Cardano 项目发起于 2015 年，是一个完全开源的区块链平台。由两位重量级的人物创办：Charles Hoskinson 和 Jeremy Wood，均为前以太坊的核心成员。

Cardano 的目标不是构建一个类似于以太坊的协议，Cardano 的目标是构建一个分层次的区块链生态系统，即清算层（Settlement Layer）和计算层（Compute Layer）。听起来有些抽象？用简单的语言来说 Cardano 就是一个集成了数字货币（如比特币，莱特币）和智能合约（以太坊，EOS）的区块链生态系统。Cardano 的直接竞争对手为比特币，以太坊和 EOS。

区域自治，分层区块链生态

为了满足实际的商业需求，Cardano提出核心的分层概念解决当下区块链难以扩展问题。分层是指，目前主流公链中的存储交易是在一条链上进行，而Cardano实行双层双链，分层自治的方针，分为清算层和计算层。

所以 Cardano 提出了分层架构理念，试图将整个体系划分为清算层和计算层两个层次，分别来解决货币和智能合约两个层面的东西。大家可以把它简单理解为区域自治的概念，货币和应用程序可以分别根据各自的特点采用不同的治理策略。这似乎与传统 IT 架构模式：分层式架构模式有点像，Cardano 由两个层次组成：

Settlement Layer 清算层：Cardano 的代币 ADA 在该层进行流通，并且在这一层用户交易是匿名的。清算层是整个系统的支付和清算的基础，主要用来处理数字货币价值的转移。

Computation Layer 计算层：计算层可以简单理解为是改进版的以太坊，主要用来服务智能合约、身份认证、消息通信等功能，以方便开发者在此开发 DApp。

采用分层的技术设计，这样的好处在于，可以针对不同的功能需求做出不同的系统升级或者代码部署，有更高的灵活性。比如，在清算层，如果数字交易出现问题，技术人员是可以通过软分叉来进行代码迭代，而在计算层，如果 DApp 的运行需求有大的变化的话，也是可以单独在计算层进行性能的拓展和升级。这样，就使得整个系统边界清晰，运行良好，同时也实现了更好的拓展和交互性。

值得注意的一点是，Cardano 的分层和 EOS 的分片技术，是不同的概念。分片是同类型链之间的信息交互，而分层则是两条治理理念和治理方式完全不同的链，在同一个生态体系下运行。

除了 Cardano 的分层区块链概念可以用来提高公链的扩展性，我们看到当前主要的区块链扩容方案还有很多，比如 Layer 1 扩容和 Layer 2 扩容。

那 Cardano 的分层区块链生态与 Layer1 和 Layer2 有何不同呢？Cardano 实行的双层双链的治理模式，而 Layer1 主要是在链上操作，Layer2 则是在链下完成，两者不在一个区块链生态系统中运行。

Layer 1 扩容方法，即改进区块链自身，主要是通过增加区块大小和分片（sharding）。Layer 2 扩容方法，则是把计算移到链下，即把运算、交易等业务处理拿到主链之外来执行，只在主链上反映最终的结果，中间过程不在主链做记录。目前，具体的解决方案主要有状态通道（ State Channel ）、侧链、Plasma、Truebit 等，尽管它们解决的问题不尽相同，但它们都是通过链下操作而非链上来实现功能，同时保证足够级别的安全和完整性。业内人士向我们透露，目前，公链扩容已经从 Layer 1 到寄望于 Layer 2。

业内普遍的想法是让共识由 layer 1 来做，layer 2 只负责扩容、提升性能。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。所以，Layer 1 和 Layer 2 的安全等级也是不一样的。

动态权益证明共识算法：Ouroboros

Ouroboros 是 Cardano
采用的共识算法，用于Cardano的清算层，用于代币的价值转移，由 Cardano 自己研发。

但是 EOS 技术负责人 BM 认为 Ouroboros 是 DPOS（Delegated Proof of Stake，权益代理证明算法）的复制品，并且做了相关的修改。Cardano 的创世人兼技术负责人 Charles Hoskinson 和 BM 是前同事，借鉴 DPOS 的一些用法，是有可能的。BM在 2018 年初还曾在 Steemit 上发文畅谈 Ouroboros 算法，认为 Ouroboros
不适合去中心化应用，感兴趣的朋友可以阅读《Peer Review of Cardano's Ouroboros》。

其实，Ouroboros也是一种 POS 机制，与通常的理解的权益代理证明 DPOS 不同，它是动态权益证明(Dynamic Proof of Stake)。

在 Cardano 的运行中，时间被分为 slot，每个 slot 时长为 20 秒。每个 slot 只能产生一个块，若这个块有问题，或者应该产出这个块的“矿工”(也就是 stakeholder 的候选人)不在线，或者产出的块没有广播给大多数人，那么这个 slot 是当作废弃的，也就是会跳过这个 slot 的块。多个 slot 为一个 epoch，权益的计算是以每个 epoch 开始前的历史来计算，也就是说在这个 epoch中所产生的权益变化不影响当前的这个 epoch 中的 slot 的出块者的选择和其他和历史相关的东西。当前 epoch 中所产生的这些历史只能在以后的 epoch 中生效。

