间的互通性。交易由以太坊智能合约系统执行，可以公开访问及免费使用，且任何 DApps 都可以接入，建立在 0x 协议之上的 DApps 可以访问公共流动资金池或创建自己的流动资金池，并对其交易量收取交易费用。

047. 库币/ KuCoin Shares / KCS ——库币发行的用以抵扣交易手续费的代币

KuCoin Shares（库币）是一个区块链资产的交易平台，旨在为用户提供更加安全、便捷的区块链资产交易和兑换服务。KuCoin Shares （库币）是库币交易平台推行的兑换代币，总量恒定为 2 亿个并永不增发，库币是基于以太坊区块链发行的 ERC20 标准代币。

048. 阿朵币/ Ardor / ARDR

——未来币 *2.0* 系统的代币

Ardor（阿朵币）是基于 NXT（未来币）的升级版本，Nxt 是一个老牌区块链服务平台，而阿朵是一个运行所有子链和运行所有交易的 BaaS 平台，用户可以通过主链 Nxt 上创建子链的方式直接享有 Nxt 的区块链技术，除了继承了 Nxt 稳定和强大的功能外，阿朵的创新体现在三个方面：账本数据可剪切、父链 -子链结构、子链即插即用。因为阿朵是 100% 的 PoS，不需要矿工也没有新币被创建。

049.U.CASH / UCASH

——零售服务提供商的点对点网络

U.CASH 是零售服务提供商（转换器）的点对点网络，结合在线和移动应用程序，旨在提供财务授权，它可以让世界上的任何人访问像银行一样的服务，而不必与银行实际上进行交互。UCASH 也是网络本地货币 UCASH 的名称。UCASH 用于以分布式的方式促进高效的对等事务，它也被用作网络燃料，为所有类型的金融服务付费。它使用自己的区块链来构建，以获得强大的智能合约和便宜的交易功能。

050.Ark / ARK

——加密货币大规模应用的生态系统

Ark 是一个被设计成大规模应用的安全平台，Ark 为用户、开发者和初创公司提供创新的区块链技术和服务。目标是建立一个完整的区块链生态系统，使其具有高度的灵活

性、适应性和可扩展性。

051.Revain / R

——基于区块链的下一代用户反馈平台

Revain 是基于区块链的下一代用户反馈平台，在平台上用户发表针对产品、服务或公司的评论将获得奖励，而且这些评论无法被修改、编辑或删除。

052. 龙链/ Dragonchain / DRGN

——可开发商业应用的区块链服务平台

源于迪士尼内部区块链项目的 Dragonchain （龙链）是独立的公有链平台，基于龙链可以创建智能合约、开发区块链应用（DApps），并且支持多种编程语言，龙链致力于打造一站式区块链商业服务平台，并可能进一步发展成为类似以太坊的生态系统，而龙链孵化器旨在帮助区块链初创项目快速成型并实现商业化，通过战略合作的方式，发展成功的代币化生态系统。

053.DigixDAO / DGD

——基于以太坊的金本位资产代币化平台

DigixDAD 是一个智能合同套件，由去中心化自治组织（DAOs）创建，由 DigixGlobal 部署在区块链上，目标是与社区一起治理并建立 21 世纪以太坊金本位金融平台。DigixDAO 利用以太坊智能合同建立标准，DigixDAO 代币持有人能直接对那些致力于 DigixCore 黄金平台成长和宣传的决定产生影响，并给予代币持有人以太坊平台 Digix 黄金代币交易费作为奖励。DGX 是 DigixDAO 发行锚定黄金的代币，1 枚 DGX=1 克黄金，每一个记录 PoA 资产卡被发送到铸币智能合约时，相应的 DGX 代币就被发行出来；而 DGD 是 DigixDAO 的代币，是一种分红收益的币种。DGX 的交易会收取 0.13% 的手续费，这些手续费将会成为 DGD 币的分红来源。

