Ολυμπιακοί Αγώνες

OA

OLYMPIC GAMES FOR ALL RESHUFFLE

全民奥运·重新洗牌

《OA白皮书》

ΟΛΥΜΠΙΑΚΟΙ ΑΓΩΝΕΣ

奥运精神·奥运之光

OLYMPIC SPIRIT·OLYMPIC LIGHT

目　录

简　介

2020 年伊始，新冠疫情席卷全球，给全球经济带来重创，也改变了各国民众的生活方式。诺贝尔和平奖得主曼德拉曾说，体育具有改变世界的力量。而当世界因疫情而重塑时，体育和奥林匹克精神也显示其重要作用。奥林匹克主义希望通过体育创造一个更美好的世界，倡导相互了解、友谊、团结和公平竞争的奥林匹克精神。世界人民在抗击疫情中所表现出的勇于拼搏、坚持不懈和团结互助，也正是奥林匹克精神的生动写照。

在这样的背景下，由本项目团队和国际奥林匹克委员会共同研发的 OA（希腊语Ολυμπιακοί Αγώνες，奥运会）项目诞生了。该项目是一个基于区块链技术的，以弘扬奥运体育精神，提升运动质量，传播体育文化，发展慈善事业，创造共享经济价值为支撑的区块链项目。OA 充分应用了区块链去中心化、可信赖、智能合约等特点，力图打造一个以奥运精神为驱动的全球化运动生活平台。在 OA 平台上，产业链上的各个主体和个体都可进行在 OA 上进行信息传输、精准数据、资产交易和资金分配等活动，这些行为都受到区块链技术的保护和鼓励。

核心价值：去中心化、公开、透明、公平、共享

发展愿景：将区块链技术运用到全民体育运动健身领域，构建全球全民运动生活平台。

OA 将恒量发行 2 亿枚数字货币。OA 币可以被用作体育运动领域的价值流通和交易媒介，不仅可以作为记账奖励，也可以作为一般等价物的数字货币流通使用。通过 OA 币，可以为体育运动和奥运精神传播行业的发展提供良好的数字服务支持。

1、项目背景

1.1 行业背景

2020 年伊始，新冠疫情席卷全球，给全球经济带来重创，也改变了各国民众的生活方式。诺贝尔和平奖得主曼德拉曾说，体育具有改变世界的力量。而当世界因疫情而重塑时，体育和奥林匹克精神也显示其重要作用。奥林匹克主义希望通过体育创造一个更美好的世界，倡导相互了解、友谊、团结和公平竞争的奥林匹克精神。世界人民在抗击疫情中所表现出的勇于拼搏、坚持不懈和团结互助，也正是奥林匹克精神的生动写照。

社交隔离、旅行限制给人们的生活带来不少变化，但更多的人也在此期间意识到体育的重要：体育不仅带给人们健康的体魄，更可以增强不断战胜挑战的信心和决心。正如《奥林匹克宪章》开篇所说，体育是一种生活的哲学。在这个特殊时期，人们更有理由学习和掌握体育的生活哲学。

新冠疫情把更多的家庭带入低收入群体，从而加剧了个体运动量的差距。2019 年，在年收入低于 25000 美元的美国受访者中，有 46％表示自己缺乏运动；收入超过 10 万美元的受访者中，不运动的人只占 19％。体育行业应紧密合作，面向不同群体提出有针对性的运动解决方案。

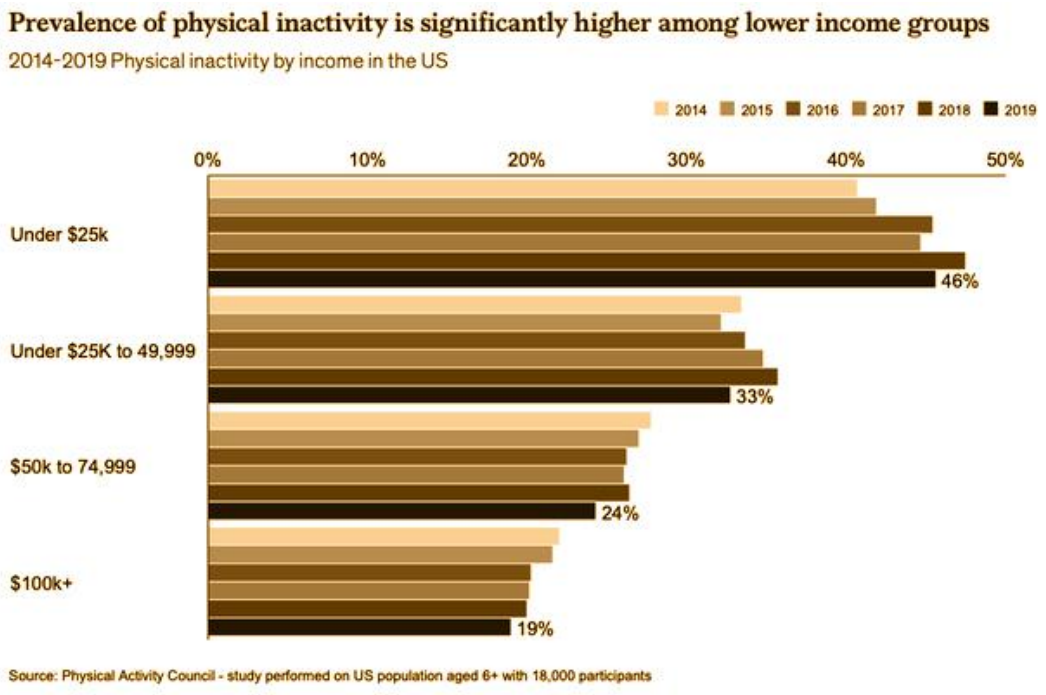


图 1-1：运动量与收入水平正相关

在过去的一年中，由于保持社交距离和居家隔离的规定，数字体育运动及线上运动社区得以快速发展。数字体育运动将继续成为 2021 年及来年的热门趋势，和传统体育运动互为补充，激励与锁定用户群。

