区块链的下一个十年——甲子光年

自从2008年中本聪发表了比特币白皮书，至今区块链已经发展了十年的时间。2017年，它更是获得了社会广泛的关注。以下内容或许能够帮助大家，从零开始快速熟悉十年来区块链技术的一些基本概念，以便探讨未来十年区块链领域的发展机会。

区块链技术的基本概念和基本判断

相信大家对区块链技术的基本概念已经有所理解，从这些概念出发，有四个基本判断:

1）区块链的颠覆之处，在于它解决了“信任”这个人性问题，仅仅从技术角度出发，无法理解它的强大。一些原本彼此并不信任的人或者团体，各自出一台服务器，在大家彼此监督、大多数人遵守共识协议的情况下，能维护一份公认的记录——这就足以打开无穷的想象空间。

2）抛开能够实现价值流动的“币”，仅仅考虑区块链对生产力的改造，其创新程度远远比不上人工智能。

区块链其实就是一个分布式的数据库，每个区块中保存的内容，相当于数据库中的表格，它和传统分布式数据库的区别在于:①参与者可以任意地加人，不需要许可； ②任意地离开，不影响系统运行；③数据库的内容对所有参与者公开；④以往的所有交易数据，即数据库的日志，永不删除； ⑤高度冗余，高度可靠； ⑥低效，需要多个确认，才能认为交易真的

完成了。

加密数字货币只是区块链技术的应用之一。从数据库技术角度看来，加密数字货币的记账方式和支付宝、微信支付记账的方式并无本质的不同，比特币交易的速度还很慢，大额交易一般要等六个确认，耗时一个小时左右。

加密数字货币的优势在于它们实现了虚拟世界中价值的低摩擦力流动。法币在比特世界中流动起来有非常大的摩擦力，发送方和接收方都要和公民的身份相绑定，有各种各样的限额，而且跨境流动非常困难。与之相比，多等几个确认的时间真是细枝末节的小事了。如梁斌博士所言: " 财富的自由流动、不受限地自由流动是很多富人的终极需求，我想这是包括比特币在内的加密数字货币最核心的价值 " 。

但在加密数字货币的应用之外，作为纯粹可信数据库的区块链技术目前看来，最先落地的应用很可能是“溯源 " 。

例如天猫国际的全球溯源计划，主要是通过区块链、药监码等技术运用大数据跟踪进口商品全链路，实现集生产、通关、运输等各方面信息于一身的目的，以期为各个跨境商品添加“身份证 " 。

这类应用，传统的、中心化的、高可靠的数据库一样可以搞定，因止从生产角度来看，区块链只提供增量式的进步，想象空间不大。

3）区块链真正的想象力在于生产关系角度的 " 去中心化”

4）和任何技术一样，不能对区块链本身进行价值判断，它有可能被用来作恶，也有可能促进经济、社会发展。

从互联网发展历史上讲，非法经济还有游戏，经常是首先应用新技术领域。以区块链为基础的加密数字货币，就曾被非法组织作为交易货币之一。

另一个历史规律是，遏制新技术的发展从来不是解决负面应用真正有的方法。在区块链技术已经兴起，大量资本和人才涌人的情况下，只有花更多力气发展有益应用，才能避免有害应用的流行。

从整个人类历史的高度来看，如同郑渊洁所说:“某些高科技首先为了军事目的而研制的，尔后才转为民用。”如果区块链技术真的如大家想象得那么伟大，那它在未来会带来多少美好，眼下就可能带来多少混乱。或者说，它眼下带来多少混乱，说明它未来就有潜力带来多少美好。

加密数字货币八问

首先来看区块链技术目前最杀手级的应用-加密数字货币。这是目前建立在区块链技术上最风靡的应用，甚至要撼动全球金融体系。以至于有一种说法是“离开加密数字货币谈区块链都是耍流氓”。

加密数字货币的本质是“信”，有信货币就能成立。只要有一个群体，他们把某种可交换的物品当作统一价值表现材料，那么该物品对于这个群体而言，毫无疑问就是货币。

" 群体” “当作”这两个词可不简单，背后有一个大大的“信”字。黄金的价值也来自于信任、信赖、信念。信任它是有限的、稀缺的，信赖整个社会的其他人都认可它的价值从而愿意拥有它，同时，还必须抱有信念:它在未来仍然是稀缺的、人们愿意持有的。

