Cardano 项目研究报告

2018 年 9 月

TokenClub 研究院

目录

1.项目综述

Cardano 项目研究报告

项目	Cardano
评级	A 级
风险	低
发展时期	成长期
标签	底层公链
时间	2018 年 9 月

Cardano 项目发起于 2015 年，名字的由来是来自 16 世纪的意大利数学家 Gerolamo Cardano。而 Cardano 的代币 ADA 则是以 19 世纪英国贵族 Ada levea 的名字来命名，她是拜伦的女儿，被称为人类史上的第一位程式员。

Cardano 是第一个采用多元科学、同行评审的学术型区块链项目。Cardano 的目标是构建分层次的、集成了数字货币功能和智能合约功能的区块链生态系统。Cardano 系统的原生代币为 ADA，基本数据如下：

基本情况	
项目名称	**Cardano**
市值	$27.4 亿
流通量 / 发行总量	25,927,070,538 / 45,000,000,000
流通率	57.61%
发行时间	2017-10-02
最近 24 小时交易量	$0.73 亿

募资情况	
募资时间	2015 年 10 月-2017 年 01 月 共经历（T1、T2、T3、T4）四个阶段
募集资金	$6000 万
众筹成本	$0.0020-0.0026
现价/最高价	$0.105/ $1.22
ICO 涨幅 / 最高涨幅	52.5 倍 / 610 倍

Cardano 设计了一个会计和计算的分层协议，分为结算层 CSL 与计算层 CCL。结算层可以提供转账、挖矿等基础服务；而计算层用户可以运行用 Plutus（智能合约开发语言）编写的智能合约，ADA Token 可以在这两个层间流动。但现实落地过程中存在较大风险。

Cardano 采取权益证明的共识机制 Ouroboros，该算法出自 IOHK 的几位密码学专家发表在顶级会议（CRYPTO2017）上的一篇学术论文，这是一种经过理论证明的 PoS（Proof of Stake）共识算法。

Cardano 开发总共有五个阶段 :拜伦(Byron),雪莱(Shelley),哥根(Goguen),芭蕉（Basho）,伏尔泰（Voltaire)。Cardano 目前处在第一阶段拜伦（Byron），已发布了结算层网络和电子钱包 Daedalus ,可以实现 ADA 数字货币的交易功能；2018 年 9 月份将进入第二阶段雪莱（Shelley）。

目前 ,Cardano 项目对节点的激励只有交易费用 ,而不包括区块生成的额外激励，这可能不利于前期节点的参与。但其采用财政系统的治理机制设计具有创新性，有利于生态系统的建设。在生态建设上，Cardano 开发了 Traxia 应用。

Cardano 项目由 IOHK、Emurgo 和 Cardano 基金会三个实体负责，有很好的区块链技术支持、学术成果和较好的项目孵化能力，同时也有代码审计和众筹审计等监督措施。但是，与竞争者 ETH 和 EOS 相比，目前 Cardano 在社区热度、代码活跃度以及生态建设上明显偏弱。

因此，认为 Cardano 项目评级为 A 级，风险低，处于成长期。

2.行业分析

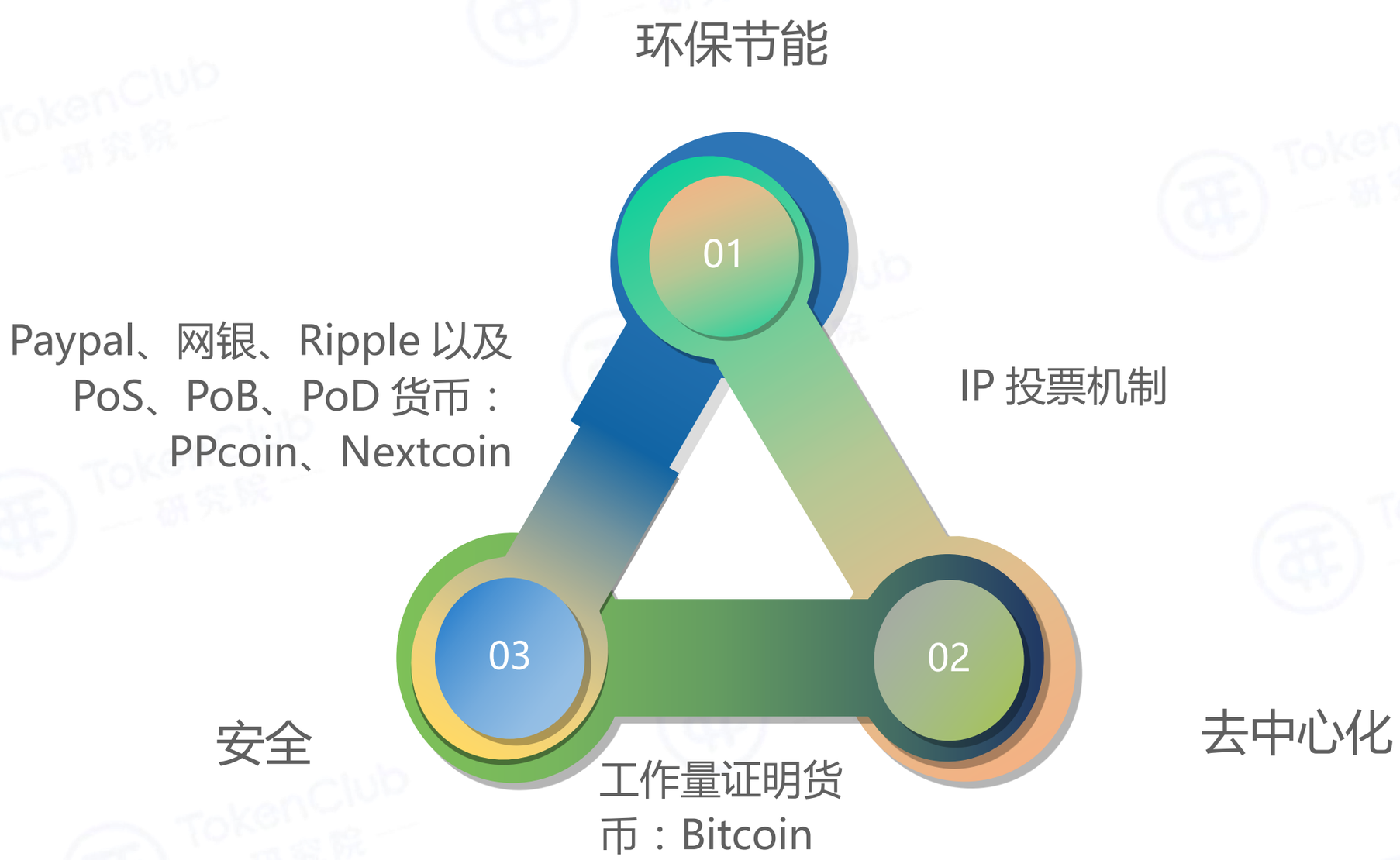
自 2009 年比特币面世以来，短短几年间，区块链和数字货币获得了飞速发展，纵观区块链技术的发展，可以分为三个阶段：

对于整个区块链和数字货币市场而言，区块链项目遵循的是“底层公链 → 解决方案 → 行业应用”的发展逻辑。

底层公链是基础，解决方案是为了拓展底层公链的性能，或是便利底层公链的商业应用，在这些基础上，行业应用才能蓬勃发展。因此，底层公链技术在整个区块链产业链处于头部位置。

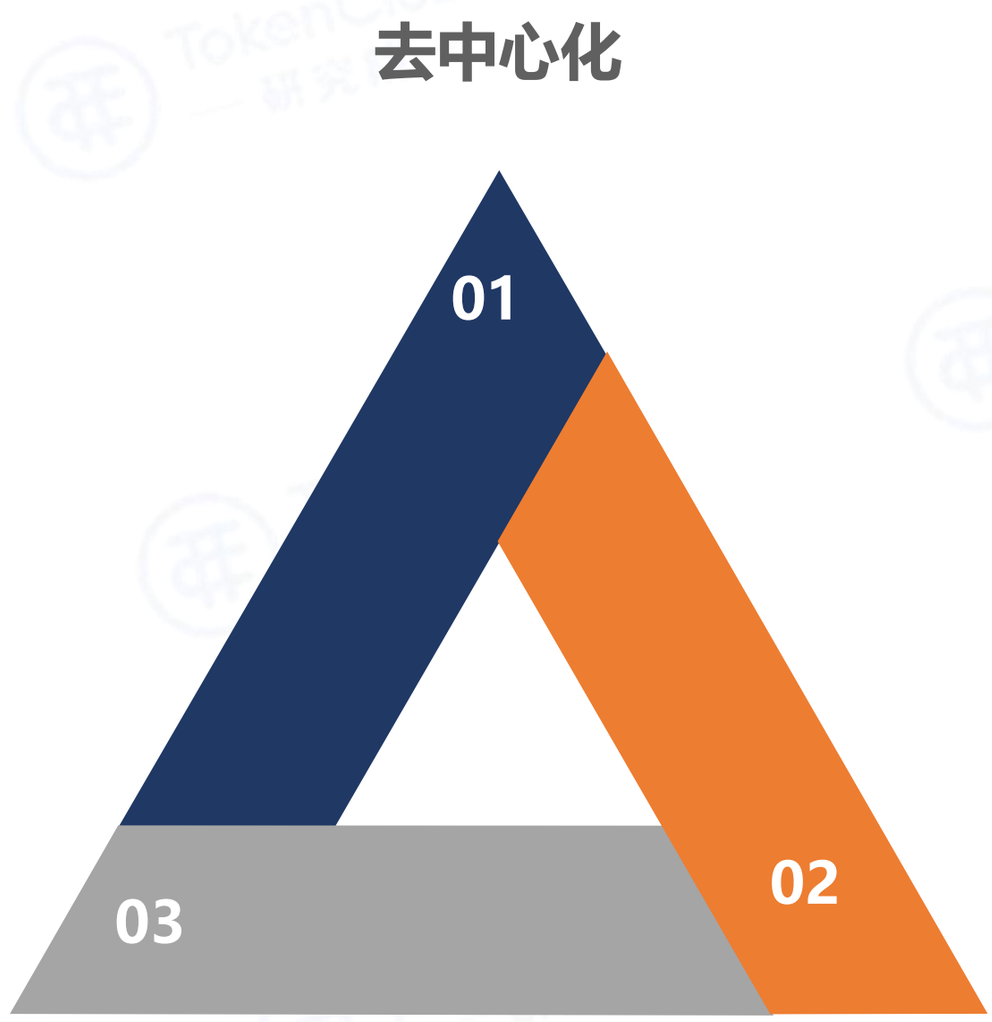
而对于底层公链来说，目前在区块网络转账速度、出块时间、吞吐能力，系统高并发、容错性、稳定性等可扩展性方面有很大限制，离大规模商用性应用（如银行、证券交易所等的交易吞吐量），还有很长的路要走。

巴比特创始人长铗提出了区块链“不可能三角”理念：去中心化、安全、环保构成一个不可能三角形，设计一个符合其中两个特性的数字货币，则必然会使得第三个特性无法达成。



具体到底层公链项目而言，去中心化、可扩展性和安全性三个方面，不可能面面俱到，想要完全的去中心化，则会牺牲一定的可扩展性和性能，想要达到很高的可扩展，也必然面临着中心化的危险，在这两者之外，还要权衡系统的安全性，

目前的区块链技术，还无法实现三者的融合。



以太坊推出了图灵完备的智能合约开发平台，支持代币 Token 经济模型，便利了区块链应用的开发，方便了众多区块链项目的 ICO 众筹、DAPP 智能合约的开发，但由于其可扩展性和性能问题，容易出现网络拥堵、手续费贵等问题，限制了商业化推广和发展。

Cardano 采用 POS 共识算法，通过分层治理来构建区块链体系架构，目标是支持数字货币功能的同时支持智能合约。Cardano 的 POS 具有独创性，他试图在可扩展性、效率、维护成本等方面寻找新的平衡。

3.项目分析

3.1 Cardano 设计目标

3.1.1 采用分层的生态体系设计

Cardano 采用了分层体系，共分 2 层，结算层(CSL）和计算层(CCL)。

结算层(CSL)，是一个通过 POS 协议提供极高网络安全性的区块链协议，Cardano 的代币 ADA 就是在结算层流通

计算层(CCL)，分散式应用 DApps 以及任何智能合约都可以通过该层独立运行

Cardano 的分层与升级版以太坊将采用的分片技术，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。

3.1.1.1 结算层 CSL

Cardano 结算层（Cardano Settlement Layer，又叫清算层）是由 IOHK 联合爱丁堡大学，雅典大学和康涅狄格大学共同设计开发的一种加密货币，代号 ADA。

CSL 承担着保存账户余额的账簿的作用，类似于许多其它现有区块链的功能。同时，ADA 持有者对网络协议的未来发展有发言权和投票权，避免很多不必要的硬分叉。任何对现有网络的更新都会是软分叉，并且保证网络中所有的节点都可以及时更新。

3.1.1.1.1 CSL 账户模型

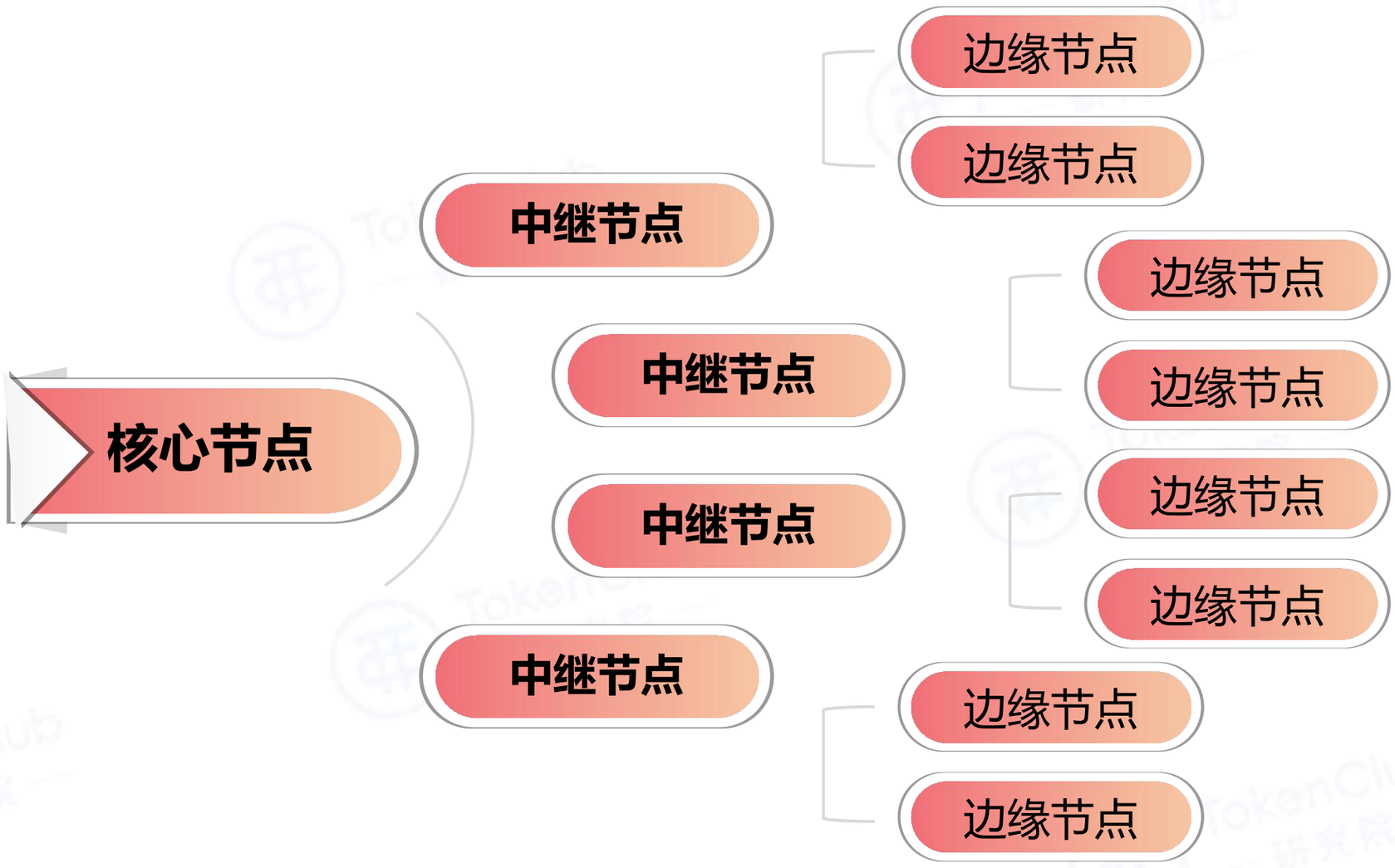
因为结算层对标的是比特币，相对来说是比较单纯的数字货币（所谓单纯是指未附加智能合约之类的设计），所以很多设计沿用了比特币的做法，比如账户模型就采用了 UTXO 模型。