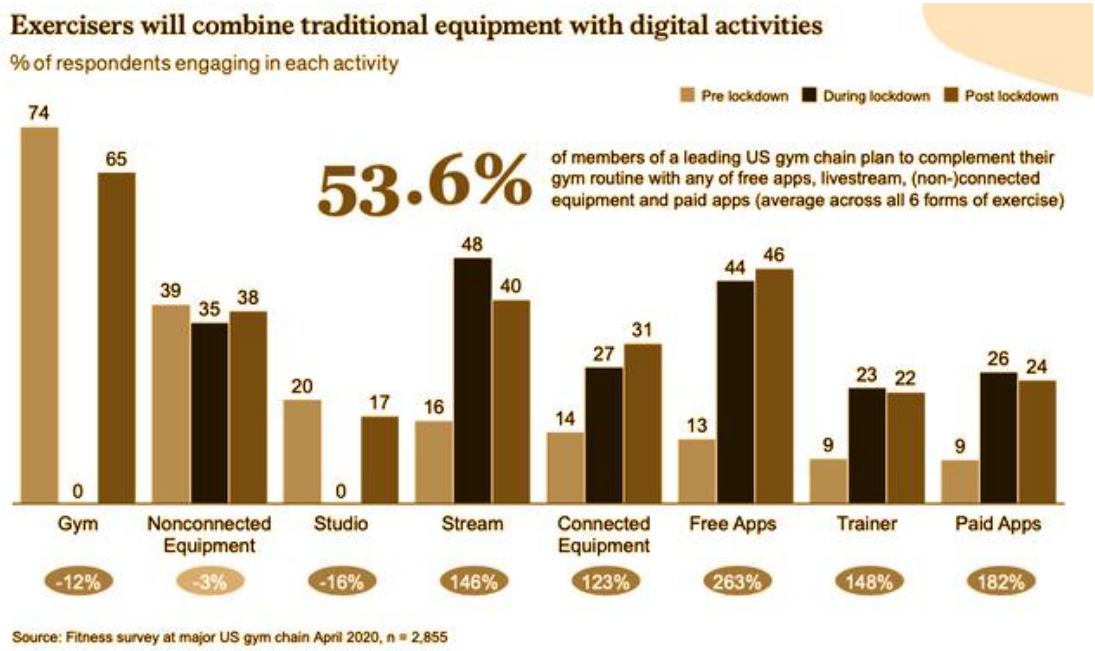


图 1-2：数字化运动比例

1.2 面临的问题

后疫情时代，体育的经济功能将得到进一步凸显，体育不应成为这场危机的组成部分，而应成为解决这场危机的有力手段。体育将成为使不同社会、政治、宗教或文化背景的参与者整合在一起的工具，奥林匹克精神中团结、和平、尊重的重要原则也将在全球得到进一步推广。但是在当前的技术条件下，奥林匹克精神的传播和推广还存在着一些问题

1、信任体系不健全：在文化传播过程中，因为中心化体系的原因和监督机制的缺乏，都存在信任体系不健全的问题。这样会导致很多问题的发生，比如信息传播失真、公益捐赠下降、用户流失等。

3、缺乏激励机制：在奥林匹克文化传播领域中，用户共享资源或贡献资源的目的虽然主要不是为了收益，但如果长期没有激励，这种行为也是难以持续的，市场始终难以扩大。

3、缺乏标准化和规模化：奥林匹克的精神的内核在于自强不息，通过这种精神可以让人们多多参与体育运动，强健身体。但是奥林匹克文化的传播没有办法实现标准化和规模化。大多数机构和组织都是单打独斗，很少能够协同创新发展，导致竞争格局非常分散，内耗严重。

1.3 解决思路

1.3.1 解决思路

上述的问题看起来虽然纷繁复杂，但我们抽丝剥茧，透过现象看本质就会发现，这些问题的最终根源在于两点：

1、中心化组织带来的行业不透明。在中心化的组织架构下，不同主体之间的交易内容缺乏外部监督，相互之间知情权缺乏，必然会导致价格虚高，以次充好等现象。

2、不同环节中不同的交易主体之间的互信机制缺失。交易主体之间缺乏信任，从而带来交易成本增加和交易效率的下降，交易主体为了抵消这种负面影响，会通过各种方式提高自身的收益，降低自身的风险，从而出现种种问题，更重要的是，环节的增加会把这种互信缺失带来的影响进一步放大。

想要解决这些问题，就必须打破中心化的组织，让交易主体直接对接，提高效率，并提高行业的透明度。但是这样一来又会带来更为严重的问题——在没有中心组织的制约下，人类的现有技术条件难以维持交易互信。交易互信的问题从人类诞生以来就伴随着社会的发展而一直存在，人类为了实现交易互信建立了大量法律和技术方面的约束条件，却一直无法杜绝交易欺诈的现象。而去中心化或弱中心化会让交易更加混乱——这就把通过传统的技术力量或模式改造解决问题的道路堵死了。所以需要我们引入新的技术概念。

1.3.2 解决方案

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。从客观上来看，区块链技术的特点对于解决交易互信问题有决定性的作用，可以从根本上解决目前健康和文化市场中存在的种种问题，具体表现在：

1、去中心：基于去中心化的特点，点对点的交易得以实现，每一个交易主体，从用户到互联网服务器，都是区块链的一个节点，节点和节点之间可以直

接交易，避免过多的环节。而且每个节点的历史记录、流转情况等信息是不可更改的，大大提高交易双方的可信度。

2、安全性：在产业链中，数据多由核心企业或参与企业分散孤立地记录保存在中心化的账本中。当账本上的信息不利于其自身时，存在账本信息被篡改或者被私自删除的风险。区块链技术的链上数据不可篡改和加盖时间戳的特性，能够保证所有数据都不被篡改。数据不可篡改使信息的不对称性大大降低，征信以及企业间的沟通成本均随之降低，这一应用帮助企业间快速建立信任，同时分化了核心企业所承担的风险。

3、信息透明：基于区块链数据信息透明，不可更改的特点。每一个节点都可以看到数据应用的溯源情况。如此企业将不可能再进行数据造假，用户的安全隐私也可以得到充分保障，其体验性大幅度提高。