黄金和白银用数千年时间赢得了信任、信赖、信念。法币则依靠权力机关和宣传机关，快速建立了自己的信用-再强调一下，国家背书只是获得信用的手段之一，这个手段也未必好使，法币信用崩溃的例子，出现过和正在出现的，不胜枚举。

《人类简史》的作者赫拉利曾说:“任何大规模人类合作的根基，都在于某种只存在于集体想象中的虚构故事。讨论虚构事物正是智人语言最独特的功能。人类可以一起想象，共同编制出故事:传说、神话、神和宗教应运而生。智人的合作不仅灵活，还可以和无数陌生人合作，正因如此，智人才统治了世界”。

既然数亿的人口可以共同相信某个传说，在规模不算小的群体内部，大家都笃信比特币，这又有什么稀奇?

理解了“信”字，很多关于比特币和加密数字货币的问题就很容易解答了。

问:加密数字货币的价值到底体现在哪里？它对人类有什么贡献?

答:货币对人类的贡献在于它可以让原本无法发生的交易发生。要做出这样的贡献，它就必须是有价值的。它的价值在于它的信用，即对它持有信任、信赖、信念的人的数量，以及“信”的深刻程度、专一程度。但这些标准又太虚无缥缈了，如何量化？量化标准就是人类对这个货币进行了多少交易。

问:加密数字货币可以仅仅作为类似黄金的储值手段，而不进行日常交易吗?

答:只要有人“信”就可以。但是，不进行日常交易，相当于瘸了一条腿，用上面的量化标准衡量，就大打折扣了。

问:加密数字货币如何建立自己的信用?

答:加密数字货币本身的代码和理念要好。可是复制比特币的代码无法实现另外一个比特币，在建立信用的过程中，技术只是很小的因素。

只有一件事情是肯定的:要在极大规模的人群中建立信用，主要靠人性，而不是依靠科学、理性、说服、教育-人性使然，没有办法。

问:加密数字货币或者区块链可以实现去中心化吗?

答:注意前面描述去中心化时，加了“服务器”这三个字。只有计算科技这个领域，可以谈论去中心化。只要有人群的地方，都不存在彻底的去中心化，必然存在领袖和群众、先锋和跟随、先进和后进。换言之只有去中心化的技术，没有去中心化的人群-人性使然，没有办法。

但是，技术上去中心化，多多少少还是降低了人群的中心化程度。例如，互联网的出现，让个人更加容易地公开发表自己的看法，以前，只能通过报纸和杂志这些传统媒体，现在只需要发微博、写知乎。

问:加密数字货币的分叉是怎么回事

答:分叉有两种:一种是由于网络通信造成的偶发分叉和孤块；另一种是由于使用某种加密数字货币的社区内部发生共识分裂，造成永久的、非偶发的分叉。

永久分叉之后，社区中一部分人的服务器在一个分叉上追加块，用他们认为合适的代码；另一部分人用另外的代码在另一个分叉上追加块——统一的社区分裂成了两个。

人群中天生存在分歧，有一句话说得好，“要想一个去中心化系统永不分叉，就好像一个中心化系统想要千秋万代一样可笑

现在甚嚣尘上的分叉之风，绝大多数只是假装有分歧，假装社区产生了分裂，以此来骗钱而已。没有社区“信”的货币，价值为零。

问:比特币会消亡吗，谁能和它竞争?

答:比特币已经积累了非常大的社区和信用，应该不会消亡，但相对而言，它具有大概率会变得越来越弱势。

首先，代码和理念比它先进的以太币等竞争币种正在赶超它。

另外，世界上传统的势力，如大公司、大财团、政府、宗教等，它作被比特币打蒙了，猝不及防。一开始是看不懂，后来是看不起，但是等它们缓过劲来，学会背后的这个“信”字，必然会用区块链的技术和理念来反击比特币。

问:比特币能抗通胀吗?

答:比特币的总量2100万个，不会超发。因此，如果“信 " 比特币的群体越来越大，而且“信”得越来越深入，越来越专一，它肯定可以抗通胀。

事实上呢？考虑一下人性吧。

问:比特币挖矿，是一种能源的浪费吗?