所谓 UTXO，就是指未花费的交易输出，每一笔交易都应该有 N 个交易输入，同时产生 M 个交易输出（N 与 M 可以不等）。其中交易输入是前序任意交易的未花费的交易输出，如果当前交易成交，该前序交易的输出也就变成了成交的交易输出，也就失去了成为交易输入的资格。因此在网络中的每个 slot 领导者不仅仅接收交易，还会验证交易输入的合法性。

为了验证交易，每个节点都必须保持对未花费交易输出的跟踪，这样就可以验证当前交易中的输入是否还未被花费，如果所有的交易输入都是未花费的，那么该交易就被证明是合法的，会被当前领导者接收，打包成块。UTXO 模型能够追踪数字货币的流向：未花费的交易输入告知货币是从哪里来的，未花费的交易输出告知货币往哪里去。

3.1.1.1.2 CSL 网络架构

典型的区块链中的节点间是对等的，随着数据量的增多，才渐渐出现了全节点和轻节点的区别。而 ADA 在网络架构层次上对节点分了层，现阶段，主要有以下三组节点：



- 核心节点，是整个网络的重中之重，所有的权益都集中在核心节点，只有核心节点才可以是权益所有人。只有核心节点是区块链节点，其余两种节点只是辅助节点。而且为了加强核心节点的安全性，完全可以将核心节点与公网隔离，只通过中继节点与外界通信；
- 中继节点，是公网与核心节点的通信代理，由于中继节点是不隔离的，所以他可能被攻击。但是中继节点被设计成无状态的，因此可以使用负载均衡分散流量。中继节点即便被攻击，对核心节点的影响几乎为零；
- 边缘节点，可简单的认为是与区块链交互的客户端，主要负责发起交易，而核心节点和中继节点没有权利创建交易。从名字就可以看出来，边缘节点是没有机会直接与核心节点交流的，必须通过中继节点转接。

3.1.1.1.3 CSL 交易确认

在 ADA 中，领导者出块因为有区块扩散的过程，因此不是一个确定性的共识算法。官方给出了一个交易安全确认的等级表，攻击者的比例越高，需要确认的区块数越多；确认水平越高，相对应的需要的区块数也越多。

3.1.1.2 计算层 CCL

Cardano 计算层（Cardano Computation Layer）包含交易产生的信息和规则，将提供智能合约，身份认证，消息通信等等功能，以方便开发者在此开发程序。由于 CCL 层分离于承担账簿功能的 CSL 层，所以 CCL 的不同用户可以对处理交易创建不同的规则。

CCL 智能合约将使用以太坊采用的 Solidity 编程语言。不仅如此，Cardano 团队正在设计一种名字为 Plutus 的新语言来在 CCL 上开发智能合约。

3.1.2 探索监管与自由之间的哲学平衡

众所周知区块链最核心的理念是去中心化，但不容否认，中心化依然是目前社会运行的主体模式。区块链的去中心化思维难免会和中心化的传统监管之间产生冲突和摩擦，尤其在银行等金融领域显得更为突出，无论是在今天还是在未来，各国政府都很难去主动支持无任何监管下的金融交易。

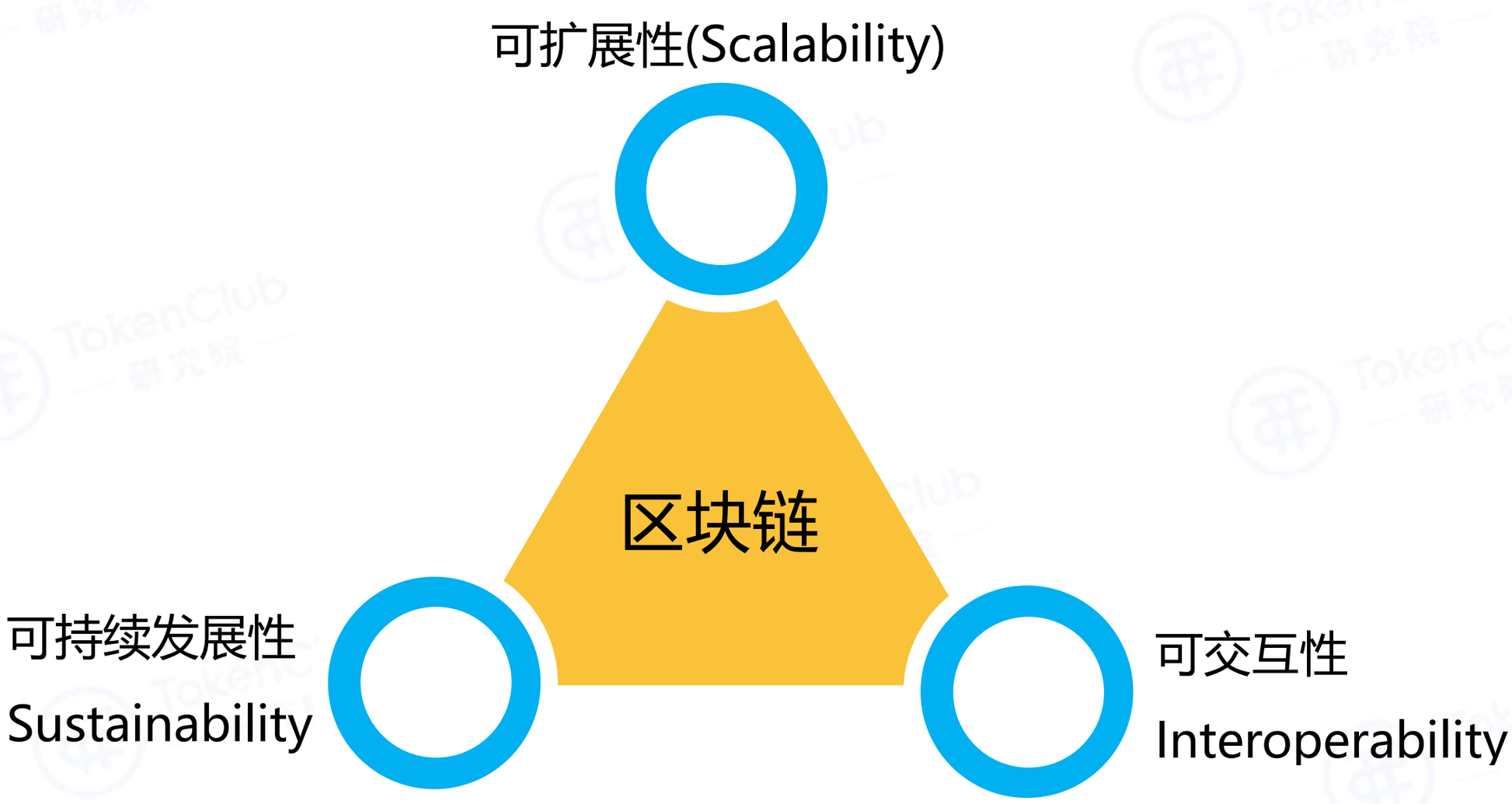
在这个问题上，Cardano 进行了理性审视，并做了另辟蹊径的思考，采取了更稳健实用的折中策略，它认为技术层面需要去中心化的方式来实现，但并不意味着是完全的去监管化。

在 Cardano 的设计哲学中，充分考虑了监管需求，同时也尽可能考虑用户的隐私性，并设法达到二者之间最优平衡点。比如，在必要且用户自愿的情况下，可以针对性的选择提交 KYC（客户身份）和 AML（资金流向）等信息，满足最基本的监管需求。这一切的目的都是希望让区块链金融被社会主流群体更容易接受和使用。

相对于比特币的近乎乌托邦理想，Cardano 未来与政府合作的可能性更大，在中心化组织内部署的阻力会更小。

3.1.3 良好的扩展性、交互性和可持续性

目前区块链生态面临的三个问题：



Cardano 的设计哲学是在学习和继承现有基础公链优点的基础上，进行概念和技术的创新，希望能最终解决上述三方面问题。Cardano 团队展现出了极大的野心，意图集合学术界的前沿成果与工业界的成功经验，打造出一个能被广泛使用并可持续发展的新系统。

3.1.3.1 可扩展性（Scalability）

Cardano 认为是否具有可扩展性，主要受三个因素的影响：TPS、网络带宽以及数据量。

3.1.3.1.1 TPS（Transaction Per Second，每秒钟能够交易的数量）

Cardano 的团队研究了一种被命名为 Ouroboros 的算法。与比特币及它的工作量证明（Proof of Work，简称 PoW）机制相比，Ouroboros 所采用的 PoS 运行成本相对较低，TPS 相对较高。它会根据每个 Daedalus 钱包所拥有的 Cardano 币的数量，随机地进行工作量的分配。这套机制计划在 2018 年 Q2-Q3 开始运行。

3.1.3.1.2 网络带宽

网络带宽指的是进行交易时所携带的数据在进行网络通信时所需要的网络资源。当区块链的规模越来越大时，所需要的网络带宽也将会越来越多，实际上不可能做到每个区块链的节点都支撑所有节点之间进行的通信。

为了解决这个问题，Cardano 采用了 RINA。RINA，名叫递归网络架构（Recursive InterNetwork Architecture）。概括地解释：它应该是一种类似于 TCP/IP 的架构，它可以非常自然地让节点之间的通讯就像进程间通讯（IPC）一样，自然地进行规模化的通讯。RINA 计划会在 2018 年开始加入一部分到 Cardano 当中，并且在 2019 年完成。

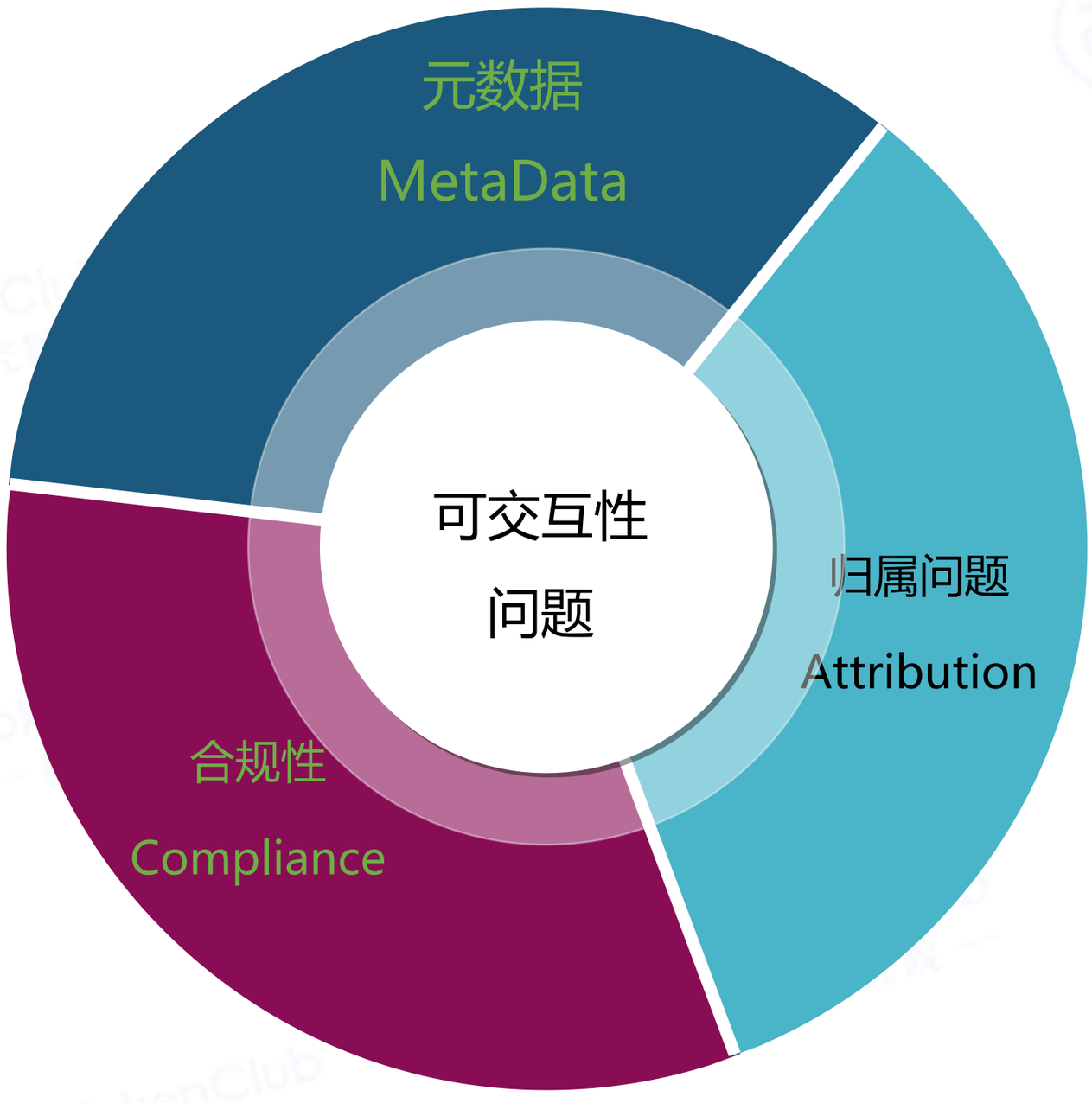
3.1.3.1.3 数据量

在压缩技术上，Cardano 还会涉及到侧链（SideChain）技术。通过侧链，可以使得那些非常小的数据块以双向绑定的形式连接到一起，使得它们具有高级别的安全性和正确性。Cardano 会开发出一种新模式，使得用户只需要保留非常小的数据的同时，获得同样的安全和正确性保障，以应对无限增长的数据量。

3.1.3.2 可交互性（Interoperability）

世界上有非常多种区块链系统，比如比特币、以太坊、瑞波币（Ripple）等。除此之外，还有传统的银行网络系统。这些系统都有自己的业务逻辑和规则，这也导致了系统与系统之间非常难以明白对方。

总的来说，Cardano 在交互性上需要面对三个问题：



3.1.3.2.1 元数据

元数据就是像是每笔交易从哪里来、要去哪里、交易双方是谁、为什么交易等数据，这些数据在区块链世界并不关心，但传统金融系统非常关心，所以需要将这些元数据保存在区块链当中。但是这会涉及到一个隐私的问题，因为元数据都是一些敏感的数据，当然这些数据是不能直接公开的。而 Cardano 要做的，就是弄明白到底哪些元数据需要放到区块链当中，以及怎么放（比如怎么加密）、什么时候放等。并且在存放之后，什么人可以看到。

Cardano 的钱包 Daedalus 在未来的 12 个月内，会支持大量的功能来标注交易和金融活动。这些元数据可以根据用户认为是必需的需求，进而导出或共享。此外，数据可以由三方应用程序操作，用于特定目的（例如税务会计）。其次，Cardano 也正在探索添加对可涵盖散列和加密字段的特殊地址的支援。这种结构将允许用户在区块链上发布元数据，而不需公开揭示它。但是，如果用户想要共享数据，那么它将具有交易享有的所有可审计性、不可变性和时间戳保证。

3.1.3.2.2 归属问题

归属问题说的是关于身份识别，也就是如何识别一个用户。其实它也算是元数据的一种，但是它特别重要。在现在的互联网中，常用用户名和密码去进行识别，但这种方式实际上是非常容易被猜到和被黑掉的。如果说每个人都有一个公钥，那这样在网上就可以非常方便地识别每一个人。而加密币正是生产令牌的工厂，这些令牌可以作为公钥存放在区块链当中。Cardano 正使用这种的方式，来让用户保存和保户自己的资产，以及让互联网识别自己。

3.1.3.2.3 合规性

在金融领域，有三大监管条例：KYC（认识客户）、AML（反洗钱）和 ATF（反恐怖融资）。在加密币世界当中，这些条例并没有被重视，但在传统合法金融体

系中，这三大条例是关键因素。Cardano 正在试图在加密币世界和传统合法金融体系中寻找到一个健康的平衡点，一方面能够提供加密的能力，另一方面也能在每次交易当中加入元数据。

3.1.3.3 可持续发展性（Sustainability）

Cardano 使用了一个名为「国库」(treasury)的“链上资助计划”来解决可持续发展性问题。

每个区块奖励的一部分（25%）会流入国库(treasury)中。国库(treasury)是一个不被任何人所控制的特殊钱包，开发者需要向社区提交改进意见，以及他想要实现这一提议所需要的经费，社区会给这些提议投票，选出最重要的改进提议，一段时间后，国库(treasury)就会给最热门的提议释放资金，来鼓励和资助开发者实现这一改进方案。

国库(treasury)链上资助计划保证了 Cardano 项目的可持续发展，能够源源不断的为后续的研究和开发提供资金保证。

3.2 Cardano 共识机制

所谓“共识机制”，同时也称共识算法（consensus plugin），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，就可以认为全网对此也能够达成共识。

现今区块链领域里常见的共识机制有：工作量证明机制（PoW—Proof of

Work）、权益证明机制（PoS—Proof of Stake）、股份授权证明机制（DPoS—Delegated Proof of Stake）、拜占庭容错证明机制（PBFT/DBFT/BFT—Byzantine Fault Tolerant）。