4、智能合约：在区块链定义的规则下，整个产业链的各个交易主体可以通过区块链技术自动执行智能合约，而不再需要人为的甄别真伪，这使得他们可以大幅度降低管理和时间成本。而且节点间自动交易的能力会催生全新的商业模式，网络中每一个节点都可以充当独立的商业主体，以很低的交易成本，与其它节点分享自己的数据和资源，这为新的商业模式建立带来很大的想象空间。

从上述内容可以看到，去中心、安全性、信息透明、智能合约等特点，在根本上解决了不同环节交易主体之间的互信问题，这种解决方案是从底层技术来完成的，对于解决当前奥运精神传播和运动生活领域中的问题有决定性的意义。

2、项目阐述

2.1 项目模式

在这样的背景下，由本项目团队和国际奥林匹克委员会共同研发的 OA（希腊语Ολυμπιακοί Αγώνες，奥运会）项目诞生了。该项目是一个基于区块链技术的，以弘扬奥运体育精神，提升运动质量，传播体育文化，发展慈善事业，创造共享经济价值为支撑的区块链项目。

发展愿景：将区块链技术运用到全民体育运动健身领域，构建全球全民运动生活平台。

在 OA 上，各个主体都可以对等地进行信息传递、资产交易、转账和数字资产分配等活动，这些行为都受到基于区块链技术的保护和鼓励。会激励全球奥运精神的传播。此外，通过数字货币的应用，可以显著提高运动效率，完善以奥运为核心的慈善服务，市场会更加繁荣。在这个基础上，会诞生在线商城、社群服务、体育竞猜等一系列衍生的服务。

图 2-1：OA 的模式

2.2 应用场景

在 OA 平台上有着各种应用场景，包括但不限于：

2.2.1 奥运精神传播

在传统的模式下，奥运精神的传播要经过多层环节，过程中很可能出现信息失真的问题，最终影响奥运精神传播的效果。而在 OA 上，通过区块链技术的去中心化和高度安全性特点，奥运精神可以以文化、慈善、创意等多种形式无障碍传播。各类企业、组织机构和个人都可以成为传播的节点，所有的数据也都会上链保证信息不失真，同样，在传播过程中做出贡献的人将得到数字资产的奖励。通过这种方式，奥运精神的传播效率将得到大大的提升，让更多的人接触到奥运的精神内核，让世界上的贫穷落后国家建立自己的奥运精神以及奥运援助，积极地将运动和生活融为一体，让世界免受战乱之苦，疫情之害。特别地，奥运委员会将会周期性通过 OA 币向落后国家进行援助和慈善活动。

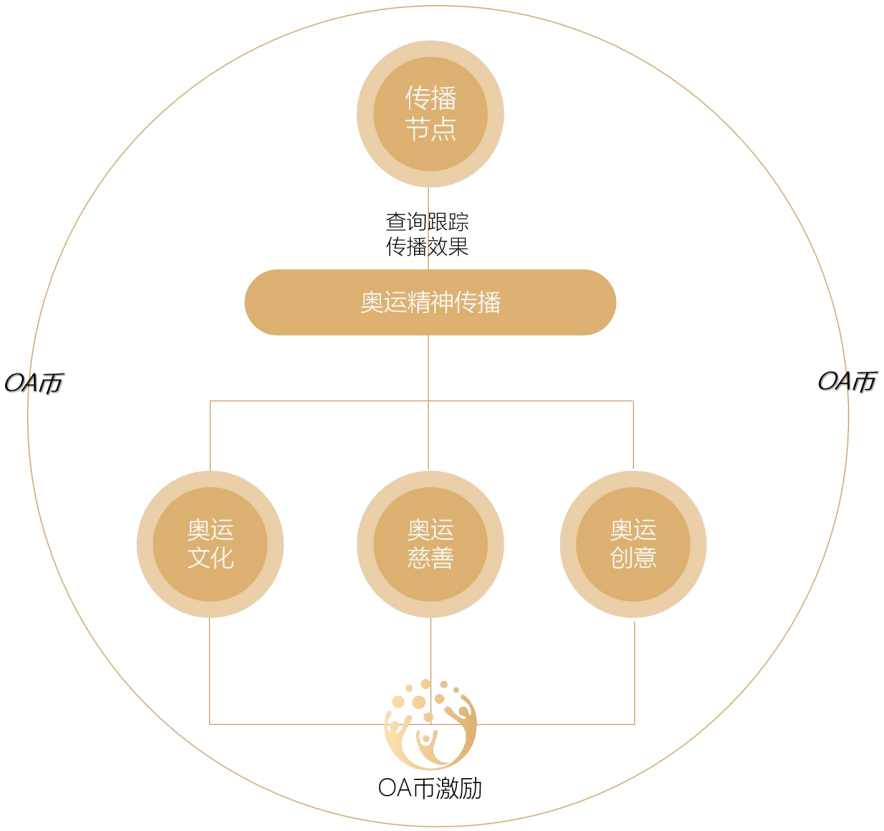


图 2-2：奥运精神传播

2.2.2 在线商城

用户得到 OA 币后，可以在 OA 的在线商城中进行一些交易和互换，比如说购买运动健身器材、运动场地的消费时间、运动服装等。传统的技术条件下，商品交易必须要经过多个环节，每个环节都要增加成本，而且信息极不透明。而 OA 在线商城可以为交易各方提供低成本，透明化，便捷的交易方案，通过去中心化和智能合约的特点，让点对点的交易成为可能，生产厂商可以和终端消费者直接交易，可以显著提高交易效率，降低交易成本，并及时获取市场反馈信息。而且通过智能合约，所有的费用按照约定的内容自动执行，无需双方投入太多精力和时间，大大提高了双方交易的效率。