054. 以利币/ Electroneum / ETN

——基于移动端的加密货币及离线钱包

Electroneum（以利币）专注于发展移动端的加密支付及离线钱包，包含 PC、iOS、Android 操作系统，可以将用户所有的转账交易记录加密。Electroneum 可以保护用户的交易记录和钱包内容免于被窥视（即通过 UTXO 查看交易记录以及钱包内容），同时也留下可选择公开访问的交易哈希码用于认证。目前 Electroneum 意图在手游和网上赌场两大领域发展。

055. 字节雪球/ Byteball / Bytes / GBYTE

——存储和传输价值的去中心化系统

Byteball（字节雪球）是一个存储和传输价值的去中心化系统，允许任意数据的防篡改存储，包括可转移价值的数据，例如货币、产权、债务、股份等。这些存储单元彼此链接形成 DAG （定向非循环图），每个存储单元包括一个或多个早期存储单元的散列值，既用于证实早期的单元又用于确立它们的偏序关系。字节雪球允许每个用户在支付费用

的前提下添加新的存储单元，而随着新单元的添加，每个早期单元都将直接或间接地接收越来越多后来单元的确认。

056. 极特币/ DigiByte / DGB

——全球性的去中心化支付网络和数字货币

DigiByte（极特币）是一个开源的全球性的去中心化支付网络和数字货币，DigByte 允许通过互联网移动资金，只需极少费用或无费用即可实现闪电般的快速交易，无需注册、登录。DigiByte 使用 P2P 技术，没有中央管理机构，网络集体管理交易及发行极特币。

057.（小蚁币）/ （小蚁蛋）/ NEOGas / GAS

——非盈利的社区化的区块链项目

NEO 中内置两种原生代币：NEO（小蚁股（曾用名））和 NEOGas（小蚁币（曾用名））。NEO 是管理代币，总量 1 亿枚，用于实现对 NEO 网络的管理权；GAS 是燃料代币，总量 1 亿枚，最小单位为 0.00000001，伴随着每个 NEO 新区块的生成而产生，并免费分发给 NEO 持有人，用于实现对 NEO 网络使用的资源控制。NEO 网络对代币转账和智能合约的运行和存储进行收费，从而实现对记账人的经济激励和防止资源滥用。

058. 注意力币/ Basic Attention Token / BAT

——基于区块链的数字广告平台

Basic Attention Token（注意力币）是 Javascript 创始人、Mozilla 和 Firefox 浏览器联合创始人 Brendan Eich 创办的，是基于区块链的去中心化、透明的数字广告平台，用于解决浏览器中的广告展示和用户激励问题。项目基于 Brave 浏览器开展去中心化数字广告业务，通过零知识证明的运用保护用户隐私，并采用 Anonize 算法统计用户行为，将“注意力”概念进行量化，并可以使用户的关注得到 BAT 代币奖励。

059. 比原链/ Bytom / 比原币/ Bytom Token / BTM

——多元化资产的登记和流通的去中心化网络

Bytom （比原链）是一种多样性资产的交互协议，与当前应用重心尚未明确的以太坊等公有链不同，比原链只专注于资产登记和流通领域，运行在比原链区块链上的不同形态的、异构的比特资产（原生的数字货币、数字资产）和原子资产（有传统物理世界对应物的权证、权益、股息、债券等）可以通过该协议进行登记、交换、对赌和基于合约的更具复杂性的交互操作，连通原子世界与比特世界，促进资产在两个世界间的交互和流转。

060. 路印/ Loopring / LRC

——新一代区块链资产交易协议和交易所

Loopring （路印协议）是新一代区块链资产交易协议和交易所。它采用去中心化技术，提供零风险的代币交易所模式，并允许多家交易所通过竞争，对同样的订单进行链外撮

