基础知识

一级市场，也称发行市场或初级市场，相对二级市场来讲的。币圈通俗理解就是上交易所之前的市场，一级市场可以用最低的价格买到项目方代币Token，等项目代币上线交易所后拉盘升值达到一定收益即出货，以最低的成本换取最大化的利润。理论上一般的项目会经过种子轮、私募轮、公募轮，每一轮价格递增，成倍价差也属常见，特别是项目种子轮价格也是非常低的。项目代币上线交易所后，即二级市场，此时一
级市场与二级市场价差
极为明显，再来了解一下二级市场，传统金融
对二级市场的解释是有价证券的交易场所、流通市场，是发行的有价证券进行买卖交易的场所。币圈二级市场通常指的是交易所，通俗说的炒币就是指二级市场交易
。

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

协议分类账(Agreement ledger
)是由两方或多方用来协商和达成协议的分布式分类账。

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

认证分类账(Attestation Ledgers)是分类账，提供持久的协议，承诺或声明记录，提供证据(证明)这些协议，承诺或陈述是人为作出的

ASIC是“专用集成电路”(Application Specific Integrated Circuit)的缩写。 ASIC是专门设计用于执行单个任务的硅芯片。在比特币中，它们被设计为处理SHA-256散列问题以挖掘新的比特币。

比特币(Bitcoin)是一个众所周知的加密货币，基于POW区块链

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

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

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

块奖励(Block
reward)给予已成
功散列一个事务块的矿工。块奖励
可以是硬币和交易费用
的混合，取决于所讨论的加密货币使用的策略，以及所有的硬币是否已经被成功开采。比特币网络的当前块奖励是每个块有6.25个比特币。

中央类帐(Central ledger)是指由中央机构维护的分类帐。

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

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

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

共识流程(Consensus
Process)是一组对等点，负责维护分布式账本的使用，以达到分类账内容的共识

密码分析(Cryptoanalysis)是研究获得加密信息的含义的方法，而不需要访问通常需要的秘密信息

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

密码使用法(Cryptography)是指加密和解密信息的过程

dApp是一个分散的应用程序，必须完全开放源代码，它必须自主运行，并且没有实体控制其大部分代币

一个DAO(分散的自治组织)可以被认为是一个没有任何人的参与下运行的公司，在一套不可变的商业规则的控制之下

DAO(是的，与一个DAO有区别)是建立在以太坊上的一个风险投资基金，它引发了一次软/硬分叉

解密(Decryption)是将密文变成纯文本的过程

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

以太(Ether)是以太坊区块链的原生代币，它用于支付交易费用、矿工奖励和网络上的其他服务

以太坊(Ethereum)是一个基于区块链技术
的开放式软件平台，支持开发人员撰写智能合约，构建和部署分散式应用程序

以太坊经典(Ethereum
Classic)是现有加密数字货币的分拆，经过硬分叉后的以太坊。

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

数字商品(Digital
commodity)是一种稀缺的，可电子转让的，无形的，具有市场价值的虚拟商品。

数字身份(Digital
identity)是由个人，组织或电子设备在网络空间中采用或声明的在线或网络身份

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

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

双倍支出(Double spend)指的是比特币网络中的一种情况，即有人试图同时向两个

不同的收款人发送比特币交易。但是，一旦比特币交易得到确认，就几乎不可能将花费翻倍。特定交易的确认越多，双倍花费比特币就越难。

菲亚特货币(Fiat currency)是指政府宣布为履行财务义务而有效的任何货币(如美元或欧元)。

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

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

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

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

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

哈希率(Hashrate)是比特币矿工在给定的时间段(通常是一秒)内可执行的哈希值

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

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

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

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

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

节点(Node)是连接到区块链网络的任何计算机。

完整节点(Full node)是完全实施区块链的所有规则的节点

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

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

被许可的区块链(Permissioned blockchain)提供了高度可验证的数据集，因为共识流程创建了数字签名，各方都可以看到。

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

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

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

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

协议(Protocol)是描述如何传输或交换数据的正式规则集，特别是在整个网络中。

Ripple

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

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

SHA 256是用作比特币工作证明系统基础的密码函数

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

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

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

代币(Token)是可以被获取的东西的数字身份。

无代币分类帐(Tokenless ledger)是指不需要本地货币操作的分布式分类帐

交易区块(Transaction block)是比特币网络上的交易集合，集合成一个块，然后可以将其散列并添加到区块链中

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

钱包(Wallet)是一个包含私钥集合的文件。

token是什么？token，通常翻译成通证。Token是区块链中的重要概念之一，它更广为人知的名字是“代币”，但在专业的“链圈”人看来，它更准确的翻译是“通证”，代表的是区块链上的一种权益证明，而非货币。