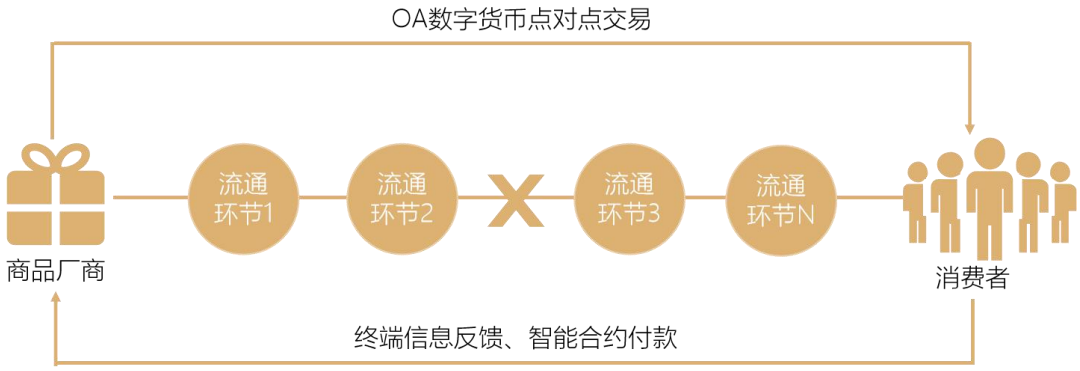


图 2-3：OA 在线商城

2.2.3 社群服务

OA 将建设用户社群，让大量的运动爱好者、俱乐部机构和运动场地运营方可以自由讨论奥运领域的各类问题，互通奥运精神、运动知识等。而且考虑到运动健身是一项专业性比较强，能够建立长期社交关系的领域，OA 还将开放内容发布模块，用户可以在平台上发布原创内容，帮助其他用户学习相关知识，觉得知识有价值的用户可以对这些内容进行打赏订阅，激励发布者的行为。所有的报酬均以 OA 数字货币支付。

图 2-4：OA 社群服务

2.2.4 体育竞猜

体育竞猜是体育运动行业中一个非常重要的领域，依托于区块链的各种技术特性，OA 平台实现了公开公平公正的透明化竞猜机制，所有的体育竞猜项目都在智能合约的作用下面向全球用户开放，并使用非交互式随机数算法保证了开奖的绝对公平。更重要的是，通过 OA 平台，以区块链为媒介，可以让全球的用户都可以方便快速地进行竞猜服务的购买和奖金结算。传统技术条件的外汇兑换的低效率以及地下钱庄的高汇率情况将不复存在。用户使用 OA 币，可以像使用本国货币一样购买任意国家的体育竞猜服务（只要它登录了 OA 平台），奖金也可以瞬时到账。

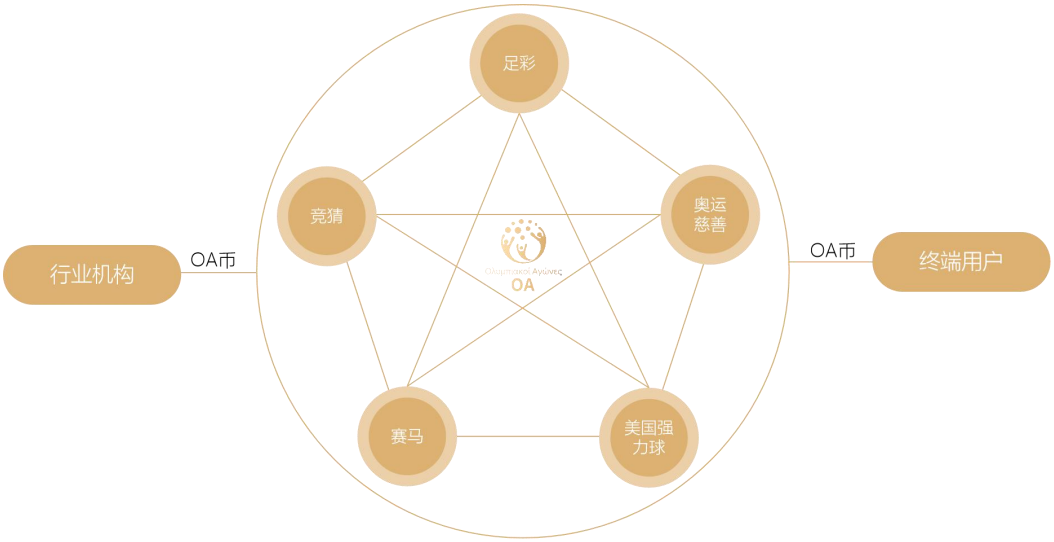


图 2-5：体育竞猜

综上所述可以看出，只要有奥林匹克精神的存在，就有 OA 存在的价值和意义。更重要的是，本项目依托于奥林匹克委员会作为背书，所以在全球奥运体育运动行业中，我们可以想象到的应用场景非常多，这将为 OA 的落地和应用提供足够的价值支撑。

3、技术实现

3.1OA 技术原理

OA 是一个在现有区块链技术基础上进行改良的创新性区块链技术平台，不仅支持 DAPP 一站式开发，而且支持不同链无缝融合交互，具有功能完整、体系丰富、可塑性强等特点。

OA 的设计目标是一条面向全球的公链，支持 P2P 网络传输协议，PAOS 共识算法、智能合约和虚拟机技术，并使用多重签名对同一个文件使用多个私钥进行签名，提高该文件访问的安全级别，交易匿名保护则使用环形签名技术，多链融合则能够使 OA 和其他链的交互快速简单。服务层对区块链存储的数据进行简单加工处理，对 DAPP 提供各种应用所需要的服务调用接口。

3.2 解决方案

3.2.1P2P 通信技术

OA 网络由 OA 协议实现的 P2P 点对点网络，OA 协议是一套在互联网上进行交易的协议。 该协议的使得人们可以在分布式网络中转移价值，就像可以发送钱的邮件。实际上 OA 网络协议的目的就是能够快速实现交易信息在全网