合及链上清结算，路印协议将彻底解决现有中心化交易所模式的一些固有风险。

061.Kyber Network / KNC

——去中心化数字资产交易平台

Kyber Network 是一个支持多种数字资产即时交易和兑换的系统。为了实现所有用户在不同代币之间的无缝支付，Kyber Network 将提供丰富的支付 API 以及新一代的合约钱包，来扩展 Kyber Network 的整体交易能力。此外，用户还可以通过 Kyber Network 的衍生品交易来减少加密货币世界中的价格波动风险。

062.Zilliqa / ZIL

——下一代高吞吐量区块链平台

Zilliqa 是世界首个实现可扩展性高吞吐量的公有区块链平台，旨在确保安全性的同时解决交易速度与扩展性问题。它将分片技术从理论变为实践，运用创新的密码技术和共识协议支持每秒数千次的交易，并且随着网络增容而不断提高交易的处理能力，可以满足如数字广告业务、电子资产管理、支付、共享经济和产权管理等大规模、高吞吐量应用的规模化要求。

063.Dentacoin / DCN

——牙科行业需求整合的区块链解决方案

Dentacoin 是第一个为全球牙科行业设计的区块链概念，定位于成为改善牙齿健康的一种方式，Dentacoin 旨在全球范围内通过把社区的患者和牙医集中在一起，共同改善全球的牙科护理，并使其价格合理。Dentacoin ERC 20 代币设置为供大众在全球范围内使用。

064.Golem / GNT

——基于以太坊的去中心化全球算力网络

Golem 是基于以太坊区块链的去中心化算力网络，Golem 结合灵活的开发工具，帮助开发者发布软件并获得奖励，进而改变了算力任务的组织和执行方式。通过实现去中心微服务和异步任务执行，用户可以通过 Golem 成为算力的发售方和租用者，大幅降低计算价格。意味着用户可以在其他人的计算机上完成需要算力的工作，或者将自己空闲的算力出售给需要的人。基于以太坊的交易系统被应用于 Golem 平台，用于结算算力提供者的收益和算力使用者所需要支付的费用。

065. 普维币/ Private Instant Verified Transactions / PIVX / 普维零币/ Zerocoin PIV / zPIV

——私人即时验证交易

PIVX（普维币）即私人即时验证交易，是基于比特币核心 0.10.x 和 DASH 技术的开源加密货币。它使用权益证明（PoS）3.0 协议以确保网络安全，并使用创新可变翘板奖励机制，动态平衡主节点与权益累积节点之间 90% 的区块奖励，剩余 10% 用于预算提案。普维币在引入零币协议后实现了将可公开查看的普维币转换为匿名普维币的功能，

该过程被普维币团队称为零币化普维币，即“Zerocoin PIV”或普维零币“zPIV”。

066. 系统币/ Syscoin / SYS

——去中心化的分布式市场

Syscoin（系统币）是一种区块链协议，在区块链中附加了金融基础功能，能够为个人或者商业团队保障数据和市场的安全。系统币旨在为企业和个人提供商品、资产、数字证书和数据交易的去中心化商城，并提供诸如加密通信等创新的内置服务；系统币在 2017 年 3 月底成功启动隔离验证，完成闪电网络测速，并在年中发布区块链商城客户端。系统币总发行量 9 亿枚，流通量 5.5 亿枚。

067.ælf / ELF

——去中心化云计算区块链网络

ælf 是一个去中心化云计算区块链网络，是对标以太坊的下一代去中心化底层计算平台，重点解决目前以太坊存在的性能不足、资源不隔离、治理结构不完善三方面的问题，具有高性能、资源隔离特性以及更完善的治理和发展结构。在 ælf 网络中，节点根据类型进行划分：专业化记账节点（全节点）能够运行在服务器集群之上，提高整个区块链网络性能；“主链 + 多侧链”结构，有效实现资源隔离、“一链一场景”；设立代币持有人的委托票选制度，保障网络高效治理及良性发展。elf 主要用于 ælf 的付费资源支付及治理决策，其中付费资源包括智能合约部署、升级及执行等操作（如交易手续费、跨链数据传输手续费），治理决策包括记账节点的选择、系统新特性的审批及产品重大更新的决策。

