NYLife360.com, Tel: 929-633-1888, VX：NYLife360

1. 学习材料

查阅火币新手资料库，从小白到精通的第一步。链接:

https://pan.baidu.com/s/1KhwbFK8xHF6Mva-1SMCemA 提取码: rtgc

https://epubw.com/

火币成长学院

https://www.huobi.so/zh-cn/guide/

币安学习教程

https://www.binance.vision/zh/tutorials

Coindesk 学习资料

https://www.coindesk.com/learn

金色财经课程

http://www.jinse.org/hall.html

巴比特课程

https://www.8btc.com/course

NYU Blockchain community： telegram：http://t.me/NYUBlockchain .

Webinar recording：

https://zoom.us/recording/share/XDUXpaGPMR_PhMoasvGc19nFje04FNmRrxAFmHwOJRGwlumekTziMw?startTime=1575824472000

2. 区块链行业基本知识

2.1. 区块链行业发展梗概

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链（Blockchain），是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。

2008 年 11 月 1 日，一位自称中本聪(Satoshi Nakamoto)的人发表了《比特币:一种点对点的电子现金系统》一文，阐述了基于 P2P 网络技术、加密技术、时间戳技术、区块链技术等的电子现金系统的构架理念，这标志着比特币的诞生。

2009 年 1 月 3 日，第一个序号为 0 的创世区块诞生。

2009 年 1 月 9 日，出现序号为 1 的区块，并与序号为 0 的创世区块相连接形成了链，标志着区块链的诞生。

2013 年 11 月，Vitalik Buterin（俄罗斯人）发起了 Ethereum 项目，并在 12 月发布了以太坊白皮书首个版本。

为方便理解区块链的历史与趋势，可将其发展划分为六个阶段。

1. 技术实验阶段（2007—2009）。化名中本聪的比特币创始人从 2007 年开始探索用一系列技术创造一种新的货币——比特币，2008 年 10 月 31 日发布了《比特币白皮书》，2009 年 1 月 3 日比特币系统开始运行。支撑比特币体系的主要技术包括哈希函数、分布式账本、区块链、非对称加密、工作量证明，这些技术构成了区块链的最初版本。从 2007 年到 2009 年底，比特币都处在一个极少数人参与的技术实验阶段，相关商业活动还未真正开始。

2. 极客小众阶段（2010-2012）。2010 年 2 月 6 日诞生了第一个比特币交易所，5 月 22 日有人用 10000 个比特币购买了 2 个披萨。2010 年 7 月 17 日著名比特币交易所 Mt.gox 成立，这标志着比特币真正进入了市场。尽管如此，能够了解到比特币，从而进入市场中参与比特币买卖主要是狂热于互联网技术的极客们。他们在 http://Bitcointalk.org 论坛上讨论比特币技术，在自己的电脑上挖矿获得比特币，在 Mt.gox 上买卖比特币。仅仅 4 年后，这些技术宅中的一些人成了亿万富翁和区块链传奇。

3. 市场酝酿阶段（2013-2015）。2013 年初比特币价格 13 美元，3 月 18 日金融危机中的塞浦路斯政府关闭银行和股市，推动比特币价格飙升，4 月最高至 266 美元。8 月 20 日德国政府确认比特币的货币地位。10 月 14 日中国百度宣布开通比特币支付。11 月美国参议院听证会明确了比特币的合法性。11 月 19 日比特币达到 1242 美元新高！然而，此时区块链进入主流社会经济的基础仍不具备，价格飙升包含了过于乐观的预期。中国银行体系遏制、Mt.Gox 的倒闭等事件触发大熊市，比特币价格持续下跌，2015 年初一度至 200 美元以下，许多企业倒闭，不过经历严冬活下来的企业的确更加强壮了。无论如何在这个阶段，大众开始了解比特币和区块链，尽管还不能普遍认同。

4. 进入主流阶段（2016-2018）。以 2016 年 6 月 23 日英国脱欧，2016 年 9 月朝鲜第五次核试验，2016 年 11 月 9 日特朗普当选等事件为标志，世界主流经济不确定性增强，具有避险功能从而与主流经济呈现替代关系的比特币开始复苏，市场需求增大，交易规模快速扩张，开启了 2016-2017 牛市。尽管中国市场受到政策的严厉遏制，但韩国、日本、拉美等市场快速升温，比特币价格从 2016 年初的 400 美元最高飙升至 2017 年底的 20000 美元，翻了 50 倍。比特币的造富效应，以及比特币网络拥堵造成的交易溢出带动了其他虚拟货币以及各种区块链应用的大爆发，出现众多百倍、千倍甚至万倍增殖的区块链资产，引发全球疯狂追捧。使比特币和区块链彻底进入了全球视野。芝加哥商品交易所上线比特币期货交易标志着比特币正式进入主流投资品行列。

5. 产业落地阶段（约 2019-2021）。在市场狂乱之后，2018 年的虚拟货币和区块链会在市场、监管、认知等各方面进行调整，回归理性。2017 年造富效应和区块链理想造就的众多区块链项目中，大部分会随着市场的降温而消亡，小部分会坚持下来继续推进区块链的落地。2019 年这些项目将会初步落地，但仍需要几年时间接受市场的检验，这就是一个快速试错过程，企业产品的更迭和产业内企业的更迭都会比较快。到 2021 年，在区块链适宜的主要行业领域应该会有一些企业稳步发展起来。加密货币也会得到较广泛应用。

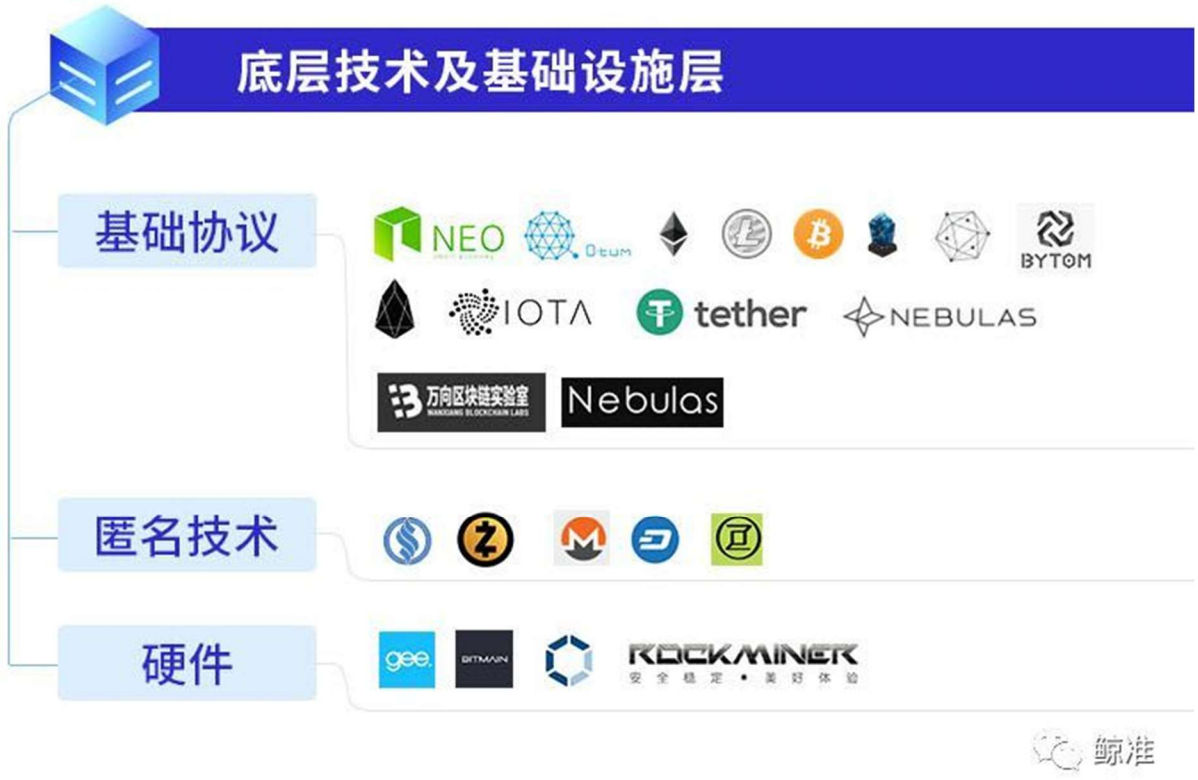
6. 产业成熟阶段（约 2022-2025）。各种区块链项目落地见效之后，会进入激烈而快速的市场竞争和产业整合阶段，三五年内形成一些行业龙头，完成市场划分，区块链产业格局基本形成，相关法律法规基本健全，区块链对社会经济各领域的推动作用快速显现，加密货币将成为主流货币，经济理论会出现重大调整，社会政治文化也将发生相应变化，国际政治经济关系出现重大调整，区块链在全球范围内对人们的生活产生广泛而深刻的影响。

区块链的这六个发展阶段还可以再简化一下，前两个阶段可以看做技术试验阶段，中间两个阶段是主流认知阶段，后两个阶段是产业实现阶段。我们当前仍处在社会认知广度已经足够，但认知深度尚嫌不足的时期。需要深入推进区块链知识的研究和普及，为产业发展成熟奠定基础。无论如何，区块链对全球经济的巨大价值已经被充分认识到了，对于全球社会政治生态改善的价值也在逐步显现，这是一个值得各国大力投入、抢占先机的社会经济新动力。

2.2. 区块链行业项目分类

底层技术及基础设施层，主要是代表了提供区块链最底层的协议代码和基础硬件设施。

NYLife360.com, Tel: 929-633-1888, VX：NYLife360



基础协议通常是一个完整的区块链产品，类似于我们电脑的操作系统，它维护着网络节点，仅提供 Api 供调用。这个层次是一切的基础，使用网络编程、分布式算法、加密签名、数据存储等技术来构建网络环境、搭建交易通道以及制定节点的奖励规则，典型的例子国外的以太坊，国内的 NEO（小蚁）。

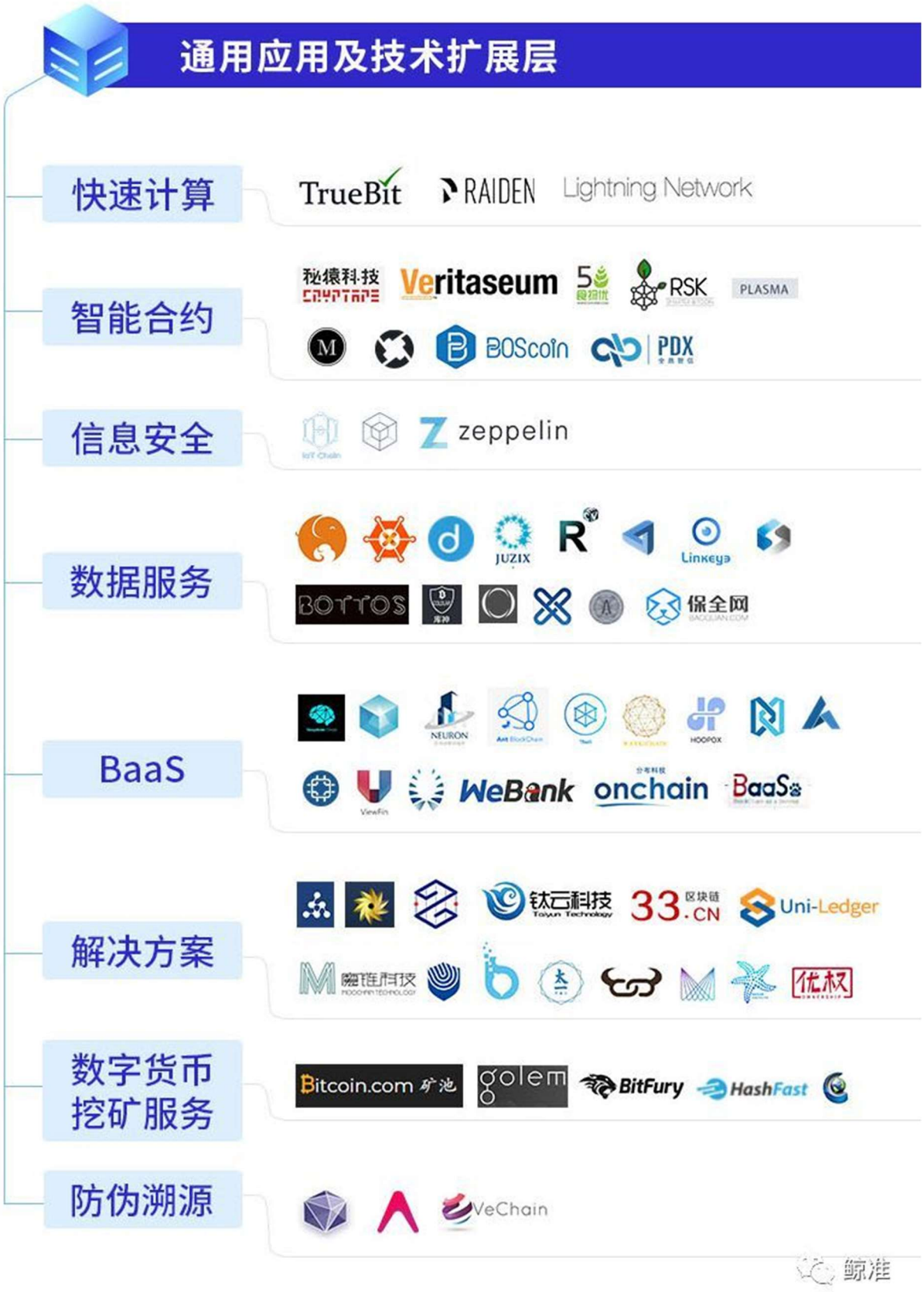
代表项目：NEO、Ethereum、量子链

区块链相关硬件则主要由比特币矿机的制造售卖厂商以及区块链路由器提供商构成，以比特大陆和极路由为代表。

代表项目：嘉楠耘智、RockMiner、极路由

通用应用及技术扩展层

通用应用及技术扩展层主要是为了让区块链产品更加实用以及面向开发者提供服务以便构建基于区块链技术的应用，这一层使用的技术基本没有限制，之前提到的分布式存储、机器学习、大数据等技术均可被使用。



快速计算：快速计算主要是在底层区块链基础上进行优化，借以解决底层区块链固有的一些问题，提高区块链的计算速度。例如闪电网络（lightning network）是创建一个能够以高容量和高速度进行交易的参与者的安全网络，具有即时付款、扩展性强、低成本、可跨区块链交易的特点。

代表项目：lightning-network、truebit、raiden

智能合约：智能合约就是“可编程合约”，或者叫做“合约智能化”，其中的“智能”是执行上的智能，也就是说达到某个条件，合约自动执行，比如自动转移证券、自动付款等，这将是区块链技术重要的发展方向。

代表项目：秘猿科技、全息互信、SCRY.INFO

挖矿服务：挖矿服务主要为需求方提供算力，此类项目要么与矿厂进行合作，要么集合全网用户的算力进行再分配。

代表项目：MaidSafeCoin、bitfury、hashfast

信息安全：信息安全部分的项目主要是保障开发的安全性以及区块链网络中信息内容的安全性，可以使得开发者进行更加安全的开发和管理应用程序，个人和企业的交易数据得到保障。

代表项目：万物链、zeppelin、gladius

数据服务：数据服务主要包括数据共享、数据库、数据保护三项服务，数据共享项目是建立一个基于区块链的市场和管理平台，在此基础上提供数据保全和安全存储的服务则构成数据保护，数据库则是为开发者或企业提供数据库基础设施。