答:不是，挖矿是比特币建立信任的手段。比方说，男女谈恋爱时女性希望男性对自己舍得花钱，甚至希望花一些很浪费、很不“居家”的钱-这是在建立信任，考验你是不是“对我好 " 。比特币在比特世界工作，原子世界为比特世界花钱，还能让比特世界定量地感知到，有什么手段？除了烧电做哈希碰撞，好像没了。不采用工作量证明的挖矿方式也有，例如Pos （权益证明），它不按照电力投票，而是按照以往拥有的币来投票，隐含的逻辑是相信这个链上的既得利益者。

“无政府主义”和价值流动的黑暗面

区块链的巨大想象空间，在于它对生产关系的“去中心化改造”

预计去中心化有两种路径:一是“无政府主义”的应用；二是在一定监管体制下的去中介化应用。前面提到，如果区块链技术真的如大家想象的那么伟大，那它未来会带来多少美好，眼下就可能带来多少混乱。首先来看看，在2017年的ICO，IFO、IMO之后，短期内还可能看到多少混乱。

以往，加密数字货币在非法交易上已有不少应用，因为加密数字货币有很好的保密性。

网上博彩非常容易实现去中心化，封掉它们的网站是没用的。只要人们已经拿到了它的公钥，它就能通过各种渠道把用于博彩的加密数字货币地址广播给大家，并且通过签名技术确保这些地址没有被渠道篡改。

以往，互联网只有信息的流动，没有价值的流动（或者流动起来摩接很大），只有复制，没有交换（因为无法确权）。互联网上信息的传播是中心化的，微信、微博、直播、快手，无不如此。因为商业模式是“数据传输本身免费，靠广告变现”。

如果数据传输本身可以通过赚取加密数字货币来盈利，任何做数据中继的节点都有钱赚，信息的流动就可以变成去中心化的。这里面的技术实现起来并不困难。

试想一下，微信、微博、直播、快手这样应用，如果有了去中心化的、信息全球流动且不受审查的版本，它们的杀伤力会有多大?

最近，区块链还成功地应用在“骗”上。方式就是ICO、 IFO、IMO等，其中有大量虚假项目和泡沫，对社会造成了很大的困扰。

去中介化- " 最不坏”的选择

有一种说法，认为人类大部分经济活动都可以通过区块链进行，人头现有的大部分组织都可以被区块链代替，包括国家，最终会建立一个无国界的新世界。听起来好刺激，但是这样一个新世界由谁来建立？

——如果这个新世界将由现在币圈和链圈的大咖建立，你会相信吗？

——如果这个新世界由最擅长推广“赎罪券”的势力建立，你会相信吗？你会愿意吗？

——如果未来强势、先进国家主导的区块链，逐步渗透到弱势、落后国家的经济活动中，最终建立了这样一个新世界，你会相信吗？你会愿意吗？

我们感觉，估计还是最后一种可能性更大，而且相比较而言，在上述三种可能性中，它是“最不坏”的那个。

去中介化，说白了，就是看现在的互联网巨头不爽，要斗地主分田地。有一段话：" Uber-世界最大计程车行，却没有自己的车； Facebook.世界最红的媒体，却没有自创的内容； Alibaba-世界最大量交易的商场，却没有自己的库存； Airbnb-世界最大住宿提供者，却没有自己的地产。”

此话真的是在赞扬这些平台公司吗？还是有莫名的情绪在里面？举例而言，Alibaba，它可以很自豪地说靠一已之力把我国带入了电子商务时代；但从另外一个角度讲，也可以说tmall.com和1688.com上众多商家苦哈哈，才养活了Alibaba-家风风光光。

平台型公司，连接消费者和生产者（无论生产的是信息、实物还是服务），然后利用这个“连接”来赚钱。它们从供需双方那里赚的钱越多，意味着供需双方所付出的显性和隐性的成本也越多。如果成本过高，人们必然希望有新的解决方案。这是区块链的优势之一——成本。

从这个角度讲，用区块链的技术挑战某个巨头，就算斗地主成功了，也远远不会成为另一个地主，可以永远高枕无忧躺着数钱？区块链属于使用链的每一个人，底层代码的开发者也无法控制它，一味独断专行地控制，链就会分叉。

