





目录

前言	3
认识加密货币	5
认识区块链	9
区块链的类型	9
基础概念	10
技术名词	16
区块链挖矿	19
认识公链	21
公链的类型	21
共识机制	23
扩容方案	25
合约编程	28
合约标准	30
认识 Defi	32
基础概念	32
Defi 应用	35
认识元宇宙	38
基础概念	38
NFT 与数藏	40
认识交易投资市场	44
Token 发行市场	44
投资市场	47
Web3.0 场景赛道	52
附录：Web3 社群俚语	56



前言

Web3.0 到底是什么？

几乎所有第一次听到这个名词的人，都会问出这个问题。假如在百度、谷歌搜索答案，也会得到至少 5 种以上不同的概念，每一种说法都似是而非，让人不明就里。

我们很想以一种通俗易懂的方式告诉你答案，但说实话，比较困难。就像大家很难向一个没有使用过互联网的人解释什么是互联网一样，你用了就很容易理解。要是下定义，就不太容易。

Web3 的愿景其实不难理解，其目的在于构建一个去中心化的互联网系统：**区块链负责底层技术、加密货币充当交易媒介、Defi 构建金融系统、NFT 彰显你的个人属性与权益价值、去中心化钱包作为你的护照**。至于我们所熟知的元宇宙，只是 Web3 生态中的一个线上虚拟空间，并不能等同于 Web3 本身。

基于这个逻辑，我们就需要去理解：什么是加密货币、什么是 Defi、什么是区块链等等，只有完全理解了这些概念，就能对 Web3 有深入的认知。但我们同时注意到，在今天的中文圈里，尚未发现一本简单的、详实的、系统的科普读物去告诉大家这些概念。要么是机器翻译的低质量内容、要么是零散的说法、要么是晦涩难懂的技术语言，无法起到传播与学习的作用。

为此，BlockWeeks联合PandaTool历时一个月，共同制作了这本“Web3.0百科词典”，将Web3领域的诸多概念以浅显易懂的方式告诉你。相信任何一个拿到这本词典的用户，都能最简单、最快速、最低成本的 学习到Web3知识。

[BlockWeeks](#)区块周刊是专注于区块链和Web3.0的顶级媒体，致力于为读者提供最新的行业动态、市场分析、技术解读和深度报道。[PandaTool](#)是全网最强的Web3多链无代码工具，通过可视化的界面，让用户能够快速创建、部署和管理自己的加密货币，而无需编写代码。即便不懂编程的小白用户，也能在这里体会到区块链的魅力。



2014年以太坊联合创始人Gavin Wood提出Web3这个概念时，还不被人所重视。但在2022年的今天，Web3.0的热度日益走高，元宇宙、数藏等产业也迎来了发展。但是加密货币、区块链等依然处于被妖魔化的边缘。因此，所有行业的参与者和关注者，以及想要进入这个行业的新人，都亟需这样一份系统的工具来客观认识Web3.0。

我们期待这本“Web3.0百科词典”，能帮助你建立对Web3.0的有效认知，成为你进入Web3.0世界的一把钥匙。与此同时，我们也要声明，本书的所有内容、观点以及涉及到的任何项目，仅作为解释说明与参考学习，**均不构成任何投资建议**。加密货币市场存在极大的不确定性，风险指数远远高于股市。**我们非常不鼓励盲目投资加密货币的行为**，对任何损失皆不负责，请读者谨慎。

最后，考虑到 Web3.0 相关概念范围较大、各类名词术语仍存在争议，故本书可能会存在错误、偏差或遗漏。如您对本书有任何建议与批评，或者希望增加新的词汇，欢迎发邮件联系。我们采纳您的意见后，将在下一版本中进行优化更新，感谢支持。邮箱：contact@blockweeks.com。

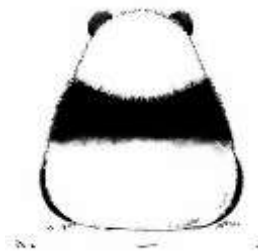
进入 BlockWeeks，掌握新鲜的 Web3 资讯，下载更多 Web3 文档

- 官网：<https://blockweeks.com/>
- X：<https://x.com/blockweeks>



了解 PandaTool，体会无代码 Web3 工具的乐趣

- 官网：<https://www.pandatool.org/>
- X：<https://x.com/PandaTool>
- 社群：<https://t.me/pandatool>





认识加密货币

加密货币是一种使用密码学原理来确保交易安全、不依靠法定发行机构的交易介质，它们基于去中心化共识和区块链技术，在传统银行系统范围之外自主运作。它提供了一种低廉、高效、快捷的转账方式，国际转账无需使用当地的法币，且速度快、手续费低。

在 Web3 生态中，合理的代币经济学设计，可以推动项目的发展与生态的壮大。但是近些年，利用加密货币进行恶意炒作的行为越发普遍，资金盘、割韭菜、违规金融活动等，也让加密货币受到了一些指责与误解。不鼓励大家进行加密货币投资，但是认识加密货币的类型，可以有助于我们更深一步了解 Web3 的经济活动。

比特币 (Bitcoin)

- BTC 是一种基于去中心化，采用 POW 共识机制，以区块链作为底层技术的加密货币。比特币概念由中本聪于 2008 年 11 月 1 日提出，2009 年 1 月 3 日正式诞生，是迄今为止全球最知名的加密货币。

代币

- 在区块链系统里被普遍认可和执行的价值单位，在说法上，与“加密货币”可以互换使用。在国内官方报道中，通常以“虚拟币”指代“代币”或“加密货币”。

主流币

- 在全球范围内，被更多用户认可、在主流交易所上市、市值排名在至少前 50、有具体产品落地或使用场景支撑的加密货币，也称“蓝筹币”。

山寨币 (Altcoin)

- 山寨币也叫替代币，是以比特币或其他主流币代码为模板，对其底层技术进行了一些修改的新型加密货币，如莱特币 (LTC) 就是比特币的山寨币。从广义上来说，所有非比特币都是山寨币。



稳定币 (StableCoin)

- 稳定币的特点在于价格相对稳定, 通过与某一**法币**挂钩, 以现金或现金等价物来保证价格 1:1 锚定, 如美元稳定币 USDT、USDC 等, 价格常年稳定在 1 美元左右。



2022 年 8 月 TOP15 稳定币市值 (来源: cryptorank.io)

公链币

- 由公链推出的原生**通证** (Token), 在具体某个公链生态系统中, 充当价值尺度与交换媒介, 起到类似于货币的作用。我们所熟知的 **ETH**、Sol、ADA 均属于公链币。

分叉币

- 分叉指的是区块链在进行“升级”时发生了意见分歧, 从而导致分叉。区块链在**硬分叉**之后, 会产生一条新的链及代币, 这个币就是分叉币。如比特币的分叉币 BCH、以太坊的分叉币 ETC 等。

匿名币

- 匿名币就是在交易过程中隐藏交易金额、隐藏发送方与接收方的一种特殊的加密货币。**门罗币**(XMR) 被视为是现阶段隐匿性最强的加密货币, 在暗网市场认可度很高。它使用加密技术来屏蔽发送和接受信息以及交易金额, 采取**环签名**和**混淆地址**的方式来保证匿名性。



平台币

- 中心化交易所平台推出的加密货币，一般可被用来抵扣交易手续费、进行 IEO 打新、锁仓挖矿等等，比较主流的平台币有：BNB（币安交易所）、OKB（欧易交易所）、HT（火币交易所）。

模因币（MEME）

- 也叫迷因币，是灵感源于互联网和社交媒体模因或笑话的加密货币。模因币行情极易波动，其价值取决于市场的造势和宣传，如狗狗币（DOGE）、屎币（SHIB）就是典型的模因币。



2022 年 3 月份 MEME 币市值

法币

- 法币是法定货币，是由国家和政府发行的合法流通的货币，如美元、欧元等等。

POW/POS 币

- 以共识机制为标准划分的代币种类。POS 币指的是以权益证明（POS）为共识机制的代币，如 ETH 等。POW 币指的是以工作量证明（POW）为共识机制的代币，如 BTC 等，这类币也叫“矿币”。

锚定币

- 也叫挂钩币、包裹币,是锚定某种代币在其他公链上发行的跨链资产。比如在 ETH 链上发行的 WBTC、在 BSC 链上发行的 BTCB 等,都是比特币锚定币,价格与 BTC 基本保持一致。



比特币锚定币 WBTC 发行逻辑

妖币

- 妖币是充满争议的加密资产,没有足够强大的技术和生态落地,但价格却能毫无逻辑地在短时间内暴涨,市值排名常年稳居高位。

空气币

- 没有任何实际价值支撑及任何应用场景的加密货币,价格随时有可能归零。

传销币

- 指的是涉及拉人头,拉资金的币。打着加密货币的旗号,鼓励会员以“拉人头”的方式赚取回报,不断吸纳会员会费达到敛财目的。早年间的积分盘,本质来说也可称之为传销币。

土狗币

- 指某类没有技术含量、没有任何产品,甚至连官网都没有的加密货币。该类代币主要在去中心化交易所上市,依托各种微信群、tg 群进行宣传造势,大多存活周期不超过一个月。



认识区块链

区块链（英语：blockchain）指的是按照时间顺序，将数据区块以顺序相连的方式组合成的链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

中本聪在 2008 年于《比特币白皮书》中首次提出“区块链”概念，并在 2009 年创立了比特币网络，开发出第一个区块，即“创世区块”。至此之后，区块链开始大行其道。

区块链是 Web3 的支柱和底层技术，如果我们要真正理解 Web3，就必须熟知其基础概念、技术原理与实现路径。在区块链的基础之上，才能更好的认知到 Web3 的真正价值所在。

区块链类型

公有链

- 公有链即公链，是指人人可参与、交易数据公开透明、用户权益不受任何机构控制、数据安全性高不可篡改的公共区块链。
- 代表项目：比特币网络、以太坊

私有链

- 私有链是单独对个人或企业开放的区块链系统，其读写权限掌握在某个中心化组织或机构手里，由该组织根据自身需求决定区块链的公开程度，适用于数据管理、审计等金融场景

联盟链

- 也叫行业链，是由若干组织一起合作维护的区块链，该区块链的使用必须是带有权限的限制访问。各个节点成员通常有对应的实体机构、共享数据资源，只有得到联盟的批准才能加入或退出系统。
- 代表项目：蚂蚁链、长安链、R3 链



	公有链	联盟链	私有链
参与者	任何人都可以自由出入	联盟或者许可成员	公司内部
记账人	任何人	许可成员	公司自定义
激励机制	必须要	可选	可选
中心化程度	去中心化	弱中心化	中心化
特点	区块链所有特点	准入性 (CA+权限)	内部透明和追溯
共识机制	POW/POS/DPOS	PBFT/kafka	PBFT
监管	不支持	支持	支持
应用场景	Dapp开发可支持很多场景	支付/结算/政务/物联网/运输...	审计/积分