代表项目：公信宝、众享比特、矩阵元

区块链 BAAS：区块链 BAAS 是基于已有的区块链技术开发的去中心化平台，提供基于公链的实例服务。

代表项目：百度 Baas、趣链科技、快贝

NYLife360.com, Tel: 929-633-1888, VX：NYLife360

区块链解决方案：区块链解决方案为区块链的企业级应用，为特定的商业场景提供一整套的解决方案。

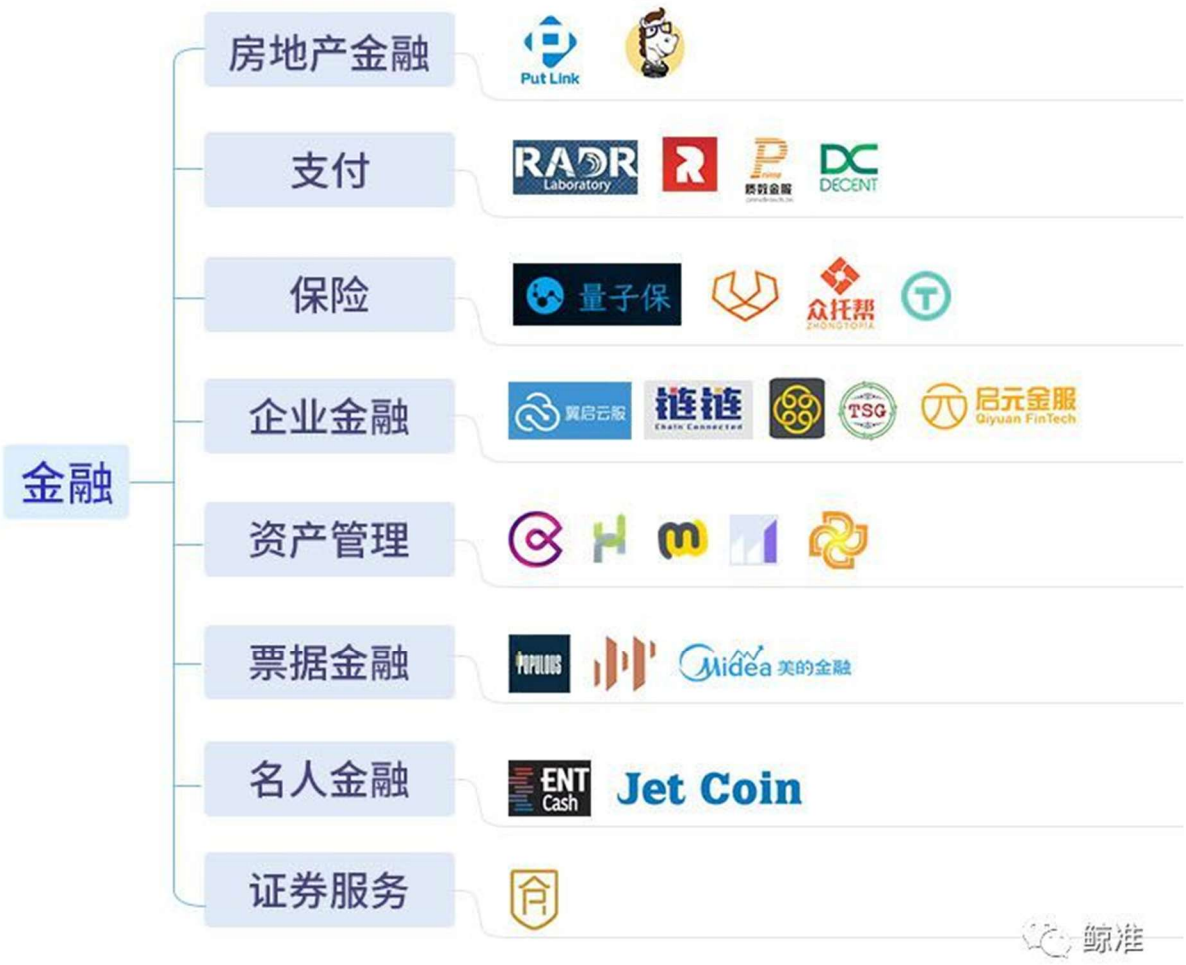
代表项目：海星区块链、塔链网络、网录科技

防伪溯源：平台级别的防伪溯源项目一般基于区块链、物联网等相关技术辨别商品、产品的真假，解决中间链条不透明的问题。

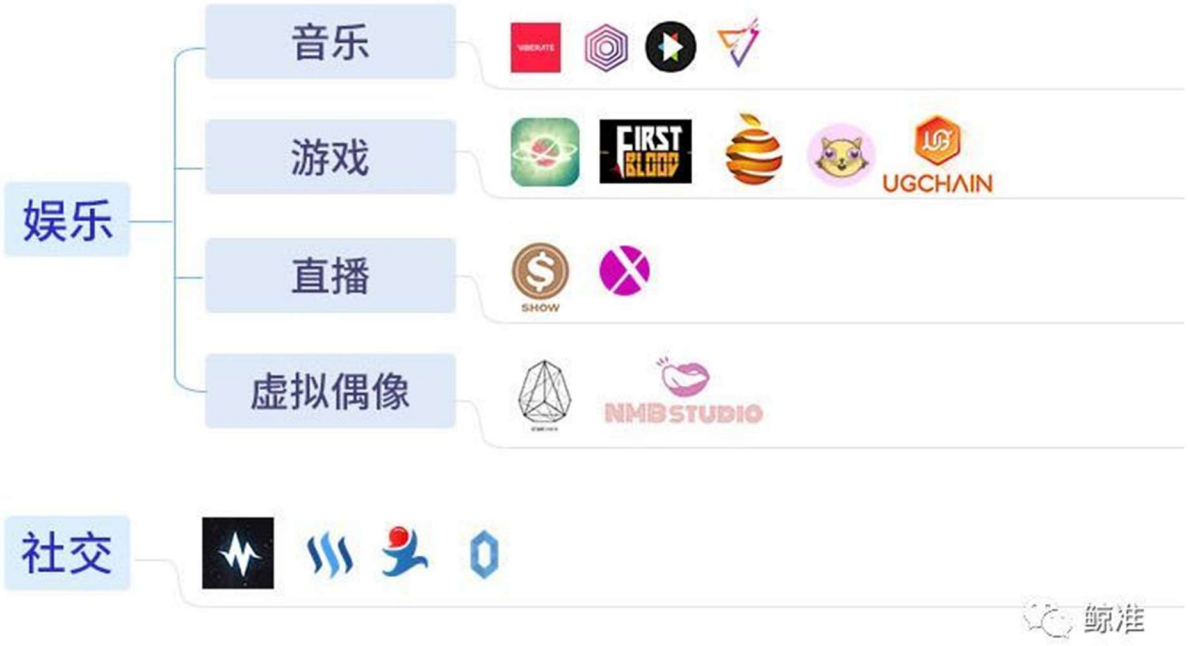
行业应用层

区块链项目在金融领域的探索主要集中在支付、房地产金融、企业金融、保险、资产管理、票据金融等领域。在国内，不仅是新兴区块链创业企业，如中国银联、招商、民生等银行和蚂蚁区块链、众安科技在内的科技巨头已经开始布局并落地了相应的平台与项目。利用区块链的去中心化、不可篡改的特性对于金融各个环节的风险有了更好的把控，从而降低了金融流程中的成本。

NYLife360.com, Tel: 929-633-1888, VX：NYLife360



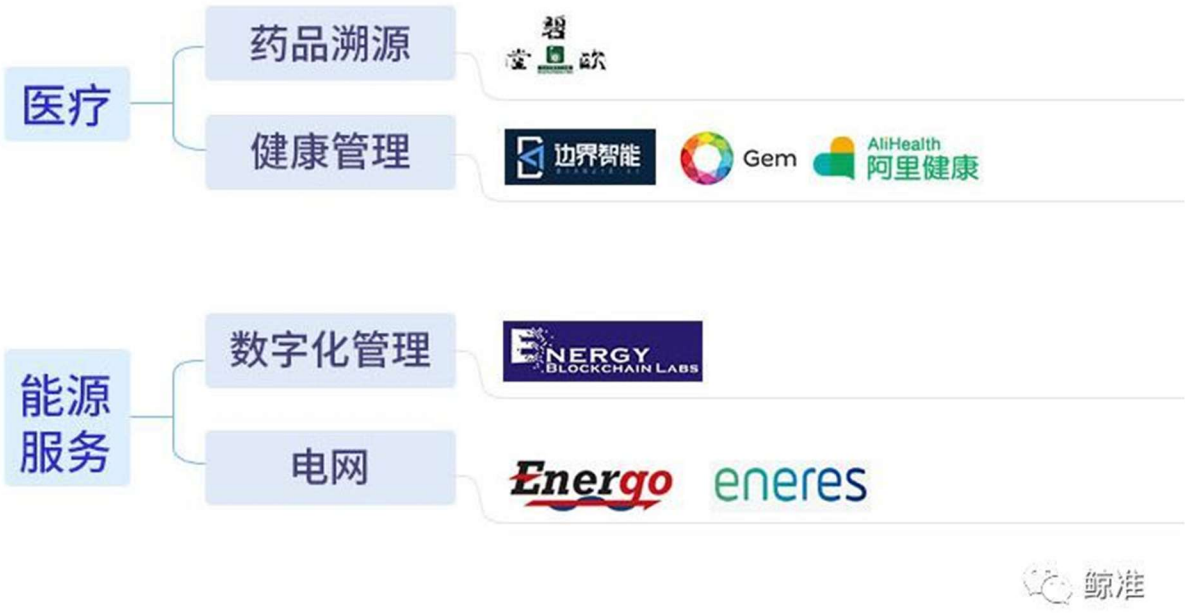
NYLife360.com, Tel: 929-633-1888, VX：NYLife360



区块链应用较为早期的 2C 类业务主要衍生在娱乐社交领域。在音乐创作中区块链可以帮助创作者规避抄袭的争议。基于区块链做的虚拟偶像、游戏、直播等项目让虚拟财产交易和保护更加透明。

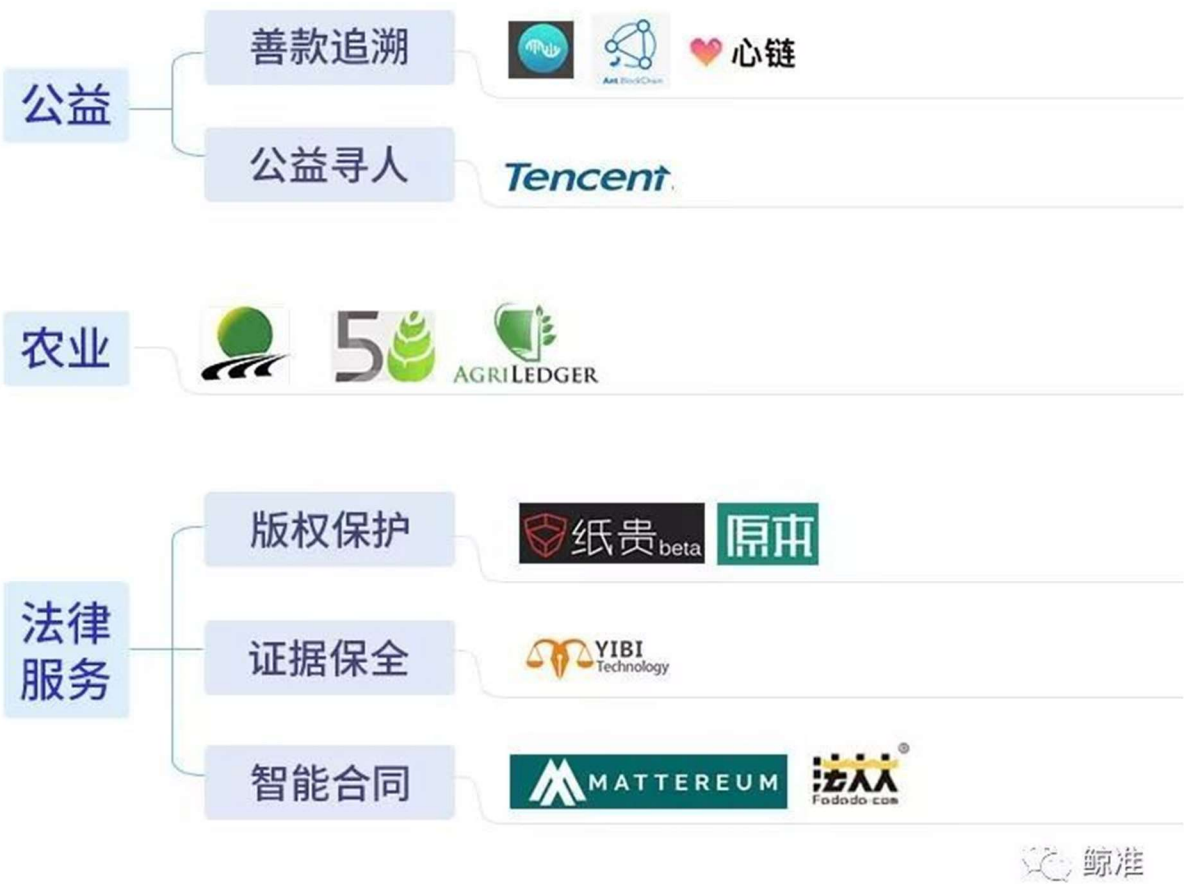
曾有机构预言供应链和物联网将是区块链迅猛发展的下一片沃土。这得益于区块链带来的交易共享性和不可篡改性，这提高了供应链在物流、资金流、信息流等实体协作沟通效率，改善了多方协作时的争议。

NYLife360.com, Tel: 929-633-1888, VX：NYLife360



在能源领域最为广泛应用的是智能电网。针对每一度电用区块链可以从来源到使用建立完备的数字档案，为电站提供数据支持和资产评估依据。区块链还可以释放分布式资源的多余电力，如回购民用屋顶太阳能产生的冗余资源。

NYLife360.com, Tel: 929-633-1888, VX：NYLife360



针对医疗的数据安全和患者隐私保护，区块链的匿名和去中心化的特性得到了很好的应用。这让医联体之间进行远程数据共享、分布式保障与存储管理更加安全。

在公益事业和农业中，应用最多的还是区块链的溯源能力，追溯善款的去向，让捐赠者安心；追溯农产品的来源，让食用者放心。

区块链的分布式存证让在法律层面主要体现在版权保护、证据保全和电子智能合同三个方面。对于版权保护，区块链让版权交易标准化成为可能；而对于电子证据来说，区块链实现了保真和验真。

最全区块链生态图谱发布，一张图看清 2400 个典型项目

https://36kr.com/p/5114727

2.3. 共识协议

2.3.1. 什么是共识协议

共识机制就是所有记账节点之间怎么达成共识，去认定一个记录的有效性，这既是认定的手段，也是防止篡改的手段。区块链提出了几种不同的共识机制，适用于不同的应用场景，在效率和安全性之间取得平衡。

共识机制是区块链的核心基石，是区块链系统安全性的重要保障。区块链是 一个去中心化的系统，共识机制通过数学的方式，让分散在全球各地成千上万的节点就区块的创建达成一致的意见。共识机制中还包含了促使区块链系统有效运 转的激励机制，是区块链建立信任的基础。

区块链公链常用的共识机制有 POW、POS、DPOS、BFT 以及多种机制混合而成的共识机制等。共识是指系统节点达成一致的过程，而分布式系统的一致性体现在三个方面:

- 最终性(Termination): 所有进程最终会在有限步数中结束并选取一 个值, 算法不会无尽执行下去。
- 统一性(Agreement): 所有进程必须同意同一个值。
- 合法性(Validity): 输出内容是输入内容按照系统规则生成的，且输出内容合法。

最终性衡量了达成共识的效率，在一些对交易确认的实时性要求高的场景显 得非常重要，而统一性和合法性表征了共识的安全性。在区块链系统中，去中心化程度表征了分布式系统的大规模协作程度。因此，我们从效率、安全性和去中心化程度这三个维度去评价各种共识机制，也就是长铗提出的著名的“不可能三角”理论。

区块链共识协议最详细的分析

https://blog.csdn.net/ITleaks/article/details/80228896

2.3.2. POW 工作量证明

比特币采用的 POW 工作量证明共识机制，在生成区块时，系统让所有节点公平地去计算一个随机数，最先寻找到随机数的节点即是这个区块的生产者，并 获得相应的区块奖励。由于哈希函数是散列函数，求解随机数的唯一方法在数学上只能是穷举，随机性非常好，每个人都可以参与协议的执行。由于梅克尔树根的设置，哈希函数的解的验证过程也能迅速实现。因此，比特币的 POW 共识机 制门槛很低，无需中心化权威的许可，人人都可以参与，并且每一个参与者都无 需身份认证。

同时，中本聪通过工作量证明的机制破解了无门槛分布式系统的“女巫攻击” 问题（女巫攻击 Sybil 攻击是指利用社交网络中的少数节点控制多个虚假身份，从而利用这些身份控制或影响网络的大量正常节点的攻击方式）。对系统发起攻击需要掌握超过 50%的算力，系统的安全保障较强。

POW 共识的优点可归纳为:

- 算法简单，容易实现，节点可自由进入，去中心化程度高。
- 破坏系统需要投入极大的成本，安全性极高。
- 区块生产者的选择通过节点求解哈希函数实现，提案的产生、验证到共识的最终达成过程是一个纯数学问题，节点间无需交换额外的信息即可达成共识，整个过程不需要人性的参与。

比特币系统的设定在保证安全性的的前提下，牺牲了一部分最终性。

POW 共识算法也存在一些问题:

- 为了保证去中心化程度，区块的确认时间难以缩短。
- 没有最终性，需要检查点机制来弥补最终性，但随着确认次数的增加，达成共识的可能性也呈指数级地增长。 由于这两个方面的问题，一笔交易为了确保安全，要在 6 个新的区块产生后才能在全网得到确认，也就是说一个交易的确认延迟时间大概为 1 小时，这无法 满足现实世界中对交易实时性要求很高的应用场景。

另一方面，POW 共识算法带来了硬件设备的大量浪费。随着比特币价值的 增长，比特币算力竞赛经历了从 CPU 到 GPU，再到 ASIC 专用芯片的阶段。算力强大的 ASIC 芯片矿机将挖矿算法硬件化，而 ASIC 芯片矿机在淘汰后，没有其他的用途，造成了大量的硬件浪费。

2.3.3. POS 权益证明

POS(Proof of Stake)共识机制，是一种由系统权益代替算力决定区块记账权的共识机制，拥有的权益越大则成为下一个区块生产者的概率也越大。POS 的合理假设是权益的所有者更乐于维护系统的一致性和安全性。如果说 POW 把 系统的安全性交给了数学和算力，那么 POS 共识机制把系统的安全性交给了人 性。人性问题，可以用博弈论来研究，POS 共识机制的关键在于构建适当的博弈 模型相应的验证算法，以保证系统的一致性和公平性。

POS 共识机制没有像 POW 那样耗费能源和硬件设备，缩短了区块的产生 时间和确认时间，提高了系统效率。但存在的缺点也有很多，包括:

- 实现规则复杂，中间步骤多，参杂了很多人为因素，容易产生安全漏洞。
- 与 POW 共识机制一样没有最终性，需要检查点机制来弥补最终性。

2.3.4. DPOS 代理权益证明

DPOS(Delegated Proof of Share)，代理权益证明共识机制，是一种 基于投票选举的共识算法，类似代议制民主。在 POS 的基础上，DPOS 将区块生产者的角色专业化，先通过权益来选出区块生产者，然后区块生产者之间再轮 流出块。

DPOS 共识由 BitShares(比特股)社区首先提出，它与 POS 共识的主要区别在于节点选举若干代理人，由代理人验证和记账。DPOS 相比 POS 能大幅度提升了选举效率，在牺牲一部分去中心化特性的情况下得到性能的提升。

DPOS 共识机制不需要挖矿，也不需要全节点验证，而是由有限数量的见证节点进行验证，因此是简单、高效的。由于验证节点数量有限，DPOS 共识被 普遍质疑过于中心化，代理记账节点的选举过程中也存在巨大的人为操作空间。

2.3.5. Others

(1)PBFT

最常用的 BFT 共识机制是实用拜占庭容错算法 PBFT(Practical Byzantine Fault Tolerance)。该算法是 Miguel Castro 和 Barbara Liskov 在 1999 年提出来的，解决了原始拜占庭容错算法效率不高的问题，将算法复杂度由节点数的指数级降低到节点数的平方级，使得拜占庭容错算法在实际系统应用中变得可行。

PBFT 是针对状态机副本复制为主的分布式系统执行环境开发的算法，旨在 让系统中大部分的诚实节点来覆盖恶意节点或无效节点的行为。PBFT 算法的节 点数量是固定的，节点身份提前确定，无法动态添加或删除，只能适用于节点数 目固定的联盟链或私有链场景中。

PBFT 算法存在的问题:

- 计算效率依赖于参与协议的节点数量，不适用于节点数量过大的区块链系统，扩展性差。
- 系统节点是固定的，无法应对公有链的开放环境，只适用于联盟链或私有链环境。
- PBFT 算法要求总节点数 n>=3f+1(其中，f 代表作恶节点数)。系统的失效节点数量不得超过全网节点的 1/3，容错率相对较低。

(2)DBFT

考虑到 BFT 算法存在的扩容性问题，NEO 采用了一种代理拜占庭容错算法— —DBFT(Delegated Byzantine Fault Tolerant)。它与 EOS 的 DPOS 共识机制一样，由权益持有者投票选举产生代理记账人，由代理人验证和生成区块，以此大幅度降低共识过程中的节点数量，解决了 BFT 算法固有的扩容性问题。

为了便于在区块链开放系统中应用，NEO 的 DBFT 将 PBFT 中的将 C/S(客户 机/服务器)架构的请求响应模式，改进为适合 P2P 网络的对等节点模式，并将静 态的共识参与节点改进为可动态进入、退出的动态共识参与节点，使其适用于区 块链的开放节点环境。

DBFT 的算法中，参与记账的是超级节点，普通节点可以看到共识过程，并 同步账本信息，但不参与记账。总共 n 个超级节点分为一个议长和 n-1 个议员， 议长会轮流当选。每次记账时，先有议长发起区块提案(拟记账的区块内容)， 一旦有至少(2n+1)/3 个记账节点(议长加议员)同意了这个提案，那么这个 提案就成为最终发布的区块，并且该区块是不可逆的，所有里面的交易都是百分 之百确认的，区块不会分叉。

NEO 的 DBFT 共识机制下只设置了 7 个超级节点，以一种弱中心化的模式 实现较高的共识效率。目前，这些代理节点是静态选出的，并完全由项目方部署， NEO 由此被外界质疑为过于中心化。

DBFT 的优点一方面是效率高，NEO 每 15~20 秒生成一个区块，交易吞吐 量可达到约 1000TPS，通过适当优化，性能可达 10000TPS;另一方面是其良 好的最终性，区块不会分叉，以此来验证参与者的身份，保护网络安全，使区块链能够适用于对交易确认实时性要求高的真实金融场景。

DBFT 的缺点也不容忽视，一方面体现在较低的容错率，当有 1/3 或以上超级节点为恶意节点或宕机后，系统将无法提供服务;另一方面体现在超级节点数 量过少，中心化程度高。

2.4. 知名公链

2.4.1. 什么是公链及公链生态

公链也称“公有链”，比特币是世界上第一个共有链，所谓公和私区别就在于链上的节点是否是自己可控，公有链对应的就是私有链；比特币、以太坊是时下最流行的公有链。

公有链是指全世界任何人都可以随时进入到系统中读取数据、发送可确认交易、竞争记账的区块链。公有链通常被认为是“完全去中心化”的，因为没有任何个人或者机构可以控制或篡改其中数据的读写。

公有链一般会通过代币机制（Token）来鼓励参与者竞争记账，来确保数据的安全性。从应用上说，区块链公有链包括比特币、以太坊、超级账本、大多数山寨币以及智能合约，其中区块链公有链的始祖是比特币区块链。

目前，大多数以太坊项目都依靠以太坊作为公有链，以太坊是一个全新开放的区块链平台，它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用。 以太坊是可编程的区块链 ，允许用户按照自己的意愿创建复杂的操作，可以作为多种类型去中心化区块链应用的平台。

除金融类应用外，任何对信任、安全和持久性要求较高的应用场景，比如资产注册、投票、管理和物联网等等 3.0 时代应用，都会大规模地受到以太坊平台影响。

公链当前面临的最大问题是安全和效率的矛盾，即如何在去中心化程度和高 TPS 两者之间取得平衡，最典型的代表如 Ethereum 和 EOS 之争。

2.4.2. ETH

以太坊原是一个平台和一种编程语言，由杰弗里•维尔克创立，该平台可以使开发人员能够建立和发布下一代分布式应用。 以太坊可以用来编程，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等。

以太币（ETH）正是以太坊（Ethereum）平台上的一种数字代币，开发者们需要支付以太币（ETH）来支撑应用的运行。以太币和其他数字货币一样，可以在交易平台上进行买卖，目前流通中的 ETH 超过 9000 万个。自上市以来，ETH 以其优质的属性和良好的口碑不断扩大其市场份额，如今更是在全球加密货币市值排名中蝉联亚军宝座，仅在比特币之下。其价值从最初的 1 美元左右飙升至 200 美元以上，涨幅高达 200 多倍。

白皮书：

https://github.com/ethereum/wiki/wiki/%5B%E4%B8%AD%E6%96%87%5D-%E4%BB%A5%E5%A4%AA%E5%9D%8A%E7%99%BD%E7%9A%AE%E4%B9%A6

2.4.3. EOS

EOS，可以理解为 Enterprise Operation System，即为商用分布式应用设计的一款区块链操作系统。 **EOS** 是引入的一种新的区块链架构，旨在实现分布式应用的性能扩展。 注意，它并不是像比特**币**和以太坊那样的**货币**，而是基于 **EOS** 软件项目之上发布的代**币**，被称为区块链 3.0。

一句话描述 EOS.IO：高性能的下一代区块链底层商用操作系统。

EOS.IO 软件是 Block.One 公司正在研发的一个动态通用型底层区块链平台，在它之上可以构建应用程序，使去中心化的应用可以更好地横向和纵向扩展。

EOS 提供帐户、身份验证、数据库、异步通信和跨越数百个 CPU 内核或集群的应用程序调度。它可以扩展至每秒处理百万级交易，消除用户的手续费，并且允许快速和轻松的部署去中心化的应用。

EOS 在什么背景下出现，解决了什么痛点？

比特币没有实现图灵完备，无法实现更多的功能扩展，同时比特币也暴露出了处理速度慢，手续费高等等问题。

以太坊为执行智能合约而生，最大的改进是支持了“图灵完备”，成为了一个可编程的区块链网络系统。目前主要用途体现在 ICO 发币。

为了抵御黑客攻击和无限循环 bug 耗费全网资源设计了 gas 收费机制，这注定以太坊上不可能建大型通用的应用。试想一下一个区块链的社交平台如果运行在以太坊上，用户之间发消息的成本多高。

而且以太坊每个新区块有 15 秒延滞，对于以太坊钱包来说没什么影响，但是如果要实现发文章、点赞这种功能来说，15 秒太慢了。

现有的区块链平台转账速度慢、交易费用高、系统并发处理难度高、安全缺陷、开发难度高等痛点都阻碍着区块链技术的大面积应用。

要做一个成功的区块链应用，必须满足以下要求：支持百万级别用户、免费使用、轻松升级和 Bug 修复、低延迟、串行性能和并行性能。

EOS 就是奔着这个目标来的：做一个能够真正支持商业级应用的操作系统。

2.4.4. TRON

TRON（TRX）波场币，**是 TRON** 的官方货币，**TRON 是**一个娱乐内容共享平台，利用了区块链和点对点网络技术。**TRON** 的开放，分散式平台和存储技术将允许数字内容创作者切断 Apple Store 和 Google Play Store 等中间商。因此，内容制作者将能够直接从消费者那里获得资金。

6 月 25 日，TRON 的团队推出了主网。这意味着该公司已经推出了自己的专有区块链，并将其迁移到之前在以太坊区块链上传播的所有 TRX（ERC-20）代币。此事件被称为 TRON 独立日。

Freewallet 是最早全面支持 TRON 硬币的公司之一。Multiwallet 应用程序管理多个硬币，使用户可以在一个地方进行交叉交换。

波场 TRON 是基于区块链的去中心化内容协议，其目标在于通过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，这个协议可以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，形成去中心化的内容娱乐生态。

据虚拟货币行业内最权威网站 coinmarketcap.com 数据显示，目前波场 TRON 官方代币 TRX 总市值已超过 1 亿 6000 万美元，全球虚拟货币排行榜居 40 位左右。

波场（TRON）的特点
波场（TRON）作为去中心化的内容协议，与中心化的互联网结构相比，具有以下四个基本特征：

1. 数据自由：自由而不受控制的上传、存储并传播包括文字、图片、音频和视频在内的内容
2. 内容赋能：通过内容的贡献和传播获得应有的数字资产收益，经济激励赋能
3. 内容生态人人发行数字价值：个人可以自由的发行数字资产， 他人则可以通过购买数字资产享受数据贡献者不断发展所带来的利益与服务。
4. 基础设施：分布式的数字资产则会匹配一整套完整的去中心化基础设施，包括分布式交易所，自治性博弈，预测，游戏系统。

NYLife360.com, Tel: 929-633-1888, VX：NYLife360

波场币 TRON(TRX)是什么？
https://www.jinse.com/news/bitcoin/100044.html

2.4.5. NEO

什么是 NEO（小蚁币）？

NEO 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，自成立以来，NEO 团队亲历了区块链行业的高潮与低谷，数字货币市场的狂热与冷却。我们相信，科技是这个时代变迁的原动力，在这股动力的推动下，我们将迈入新的“智能经济”时代。NEO 区块链通过将点对点网络、拜占庭容错、数字证书、智能合约、超导交易、跨链互操作协议等一系列技术相结合，让你快速、高效、安全、合法地管理你的智能资产。

NEO 中内置两种原生代币，NEO（缩写符号 NEO）和 NeoGas（缩写符号 GAS）。NEO 是管理代币，总量 1 亿份，用于实现对 NEO 网络的管理权。管理权包括投票进行记账人选举，NEO 网络参数更改等。NEO 的最小单位为 1，不可再分割。GAS 是燃料代币，最大总量上限为 1 亿，用于实现对 NEO 网络使用时的资源控制。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。GAS 的最小单位为 0.00000001。

不少人把小蚁（NEO）称为“中国的以太坊”，因为都涉及 Gas 费用、都有智能合约等，虽然同样是区块链底层公链项目，但两者也是有明显区别的。

小蚁（NEO）和以太坊的主要区别是什么？

1. 以太坊的智能合约只用以太坊自己的编程语言 Solidity，而小蚁（NEO）能兼容所有的编码语言。NEO 的智能合约比起以太坊，更能体现高确定性、高扩展性、高兼容性等特点，在小蚁上开发，智能合约的开发者不需要学习 Solidity（以太坊平台开发要用的语言），就能使用熟悉的 Java、C/C#、Go 等编程语言编写智能合约，快速上手并融入区块链开发的世界。

2. NEO 需要智能合约技术，但不如以太坊完善。以太坊以智能合约来创建数字资产的发行标准，但欠缺的是数字身份认证机制。 此外，在共识算法上也有不同。小蚁（NEO）采用独创的 dBFT 共识算法，而以太坊则采用“PoS”算法。

3. NEO 项目的主要目标就是为“智能经济” 提供分布式网络的基础架构。那么 “智能经济” 又是什么呢？智能经济= 数字资产+数字身份认证+智能合约，这三者的结合也构建出了 NEO 的生态环境。

https://zhuanlan.zhihu.com/p/34645032

2.4.6. 其他

2.5. Layer 2 技术

2016 年 1 月，距离比特币创世区块诞生 7 年之后，一篇名为《The Bitcoin Lightning Network：Scalable Off-Chain Instant Payment》的白皮书发布，这是第二层扩容方案（Layer 2 Scaling Solutions，简称 Layer 2 ）的开端；到 2018 年的年末，光是技术类型就已经有状态通道、Plasma、Truebit 等各类 Layer 2 方案，出现了 Celer Network、AlphaWallet、Raiden Network、Alacris 等等一众新星，在时间和资源都极度稀缺的情况下根据自己发现的需求，针对不同的场景给出自己的解决方案，准备迎接未来加密经济应用的爆发。

区块链带来了强大的去中心化应用生态，无数人对它寄以厚望，希望区块链能够打破金融孤岛。2017 年上百个公链项目展开角逐，但到了 2019 年，大规模应用落地仍旧困难：区块链发展受到 Vitalik 提出的不可能三角的瓶颈性限制————也就是区块链系统设计无法同时兼顾可扩展性、去中心化和安全性，三者只取其二。

2.5.1. 什么是 Layer 2 技术

社会的发展带来的是更精细的分工，区块链的技术发展也如是——- 分层，本质上就是一种分工。公链不能做所有的事情，那么就让它来做它擅长的东西。由此，也就是第二层扩容方案的思路，我们称为“ Layer 2”，是构建在底层区块链（Layer 1）之上的基础架构，为丰富的区块链应用提供更好的可扩展性、隐私性和可用性。 Layer 1 来保证安全和去中心化，绝对可靠、可信；它能做到全球共识，并作为「加密法院」，通过智能合约设计的规则进行仲裁，以经济激励的形式将信任传递到 Layer 2 上。而 Layer 2 追求极致的性能，它只能做到局部共识，但是能够满足各类商业场景的需求。