共识算法	工作原理	优缺点	应用
POW	竞争性哈希计算来确定记账	优点：BFT，不可逆 缺点：消耗大量电能，记账成本高，记账速度慢	以太坊/比特币
POS	用资产的多寡来取得分配获得记账权的概率	优点：低能耗，速度快，不可逆 缺点：寡头优势，失去公平性	以太坊/Casper
DPOS	选取一小群节点做代表进行POS记账	优点：速度更快，相对于POS民主化 缺点：没有考虑账户的重要性	Bitshare/EOS

POW 是算力竞赛，设计一个计算哈希的难题，谁先算出来谁赢，算力高的赢的概率高，算力低的赢的概率低，以这样的方式保证胜出者是随机的，且易于验证。

POS 是选举，根据区块链账本中股权者所拥有权益的比例，随机投票选举下一个出块人。POS 的选举投票需要在非常多的节点之间达成一致，这对一致性验证、防伪等要求较高。为了解决 POS 达成一致性效率低以及无利益攻击（Nothing-at-stake attack）的问题，DPOS 采取在拥有权益的有限集合范围内（即 Leader 之间）进行投票达成一致。

验证基于链的 POS 方案尝试从链上现有数据入手，比如使用上一个区块的哈希值，上一个区块的时间戳等等来作为随机数的来源，但这些会带来额外的安全风险。因为区块本身的信息就是节点写进去的，然后又要根据这些信息来选取后续的出块者，存在循环论证的嫌疑，安全性不会太好。这也是为什么普遍认为 POS 方案不如 POW 可靠的部分原因。

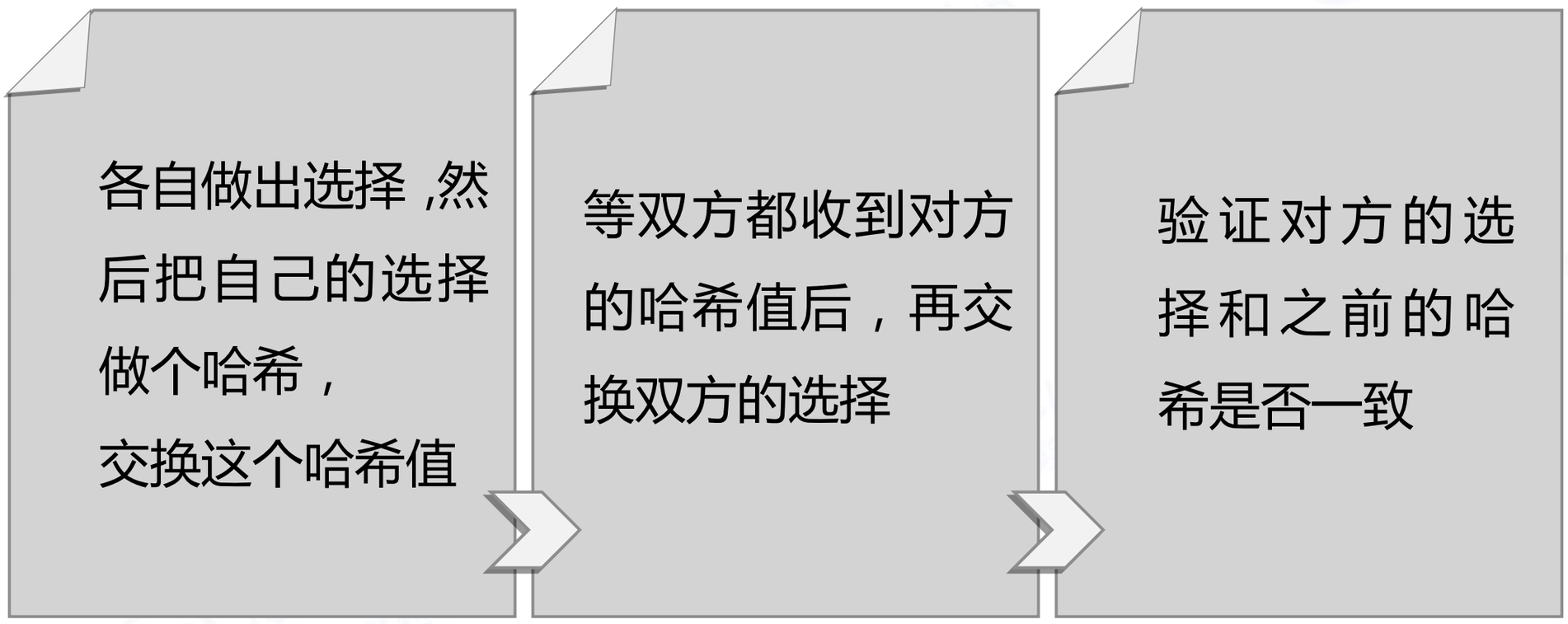
为了确保区块链的安全性，选取股权者来产生区块的方法必须是真随机的。为了

实现领导者选举（Leader election）过程的随机性，IOHK 首席科学家 Aggelos Kiayias 教授领导的团队设计了名为乌洛波洛斯(Ouroboros)的共识机制 ,这也是一种 POS 机制 ,与通常的理解的权益代理证明(Delegated Proof of Stake)不同，它是动态权益证明(Dynamic Proof of Stake)。乌洛波洛斯是第一个具有科学凭证其安全性的权益证明协议，该协议由系统随机筛选产生记账者，从而不会产生恶意攻击。下面首先详细介绍该机制的运作原理。

3.2.1 随机数协议

3.2.1.1 简单随机数协议（Coin-Tossing）

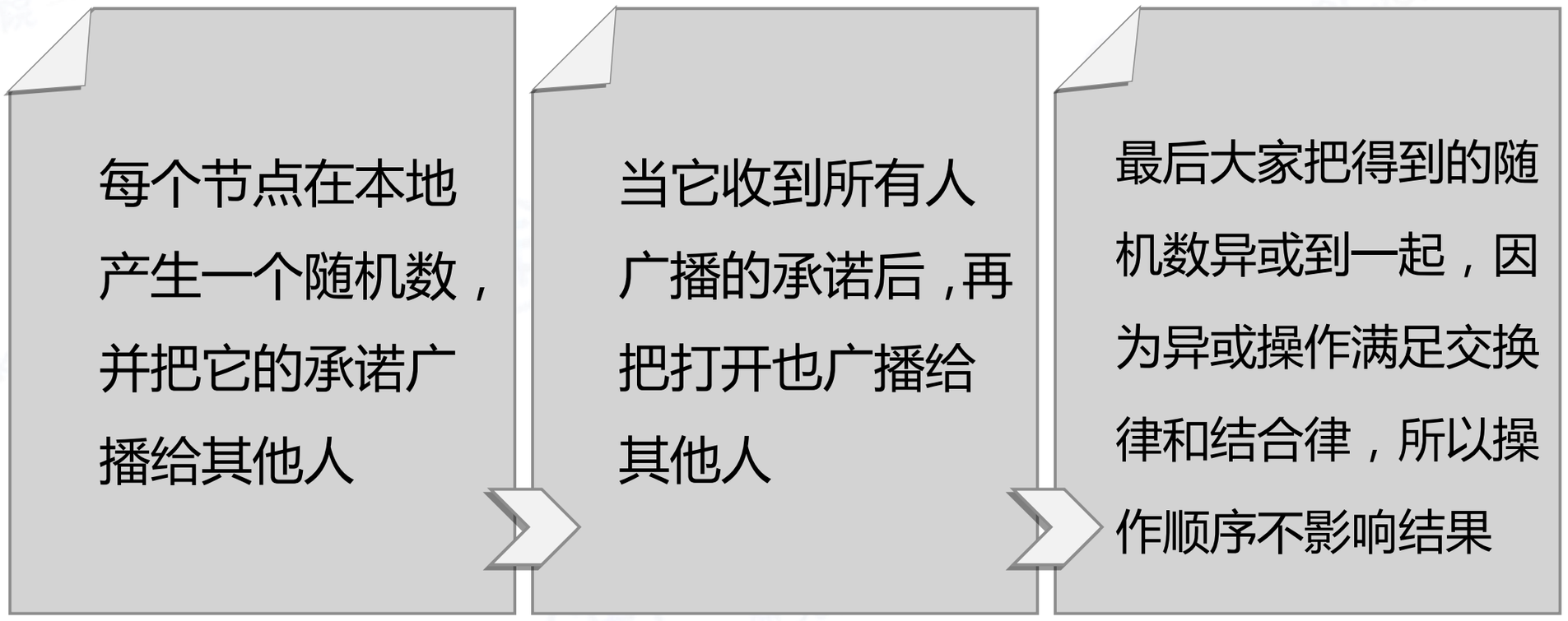
假设张三李四要玩剪刀石头布，用传统方式作弊者如果稍微出的晚一点，可以等看到对方的手势后再做选择。为了防止这种情况，他们分三步执行一套“分歧终端机”流程：



这样双方都知道了对方的选择，也能确认对方的选择是提前就做好的。这个哈希值就叫做承诺（Commitment），因为它里面包含了保密信息，但又没有泄漏保密信息，而最终发送对应的保密信息，就叫做打开承诺（Open）。

3.2.1.2 多方随机数协议

简单随机数协议只是一个两方参与的协议，下面扩展该协议来设计一个生成多方随机数协议：



最终大家都得到了一个一致的无法被操纵的随机数。但这个协议的问题在于，部分节点可能因为网络掉线或者因为恶意可以选择终止协议不发送自己的打开，会使得其他人无法进行下去。

3.2.1.3 可验证秘密共享（Verifiable Secret Sharing）

为了解决多方生成随机数协议中部分节点不可用的问题，乌洛波洛斯引入了可验证秘密共享方案。该方案的规则如下：把一个需要保密的信息，拆分成 N 份，分别发送给 N 个人，只要恶意节点不超过一定数量，最终大家可以综合各自的信息片段把原始信息还原出来。并且就算分发者如果作弊，也可以检查出来。

结合该技术，就有了一个完整的随机数生成协议了。

下面综合一下来看整个协议流程：

提交阶段

每个节点本地生成随机数和对应的承诺，同时把随机数拆成 N 份匹配其他的投票节点，并且用相应投票节点的公钥对每一份信息进行加密，保证它只能被对应的节点解密，然后把承诺和加密后的拆分信息一起广播给区块链

打开阶段

当大家收到大部分节点的承诺和拆分信息后，每个节点把自己的打开广播到链上

恢复阶段

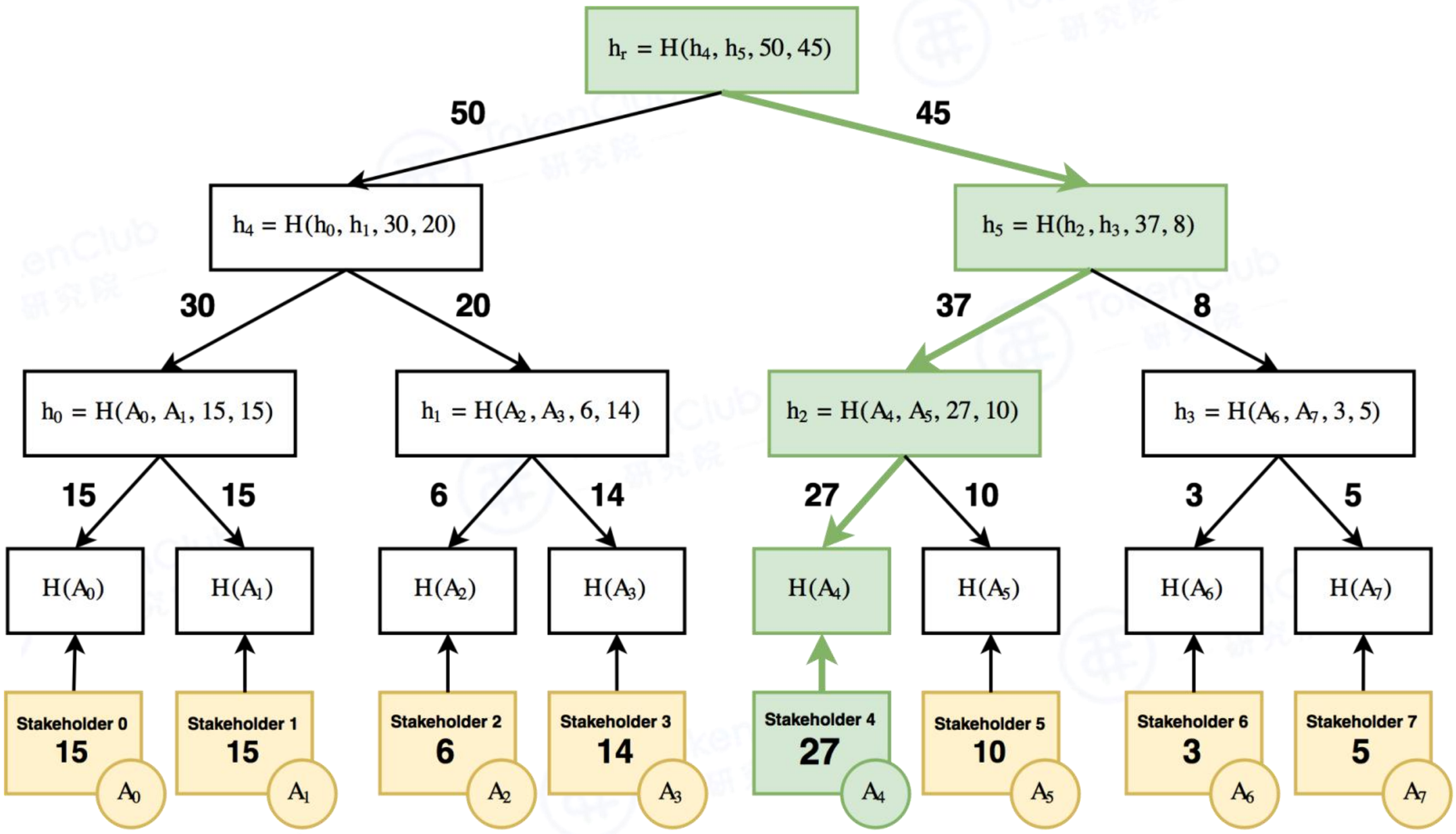
每个节点检查是否有节点发送了承诺但没有发送打开，如果有，则解密自己对应的那份拆分信息并发布，然后根据大家发布的拆分信息恢复出该节点的随机数。现在大家就有了所有节点的随机数，把它们异或到一起，最终得到了一个一致的随机数。

3.2.1.4 追寻中本聪算法（Follow the Satoshi (FTS)）

有了安全的随机数，就可以用该随机数作为随机源，按照各节点的权益比例选择出下一个出块的 Leader，乌洛波洛斯是通过追寻中本聪算法来实现该选择过程的。

```
                +-----+
SEED --->| FTS |---> ELECTED_SLOT_LEADERS
                +-----+
```

追寻中本聪算法的原理非常简单：将所有的权益组成一棵 Merkletree，其形式是非叶子节点的权重为左右子树的权重之和，叶子节点的权重即为某个权益所有者的权益值。然后根据随机数在左右子树中进行选择。



下面分别就选择、验证与实现 3 个阶段来介绍追寻中本聪算法：

3.2.1.4.1 选择

从该 Merkletree 的根节点开始，以前面生成的随机数作为随机源，使用伪随机数生成器生成一个小于当前树节点权重的随机数，如果该随机数小于左子树的权重则选择左子树继续遍历，否则选择右子树继续遍历，直到选择某一个叶子节点，也即选择了该叶子节点所代表的权益所有者作为下一个出块的 Leader。