私有链、联盟链、公有链区别

基础概念

智能合约 (Smart Contract)

- 就是一段写在区块链上的代码，一旦某个事件触发合约中的条款，代码即自动执行，即智能运行的合约。其具有内容公开透明、不可篡改、去中心化几个特点。广义上看，DAPP、加密货币等运行在区块链中的应用或程序，都可以被界定为智能合约。

去中心化 (Decentralization)

- 指的是一个系统里没有统一的中心，即所有人都是中心，也都不是中心。你做的事情我也可以做，大家都一样。比如在教室上课的时候，老师就是一个中心，这就是中心化。而在英语角，每个人都能发言，大家各抒己见，这就是去中心化。

不可篡改

- 区块链的每一个新区块都会按照时间次序依次加到链内。由于每个区块都与上一个区块相连，并记录了上一个区块的交易数据，而这个数据的副本也会保存在相应的节点里。因此任何人要想篡改区块的数据，就需要更改成百上千个节点里的数据，这是几乎不可能的。

通证 (Token)

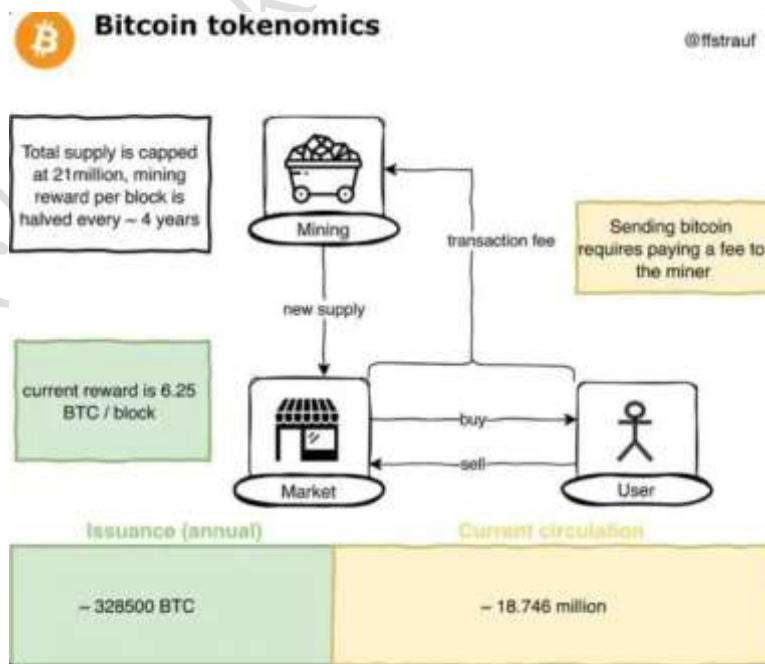
- 广义上来说, Token 的意思是通证、令牌, 即可流通的加密数字权益证明。类似于公司的股权, 拥有某个项目的治理 Token 类似于持有其潜在优势的股份。但是狭义上, 大家习惯将 Token 翻译成“代币”。两个说法都可以日常使用, 不影响。

白皮书 (WhitePaper)

- 一个 Web3 项目的白皮书, 就是项目官方向市场展示商业模式、技术实力、团队能力、发展前景的公告, 是我们判断这个项目好坏优劣的重要依据之一。例如中本聪发布的比特币白皮书《比特币: 一种点对点电子货币系统》。

代币经济学 (Tokenomics)

- 代币经济学并不是一门学科, 而是 Web3 项目的激励模型和工具。为了实现项目生态的良性循环, 生态系统中每个参与者的行为非常重要。而这些行为, 将通过代币予以激励协调。包括代币的发行量与发行方式、分配逻辑、激励措施、价值捕获等。



比特币的代币经济学



路线图 (Roadmap)

- 路线图是显示项目团队在一年或更长时间内想要实现的目标、计划。它让您了解即将到来的功能，以及这些功能何时发布。

通胀 (Inflationary) / 通缩 (Deflationary)

- 所有的代币经济学模式，大致都可以分为通胀型和通缩型这两种。没有最大供应量限制的 Token 采用的是通胀模型，反之是通缩模型。例如每年增发 5%、总量没有上限的狗狗币就是通胀模型。

销毁 (Burn)

- 也叫“燃烧”，即销毁代币。销毁的目的主要是为减少流通中的代币以调整代币的总体供给。不同的项目可能会采取不同的销毁方式，有些是项目方主动回购代币进行销毁（例如 HT）、有些则是依托智能合约自行销毁（例如 ETH）。

黑洞

- 黑洞地址是区块链上一个没有私钥的地址，就像黑洞一样，只进不出，任何代币打到黑洞地址里就不可能再转出来进入市场流通了。所以销毁的方法就是把代币转入黑洞地址里。以太坊链的黑洞地址是：0x00000000000000000000000000000000dead

减半

- 主要是指比特币减半，即比特币网络区块产生时(大约每 10 分钟)，给予矿工的比特币奖励数量减少一半。刚开始时，每诞生一个新区块奖励矿工 50 个比特币。经过三次减半后，现在的奖励已经降到了 6.25 个。减半大概每 4 年左右发生一次。

安全审计

- Web3 项目方邀请第三方审计机构，对其智能合约的代码进行安全审计，以避免可能存在的安全漏洞。在此过程中，审计机构会把发现的问题交给项目方进行修改。结束后，由审计机构出具审计报告。CertiK、慢雾、链安等共识均是知名的审计机构。



51%攻击

- 51% 攻击是针对工作量证明（POW）区块链的潜在攻击，指单个实体或组织能够控制大部分挖矿算力（最好 51%以上），从而可能扰乱网络。比如故意排除或修改交易的顺序，或者撤销已做出的交易，进而导致双花问题。

双花问题

- 指同一笔资金被重复支付给两位收款方。比如，我们微信钱包里有 100 块钱，我们先去饭店吃了顿饭，结果微信出了 bug，这一笔钱并没有被银行同步，还留在钱包里，于是我们又用这 100 块买了张电影票，这就属于双花问题。

钱包

- 钱包是一个生成和存储私钥的工具，可以用它来接收、发送你的代币。但注意，你的资产并不存储在某个钱包软件里，而是「保存」在由私钥推导出来的钱包地址中。

冷钱包与热钱包

- 冷即离线、断网，也就是说，私钥存储的位置不能被网络所访问，比如硬盘、人脑等。热即联网，也就是私钥存储在能被网络访问的位置，比如手机 App 钱包。

单链钱包与多链钱包

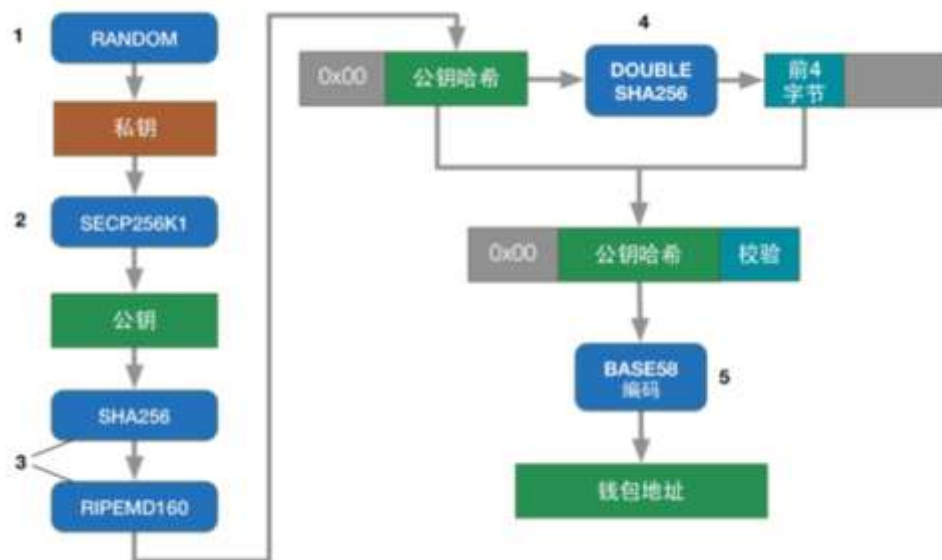
- 单链钱包是指只能存储、收发某一公链 Token 的钱包。比如只支持比特币的钱包 Bitcoin Core、只支持 TRX 及 TRC20 代币的波宝钱包等。多链钱包，简单说就是可支持多种主链平台 Token 的钱包。常见的多链钱包有：TokenPocket、ImToken 等。

多签钱包

- 多签，即多重签名。该类钱包并不是某个钱包软件，而是指需要多个人去签名确认的钱包。使用设置好的多签钱包进行转账时，往往需要 ≥ 1 个人去签名确认，转账操作才真正完成，这样就多了一层安全性。

公钥、私钥、地址

- 私钥是一串 64 位的十六进制字符串，使用私钥可以生成公钥，再由公钥生成一个钱包地址。从转账角度来说，公钥相当于你的银行户头、地址相当于你的银行卡号、私钥相当于你的银行密码。区别在于，私钥不能修改，一旦丢失无法找回。



钱包地址生成过程

硬分叉

- 硬分叉是指当区块链代码或共识机制发生改变后旧节点拒绝接受由新节点创建的区块，不符合原规则的区块将会被忽略，矿工将按照原规则在他们最后验证的区块之后创建新的区块。硬分叉大概率诞生新的一条区块链和 Token，例如以太坊（ETH）硬分叉诞生了以太经典（ETC）。

软分叉

- 软分叉是指区块链代码或共识机制发生改变后，旧的节点并不会感知到区别，并继续接受由新节点创建的区块，矿工们可能会在他们完全没有理解或验证过的区块上进行工作，软分叉新旧节点双方始终都工作在同一条链上，不会诞生新的代币。



快照

- 指的是在某一时刻记录某一**区块高度**的区块链状态，包括某个代币的所有持仓人和持仓数量，一般是为了**空投**使用。

DAPP

- 即去中心化应用，运行在各条公链之上，如 Uniswap、Cruve 等。Dapp 和公链的关系，类似于 App 和操作系统（安卓）的关系。不过 Dapp 大多数只是一个交互网站，且无需账号密码登陆，与 App 的概念区别很大。

TPS

- 即每秒交易速度，或称“吞吐量”，是衡量公链性能的标准之一。

Gas Fee

- 也叫 gas 费、燃料费、汽油费，是各个公链生态内交易产生的**手续费**，主要使用公链型代币支付。如在以太坊上进行转账、买卖、授权等动作，均需要支付小额的 ETH 作为 Gas 费。费用的多少，主要取决于该时段网络是否拥堵。