如麻省理工学院媒体实验室数字货币计划（MITDCI）的负责人 Neha Narula 所讲，Layer2 的关键特征是“计算被移除至链下，以实现隐私或节省计算资源的目的”。如是，产生了由“区块链网络中的每台计算机执行特定程序的脚本”到“仅由交易中涉及的两台或多台计算机来实施”的一种转变。

Why Layer 2 ？

试图用一层区块链方案解决所有问题的人，往往没有思考过一个很重要的问题：公链虽能够达成全球共识，公共可验证，但是否所有的信息都需要让所有人验证、知道？我们之间的日常交易是否需要让全世界的人审核？

如果我不做违法的事情，当然不会介意，但是这显然没有必要。我们只需要将最关键的信息让所有人验证、获取保障就够了。而 Layer 2 恰好就能满足这样的需求：我们将大量工作放到链下（Off Chain），仅将最重要的内容提交 Layer 1 链上（On Chain）进行验证，并且 Layer 1 能够保证 Layer 2 的安全。

因此，我们提出最核心的两个观点：

· 不是所有的东西都需要全球共识

· 公链就该做它应该做的事情，其他的事情完全可以链下完成

那什么样的方案能够被称为 Layer 2 ？

· 首先，应用的主要工作都是在链下；

· 其次，仅用 Layer 1 作为安全的锚点，保证链下环境的安全；

· 最后，和 Layer 1 尽量保有同样的风险模型（很遗憾，跨链和侧链方案并不符合这一条，因为它们将资产在一条链上锁定在另一条链上释放，资产进入了另一个安全性完全不同的环境）

显然，这里 Layer 1 和 Layer 2 的安全等级是不一样的：

Layer 1 的安全性是由去中心化（Decentralized）保证，这意味一组无中心的节点取代了可信第三方的角色。在这里：1.被接受的交易就会按照规定执行；2.交易次序是确定的；3.双花是禁止的。

但是 Layer 2 的安全等级远小于此，它的安全性需要通过 Layer 1 来保证，因此只需要达到「去信任」（Trustless）：不保证交易在 Layer 2 上一定能够执行，但是能够保证若交易不被执行能够有一种方式让资产安全地从 Layer 2 撤回。

Layer 1 保障安全性和去中心化，Layer 2 来满足性能的需求，Layer 1 为 Layer 2 传递信任，这是未来加密经济的基础设施。

http://www.qukuaiwang.com.cn/news/15881.html

2.5.2. 跨链技术

区块链行业大家经常会聊起跨链，大概半年前有很多人认为跨链是个特别没意义或者太过超前的话题。不过随着公链项目增多，也有更多的跨链项目出现，显得这个问题更值得讨论了。已有的跨链项目有 Cosmos、Polkadot、Fusion、Iris、 ICON 、AION、RSK、Ripple 的 Interledger 等。

跨链是什么？

跨链简单来说就是信息从一条链到另外一条链。由于现在我们说起区块链，脑海中浮现的基本都是 token，所以其实更多的是作为资产的 token 从一条链去另外一条链。最容易理解的是拿 ETH 换 BTC，简单来说就是资产交换。

从互联网的角度理解，有点像信息从一个内网到另一个内网。这对于已经有了底层标准化传输协议互联网来说不成问题。可是区块链每一个网络都是一个相对封闭、且互不信任的系统，每发生一件事都要“投票”（共识）一下，怎么能轻易相信链外的东西呢？原来互联网上的各个后台信息都是可以相互传递，几乎无需验证。吕旭军认为，由于区块链的资产属性尤其明显，使得其跨链不同于传统互联网信息传递，参与者说谎的动机增强。

跨链有什么用？

跨链第一个“最痛”的应用场景就是去中心化交易所，解决了刚刚提到的第一个资产交换的问题。现在很多人用中心化交易所的方式也能解决，加上现行的去中心化交易所交易体验差、速度慢、还不能跨链交易，小白用户都不喜欢，看起来实在没什么戏。不过理想主义者会说：作为一个追求去中心化的行业，话语权最大的却是一大堆中心化的组织，大家觉得这实在太诡异了，而且中心化交易所作恶多端。

另外一种应用场景就是部署在 A 链上的应用支持其他链的 token。比如以太坊上的智能合约想用比特币支付——听到这个场景我的同事马上一脸懵逼地问：“为啥呀？”他这个反应也是对的，因为这个听起来貌似没有必要，但是有人就是希望支持比特币或者其他 token，希望扩大用户群。其实这个问题同样可以用中心化交易所解决。

这个问题也能泛化为，某个 DAPP 的不同模块可能部署在不同链上，那它怎么调用其他链上的模块、不同的模块之间怎么交互？也就是链 A 需要得知链 B 的才能进行下一步或者执行。说白了，这也还是可以用“链外”的方式解决，就像一个权威中介，这说起来很像预言机（提供链外可信数据）。

V 神 2016 年给 R3 写的那篇报告里提到提到了五个 use cases，都离不开以上三种，包括：1、资产（原子）交易（Payment-versus-payment or payment-versus-delivery - in technical circles, this concept is also often called "atomic swap"）；2、可转移的资产（Portable assets，资产可以多链之间来回转移和使用）；3、跨链数据预言机（Cross-chain oracles ）；4、资产留置或抵押（Asset encumbrance，某资产在链上被锁定，是否解锁取决于另一链上的结果）5、通用跨链合约（ General cross-chain contracts ）。

跨链的应用场景其实都能用链外方式解决。因此，我曾经跟 ArcBlock CEO 冒志鸿交流过，他就对 “双向锚定” 的跨链比较悲观，一方面两条链能 “互读” 的难度非常高，“interledger 就是建起桥梁，两条链的东西还得是一致的，但是两条链确实是不一样的”；一方面实际应用需求很少，“99% 都只需要应用级的跨链，只有很少需要 interledger 级别的跨链，比特币和以太坊为了安全性，可能要这种”。

这个判断，是他以 “数据库历史” 为鉴得出。他介绍，在 80、90 年代，曾经有一个概念叫联邦分布数据库，愿景是：两家企业用的数据库供应商不同，该技术希望数据库的角度让交易保证数据交易的原子性，难度极其高，但是后来证明在现实中根本不需要。“既然可以通过应用层保证一致性，为什么一定要在底层做呢？因此我们其实在整体设计上比较实用主义。”

怎么跨链？

其实不可能真正意义上某个币真的 “到了” 另外一个链上，大部分只是 B 链上生成了一个 A 链的锚定币，同时 A 链会将等值代币“锁定”。

如果以资产交换这个思路来理解，我理解跨链有三种的情况：

第一种是双方都不知道自己在跨链，或者说双方不能 “读” 对方，比如中心化交易所这种的。

第二种是其中一条链能读别的链，比如侧链 / 中继链的方式，就是 A 能读 B，B 不能读 A；如果一条 C 链能读到所有链，按理说也能成为一个 “链上” 中介，整个过程就是“A-C-B”。当一条 “侧链” 链接了很多主链时，它就变成一条中继链。

其中资产交换的过程可能是用户把 BTC 和 ETH“充值”到这个链上，各个代币在这个网络中都能流通（其实就是给每个币在这个跨链网络里都有一个锚定币，类似以太坊的 ERC 20），然后分别 “提现”。万维链和阿希链的模式有点像这种，他们能跟很多链交互，但是这些链之间不能直接交互。以阿希链为例说明：

用户将 BTC“充值”到阿希链上，需要先把 BTC 转到网关账户（就是比特币链上的一个普通账户，但是管理者是一组节点）；跨链网关收到信息以后锁定网关账户并验证，经过大多数节点验证后；网关会在阿希链上给用户解锁等值数字资产，用户即可在阿希链上使用 BTC。BTC 和 XAS 好像是两个国家的商人，双方不能互相信任而且使用不同的货币，无法直接交易。因此，双方协商了一套规则（相当于跨链网关协议）并且设立了一个专门的交易场所来处理交易，由本国有声

望的大商人（相当于网关节点）作为代表来共同管理，这些大商人还需要拥有足够数量的资产作为担保。

第三种是 A 和 B 都能读到对方的，这种理论上可以通过统一的协议实现，不过现在还没有类似协议落地。

说白了，链下也能做“跨链”；只是有人认为链上更安全。

结合万维链的看法，这里的安全可以拆解为两个问题：一是保证跨链信息是正确的，即如何验证原链上的交易状态。如果要考虑到使用 POW 机制的区块链上没有终局状态（始终存在分叉的情况，只是随着确认块的增加，概率逐渐变小），这个问题的复杂度会更高。二是是保证交易的原子性，即如果交易处理的某个环节停止，整个交易能够撤销；否则，部分成功的情况可能会导致双花。
https://www.odaily.com/post/5133506

目前主流的跨链技术包括：
1、公证人机制（Notary schemes）
2、侧链/中继（Sidechains/relays）
3、哈希锁定（Hash-locking）
不论对于公有链还是私有链来看，跨链技术就是实现价值互联网的关键，它是把区块链从分散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。
4、分布式私钥控制（Distributed private key control）

区块链中有哪些跨链技术？
https://36kr.com/p/5117175
跨链技术的分析和思考
https://learnblockchain.cn/2019/03/23/blockchain_interoperability/

2.5.3. 侧链技术

侧链（sidechain）的正式定义应该是“缠绕链”，负责缠绕对接“应用链”和“结算链”。这三者的关系是分层的，类似 IP、TCP、HTTP，这是三种不同的协议、不同的报文格式，只有小部分功能特征相似，但主要功能是分层次松耦合度的，各自为政，各自可以对各自透明。TCP 的 80 端口可以对接 HTTP，也可以对接其他应用。同理，这三种链也可以做到各自对各自透明，但是又可以对接协同工作。

侧链协议本质上是一种跨区块链解决方案。通过这种解决方案，可以实现数字资产从第一个区块链到第二个区块链的转移，又可以在稍后的时间点从第二个区块链安全返回到第一个区块链。其中第一个区块链通常被称为主区块链或者主链，每二个区块链则被称为侧链。最初，主链通常指的是比特币区块链，而现在主链可以是任何区块链。侧链协议被设想为一种允许数字资产在主链与侧链之间进行转移的方式，这种技术为开发区块链技术的新型应用和实验打开了一扇大门。

侧链最大的优势是可以让用户访问大量的新型服务。例如，你可以将比特币移动到另一个区块链上，从而利用相应区块链的隐私特性、更快的交易速度和智能合约。”

为了将侧链由概念转化成现实，Adam Back、Matt Corallo 等比特币核心开发者共同发起成立了 Blockstream 公司，并在同年十月，发布了白皮书《Enabling Blockchain Innovations with Pegged Sidechains》，首次明确提出了侧链的概念及其协议实现方案。

通过侧链，可以在主链的基础上，进行交易隐私保护技术、智能合约等新功能的添加，这样可以让用户访问大量的新型服务，并且对现有主链的工作并不造成影响。另外，侧链也提供了一种更安全的协议升级方式，当侧链发生灾难性的问题时，主链依然安然无恙。

侧链机制，简单的说，就是一种使货币在两条区块链间移动的机制。

实现方案

侧链实现的技术基础是双向锚定（Two-way Peg），通过双向锚定技术，可以实现暂时的将数字资产在主链中锁定，同时将等价的数字资产在侧链中释放，同样当等价的数字资产在侧链中被锁定的时候，主链的数字资产也可以被释放。双向锚定实现的最大难点是协议改造需兼容现有主链，也就是不能对现有主链的工作造成影响，其具体实现方式可以分为以下几类：

（一）单一托管模式
（二）联盟模式
单一托管模式与联盟模式的最大优点是它们不需要对现有的比特币协议进行任何的改变。

（三）SPV 模式

（四）驱动链模式

（五）混合模式

典型范例

目前，比较著名的侧链包括基于比特币网络的侧链 BTC Relay、Rootstock 的 Liquid，以及非比特币的侧链如 Lisk 和国内的 Asch 等。

BTC Relay 是由 ConsenSys 的推出的基于以太坊区块链的智能合约的侧链解决方案。BTC Relay 把以太坊网络与比特币网络以一种安全去中心化的方式连接起来。BTC Relay 通过使用以太坊的智能合约功能允许用户在以太坊区块链上验证比特币交易。以太坊 DApp 开发者可以从智能合约向 BTC Relay 进行 API 调用来验证比特币网络活动。

Liquid 是 Blockstream 的开源侧链项目，使用了比特币双向锚定技术，Liquid 目的是实现使得比特币可以在主链和侧链中互转，旨在提高隐私性、降低成本、加速交易所和经纪商之间的价值转移及结算流程。

Lisk 是一个致力于为 JavaScript 开发者提供创建分布式应用程序的区块链平台，由德国的 Max Kordek 和 Oliver Beddows 于 2016 年初成立。它把每一个分布式应用程序都会在其自己且独一无二的区块链，也就是侧链上运行，这种封装使得主要的 Lisk 的主网高效，迅速和精简 Asch 是国内推出的一个基于侧链技术的去中心化应用平台，由单青峰于 2016 年初成立。

Asch 平台提供的服务包括一个主链和一套应用软件开发工具包。Asch 的主链主要负责构建基础设施、应用间的数据共享以及资产路由，应用软件开发工具包内置了侧链协议，主要负责构建具体的应用，通过侧链协议可以与主链进行资产互通。

总结

侧链是以融合的方式实现加密货币金融生态的目标，而不是像其它数字资产一样排斥现有的系统。侧链技术进一步扩展了区块链技术的应用范围和创新空间，使传统区块链可以支持多种资产类型，以及小微支付、智能合约、安全处理机制、财产注册等，并可以增强区块链的隐私保护。利用侧链，我们可以轻松的建立各种智能化的应用如金融合约，股票、期货、衍生品等。

几点说明
1、比特币在侧链里流通时还是比特币，侧链的比特币与主链的比特币通常是 1 比 1 的汇率，也可能有预定的汇率。
2、侧链的挖矿不能产出比特币，侧链可能有自己的币，也可能没有自己的币，仅是为了比特币的流通。
3、侧链可能是对等的和非对等的。对等的侧链独立存在，其也可成为主链。主侧是相互的，如果有足够的需求，比特币也可成为莱特币的侧链。非对等侧链依赖主链而存在。
4、去中心化没改变，每个人或公司都可创建自己的比特币侧链，用户和矿工认同的会成为主流。
5、当然侧链要有足够的算力保证侧链的可靠和安全。
6、侧链白皮书提出了清晰的侧链框架，具体侧链怎么实现容许设计者自由发挥。

侧链可能实现的一些创意想法
1、滞留费
即长期不移动的币随着时间的推移将减值，减去的金额回馈矿工。
比如超过 1 年不动的币，每年减值 10%。
现在的比特币网络，时常有大户丢失密钥，相应的币也就丢了。
这将降低比特币经济体货币的充足性和流动性，被认为是比特币潜在的一个风险。
通过滞留费，鼓励货币流动，激励矿工，也可回收一些因丢失密钥丢掉的币。
2、新的挖矿所得约定
矿工的算力如果威胁到网络安全，将扣发挖矿所得。比如，算力超过 50%的矿工没有奖励，这样可约束矿工节制算力，防止 51%攻击。
3、挖矿所得延期支付约定。
现在，矿工挖到矿后立即得到奖励和交易费。这个约定把挖矿所得延期支付。 比如：在挖到矿的 100 个区块后支付挖矿所得。
这有助于激励矿工维护网络的正常运作。
4、定期可动用地址。

新增一种与时间有关的地址。只有到了特定的时间才可动用该地址的币。
比如人们可以把 10 个币发到这类型地址，设定 10 年后用。时间没到时，任何人，包括拥有者，也不能动里面的币。
全面理解区块链侧链技术
https://zhuanlan.zhihu.com/p/42769604

2.5.4. 闪电网络

闪电网络（英语：Lightning Network）是工作在区块链上（主要面向比特币）的第二层支付协议。 其设计目的是实现交易双方的即时交易，而区块链的交易频率则受限于其容量。闪电网络（Lightning Network）是一个去中心化的系统。闪电网络的卓越之处在于，无需信任对方以及第三方即可实现实时的、海量的交易网络。