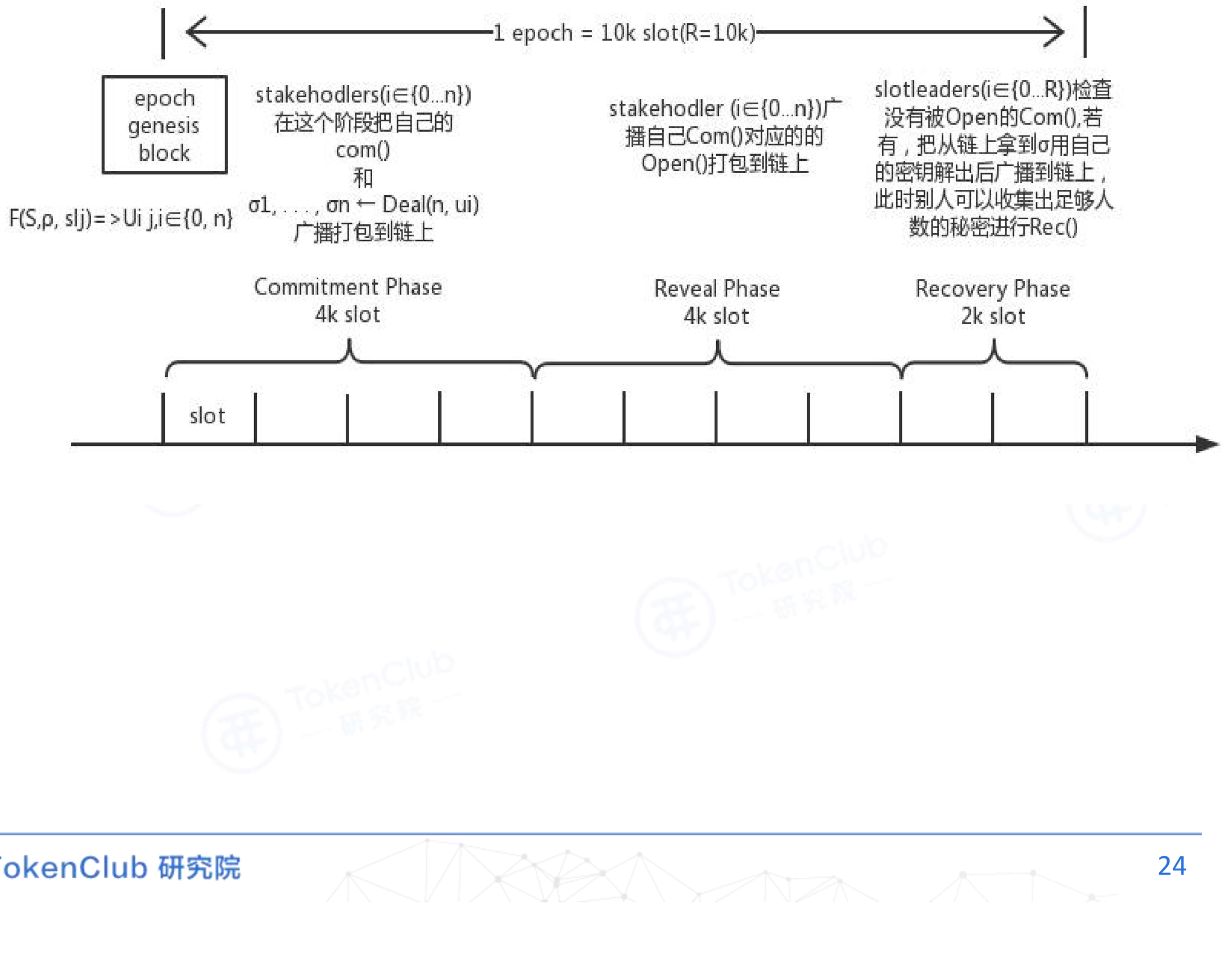
3.2.1.4.2 验证

由于使用的是伪随机数生成器，因此当不同生成器使用同一个随机数当做随机源来生成随机数序列时，该随机数序列是相同的。因此验证的过程与选择的过程类似，从该 Merkletree 的根节点开始，以前面生成的随机数作为随机源生成随机数进行节点选择，然后比较选中的树节点的哈希值，相等则验证通过。

3.2.1.4.3 实现

在 Cardano 的运行中，时间被分为 slot（可以理解为时间段），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（理解为时间片），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。



具体的实现流程如下：

- 1.销售收益审查 – 销售活动收取的资金调节
- 2.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。
- 3.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。
- 4.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。
- 5.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。
- 6.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。

3.2.2 乌洛波洛斯（Ouroboros）协议

乌洛波洛斯（Ouroboros）共识协议，由开发团队的密码学小组设计而成，由爱丁堡大学的 Aggelos Kiayias 教授带领。

Ouroboros 协议将时间分片，称为 epochs。每个 epoch 又划分为多个 slot，在一个 slot 时间段（20 秒）内，有且只有一个领导者，由他负责产生一个区块。如果领导者在他的 slot 期间因为一些原因未能产生区块，那么他就浪费了这次机会，除非再次被选做领导者。也就是说可以有一个或多个 slot 是空的（不产生区块），但是在一个 epoch 期间，必须由大部分的 slot（50%+1）都有区块产生，也就是需要大部分的节点都是诚实的。

slot 领导者被选出来的基本条件是权益所有人，但并不是所有的权益所有人都能被选举，有准入门槛，比如节点权益占比全网权益的 2%。如果按 2% 的准入门槛，那么整个 ADA 网络中，能够成为候选人的节点不会超过 50 个。

随着权益分散，候选人会越来越少，权利会更加集中，而且权益所有人拥有的权益越多，它被选举为 slot 领导者的可能性也就越大，所以也可以说 PoS 是富人的游戏，但是 ADA 中又有一个权益委派的功能，简单理解为：可以将多个账户的权益集中起来使之成为候选人，每个账户可以按照比例获得分红。

在确立了候选人之后，如何选举出在下一个 epoch 阶段的 slot 领导者呢？选举的根本是随机性，在 ADA 中，采用多方计算（multiparty computation）方法来实现选举的随机性，每个候选人都独立的产生自己的随机结果，但经过多方协调后，他们最终得到相同的随机种子。

在对应的 epoch 开始后，所有的候选人节点根据“追随中本聪（follow-the-satoshi）”算法，输入随机种子和 slot 的索引，就可以知道当前对应 slot 的领导者了。如果是节点自己，那么就将自己收到的交易打包成块，跟比特币类似；而如果当前 slot 的领导者不是自己，那就等待着区块广播，如果超过 slot 时间后还未收到区块，则认为该区块跳过。

3.3 Cardano 激励机制

虽然 Cardano 通证的激励机制设计目前还在研究中，但通过官方的资料可以发现，Cardano 的激励机制设计与 ETH 的激励机制设计类似，二者都采用消耗交易费用的方式，且总量有限。但有所不同的是，ETH 的节点挖矿收益来自于前期区块奖励和交易费用，而 Cardano 节点通过区块生成获得的收益只来自于交易费用（不排除通过财政系统给予区块奖励）。与 EOS 的用户激励设计相比较，Cardano 在用户友好程度方面还有部分值得借鉴之处，如 DApp 使用者无直接的使用费用。Cardano 和 EOS 的都是升值的，那么使用 Cardano 的成本肯定会逐渐增加，且币减少；而 EOS 如果整个生态价值的增长每年超过 5%，扣除增发，用户手中的币不变，价值却依然增长了，当然一切的前提是生态发展。

4.团队分析

Cardano 团队由三个组织构成，由 Cardano 基金会，Input Output HK(简称 IOHK)和 Emrugo 公司三方组成。

机构名称	介绍	合作伙伴
IOHK	IOHK 是一家世界级的区块链工程公司，负责构建 Cardano 区块链	-
Emurgo	致力于发展、扶持和孵化商业投资公司并将其整合进 Cardano 去中心化区块链的生态系统中	SIRIN LABS; CHINACCELERATOR; MOX; BLOCKCAMP; LiqEase; SPES
Cardano 基金会	标准化、保护和推广 Cardano 协议技术及其应用	-

4.1 Cardano 基金会（Cardano Foundation）

Cardano 基金会（Cardano Foundation）主要负责 Cardano 的资金监管。该公司是位于瑞士的独立标准机构，其职责核心是支援 Cardano 用户社区，主旨目标是影响和发展新兴商业和立法形式的区块链技术和加密货币，并主动接触政

府和监管机构，与商业，企业和其他开源项目组成战略合作伙伴关系。

基金会工作人员

迈克尔·帕森斯(MICHAEL PARSONS)

主席

英国合格的特许会计师（FCA）和英国数字货币协会(Digital Currency Association ;DCA)创始人一迈克尔·帕森斯（Michael Parsons）是一位知名和受尊敬的独立的区块链技术和数字货币顾问，亦是一位企业家和丰富经验的主讲人。任职过莫斯科毕马威商学院和伦敦普华永道的毕马威银行顾问，迈克尔在银行运作方面拥有超过25年的经验和理解，其中包括领导在迪拜开设银行，这使得他对区块链的新兴潜力，金融服务等领域的分布式分类帐和加密技术应用程序方面有独到之见。

4.2 Input Output HK(简称 IOHK)

IOHK 由查尔斯·霍斯金森（Charles Hoskinson）于 2015 年成立，位于中国香港，是一家领导隐私安全研究和开发的公司，建造和维护 Cardano 平台的合约到 2020 年，专门负责 Cardano 整个技术的开发。

IOHK 负责人为查尔斯·霍斯金森（Charles Hoskinson）和杰瑞米·伍德（Jeremy Wood）

Charles Hoskinson 是一位数学家，在 2013 年 7 月至 2013 年 10 月期间，在比特股担任联合创始人和代理 CEO 职务，后来于 2013 年 12 月至 2014 年 5 月为以太坊这个项目服务，并担任 CEO。Charles Hoskinson 有过与 V 神和 BM 两位圈内大神的共事经历，另一位合伙人杰瑞米·伍德（Jeremy Wood）也是以太坊曾经的高管。

4.3 Emrugo 公司

Emurgo 负责 Cardano 项目生态布局，他的角色是开发、支援和孕育商业企业，并且协助将这些业务整合至 Cardano 的分散区块链生态系统中。Emurgo 将辨别、援助和投资于在 Cardano 平台上建立应用程序的早期阶段区块链公司。除了投资之外，创投公司还将通过与其他区块链公司一起合作，获得研发设施资源，并与需要开发应用的外部公司联系，将其纳入项目中。

Emurgo 已经在菲律宾、韩国和越南等重要地理位置建立了研发中心，总部在日本。在建设社区的第一阶段，Emurgo 将专注于建立基础设施，以便今后部署资金至策略性项目和应用程序构建者。

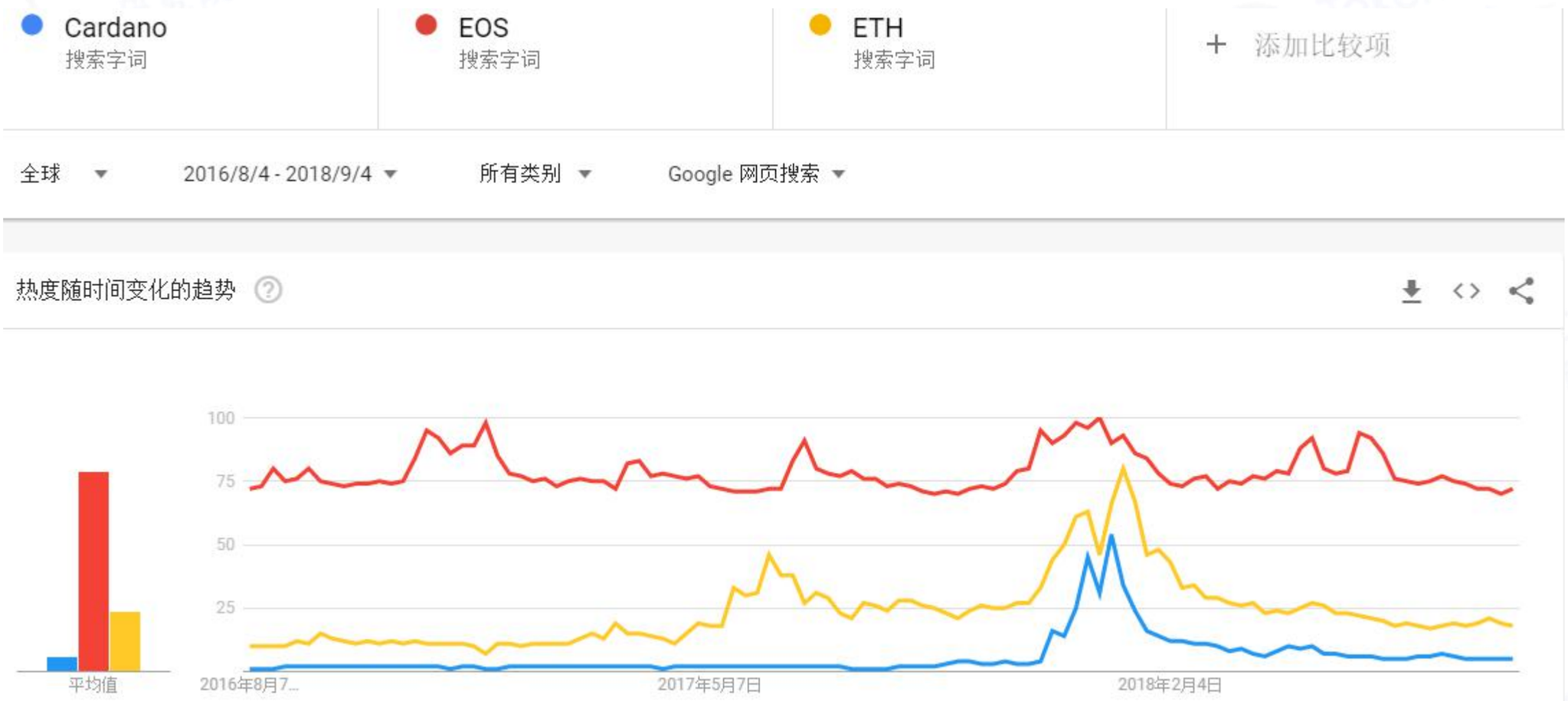
4.4 专家团

除 IOHK 公司外，整个 Cardano 团队还集合了世界各地的专家，核心技术团队由 Well Type、Serokell、Runtime Verification、Predictable Network Solutions 和 ATIX 组成。另外，团队还拥有外部审核人员，如 Grimm、RPI Sec 和 FP Complete，以确保 Cardano 的质量，并负责将团队的承诺传递给大众。

5.社群分析

5.1 Cardano 搜索热度

选取了 Cardano(ADA)、EOS、Ethereum(ETH)、三个主流币种 ,对其 Google 搜索热度进行对比，比较图如下：

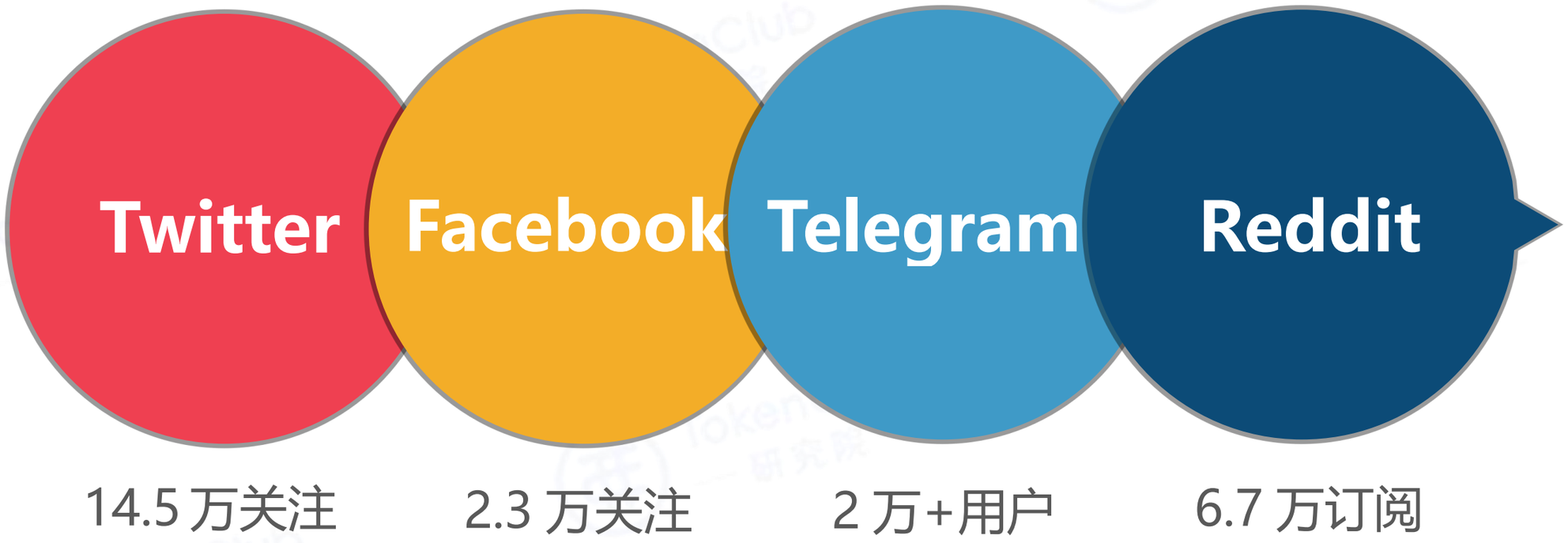


比较 ADA、EOS 和 ETH 的谷歌搜索热度，ADA 的搜索热度在 2017 年 11 月之后出现明显增加，但在 2018 年 1 月之后出现快速回落，其波动趋势与 ETH 相关程度高。近期，ETH 与 Cardano 的搜索热度相近，但有所不同的是，前者还有较高位的热度，后者已降至低位。

综上所述，Cardano 的搜索热度比较一般，市场热度状态处于中游水平。

5.2 Cardano 运营

在社群运营方面，评判的方式主要来自 Telegram、Twitter、Facebook、Reddit 等社区的用户数量和活跃情况，从这些社区来看，ADA 的社群一般。



Cardano 社区遍及德国，西班牙，巴西，新加坡，发过，俄罗斯，意大利，澳大利亚，荷兰，日本，中国，美国，国际化程度较高。

Cardono 的市场运营显得比较低调，负责运营的团队 Emurgo 是一家日本公司，所以 Cardano 在日本市场发展的挺好，其次是韩国，在中国 Cardano 显较为普通，在热度上逊于同类项目 EOS 和以太坊。