Staking

- 权益质押，或叫“质押挖矿”。在基于 **POS** 机制的公链里，用户可以通过质押自己的加密资产进行**锁仓**获得代币收益，有点类似于银行的储蓄生息。这里的“挖矿”并非传统意义上的矿机挖矿，而是“代币收益”的一种指代说法。

On-Chain/Off-Chain

- “链上”及“链下”的意思，指的是相关动作发生在区块链上或者区块链下。真正的 Web3 项目，交易信息和数据都要上链，以确保透明性和不可篡改性。如果不能上链，就是打着区块链旗号的假项目。

技术名词

区块 (block)

- 区块是区块链的基本组成单元，用来存储有价值的信息。区块由区块头和区块体组成，其中区块头里包含上一个区块（父区块）的哈希值，本区块体的哈希值，以及时间戳（TimeStamp）、随机数、默克尔根等；区块体则包括本区块内的所有交易信息。



区块内部结构

区块高度

- 指的是该区块在区块链中的坐标位置，即“编号”。比如以太坊于区块高度 15537393 完成合并升级。

区块容量

- 也称区块大小，代表了一个区块能容纳多少数据的能力。例如比特币网络的区块大小是 1M，大概可以包含 2000~3000 笔交易。



哈希 (Hash)

- 哈希又称“散列、杂凑”，它接收任何一组任意长度的输入信息，通过**哈希算法**转换成固定长度的数据输出形式，如字母和数字的组合，该输出就是“**哈希值**”。目前我们看到的比特币地址、以太坊地址都是哈希值。

哈希算法

- 某一类数学算法的统称，包括 MD5、SHA-1 和 SHA-2 等。SHA 是一个 Hash 函数族，分为 SHA-1、SHA-2、SHA-3，代表了三代哈希标准，比特币使用的 **SHA-256** 算法隶属于 SHA-2 系列。

哈希率

- 也是就我们平时所说的**算力**，它是指用于在**工作量证明** (PoW) 区块链上挖掘和处理交易的总计算能力，也可以理解成每秒处理数据的速度。

时间戳 (Time)

- 记录这个区块生成的时间，精确到秒。每诞生一个新的区块，就会被盖上相应的时间戳，这样就能保证整条链上的区块都按照时间顺序进行排列。

随机数

- 顾名思义，随机数就是区块链系统里随机生成的一个或一组数的序列，具有不可预测性、不可篡改性。所有**节点**共同参与计算这个随机数，谁先算出来，就拥有了区块打包权，可以获得奖励，这个过程就是**挖矿**。

默克尔根 (Merkle Root)

- 在区块主体中，所有交易信息先进行两个一组的哈希计算，这种结构叫做默克尔树 (Merkle Tree)。**默克尔树**逐层计算哈希值，并沿着路径层层传导至树根的位置，最终得出的主哈希值，也就是默克尔根。

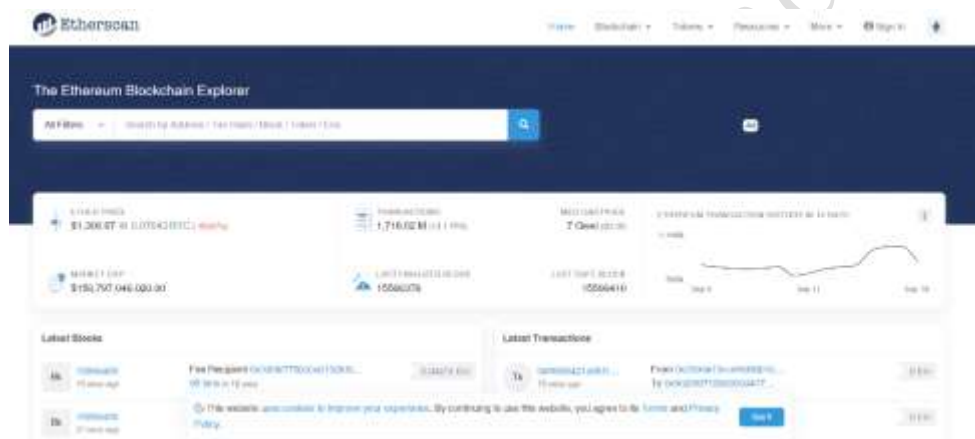


非对称加密

- 指的是加密和解密使用不同的密钥，两者不对称，故称之为非对称加密。其中**公钥**(Public Key)用作加密，**私钥**(Private Key)则用作解密。公钥可以公开与发布，私钥不可以公开，必须由用户自行严格秘密保管。

区块浏览器 (Scan)

- 区块浏览器并不是一个浏览器软件，只是提供用户浏览与查询区块链所有信息的网站，比如搜索链上交易记录，区块高度、区块数据、Token 信息等等。不同的区块链项目，需要使用不同的浏览器。



以太坊浏览器

节点

- 节点指的是区块链网络中的计算机客户端，比如电脑、矿机和服务器等等。这些节点会打包区块、广播交易信息、存储区块链的**数据副本**，并与其他节点共享信息。不同的区块链对节点的要求不同，一般需要有较高的计算资源。

图灵完备

- 图灵完备是指一台机器，只要有足够的时间和内存以及必要的指令，理想状态下就可以解决任何计算问题，无论多么复杂。一个例子是以太坊虚拟机 (EVM)。

区块链挖矿

挖矿 (Mining)

- 矿工利用电脑或矿机的算力,经过大量的计算(或称“哈希碰撞”),试出一个正确的区块哈希值,进而得到区块打包权(记账权),从而获得区块奖励(加密货币)。

矿工

- 进行挖矿工作的人被称为矿工。在比特币网络,大约每 10 分钟,全网矿工一起进行哈希碰撞,谁先算出随机数,就相当于挖到了这个区块,他便能获得系统新产出的比特币奖励。

矿机

- 矿机是指通过运行大量运算争夺记账权从而获得加密奖励的专业设备,一般由挖矿芯片、散热片、风扇、电源等原件组成。早期挖矿主要是用电脑 CPU,之后有公司发明了基于挖矿芯片(ASIC 芯片)的专业挖矿设备。嘉楠科技、比特大陆等是业内规模较大的矿机制造商。

矿场

- 矿场是集中管理矿机的场所,一般选址在电费相对便宜并且地理偏远的地方,如四川、新疆等地。2021 年 9 月十一部门联合发文整治后,矿场在国内基本清退。



某比特币矿场



矿池

- 随着参与挖矿的人数越来越多，单个设备或少量的算力难以获得奖励。矿池把全球零散的矿工与矿场集合起来化为一个整体，去全网竞争区块打包权，然后根据矿工提供的算力按比例分配奖励。出名的矿池有：蚂蚁矿池、鱼池等。

挖矿算力

- 算力也叫哈希率，单位是 hash/s。单个设备在每秒钟能够做到几次的哈希碰撞，就是该设备的算力。所谓“竞争区块打包权”，实际上就是不断地进行哈希碰撞得到正确的随机数。算力越高，得到正确结果的概率越大。

挖矿难度

- 简单来说就是算出正确结果的时间。矿工、矿机越多，挖矿难度越大。比特币网络会在大约 2 周左右进行一次难度调整，以确保矿工挖掘新区块的时间尽可能地接近 10 分钟的平均值。

CPU

- 即中央处理器，是一台计算机的运算和控制核心。只是 CPU 结构中包含一些对于挖矿并无帮助的模块，同时也不擅长并行运算（即重复性的工作），因此并不适合用作挖矿。

GPU

- 俗称显卡，是一种专门在个人电脑、游戏机和一些手机上进行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 会更适用于某些加密货币的挖矿。

ASIC

- 即专用集成电路，为某种目的而设计的集成电路。ASIC 挖矿芯片，是一种专门定制和设计、只用于完成比特币挖矿算法的芯片，其成本和功耗远低于 CPU、GPU，但是算力比同时代的 CPU、GPU 高出几万倍甚至更多。



认识公链

区块链技术是实现 Web3 的核心技术,而得以体现其核心价值的直接载体就是公链。公链对于催化 Dapp 开发, DeFi 热潮和 Web3 革命, 始终以中流砥柱的角色存在, 它是各类 Web3 构建得以进行和运转的必要条件。

和带有封闭性的私有链、联盟链完全不同, 公链作为一个任何人都可以自由加入的网络, 要打造的是完全可接入万事万物的庞大生态, 是类似于安卓、IOS 操作系统的存在。因此, 认识和了解公链, 对于我们解读 Web3 有重要作用。

公链的类型

王者级公链

- 价值认同远超其他公链、用户规模远超其他公链、TVL 远超其他公链、生态应用远超其他公链、市值排名第一的公链, 就可以称之为王者级公链。
- 代表项目: 以太坊 (ETH)

古典型公链

- 在 2017 年或更早之前就推出的公链, 由于没有及时转型或 Web3 生态建设不够、运行动力不足, 以至于不被大多数人认知的公链。
- 代表项目: Tezos、Cardano

高性能公链

- 近两年来推出的、为改进以太坊吞吐量不足而上线的公链, 主要特点是: 高 TPS、低 Gas 费、技术扎实、有一定的生态布局, 堪称二线公链。
- 代表项目: Solana、Avalanche、Near



模块化公链

- 将公链的技术、应用、规则和标准进行模块化，便于不同的项目开发者根据个性化需求匹配处理方案。该类公链的节点只专注于某一个模块，例如只专注于做交易执行，或者只专注于网络共识。
- 代表项目：Assembly、Celestia

垂直型公链

- 专注于为某一赛道提供底层基础设施的垂类公链，通过技术深耕和生态布局在一领域内占据领先地位，其成长天花板取决于该领域的市场规模。
- 代表项目：NFT 公链 Flow、隐私公链 Mina

跨链型公链

- 由于区块链上传递的价值和信息都仅局限于该条链，链与链之间如同孤岛。跨链型公链旨在让链和链之间可以互联互通，以实现互操作性和生态发展的可组合性。
- 代表项目：波卡（Polkadot）、Cosmos

侧链型公链

- 侧链也是一种公链，其目的在于解决原生公链（主链）的扩容问题。侧链与主链并行运行，是独立的一条链，以双向挂钩的形式与主链连接。
- 代表项目：Polygon（以太坊侧链）

古典型	成立时间较早，运行动力不足	Tezos, CARDANO, eosio
高性能	主攻高TPS, 低Gas费	SOLANA, NEAR, APTOS, sui
模块化	性能完备具有可组合性	assembly, CELESTIA, EEM.IT
专用型	专注NFT/隐私/元宇宙某一赛道	flow, MINA, ImmutableX
跨链型	实现跨链互操作和业务生态发展的可组合性	Polkadot, COSMOS
侧链型	解决原链的扩容问题，侧链也是一种跨链方案，影响较大因此单独分类	polygon, B