闪电网络是基于微支付通道演进而来，创造性的设计出了两种类型的交易合约：序列到期可撤销合约 RSMC（Revocable Sequence Maturity Contract，哈希时间锁定合约 HTLC（Hashed Timelock Contract）。

RSMC 解决了通道中币单向流动问题，HTLC 解决了币跨节点传递的问题。这两个类型的交易组合构成了闪电网络。

什么是比特币的闪电网络？
https://www.zhihu.com/question/46515457

2.5.5. 分片技术

任何一个曾经开发过 DApp 的程序员都必须考虑到当前公共区块链的局限性，其中区块链局限性的最重要和最明显的问题就是有限的吞吐量，比如，每秒处理的交易量过少。为了运行一个能够处理实际吞吐量需求的 DApp，区块链就必须具有可扩展性。

进行区块链扩容的一个答案就是分片技术（Sharding）。分片技术承诺通过改变网络验证的方式来增加吞吐量。分片技术独特于其他解决扩容的链上技术的关键特性，就是它可以进行水平扩容，也就是说，网络的吞吐量随着挖矿网络的扩展而增加。这种特殊的特性可能使它成为推动区块链技术被快速采用的理想技术。

分片技术（sharding）——区块链扩容问题的良方

https://www.8btc.com/article/179733

2.5.6. 其他

2.6. 根据具体业务项目简介

2.6.1. 货币及支付结算属性

2.6.1.1. BTC

比特币（Bitcoin，缩写 BTC）是一种总量恒定 2100 万的数字货币，和互联网一样具有去中心化、全球化、匿名性等特性。向地球另一端转账比特币，就像发送电子邮件一样简单，低成本，无任何限制。比特币因此被用于跨境贸易、支付、汇款等领域。

比特币由于广阔的前景和巨大的遐想空间，自 2009 年诞生后价格持续上涨，2011 年币价达到 1 美元，2013 年最高达到 1200 美元，超过 1 盎司黄金价格，有“数字黄金”的美称。

比特币始于 2008 年神秘人物中本聪（Satoshi Nakamoto）的论文《比特币：一种点对点的电子现金系统（中文版）》。在诞生后的六年里，比特币作为一种前所未有的新型货币，经历了无数的市场考验和技术攻击，始终屹立不倒。现在比特币已成长为一个在全球有着数百万用户，数万商家接受付款，市值最高达百亿美元的货币系统。

比特币相关企业也吸引了来自上百家著名风险投资基金、公司、个人近十亿美元的风险股权投资，其中不乏传统金融巨头，例如：

Visa、纳斯达克、花旗：《Visa，纳斯达克等巨头投资区块链公司 Chain 3000 万美元》；

万事达卡（MasterCard）：《万事达卡、纽约人寿保险加入数字货币集团新一轮融资》；

高盛、IDG 资本：《比特币公司 Circle 获 5000 万美元融资》；

PayPal 联合创始人，eBay 联合创始人、高通：《初创比特币公司 21 获 1.16 亿美元巨额融资》；

纽约证券交易所（NYSE）：《Coinbase 正式完成 7500 万美元 C 轮融资》；

雅虎创始人杨致远、李嘉诚旗下风投：《比特币商业交易平台 BitPay 融资 3000 万美元，估值达 1.6 亿美元》等等。

亦有部分风投资金直接购买了比特币，例如在美国 FBI 对暗网黑市缴获比特币的拍卖中，硅谷最知名的投资人之一 Tim Draper（百度，Hotmail，Skype，特斯拉的领投人）斥资 2000 万美元购买了 3.2 万个比特币，美国的比特币投资信托基金（Bitcoin Investment Trust）购买了 4.8 万个比特币等等。（网易新闻《三匿名竞标者拍走“丝绸之路”五万比特币》）

比特币是什么？
https://www.zhihu.com/question/22076666

2.6.1.2. XRP

瑞波币是 Ripple 网络的基础货币，它可以在整个 ripple 网络中流通，总数量为 1000 亿，并且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）。

瑞波币是 ripple 系统中唯一的通用货币，其不同于 ripple 系统中的其他货币，其他货币比如 CNY、USD 不能跨网关提现的，换句话说，A 网关发行的 CNY 只能在 A 网关提现，若想在 B 网关提现，必须通过 ripple 系统的挂单功能转化为 B 网关的 CNY 才可以到 B 网关提现。而瑞波币完全没有这方面的限制，它在 ripple 系统内是通用的。

2018 年 1 月 1 日，瑞波币（ripple）交易价格在上周五暴涨近 56%，创历史新高，市值一举超越以太币，成为第二大加密货币[1] 。

Ripple（瑞波）的出现让货币在全球范围内的流通变得更加简单方便了。但不同的是，比特币是一种虚拟货币，而 Ripple 是一种互联网交易协议，它允许人们用任意一种货币进行支付。例如，甲方可以利用 Ripple 以美元支付，而乙方则可以通过 Ripple 直接收取欧元 [2] 。

位于旧金山的 Ripple Labs 是一家初创公司，正致力于推动 Ripple 成为世界范围内各大银行通用的标准交易协议，使货币转账能像发电子邮件那样成本低廉、方便快捷。

同比特币一样，Ripple 也是一种可共享的公共数据库，同时它也是全球性的收支总账。共识机制允许 Ripple 网络中的所有计算机在几秒钟内自动接受对总账信息的更新，而无需经由中央数据交换中心。这种处理速度是 Ripple 在工程学方面的一次重大突破。它意味着 Ripple 的交易确认时间仅为 3 ～ 5 秒，而比特币则需要 40 分钟。

瑞波币
https://baike.baidu.com/item/%E7%91%9E%E6%B3%A2%E5%B8%81/4956309?fromtitle=ripple&fromid=6901044

起底 XRP 瑞波币，它到底值不值得投资

https://zhuanlan.zhihu.com/p/41919923

2.6.1.3. 匿名币

2.6.1.3.1. 什么是匿名币

匿名币是加密货币的演变，例如比特币。比特币交易是匿名的，因为每个钱包的所有者是未知的，但每个交易都是公开广播的，可以在公共分类账上查看。这意味着可以查看和查看给定钱包的所有事务。因此，如果一个人的真实世界身份与比特币钱包地址相关联，则匿名性会受到影响。
与比特币一样，大多数匿名币使用公共分类账进行交易，但使用各种方法来模糊交易的发送方和接收方。领先的匿名币实现了针对此问题的不同解决方案，但主要内容是封闭了给定事务的发送方和接收方之间的链接，这阻止了活动跟踪钱包地址。

为什么要使用匿名币？

为什么需要匿名币？如上所述，公共分类帐是透明的，并显示给定钱包的持有和活动。在许多情况下，这不是问题，也不需要解决方案。但是，随着继续使用比特币，很容易想象未来更多的钱包地址与真实身份和隐私相关联。例如，公司与制造商和供应商进行贸易，并且在产品发布之前不愿向公众广播。此外，如果他们的钱包地址与其真实身份相关联，则比特币“富名单”（具有最多资产的钱包列表）上的大持有者可能会关注其安全性。匿名硬币旨在解决这些问题，并以分散和可扩展的方式授予交易匿名性。

2.6.1.3.2. XMR

门罗币 Monero（XMR）
门罗被设计为一种私人的，无法跟踪的货币。在门罗上，交易和交易金额中涉及的地址（包括发件人和收件人）在分类账上是私有的，这意味着钱包的余额也是私有的。门罗使用称为环签名的方法实现交易隐私（首次使用于 2017 年 1 月，并授权 2017 年 9 月之后的所有交易），这是环签名的演变。如果区块链上没有地址和余额，商家和个人可以隐藏他们的净资产。

RingCT（环形签名）：门罗链以三种方式保护隐私。环签名允许发件人隐藏在其他事务输出中，不可见地址隐藏事务的接收地址，并且 RingCT 隐藏事务量。因此，门罗具有不透明的区块链。这与比特币使用的透明且可追踪的区块链形成对比。因此，门罗被称为“私有，可选透明”。

2.6.1.3.3. DASH

达世币 Dash

达世基于 PoW 工作量证明共识机制，系统在网络中使用两种类型的节点; “主节点”和“矿工”。主节点提供即时发送和私有发送。即时传递允许主节点在一秒钟内达成共识，从而导致不可逆转的交易。 “私密发送”使用硬币技术来屏蔽给定事务钱包的发送者和接收者。由于网络是工作量的证明，因此还有挖掘节点计算哈希值以保护加密的达世区块链。区块奖励分为三组，其中 45％用于矿工，45％用于大师，10％用于基金会。为了继续开发和营销业务，达世将支付“冻结税”。达世依赖主节点发送匿名事务，但不需要这种类型的事务。与门罗不同，可以在区块链上看到地址和持有量，并且可以审核未使用匿名发送执行的交易。

2.6.1.3.4. GRIN

提到 Grin，首先要提到它的底层协议 MimbleWimble。MimbleWimble 出自于《哈利波特》中的一句咒语，目的是让被施咒人不再能开口说话。

MimbleWimble 在交易结构的设计上体现了一个关键原则，即强大的隐私性和保密性。
MimbleWimble 的交易确认依赖于两个基本属性：第一是零和验证，即输出总和减去输入总和总是等于零，证明交易没有凭空创造新的资金，而且不会显示实际金额；第二是拥有私钥即拥有交易输出的所有权，在 MimbleWimble 中，证明一个所有者拥有这些私钥并不是直接通过签署交易来实现的。

Grin 则是基于 MimbleWimble 协议的开源软件项目，有以下主要目的和特性：

1、隐私保护的缺省特性。这使它具备了完全可替代性，且保留了按需选择性披露信息的能力。

2、区块大小与交易量相适配。历史交易仅仅保留了约 100 字节的交易核，相比其他区块链节省了大量空间。

3、强大且经过验证的密码学。MimbleWimble 只采用椭圆曲线密码，该密码技术已经经过了数十年的试用和测试。

4、简单的设计使得日后的代码审查和维护变得容易。

5、社区驱动。采用一种抗拒 ASIC 的挖矿算法（Cuckoo Cycle 算法），借此来鼓励去中心化的挖矿。

6、社区未被任何机构、个人控制或入股，开发团队仅接受捐赠。

新一代隐私币 Grin 是「何方妖孽」？MimbleWimble 协议或成新机会？

https://www.chainnews.com/articles/834353144938.htm
匿名币是 2019 年热点？简评三大匿名币，谁的综合实力更强？

https://www.chainnews.com/articles/674550648500.htm

2.6.1.4. 稳定币

2.6.1.4.1. 什么是稳定币

如果想要推广加密货币在日常生活中的应用，币值稳定非常重要，这也是稳定币诞生的现实基础，只有做到了币值稳定，基于区块链的贷款、金融衍生产品、预测市场等应用才能实现。
由于加密货币在全球各国跨境流通，那么保持币值稳定，一个稳定币需要满足以下特点：1、价格稳定；2、可扩展性；3、隐私保护；4、弱中心化。
为了达到这些特点，目前有若干种尝试方法。
第一种方法是中心化资产抵押发行代币，例如 Tether（USDT）。
针对 USDT 的种种弱点，TrueUSD（TUSD）提出了第二种稳定方式，是对于第一种方式的改善。TUSD 保证完全美元储备以提供定期审计；其次 TUSD 实行严格的 KYC、AML 验证；独立托管，不由该项目团队经手资金。
第三种方式就是超额抵押线上资产，例如 Bitshares、Maker 等，这些“稳定币”所抵押的资产本身就在链上，一般要求抵押物的总价值要高于所创造出的稳定币，即超额抵押。

稳定币是什么？

https://www.jinse.com/news/bitcoin/240521.html
关于稳定币，你想知道的一切

https://36kr.com/p/5154797

2.6.1.4.2. USDT

Tether USD（简称 USDT），中文名称为泰达币。发行 USDT 的 Tether 公司，原名 Realcoin，注册地为马恩岛和香港。2014 年，Realcoin 公司更名为 Tether。2015 年，Tether 公司发行的 Tether 在交易平台 bitfinex 和 Poloniex 上线，此后又在更多的大型交易平台上线。

数字货币 USDT (Tether)是什么？有什么用？
https://www.zhihu.com/question/68045424

2.6.1.4.3. PAX

2018 年 9 月 10 日，纽约金融服务部（NYDFS）同时批准了两种基于以太坊发行的稳定币，分别是 Gemini 公司发行的稳定币 Gemini Dollar（以下简称 GUSD），与 Paxos 公司发行的稳定币 Paxos Standard（以下简称 PAX），每个代币有 1 美元支撑，旨在提高法币的稳定性，以及加密货币的速度和无国界性质。
PAX 币（Paxos Standard）是全球首个合规的稳定币，由区块链创业公司 Paxos 发行，PAX 旨在通过提供“现金的数字替代品”来为交易加密资产的投资者提供流动性，用于所有资产类别的即时交易结算。

PAX 是一款以 1:1 美元为支持的稳定币，1PAX 等于 1 美元，PAX 全部储备将按全额持有的美元进行 100%抵押。PAX 基于以太坊的 ERC-20 标准构建，可以在以太坊网络上的任何两个钱包之间发送，经过验证的 Paxos 客户可以在其公司网站上购买或兑换 PAX。
GUSD 和 PAX 其实只是两种官方加持的“稳定币”，受官方监管，并不是官方发行。对于投资者来说，稳定币的意义在于避险，特别是在市场趋势不明的背景下，持有稳定币能规避波动风险。
GUSD 和 PAX 这两种稳定币则具有其他的价值，它们的出现要比其存在更具意义，这标志着数字美元的成形又向前迈进了一大步。
新稳定币 GUSD 和 PAX 是什么币？

http://www.wangrunyu.com/jiaocheng/93.html

2.6.1.4.4. USDC

USDCoin（USDC）由 CIRCLE 发行，是一个完全抵押美元的稳定币，并基于 CENTER 开发的开源法币稳定币框架。 项目简介：USDCoin (USDC)是一个完全可抵押的对标美元的稳定币，它提供详细的财务和运营透明度，并在美国货币流通法的框架内运行，而且跟多家银行机构和审计团队合作。
关于 USDC，看这一篇就够了

NYLife360.com, Tel: 929-633-1888, VX：NYLife360

https://bihu.com/article/1909971649

2.6.1.4.5. 其他

2.6.2. 借贷

2.6.2.1. 中心化借贷

中心化与去中心化借贷孰强？一文读透加密货币借贷行业

https://www.chainnews.com/articles/638121155675.htm

2.6.2.1.1. 中心化借贷模式种类

2.6.2.1.2. Celsius

Celsius，一个来自美国的项目，目的是构建一个真正意义上的 P2P 去中心化借贷平台，打造区块链版蚂蚁金服。Celsius 制作了一款自己的区块链钱包，用户在此钱包内的区块链资产都可以直接便捷地得到利息（最高年化 9%），Celsius 相当于美国的区块链版本蚂蚁金服。机构投资者可以向 Celsius 贷款进行一系列的金融活动，并且其所缴利息远低于华尔街金融借贷产品，非常有吸引力。

Miao 说项目解读：区块链版蚂蚁金服 Celsius

https://www.linksfin.com/article/51485

2.6.2.1.3. CRED

简介
Cred（LBA)由前 PayPal 技术和金融团队创立，是全球领先的区块链资产金融服务平台，可随时随地为用户提供快捷便利的信贷服务。Cred（LBA）利用去中心化智能合约技术，为借款人提供灵活的贷款选择，其中包括加密 token 和法定货币。Cred（LBA）旨在通过一个已建立的全球借贷网络、多元化的核心团队以及区块链技术的力量，为金融服务行业带来革命性的变化，致力于成为区块链资产金融服务领域的领导者。

项目特点
CRED 是一个去中心化的借贷生态系统，基于由 CRED 基金开发的以太坊区块链技术为基础，随时随地开放信贷。CRED 将于 2018 年 7 月推出，其行业领先的信贷管理能力和四个独特的合作关系网络构成了世界一流的贷款生态系统，其中包括：

- 内部专有的基于 AI 的信用模式;

- 客户获取和电子钱包合作伙伴关系推动采用;

- 贷款人与稳定币合作关系推动流动性;