068.Quoine Liquid Token / QASH

——全球化的流动性平台

QASH 是日本 QUOINE 公司推出的一款数字加密货币，是基于 LIQUID 而产生的加密货币（LIQUID 平台是一个全球化的交易平台，是一个可以使整个加密经济受益的财务实用工具，代币发行者、代币持有人、创新者和下一代金融服务用户都能够因流动性而受益），其愿景是通过私有链技术和 QASH 打通个交易所之间的交易壁垒，为加密货币提供更好的流动性，并用 QASH 作为统一的手续费结算标准。

069.Worldwide Asset eXchange / WAX

——去中心化的全球虚拟资产交易所

Wax 是一个去中心化的全球虚拟资产交易所，是面向网络游戏虚拟财产交易的通用去中心化平台。该项目提供软件包 + 小程序，构建类似淘宝的小商家去中心化的网络虚拟财产交易所，主要面向虚拟游戏资产交易、流转等市场，允许任何用户在其功能齐全的虚拟交易平台上交易。Wax 代币在虚拟游戏项目中拥有明确的使用场景和价值，具备执行储蓄功能，可用其购买、销售、出租或者交易虚拟装备，并提供即时支付、安全和信任服务。

070. 星云链/ Nebulas / NAS

——去中心化区块链搜索框架

Nebulas（星云链）是全球首个区块链搜索引擎，目标是发掘区块链世界的价值新维度。通过定义区块链世界的基本价值尺度，Nebulas Rank （星云指数、NR）帮助用户更高效地发现和使用区块链上日渐丰富的价值信息。同时，星云链通过内生的 Nebulas Force （星云原力、NF）、Developer Incentive Protocol （开发者激励协议、DIP）、去中心化应用搜索引擎模块，实现区块链协议、系统自身的平滑升级和自我进化。

071. 比特核/ Bitcore / BTX

——比特币的第一个分叉币

Bitcore（比特核）是对比特币进行了改良更新的区块链资产，开发团队为 Bitsend，在 2017 年 4 月 24 日第一个 BTX 诞生。BTX 的总发行量为 2100 万个，区块大小达 20M、支持 SegWit。BTX 使用 Timetravel10 算法，使用 GPU 挖矿并且每隔 2.5 分钟就可以生成一个区块。BTX 的分发方式包含挖矿、空投及快照索赔。

072.Cryptonex / CNX

——全球化的去中心加密货币

Cryptonex 是在其自身区块链平台上开发的一个全球化的、去中心化的新一代加密货币，拥有自己的区块链网络。Cryptonex 的主要目的是提供任何现实中的法币和任何加密货币的兑换，并可以通过手机、支付卡快捷支付购买到理想的商品和服务。

073.Pillar / PLR

——开源多链的私人数据保险箱

Pillar 是持有用户资产的开源数字钱包，并将拓展到用户的现金、资产、财务记录、医疗记录、简历等方面。用户全部的所有权将存储在不同的区块链上，通过 Pillar 用户将不需要任何账户，而转换为持有原子化的个人产权证明。而使用者也不再需要 Apps，个人数据保险箱将取代 ios 或 Android 成为新的操作系统，当旅行、购物、就餐、浏览媒体、使用服务时，个人数据保险箱将完成所有消费项目的支付，而用户只需要接受服务。

074.Ethos / BQX

——去中心化的价格管理平台

Bitquence 是一种针对区块链的人力驱动的加密服务，目的是让每个人都能获得参与到加密货币市场的机会，加速区块链技术的采用，并让加密货币的所有权民主化。通过 Ethos 钱包，终端用户可以方便地进行数字资产投资，根据 Ethos 社区的加密货币评级结果，会自动构建一个一篮子加密货币投资组合，如同购买加密货币的指数基金。Ethos 是 Bitquence 的项目代币。