法币，是法定货币
，是由国家和政府发行的，只有政府信用来做担保，如人民币、美元等等。

Token的三个要素

是数字权益证明，通证必须是以数字形式存在的权益凭证，代表一种权利、一种固有和内在的价值；

是加密，通证的真实性、防篡改性、保护隐私等能力由密码学予以保障；

是能够在一个网络中流动，从而随时随地可以验证。

梭哈是什么？币圈梭哈就是指把本金全部投入。

建仓是什么？

币圈建仓也叫开仓，是指交易者新买入或新卖出一定数量的数字货币

空投是什么？空投是目前一种十分流行的加密货币营销方式。为了让潜在投资者和热衷加密货币的人获得代币相关信息，代币团队会经常性地进行空投

锁仓是什么？锁仓一般是指投资者在买卖合约后，当市场出现与自己操作相反的走势时，开立与原先持仓相反的新仓，又称对锁、锁单，甚至美其名曰蝴蝶双飞

糖果是什么？币圈糖果即各种数字货币刚发行处在ICO时免费发放给用户的数字币，是虚拟币项目发行方对项目本身的一种造势和宣传。

破发是什么？破指的是跌破，发
指的是数字货币的发行价格。币圈破发是指某种数字货币跌破了发行的价格。

私募是什么？币圈私募是一种投资加密货币项目的方式，也是加密货币项目创始人为平台运作募集资金的最好方式。

K线图怎么看？K线图（Candlestick Charts）又称蜡烛图、日本线、阴阳线、棒线、红黑线等，常用说法是“K线”。它是以每个分析周期的开盘价、最高价、最低价和收盘价绘制而成。

搬砖是什么？把现金充值到币价更低的 A 平台，然后买入比特币；然后从 A 平台上提现比特币，收到后马上充值到价格更高的 B 平台；充值的比特币到B平台后，马上卖掉，收到的现金马上提现，然后重复步骤。

ICO是什么？Initial Coin
Offering，源自股票市场
的首次公开发行（IPO）
概念，是区块链项目以自身发行的虚拟货币
，换取市场流通常用的虚拟货币的融资行为。

对冲是什么？一般对冲是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。在期货合约市场，买入相同数量方向不同的头寸，当方向确定后，平仓掉反方向头寸，保留正方向获取盈利。

头寸是什么？头寸是一种市场约定，承诺买卖合约的最初部位，买进合约者是多头，处于盼涨部位；卖出合约为空头，处于盼跌部位。

利空是什么？促使币价下跌的消息，如比特币技术问题，央行打压等

利好是什么？利好：指币种获得主流媒体
关注，或者某项技术应用有突破性进展，有利于刺激价格上涨的消息，都称为利好

成交量是什么？反映成交的数量多少和买卖的人的多少。一般可用成交币数和成交金额来衡量。

反弹是什么？币价在下跌趋势中因下跌过快而回升的价格调整现象。回升幅度小于下跌幅度。

盘整是什么？通常指价格变动幅度较小，比较稳定，最高价与最低价相差不大的行情

回调是什么？在多头市场
上，币价涨势强劲，但因价格过快上升而出现暂时回跌，称回调。下跌幅度小于上涨幅度。

杠杆是什么？杠杆交易
，顾名思义，就是利用小额的资金来进行数倍于原始金额的投资，以期望获取相对投资标的物波动的数倍收益率，抑或亏损。

币圈AMA全称“Ask Me Anything”，意思是“问我什么都可以”。通常是指项目方或交易所负责人不定期举办的回答用户问题的活动会出现的标题。

IOU全称“I owe you”，意为“我欠你的”。指的是交易所先欠着投资者的币，等交易所有了币后再分配给相应的投资者

TTM全称“TO THE
MOON”
，意为“到月球上”
，就是说希望价格能涨到月球。因为此前狗狗币

被炒的时候，马斯克曾表示将该币带到月球上，然后狗狗币大涨。

ERC-20：一种代币标准。2015年11月份推出，是基于以太坊的网络，由以太坊智能合约创建的代币类型，描述的是这种代币合约必须要实现的功能和事件。在很多情况下，这些代币都是可以立即进行交易的

Gas：在区块链上执行交易的单位。简单说就是手续费（付给矿工的费用）的意思，类似于汽车需要加油才能跑起来，你的转账交易也需要充气才能完成。在交易时你设置的Gas越多，交易就会完成得越快，因为奖励越高，就会有更多的矿工尽早处理任务

SAFT即 Simple Agreement for Future Tokens，「未来代币简单协议」。是指项目方向合格投资者提供的投资合同，承诺在网络或公司运行时交付一定数量的代币。与标准 ICO 不同之处在于，ICO 会立即发放代币或硬币，而 SAFT 实际上是一种未来
交付代币的承诺。投资者购买的是未来发行的代币购买权利，更像是一种期权。

CDP全称是 Collateralized Debt Position，意为「债务抵押仓位」。

在 MakerDAO 等去中心化金融（DeFi）系统中，用户需要将自己持有的 ETH 等数字加密货币资产抵押给系统，获取系统发放的稳定币。

PnD全称为 Pump and Dump，简单来讲就是拉盘砸盘。拉盘为 Pump，砸盘为 Dump。这是一种在任何具备二级市场的市场中都会出现的常见骗局。

FOMO Fear of Missing Out，意为「害怕错过赚钱的机会」，也可以将其意义扩大为从众心理。在币圈，这指的是一种非常特殊的通证经济模式。