- 广泛的 Exchange 合作伙伴网络可最大限度地减少违约

- 身份验证合作伙伴网络可加快 KYC 和验证流程。

Cred/LBA
https://www.dprating.com/project/136

2.6.2.1.4. Nexo

由于我们日常生活中仍然需要使用法定货币。这意味着，在需要时我们得把加密货币换成法币。但加密货币持有者出于投机需求、纳税以及提现到账周期等情况不太愿意将加密货币换成法币。为加密用户解决这些问题是 Nexo 项目的初衷。Nexo 通过在线即时为加密货币持有者提供贷款能让用户很便捷的获得流动性，简化税收的同时无需牺牲出售其部分资产潜在收益。

Nexo 是一个旨在为用户提供即时加密贷款的金融科技应用程序。该平台由 Credissimo 提供支持，Credissimo 是一家领先的金融科技集团，过去十年来一直为欧洲数百万客户提供服务。

Nexo 加密贷款平台的技术解决方案叫 Nexo Oracle 。Nexo Oracle 是一个可以实时进行资产监控、贷款设置、还款分析、自动通知、数据分析和钱包维护的独立系统。

在 Nexo 上使用加密货币贷款，首先需要将加密资产转移到 Nexo 钱包。一旦钱包收到加密资产，Nexo Oracle 就会根据用户钱包持有的加密货币的市场价值自动计算客户的贷款限额。然后，贷款将立即通过银行转账或免费的 Nexo 信用卡提供给用户。Nexo 无需信用审查，贷款金额完全由用户 Nexo 钱包中持有的加密资产作担保。

偿还贷款时，用户可以通过银行转账以法币偿还（目前支持美元，欧元和日元），通过 NEXO 代币偿还贷款（可获得利率折扣），通过销售 Nexo 钱包中部分加密资产来偿还。目前这些偿还方式 Nexo Oracle 都支持。如果逾期未还款，Nexo 可以按照贷款合同的约定获得存储在用户 Nexo 钱包中的加密货币。

Nexo 的代币 NEXO

NEXO 代币是首个符合美国证券交易委员会标准、支付股息、资产支持并具有额外的实用功能的安全代币。“支付股息”对投资者来说就是 Nexo 贷款利息的 30％将直接与 NEXO 代币持有人共享。“符合美国证券交易委员会标准”意味着 Nexo 不会成为监管的牺牲品。

NEXO 的两个实用功能是：

- 降低使用 NEXO 代币偿还贷款的客户的利率。

- NEXO 代币可存放于 Nexo 钱包，根据其价值和利率折扣获得即时融资。

深度分析 Nexo 项目

https://zhuanlan.zhihu.com/p/51001253

2.6.2.2. 去中心化借贷

去中心化贷款产品对任何人、任何地方都可用，而且只需要一个以太钱包即可使用。这些产品今天已经看到了实际的使用，总金额达数亿美元。

实际用例

贷款

借款
抵押借款

一文看懂去中心化借贷

https://www.chainnews.com/articles/076735240429.htm

最为有名的四个去中心化贷款协议分别为 Compound、Dharma、dYdX 和 MakerDAO，我们将其归纳为三种模式：

（1） P2P 撮合模式

Dharma 和 dYdX 都是撮合借方和贷方的点对点协议。因此，基于这两个协议的贷款和借款数量是相等的。

如，Dharma 中由智能合约充当“担保方”角色，评估借方的资产价格和风险。债权人则根据“担保方”提供的评估结果决定是否贷款给借款人，同时当借款人无法按时还款时，“担保方”自动执行清算程序。Dharma 平台的借款期限最长为 90 天，贷款利息是固定的。贷款人在放贷期间资金被锁定，只有在与借款人匹配后才开始赚取利息。

dYdX 协议也是 P2P 模式，但它与其他借贷平台之间的主要区别是，dYdX 也支持除了借入借出之外的其他交易，如期货交易。交易者在 dYdX 开仓时，会借入保证金，并与贷方通过平台就条

款协议达成一致，进行保证金交易。所以 dYdX 的目标客户主要是保证金交易商。dYdX 平台的利息是可变的，用户在 dYdX 上贷款时没有锁定期或最长期限。

（2） 稳定币模式

这一模式的典型是 MakerDAO，没有贷方只有借方，且唯一可借入的资产是 DAI。借款人通过抵押数字资产（现为 ETH）借入新创造的 DAI。DAI 是 MakerDAO 平台发行的、与美元挂钩的稳定币。质押资产和借款的质押比率必须保持在 150% 以上。而其利息是全球性的，由 MKR 持有者通过投票来决定。利息并不稳定，曾在一个多月的时间里从 2.5% 上升到 19.5%。

（3）流动池交易

以 Compound 为例，借方和贷方通过流动性交易池进行交易，而不是与交易对手进行匹配。每个贷款和借款的利率由池子的流动性大小来确定，即由贷方提供的货币总数量和借方的需求总数量之间的比率而波动。Compound 不设置固定的贷款期限，贷款人可以把资金存入贷款池子持续赚取利息，并随时提取资产。借款人有无限的合约期。

2.6.2.2.1. 什么是 DeFin，去中心化借贷模式种类

我们命名叫 DeFin 而不是 DeFi，是因为区块链是大数据和 IT 技术的结合，叫金融科技更准确些。所以我们把 DeFi 改为 Decentralized Fintech 的 DeFin。

关于 DeFin 的构想，总的来说会从四个方面来展开：对传统金融体系的解构；金融体系在区块链上面的重构；之后对重构后的区块链上协议和应用层进行分解和解释。
DeFi 有点过时，我们来谈 DeFin，看去中心化金融科技如何重构传统金融

https://www.chainnews.com/articles/082367895378.htm

2.6.2.2.2. MakerDao

MakerDAO

MakerDAO 是目前可用的最复杂且使用最广泛的去中心化借贷平台。MakerDAO 是 DAI 的创建者，DAI 是一种目标价格为 1 美元的加密货币 (称为稳定货币)。

NYLife360.com, Tel: 929-633-1888, VX：NYLife360

Dai: 生成机制

Maker 是以太坊上的智能合约体系，提供了第一个去中心化的基础稳定货币 Dai（可简单理解成以太坊上的美元）和衍生金融体系。Dai 是通过数字资产足额抵押担保发行，1 Dai = 1 美元。自 2017 年上线以来，Dai 始终和美元保持锚定。

关于 Dai，一个最常见的问题是：Dai 与 USDT 有什么区别？

USDT 能做的事情 Dai 都可以做，很多 Dai 能做的事情 USDT 做不了。我曾写过一篇文章，详细介绍了 USDT 和类似稳定币的风险与局限，与 USDT 相比，Dai 除了公开审计、完全透明、去中心化之外，还给与了用户和机构新的价值。

除了可以作为交易所的基础货币避险资产之外，Dai 可以用作抵押贷款，有人通过 Dai 款买了车，开了咖啡店。

深入浅出理解 MakerDAO: 不止于稳定币

https://zhuanlan.zhihu.com/p/41889079

2.6.2.2.3. Compound

Compound 是一个开放协议，想要实现数字资产的借贷。它想让你在区块链世界里更容易借钱。但在区块链上实现借贷有两个主要的问题：

1. 现有的借贷机制极其有限，所以很容易导致资产的错误定价。（比如很多的垃圾币有很高的市值，因为没有渠道可以做空它们。）
2. 区块链资产有可能产生负净值，因为有链上存储的成本，也有交易的风险（不论是场内交易还是场外交易）。我们没有一套很自然的利率机制可以抵消这些成本，这样就会让资产具有挥发性，因为「持有」并不产生「激励」。

中心化的交易所提供一些保证金交易，但需要你信任中心化机构，同时对可借贷的资产类型也有很大的限制，通常只有一些主流的币种。同时，这种中心化的方式无法在链上做借贷，这样对于智能合约来说，就没办法接入这套机制了。

而另外一些点对点协议的做法也存在一些问题，包括 ETHLend, Ripio, Lendroid, dYdX 等等。 这些协议为用户提供抵押或非抵押的借贷，但去中心化导致了用户需要承担很高的成本和很不友好

的用户体验——比如，出借人需要自己发布、管理、监督借贷交易，这样借贷的过程往往需要很长的时间异步进行（因为需要花时间筹集借贷资金）。

Compound 想要提供另一种不同的借贷协议，让整个链上的体验和流程变得更简单、更流畅。

去中心化的货币市场：Compound 是怎样用区块链重构「借钱」这件事的？
https://orange.xyz/p/326

2.6.2.2.4. Dharma

Dharma 达摩的概念跟众筹相同。如果说 ICO 是针对股权的，那么 IDO （首次债务发行）是针对债券的。
首先，达摩（Dharma）是运行在 0x 协议上的，在去中心化方面达到任何 DEX 的水平。它是一个发行、资助、管理、交易不可互换债务代币的平台。在这里不要误解不可互换的意思。—— 它不是说它不能轻易进行交易。它是说不能兑换为另外的代币或资产，直到它成熟。
达摩（Dharma）的优势

- 低成本和透明的债务发行；
- 消除当前贷款处理系统的低效率；
- 在它发行的同一平台上交易代币化债务更容易；
- 以风险定义的利率来进行放贷和借款。

达摩（Dharma）的弱点

- 无法保证承销商在评估贷款风险方面的专业性；
- 缺乏对贷方和借方的声誉整合；
- 由于没有法律追索权，这对于承销商和贷方来说，如没有担保贷款风险会很高。借款人必须有一些抵押品，便于提升贷方的信心。

详解运行在 0x 协议上的去中心化借贷平台 Dharma Protocol

https://www.chainnews.com/articles/518997646902.htm

2.6.3. 中心化交易所

2.6.3.1. 中心化交易所的分类，优势，及问题

中心化交易所的交易过程：钱包→交易所给的地址→交易所总地址→撮合交易→钱包 交易所总地址币值高，受到黑客攻击的可能性大。

去中心化交易所的交易过程：钱包→交易所注册地址→撮合交易→钱包 没有交易所总地址，受到攻击的可能性很小，整个过程用户拥有掌控权。

中心化交易所的优点和缺点

优点：体验较好，效率高。 钱包充值到交易所给的地址以后，自动的转入到了交易所的总地址，然后用户发出指令，交易所进行撮合交易，整个工程中只要订单达到一定数量以后，撮合交易的效率更高。

缺点：安全性令人担忧，缺乏信任和透明 。中心化交易所最为大家担心的就是被盗或者是跑路，跑路在大平台存在的可能性比较低，但是被盗风险都是比较高的，因为大平台的总地址上的币值是比较大的，所以面临的被盗的风险自然而然就更大的，近年来也是发生了很多交易所被盗币的事件，或者公司内部人员监守自盗，或者是遭到黑客的攻击，导致币的损失。另一个令人担忧的问题就是交易所存在的一些暗箱操作，比如某期货平台专业爆仓，某安平台专业做空，某币平台专业宕机等，这个都是令用户担心的问题。

去中心化的交易所的优点和缺点

优点：安全透明，隐私得到保障。交易的过程是匿名的，用户的隐私得到了很好的保障。安全性也有很大的提高，每个用户都有一个独立的交易地址，黑客攻击基本上不存在，也不会出现密钥被盗的问题，因为都掌握在用户自己的手中，但是一旦用户丢失密钥的话是无法找回的。

缺点：交易速度慢，往往需要花费很长的确认时间和撮合时间。用户的交易过程是以区块交易来驱动的，受到区块确认速度的影响，目前以太坊交易确认的时间是几十秒，这对于用户体验是很不好的影响。其次目前的去中心化交易所并不能处理大量的实时交易，所以在交易深度上是比不上中心化的交易所的，这就会加长交易的撮合时间。

2.6.3.2. 集合进价交易所：Binance， Coinbase Pro，Huobi

（币安）binance.com，是由赵长鹏（CZ）领导一群数字资产爱好者，创建的一个专注区块链资产的交易平台。特点：国内早期的币币交易网，拥有海量的用户。

与其他平台相比，币安在下面几个地方做的不错：

1、交易稳定流畅

2、支持七种语言，国际化程度高

3、多平台覆盖，独有 PC 客户端

4、创新的 Binance Labs，在币安的规划里，币安并不仅仅是一个交易平台，还有媒体平台，区块链项目孵化平台等。

四、狼性运营

1、在币种上，广泛迎合用户需求，力争早上快上

2、在交易上，频繁举办交易比赛，还豁免 BNB 区交易手续费

3、在邀请上，20%手续费实时分成，充分发动群众的力量

4、在福利上，不会让用户错过任何一种福利

关于币安你知道多少？
https://www.zhihu.com/question/62883228

Coinbase Pro 是 Coinbase 的在线交易平台扩展，可能是在线购买比特币和以太坊最著名的地方。它是一家总部位于美国且受监管的交易所，为在线最大的加密货币提供多种交易对。纽约证券交易所，Andersen Horowitz，联合 Square 风险投资公司等一些严肃的智能资金支持。

专业的交易平台称为 Coinbase Pro（以前称为 GDAX），而基本交易平台简称为 Coinbase。

Coinbase Pro 与 Binance：哪一个更好？

https://0xzx.com/20190314110613730.html

80 亿估值的 Coinbase 与 CoinbasePro 有啥差别？

https://www.tuoluocaijing.cn/article/detail-16228.html

火币网于 2013 年 9 月由李林创办，是中国最大[4][5]的数字资产交易平台与数字资产金融服务商[6][7]。目前，火币网已完成对新加坡、美国、日本、韩国、香港等多个国家及地区的布局[8]。火币网先后获得真格基金、红杉资本的战略投资[9]。

火币百科
http://xiuxiubaike.com/huobipro

2.6.3.3. 拍卖(Call-Auction) 交易所：Coinbase

Coinbase 已经获得美国政府许可开展代币交易，目前，其能够提供比特币、以太币、莱特币以及比特现金的交易。相对于上百种的代币，Coinbase 仅提供比特币、以太币以及莱特币的交易，这也为明确了平台的主要客户群体。按照目前的情况分析，Coinbase 很可能申请比特币、以太币以及莱特币的衍生代币品种。

交易所介绍——Coinbase

https://zhuanlan.zhihu.com/p/33273211

2.6.3.4. 合约交易所：BitMex， OKex

BitMEX 算是非常老牌的比特币期货合约交易平台了，杠杆倍数是最大特色，适合赌徒以最快的速度亏完本金。
比特币期货市场有好几个，我推荐 2014 年成立的 BitMEX 交易所。它的期货交易量稳居全球第一，市场深度大，交易手续费低，安全措施到位。
注册 BitMEX 账号比起很多交易所都方便。首先访问 https://www.bitmex.com/register/69hdRL（身在国内的用户需翻墙）。

BitMEX 期货交易指南：入门篇

https://zhuanlan.zhihu.com/p/31805571

OKCoin 和 OKex，其中 OKCoin 包括.cn 和.com，分别代表了国内（目前已停止运营）和国际的交易。OKCoin 一开始是面对中国大陆用户的交易平台。在九四事件之后，由于所有国内的交易平台都被清退，很多交易所都纷纷出海，或者把服务器迁至境外,或者在境外注册公司等方式，规避中国对于虚拟货币交易的监管。OKEX 也就成为了 OKCoin 的替身。品牌升级后，官方宣称 OKCoin 国际站和 OKEX 账户实现了永久分离，两个平台独立进行充值和提现。
okex 是什么交易平台？okex 交易所靠谱吗？

http://www.528btc.com/college/48096.html

2.6.3.5. OTC 交易

场外交易市场(Over-the-Counter)也叫做柜台交易市场或简称 OTC 市场，通指在交易所场外进行的交易。OTC 市场最早起源于 20 世纪初美国的证券市场，那时候美国已经有很多不在证券交易所进行交易的有价证券，投资者通过银行或券商的柜台买卖这些证券，柜台交易因此而得名。

场外交易(OTC)市场介绍

https://www.cmegroup.com/cn-s/trading/otc/

2.6.3.6. 挖矿交易所

交易即挖矿”这种模式其实是模仿 BTC 挖矿的分配规则。一定比例的平台代币通过“交易即挖矿”的方式逐步回馈给交易用户，该比例全部回馈完成，“挖矿”即自动终止。简单来说，“交易即挖矿”是一种平台对用户的交易手续费返还机制。

讲交易挖矿，先讲讲“矿”，所谓“矿”就是各大交易所的平台代币，早前随着币安的 BNB 百倍升值，在数字货币市场平台代币可以说是一路上扬，一时成为币圈的热点。那么什么是平台代币？