从技术上讲，去中心化的区块链上跑的去中心化的数据库，在功能上只会小于等于中心化平台所拥有的中心化数据库；区块链可以实现的功能，中心化平台一定可以实现。而且中心化平台的服务器成本还更低。低成本从何谈起呢？需要靠持久的、充分的竞争。从共享出行领域开始，互联网创业有了个坏思潮:指望靠烧钱把所有竞争对手都熬死，然后自己赚垄断利润。在破除垄断方面，去中心化的区块链有很大的潜力。

但从另外一个角度讲，区块链的创业者也不必害怕巨头来抄袭，因为这是要砍掉它们自己赚钱的命脉，自我革命。

在成本之外，区块链的优势还有“诚信”。平台为了牟利，必然会利用供需双方的信息不对称来隐瞒甚至作假。例如某些网站会利用顾客对它的信任来“杀熟”、广告平台会伪造点击率、视频平台会伪造播放次数，等等。区块链上的所有数据都是公开的，没有作假的余地。

还一个优势是“开放”。平台垄断了供需双方的数据， 自己依赖数据做大数据分析，提供服务。信息被平台分割成了孤岛，大数据分析因此受限。另外由于缺乏竞争，平台所开发的分析算法也未必是最优的。链上的数据开放之后，会有很多第三方的公司，根据多个链的大数据分析结果，提供为供需牵线搭桥的服务，它们彼此竞争，看谁的算法最优。

接下来说说“去中介化”的一些具体创新场景。

区块链创业机会

1. 广告之痛

比起前互联网时代，衣食住行的体验改善了很多，但广告依然像从前一样讨厌，几大痛点一个也没有解决:广告很难看，而且总在不想看到它的时候出现；对推送来的广告根本不感兴趣；广告主不知道广告是否推送给了合适的人；广告主不知道点击是不是伪造的。

广告的“去中介化”意味着厂商、广告制作者、观众三者直接互动，厂商只向制作者和观众付费。“媒体做广告”这件事情，被排除在系统之外。如何用区块链来实现这个目标？

消费者购买了某类商品，就可以获得某种通证（Token），商品不同通证的类别也不同。这些过往的消费证明了消费者的消费能力。广告需要消费者支付通证才能看，但认真看过并且回答了简单问题之后，可以获得力度很大的消费折扣券，甚至可以获得一些数字货币。

观众有了通证，自然就要有个钱包来保存它们，有钱包就意味着有一个私钥，这个私朗用作数字签名。用私钥给观看记录签名，就表示这个广告是被真实的用户观看了。在区块链上，丢失私钥相当于丢失了身份，账目下的钱会被人花掉；别人用用户的私钥给一段言论加了数字签名，就相当于发表了该言论。要教育用户千万不可以把私钥交给旁人。这就避免了不法之徒搜集众多用户的私钥来伪造观看记录。

广告制造者可以是任何人，甚至可以是消费者自己。厂商自己准备一些硬广，广告制造者生产各种软广，并且从厂商那里获得很多一次性的硬广链接，插入到软广中。观众点击硬广链接并且用私钥对观看记录签名后，厂商向用户和广告制造者支付费用。消费者自己为商品写的评论，也作为一种软广来处理。

在这个系统中，提供服务者，直接向被服务的对象收费，没有扭曲没有“羊毛出在猪身上”。

这个系统中，还会有很多广告推荐商，根据观看广告、采购商品、打赏广告制作人的记录，来做大数据分析，推荐广告给用户看。这些推荐商所能看到的数据是一样的，彼此比拼算法。硬广链接中可包含推荐商的信息，推荐商据此向商家收费。

厂商想在短时间内让某产品家喻户晓，只需要降低观看广告所需要支付的通证数量、提升看完广告后可获得的奖励。

2.内容

如今内容提供商，无论它提供的是音频、视频还是普通图文，基本上盈利模式都是靠广告。广告去中介化之后，内容提供商要么转型为软广制作商，要么直接把自己的产品作为商品来销售，要么采用两者的混合。

例如电视剧制作商，可以免费提供内插了很多硬广链接的视频，也可以销售纯净版的高价视频，或者销售只插入了少数硬广的低价视频。

为了保护内容不被盗版和篡改，内容提供商所提供的文件中，内置了Javascript脚本，脚本运行在受限的执行环境中，验证自身没有被CDN （内容分发网络）节点篡改，验证呈现内容的平台具有HDCP（高带宽数字内容保护）等版权保护措施，不会被录音录屏。