从社区反映上来看，用户对 Cardano 生态规划所展现出来的高度、采用同行审议所体现出来的严谨态度、运营团队在项目进度的高度透明及专业都表现出了较高的认可。

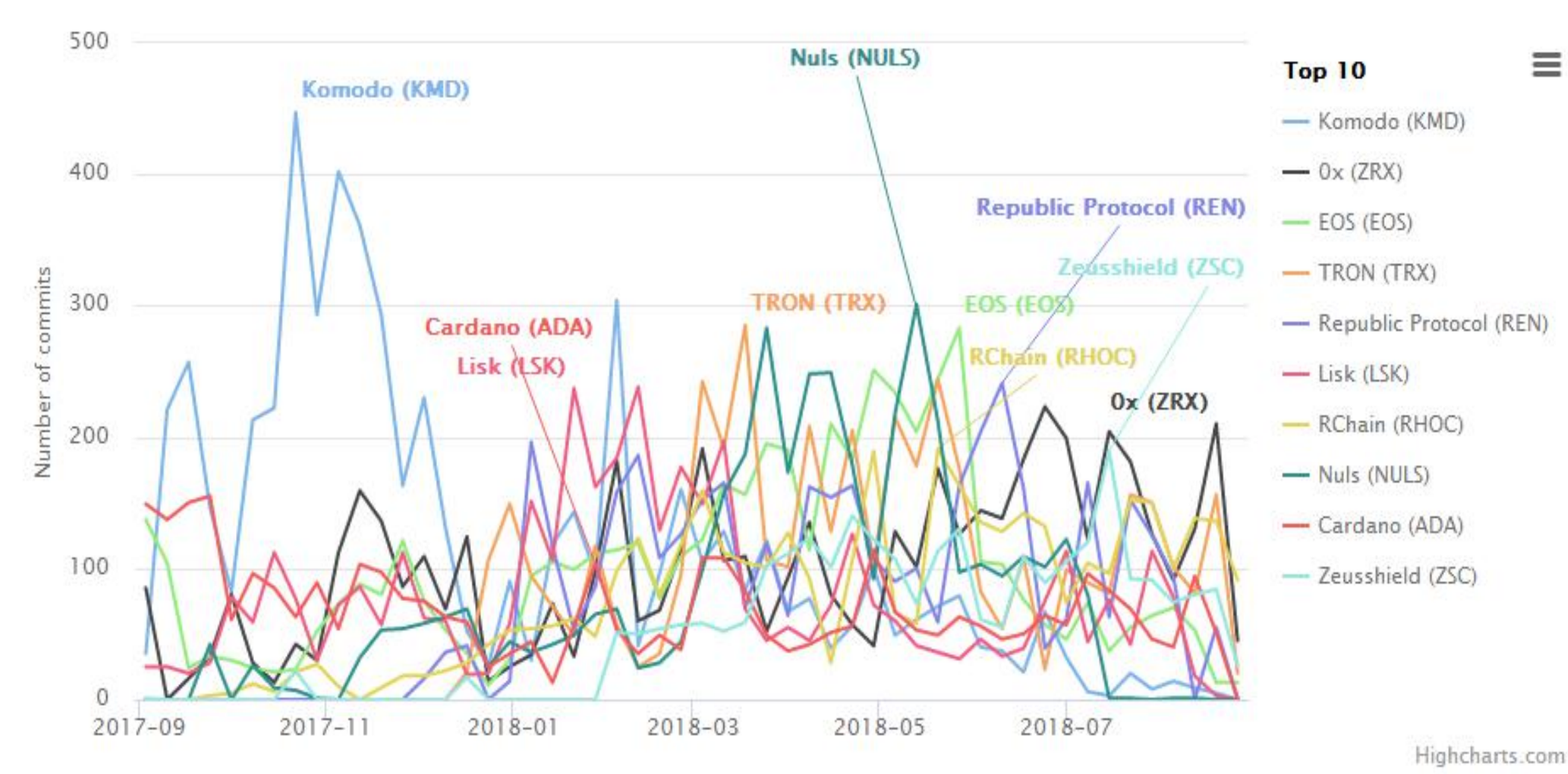
5.3 Cardano 相关活动

合作伙伴	合作内容
西印度群岛大学 The University of the West	IOHK 在该大学免费为 10 位大学生教学了 Haskell 编程语言
国立雅典理工大学 National Technical University of Athens	2017 年 7 月至 9 月，IOHK 在该大学免费为多位计算机科学研究生教学了 Haskell 编程语言
爱丁堡大学 The University of Edinburgh	2017 年 2 月 24 日，IOHK 和该大学建立了区块链科技实验室
东京工业大学 Tokyo Institute of Technology	2017 年 2 月 15 日，IOHK 和该大学创建了加密货币协作研究讲座
埃塞俄比亚的政府	2018 年 5 月 4 日，IOHK 与埃塞俄比亚科技部签署了一份协议，旨在培养该国的区块链技术人才，并在农业技术行业使用 Cardano 平台
科研论文	团队曾就方案核心在同行评审的杂志上发表过两篇科研论文，分别是 Crypto 和 ACN，虽然并非顶级期刊，但能通过同行评审，说明团队的科研素养和科研能力得到了认可

6.代码分析

Cardano 在 GitHub 上的代码已开源，使用 Haskell、JavaScript、Scala、Nix、PureScript 编程语言构建，一共有个 77 代码仓库，核心代码库为 cradano-sl，一共提交 15615 次，85 位贡献者，发布版本 32 次，被 fork 491 次，标星 2927 多次，Issues 108 条。

据 CryptoMiso 网站统计，一年以来，ADA 的代码提交率跻身排版前十，位居第九名，反映出 ADA 代码提交量较高。



据 Openhub 的统计数据可以发现，代码库 cardano-sl 的代码总行数在 2017 年期间迅速增多，但在 2018 年之后代码总行数几乎没有增加，开发进度明显放缓。

Cardano 选择了很多第三方参与代码审核与建议，其中 FP Complete 会定期对项目整体状况出具审计报告。报告主题共分为六大部分：代码、代码管理、整合一致性、依赖关系、文档与质量，分别从细节上对项目代码的各个方面进行审核并提出建议。从报告中可以看出，FP Complete 对 Cardano 的开发过程有着持续的关注，并且对发现的问题会区分优先级进行跟进。对提出的问题，Cardano 开发团队都会进行研究并做出解释。这种正式的第三方代码审计在开源项目中并不多见，这一方面显示了 Cardano 团队对开发质量的重视，另一方面可能也与 Haskell 的开发者较少，无法完全依靠社区进行监督有一定关系。

7.项目进度及落地分析

7.1 Cardano 开发路线图

从官网披露的蓝图规划上，Cardano 总共有五个阶段：

拜伦(Byron),雪莱(Shelley) ,哥根(Goguen),芭蕉(Basho),伏尔泰(Voltaire)

拜伦

目标：结算层主网，Ouroboros 共识协议，Deadalus 钱包，交易所 API，日至提交机制

目前进度：结算层主网于 2017 年 9 月 28 日启动，Deadalus 钱包可以下载使用，作的交易所提供的性能优化以及交易速度的提升，性能优化及交易速度提升已完成 90%。

雪莱

目标：委托于权益池测试网，多重签名账户、纸钱包、多账户钱包与第三方钱包等功能，改进网络层安全性与性能，抗量子签名，团队与社区建设

目前进度：授权代表团（核心节点）开发已完成 75%，共识奖励和费用研发已完成 80%，其余钱包与客户端的改进大部分已经过百，整体进度符合预期

哥根

目标：整合智能合约，实现侧链（计算层），实现多种记账模型和多种通证账本，实现编写运行智能合约所需组件，如 Plutus，Plutus Core,IELE 等

目前进度：侧链开发已完成 75%，记账模型完成 60%，将于 5 月 28 日发布 KEVM，8 月 29 日发布 IELE VM。整体哥根测试网络完成 50%

芭蕉

目标：性能改进

伏尔泰

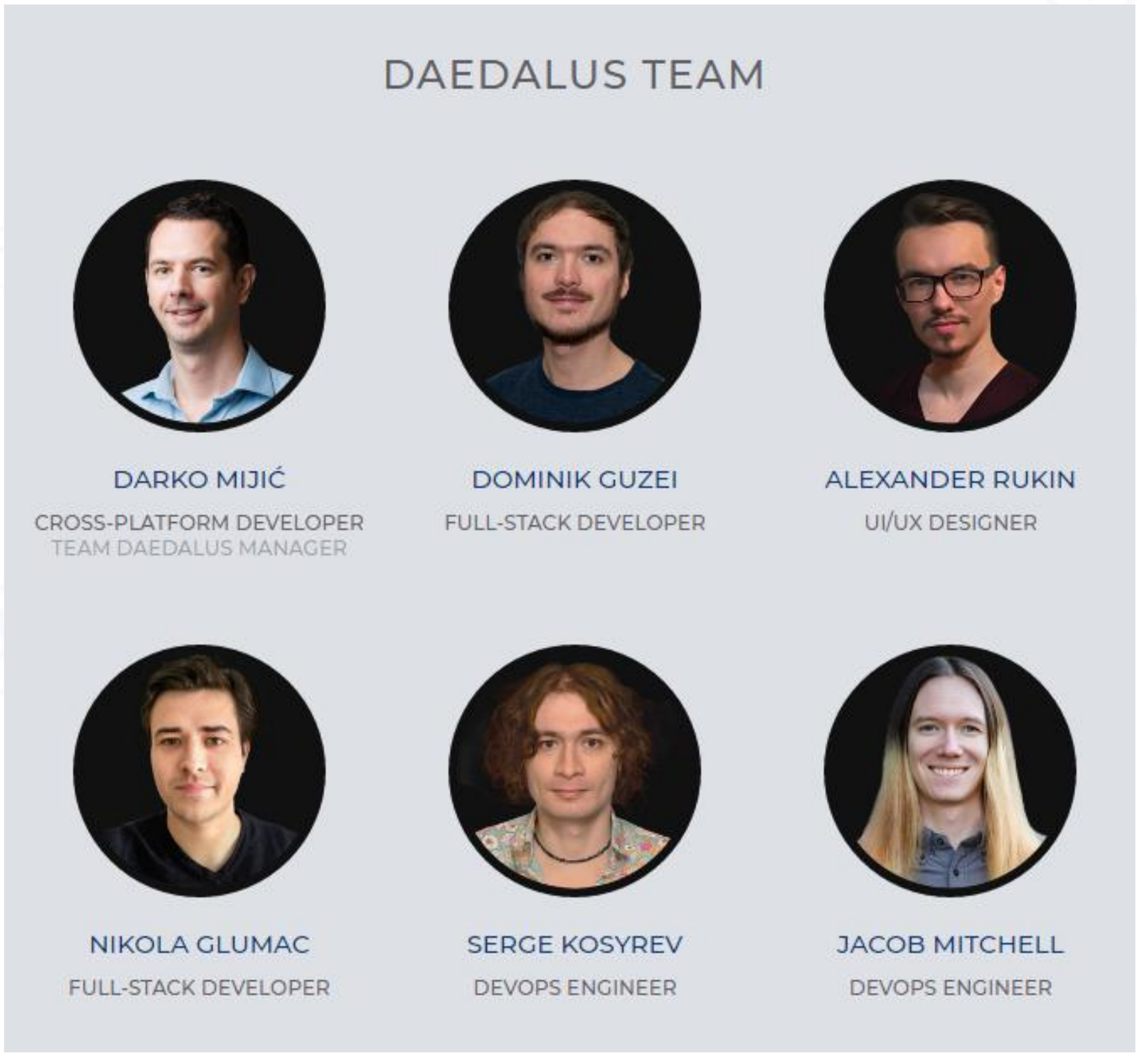
目标：实现财务系统和治理系统

7.2 Cardano 项目进度

Cardano 目前处在第一阶段拜伦（Byron），已发布了结算层网络和电子钱包 Daedalus，可以实现 ADA 数字货币的交易功能；2018 年 9 月份将进入第二阶段雪莱（Shelley）。Daedalus 钱包是现阶段唯一可用的 Cardano 钱包，它是一个 Web 版钱包，钱包下载后，最少需要 6 小时以上的区块同步才能使用。Daedalus 钱包出现后，欧洲部分连锁酒店品牌也已经开始接受 ADA 数字货币支付。

目前来说，Daedalus 只能存储 Cardano 代币 ADA。未来，Daedalus 也可以存储和传输比特币和以太坊经典这样的加密货币。除了作为钱包使用外，Daedalus 未来也将具有分发应用程序的功能。这些应用程序是由 Daedalus 社区开发的。

Daedalus 钱包开发社区主要成员



IOHK 将要在 2018 年 9 月份发布 Icarus 钱包，一个轻量级的钱包。这将使开发者可以为 Cardano 创建他们自己的钱包。Yoroi 是第一款使用 Icarus 构建的 Cardano 钱包，这是 IOHK 发布的参考实现。

Yoroi 是一款新的 Cardano 轻客户端钱包，这个钱包简单，快速，安全，并且以插件的方式运行在 Chrome 浏览器。这也是除了 Daedalus 钱包以外的另一个选择。测试版的钱包将在八月中旬连上 Cardano 的测试网，而最终版本会在九月中旬发布。

在官网中，Cardano 会不定期更新的还有每周的审计报告和技术报告。
不过，官网的每周技术报告，到 2018 年 3 月 1 日就停更了。而且，2017 年 7 月-10 月的报告还比较详细，但是到 2017 年 11 月以后的报告就仅仅列了标题，并没有详细内容。

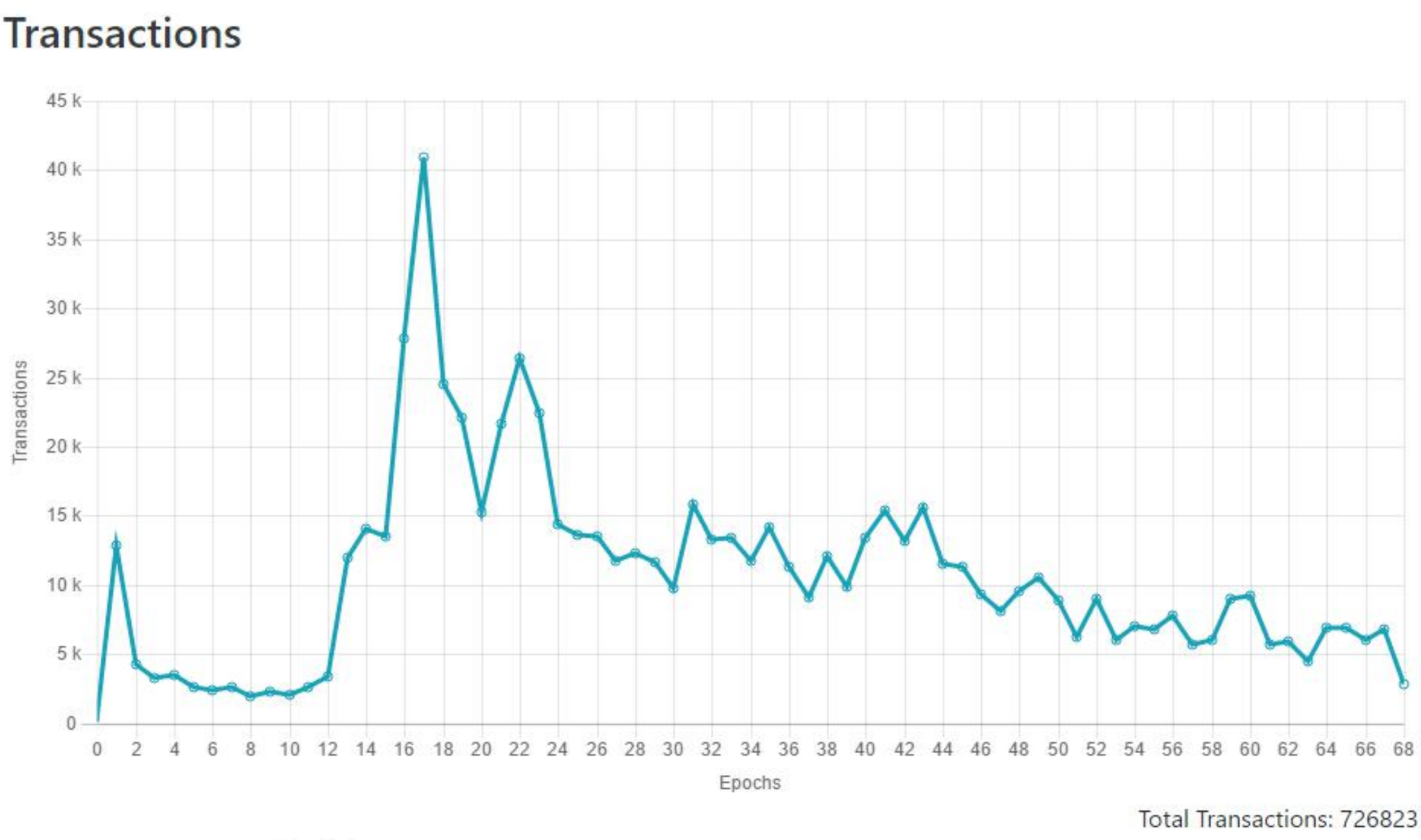
Traxia 是 Cardano 上构建的首个应用。它是一个通过智能合约在区块链上运行的新的贸易融资平台，它结合了区块链和开放的互联 IT 架构，来打造贸易融资新的生态系统，以改善全球贸易融资。Traxia 的愿景是建立一个开放和分散的生态系统，它允许企业从创建智能合约到自动执行，可在货物通过供应链时实时触发付款和收据。