平台币由数字资产交易平台官方发行的平台数字资产。简单来说，就是各交易所发行的自家币，比如，BTBTOP 发行的平台币 EBC，Fcoin 的 FT，币安发行的平台币 BNB，火币发行的平台币 HT。而这些平台币就是交易即挖矿中的“矿”

交易挖矿 TOP1 代表——FCoin

交易即挖矿小而美代表——BTBTOP

加盟模式-OKEX

交易即挖矿是什么？盘点交易挖矿平台

https://www.jinse.com/bitcoin/231598.html

2.6.4. DEX

2.6.4.1. 什么是 DEX，和中心化交易所相比的优势和存在的问题

去中心化交易所(DEX)，最常見和比較多人使用的去中心化交易所，包括 EtherDelta、IDEX、OpenLedger DEX 等。

交易所使用去中心化的方式可以避免许多用户的资产卷入因入侵者带来的危险而引发的问题。去中心化交易所不需要用户将他们的钱信托与交易所:用户的钱包并不受单一实体所操控。订单由用户本人直接数字签名，以此作为授权程序。用户可以掌控自己的资金，但是链上交易有个弊处，就是无法像中心化交易所那样实时交易。

https://docs.wavesplatform.com/zh/platform-features/decentralized-cryptocurrency-exchange-dex.html

2.6.4.2. Binance DEX

Binance DEX 既承载了币圈人对 BNB 市值的期待，也寄托了链圈人对区块链技术落地的希望。在此之前，币安平台币 BNB 陆续突破多个阻力位，很多人认为币安 DEX 及其它所在的币安链（Binance Chain）是主要推力。对于二者，币安创始人赵长鹏也曾表示，币安链能够实现每秒产生一个区块，DEX 的 TPS 达到每秒数千笔。
币安去中心化交易所 Binance DEX 初体验

https://www.chainnews.com/articles/211700481176.htm

2.6.4.3. Kyber network

Kyber Network 是一个以太坊区块链平台，它是新加坡项目，由 Loi Luu、 Yaron Velner 和 Victor Tran 联合创建。 Kyber Network 还是一个 P2P 的去中心化加密货币交易所。 它拥有较深的加密储备池，为网络提供了巨大的流动性，并能够以极低的转换率进行快速交易。此交易所的代币被称为“Kyber Network Crystal”（简称 KNC 币）。KNC 币是私有的 ERC-20 加密货币代币。
此外，Kyber Network 提供四种服务，即：

1. 储备实体——他们提供流动资产。此功能可确保网络上代币交易的顺利。它允许两种实体注册，即公共注册和私人注册。
2. 储备贡献者——只有当储备实体公开时，储备贡献者才与其他贡献者共同使用其储备利润。
3. 储备管理者——他们是 Kyber network 的会计师。他们负责估算并计算交易所的汇率，并保持储备金。
4. Kyber Network 运营商——它负责 Kyber Network 的运营。它检查、验证和通过储备实体，列出可交易的代币，并确保 Kyber Network 的所有运营都处于一个安全的环境中。

关于 Kyber，你需要知道的事

https://www.chainnews.com/articles/117674150404.htm

2.6.4.4. Airswap

AirSwap 是以太坊上的去中心化交易协议，提供基于点对点交易的去中心化解决方案。主要通过交易者索引机制、定价机制以及具有交易结算功能的智能合约这三个核心服务内容，帮助促成 ERC20 通证间交易。优势在于通过连接交易商克服其他去中心化交易平台的前端运行问题;劣势在于匿名用户可能违反 KYC 和反洗钱规则，而且目前没有看到相关风险预警和防范措施。

AST(Airswap)是什么币？AST 币总量、官网及白皮书介绍
http://www.120btc.com/baike/coin/356.html
https://www.huobiinfo.com/news/baseDetail_51173/

2.6.4.5. 其他

2.6.5. 平台币

2.6.5.1. 什么是平台币，平台币模式种类

平台币是数字加密货币类型当中的一种，是由加密货币交易平台官方发行的加密货币。一般情况下，持有平台币通常可以享受到一些特殊的权利，比如在交易平台上使用本平台的平台币进行交易，可以减免手续费，以及参与平台活动等。
“平台币”这个概念最先出现是币安推出的“BNB”，被广大用户接受以后，引发了非常多的平台效仿，平台币发行十分火热，比如火币、OKEx、Fcoin、Bit-Z 等都发行了自己的平台币。但是一个交易平台是否优秀，并不决定于它所发行的平台币，相反的良好的用户体验、优质的币种质量、负责的客服态度、低廉的手续费等。
也就是说，平台体验越好，用户越多，这意味着平台的盈利能力越强，平台币的使用价值就会上升。
平台币生态研究报告
https://wxappres.feeyan.com/block/2018/06/aZwvdzotUEP7fFSmu5xRNGlhJq1iVK0s.pdf

2.6.5.2. BNB

BNB，是由币安 Binance 平台发行的代币，其发行总量恒定为 2 亿个，对外 公开发行1 亿，且保证永不增发。BNB 在币安平台上线后，每个季度将币安 平台当季净利润的 20%用于回购 BNB，回购的 BNB 直接销毁，直至销毁到 总量为 1 亿个 BNB 为止。
BNB用途
1.手续费折扣：在币安平台上参与交易的用户，无论交易何种代币，在需支 付交易手续费时，如持有足额 BNB，系统会对所需支付的手续费进行打折 （第一年 50%，第二年 25%，第三年 12.5%，第四年 6.75%，第五年无折 扣），并按当时市值折算出等值 BNB 数量，使用BNB 完成手续费的支付。
2.上币费用：币安上币有投票制和审核制两种制度，这两种制度需要团队在 市场中购买币安币作为上币费，目前还有大量币种在排队等待上币。

2.6.5.3. HT

火币全球通用积分，简称 HT，是由火币 pro 平台发行的代币，是基于区块链 发行和管理的积分系统。HT 发行总量限定 5 亿，100%用于赠送，其中 60%（3 亿）用于购买点卡套餐赠送（每日限量）；20%（1 亿）用于用户 奖励和平台运营；20%（1 亿）用于团队激励，锁定期四年，每年解锁 2500 万。每个季度火币全球专业站收入的 20%用于流通市场回购，回购的 HT 全 部计提火币投资者保护基金, 用于平台突发风险时对火币用户进行先行赔 付，保护投资者权益。
HT用途

1.手续费折扣：使用HT 购买 VIP，不同等级的 VIP 享有不同的手续费折扣， 最高可获得 5 折交易手续费率优惠。

2.法币交易区认证商家保证金：使用HT 充当保证金，成为认证商家，获得 一对一客户服务。

3.HT 持有者专享活动：火币 Pro 会针对 HT 持有者不定期做专享活动，比如 空投在火币全球专业站上交易的新币等。

4.投票参与火币业务：火币会不定期向 HT 持有者发起投票，让 HT 持有者来 参与业务方向和细节。比如，针对评级达到火币全球专业站上线要求的项 目，使用HT 可以为看好的项目投票，火币全球专业站优先处理。

OKB

OKB 是由 OK Blockchain 基金会发行的全球通用积分，简称 OKB。OKB 的发行总量为 10 亿枚，不做 ICO，不公开向投资者募资。OKB 初期是基于以太坊 ERC 20 协议发行，未来会转移到自研的公有链 OKChain 之上。

发行方式：60%赠送
1.60%（6 亿）分别在 2018 年与 2020 年分 2 期免费派发给用户，赠送的形式为购买手续费套餐赠送 OKB；
2.10%（1 亿）用于基金会的运营，3 年后释放 1 亿枚；
3.10%（1 亿）部分早期股东购买，2 年后释放 1 亿枚；
4.20%（2 亿）团队持有，1 年后分批释放，逐年释放 2000 万枚。
用途：
OKB 可以被用来支付 OKEx 交易平台的手续费、融资融币利息，并且均可享受折扣。同时，拥有 OKB 的用户可以参与平台上币投票，支付认证商家保证金，购买独享 API 交易服务器、独享 API 交易网络和 IP 地址等专属服务以及其他增值服务。

超级鼓励金机制：

OKB 激励投资者持有的方式很直接、很粗暴，就是直接给持有者分红。根据方案，平台会在每周五根据用户 OKB 持有量占比，将当周手续费的 50%作为超级鼓励金以 BTC 形式分配给 OKB 用户。截止 5 月 7 日，OKB 已完成三期超级鼓励金的发放。

2.6.5.4. 其他平台币

2.6.6. 无币区块链

区块链可以脱离“币（Token）”存在，也就是发展“无币（Token）”区块链。

2.6.6.1. 简介及例子

区块链技术层次包括分布式网络、点对点通讯、加密机制、共识机制还有就是激励机制。当前说Token，属于激励机制的一种形式，“无币（Token）”区块链就是去掉了激励机制的区块链技术。

无币区块链十大案例：

1 支付宝 X GCash：跨境汇款

2 点融：区块链供应链金融

3 香港经管局：区块链贸易融资平台

4 IBM：汽车电子钱包

5 爱沙尼亚：数字身份

6 深圳：区块链发票

7 众享比特：政府敏感数据审计平台

8 佛山：“我是我”信用认证体系

9 食物优

10 关爱链

无币区块链十大案例

https://zhuanlan.zhihu.com/p/44316053

2.7. 区块链行业常用名词 （50-100 个）

1、Blockchain——区块链
区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。是一个共享的分布式账本，其中交易通过附加块永久记录。
2、Block——区块
在比特币网络中，数据会以文件的形式被永久记录，我们称这些文件为区块。一个区块是一些或所有最新比特币交易的记录集，且未被其他先前的区块记录。
3、Node——节点
由区块链网络的参与者操作的分类帐的副本。
4、去中心化
去中心化是一种现象或结构，必须在拥有众多节点的系统中或在拥有众多个体的群中才能出现或存在。节点与节点之间的影响，会通过网络而形成非线性因果关系。

5、共识机制
共识机制是通过特殊节点的投票，在很短的时间内完成对交易的验证和确认；对一笔交易，如果利益不相干的若干个节点能够达成共识，我们就可以认为全网对此也能够达成共识。
6、Pow——工作量证明
Proofof Work，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。
7、PoS——权益证明
Proofof Stake，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。
8、DPos——股份授权证明
类似于董事会投票，持币者投出一定数量的节点，代理他们进行验证和记账。
9、Pool——验证池
基于传统的分布式一致性技术，加上数据验证机制；是目前行业链大范围在使用的共识机制
10、智能合约
智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。
11、时间戳
时间戳是指字符串或编码信息用于辨识记录下来的时间日期。国际标准为 ISO 8601。
12、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。
13、Dapp——去中心化应用
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。
14、DAO——去中心化自治组织
可以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。
15、PrivateKey——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。
16、PublicKey——公钥
是和私钥成对出现的，公钥可以算出币的地址，因此可以作为拥有这个币地址的凭证。
17、矿工
尝试创建区块并将其添加到区块链上的计算设备或者软件。在一个区块链网络中，当一个新的有效区块被创建时，系统一般会自动给予区块创建者（矿工）一定数量的代币，作为奖励。
18、矿池
是一个全自动的挖矿平台，使得矿工们能够贡献各自的算力一起挖矿以创建区块，获得区块奖励，并根据算力贡献比例分配利润（即矿机接入矿池—提供算力—获得收益）。
19、公有链
完全开放的区块链，是指任何人都可读取的、任何人都能发送交易且交易能获得有效确认的、全世界的人都可以参与系统维护工作，任何人都可以通过交易或挖矿读取和写入数据。
20、私有链
写入权限仅面向某个组织或者特定少数对象的区块链。读取权限可以对外开放，或者进行任意程度地限制。

21、联盟链
共识机制由指定若干机构共同控制的区块链。
22、主链
主链一词源于主网（，相对于测试网），即正式上线的、独立的区块链网络。
23、侧链
楔入式侧链技术（pegged sidechains），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，就可以访问新的加密货币系统。
24、跨链技术
跨链技术可以理解为连接各区块链的桥梁，其主要应用是实现各区块链之间的原子交易、资产转换、区块链内部信息互通，或解决 Oracle 的问题等。
25、硬分叉
区块链发生永久性分歧，在新共识规则发布后，部分没有升级的节点无法验证已经升级的节点生产的区块，通常硬分叉就会发生。
26、软分叉
当新共识规则发布后，没有升级的节点会因为不知道新共识规则下，而生产不合法的区块，就会产生临时性分叉。
27、Hash——哈希值
一般翻译做"散列"，也有直接音译为"哈希"的。简单的说就是一种将任意长度的消息压缩到某一固定长度的消息摘要的函数。
区块链常用名词解释 http://www.360doc.com/content/18/0330/21/51800720_741631619.shtml

2.8. 区块链行业知名机构 （50-100 家，分类）

加密行业 TOP 100 最活跃的投资机构

https://www.block123.com/zh-hans/feature/top100-crypto-venture-capital-firms

3. 区块链项目营销

3.1. 项目基本面打造

项目本身做什么，什么应用，对外宣传资料，产品设计

好的项目如何设计
好的区块链+项目，应具备如下要素：
1、区块链技术特性要被嵌入到具体应用中
如“分布式存储”具有价值传递、半匿名、不可篡改等要素，如果能融入到你的区块链+应用中，就是一个有价值的区块链+。
2、区块链+应用要充分利用原有数据
一个好的区块链+应用，应当能够充分利用原有项目或公司的用户，用这些数据来对用户行为进行分析，从而更好为更多用户服务。

3、站在全球视角考虑问题
好的区块链+项目，应该让全球价值传递的本质进行体现，从“自己玩”过渡到“行业内竞争对手、合作伙伴一起玩”，在一个系统里面共建社区和生态，达到行业内部各个板块的共赢。
4、实现稳定的共识和激励机制
这种稳定的共识机制，可以激励积极的和善意的行为，同时降低交易成本。
共同点一：理论基础扎实
共同点二：从业经验丰富
共同点三：从人才到社区的全面国际化
好的区块链项目，都有这三个共同点
http://www.woshipm.com/blockchain/1027515.html

判断区块链项目的 8 个价值维度
第一是合基金会的所有牌照。假设国家要取缔项目一定先取缔这些没有牌照的，清零的风险很大。所以，区块链项目首先要做到合规。
第二是应用性。区块链项目必须要有应用场景，能够解决实际问题，不能讲故事自嗨。
第三是产品。建议项目上交易所之前先做好产品，产品是不是已经有 Demo 了？代码是不是经过测试验证了？把数据、产品、代码在沙盒系统里跑一遍，评个分，看到底能不能落地，这是最负责任的行为。
第四是白皮书。白皮书里主要看它的通证经济系统怎么设计的，以及商业逻辑是怎样的，这个产品的通证本身在这个商业系统里是不是有流通。
第五是顾问和投资人的水平。这里要看项目规性。现在很多的项目基金会都没有注册，所以公司手续办齐了吗？让他们展示一下办有没有知名的投资机构和投资人背书，以及有没有可信的技术大咖、擅长市值管理的运营顾问等等。
第六是营销和 PR。链圈大部分人都是做技术出身，建议这些项目找一些公关策划高手作为合伙人。比如有一个项目直接把创业家一个合伙人挖过来，给了年薪一百多个比特币。
第七是社区管理。区块链项目的团队要在社区里进行充分的信息披露，然后激励社区成员在里面讨论，提供建议和挑刺，督促项目本身的成长。
第八是利他性。项目发起人非常重要，这个人得胸怀天下，能够笼络人。
https://36kr.com/p/5127285

不好的项目的特点
目标样本死亡原因主要分为：项目方关停、违规运营、国家政策影响、安全问题导致关闭等。
区块链创业死亡名单：全球 34 家失败案例总复盘

http://tech.sina.com.cn/it/2019-04-06/doc-ihvhiqax0455432.shtml?cref=cj

3.2. PR

3.2.1. 一类媒体 （中/英）

中：

1.金色财经

算是区块链媒体里的“先行者”了，月收入更是高达数千万。据官网信息，金色财经是一家专注于区块链产业的服务平台，多家搜索引擎新闻源合作媒体，并与数十家财经及科技媒体达成内容合作；截止到 2017 年 7 月，金色财经已有 1000 余家企业、个人自媒体、行情分析师入驻平台，每日 200 篇以上的内容输出。

2.巴比特

OKCoin 巴比特

巴比特始建于 2011 年，是国内最早的区块链（blockchain）资讯社区门户，为区块链创业者、投资者提供信息、交流与投融资服务。开放是我们的广度，中立是我们的态度，敏锐是我们的深度，欢迎一切区块链技术的探讨争鸣。目前有 200 多位区块链意见领袖、研究者入驻平台。