有些小的内容提供者，比如微博的博主，每条信息都很短，如何收费呢？每条收费一分钱估计都有人嫌多，但人民币的支付单位最小也就是-分钱。这个时候，用户向他们支付的费用，用抽奖券代替。比方说每个奖手有千分之一的概率可以抽到一块钱通证。

3.零售

上面描述的这个链，直接在上面做零售是顺理成章的，每个硬广里面都可以内置订购链接。订购的网站是商家自己的， U1 （用户界面）由自己设计，只需把订购的信息放在链上，受公众监督。未确认的交易资金被网站保管这一行为，被链上的锁币操作替代。

客户可能不希望泄漏自己在哪家商户采购了商品（例如情趣商店）这时，零知识证明等手段，可以用来保护客户的隐私。

客户购买了商品之后，什么也不说，相当于好评。如果想要差评，需要自掏手续费在链上刊载抱怨商家的言论。有实名交易的差评，节点才会打包到区块内。如果客户实在太喜欢这个商品了，就自己去做软广，或许还有机会赚到钱。

有了区块链上的智能合约支持，还可以预售。商家承诺说某个日期发货，客户付少量订金承诺说那个时候我必然花钱，任意一方违约，都要

付出违约金，而且违约金是自动扣的。如果客户不想要货，还可以把合约专让给其他人，避免违约金。这样一来，还没有养大的猪、还没有收获的水果、刚刚设计好但拿不准会不会大卖的衣服，都可以提前“试试水温”。这种机制可以有效地指导产品的生产，如果没人愿意买预售合约，则说明产品到时候必然卖不出去。

4.社交

有了CDN的支持，每个人都可以委托一家CDN把自己给朋友的加密信息传递过去，如果和朋友不在同一家CDN服务商，那么CDN服务商之间的信息中转成本由它们彼此谈判消化。这就形成了去中心化的社交阳络， CDN服务商之间通过信息路由的用户体验来竞争，每个人的公钥就是自己的账号，适用于所有的CDN服务商。

朋友圈的功能类似于微博，需要把发圈的人当作内容提供商来看待所发的内容别人是要付费的，哪怕一条只有0.1分。发得太频繁，就会被屏蔽。

微信群的功能，通过给群里所有人都发信息来实现。

这里要澄清一个误区，很多人认为加密的聊天工具就是给不法之徒提供服务的，因此聊天工具不应该使用公钥私钥的机制，最好直接传送明文或者至少在服务器端保存明文，大错特错。借助现有的社交工具，传递完全加密的信息非常容易:把加密后的信息嵌入到图片中，对方从图片中抽取信息再解密。

作为公民，使用加密技术保护自己的隐私，公开发表符合法律的言论，是基本的权利，如果这些权利通过阳光的渠道无法行使，那么由加密数字货币驱动的去中心化版本社交工具就会大行其道，这算是21世纪的“道路以目 " 。

5.无处不通证

既然货币的本质就是信用，那么拥有信用的个人、公司也可以发行通证，这些通证被分割，在链上自由流动。这意味着什么呢?

比方说有一家叫时空梭的公司，它准备把名人的时间变成通证放在链上来卖。有些类似于巴菲特拍卖与他共进午餐的机会。普通专家也可以卖自己的午餐，或者咨询某个专业事项的时间。大大小小的明星也可以向“粉丝”销售共进午餐，共同打球、游泳之类的时间。只要他们有信用，即这些时间都真的兑现了，那么之后就可以继续销售自己的通证。

一家公司，甚至某个人，如果有好的项目以后能赚到钱，但缺启动资金，可以用自己的信用卖通证来融资。有一家叫做SelfSell的公司，允许个人用信用发行通证来贷款，义务就是在未来某个时间开始向贷款者支付本息。

一家公司在推广自己的业务过程中，用发通证的方式来激励用户，例如在酷我听歌就相当于挖矿，听得越久获得的通证越多；例如在阿里妈妈麻吉宝来奖励用户的互动，邀请、分享、答题，都可以获得麻吉宝。这方式让用户可以享受到公司业务未来发展的红利，因为公司做得越好，通证的价值就越高，公司甚至可以直接向通证的拥有者“撒币”。不过，这种基于通证的用户激励出于政策模糊地带，酷我和阿里巴巴由于政策风险都暂停尝试了。