公链的广义分类（来源：LDcapital）



共识机制

共识算法

- 区块链网络中，节点达成并维护某种共识的方式，就是共识机制，或称为“**共识算法**”。比如在公司董事会做决策的时候，大家普遍的共识是“股份多的人投票权大”。在区块链中也一样，谁能拥有更大的记账权力呢？区块链各节点就这个问题需要达成共识。如果不同意，就会引发**分叉**。

分类			举例
不能容忍拜占庭错误	Paxos, RAFT		
能容忍拜占庭错误	间接形成共识（竞争记账权）	PoW	BTC
		传统 PoS	Nextcoin
		PoW+PoS 混合共识	Casper FFG
		PoA	Decred
		改进的 PoS	PoSV
		PoSV	Reddcoin
		Ouroboros	Cardano
	其他	PoST, PoBurn 等	IPFS 等
	直接形成共识	基于拜占庭容错	pBFT
		基于联邦拜占庭协议	瑞波共识机制
		恒星共识机制	Ripple
	通过选举间接形成共识	早期 DPoS	Bitshares
		验证人直接形成共识	DPoS+BFT, DBFT
	直接对交易形成共识	DAG 类共识	Tangle
			IOTA

主流共识机制（来源：通证研究院）

工作量证明（POW）

- 就是用工作量结果来证明贡献大小，再根据贡献大小确定**记账权**（区块打包权）和奖励。简单来说就是多劳多得。比特币网络使用的就是 POW 机制，谁的**算力**大，理论上谁获得奖励就越多。POW 的优点是：完全**去中心化**、安全性极高，但交易缓慢，且容易引发能源浪费。
- 代表项目：比特币、以太经典（ETC）

权益证明（POS）

- 拥有越多权益，就可以获得更大的记账权。这里的权益是指你持有的代币的数量和时间，即**币龄**（币龄=持币数*持币时间）越大权益越大，也就有更大的记账权。POS 的优点是吞吐量大、节省能源。不够去中心化，持币大户造成垄断。
- 代表项目：ETH2.0、Cardano



委托权益证明 (DPOS)

- DPOS 是在 POS 基础上优化而来的，类似于董事会投票。持币者投出一定数量的节点，由节点选择 **代理人**，代理他们进行验证和记账。简而言之，就是将自己的币委托给别人。其优点是效率高、吞吐量更大，但去中心化程度也更低。
- 代表项目：EOS

重要性证明 (POI)

- 根据账户的重要性评分来分配记账权的概率，重要性越大，记账权越大。
- 代表项目：NEW

权威证明 (POA)

- 部分权威的节点账户享有记账权，这些账户是其他节点获取真相的权威。POA 具有较高的吞吐量，并针对专用网络进行了优化。由于 POA 过于中心化，公链一般不会采用这种机制，大多用于 **私有链** 或 **联盟链**。

实用拜占庭容错 (PBFT)

- 基于拜占庭容错 (BFT) 的共识机制，一个节点代表一票，选择大多数的结果作为解决办法，即少数服从多数。PBFT 将 **容错量** 控制在全部节点数的 1/3，即只要有超过 2/3 的正常节点，整个系统便可正常运作。
- 代表项目：Zilliqa (PBFT+POW 的混合共识机制)

有向无环图(DAG)

- DAG 是 **非区块链** 形式的一种分布式账本技术。“有向”指有方向，准确的说应该是同一个方向，“无环”则指够不成闭环。在 **DAG** 中，没有区块的概念，他的组成单元是一笔笔的交易，每个单元记录的是单个用户的交易，这样就省去了打包出块的时间。该结构的特点在于：交易速度快、无手续费。
- 代表项目：IOTA、Fantom、Conflux



其他共识机制

共识机制是每个公链的灵魂，以下这些机制，大多都是基于上述共识进行了组合、更新与改变。

- Comsos 机制：Tendermint Core
- Algorand 机制：PPOS（纯权益证明机制）
- IOST 机制：POB（置信度证明机制）
- Elrond 机制：SPOS（安全权益证明机制）
- Ripple 机制：FBA（联邦拜占庭协议）
- Helium 机制：POC（容量证明机制）
- Filecoin 机制：POSt（时空证明）+ PORep（复制证明）的混合机制
- BSC 机制：POSA（权威权益证明）

扩容方案

每一条区块链，都面临着由去中心化、安全性、可扩展性组成的不可能三角。其中，去中心化是区块链技术最大的优势，需要优先保障。而若是想建立长久、可持续的生态，安全性也是不得不做到极致的要素。这就造成了当前公链可扩展性普遍较低。

以 ETH 为例，随着使用人数的不断增加，导致区块链时常会出现交易缓慢、gas 费高等问题（拥堵）。因此，提升区块链的吞吐量=扩容，是亟需解决的问题。目前市场上有多种扩容方案，包括推出新的高性能公链，或研究侧链，或改变自身的共识机制等。

Layer0

- 简称 L0，指的就是区块链最基础的底层协议，负责基础的数据传递及建立共识达成效率，相当于手机软件的开发语言。Layer0 公链旨在通过跨链的方式实现扩容。
- 代表项目：波卡（Polkadot）、Cosmos、雪崩协议（Avalanche）



Layer1

- 简称 L1, 主要是执行各类智能合约协议和 DAPP 的公链, 相当于手机上的安卓或苹果系统。Layer1 的扩容大多是优化自身的共识结构, 即链上扩容。
- 代表项目: ETH2.0、BSC (BNB Chain)

Layer2

- 简称 L2, 是建立在 Layer1 公链之上, 以优化交易速度和计算的第二层区块链网络。Layer2 的扩容也叫链下扩容, 即 Layer1 做好去中心化和安全, Layer2 提高效率。
- 代表项目: Optimism、ZKsync

Layer3

- 简称 L3, 并不是扩容方案, 只是在 L1 或 L2 链之上运行的应用层, 是作为消费者实际使用的平台 (例如各类 DAPP)。
- 代表项目: Uniswap、OpenSea

Layer 4

- 简称 L4, 是专注在用户与区块链之间的交互、帮助用户使用 L3 应用的工具, 主要组件是 API、UI、插件等等。
- 代表项目: Metamask (钱包)、Brave (浏览器)

Rollups

- 主流的 Layer2 扩容方案, 其做法是在以太坊主链之外搭建一条兼容以太坊的平台 (Layer2 链), 然后所有的人在 Layer2 上交易, 最后将交易打包存回以太坊上。Rollups 有两种方式: Optimistic Rollup (欺诈证明) 和 ZK rollup (零知识证明)。
- Optimistic Rollup 代表项目: Arbitrum、Optimism
- ZK Rollup 代表项目: zkSync、StarkWare



Plasma

- Plasma 是一种依赖于欺诈证明的扩容方案，数据可用性保存在链下，是以太坊最早的 Layer2 扩容方案，当前吸引力不强。
- 代表项目：早期的 OMG Network

Validium

- Validium 运行方式类似于 ZK rollup，不同之处在于数据被保存在链下。因为交易数据不是发布在区块链上的，所以有必要采用额外的信任假设，用户必须信任操作员，以便在需要时可以访问数据。
- 代表项目：DeversiFi

状态通道 (State channels)

- 状态通道是入门级的 Layer2 方案，比特币上的闪电网络就是一种状态通道。其设计思路是把一部分的交易放在区块链之外，把区块链的共识由确认每一步变成只确认结果，这样便减少了交易步骤提高了速度。
- 代表项目：Celer Network、Liquidity Network

侧链 (Sidechain)

- 是平行于主链的一个独立区块链，与主链兼容（例如 EVM），并通过跨链机制实现主链与侧链的资产交互，并在侧链运用，以分担主链的流量压力。
- 代表项目：XDai、Polygon（有争议）

分片 (Sharding)

- 典型的 Layer1 扩容方案，将区块链划分成若干个子网络(或称分片)，每一个分片都会包含一部分节点，网络中的交易会被随机分配到各个分片中做处理。这样便可以并行打包区块，提高效率。每个分片公链的分片方式有所不同，这里不做展开。
- 代表项目：NEAR（夜影协议）、Harmony、Elrond



侧链	Skale Network、xDai Stable、Injective Protocol
分片	Near、Harmony、Elrond、Zilliqa
状态通道	Celer Network、Raiden Network、Liquidity Network、Spankchain (基于 Connex)
Plasma	OMG Network、Matic Network、Loom Network
ZK Rollup	Loopring、zkSync、Aztec、Curve
Optimistic Rollup	Optimism、Synthetix、Unipig(uniswap v3)、Coinbase Wallet、Fuel Labs、IDEX、MCDEX
Validium	dYdX、DeversiFi

扩容方案总结

合约编程

EVM

- 以太坊虚拟机，ETH 链上的智能合约运行环境，用来处理智能合约的部署和执行。其他公链可通过兼容 EVM 虚拟机，实现 DAPP 的轻松迁移，这类公链也叫“EVM 兼容链”。BSC、HECO、Avalanche 等公链均兼容 EVM。

Javascript 语言

- Web2 世界非常流行的一门高级编程语言，入门难度较低，支持函数式编程。
- 应用场景：NEO 链

Solidity 语言

- Solidity 是一门面向智能合约的静态类型语言，语法接近于 Javascript，易于被掌握和使用。它是为 EVM（以太坊虚拟机）而生的，是智能合约开发的主要编程语言。
- 应用场景：ETH 链、兼容 EVM 链



Rust 语言

- 一种系统级、强类型的编译型编程语言，专注于安全，尤其是开发安全，支持函数式和命令式以及泛型等编程范式的多范式语言。
- 应用场景：Solana、NEAR、Polkadot

Go 语言

- 全称是 Golang，当今最好的区块链编程语言之一，具有简单易读的语法和快速的编译时间。
- 应用场景：Polygon SDK、Cosmos 链

C++语言

- 最古老的通用编程语言之一，也被许多世界著名的项目用作区块链编码语言，中本聪曾用其创建了比特币。
- 应用场景：Ripple 网络、EOS 链、Stellar 链

Move 语言

- 是 Meta(原 Facebook)为其稳定币项目 Diem(原 Libra)开发的编程语言，被誉为最适合编写区块链智能合约的语言之一。
- 应用场景：Aptos 链、Sui 链

OpenZeppelin

- OpenZeppelin 是一个以太坊智能合约开发代码库，这些合约代码经过了大量的测试和安全审查，可以有效提高开发效率

测试网

- 这是一种模拟主网生态环境的网络，开发者可以使用测试网对尚未部署的智能合约进行功能测试，以此来发现问题并修复错误。



测试币

- 可免费领取的测试网代币，无实际价值。开发人员在测试项目阶段，测试币用以支付各种 gas 费、交互费，以此降低开发成本。

合约标准

ERC

- ERC 是 Ethereum Request for Comment 的缩写，即“以太坊征求意见”的意思，是以太坊开发者的协议提案。包含如：代币标准合约（ERC-20），域名注册（ERC-137），URI 方案（ERC-681），库/包格式（EIP190）和钱包格式（EIP-8）等。