专业媒体：

https://www.zhihu.com/question/264321156

英

1. CoinDesk

CoinDesk 是区块链技术和加密货币的顶级媒体网站之一。该网站于 2003 年开始发布，从那以后一直在快速增长。 CoinDesk 提供有关比特币和其他商业信息的最新消息，以及最近区块链技术发展的最新消息。 CoinDesk 还维持比特币价格指数，这是比特币交易所比特币价格的平均值。

Forbes 福布斯

3.2.2. 二类媒体（中/英）

中

3.链得得

钛媒体旗下的新资讯平台，它将更偏重于金融与区块链技术的落地商业和政府应用，其核心用户群将集中在技术开发者、全球投资者和监管者。

4.非小号

专注数字货币行业大数据分析。

5.深链财经

深链财经是区块链领域第一深度报道媒体，由多位资深财经媒体人联合创立。目前已获得了梅花天使、PreAngel、千方基金、Dfund 等 8 家顶级基金联合投资。在内容层面，设置了人物专访、人物群像、项目调查、项目评测等多个板块。

6.白话区块链

区块链资讯文章平台，最近做的 EOS 节点竞选专题挺棒的。

7.币圈子

8.比特社区 （和非小号相仿）

9.币乎

10.币世界

11.币源社区

12.猎云财经

英

2. TodayOnChain

TodayOnChain 是区块链和加密货币的新闻聚合器。在这个网站上你可以找到来自许多不同资源的大量新闻，包括区块链/加密媒体，如 CoinDesk，CoinTelegraph，CCN 等，以及主流媒体，如财富，福布斯，CNBC 等。TodayOnChain 的主要特色在于因为它是一个非常全面的聚合网站，您可以访问这个单一站点来访问来自许多不同来源的新闻。换句话说，TodayOnChain 是区块链和加密新闻的一站式场所。

3. CoinTelegraph

CoinTelegraph 提供有关比特币，以太坊和其他加密货币的新内容，以及有关区块链技术和加密市场的分析和评论。这是一个非常活跃的网站，每天发布许多新闻和文章。此外，CoinTelegraph 还提供多种语言版本，包括英语，西班牙语，巴西语，塞尔维亚语和日语等。

4. CCN

CCN 是在挪威注册的媒体公司的一部分。 CCN 的网站提供有关加密货币的新闻和文章，如比特币，以太坊，以及区块链领域的工业新闻。除了区块链和加密新闻，CCN 还提供加密市值，加密货币新闻，ICO 日历，事件日历和其他类型的资源等信息。

5. Null Tx

Null TX（前身为 The Merkle）提供加密的最新消息以及有关比特币，以太坊和其他加密货币的教育文章。它还有一个专门的财务专栏，其中包含金融技术领域的新闻。该网站每天发布许多新闻和文章。 NullTX 成立于 2014 年，总部位于旧金山。

6. NewsBTC

NewsBTC 是区块链和加密的新闻和资源平台，自 2013 年开始运营。NewsBTC 向区块链和加密货币社区提供新闻，评论，技术分析和其他信息。 NewsBTC 每天发布许多文章和新闻，还提供其他资源，如教育文章，区块链公司目录，ICO 列表和事件日历等。

7. Bitcoinist

Bitcoinist 成立于 2013 年。Bitcoinist 不仅涵盖比特币，还提供有关其他加密货币和区块链技术的新闻和消息来源。Bitcoinist 每天发布几篇文章和新闻，涵盖加密和区块链中的一系列主题。

8. Bitcoin Magazine

Bitcoin Magazine 是第一本专门用于比特币的出版物。它的创始人包括 V 神 Vitalik Buterin，以太坊的创造者。现在 Bitcoin Magazine 不仅涵盖比特币，还涵盖其他加密货币和区块链技术。比特币杂志在金融和技术的交叉点提供分析，研究，教育和思想领导力。

9. CryptoSlate

CryptoSlate 是一家区块链媒体，其使命是“提供关于加密货币和区块链的透明、准确的报道”。这家媒体成立于 2017 年，总部设在西雅图。 CryptoSlate 的网站提供与区块链和加密货币相关的定期更新的新闻和文章。它还提供 ICO，加密货币排名等内容。

10. Subreddits

Reddit 是一个新闻聚合、网络内容评级和讨论平台。 有许多板块专注于区块链技术和加密货币。提供文章链、新闻和用户的帖子，还有一些关于不同主题的讨论。 以下是 Reddit 与区块链和加密货币相关的一些板块：

r/BlockChain/

r/CryptoCurrency/
r/Bitcoin/
/r/ethereum/

3.2.3. 自媒体（中/英）

中

1、大炮评级
ID:DarpalRating

推荐语：大炮评级原名“未来虚拟币”，2 月 25 号刚改的名。大炮是我的江西老乡，我认识他的时候他还在阿里，还没有出来创业做这个区块链评级项目。我也付费加入了大炮的知识星球和社群，群内币圈资深投资大咖和项目负责人众多，是我觉得除了三点钟主群之外含金量第二高的币圈社群。

按照大炮的设想，大炮评级定位为区块链领域的穆迪，致力于通过评级，协助数字资产投资者从近万个数字资产里挑出价值资产，并推动行业里的“优币驱逐劣币”。另外，大炮项目也早已拿到风险投资

2、陈菜根频道
ID：chen-cai-gen

推荐语：菜根兄原是蛮子基金团队成员，后来出来自己做了为友资本合伙人。大家都知道，薛蛮子老师在 2017 年上半年的时候从互联网 VC 转型为区块链 VC，投了很多区块链项目，在团队的熏陶之下，菜根兄对区块链的思考也是愈加深刻。

“陈菜根频道”的文章经常在朋友圈刷屏，因此不仅近期受邀入驻钛媒体的“链得得”，而且也在年初就获得了 preangel 王利杰的天使投资。

3、数字货币先生
ID：szhbxs

推荐语：大家可能发现了，我们两个号的名字很像，但其实我们没什么关系，不是一个公司的，也不是同一个团队运营，只是我前些天改名时借鉴了一下（现在取个不重复的公号名字实在是不容易...）。随着对区块链的了解越深，我越觉得那些币市上的那些 token 和 cryptocurrency 不应是数字货币，而更像是数字资产，因此我觉得我的数字资产先生比他的数字货币先生更接近本真。

而且，就如业内力促把 token 的翻译由“代币”改成“通证”一样，我是比较建议把“数字货币”改称为“数字资产”。一来是数字资产更能涵盖“加密货币”和“通证”两者，二来也可以减少不必要的 ZF 监管。

最后，虽然币市还处于消息市场，现在进行 K 线分析很不靠谱，但是数字货币先生在 K 线分析之前的行业解读很有见地。因此，虽然小有竞争关系，但我还是要推荐下。

4、币圈早知道
ID：bqzzd888

推荐语：币圈早知道给我的第一印象就是总能第一时间发布电视媒体上有关币圈的视频片段。因此，如果你烦够了阅读文字，想通过视频了解些币圈资讯，那“币圈早知道”应该可以帮你换换胃口。

5、镖客往事
ID：coinstory

推荐语：这个号是比我早四个月入圈的朋友推荐给我的。经我一段时间的观察，虽然不长更新，内容也很短，但三观很正，内容干货含量也很高。

6、猫说
ID：laomaogulu

推荐语：猫说是前云币网创始人、现 BIGONE 创始人和硬币资本合伙人老猫的个人自媒体。虽然 BIGONE 交易所的用户体验不怎么好，但是“猫说”的公号和知识星球内容质量很不错，如果你想站在币圈老人的肩膀上实现“春江水暖鸭先知”，那么“猫说”便是一个值得你关注的自媒体。

与“猫说”同样类型的，还有李笑来的“学习学习再学习”和王利杰的同名公号“王利杰”，为了能推荐更多的优质币圈自媒体，因此只能把它们放在一起推荐了。当然，这也跟“王利杰”的不常更新和“学习学习再学习”渐渐成为“一块听听”的宣传口有一定联系。

7、区块链投资内参
ID：qukuailian365

推荐语：“区块链投资内参”和“猫说”、“陈菜根频道”等自媒体一样，是我既关注了公号，又参与了付费社群的自媒体。内参君早在一年前就转型为区块链自媒体，并随着 17 年下半年的币市火爆而发展迅猛，目前已在社群基础上在新加坡成立了“读数基金”。而且，除了这个主号，还软分叉出了小号“币圈韭妹”。

8、蓝狐笔记
ID:lanhubiji

推荐语：蓝狐笔记是我付费参与的第一个知识星球，当时参与的时候蓝狐笔记还不是垂直于区块链这块，而是泛科技点评。而当我去年 12 月开始聚焦于区块链时，才发现“蓝狐笔记”也已转型为一个优秀的币圈自媒体。

目前，蓝狐笔记会经常发布一些蓝狐组织翻译的优质国外区块链文章。

9、币圈肆无忌惮的少主
ID:QTUMChina

推荐语：如果你烦腻了温文尔雅、平铺直叙的行业点评，想看一些辛辣的、尺度大的甚至是直接骂人风格的币圈吐槽，那么“币圈肆无忌惮的少主”就千万别错过。搜索关注后，你可以去历史消息里翻翻少主是怎么骂 OKEX、波场、英雄链等行业乱象的，真是语不惊人死不休，非常敢骂，也让人很是痛快。当然，这也许也跟少主肉身不在国内有关....

10、火币资讯
ID：huobizx

推荐：严格来说，“火币资讯”不算自媒体，而是机构媒体，因为是交易所火币网旗下的。但我觉得，偶尔转换下视角从交易所角度来看分析币市动态也很有帮助。何况，火币网制作的动画短视频“区块链 100 问”能帮助币圈新人简洁易懂的了解区块链知识。

3.3. 社区

3.3.1. 社交频道

3.3.1.1. Twitter

一。 Vitalik Buterin – @VitalikButerin

Vitalik Buterin 是 24 岁的以太坊平台和球第二大市值加密货币的开发者。 在他的推特中，他说许多主题关于加密货币市场、区块链和虚拟货币技术方面以及经济原理， 他还交流思想和预测。 另外，他发布超越加密货币主题的其他有趣信息。 截至 2018 年 4 月中旬，Vitalik 拥有 73 万以上名追随者。

二。加文安德烈森 – @gavinandresen

加文是比特币核心的首席开发人员。比特币核心是由中本聪创建的原始开放源代码软件。当神秘的比特币创始人宣布离开时，他直接从中本聪拿手维护代码。在他的推特中，你会发现很多与加密相关的信息，包括税务，法律状态，比特币，比特现金等等。

三。查理李 – @SatoshiLite

查理称为莱特币虚拟货币的创始人，目前它是市值最高的五大硬币之一。他还是美国 Coinbase 加密货币交易所的前工程总监。查理李拥有 75 万以上名追随者。

四。Nick Szabo – @NickSzabo4

Nick Szabo 是区块链，加密货币和智能合约的先驱。他是一位密码学专家，他 1998 年创立了数字货币 Bit Gold 的概念。这项技术被认为是比特币架构的直接前奏，Nick 曾多次声称是中本聪。

五。Tuur Demeester – @TuurDemeester

Tuur 是投资者和分析师。他有经济教育，擅长研究繁荣和萧条的经济周期。如今他主要关注比特币，并且经常提供有关虚拟货币及其经济学的专家意见，这对确定加密资产的市场和投资视角非常重要。

六。 斯宾塞博加特 – @CremeDeLaCrypto

斯宾塞博加特是第一批专注于加密货币的华尔街分析师之一。他是 Blockchain Capital 的合伙人和研究员，并在他撰写文章的福布斯杂志中称自己为“一位具有独特深度经验分析加密货币和传统股权机会的基础投资分析师”。他积极讨论分享他的专家意见的密码相关主题，并拥有超过 7.7 万的关注者。

值得关注的 100 个最佳关于数字货币的 Twitter 帐户

https://www.chainnews.com/articles/194505964658.htm

3.3.1.2. Medium

Medium 是一个基于主题的协作型媒体平台，它的一个重要的属性是：高质量。

https://medium.com/topic/blockchain

3.3.1.3. 微信公众号

区块链公众号影响力榜单 Top50 名录（周榜）

https://www.linksfin.com/article/38074

3.3.2. 社区运营

3.3.2.1. 微信社区

3.3.2.2. Telegram

每个人注册 Telegram, 添加 Jane0810，加入公司项目和其他好项目社区，用大号和小号活跃社区。

3.3.2.3. 其他

3.3.2.3.1. Reddit

注册账号并使用

Reddit 该怎么玩儿？

https://www.zhihu.com/question/19932645

3.3.2.3.2. Steemit

注册账号并使用

30 分钟全面搞懂 Steem

https://steemit.com/steem/@gaoduzhu/steem

3.3.3. 喊单

3.3.3.1. 什么叫社区喊单

喊单是一种外汇术语，就是公开讲自己的做单计划，让投资者或外汇爱好者根据喊单人所给的提示作为参考来做自己的真仓或模拟，喊单者会把自己开仓的价位，止损，止盈等信息传输给你，让你做个参考。

3.3.3.2. 示例

半年狂割 50 亿！神秘团伙靠“喊单”吸血币圈

https://www.chainnews.com/articles/416624074912.htm
大饼柚子实时喊单操作

https://www.jinse.com/blockchain/408845.html

4. 入场准备工作

熟悉了解区块链行业基础知识，了解公司文化，使命及项目基本信息，注册社交媒体账户并添加及关注项目及知名账户，活跃项目社区，关注区块链行业相关知名中外媒体，保持好奇及进取心。准时上下班，分享知识，信息及活动。

4.1 block chain 基础学习：

Coursera Class

There are four courses in this package, please at least pass the first course: Blockchain Basics. (One-month class registration fee will be reimbursed if you passed the course, ps: after you passed the course, you will get a certification which can be listed on your LinkedIn profile)

https://www.coursera.org/specializations/blockchain

学习 Excel https://drive.google.com/open?id=1GmSpvjl092fCnBkjR0GD-D39yfhA2Akc

包括交易所，机构，项目，名人的一些排名和介绍。

区块链社会：https://drive.google.com/open?id=1dCjJg3V-0rstLXt-bRq-88G98ivdkJA3

主要讲了区块链在不同行业的一些应用。

比特币白皮书：

英文：
https://drive.google.com/open?id=1Oa9sW5QtKu92d4p0MKpZO9ZCYatFuuzY

中文：https://nakamotoinstitute.org/static/docs/bitcoin-zh-cn.pdf

一种点对点的电子现金系统，讲了原理和应用。

NYLife360.com, Tel: 929-633-1888, VX：NYLife360

下载钱包并使用：

ImToken

Mycelium

Trust Wallet

注册交易所：

Robinhood 注册链接：https://join.robinhood.com/janew119

Coinbase 注册链接：https://coinbase.com/join/wan_gfj?src=ios-link

Binance：https://www.binance.com/?ref=36863455

比特币等价黄金价值理论：https://nylife360.com/archives/10714

注：现在 BTC 还在下跌阶段，举例下一次减半时间将近，身边高人观点 BTC 会最终在 1 万 2-1 万 9 之间反弹，这期间会是比较好的入场时机，想入场的可以留意这个时间，可以注册交易所 Robinhood 或者 Coinbase，Coinbase Pro, Gemini,各有利弊，考虑交易费用，个人推荐 Robinhood. 除了买币，也可以考虑投资矿机，买一只下蛋母鸡，静候佳音，和时间做朋友。

Robinhood 注册链接：https://join.robinhood.com/janew119

Coinbase 注册链接：https://coinbase.com/join/wan_gfj?src=ios-link

另外 NYLife360 代理位于德州和俄亥俄的矿产，可以出售矿机和算力，提供托管服务，感兴趣可以 VX: NYLife360, cell: 929-633-1888.

行业新闻 News:(we are using the lst and 2nd web to generate our daily news)

https://www.coindesk.com/

https://cointelegraph.com

https://www.stateofthedapps.com/

www.8btc.com

NYLife360.com, Tel: 929-633-1888, VX：NYLife360

行业数据 Data:

https://coinmarketcap.com/

https://etherscan.io

微信账户 Wechat official accounts:

DAPPREVIEW

区块链铅笔 blockchain

白话区块链

Dappso