基本情况	
项目名称	**Traxia**
市值	$43,516,521 亿
流通量 / 发行总量	490,466,667/1,000,000,000
流通率	49%
发行时间	2018-4-30
最近 24 小时交易量	$0.73 亿
现价/最高价	$0.0129/$0.1057

募资情况	
募资时间	2018 年 5 月 3 日至 2018 年 6 月 2 日
众筹成本	$0.055
众筹用币	ADA，ETH 或 BTC
众筹金额	$1510 万
首发交易所	2018 年 6 月 6 日，首发 trade.io 和 gatecoin.com

7.3 Cardano 主网情况

Current Epoch	Time Remining	Txs Rank	ADA Flow Rank
68	3 d 20 h 39 m 20 s	60th	67th



此图为 Cardano 主网运行以来所有 Epoch 的 token transactions(ADA 币转账次数）统计。

根据 https://adatracker.com/charts 网站显示的信息，自 Cardano 主网 2017 年九月底上线以来 ,截止 2018 年 9 月 1 日 ,Cardano 主网运行至第 68 个 Epoch。目前的主网完全由 IOHK 运行的，并没有做到去中心化。2018 年 Q2 和 Q3 会将允许开发者创建权益池并逐渐使得 Cardano 去中心化。

根据 https://arewedecentralizedyet.com/提供的数据 ,现阶段还是由 Cardano 自己运行节点服务，从外部看来，Cardano 只有一个节点服务器。

Name	Symbol	Consensus	Miners/voters Incentivized?	# of entities in control of >50% of voting/mining power	% of money supply held by top 100 accounts	# of client codebases that account for > 90% of nodes	# of public nodes	Notes
Bitcoin	BTC	PoW	Y	4	19%	1	9624	
Ethereum	ETH	PoW	Y	3	34%	2	15708	
Ripple	XRP	RPCA (voting system)	N	1	81%	1	732	
Bitcoin Cash	BCH	PoW	Y	3	25%	2	2124	
Stellar	XLM	FBA	N	1	95%	1		
Litecoin	LTC	PoW	Y	3	44%	3		
Cardano	ADA	PoS	N	1	40%	1	1	

During the "Boostrap" era, Cardano runs all the validating nodes themselves. Hence 1 for everything.

目前 ADA 平均出块时间：3.5 分钟。Cardano 主网被限制在 10 到 20 左右 TPS，Ouroboros 在测试环境下能达到 250 TPS，未来有望提高。

8.代币经济模型分析

8.1 代币分配方案

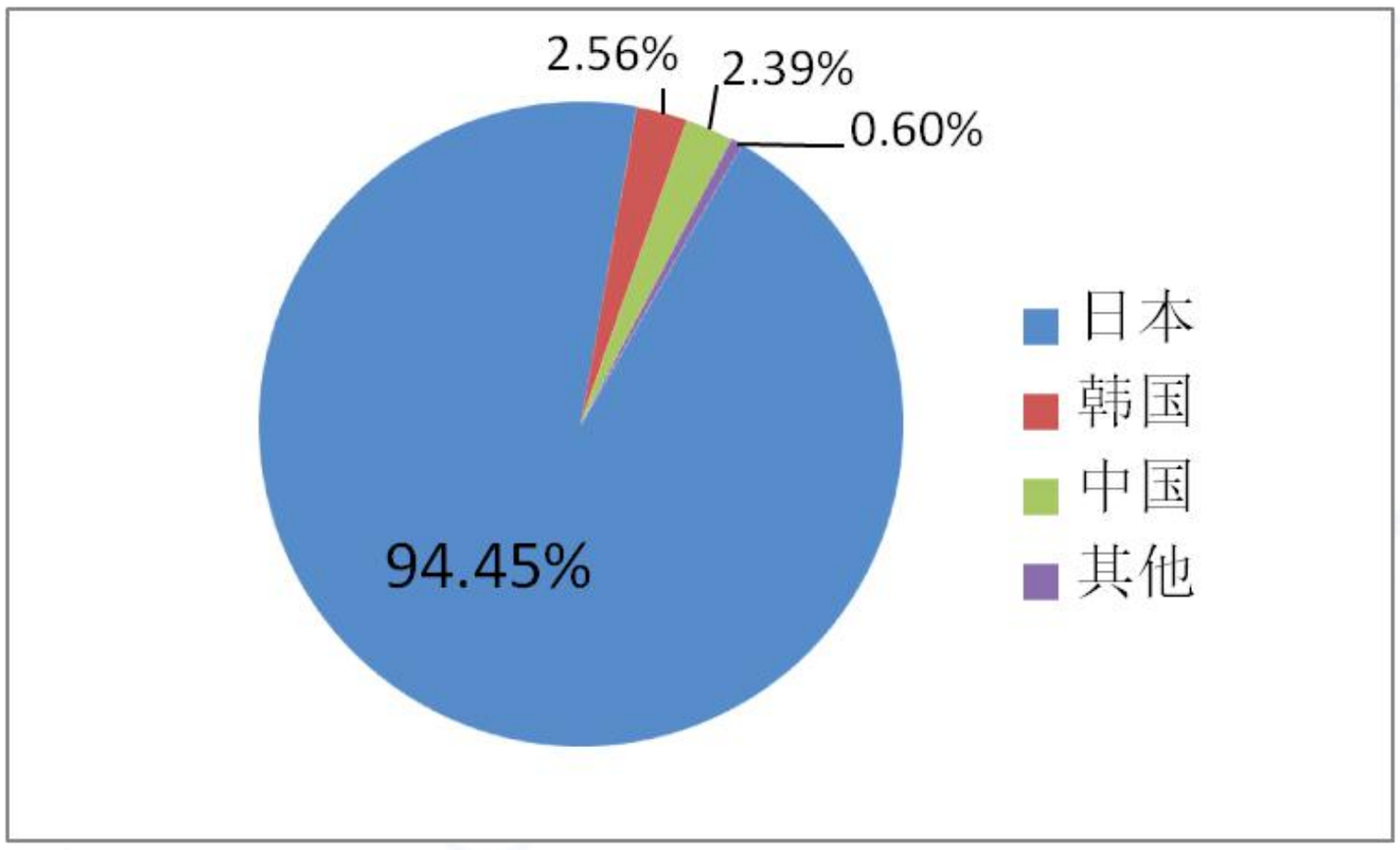
根据 Cardano 官网提供数据 ,作为 Cardano 结算层之一的 ADA token ,在 2015 年 10 至 2017 年 1 月初期间，主要在亚洲市场进行了四个阶段的募集，共募集资金 6000 万美金。ADA 总量 450 亿 ,预售期将投入 300 亿个艾达币 ,其中 250 亿个用于 ICO 其余 50 亿用于开发公司运营公司的资金支持。还有 150 亿个 ADA 币剩余，这部分将会以奖励等形式不断发放。

Cardano 区块奖励将以每 3.5 分钟发放一次，发放频率参考如下：最初每个区块产生 2000 个艾达币，共计 3,744,961 区块；第二阶段每个区块产生 1000 个艾达币，共计 3,744,961 区块；第三阶段每个区块产生 500 个艾达币，共计 3,744,961 区块。以次类推，以每 3,744,961 区块为单位陆续减半，以每分钟产生 3 个区块的速率,直到全部释放完，大概需要 24 年的时间。每个区块产生的艾达币 75% 用于持有者的奖励，25% 作为项目启动后，技术开发、生态建设者的奖励。只要参与 cardano 应用的研发建设，都有可能获得奖励。

理论上，假设市场容量（Market Cap）恒定的话，每个 ADA 的价值会降低，但这种情况包括比特币等很多加密货币都存在，作为投资者应该理性分析货币流通数量增加会带来的影响。

从官方更新的募集数据来看，Cardano 的日本投资者占到了众筹总额度的 94.45%，韩国投资者占到 2.56%，中国投资者占到 2.39%。中日韩投资者占到

众筹总额度的 99.4%。从这些数字可以看出，无论是公募阶段，还是目前的交易，论坛的数据，较为活跃的 Cardano 参与者大多为亚洲投资者，美国、欧洲等其他国家的主流玩家还没有深度参与。



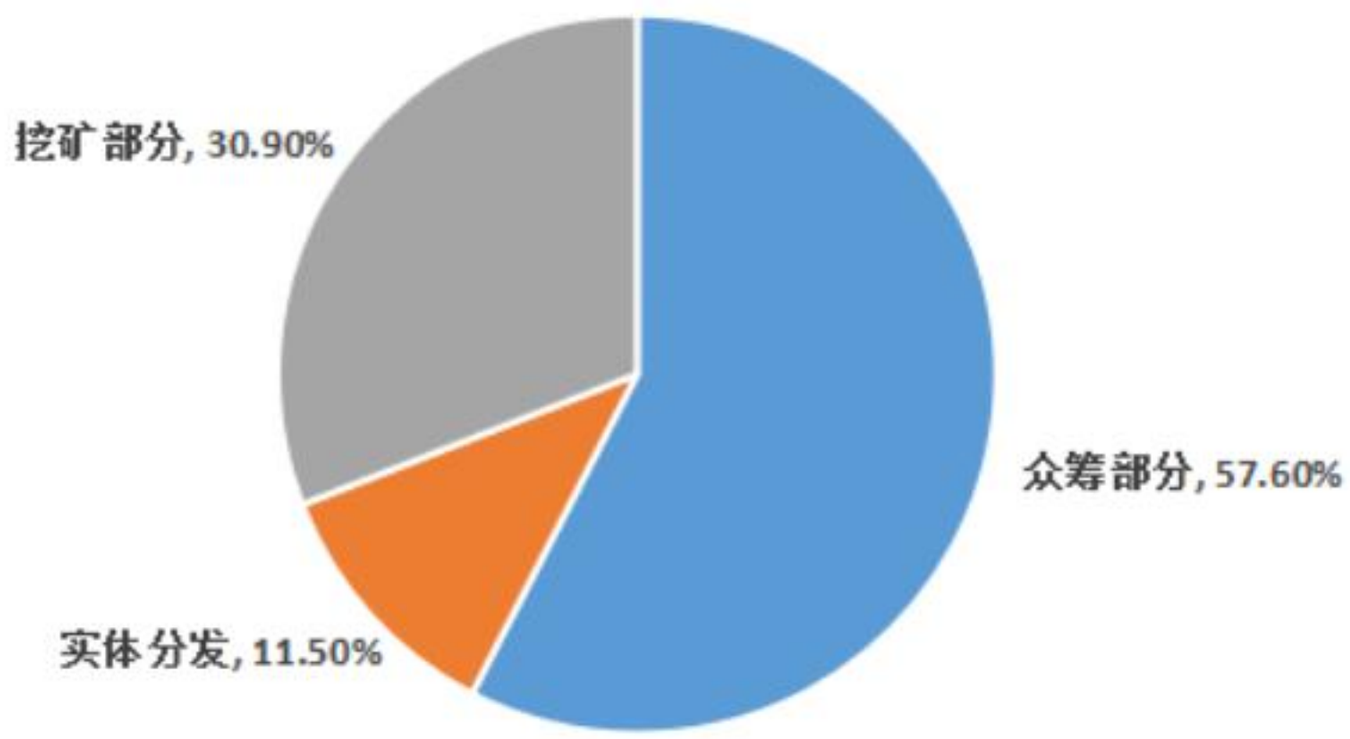
截止 2018 年 9 月 2 日。根据 https://adatracker.com/richest 提供的数据，ADA 代币持数量前 20 名的情况如下。

The Richest Cardano Addresses

#	Address	Balance (ADA)	Share	Tx Num	First Tx	Last Tx
1	DdzFFz...P9uv8K	2,778,785,379.133259	9.48245%	132	2018-08-22	2018-08-29
2	Binance	2,661,357,121.002707	9.08173%	86813	2017-11-30	2018-09-02
3	IOHK	2,414,658,116.670523	8.23988%	7	2017-12-08	2018-08-28
4	DdzFFz...2PLrTm	1,037,082,821.000000	3.53899%	2	2018-01-22	2018-01-22
5	DdzFFz...BneRas	648,176,761.600000	2.21187%	8	2018-06-27	2018-06-27
6	DdzFFz...uq4Atb	337,051,917.000000	1.15017%	2	2018-08-27	2018-08-27
7	DdzFFz...WhHPZ4	269,252,741.850194	0.91881%	2277	2017-12-18	2018-09-02
8	DdzFFz...8uknce	266,135,694.758598	0.90817%	1	2018-07-04	2018-07-04
9	DdzFFz...pjfpPN	233,343,635.000000	0.79627%	2	2018-08-27	2018-08-27
10	DdzFFz...XCfydi	231,093,408.491064	0.78859%	1	2018-06-25	2018-06-25
11	DdzFFz...M7L2va	200,000,000.000000	0.68249%	2	2018-05-05	2018-05-05
12	DdzFFz...ZkXHp3	182,786,646.925087	0.62375%	1	2018-08-28	2018-08-28
13	DdzFFz...ooCcBd	175,352,502.559665	0.59838%	1	2018-07-21	2018-07-21
14	DdzFFz...bJYYCD	140,623,918.285555	0.47987%	1	2018-03-18	2018-03-18
15	DdzFFz...6vgLb9	120,012,700.536160	0.40954%	1	2018-08-22	2018-08-22
16	DdzFFz...ocVPSV	118,322,841.597973	0.40377%	4544	2018-04-20	2018-09-02
17	DdzFFz...PVbNmS	104,342,328.733984	0.35606%	935	2018-02-26	2018-09-01
18	DdzFFz...siDrsG	101,363,636.000000	0.34590%	1	2017-10-03	2017-10-03
19	DdzFFz...6dgyNu	99,848,805.379016	0.34073%	1	2018-08-13	2018-08-13
20	DdzFFz...AV5fjy	90,771,187.600000	0.30975%	47	2018-06-14	2018-08-30

8.2 众筹资金用途

ADA 通证的最大供应量为 450 亿，其中，57.6%（259.27 亿）已于 2015 年至 2017 年期间用于公开众筹，11.5%（51.85 亿）分发给组成 ADA 技术和业务生态系统（Technical and Business Development Pool）的三个实体：IOHK、Emurgo 以及 Cardano 基金会，剩余的 30.9%（138.87 亿，会剔除少量交易费）用于财政系统（Treasury System）。



Cardano 基金会对公募销售业务进行了三次独立审核。这些审核是运营和财务审计方法的定制混合。第一次审核含括 T1 和 T2，第二次含括 T3 / T3.5，第三次含括 T4。Cardano 基金会在英国和日本，对于承办募集资金的 Attain 公司的代表者进行了访谈。Attain 公司对于源头数据的处理，已将其独立权限限制。Cardano 基金会在适当的情况下提供了最佳建议，以改善流程和内部业务。

每次审核的范围为：

- 销售收益审查 – 销售活动收取的资金调节
- 客户销售分析 – 在销售期间检查检查可疑活动
- 经销商活动分析 – 检查经销商的任何不当行为或欺诈行为的证据
- 检查 KYC / CFT 遵守情况 – 评估是否检查 Attain 应用了商定的 KYC 程序
- 审查 Attain 公司实体 – 对良好的内部治理进行营运检查

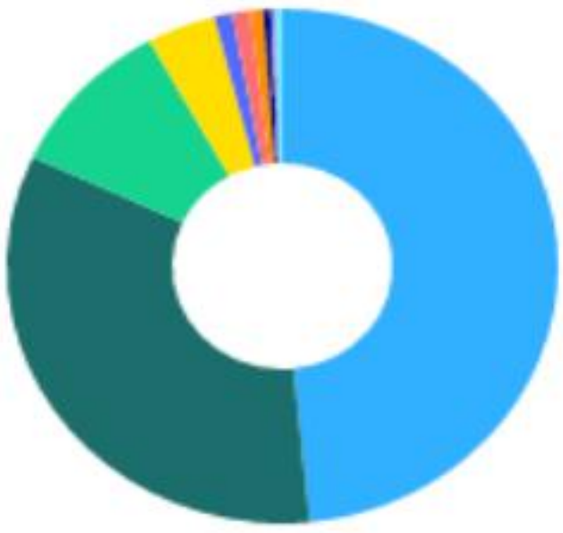
根据 Statement on IOHK’ s Ada Holdings 5 的报告，三分之一的 ADA 已经在 2017 年 9 月底 Cardano 主网开始运行之后发放给了 IOHK，另外三分之一的 ADA 会在 2018 年 6 月 1 日 发放给 IOHK ,最后三分之一的 ADA 会在 2019 年 6 月 1 日 发放给 IOHK。据 IOHK 声称，直到 2019 年，IOHK 不需要抛售任何 ADA 来弥补开发 Cardano 的开支。