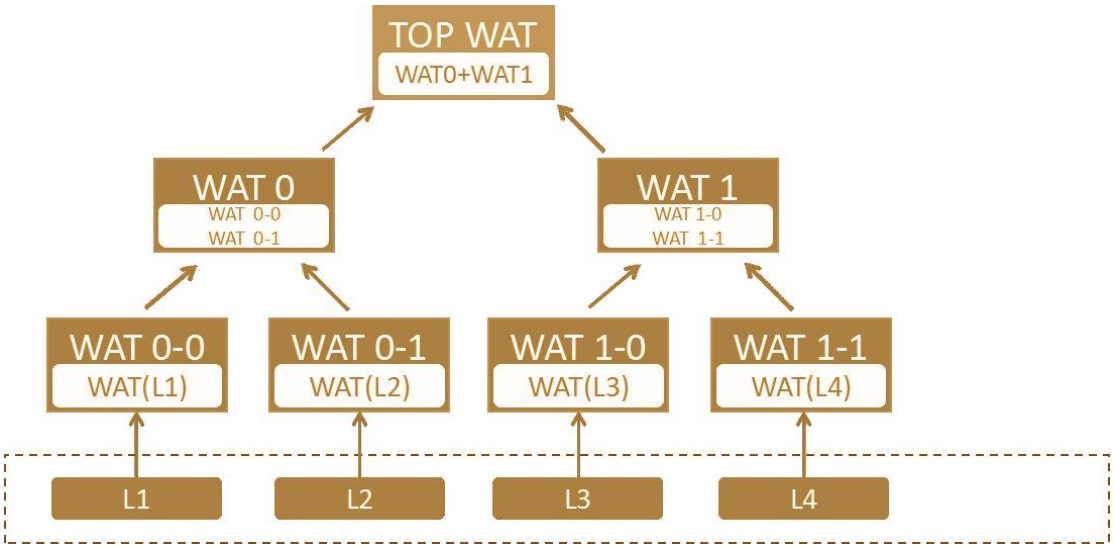
节点之间的一致性，这为共识过程提供基础。

3.2.2 双重侧链

在我们的设想中，OA 将建立一个新的底层技术平台用以链接各种不同 的区块链技术，从而让基于信任的价值在不同的区块链系统中自由流通。

OA 是 Block Chain 和 DAG 系统的双重侧链。实现基于区块链和基于非区块的分布式系统信息与价值的互联互通。其中 OA 是跨平台价值互通的媒介，而 OA 平台本身是跨平台信息交换的载体。基于 OA 系统的设计特 点，OA 在系统初始设计阶段已经考虑到了对基于区块链的系统（包含基于 UTXO 和 Account Based）和 DAG 为基础的分布式账簿信息的读取。未来可以基于 OA 实现区块链与 DAG 系统之间直接发送或接受明（White）暗（Black）代币。同时，也能够在 OA 客户端之间实现基于零 知识证明的完全加密通信，以及其他一系列激动人心的特性。

传统的区块链比如比特币、以太坊还是采用基于诸如默克尔树这样的二叉树数据结构：



OA 的技术团队由深耕大数据、云计算以及密码学和区块链领域多年的技术专家组成，OA 将规划建立两个完全不同底层数据结构系统之间的通道，从而在底层技术层面兼容主流的区块链技术标准。

3.2.3 共识算法

1、共识基础

在 OA 链中，节点分为 2 种类型：轻节点、全节点。轻节点不参与共识，且只保存哈希树与自己相关的交易数据；全节点参与共识且存储所有发生的 交易数据。

在 OA 链中，存在 3 种交易类型：普通交易、合约交易、加密交易，普 通交易直接入库；合约交易由智能合约和虚拟机触发执行，具有安全性高、 自治等特点；加密交易则使用环形签名等技术，加密交易的数据通过共识达 成一致性后，使用智能合约执行入库操作，同时为了避免双花问题，我们将 会有更多地处理方式。

2、特点

- 数据吞吐量大：经过实践认证，OA 的吞吐量达到 1000 条每秒。
- 交易速率快：新区块生成时间 2-10 秒，相比比特币的 10 分钟和以太坊

的 1 分钟而言，大大促进了商业化项目落地。

- 容错率高：和比特币一样支持 50%的容错，对于攻击者来说，攻击者需要花费 50%的费用才能使得该条交易数据的账本进行改变。

- 交易费低：每次交易只收取极少的交易费，这使得电子支付在跨境转账、频度较高的小额支付等领域大放异彩。

- 安全性高：由于综合技术的运用，安全性得到了大大的加固。如智能合约、虚拟机、环形签名、加密算法等等。

3、共识过程

OA 网络每隔 2-8 秒产生一个新的区块，新区块使用名为 PAOS 的共识 机制进行交易共识，新区块的被全网认可的过程就是所有网络节点进行共识的过程。共识分两个阶段完成，第一阶段是达成交易集的共识，第二阶段是 对新生成的区块进行提议，最终形成被共识过的区块。达成交易集的共识分 轮进行，在每一轮中进行下面的操作：

- 每个节点在共识开始时尽可能多地收集需要共识的交易，并放到"候选集"里面；

- 每个节点对它信任节点列表中的 "候选集"做并集，并对每一个交易 进行投票；

- UNL 中的服务节点交易的投票结果，达到一定投票比例的交易会进入到下一轮，达不到比例的交易会被丢弃，或进入下一次共识过程的候选集；

- 在最终轮中，所有投票超过 80%的交易会被放到共识过的交易集；与比特币类似，交易集也采用 Merkle 树数据结构。 形成交易集后，每个节点 开始打包新的区块，打包区块的过程如下：

把新的区块号、共识交易集的 Merkle 树根 Hash、父区块 Hash、当前时间戳等内容放到一起，计算区块哈希；每个节点广播自己得出的区块哈希到它可见的节点；节点收集到它所有可信列表中节点广播过来的区块哈希后，结合本节点生成的区块哈希，计算每个区块哈希的出现次数（即每个节点"投票"区块 哈希的次数），如果某 区块一哈希的比例超过阈值（一般是 80%），则认为这个区块哈希是共识通过的区 块的哈希。如果本节点生成的区块哈希与之相 同，则说明本节点打包的区块得到了确，是新的被共识过的区块，直接存到本地，并且更新状态。如果本节点生成的区块哈希与共识通过的哈希不同， 则需要去某个区块哈希正确的节点索要新的区块信息，然后存储到本地并且 更新当前状态；

如果上述环节中没有任何一个区块哈希的出现次数（投票比例）超过设 定的阈值，则重新开始共识过程，直到满足条件。 至此，一个区块的共识过 程结束，开启下一轮共识过程。

3.2.4 数字网关

OA 数字网关是资金进出 OA 系统的进出口。它像一个中介，人们可以通过这个中介将各类货币（不论是各国法币，还是比特币等虚拟货币）注入或抽离 OA 系统。这样的话，即使两个人互相是无信任的陌生人，只要他们两个人同时都信任同一个网关，这两人之间的转账就可以进行。