075.Power Ledger / POWR

——去中心化的能源交易平台

Power Ledger 是一个去中心化、透明和可交互操作的能源交易平台，通过可交易和无摩

擦成本的能量交易代币 SParkz，支持不断扩大的能源应用套件生态系统。Power Ledger 在电能的生产者和使用者之间建起了直接的联系，通过平台实现消费者之间直接的能源买卖，创造一种不需要中间商的能源交易模式。Power Ledger Token （POWR）是 Power Ledger 生态系统的燃料，在公开交易所购买并通过在 Power Ledger Token Exchange 交易应用上进行交易，消耗 POWR 并创建 Sparkz。目前，用户通过使用无锚货币购买和兑换 Sparkz，且使用独特的交易平台进行能源和 Sparkz 之间的闭环交易。通过在两个区块链层中部署双重代币生态系统（POWR 与 Sparkz），生态系统的市场灵活性得以促进。POWR 代币为无阻塞成本的区块链代币，可让应用程序宿主和参与者访问和使用平台（如同有限的软件许可权限）；Sparkz 代币通过智能债券按照托管的 POWR 代币发行，并由应用程序宿主载入其客户。

076. 公信链/ GXChain / 公信宝/ GXShares / GXS

——基于区块链的去中心化数据交易所

公信宝是一个基于区块链实现的去中心化数据交易所，旨在打通各平台数据源信息，实现各个机构之间的数据点对点交易和共享。公信宝数据交易所是一个通用的数据交换平台，底层是基于区块链打造的一条联盟链——GXChain （公信链），适用于各行各业的数据交易。GXShares （与项目同名，也作公信宝）是公信链上发行的加密货币，主要用于在公信链上开发、认证应用、使用链上服务的费用、数据交易所的交易佣金、选举见证人时的选票。

077. 萌奈币/ MonaCoin / MONA

——基于 P2P 技术的网络加密货币

MonaCoin （萌奈币）于 2014 年 1 月在日本发布，是一种基于 P2P 技术的网络加密货币，可以帮助用户即时付款给世界上任何一个人。使用萌奈币可以直接消费卡中的比特币、以太币或基于 ERC20 的加密货币。萌奈币网络每 1.5 分钟就可以处理一个块，已激活了隔离见证并实现了闪电网络功能，更好地应对即时支付和跨链交易。采用 Lyra2REv2 算法进行 PoW 挖矿，能够有效阻止 ASIC 专用矿机以让更多人参与挖矿，更好地做到去中心化并有效避免 51% 攻击。

078.Internet of Services Token / IOST

——下一代的安全及高度可扩展的服务生态系统

IOS 是一个创新、安全的区块链技术，致力于为线上虚拟服务以及数字货品交换提供一个高可扩容、高吞吐的生态环境。此外，IOS 生态系统也使开发者们可以极其便利地在区块链上部署的大型去中心化应用为海量用户提供服务。IOS 网络采用了包括 EDS（高效分布式分片）技术以及 POB （置信度证明）共识机制在内的一系列独创技术，在极大地提升系统吞吐能力的同时保障了系统的安全可靠。

079. 公证通/ 公证币/ Factom / FCT

——基于比特币区块链的分布式匿名数据协议

Factom（公证通）是基于比特币区块链协议而构建的另一层分布式的、匿名的数据协议，利用区块链技术来革新商业社会和政府部门的数据管理和数据记录方式，帮助各种各样应用程序的开发，包括审计系统、医疗信息记录、供应链管理、投票系统、财产契据、法律应用、金融系统等。开发者能够创造新的应用程序，并把数据保存在区块链上面，同时不用受到直接把数据写入比特币区块链的各种限制：例如写入的数据速度、成本、大小等限制。