ERC-20

- 基于以太坊的一种同质化代币标准，由 V 神于 2015 年提出。比如 ETH，你手里的 1 个 ETH 和我手里的 1 个 ETH 可以互换，这就是同质化代币。基于该标准创建的代币，都是同质化代币。

ERC-721

- 最早诞生的非同质化代币（NFT）标准。NFT 代表的是独特性资产，每一个 NFT 都是独一无二的，具有不可分割性和唯一性，这就是非同质化。基于该标准铸造的 NFT，都是非同质化的。

ERC-1155

- 融合了同质化代币和非同质化代币的标准，在同一个智能合约中，两个标准的代币可以互转。该标准支持开发者创建海量的物品，每个物品可以是 ERC-721 那样独立的，也可以像 ERC-20 一样同质化。

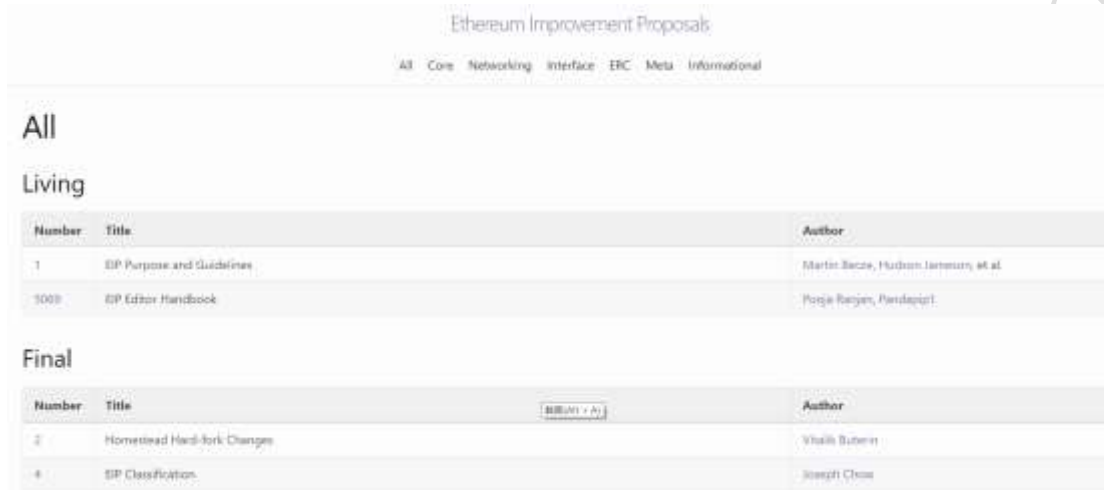
ERC-998

- 指的是可组合非同质化代币（CNFT），即一个 CNFT 可以包含多个 NFT 和 ERC20 代币，转账一次就能打包所有不同的 Token。例如一只猫咪作为 CNFT，其耳朵、鼻子、眼睛、颜色、尾巴都算是不同的 NFT。



EIP-XXX

- EIP 是 Ethereum Improvement Proposal 的缩写，代表以太坊改进优化提案。提案一般包括含有技术规范的设计文档与设计逻辑，为以太坊社区建言献策。例如 EIP-1559 提案，就改进了以太坊 gas 费收取标准。



The screenshot shows the Ethereum Improvement Proposals (EIP) website. It features a navigation bar with links: All, Core, Networking, Interface, ERC, Meta, and Informational. Below the navigation bar, there are three sections: 'All', 'Living', and 'Final'. Each section contains a table of proposals. The 'Living' section shows two proposals: EIP-1 (EIP Purpose and Guidelines) by Martin Becze, Hudson Jameson, et al., and EIP-1559 (EIP Editor Handbook) by Pongja Rongjan, Paragajit. The 'Final' section shows two proposals: EIP-1559 (Homestead Hard-fork Changes) by Vitalik Buterin, and EIP-1559 (EIP Classification) by Joseph Chou.

Number	Title	Author
1	EIP Purpose and Guidelines	Martin Becze, Hudson Jameson, et al.
1559	EIP Editor Handbook	Pongja Rongjan, Paragajit

Number	Title	Author
1559	Homestead Hard-fork Changes	Vitalik Buterin
1559	EIP Classification	Joseph Chou

EIP 提案社区

BEP20 和 BEP721

- 分别是基于币安智能链（BSC）的同质化代币标准和非同质化代币（NFT）标准。

TRC-20 与 TRC-721

- 分别是基于波场网络（TRON）的同质化代币标准和非同质化代币（NFT）标准。

HRC-20 和 HRC-721

- 分别是基于火币智能链（HECO）的同质化代币标准和非同质化代币（NFT）标准。

KIP-20 和 KIP-721

- 分别是基于 OKC 公链的同质化代币标准和非同质化代币（NFT）标准。



认识 Defi

去中心化金融（英语：Decentralized finance，俗称 DeFi）是一种建立于区块链上的金融体系。它不依赖券商、中心化交易所或银行等金融机构提供金融工具，而是利用区块链上的智能合约进行点对点金融活动。

迄今为止，DeFi 的创新金融应用是目前 Web3 领域最引人注目的发展。DeFi 让个人可以访问传统金融的所有服务（投资、保险、交换、借贷和借贷），而不需要金融机构或中介机构介入，从而在金融领域践行着 Web3 的使命和意义。

基础概念

Defi 协议

- Defi 协议是为用户提供各种去中心化金融服务的平台，该类平台利用了区块链的去中心化技术特征，同时使用 DAO（去中心化组织）进行治理，类型上包括借贷协议、稳定币协议、交易协议、跨链协议等。

Defi Summer

- 也叫 Defi 之夏，指的是 2020 年夏天。当年那个夏天，各类 DeFi 项目和用户量实现爆发式增长激增，这种繁荣的盛况被加密爱好者称为 "DeFi 之夏"。

流动性资金池（Liquidity Pool）

- 锁定在智能合约中的加密货币交易对。用户在 DEX 平台按照某种比例添加两种代币作为交易对（如 ETH-USDT），就形成了流动性资金池。其他用户便可以用 USDT 与资金池进行交易换取 ETH，整个交易基于 AMM 机制。



自动做市商 (AMM)

- AMM 是一种交易机制, 允许用户在**无需对手方**的情况下直接与流动性资金池池进行交易, 其**定价算法**会自动计算出交易价格。如果不好理解, 可以把它简单想象成一个自动化交易机器人。

收益耕作 (Yield Farming)

- 用户试图通过不同的 DeFi **协议**来实现资本回报率最大化的方式。我们把这些投资者称为**"收益农民"** (Yield farmers), 把收益率机会称为 **"农场"**。许多收益农民不断轮换他们的农场, 以寻找最高收益率的机会。

总锁仓价值 (TVL)

- TVL 全名 Total Value Locked, 泛指一个 DeFi 平台 (或一条公链) 中用户所抵押、质押、**被锁定的**加密资产总价值, 通常以美元为单位。TVL 是用来衡量 Defi 生态发展潜力的指标之一。

年度收益率 (APY)

- APY 采用复利计算, 它衡量用户将资金存入不同的 Defi 借贷和收益农场时的回报率。

流动性提供者 (LP)

- 向流动性资金池中添加交易对 (流动性) 的用户, 称之为 LP。LP 会获得其他用户的交易手续费作为奖励。LP 在添加流动性后会获得**凭证代币** (LP Token), 该凭证可以转移、**销毁**、锁定。

锁池

- LP 将自己的 LP 凭证代币转移至其他智能合约锁定的过程, 就是锁池。锁池期间, LP 将无法撤出自己所拥有的流动性。若 LP 凭证代币转移至**黑洞**, 将永远无法撤出。

权限销毁

- 代币合约发行方将合约权限转让至**黑洞**, 即被视为权限销毁。



拉黑

- 代币合约发行方利用智能合约权限，将某一用户的钱包地址拉入**黑名单**，使其无法使用该代币进行买卖和转账。

合约开源

- 代币或者 DAPP 项目方，将合约代码完全公布在链上，就意味着该智能合约已经开源。任何用户或机构都可自行复制、审查开源的代码，防止项目方作恶。

滑点 (Slippage)

- 在 **DEX** 进行交易时，价格和最后成交价的**差额**比例就是滑点。滑点可以在交易时自行设置。流动性好的资金池，滑点相对较低。

貔貅盘

- 一种只能买入，无法卖出的币。项目方在智能合约中设定用户只能买入不能卖出，从而达到收割韭菜的目的。这类代币主要集中在**去中心化交易所**上。



某貔貅盘合约检测结果



Defi 应用

去中心化交易所 (DEX)

- DEX 可以让用户快速实现代币的现货交易而无需中介机构。和币安等中心化交易所不同, DEX 不会存储你的个人资产, 也不用账号、密码及 KYC。
- 代表项目: Uniswap、SushiSwap、PancakeSwap

去中心化稳定币

- 和 USDT 等中心化稳定币不同, 去中心化稳定币不存在现金抵押物, 是由加密资产超额抵押或铸造。如 Maker DAO 推出的去中心化稳定币 DAI, 旨在通过以区块链上的智能合约自动化系统将其价值保持在尽可能接近一美元的水平。
- 代表项目: DAI (戴)、LUSD

算法稳定币

- 和 DAI 这类超额抵押的稳定币又有所不同, 算法稳定币没有任何抵押品, 主要是依托一种供需算法机制来保证其价格维持在 1 美元。Terra 推出的 UST 本是算法稳定币的代表项目, 但是在 Luna 崩盘事件中已经实质性失败。由此可见, 算法稳定币项目风险较高, 并不成熟。

稳定币交易所

- 是 DEX 的一种类型, 专注于各类稳定币、锚定币 (WBTC 等) 交易的平台。和常规 DEX 相比, 该平台在进行大额稳定币交易时滑点更低、损失更小, 其流动性也更好。
- 代表项目: Curve

合成资产

- 合成资产是以加密资产作为担保品, 生成锚定现实世界的股票、债券、外汇等资产价格的代币, 以及反向代币 (做空)、指数代币等衍生品。
- 代表项目: Synthetix、Duet



聚合交易

- 一个 DeFi 生态系统中，通常不会只有一个 DEX，以太坊生态中就存在超过 20 个平台，这意味着资产的流动性会被分散在各地。[聚合交易平台](#)的功能，就是帮用户在各个平台捕捉最优惠的价格，并在一笔交易中完成，将滑点将至最低。
- 代表项目：1inch、Matcha