把每个 epoch 的 slot 分成 10 等份，整个 epoch 被分为了三个阶段：Commitment Phase, Revel Phase, Recovery Phase，分别占比 4:4:2，对应可验证秘密共享协议的三个阶段。

参看知乎网友金晓的文章，简单的实现流程如下：

1. 从链的真正创世块开始，硬编码进入了一些公钥和这些公钥对应的权益S及初始的随机种子 ρ，之后，这个 epoch 会采用这些基础信息继续运行。

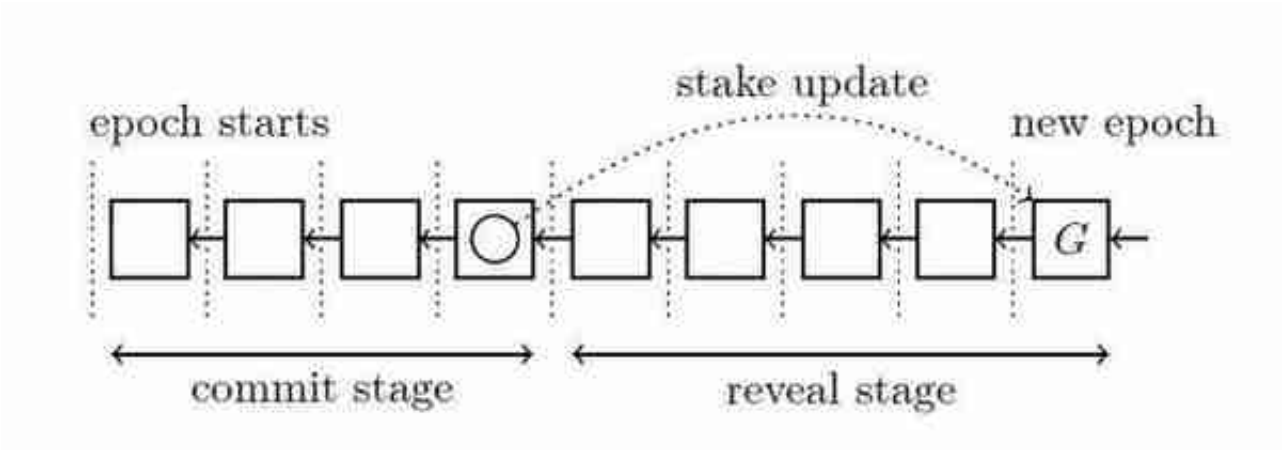
2. 每个节点自己独立运行代码，根据当前 epoch 的随机种子 ρ，执行追寻中本聪算法 F，把 genesisblock 中的权益，随机种子ρ和 slot 的 index 作为输入，根据概率获得当前这个 slot 应该由谁出块。若发现是自己出块，则执行打包交易等等操作，和bitcoin没有太大区别，但是除了基础工作之外，还会生成一个随机数，但是这个随机数不放到链(块)中，而是放一个承诺 Com中。若不是自己出块，则等待出块者出块并广播。收到这个块的时候就进行和bitcoin类似的

检查，要是长时间未收到(超出这个slot 的时间)则会认为这个 slot 的块废弃。

3. 在当前 epoch 中不断重复 2 的流程直到这个 epoch 中的所有 slot 结束。

4. 在整个 epoch 的过程中会产出一个在这个 epoch 参与出块者们(slot leaders)都共同认同的随机种子 ρ。

5. 在自己的内存里记录好这个随机种子 ρ 及下一个 epoch 参与的 stakeholders，开启下一个 epoch 周期，进入 2 的流程。



以上就是 Ouroboros 大致执行流程。

Ouroboros的根本目的就是为了根据权益多少，随机的选出一个记账者，并且随机选择的这个过程是不可预知的。所以看完Ouroboros的执行流程大家应该就可以明白，与DPOS相比，Ouroboros非常重视对随机性的无信任源的需求，以确保生产者调度不受制于区块生产者操纵区块内容以控制调度，用随机性来解决安全问题，所以Cardano生态里的记账权是随机的而且动态的，更加去中心化。

而DPOS共识最大的特征，就是在POS权益证明的基础上，加入了现实世界中的议会选举制度，靠所有持币用户投票选举诞生EOS生态中最终获得记账权的21个超级节点，记账权是可以被人为选择的。