080.Dent Wireless / DENT

——基于以太坊的移动数据流量交易平台

Dent Wireless 是基于以太坊区块链技术的智能合约系统，在以太坊的区块链平台上创建世界上首个移动数据流量交易平台，在这个平台中，世界各地的用户通过使用 Dent 发行的加密代币或以太币购买移动数据流量，用户也可以将自己没用完的流量放到该平台上出售以换取 Dent 代币或以太币。

081.Aion / AION

——第三代的多层区块链网络

Aion 是一个先进的第三代区块链，Aion 协议支持联合区块链网络的开发，可以将类似于互联网的不同区块链系统，无缝集成到多层集线器模式中，旨在支持自定义区块链体系结构，同时为跨链互操作性提供去信任的机制。Aion 被设计用于连接其它区块链并管理其自身的大量链上程序，AION 令牌作为整个网络的燃料可用于创建新的区块链、货币化跨链桥梁和保护整个网络的安全。

082.Cindicator / CND

——去中心化的混合智能预测平台

Cindicator 旨在建立混合人工智能（集体智能 + 人工智能）的底层基础设施架构，在高度不确定的新型经济环境中做出有效决策。项目包括两个层面：集体智能层面通过去中心化的预测市场得到高质量的数据集；人工智能层面针对数据集进行分析和学习并得到最终的决策。基于区块链技术的预测市场能够提供更加真实的数据，随参与者不断增加，数据丰度和准确率也更有保障。在整个体系中，区块链技术解决了其擅长解决的问题，即数据的真实高效性，为人工智能开展学习和决策奠定了基础；其他问题交给中心化的方法解决。

083.FunFair / FUN

——基于以太坊的去中心化游戏平台

FunFair 是一个基于以太坊智能合约支持的去中心化游戏平台，旨在打造一个任何人都能随时随地参与的透明、安全、公平的线上博彩游戏，解决了博彩游戏高费用和低信任度的问题。

084.Polymath Network / POLY

——基于区块链的证券代币平台

Polymath Network 是一个促进区块链证券代币初次发行和二次交易的系统，使用基于区块链的系统来协调和激励参与者在区块链上合作和推出金融产品。通过创建一个自定义的需求嵌入到令牌本身的标准令牌协议，让这些令牌只能在经过验证的参与者之间购买和交易，一站式解决证券代币无法交易、无法监管、没有接口（成本昂贵）及没有生态圈（无法得到帮助）的难题。

085. 零币/ 小零币/ ZCoin / XZC

——通过使用零币协议来保障账务隐私的加密货币

ZCoin（零币）是一种通过使用 Zerocoin Protocol （零币协议）来保障账务隐私的加密货币，零币是第一种实现零币协议的加密货币，通过使用零知识证明确保了交易双方的相关地址信息免遭泄露。其参数和比特币一样，出块时间 10 分钟，总发行量为 2100 万枚，奖励减半周期为 4 年。零币相比于早期实现匿名功能的混币技术和环签技术，零知识证明的零币协议解决了前二者的不足，采用熔铸和烧毁的方式来彻底切断交易者之间的联系，并同时生成一份证明证实你烧毁了一个零币，并不证明你烧毁了具体哪一个零币。然后通过使用这个证明，你就可以赎回一个完全没有任何交易历史记录的崭新的零币。

086.Kin / KIN

——面向日常生活的去中心化的数字化服务生态系统

2017 年 5 月，加拿大即时通讯社交平台 Kik 宣布推出 Kin 作为聊天应用程序的代币，允许用户通过 Kin 来购买一系列应用服务，消费者可以通过开发者或开发商提供的商品或服务来交换货币，通过将 Kin 整合到聊天应用程序中，在 Kin 内建立一个加密货币生态。

087.Enigma / ENG

——保障隐私的去中心化运算平台

Enigma 是使不同方能够共同存储和运行数据计算的 P2P 网络，同时完全保护数据隐私。借助安全的多方计算技术，不同方能够对分布式存储的数据运行计算程序并得到正确结果，而无需访问原始数据本身。Enigma 分离了数据的访问和计算，使得共享数据不再是一个不可逆过程，实现了对个人数据的自主控制，为数据货币化建立了基础。ENG 币是区块链 Enigma 项目的代币，发行总量 1 亿枚。