跨链桥

- 在多链并存的时代，跨链桥允许用户在不同公链之间转移不同标准（ERC-20/BEP-20 等）的加密代币。主流的跨链方式是在两条链上流通同一种代币，发生跨链时，在一条公链上销毁（锁定）代币，然后在另一条公链上铸造相同代币。（注：跨链桥本身有多种方式，这里不做展开介绍）
- 代表项目：AnySwap、cBridge

混币器

- 无差别地帮助匿名交易混淆其资金来源、目的地的平台就是混币器。混币器在接受各种加密资金后，将其[混合](#)在一起，再传送给各自的接受者，以达到混币的目的。
- 代表项目：Tornado Cash

去中心化衍生品

- 加密衍生品是一种基于标的资产的金融合约，比如[永续合约](#)使用户能够在没有到期日的期货合约上建立一个[杠杆头寸](#)。
- 代表项目：Perpetual、dYdX

去中心化借贷

- 借贷市场是 DeFi 领域相当重要的早期应用之一，用户可以通过在这些借贷平台存放闲置资金赚取被动收益，同时也能存入抵押品，借出加密资产进行融资与杠杆交易。
- 代表项目：Compound、AAVE

去中心化保险

- 面对高风险、高波动的加密市场，对 Defi 保险的需求开始增加。例如 Nexus Mutua 推出的智能合约保险产品，主要面向托管用户资金的 DeFi 协议，因为这些协议可能会由于智能合约的错误而遭受黑客攻击。Aave、Synthetix 都是其客户。
- 代表项目：Nexus Mutual、Cover

去中心化预测

- 让投资者对于未来的某件事进行押注的平台就是预测平台。但传统的平台（如菠菜平台）往往因为提款延迟和冻结账户等问题，使用户处劣势地位。去中心化预测平台利用区块链技术，具有抗审查性、无中介、无许可等优势。
- 代表项目：Augur、Polymarket

去中心化收益聚合器

- 俗称“机枪池”，其概念类似于传统金融中的基金，用户将加密资产存入平台的智能合约，由去中心化自治组织（DAO）负责管理，实现自动复投、自动转仓等功能，以获取最大的收益回报。
- 代表项目：Yearn finance（大姨夫）

Decentralized Finance (DeFi) Ecosystem



2022 年 Defi 生态图谱



认识元宇宙

元宇宙（Metaverse）所要打造的未来很好理解，就是利用技术将现实世界的各种内容都可以投射平行宇宙中，使用户以数字人的身份沉浸其中，进行社交、游戏、创作等一系列虚拟活动。达到这一目的，需要区块链、网络算力和虚拟现实技术的支持。

但是有了技术还不够，元宇宙内必须有经济活动才能运作，作为价值元素的 NFT 将成为元宇宙内的**权益媒介**。每一个 NFT 都是独一无二的，用户可以真正享受到 Web3.0 的独有数字所有权。这些 NFT 的互相交易能带来商业繁荣，而商业中的各种经济往来也使得元宇宙真正运转起来。

基础概念

非同质化代币（NFT）

- NFT 是基于区块链的数字资产形式，具有独特性和唯一性。范围非常广泛，比如艺术品、图片、音乐、视频，甚至一条微博都可以做成 NFT。在元宇宙中，NFT 能证明土地、角色等商品的**所有权**。

GameFi

- 全称 Game Finance,是在元宇宙中将 DeFi、NFT 和 P2E 链游结合后形成的新概念,即“**游戏化金融**”。游戏中的角色、物品、土地等，都以 NFT 的形式存在，可以被出售以获得加密货币。Axie Infinity 是知名的元宇宙游戏。

SocialFi

- SocialFi 将社交平台（Social）和金融（Finance）结合的**社交化金融**，让用户通过社群平台获得收益，即将自己的社交影响力金融化。在元宇宙中，SocialFi 保持了创作者经济的灵魂。Chilliz、ENJ 等均属 SocialFi 领域代表项目。



边玩边赚 (Play-to-Earn)

- 边玩边赚 (P2E) 是一些基于区块链的游戏所用的经济模型。在 P2E 游戏的虚拟经济中, 玩家可以通过玩游戏赚取 NFT 道具或加密货币。这些 NFT 和货币可以通过去中心化市场出售给他人。

虚拟现实 (VR)

- VR 是一种沉浸式体验, 人们戴上头戴设备, 能够看到数字世界并在其中操作。VR 目前使用的是全套头戴设备而不是眼镜, 让使用者沉浸在 360 度的虚拟世界中并能够在其中四处活动。

增强现实 (AR)

- AR 是一种将虚拟信息与真实世界巧妙融合的技术, 广泛运用于多媒体、三维建模等领域。该技术可以通过全息投影, 在镜片的显示屏幕中将虚拟世界与现实世界叠加, 操作者可以通过设备互动。

混合现实 (MR)

- MR 包含了 VR 和 AR 的元素, 但其确切定义是模糊的。人们可以与虚拟和现实世界的事物互动, 而虚拟事物也可以与现实世界的事物互动。

扩展现实 (XR)

- 扩展现实是 VR、AR、MR 等经常相互重叠的概念的统称。最终, 随着“元宇宙”成为现实, VR、AR 和 MR 之间的界线可能会变得模糊, 使 XR 成为一个更合适的称谓。

镜像世界 (Mirrorworld)

- 镜像世界是现实世界的数字版本, 现实生活中的人、地方和事物在那里都有对应的虚拟形态。

角色化身 (Avatar)

- 化身是你在虚拟世界中的人物角色。这种以数字方式呈现的你可能看起来很像你, 也可能像是一个卡通形象。



数字孪生 (Digital twin)

- 数字孪生是现实生活中的事物或结构的虚拟版本，其技术在 2010 年首次被美国国家航空航天局用于进行太空舱模拟实验。[微软](#)公司特别强调了数字孪生技术对于构建“元宇宙”的必要性。

脑机接口 (BCI)

- 脑机接口是在人脑与计算机或其他电子设备之间建立直接交流和控制通路，用户可[通过大脑](#)直接表达想法或操纵设备，无需借助语言、手势或其他工具。

NFT 与数藏

铸造 (Mint)

- 艺术家或收藏者最初在区块链上发行 NFT 的行为。当你从发行方手中购入一枚全新的 NFT 时，也表明你这个收藏者正在 Minting（铸造）这一 NFT。

地板价 (Floor Price)

- 意指一个 NFT 系列在 [OpenSea](#)、[Larvalabs](#) 等交易平台上的最低成交价格，是收藏者在评估项目时最广泛使用的指标之一。

PFP

- 全称 profile picture，原意是社交媒体个人资料图片，是 NFT 的类别之一，通常称之为[头像图片类 NFT](#)。[CryptoPunks](#) 是最知名的 PFP 类 NFT。

加密朋克 (CryptoPunks)

- [CryptoPunks](#) 是世界上第一个 NFT 项目，包括 10000 个[像素](#)头像，每个头像都是 24x24 像素、8bit 样式。其中一个头像曾在 2021 年于苏富比拍卖行以 1170 多万美元的价格售出。

无聊猿 (BAYC)

- 全称是“无聊猿游艇俱乐部”，是最昂贵和最具影响力的 NFT 系列之一。除了海外明星之外，国内的李宁、绿地集团等品牌都曾购入无聊猿 NFT 以开展合作。



无聊猿系列 NFT

加密猫 (CryptoKitties)

- 也叫迷恋猫，是 2017 年上线的区块链游戏，开创了以太坊 ERC-721 这个 NFT 通用标准。自此以后，NFT 大行其道。

福洛 (FLOW)

- 加密猫团队开发的一条 POS 型公链，其最大目标是帮游戏及 NFT 相关应用打造一条专属区块链。NBA Top Shot、加密猫等知名 NFT 项目均在 FLOW 上运行。