如果"网关"是由大银行或大金融机构充任，那么这个信任链是很容易 建立起来的。"网关"的引入解决了用户之间的转账不再局限于熟人之间，陌生人之间也可以进行。

OA 数字网关算法是在网关间寻找最短路径，只要有中间网关存在，就可

以形成一个信任链，使得商品成功交换。如下图 Alex 的代理人 AgenOA 可能不相信 Beth 的代理人 Agent B，但是有可能存在相信他们双方的第三方代理人 Agent C，此时会出现 2 个欠条：Alex 的代理人欠第三方代理人；第三方代理人又欠 Beth 的代理人。第三方代理人 Agent C 则负责交易的处 理，通过第三方代理人可以形成一个支持不同币种交换的桥梁，通过融合闪电网络可以实现秒级支付。

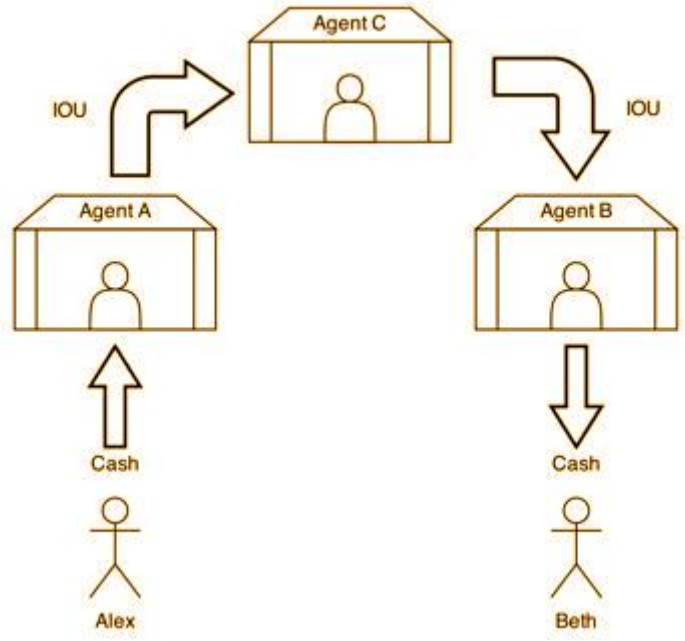


图 3-1：网关交互

区块链网关本质上就是一套基于 BTC、ETC 的支付记账系统，可以和商 户的订单系统对接，转 Token 后自动报单，也支持给会员批量转 Token 发 Token，支持后台手动批量转 Token，也支持 API 自动转 Token。

3.2.5OA 智能合约

OA 在智能合约功能实现上采用类似计算机存储体系结构的层次化思想，通过虚拟机(OAVM)。智能合约接近法律合同语言、安全性高，智能合约的 手续费根据合约所占字节计算。OA 的智能合约由陈述性和完全布尔语句组 成，

因此更接近传统的法律合同语言，支持布尔运算，数学运算，甚至数据 存储等。OA 提供了多种常用的声明式智能合约的模板供用户使用或改进以 满足自定义需求，降低了合约部署难度和出错率。

下面是一个智能合约模型：

["contract template", [

"hash of unit where the template was defined",

{param1: "value1",param2: "value2"}]]

OA 内置智能合约模块软件包，从模块结构上看，OA 智能合约模块 处于对外服务模块（如 RPC 模块）和底层设施模块（如网络模块、存储模块、 账户模块等）之间，存储模块、基本加密算法、账户模块、网络模块等其他 模块为智能合约提供底层支撑。

智能合约由上层应用定义、由解释器解释、由存储模块存储、由 OA 智能合约模块软件包运算。OA 智能合约解释器将支持多种高级编程语言。 应用开发者可以使用自己熟悉的语言设计 OA 智能合约。

3.2.6 非交互式随机数生成算法

非交互式随机数生成算法是指无需用户提供额外自定义信息参与随机数种子生成的算法。我们充分考虑到体育竞猜的公平性，因此应用了硬件种子产生的随机数，确保系统的安全性。下图展示了 OA 非交互式随机数生成过程：

