

区块链专业术语大全

你知道什么是 token 吗？你知道 kyc 的意思吗？

这是一个简单而又全面的 Blockchain 词汇表，用于令人印象深刻的 blockchain 语言世界。

ICO:

ICO 是一种区块链行业术语（是 Initial Coin Offering 缩写），直译为首次代币发行。是一种为加密数字货币/区块链项目筹措资金的常用方式，早期参与者可以从中获得初始产生的加密数字货币作为回报。由于代币具有市场价值，可以兑换成法币，从而支持项目的开发成本。

ICO 所发行的代币，可以基于不同的区块链发行，由区块链提供记账服务和价值共识，实现全球发行和流通。

ICO 参与者对于一个项目的成功非常重要，他们会在社区里为该区块链项目进行宣传，使它产生的代币在开始交易前就获得流动性。但 ICO 的参与者最看重的依然是由项目发展或代币发行后价格升值带来的潜在收益。当然，如果跌破发行价，参与 ICO 也有可能损失投资。

白皮书:

白皮书最早的概念是政府或议会正式发表的以白色封面装帧的重要文件或报告书的别称，作为一种官方文件，代表政府立场，讲究事实清楚、立场明确、行文规范、文字简练，没有文学色彩。

针对数字货币的白皮书概念是指数字货币发行方提供的官方正式文档，一般包含项目的目的、发行方、技术特点、创始人、代币数量、代币获取方式等内容。

Attack（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。

Address（地址）

加密货币地址用于在网络上发送或接收交易。地址通常表示为个数字字符

ASIC（专用集成电路）

“专用集成电路”简称。通常，与 GPU 相比，ASIC 专门用于挖矿，可能会节省大量能源。

Bitcoin（比特币）

Bitcoin 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。

Block（区块）

区块是在区块链网络上承载永久记录的数据的数据包

Blockchain（区块链）

区块链是一个共享的分布式账本，其中交易通过附加块永久记录。 区块链作为所有交易的历史记录，从发生块到最新的块，因此命名为 blockchain(区块链)。

Block Explorer（区块资源管理器）

区块资源管理器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。

Block Height（区块高度）

连接在区块链上的块数。

Block Reward（积分奖励）

它是在采矿期间成功计算区块中的哈希的矿工的一种激励形式。 在区块链上的交易验证的过程中产生新的币，并且矿工被奖励其中的一部分。

Central Ledger（中央帐簿）

由中央机构维持的分类帐。

Confirmation（确认）

去中心化的一次交易，将其添加到 blockchain 的成功确认。

Consensus（共识）

当所有网络参与者同意交易的有效性时，达成共识，确保分布式账本是彼此的精确副本。

Cryptocurrency（加密货币）

也称为令牌，加密货币是数字资产的呈现方式

Cryptographic Hash Function（加密哈希函数）

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

Dapp（去中心化应用）

Dapp（去中心化应用程序）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。

DAO（去中心化自治组织）

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

Distributed Ledger（分布式账本）

分布式账本，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。

Distributed Network（分布式网络）

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。

Difficulty（容易程度）

这是指成功挖掘交易信息的数据块的容易程度。

Digital Signature（数字加密）

通过公钥加密生成的数字代码，附加到电子传输的文档以验证其内容和发件人的身份

Double Spending（双重支付）

当花费一笔钱多于一次支付限额时，就会发生双重支付。

Ethereum（以太坊）

Ethereum 是一个基于 blockchain 的去中心化运行智能合约的平台，旨在解决与审查，欺诈和第三方干扰相关的问题。

EVM（以太坊虚拟机）

Ethereum 虚拟机（EVM）是一个图灵完整的虚拟机，允许任何人执行任意 EVM 字节码。每个 Ethereum 节点都运行在 EVM 上，以保持整个块链的一致性

Fork（分支）

分支可以创建区块链的交叉版本，在网络不同的地方兼容的运行两个区块链。

Genesis Block（创世区块）

区块链的第一个区块。

Hard Fork（硬分支）

一种使以前无效的交易有效的分支类型，反之亦然。这种类型的分支需要所有节点和用户升级到最新版本的协议软件

Hash（哈希）

对输出数据执行散列函数的行为。这是用于确认货币交易。

Hash Rate（哈希率）

采矿钻机的性能测量值以秒为单位表示。

HybridPoS/PoW（混合 PoS / PoW）

POW（Proof of Work，工作证明）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。POS（Proof of Stake，股权证明）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。混合 PoS / PoW 可以将网络上的共享分发算法作为共享证明和工作证明。在这种方法中，可以实现矿工和选民（持有者）之间的平衡，由内部人（持有人）和外部人（矿工）创建一个基于社区的治理体系。

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。

Mining（挖矿）

挖矿是验证区块链交易的行为。验证的必要性通常以货币的形式奖励给矿工。在这个密码安全的繁荣期间，当正确完成计算，采矿可以是一个有利可图的业务。通过选择最有效和最适合的硬件和采矿目标，采矿可以产生稳定的被动收入形式。

Multi-Signature（多重签名）

多重签名地址需要一个以上的密钥来授权交易，从而增加了一层安全性。

Node（节点）

由区块链网络的参与者操作的分类帐的副本

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。

Peer to Peer（点对点）

对等（P2P）是指在高度互联的网络中，双方之间的去中心化互动或更多的互动。P2P 网络的参与者通过单个调解点直接相互协商。

Public Address（公用地址）

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。

Private Key（私钥）

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。

Proof of Work（工作证明）

POW（Proof of Work，工作证明）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。

Proof of Stake（股权证明）

POS（Proof of Stake，股权证明）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

Script

Script 是一种由 Litecoin 使用加密算法。与 SHA256 相比，它的速度更快，因为它不会占用很多处理时间。

SHA-256

SHA-256 是比特币一些列数字货币使用的加密算法。然而，它使用了大量的计算能力和处理时间，迫使矿工组建采矿池以获取收益。

Smart Contracts（智能合约）

智能合约将可编程语言的业务规则编码到区块上，并由网络的参与者实施。

Soft Fork（软分支）

软分支与硬分支不同之处在于，只有先前有效的交易才能使其无效。由于旧节点将新的块识别为有效，所以软分支基本上是向后兼容的。这种分支需要大多数矿工升级才能执行，而硬分支需要所有节点就新版本达成一致

Transaction Fee（手续费）

绝大部分加密货币交易都会涉及到一笔很小的手续费。这些手续费用加起来给矿工在成功处理区块时收到的区块奖励。

Turing Complete（图灵完备）

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。一个例子是 Ethereum 虚拟机（EVM）。

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。

大家好，

区块链是目前最前沿的科技，而建立在区块链技术上的数字货币，亦是目前最火的投资项目。90 后 00 后在币圈如鱼得水，不断刷新财富神话。那些 60 后的大妈也蜂拥入场，跟风砸钱。