OS

- 是 OpenSea 的简写，OpenSea 是当前最有知名度的 NFT 交易市场之一。



数字藏品

- 简称数藏，是指使用区块链技术，对应特定的作品、艺术品生成的唯一数字凭证。需要注意的是，国内的数藏与真正意义上的 NFT 有很大区别。

台子

- 数字藏品的发布平台，如鲸探、新华数藏等。新平台称作新台子。

创世

- 指新上线数藏平台首次发售的藏品。

蓝筹

- 指被较多人认可未来将保持高价的优质藏品，但同时风险亦不容忽视。

合成

- 平台发起的活动玩法，可将多个藏品合成一个全新藏品，合成后原藏品会被销毁，通常新藏品价格会更高。

打榜

- 通过完成平台任务，如合成藏品数量、拉新等，平台进行排名，并进行奖励等。

抢购

- 对于平台限量发行的藏品，需进行抢购获得，形式如顺序抢购、抽签抢购等。

转增

- 根据平台规则，将藏品赠送给别人。比如鲸探平台要求购买藏品半年后，方可转增。



二级市场/流转中心

- 简单来讲就是买家与卖家之间互相流通买卖藏品的平台。抢官方发售的叫一级，玩家之间买卖就是二级了。该市场需根据监管政策完善资质，用户需**谨慎分辨**。

盲盒

- 和平时玩的盲盒概念一样，在开盲盒之前玩家并不知道里面是什么样的藏品有多大的价值，一切全靠运气。

破发

- 与股票破发的意思一样，指的是藏品目前市场价格已经低于当初平台的发行价格，这个时候你基本属于是被割韭菜了。

版税

- 在部分二级交易平台上买卖一个数字藏品都有两笔额外费用，即交易手续费和版税。交易手续费由数藏交易平台收取，版税由项目方/创作者收取。

序号	平台名称	主体公司	上线类型	上线名称	是否支持二级交易	平台亮点
1	ibox	海南易鑫科技有限公司	联票请	首次请	是	首创发行、盲盒发行、多形式数字藏品发行等多样发行方式。首创将数字藏品《每其他第三平台》首次数字藏品交易。
2	众数客	湖南元图文化科技有限公司	联票请	首次请	是	多家上市公司控股。2019年7月1日上线。
3	唯一艺术	唯艺（杭州）数字技术有限公司	公链	以太坊	是	唯一艺术目前推出部分数字藏品发行并认证新藏品2022年，区块链P2P交易。
4	FiguresLab	墨图科技（北京）有限公司	-	-	-	-
5	藏数圈	北京元图文化科技有限公司	-	-	-	-
6	数藏文化	深圳数藏文化科技有限公司	联票请	数藏圈	是	-
7	数藏	江西数藏科技有限公司	联票请	数藏圈	是	-
8	FiguresLab	杭州墨图科技有限公司	公链	以太坊	是	FiguresLab成立于2022年7月
9	artStation	杭州元图文化科技有限公司	公链	polymex	是	art Station平台在2022年11月28日内上线。
10	数藏	杭州数藏网络科技有限公司	联票请	数藏圈	是	2022年1月21日上线数藏交易平台上线。
11	数藏数字	江西数藏网络科技有限公司	联票请	数藏圈	是	-
12	唯一艺术	深圳唯艺文化、艺三网	联票请	数藏圈	-	-
13	数藏	武汉数藏科技有限公司	联票请	数藏圈	是	-
14	数藏	武汉数藏科技有限公司	公链	以太坊	是	-
15	数藏	湖北数藏网络科技有限公司	公链	polymex	是	-
16	数藏艺术	江西数藏网络科技有限公司	公链	以太坊	是	-
17	Metaverse	北京元图文化科技有限公司	公链	以太坊	是	Metaverse元宇宙平台（数藏圈）支持自创数字藏品。用户可通过发行、盲盒发行、多形式数字藏品等方式进行资产交易。
18	数藏	深圳数藏网络科技有限公司	公链	以太坊	是	-
19	数藏	深圳数藏网络科技有限公司	公链	以太坊	是	数藏艺术平台
20	数藏	上海数藏网络科技有限公司	公链	以太坊	是	-
21	数藏艺术	深圳数藏网络科技有限公司	公链	以太坊	是	-
22	数藏	海南数藏网络科技有限公司	联票请	天网请	是	-
23	数藏	海南数藏网络科技有限公司	公链	以太坊	是	-
24	数藏	海口数藏网络科技有限公司	公链	polymex	是	-
25	数藏	北京数藏网络科技有限公司	公链	polymex	是	-
26	数藏	海南数藏网络科技有限公司	公链	Cooperation Network	是	-
27	数藏	上海数藏网络科技有限公司	联票请	天网请	是	-
28	数藏	海南数藏网络科技有限公司	联票请	天网请	是	ChinaCollect
29	数藏	北京数藏网络科技有限公司	公链	Gasik (Blockchain)	是	-
30	数藏	深圳数藏网络科技有限公司	联票请	数藏圈	是	注册费100万
31	数藏	北京数藏网络科技有限公司	公链	以太坊	是	-
32	数藏	海南数藏网络科技有限公司	公链	以太坊	是	注册费200万

国内数藏平台盘点（来源：元力社）



认识交易投资市场

自比特币诞生的十多年以来，加密货币已成为诸多投资者获取更高利益回报的工具。加密货币投资作为 Web3 领域的重要经济活动，能给这个全新的领域带来活力、价值创新与增量。不管是项目方、个人，还是平台，都将由此获益。

然而加密货币的价格具有极高的波动性和风险性，以至于个人投资者以亏损居多，甚至于上当受骗者亦不计其数。我们无疑教导各位要投资加密货币，相反，我们反对任何无脑投资的行为。撰写此篇，仅作为信息补充，以扩充各位的知识面。

Token 发行市场

空投 (airdrop)

- 空投实际上是区块链项目将其本身的代币按照某一规则进行免费派发，以获取新的用户群体的过程。用户通常需要完成某些任务或者达到某些条件，才能领取空投。

水龙头

- 像空投一样，水龙头是一种分发和接收免费加密货币的方式。用户前往水龙头网页，输入钱包地址即可获得少量加密货币，以此提高加密货币的普及率。水龙头通常是有时间和供应量限制的。

众筹

- 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。

种子轮

- 也称基石轮，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。



天使轮

- 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，额度高于种子轮。

私募

- 私募广义上包含种子、天使以及 ICO 发行前的各个轮次融资，私募只对特定机构或投资人（PE）发行，并且无需对外公开。

公募

- 公募在区块链中一般是指 ICO 阶段，一般持续数十天，并且分为数个融资轮次。部分项目在进行公募时，会选择 Launchpad 平台。

ICO

- 俗称“爱西欧”，即首次代币发行，一种众筹资金的方式。指加密项目首次向公众发行代币，募集比特币、以太坊等主流币以获得项目运作的经费。目前国家明令禁止 ICO，建议大家不要参与任何 ICO 项目。

STO

- 即证券化代币发行，指的是利用区块链技术，在符合证券市场严格监管要求下，将私人公司的股份、房地产或知识产权等非流动性资产，在受监管情况下代币化并进行集资，并在交易所上市供投资者购买的行为。

IEO

- 即首次中心化交易所发行。中心化交易所（如币安）和项目方联合，在交易所直接向二级市场出认购额度，让高质量用户来认购，从而达到融资目的。此种项目说起来是比较靠谱，但是还得看项目方和交易所良心。



IDO

- 即首次去中心化交易所发行。项目方为 DEX 提供代币，用户在代币生成活动中锁定加密资产以换取新代币。DEX 将一部分筹集到的资金与新代币一起加入流动性资金池，其余还给项目方。

IGO

- 即首次游戏通证发行。区块链游戏项目方与 Launchpad 平台合作，参与者将锁定 Launchpad 平台代币进行申购。如果申购成功，便可提前获得游戏 Token 及 NFT，如皮肤、角色、武器等。运气好的话，当游戏上线之后直接转手卖掉，就能获得可观的收益。

Launchpad

- 中文称之为“启动版”或“发射台”，是一个帮助加密项目筹款的平台。它为投资者提供了在加密项目早期、公开上市之前进行投资的机会，可以使其以较便宜的价格购买代币。币安 Launchpad、UNICRYPT 等是知名 Launchpad 平台。

软顶 (Soft Cap)

- 软顶是项目方在 ICO 或 IDO 过程中所能获得的最低金额。在有限的时间内，如果募集到的资金没有达到软顶金额，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 ICO 或 IDO 过程中所能募集到的最大金额。

白名单 (White List)

- 简称 WL，指的是可以提前购买某种代币或者 NFT 的用户名单，这样你就可以不用在项目正式发售时，跟一大堆人“争抢”了。

AMA

- AMA 是 Ask Me Anything（问我什么都可以）的缩写，一般指加密项目在发行阶段时举行的问答活动，用户、观众可以询问任何相关的问题，主要是以文字或视频直播的形式举行。



■ 投资市场

中心化交易所 (CEX)

- 指的是以币安、FTX 为代表的传统交易所，集交易、券商和投资银行的功能为一体。优点是交易速度快、交易深度好，适合新手使用。缺点是过于中心化，资产由平台控制，存在一定风险，包括但不限于：交易所倒闭跑路、禁止提币、封禁账号、被黑客攻击等。

充值/提币

- 充值，指的是将加密货币从其他交易平台或钱包，转移至本交易所的行为。提币，就是将加密货币从本交易所转移至其他交易所或钱包的行为。

币币交易

- 也叫现货交易，主要是针对加密货币和加密货币之间的交易，以其中一种币作为计价单位去购买其他币种。普遍使用的计价币种是稳定币 USDT。

交易对

- 由两种不同的加密货币组成的‘成对的交易’，例如 BTC/USDT 这个交易对的意思是，你可以用 USDT 去购买 BTC。只有在 CEX 里存在某个交易对，才能进行两个代币之间的币币交易。

市价交易

- 即按照当前价格进行买入和卖出的交易，市价交易具有交易的优先权，如果你想更快完成交易，可以使用市价交易。

限价交易

- 也叫委托交易或者挂单交易，指的是按照一个指定的价格进行买入或者卖出的交易。如果未达到指定价格，则交易不能成功。



法币交易 (OTC)

- 也叫场外交易、OTC 交易、C2C 交易，简而言之就是使用法定货币（如美元）去购买加密货币，或将加密货币兑换成法币的交易方式。

杠杆交易

- 顾名思义，就是利用小额的资金撬动杠杆，来进行数倍于原始金额的投资，以期获得相对投资标的物波动的**数倍收益率**，抑或亏损。

合约交易

- 是指买卖双方对约定未来某个时间按指定价格接收一定数量的某种资产的协议进行交易。合约交易是一种金融衍生品，用户可以在交易中通过判断涨跌，选择**买入**做多或者卖出**做空**合约，来获得价格上涨或者下跌带来的收益。**风险太高**，不建议玩。

做多 (多头)

- 做多是指预期未来价格上涨，以较低价格买入一定数量的标的资产。等价格上涨后，高价卖出，从而赚取**差价利润**的交易行为。

做空 (空头)

- 与做多相对，做空是先向交易所借入标的资产，然后卖出获得资金。过一段时间之后，再买入标的资产归还，以此赚取利润。

敞口

- 是金融活动中存在金融风险的部分，似于开盘或仓位的概念，可以简单理解为投资者买入或卖出一种资产的行为。比如，当投资者购买了 1 万美元的 BTC，那么可以说，投资者拥有了 1 万美元 BTC 的敞口。



头寸

- 头寸是一种市场约定，承诺买卖合约的最初部位，买进合约者为多头，位于**盼涨**部位。卖出合约部位为空头，处于**盼跌**部位。

爆仓

- 用户在进行杠杆或者合约交易时，由于行情剧烈波动导致**保证金**被平台强制出售的情况。简单来说就是：本金亏没了，仓位“爆”了。



某用户爆仓情况

保证金

- 进行合约交易时，用户无需支付合约的总额，只需根据合约价格，按一定比率交纳少量资金作为履行合约的财力担保，便可参与交易。保证金越多，越不易引发**爆仓**。

搬砖 (Arbitrage)

- 从币价低的交易所买入加密货币，然后转到价格高的交易所卖掉，从而赚取差价。这类操作消耗大量时间和资金成本，同时也需要承担币价涨跌的风险。



套利

- 套利是指利用两个或多个市场的价格差异来获利的行为。套利通常包括一组**相互对应且买卖方向相反**的交易，以此将价差变成利润。

对冲 (Hedge)

- 对冲交易就是盈亏相抵的交易。具体而言，对冲交易就是指**同时**进行两笔行情相关、方向相反、数量相当、盈亏相抵的交易。

量化交易

- 量化交易是指利用统计学和数学的方法，并使用**计算机技术**进行交易的投资方式。“量化”便是指利用大量的数据，抓出数种能带来超额收益的交易策略。与人工交易相比，量化交易可以减少情绪波动的影响。

K 线图 (Candlestick Charts)

- 又称蜡烛图、棒线、红黑线等，常用说法是“K 线”。根据一段时间的开盘价、最高价、最低价、收盘价绘制而成，它是以每个分析周期分为日 k，周 K，月 K，年 K，最小单位到 1 分。

换手率

- 指在一定时间内市场中某个币种转手买卖的频率，是评价某个币种流动性的主要指标之一。

流通总量 (Circulating Supply)

- 也叫供应量，代表某个加密项目在市场上可自由交易的代币总数。

市值 (Market Cap)

- 当某一个代币上市交易之后在市场上的价值，目前比较流行的计算方式是**流通的市值**，即通过将其价格乘以其**流通总量**来计算的。



完全稀释市值 (FDV)