一家公司准备新创一种区块链，如果觉得它未来能改变世界，它就可以发行通证来筹措开发区块链底层软件代码的钱，以及推广这条链的钱-这就是现在大火的ICO了。ICO这个发明的意义，不亚于股份有限公司。只可惜现在做ICO的人，99.9%以上都是在骗钱；参与ICO的人，99.9%以上都是为了炒高通证的价格来割后进场的韭菜，并不是真的相信“改变世界”的鬼话。

6.基于公钥私钥的身份

把眼光再放得更远一些，畅想一下未来至少十年之后，强势的、先进的国家，会怎样通过区块链对那些弱势的、落后的国家进行经济渗透?

美国绿卡非常难获得，公民身份更难（但比获得中国公民身份还是简单很多）。但是，当美国公民的很多经济活动在链上进行之后，和美国公民有经济往来的其他国家的公民，不可避免地也会跑到这条链上来，他们可以非常容易地在链上拥有一个身份，只需一对公钥私钥。这个身份比起美国绿卡要差很多，但他依然可以在链上拥有美元通证和自己的信用。

两个委内瑞拉人，如果都在美元的链上，他们可以通过美元通证进行交换和经济活动。一家马来西亚公司和一家菲律宾公司，可以直接在美元的链上通过智能合约来签订合同。

如果世界上没有另外一个数字化的货币来挑战数字化的美元，那么美元必然会变得比今天更加强势。未来，谁能挑战美元？人们看好比特币吗？还是看好另外一个数字化的法币？

享受区块链红利的正确姿态

最后，希望借区块链概念投资赚钱的人，这里有一个非常稳妥的建议。

2017年下半年开始，随便什么垃圾的股票，沾上区块链的概念，立刻可以一飞冲天。这种状况是人群非理性的突出表现。对于理性的人而言，究竟买什么股票，可以无惧任何兴衰沉浮，百分之百地享受到区块链未来发展的红利呢？

答案很明显:台积电和三星公司。

台积电公司已经在享受加密数字货币所带来的红利了，目前世界三大矿机公司，比特大陆、翼比特和阿瓦隆，都在台积电公司流片。台积电公司工艺技术的高性能，是矿机的不二之选，整个半导体圈子，都被矿机厂给代工厂所下的巨额订单所震撼。

前面讲过的所有应用，不论是现有的加密数字货币应用，还是“生产力的增量式进步” “无政府主义”或“去中介化”的应用，都面临巨大的扩容压力。比特币的区块只有1MB大，平均一秒只能支持七笔交易，比特币现金（BCH）目前扩容到了8MB， 2018年5月扩大到32MB，未来会进一步扩大。2018年1月，金融大亨Calvin Ayre拥有并运营的加密数字货币媒体公司和区块链公司Coingeek宣布资助360万欧元给一个名为 " Terab Project " 的项目。Coingeek将与其合作伙伴Nchain和Lokad一起计划将比特币现金的区块大小扩展到TB级大小，扩容后BCH可每秒处理700万笔交易。

BCH十分钟一个区块，对于前面提到的能承载广告、内容、零售、社交、证券、期货的超级区块链而言，十分钟太长了。或许需要半分钟就追加一个块，一个块的大小可能远不止1TB。如此巨大的规模，外加区链需要众多节点高度冗余，会导致整个社会对服务器的需求增加不止一个数量级，对DRAM （动态随机存取存储器）、 NAND （计算机闪存设备）的需求增加不止一个数量级。

未来，不论区块链玩家谁最终胜出，对CPU的需求和存储的需求，3会推高台积电公司和三星公司的股价，它们是真正拥有原子世界核心找术的厂商，是比特世界必不可少的卖水人。

但为什么没有Intel公司呢？因为区块链服务器相对于传统服务器有巨大的范式革新，就像iPhone和安卓相对于PC （个人计算机）有非常大的革新，这个领域的大概率胜出者是ARM。

区块链简介

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

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

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

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

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

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

在解决“如何交易” “跟谁交易”的问题后，马上就会面临物理隔阂的问题，由于在交易过程中，无法确信这笔通证会不会在途中某个地方被别人修改或是拦截，因此需要一个别人无法破解的密码锁，而某个聪明的科学家就设计出了一组十分复杂的密码锁并用在一个坚不可摧的保险箱中。

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

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

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