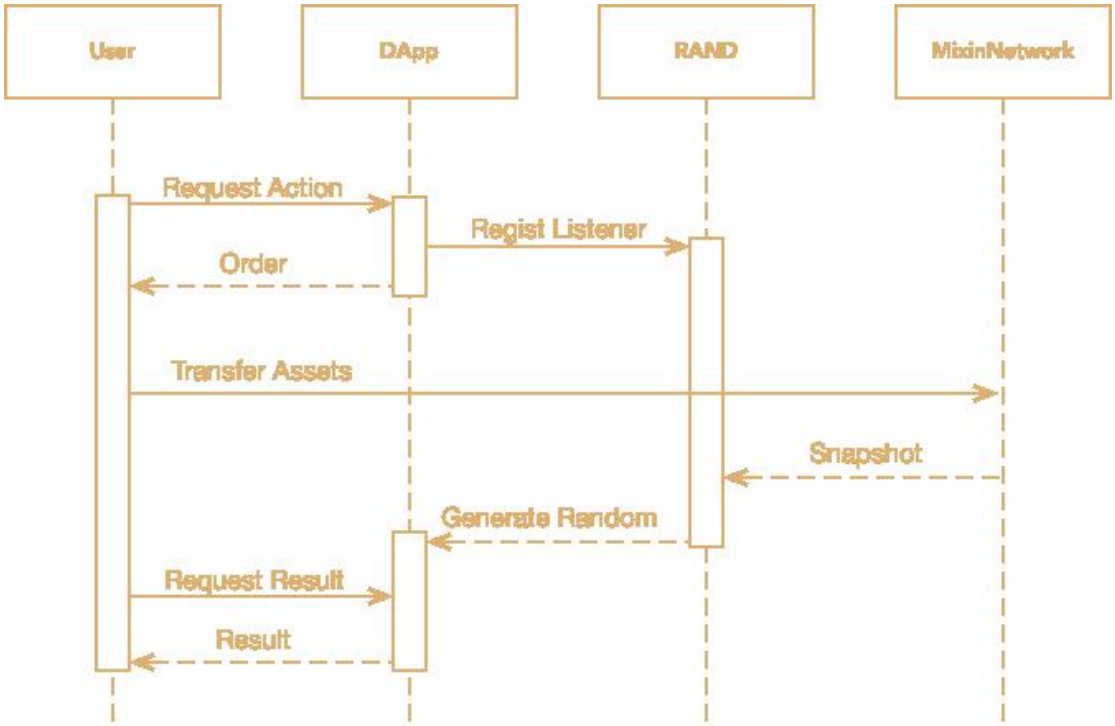


图 3-2：OA 非交互式随机数生成过程

- 用户在 OA 服务中请求注册，OA 服务将会监测注册用户的链上行为；
- 用户发起一次密码生成请求，该求被 OA 的节点验证后，将以 Snapshot 的形式记入区块链账本；
- OA 实时监听到账本中该交易产生的 Snapshot 信息，并获取该 Snapshot 的 ID 值作为随机数种子 seed；
- 选取特定的随机数生成器 rand，生成随机数 r = rand(seed) 给用户；

其中，每个 Snapshot 将由对应请求, 验证节点的签名和验证节点的上一个 Snapshot 三部分组成，将 Snapshot 的内容散列得到的 Hash 值即为 Snapshot ID。这将意味着请求的发起方和验证方都没有办法单方面预测和篡改 Snapshot ID 的值，使用 Snapshot ID 作为随机数种子是安全的。

随机数生成之后，在使用时需要验证其有效性。在 OA 上，可以直接查询到交易对应的 Snapshot，对 Snapshot 内容进行散列获得 Snapshot ID，然后使用该 ID 做为随机数种子，生成随机数并和获得的随机数进行比对，即可验证该随机数是否有效。

3.2.7 抗量子计算

在当前以比特币为代表的区块链系统中，SHA-256 哈希计算和 ECDSA 椭圆曲线密码构成了比特币系统最基础的安全保障，但随着量子计算机技术不断取得突破，特别是以肖氏算法为典型代表的量子算法的提出，相关运算操作在理论上可以实现从指数级别向多项式级别的转变，这些对于经典计算 机来说足够"困难"的问题必将在可预期的将来被实用型量子计算机破解。

加密算法	类型	作用	潜在量子计算机能力威胁造成的冲击
AES	对称密钥	加密	增大密钥长度
SHA-2,SHA-3		哈希功能	需要更大输出量
RSA	公钥加密	数字签名密钥生成	丧失安全性
ECDSA,ECDH（椭圆曲线密码）	公钥加密	数字签名密钥生成	丧失安全性
DSA（有限域密）	公钥加密	数字签名密钥生成	丧失安全性

现有区块链系统大都采用椭圆曲线数字签名方案 ECDSA，但是量子计算机下针对 ECDSA 签名算法非常高效的 SHOR 攻击算法，Shor 算法适用于解决大整数分解、离散对数求逆等困难数学问题，导致 ECDSA 签名算法在 量子攻击下相当不安全。OA 采用基于格理论的签名算法 NTRUSign-251， 算法具体实现流程如下：

1、密钥生成

在环 R 上选择两个多项式 f 和 g 使得 f 和 g 的系数中 1 的个数分别为别为 d_f和 d_g。 并根据 f 和 g, 计算公钥

h: h = Fq * (mod q)

求解多项式(F, G)使其满足方程 f*G −F*g = q

且有||F|| ≈ ||f|| , ||G|| ≈ ||g||。

2、签名过程

对消息 M 进行 HASH 变换，转化为多项式(m_1 , m_2), 其中多项式 m_1 和 m_2均为环 R q 上的一个多项式。 计算环上多项式 A,B,a,b 使其满足:

G * m1 − F * m2= A + q * B

−g * m1 − f * m2 = a + q * b

并要求 A 和 a 的各个项的系数满足大于-q/2 而且小于 q/2 的条件。 对多项式 s 进行计算: s = f ∗ B + F ∗ b(mod q)

s 即为明文 M 使用公钥 h 所计算得到的签名。

3、验证过程

对消息 M 进行 hash 变换，转化为多项式(m1 , m 2), 由待验证签名 s 和公钥多项式 h 计算得到

t = s ∗ h(mod q)

t = g ∗ B + G ∗ b(mod q)

计算多项式(s,t)和多项式(m_1 ,m_2)之间的距离$||m_1 - s|| + ||m_2 - t||$，如果该距离大于 Norm Bound 则验证失败，否则通过验证，签名有效。

总结：已知 NTRUSign-251 签名算法的安全性最终等价于求一个 502 维整数格中的最短向量问题，而格中最短向量问题是在 SHOR 攻击算法下无效的，

在量子计算机下也没有其他的求解快速算法，目前最好的启发式算法也是指数级的，攻击 NTRUSign-251 签名算法的时间复杂度约为 2168，因此采用 NTRUSign-251 算法的 OA 可以抵抗量子计算下的 SHOR 算法攻击。

4、治理结构

为了保障 OA 项目的可持续性、管理有效性，OA 团队成立了 OA 基金会，规范基金会的组织和活动，维护基金会、相关收益人和用户的合法权益，基金会遵守新加坡宪法、法律、法规、规章和政策。OA 基金会下设技术委员会、商务委员、财务及人事委员会、联席代表委员会，重大事项由技术委员会、商务委员会、财务及人事委员会选举组成的联席代表委员会决策。联席代表委员会会长由联席代表委员会选举产生，负责日常事务管理。