Cardano 团队称 Ouroboros 共识算法是第一个经过 “同行评审” 并“可证明安全”的股权证明共识算法，总体来说，这个算法还需进一步的验证，毕竟这是一个新的算法。

五个发展阶段，目前处于拜伦阶段

根据 Cardano 官网发布的 Roadmap，Cardano 发展路线图分为以下五个阶段。

第一阶段：拜伦（Byron）版本——引导的阶段。拜伦阶段为 Caradano 建立了基准，并允许用户进行交易和转让代币 ADA。

第二阶段：雪莱（Shelley）版本——变成完全去中心化的网络。

第三阶段：哥根 (Goguen) 版本——智能合约的整合。称为 IELE 的下一代虚拟机和通用语言框架，将被用作未来區块链技术的核心基础设施。

第四阶段：巴库 (Bakus) 版本——处理改进智能合约。巴库 (Backus) 版本的功能集中在性能、安全性和可扩展性上。

第五阶段：伏尔泰 (Voltaire) 版本中——IOHK 将添加一个财务系统和治理。伏尔泰 (Voltaire) 版本通过引入财政部门以重点关注保证和可扩展性，这将确保区块链和社区的永续发展和自给自足性。

Cardano 目前正处在拜伦阶段，也是起始阶段，项目目前正在进行改进。这包括代码的改进，比如钱包的后端和调试。Cardano 将改进代达罗斯钱包的设计，并让第三方集成 API 更简单。Cardano 将从拜伦转移到雪莱阶段，网络将变得去中心化。

3 月 25 日，Cardano 宣布完成其 Cardano 1.5 的主网升级。该硬分叉将 Cardano 转为权益证明（PoS）机制，Cardano 称其安全性与工作量证明（PoW）机制相当。

3 月 27 日， Cardano 官方社群宣布 Cardano 与铠钱包 (Yoroi) 和硬件钱包 Ledger Nano S 已正式宣布整合。Ledger Nano S 现在与 Cardano 的 ADA 兼容，投资者们能够通过 Ledger 的钱包保护他们的私钥，并获得更高安全性的 ADA 访问权限。 Ledger Nano S 还集成了 EMURGO 开发的 Yoroi 钱包，这是第一个支持 Cardano Ledger 硬件钱包的官方配套应用程序。

根据公开资料，Cardano 主网上线推迟到今年第二季度。有评论认为，这是因为其共识机制太过复杂，落地难度大。

代币 ADA 全球市值排名第 10

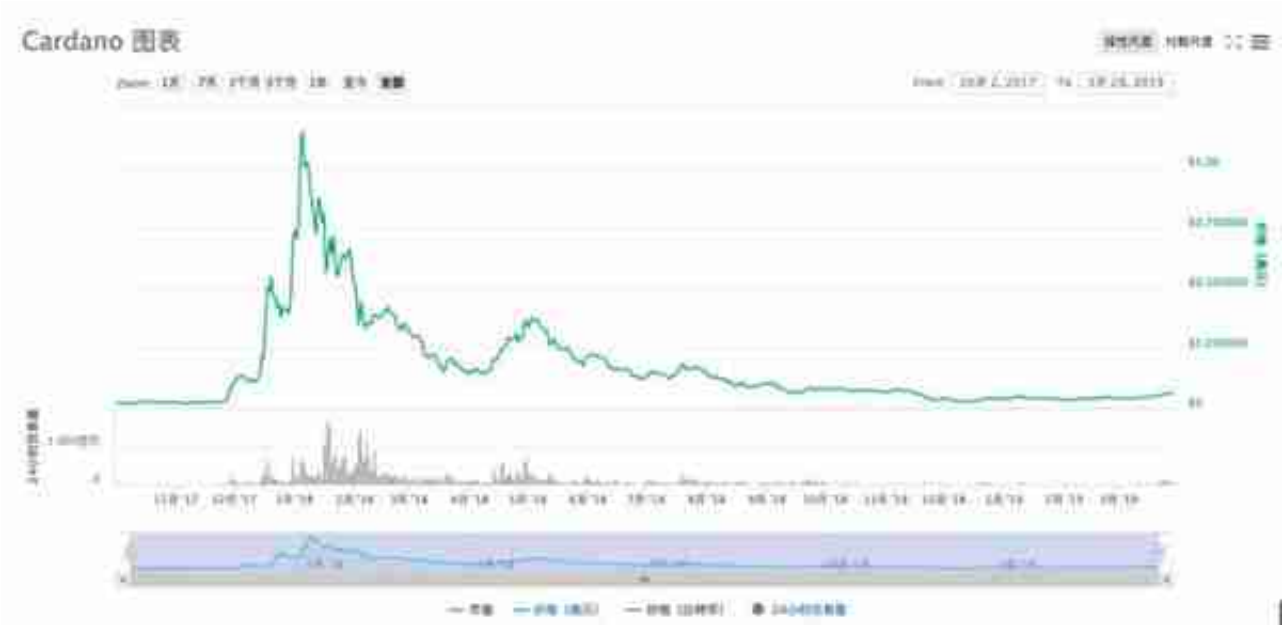
Cardano 的 ICO 并没有公开发行。Cardano 从 2015 年 10 月份开始到 2017 年 1 月结束，总共经历了四个阶段。一共发行总量 450 亿中的 300 亿。由 Cardano 发布的审计结果可以显示，Cardano 所有的投资者几乎都来自于亚洲。尤其是日本，日本投资人至少占到了 90%