- 指的是当一个加密项目的代币完全流通之后的完全市值，每一个 Token 的流通规则不一，通常一个项目 2-3 年才会完全流通。完全稀释市值要比流通市值大。

CMC

- 特指国外的加密货币数据收录平台 CoinMarketCap，在该平台可以查看加密货币的价格、市值、流通量、持仓等数据。

CG

- 特指加密货币行情数据平台 CoinGecko，与 CMC 类似。

KYC

- KYC 是 Know Your Customer（了解你的客户）的首字母缩写，指一系列法律法规要求企业了解客户的身份（要求提供身份证扫描件或其他身份证件）。

反洗钱 (AML)

- 全称是 Anti-Money Laundering，代表反洗钱的政策和相关法律法规，这可以防止非法获得的资产被掩饰及合法化。

ATH (All Time High)

- 字面的意思就是“一直以来的最高点”。在加密里指的就是某个代币的**历史最高价格**，当一个币价格创新高时我们会这么说。

定投 (DCA)

- 利用同一个周期的方式（每天、或是每 6 个小时）固定金额买入同一个币种，长时间下来有助于降低买进一个币种的成本。



Web3.0 场景赛道

正如前言所述，Web3.0 的愿景是实现去中心化的网络系统，用户能够掌握自己的资产、身份、数据和隐私等权益的所有权。而这一概念具体又是如何落地的呢？它又是如何改变各个行业的呢？

简单来说，Web3 试图通过去中心化的网络重构价值，变革企业与开发者、用户的生产关系，以构建一个全新的商业模式。比如使用加密钱包取代账户注册、通过 DAO 替代企业管理等。通过对这些应用场景及基础设施的了解，相信你对 Web3 会有更加深刻的认识。

Web3 预言机 (Oracle)

- 预言机充当了链下数据和区块链之间的桥梁，将外部信息传递到区块链，以供链上生态系统中的智能合约或 Dapp 进行验证和执行。
- 代表项目：Chainlink

Web3 存储

- 由于中心化存储平台（如百度网盘等）容易受到审查且具有可变性，去中心化存储成为 Web3 最受关注的基础设施之一。去中心化存储平台将数据复制、分割存储在不同的位置，在任一节点都可下载访问。不仅减少了数据丢失的风险，而且能够有效进行数据确权 and 隐私保护。
- 代表项目：Filecoin、Arweave

Web3 组织形式 (DAO)

- 去中心化自治组织 (DAO) 是一种将管理和运营规则写入区块链智能合约上的组织。该组织的决策主要通过提案和投票来进行，没有 CEO 或董事会，任何人都有发言权。大多数 Defi 和 NFT 项目都是以 DAO 的形式来运作。
- 代表项目：BITDAO、MakerDAO



Web3 数据索引、查询

- 在区块链的浏览器里，我们可以轻松查询到某个代币的持有人和数量。但是哪个代币交易量更高、热度更高，分析起来就困难。数据索引平台允许用户创建 Web3 数据查询 API 以供开发者购买使用。
- 代表项目：The Graph

Web3 钱包

- 去中心化钱包不仅是区块链加密资产的“账户”，也是用户通往 Web3 世界（DeFi、DAPP）的“护照”，是用户真正实现独立掌握个人资产的核心基础。
- 代表项目：Metamask（小狐狸钱包）

Web3 云计算

- 在 Web2 世界里，诸如 AWS、谷歌云等服务平台因过于中心化而存在较大的风险。去中心化计算系统将连接世界各地的计算机，为 DAPP、公链开发者提供运算和存储服务。
- 代表项目：ICP

Web3 浏览器

- 在实现所有传统浏览器功能的基础上，Web3 浏览器提供了不一样的功能：拦截网站广告及跟踪器、内置加密钱包、Tor 匿名路由、用 Token 打赏网站及内容、与 IPFS 合作提供更快的加载速度、dApps 索引目录等。
- 代表项目：Brave、Opera

Web3 域名

- Web3 世界的域名并非指某个网站的网址，而是基于个人钱包地址的域名。以太坊为例，其钱包地址是一个 42 位的字符串，非常难记。去中心化域名服务可以把这个地址转换成以.eth 或者是.bit 为结尾的域名，这样好记又方便。
- 代表项目：ENS、BitDNS



Web3 身份系统 (DID)

- 传统的 Web2 身份认证体系, 存在容易被盗、流程繁琐、各平台账号信息相互隔离等问题。而 Web3 将用户和行为数据存储在链上, 不会被篡改。无论是个人信誉、金融借贷数据, 还是用户的加密资产、NFT、域名, 都可以集中到一个身份系统里, 以访问所有 Web3 应用。
- 代表项目: Project Galaxy

Web3 音乐平台

- 基于区块链及去中心化存储技术搭建的 Web3 音乐平台, 具有无中介、透明化的特点。智能合约让音乐收益的结算更加透明高效, 而音乐 NFT 又让音乐人有了全新的作品发行渠道和方式, 用户也能通过 [Listen to Earn](#) 的模式获得收益。
- 代表项目: Audio

Web3 云服务

- 与 Web2 云服务平台提供建站和托管服务类似, Web3 云服务平台可以提供节点快速部署、DAPP 创建、服务器出租等服务。企业也可将 DAPP、节点托管至该类平台。
- 代表项目: Ankr

Web3 招聘平台

- 和 Web2 招聘平台相比, Web3 招聘网络的去中心化属性更为明显: 1、更公平的收费结构(抽佣低)。
2、人才的链上声誉系统(免去背调)。3、以 DAO 的方式组织运营(避免集权)。4、引入代币经济(激励奖励)。
- 代表项目: Braintrust

Web3 社交

- 聊天内容加密处理、个人主页/聊天表情/特效 NFT 化、通过帖子/评论进行 Token 获利、基于个人 IP 创建粉丝代币等, 都是 Web3 社交平台的独特属性。
- 代表项目: Status、Deso。



去中心化流媒体

- 颠覆传统 CDN 服务器的模式，去中心化流媒体网络让每一个用户在观看视频的时候贡献自己的闲置算力和带宽资源。而用户自动从距离自己最近的缓存节点获取视频，这样既降低了成本，又提高了视频传输的速度和画质。用户越多，画质越好。
- 代表项：Theta

Web3 内容博客

- 都是博客，区别在哪？Web3 博客作者的创作内容存储在去中心化平台、通过 Web3 钱包连接登陆、绑定 ENS 域名、付费阅读的收益直接进入钱包地址、文章可做成 NFT 出售，且每一篇文章都会有所版权声明和验证链接，作者需使用密钥签名确认。
- 代表项目：Mirror、RSS3

去中心化解析服务

- 在 Web2 市场，上传视频或者直播视频的解析转码成本高居不下。去中心化视频转码网络通过区块链技术，利用视频矿工的闲置 GPU 和带宽资源来进行视频转码工作，从而降低转码成本。
- 代表项目：Livepeer

去中心化渲染服务

- 去中心化渲染网络允许大量个人或企业的闲置 GPU 资源接入网络供渲染需求者使用，以赚取代币奖励。以这种以分布式运行的渲染网络，成本仅为传统平台的十分之一。
- 代表项目：RNDR

去中心化物联网

- Web3 物联网系统允许个人或机构，通过硬件设施（类似于路由器）形成的热点集群来构成无线网络以供任何物联网设备的探寻和造访，以达到人人供网的分布式网络。此外，通过遍及全球的硬件对停车场、水电煤气表、家畜等各类物联网数据进行采集上链，供客户使用。
- 代表项目：Helium、MXC



附录：Web3 社群俚语

大饼

- 指的是比特币，其原因不可考证，有人认为是比特币的 logo 很像武大郎的大饼，也有人认为是为了防止敏感词被屏蔽，故而以大饼指代比特币。

披萨节

- 加密圈最重要的节日之一。2010 年 5 月 22 日，一位程序员用 10000 枚比特币购买了 2 块披萨，让比特币第一次有了价格。后来这一天就被定义为“比特币国际披萨日”。

中本聪

- 比特币发明者，自称是日裔美国人，英文原名 Satoshi Nakamoto。2008 年 10 月 31 日，发布比特币白皮书。2009 年 1 月 3 日，挖出比特币网络的创世区块。2010 年 12 月 21 日，在发表最后一篇文章后消失不见。其真实身份长期不为外界所知。

V 神

- 指的是以太坊创始人 Vitalik Buterin（维他利客·布特林），1994 年出生的少年天才，19 岁便发布了以太坊白皮书。

纸飞机 (TG)

- 也叫电报，是匿名社交软件 Telegram 的昵称。该软件注重用户的隐私保护，深受加密爱好者的喜爱。其 logo 形状像一个飞机，所以也叫纸飞机。

梯子

- 一种科学上网的方式，例如要使用 Telegram 就必须通过梯子。



巨鲸 (Whale)

- 指的是拥有大量资金进行加密投资，或拥有较多比特币、ETH 等加密资产的人或机构组织。

FOMO

- 全称即 Fear of Missing Out, 指害怕错失机会的情绪。它指的是当其他人都在谈论某种加密资产时，产生的购买该类资产的紧迫感。

FUD

- 字面意思就是恐惧，不确定和怀疑。意指散播负面的消息去影响投资者，使他们感受到害怕和不确定，进而透过这种方式去影响行情。

长期持有 (HODL)

- 无论价格如何波动，都持续持有自己的加密资产，永不动摇。

登月 (To The Moon)

- 相信某种加密资产价格将在未来出现大幅飙升，价格登上月球。

聪 (Sats)

- 全称是 satoshis, 是比特币的最小单位。一聪相当于 0.00000001 BTC。

CX

- 传销的缩写，在区块链圈子里特指疯狂宣传、疯狂推荐的意思。假如你买个某个币，记得去 cx 它。

博饼

- 特指币安智能链 (BSC) 上的去中心化交易所 PancakeSwap



画门

- 某种加密资产价格猛地拉起老高，横了一阵子，又开始暴跌，K 线图像一座门。

插针

- 是加密货币的价格在某一个瞬间突然拉高或拉低，然后又迅速回落到原来的位置，可能持续时间不过几秒钟，在 K 线上留下一根很长的向上或者向下的影线，就像一根针

拉电闸

- 极端行情下，交易所出现宕机，导致用户无法交易或平仓，以此带来了巨大的损失。这种宕机的情况，被用户讽刺为交易所拉了电闸。

夹子机器人

- 也叫自动套利机器人，可以实时检测 DEX 上面所有的交易，发现一定金额以上的交易时，会通过提高 Gas 费在购买者之前提前买入，然后等他的买入成功抬高价格后，再自动卖出获利。

钻石手 (Diamond hands)

- 指即使面临巨大的售出压力，也坚持持有加密资产的人，与 HOLD 相似。

纸手 (paper hands)

- 纸手则是指过早抛售的投资者——这种行为主要是由于害怕风险并且容易恐慌。



BlockWeeks 区块周刊: <https://blockweeks.com/>

PandaTool 熊猫工具: <https://www.pandatool.org/>