088.SALT / SALT

——基于区块链的区块链资产抵押借贷平台

SALT 是一个基于会员的贷款和借款网络，允许用户利用其区块链资产抵押来获取现金贷款、抵消税收并避免交易费用。在 SALT 平台上，贷款机构与借款人将通过网络进行自动匹配，并通过关注借款人区块链资产的价值而不是信用评价来简化申请过程，用户可以使用他们的加密货币作为抵押品获得贷款。

089. 蜗牛币/ 雷德币/ 瑞迪币/ ReddCoin / RDD

——基于区块链的社交网络服务平台

Reddcoin （蜗牛币）专注于将数字货币平台与所有社交网络无缝集成，包括社交平台、游戏、媒体等，致力于将社交网络上的注意力转化为有实际价值的蜗牛币。用户可以在网站上使用蜗牛币购买物品，或者在游戏中使用它们来代替购买游戏中的信用，并成为社交网络的代币，让普通大众都能接受使用加密货币。蜗牛币采用 Scrypt 算法、GPU 挖矿，于 2014 年 2 月发布，出块时间 60 秒，每一个块中包含 10 万个币，每 50 万块产量减半，共计 1090 亿个。

090. 未来币/ Nxt / NXT

——点对点的电子经济生态系统

基于全新的代码编写的 NXT（未来币）被认为是第二代密码币，以 PoS （权益证明）代替 PoW （工作量证明），避免了比特币的诸多缺陷，如消耗资源、易受攻击等。未来币与 Linux 操作系统有许多相似之处，特别是在支持开放源代码和组织结构方面。Nxt 系统于 2013 年 11 月 24 日开始运行，是第一个采用权益证明的加密货币，有资产交易、任意消息、去中心化域名、帐户租赁等多种功能，其升级版为 Ardor （阿朵币）。

091. 互联网币/ MaidSafeCoin / MAID

——基于区块链的去中心化互联网存储平台

MaidSafe 公司成立于 2006 年，立志将互联网去中心化，MaidSafeCoin 是作为 MaidSafe 公司发行的 SafeCoin 的一个代币，并仅为 SafeCoin 最大流通量的百分之十。MaidSafe 平台的目的是为了给第三方程序提供者创造自己的应用程序环境，并由此去除创业公司的开发风险。自我认证技术允许任何使用者完全掌控自己的所有资料，使用者可以通过此 MaidSafe 自由地管理任何信息，并且免除任何第三方的介入。

092. 班科/ Bancor / BNT

——一种分层货币系统兼去中心化交易所

Bancor （班科）协议通过使用支持智能合约的以太坊区块链和储备金，让所有人创建“智能代币”，这种“智能代币”以预先设置的比率来持有一种或几种其它代币作为自己的储备金，为“智能代币”提供异步价格发现机制和连续流动性，通过使用这些储备金，新创建的代币直接获得价值以及流通性，让任何人随时通过智能合约快速兑换、销毁代币或储备货币。

093.Request Network / REQ

——基于以太坊网络的去中心化网络

Request 是一个建立在以太坊网络上的去中心化网络，允许任何人在任何地方发起支付请求，并向接收者提供安全支付方法。所有的数据都存储在一个去中心化的真实分类账里，打造资产发票、会计、审计和付款标准的金融平台。

094.Particl / PART

——去中心化的私密市场平台

Particl 是开源的、保护个人隐私的交易平台，在比特币源码的基础上，针对支付领域的需求而开发的一种新型匿名区块链。通过市场、加密货币、钱包和加密通信工具系统，实现全球范围的匿名的自由交易。