8.3 币种交易所支持度

据 TokenClub 显示，Cardano 共上架了 33 家交易所，头部交易所有 Bittrex、Binance、Huobi.pro、Upbit 等，上架交易所较多，支持力度较强，币种的流通性得到保障，有利于币种的流通和币值的稳定。

交易对 成交量占比

交易对	成交量占比	
USDT	43.53%	$27342064.51
KRW	28.69%	$18024683.85
BTC	23.19%	$14565713.58
ETH	3.78%	$2376671.88
BNB	0.37%	$229701.01
IDR	0.29%	$180757.36
INR	0.10%	$61067.41
USD	0.02%	$15390.61
ZAR	0.02%	$12108.80
other	0.01%	$7730.75



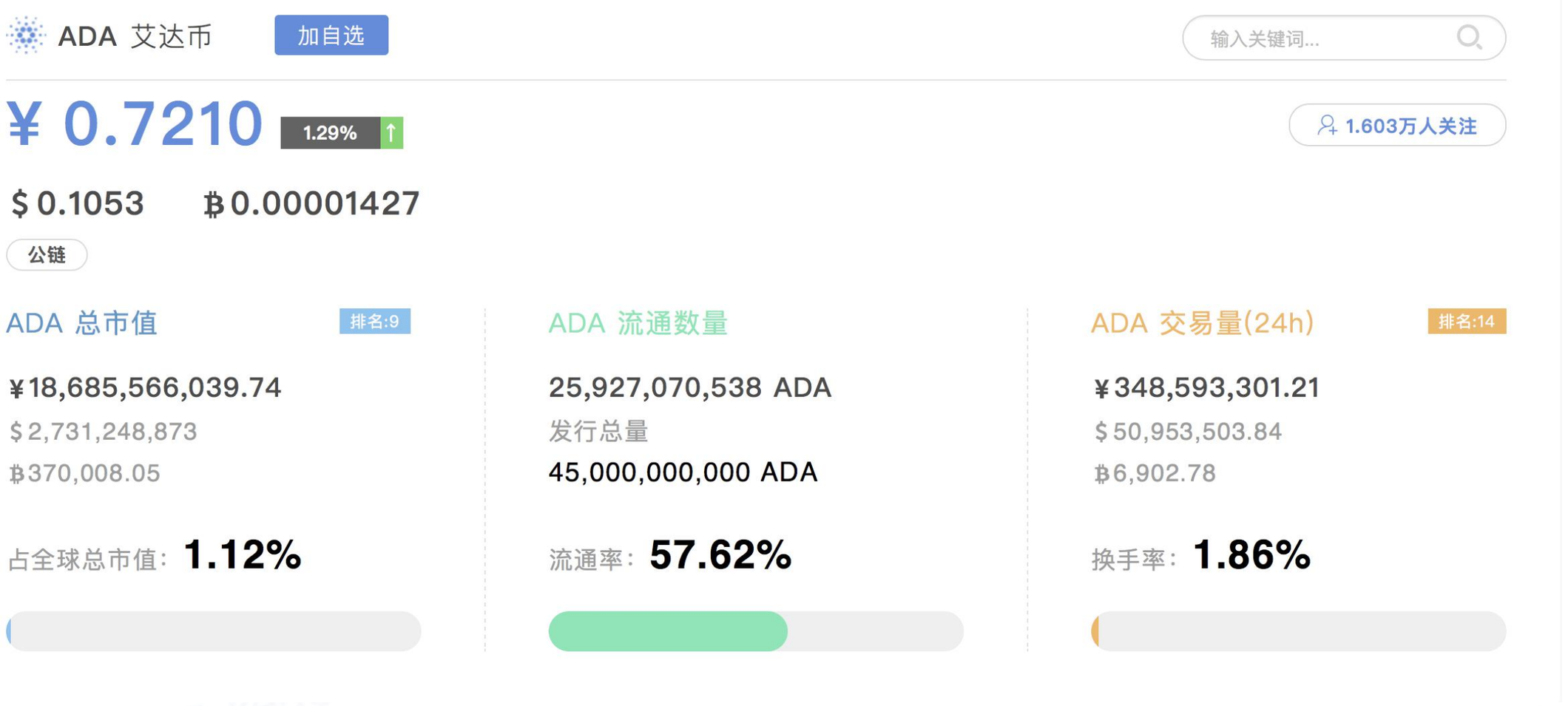
交易所 成交量占比

交易所	成交量占比	
Binance	48.43%	$30422858.67
UPbit	33.54%	$21068567.97
Huobi.pro	10.02%	$6293251.55
Bittrex	4.03%	$2532486.87
Gate.io	1.06%	$663438.03
bgj.io	1.05%	$660425.32
OKEX	0.75%	$473670.91
Bithumb	0.43%	$273016.62
Indodax	0.29%	$180757.36
other	0.39%	$247416.44

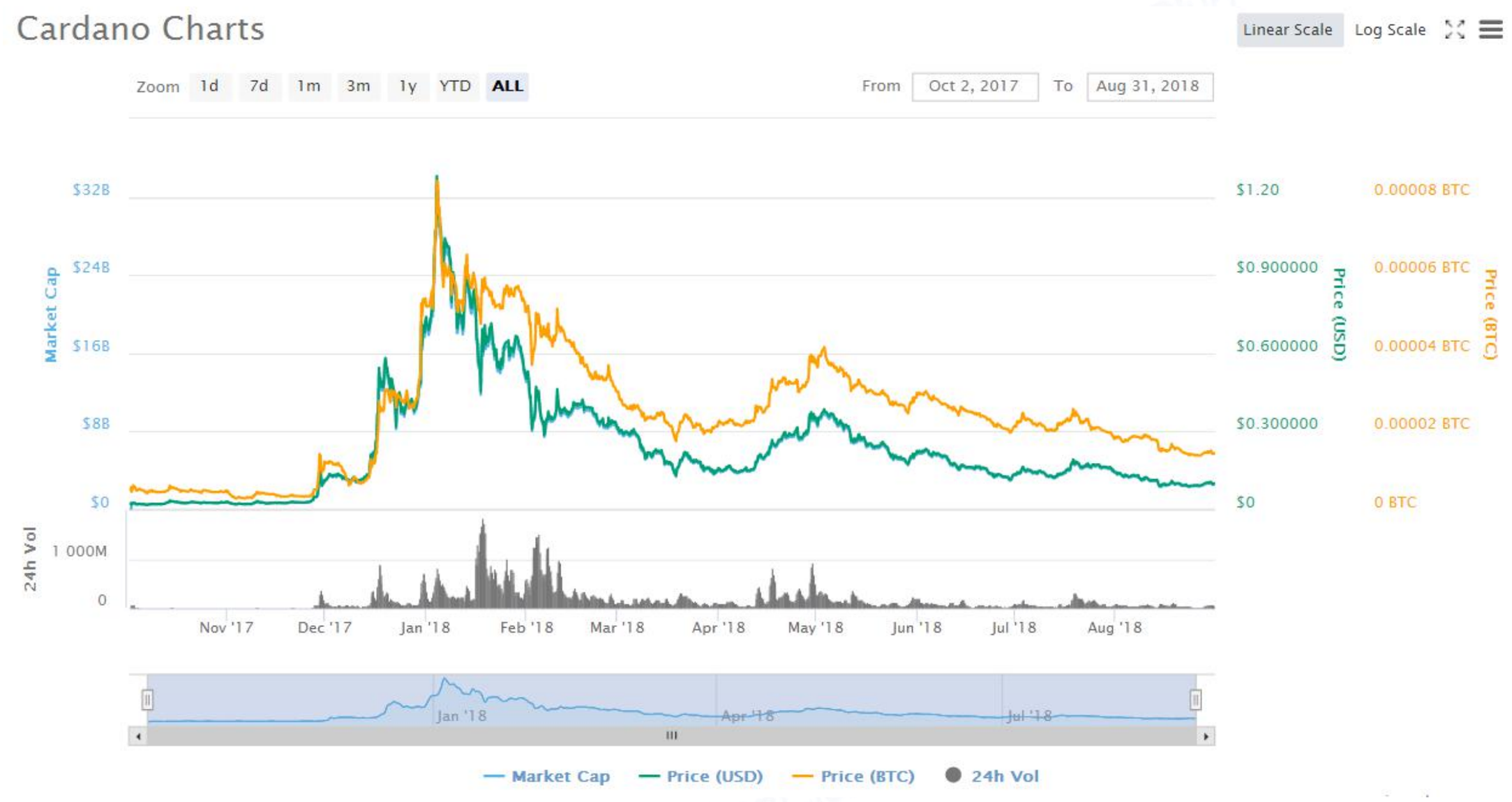
从交易对占比来看，USDT/KRW/BTC 交易对占据主要份额，显示其在日本、韩国、中国等地区接受程度较高。

8.4 币种市值及流动性分析

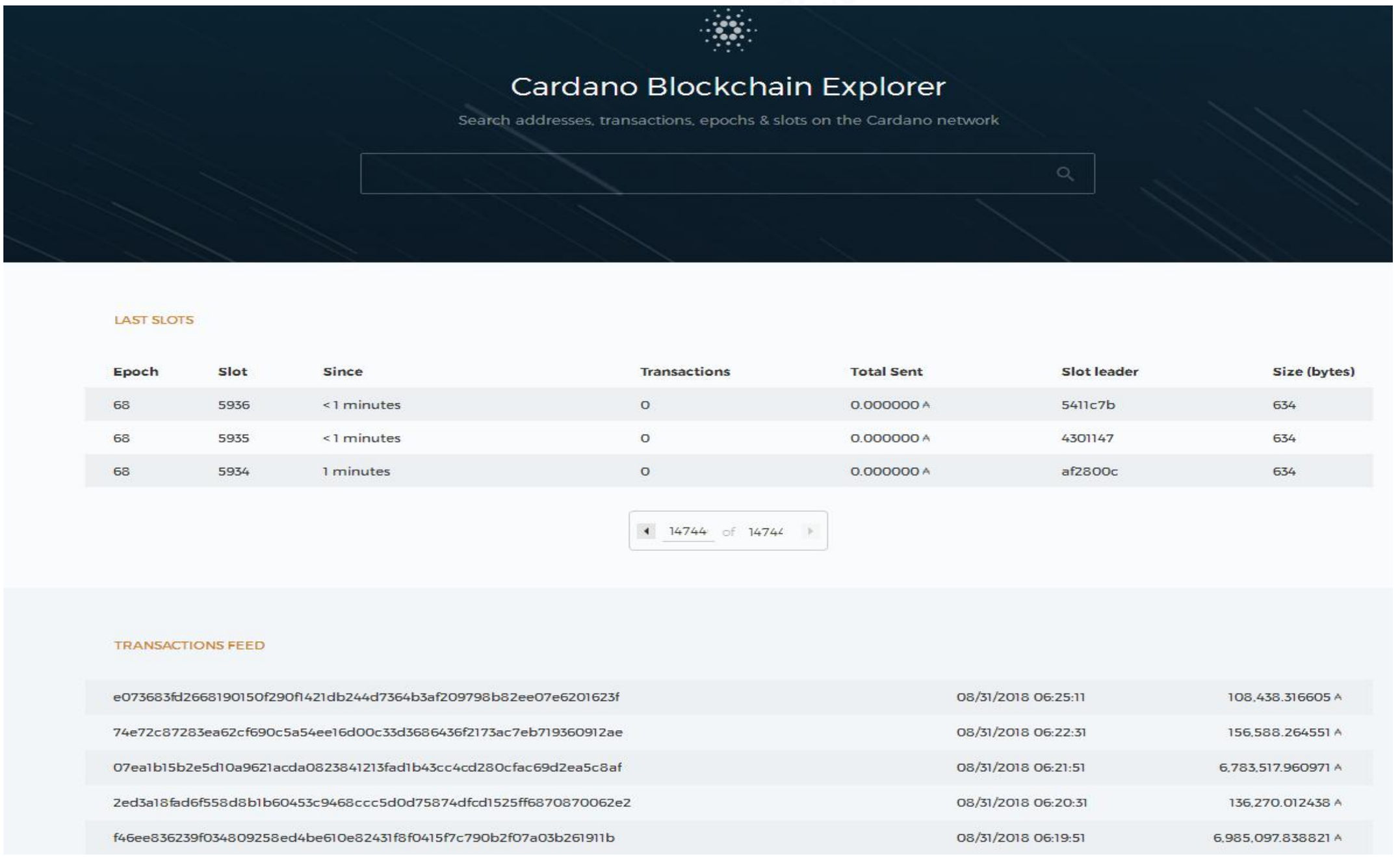
据 TokenClub 显示，Cardano 流通市值为 27.4 亿美金，排名第 9 位。Cardano 发行总量 450 亿，现阶段流通量为 25,927,070,538 亿，占总发行量的 57.62%，流通性较好；币种换手率为 2.30%，短期换手率偏低，换手率明显低于 EOS 等同类型公链项目，可见持有 Cardano 的投资者相对比较稳定。



相对于 BTC 来说，ADA 币价波动较不稳定，币价经历了 1 个大高峰期和 1 个小高峰后，开始下跌，自今年 5 月中旬以来，其价格持续下跌，与 BTC 的价格差距逐步扩大，反映出 ADA 的币价稳定性偏弱。



自 2017 年 9 月主网上线以来，截止到 2018 年 9 月 3 日，通过 ADA 网络转账的总交易量为 728389 笔，日均交易量为 1995 条以上，相对于 ETH 的 100 万笔/天，交易较少。



9.竞品分析

9.1 同类竞争者

现阶段比较热门的公链项目为 EOS、NEO、QTUM、LSK、ZIL，这些项目都是 Cardano 应该面对的很有实力的竞争对手。下面，从主网上线时间、共识算法、出块时间、TPS 和技术特点上进行简要的对比。

项目简称	主网上线时间（预计时间）	共识算法	出块时间（秒）	TPS	技术特点
ADA	2017 年 9 月	Ouroboros	20	测试 257；理论上无限制	分层架构+智能合约+侧链技术
EOS	2018 年 6 月	DPoS+BFT	1	单条测试平均 3,000；预期 1,000,000	21 个超级节点+跨链交互
NEO	2016 年 10 月	DBFT	20	实测 1,000；预期 10,000	数字证书+智能合约+跨链交互
QTUM	2017 年 9 月	PoS	120	目前 70；未来会用闪电网络（百万级）	UTXO 模型+虚拟机
LSK	2016 年 8 月	DPoS	10	目前 2.5；未来最高可达 100,000	101 个主要节点+侧链技术
ZIL	2018 年 3 季度	PoW+BFT	N/A	AWS 测试 2,088；预期达到 VISA 级	智能合约+分片

9.2 Cardano 与 EOS 的对比

Cardano 和 EOS 时常被拿来比较，两位创始人也经常隔空辩论，可以看出 Cardano 与 EOS 属于比较激烈的竞争关系。下表是一些简单类别的对比。

对比类别	Cardano	EOS
项目定位	数字现金、分布式金融应用、跨链交互	分布式商用应用、跨链交互
开发语言	Haskell 语言	C/C++/WebAssembly
主网上线时间	2017 年 9 月	2018 年 6 月
记账奖励	节点通过区块生成获得的收益只来自于交易费用（不排除通过财政系统给予区块奖励）	每年增发 5%，部分用于奖励（超级节点+提案）
资源利用机制	每笔交易消耗手续费 gas	开发者需买卖 RAM、抵押 EOS 获取 CPU/Net 资源，对用户免费
社区治理机制	同行审议+社区投票	持币人投票 + 超级节点 + 宪法
市　　值	$27.4 亿，排名第九	$58.85 亿，排名第五

9.2.1 共识机制对比

Cardano 和 EOS 都使用了 DPoS 作为其共识算法，但是 D 的含义却是不同。在 EOS 中，D 指的是 Delegated，也就是委托；而 Cardano 中的 D 指的是 Dynamic，意思是动态。EOS 通过投票委托见证人代表自己生产区块，而 Cardano 是通过动态随机的选取权益候选人作为区块的生产者。

9.2.2 激励机制对比

	ADA	EOS	ETH
用户激励	每笔交易都需要消耗 ADA，且受到 ADA 价格影响；通证持有者可将自己的权益委托给其他节点	平台用户按持币比例获得带宽资源，不受 EOS 价格影响；可租赁或转租闲置的带宽资源；DApp 使用者无直接的使用费用	每笔交易都需要消耗 Gas，且受到 Gas 价格影响；改为 PoS 后，通证持有者可将权益委托给节点
区块生产者激励	交易费用用于节点奖励，总量限定在 450 亿个	每年增发不高于 5%，部分用于提案奖励，部分用于奖励超级节点（官方透露暂定 1%）	改为 PoS 后，节点可获得部分收益，总量限定在 1 亿（目前供应量已达 0.988 亿个）
社区治理机制	设计国库系统，由部分新生成的 ADA（约 138.87 亿）以及转账费用捐赠，通证持有者可通过投票决定如何使用	账号冻结、改变代码、宪法修改等	无