以上。

因 ADA 颇受日本投资者喜爱，Cardano 也被称作“日本以太坊”。

根据 CoinMarketCap 最新数据，ADA 目前的流通市值约为 17 亿美元，目前全球市值排名第 10，紧跟在 Tether 之后。值得注意的是，其交易活跃度相对较低，换手率 7.15%，明显低于 EOS 等同类型公链项目（EOS56.93%，ETH12.91%），可见持有 ADA 的投资者相对比较稳定。

大家印象比较深的是，在 2017 年 11 月 25 日到 2018 年 1 月 5 日的 40 多天内，ADA 的价格翻了接近 40 倍，由 0.03 美元涨至 1.15 美元，当时的市值也跃升至全球 TOP5，这样的涨幅即使在波动巨大的币市也是不常见的，更何况当时主要的参与者仅仅是日本投资者。根据 CoinMarketCap 显示，至截稿时止，ADA 最新价格为 0.069美元。



“三权分立”的组织架构，矛盾不断

Cardano 由一家香港的 IT 公司 IOHK 开发，这家公司负责了 Cardano 的整体技术支撑。IOHK 成立于 2015 年，由两个重量级的人物创办：Charles Hoskinson 和 Jeremy Wood。这两位都是前以太坊团队的核心成员。

这里特别要说一说 Charles Hoskinson。他除了参与了以太坊的开发，还曾担任以太坊 CEO，还参与了 Bitshare 的开发，却因和 BM 理念不合选择退出。所以，他和 V 神和 BM（EOS

和 Bitshare 的创始人）都有着紧密的联系。

Charles（右一）与V 神（左一）合影

鉴于Charles与 BM、V
神共事的经历，还有一些媒体直言：如果进展顺利，Cardano
有望成为超越以太坊的 “史诗级” 项目。

同时 Cardano 也与以下几所世界名校保持着紧密的合作：英国爱丁堡大学，美国伊利诺伊大学，美国斯坦福大学。

除此之外，Cardano 项目还有另外两个组织共同推进。

Cardano 基金会（瑞士），主要负责 Cardano 资金监管

该基金会作为 Cardano
项目的最高管理方，提供发展和应用方向，管理项目资金，推动加密货币 ADA 的应用普及，并负责与政府和监管的沟通。

Emurgo（日本），主要负责 Cardano 项目生态布局

它的角色是支持并孵化生态内的其他项目团队，将他们接入到 Cardano 的生态系统当中，从而推进整个项目的生态建设。由于是日本公司，所以 ADA 在日本的市场开发做的更好。

不过，Cardano 虽然采用了 “三权分立” 的组织架构，看似分工明确、运营高效，实则为团队内讧埋下了伏笔。

2018 年 10 月，Charles 与 Emurgo CEO 发布联合声明，公开指责 Cardano 基金会不作为和无能，要求团队负责人辞职并接受审计。同时他们宣称将于 2020 年接管基金会。在公开声明中，Charles 还列举了基金会的八大罪状，包括财务不透明和重大事件陈述失实等。

事实上，这已不是团队第一次出现矛盾和分歧。早在今年 7 月，Cardano 中国社区负责人李德离职后便爆出了一些黑幕：负责项目生态技术布局和投资的 Emurgo CEO 平庸无能、砸盘嫖娼，资方一直在割韭菜……

总结

从底层基础公链的竞争角度来看，Cardano 显然是一个非常有实力的竞争者，分层管理的区块链生态，强大的技术研发团队，以及创始人之前的明星团队背景，未来还是有可能与以太坊和 EOS 争夺公链之王的宝座。

Cardano 的整体目标宏大，如果项目顺利完成，价值和意义都非常巨大，同时，项目的复杂度高，也必然带来很大的开发难度，对此，投资者也应适当审视。

比特币在泥潭里偷爬滚打了 10 年，它安全性是经历了时间检验的。可以说这是所有 “山寨币” 的硬伤。虽然 Cardano 2015 年就立项，但是还是不够久。对于看重短期回报的投资者来说，并不合适。由于话题性和市场认知度不高，而且市值较大交易热度较低，短期内很难有太好的表现。