095.TenX / PAY

——连接现实世界和区块链网络的支付系统

Tenx 力求在最大程度上方便用户访问尽可能多的区块链资产，利用 COMIT 标准实现完全去信任、实时和无成本的交易。TenxX 电子钱包能够实现让用户通过手机或信用卡消费 BTC、ETH、DASH 等几乎所有的数字资产，而 PAY 的持有者则可以从每一笔消费中分红。

096.ChainLink / LINK

——去中心化的 *Oracle* 网络

ChainLink 提供了与多方数据安全链接，将现实世界的数据与区块链系统连接起来，允许任何人安全地提供智能合约访问关键的外部数据，脱机支付和任何其他 API 功能，为许多应用场景提供了标准化解决方案，如财务数据传输、金融协议、保险等。ChainLink 通过链接智能合约然后再与外部任何 API 系统进行连接，实现安全的外链和广泛的对接。

097.eXperience Points / XP

——实践于现实世界的经验值奖励机制

eXperience Points（XP）是一个完全独立的加密货币，旨在将加密货币引入日常生活中，并作为一种区块链上的激励货币以及数字货币用以奖励用户，用户能够通过视频游戏、活动、运动、教育、环保获得 XP 奖励，然后在网络上、游戏中或商业街向参与的商户消费 XP。因此，可以说 XP 将用户的日常生活和区块链 XP 世界建立起一座桥梁，通过一种类似优惠券的形式，将用户的日常生活和区块链 XP 世界建立起一座桥梁。这种方法使数字货币完全独立于任何银行、政府和公司，但同时允许它们进行合作并提交方案、开放源代码、文档和内容，这些都有利于网络中的其他参与者。

098.SmartCash / SMART

——基于区块链的去中心化分散经济系统

SmartCash 旨在创建一个可靠、可转换、快捷、以商户为中心、操作简便和社群驱动的加密货币和分散经济系统。SmartCash 使用了零币协议提供隐私性和可互换性，并引入 SmartHive 和 Hive Structuring Teams （HST）技术创建和维护分布式的治理结构：SmartHive 使拥有币的任何人都可以对社区提交的提案进行投票。SmartHive 则让任何人都能参与并提交建议书，创建自下而上的管理结构。

099. 奇点网络/ SingularityNET / AGI

——基于以太坊区块链的人工智能科研平台

SingularityNET（奇点网络）是发现、连接和交易 AI 算法的协议，为 AI 服务提供了

一个去中心化的全球市场，试图同时面对三个复杂而关键的目标。通过利用分布式和开放的机制来支持尽可能广泛的贡献者贡献，并通过尽可能广泛的种类来支持利用，从而创建世界上最好的 AI 服务市场：针对包括软件、机器人和物联网等硬件在内的所有垂直市场的用户。其最终目标是创建一个分布式的 AI 市场，每个区块节点都是 AI 算法的备份、每个人工智能都可以相互通讯、互相支付或是合作，AI 研究人员和开发者可以将自己的 AI 产品分发给 SingularityNET 的用户，用户则通过专用的虚拟货币为服务付费。

100. 牛币/ Neblio / NEBL

——下一代商用区块链解决方案

Neblio（牛币）是一个区块链开发平台，在牛币区块链上可以简化并加速分布式应用程序的开发和部署。企业分布式应用在 Neblio 平台能够快速构建项目，Restful API 支持目前流行的所有编程语言，因此，开发人员可以直接在牛币区块链网络进行交互，而无需了解更为复杂的区块链技术。

声明

1. 本词典系区块链技术领域的专业人士结合自身经验所著，仅供读者参考阅读，不做任何法律上的有效承诺。本词典所存在的争议、歧义之处，请读者积极指正，不胜感激！

2. 维京研究院是维京资本在中国大陆唯一的研究机构和内容输出机构，所有的社交媒体账号（包括且不限于微信公众号、微博、知识星球、Twitter 和 Facebook），均不会设置收费。

3. 本词库的发布方为维京资本和甲子智库。其他任何机构转载时需注明出处，不得擅自商用。

索引