9.3 Cardano 自身存在的风险

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，国际化的团队做事稳健，实力强劲，透明度高。同时也存在一些缺陷，主要表现在：

9.3.1 共识机制有待检验

共识算法是一个基础公链的价值观 ,Cardano 的 Ouroboros 算法是自己独创的，目前并没有开发完成，整体的理念也还存在一些争论，这从 BM 与霍斯金森关于算法的分歧也可以看出一些端倪。EOS 的 DPOS 算法，已经在两个项目中有过应用，但近期的投票机制依然引起了轩然大波和整个生态的争论。可见，一个共识算法的成熟和完善，重要而且漫长。所以，Cardano 的共识算法是否能成功，仍需要时间和实践的检验。

9.3.2 目标宏大，复杂，难度大且周期长

Cardano 目标宏大，可以简单理解为改进版比特币+下一代以太坊。从软件工程的角度看，项目是非常复杂的，需要很扎实的开发推进和很长的开发周期。在一日千里高速变化的区块链领域，这种高难度长周期的项目定位本身也是一种风险，需要各方面的有力支撑才能顺利完成。

9.3.3 偏重技术，对营销重视不够

区块链不单单是技术，他是涉及到社会学的问题，也就是说到人们要达成一种共识，所以营销的好坏对一个区块链项目是很重要的。Cardano 营销上总体偏弱，市场热度与其市值不匹配。

9.3.4 竞争对手多且强

Cardano 目前所处是区块链生态的痛点逐步被市场认知的时间节点。市场渴望能够出现一个代表性的、解决现有区块链生态痛点的底层公链。此时，以太坊对于自身的迭代也在不断进行，更有许多有望成为区块链 3.0 代表的底层公链不断涌现，EOS 就是其中一个非常强劲的对手，在团队能力、项目定位、甚至共识算法方面，Cardano 与 EOS 都属于同一量级的，可能会成为较长一个阶段的直接竞争者。在市场热度层面，目前 EOS 已经处于领先位置。EOS 在 2018 年 4 月 6 日新发布了 EOSIO DAWN 3.0 版本，主网也已经在 6 月上线。这些无形中都是对 ADA 的巨大挑战。

9.3.5 市值较高

截至今天 Cardano 市值为 27.4 亿美元，已经是世界数字货币市值排行榜的第 9 名。这也要从两方面看；一是 Cardano 多数投资者在日本，还潜力待开发，市值还有很大增长空间。从另一方面看，Cardano 在如此不成熟的情况下市值已经 27.4 亿美元是否有高估的风险。

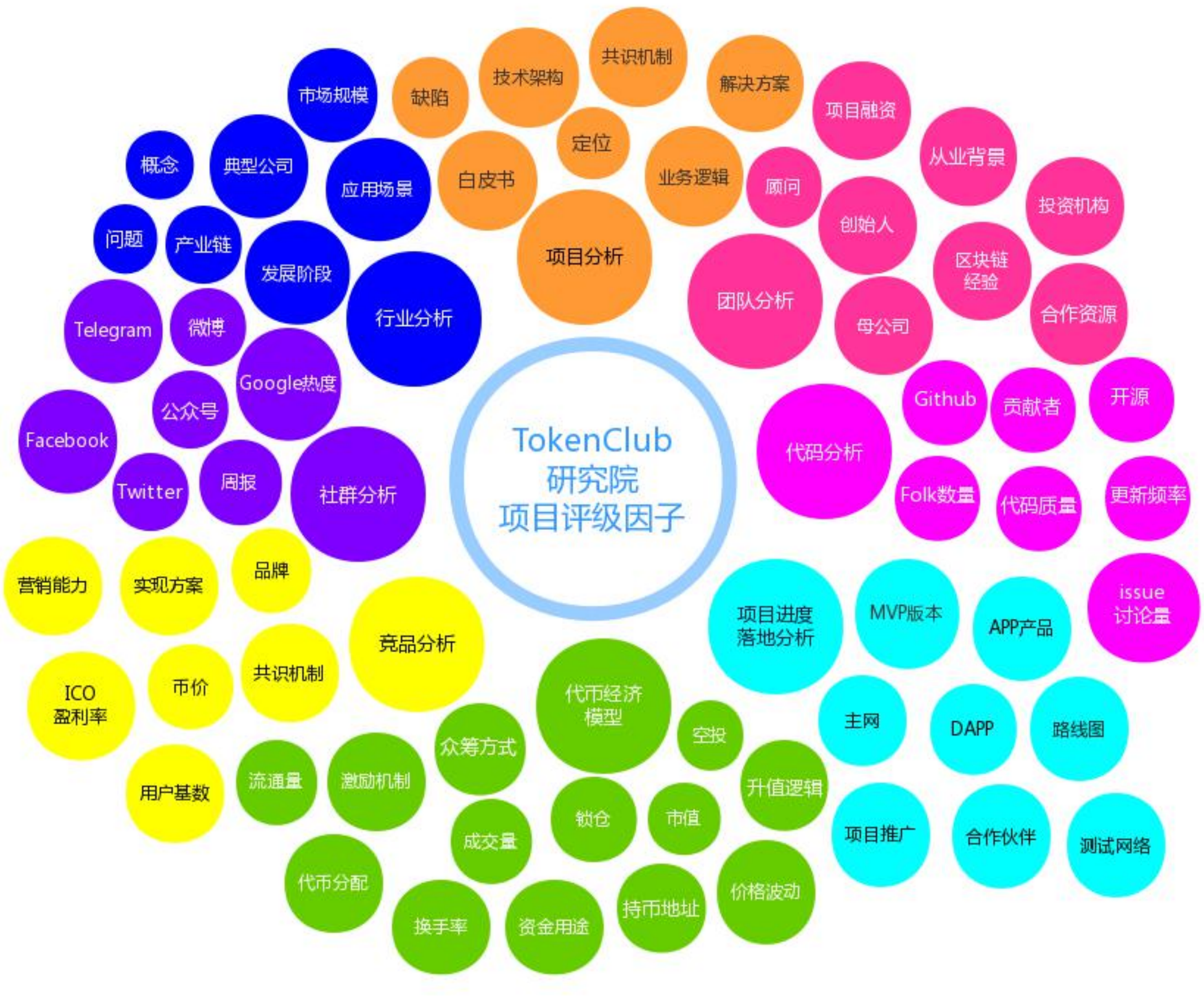
9.3.6 中心化倾向能否成为主流共识？

对 EOS 的 21 个超级节点是否是中心化的争议仿佛一直没有停止过，在 Cardano 的设计中包含了接受监管，合规审查等思想，貌似是与区块链的去中心化思路相背离的，整个市场对于这种思路的接纳程度还需要进一步检验。

Cardano 众筹阶段的 85%以上的代币持有者来自于日本，以后的挖矿收益大部分流向日本，所以就造成 POS 收益基本与其他国家的参与者无关，有一定的中心化风险。

评级说明

TokenClub 研究院立足于多年的区块链行业分析经验，同时参考市面上的一些评价标准，综合制定一套自己的区块链项目评级标准，从多个维度（所处行业、项目自身、团队、社群发展、代码、项目进度、代币经济模型、竞品），采用定量分析和定性分析结合方式，来综合评判一个项目。



TokenClub 研究院项目评级采用“项目评级 + 风险度 + 发展阶段”评级体系。

项目评级

项目评级主要从项目本身的资质、价值，项目的发展潜力，项目代币的稳定性等方面来综合评判项目。项目评级整体来说分为 12 档：AAAAA、AAAA、AAA、AA、A、BBB、BB、B、CCC、CC、C、D，各档代表含义如下表所示：

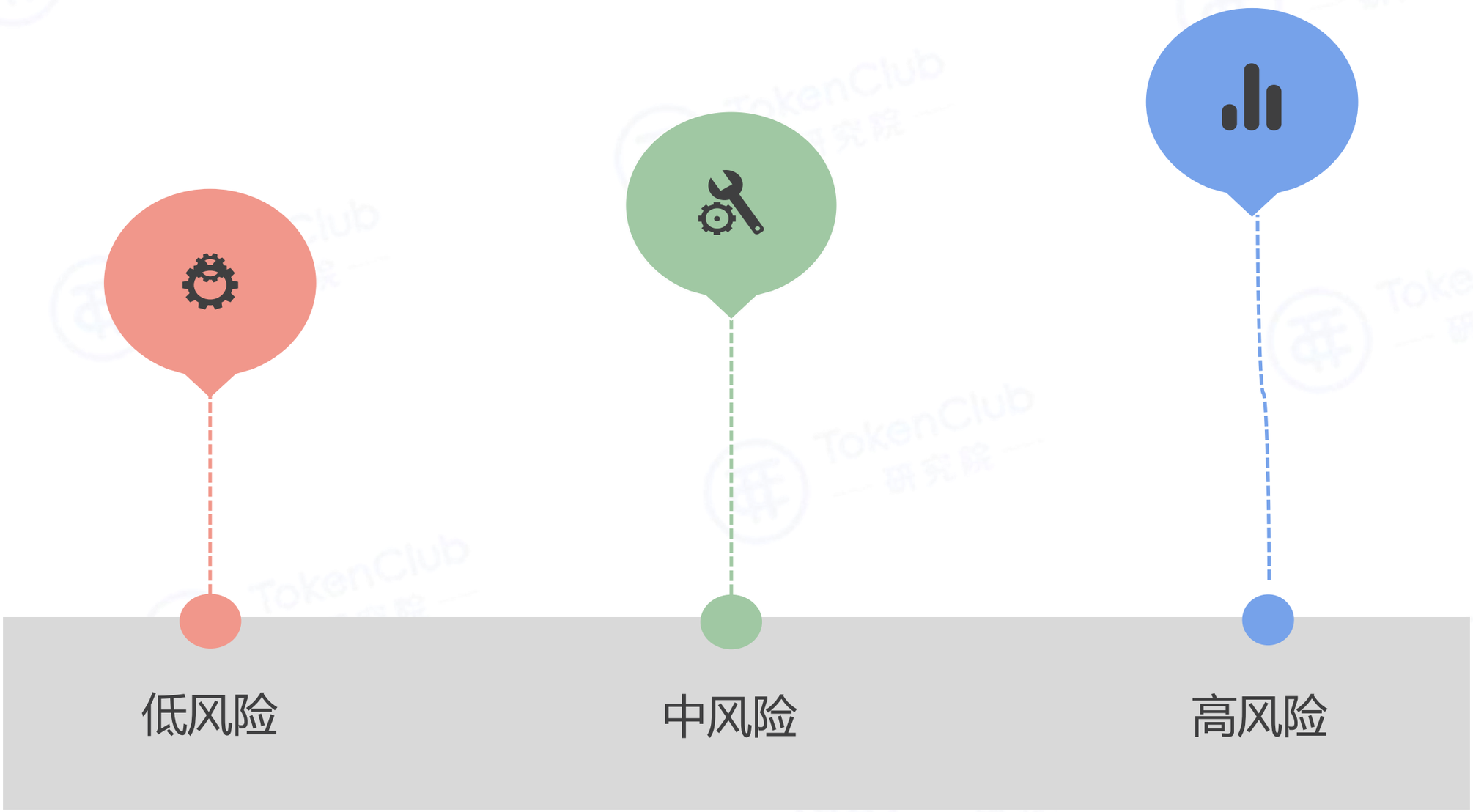
评级	含义
AAAAA	项目在行业内处于统治地位，基本无风险型项目（整个数字货币行业良性发展的前提下）
AAAA	项目处于成熟期，市场地位稳固，币价极其稳定，风险极低
AAA	项目经过市场检验，无论市场环境如何，代币有很高的稳定性，风险低
AA	项目基本获得市场检验，发展较好，代币稳定性良好，在牛市或熊市会有不错表现，风险较低
A	项目获得市场一定程度认可，发展到一定阶段，代币稳定性较好，风险一般
BBB	项目有潜力和发展前景，但易受外部因素影响，代币稳定性、风险一般
BB	项目有不错潜力，但未来发展不确定性，代币稳定性差，有一定风险
B	项目资质一般，代币稳定性较差，风险较大
CCC	项目资质较差，代币极其不稳定，风险很大
CC	项目价值偏低或信息透明度较差，风险很大
C	项目价值很低或是实现难度很大，风险极高
D	项目无价值，或项目已失败、跑路或欺诈

风险度评级

区块链项目除了受项目自身因素影响外，也会容易受到外部环境，如政府监管、行业发展、技术安全性等多种因素的影响。即使对于优质的项目，其代币 Token 价格可能被高估，也可能被低估，也就意味着短期市场的币价高低并不能很准确的反应出项目的实际情况。

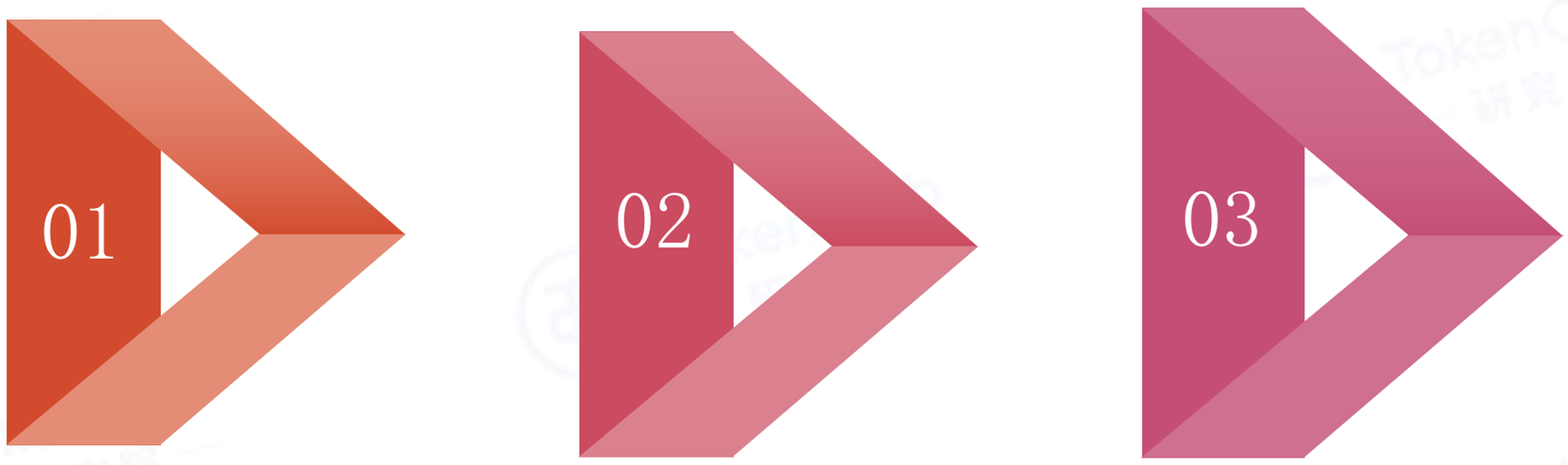
因此，我们引入风险度这一指标，根据项目各个维度的评价，结合项目目前所处的阶段，对项目的风险度进行评级，分为三档：低、中、高。

- 低：项目经过市场检验，发展良好，稳定性强，风险低
- 中：项目已上线运行，各方面情况良好，风险度一般
- 高：项目处于初始阶段，各方面发展尚不稳定，存在极大不确定性，风险偏高



发展阶段评级

同时考虑到不同的区块链项目，会处于不同的发展时期，有的项目刚 ICO 完毕上线交易所，有的项目主网已经上线，有的项目已成熟运营好几年，不能仅仅采用统一的标准来评判。因此按照时间维度，我们对项目的发展时期分为三个阶段：萌芽、成长、成熟。



萌芽期

项目刚起步或刚 ICO 完上线交易所(3 个月内)、处于早期阶段

成长期

已上线交易所，项目处于发展时期，尚未成熟

成熟期

上市已久 ,项目已稳步发展、功能完善时期

评级更新

对于区块链项目而言 ,在项目的各个发展阶段表现各异 ,如项目主网上线 ,或 APP 产品上线，团队人员发生变动，项目代币锁仓，项目出现重大变故，项目受到外部环境的影响或限制，以及其他能够影响项目发展的因素或突发事件，都会造成项目的发展受限和项目代币价格的巨大波动。

因此，我们的项目评级标准并不是一成不变的，而是会根据项目的发展阶段和市场上的表现，在一定时期过后，会动态的调整具体项目的评级，提升项目评级或调低项目评级，从而力求动态反应项目的真实情况和实际价值体现。

风险提示

本报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解，本报告清晰准确地反映了作者的研究观点，力求独立、 客观和公正，结论不受任何第三方的授意或影响，特此声明。

本报告的信息来源于已公开的资料，TokenClub 研究院对该等信息的准确性、完整性或可靠性不作任何保证。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。

TokenClub
研究院

TokenClub 是国内领先的数字货币投资社区，致力于构建一个自治、信任、高效的数字资产投资服务生态。

“TokenClub 研究院”是 TokenClub 旗下研究区块链的专业机构，专注于区块链行业研究、项目评级。

扫码关注
TokenClub 研究院

扫码下载
TokenClub APP