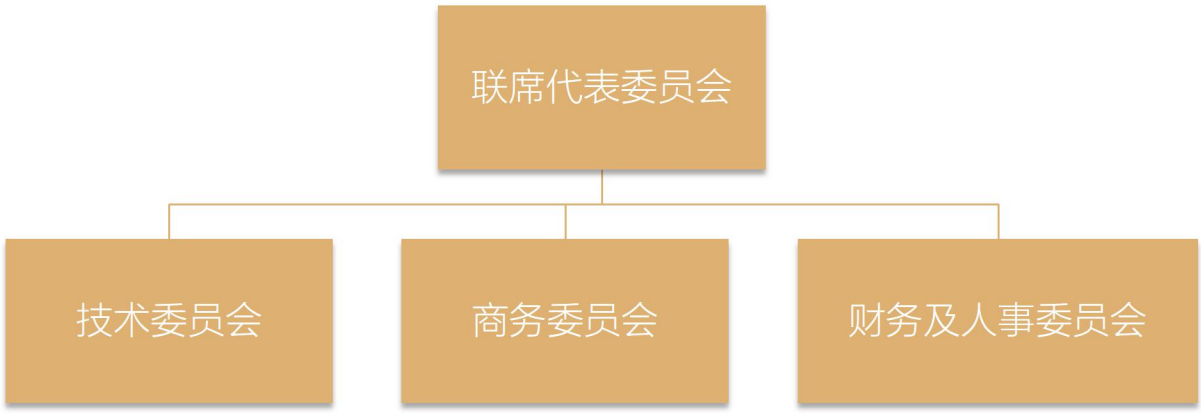


图 4-1：组织架构

1、联席代表委员会为最高决策机构，其职能包括：

（1）修改 OA 管理章程；

（2）监督 OA 章程的实施；

（3）聘任或解聘联席代表委员会会长以及各职能委员会负责人；

（4）制定或修改重要决策。

联席代表委员会成员任期为五年，联席代表委员会成员任期满后，由技术委员会、商务委员会、财务及人事委员会进行再次投票选出 5-20 位成员，被选出的成员将代表基金会做重要和紧急决策，并需在任职期间接受授信调整。

2、技术委员会：

OA 技术委员会负责底层技术开发、各产品开发、审核、管理工作等。具体包括：

（1）代码管理、代码开发、代码测试、代码审核、代码上线、漏洞修复等；

（2）召开项目追踪会议，沟通项目进展及需求；

（3）挖掘 OA 技术的应用场景，从而实现商业落地。代码开源审查，公链、联盟链开源、私链可以允许不开源。

3、商务委员会：

（1）负责 OA 技术推广、原链产品推广、各种资源对接等；

（2）塑造 OA 品牌形象、建立健全各项管理制度；

（3）负责公关事宜。若发生影响理事会声誉的事件，经内部审核评估后，统一由委员会进行公关回应。

4、财务及人事委员会：

（1）负责薪酬管理、日常运营费用审核等；

（2）负责各种行政类事务，如相关文件起草、审议，会议日程安排等。

5、发行说明

5.1OA 币简介

OA 币是驱动去中心化运动生活生态系统运转的血液。主要应用于全球体育运动健身领域的开发、保护、支付等场景。后续我们将鼓励各个公司或个人在 OA 基础上开发各种侧链及应用），届时，不同侧链和应用之间的数据交互、智能合约执行及各环节资产和信息数据交换都会消耗 OA 币，OA 币成为整个生态系统上的基础数字货币。

5.2 发行方案

OA 数字资产总发行量 2 亿枚，发行方案如下：

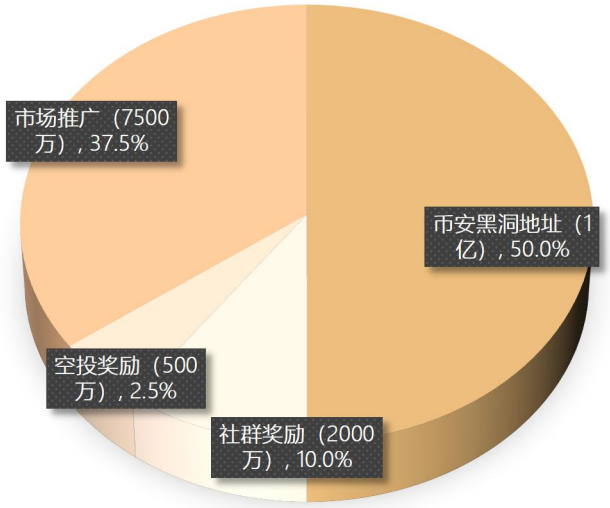


图 5-1：发行方案

原始价格：0.01USDT

空投时间每天一次：瑞士洛桑时间 12：00~15：00

6、风险提示及免责说明

6.1 免责声明

本文档仅提供和项目相关的信息；本文档或文档中的任何内容均不得视为招揽，提议购买，出售任何证券、期货、期权或其他金融工具，或向任何司法管辖区的任何人提供或提供任何投资建议或服务；本文档中的任何内容均不构成投资建议或对任何证券的适用性提供任何意见。过去的表现不一定表示未来的表现，本文档中的任何预测，市场前景或估计均为基于某些假设的前瞻性陈述，不应该被视为指示将发生的实际事件。

意向兑换人若自行决策后进行兑换，应当完全接受该等风险，并愿意自行为此承担一切相应结果或后果。基金会及团队明确表示不承担任何参与 OA 项目造成的直接或间接的损失，包括但不限于:

- 因为用户交易操作带来的经济损失；
- 由个人理解产生的任何错误、疏忽或者不准确信息；
- 个人交易各类区块链资产带来的损失及由此导致的任何行为。

6.2 风险声明

OA 开发和运营团队相信，在 OA 的开发、维护和运营过程中存在无数的风险，很多都会超出团队的控制。除本白皮书所述的其他内容外，每个 OA 的购买者还应该细读、理解并仔细考虑下述风险：OA 是一个加密数字通证。兑换 OA 不是一种投资，我们无法保证 OA 一定会增值，在某种情况下具有价值下降的可能，没有正确使用 OA 的用户有可能失去使用 OA 的权利，甚至可能失去他们的 OA 账户。基金会及团队发起人现向意向用户明确兑换 OA 的风险，

意向用户一旦参与即应当被认为明确知悉并完全了解以下风险：

信息披露风险：截止到本白皮书发布之日，OA 仍在不断完善，其哲学理念、共识机制、推演算法和代码以及其他技术细节和参数可能频繁随时发生变化和更新。尽管本白皮书包含了 OA 最新的关键信息，但并非绝对完整。且仍会被 OA 开发和运营团队为了特定目的不时进行调整和更新。OA 开发和运营团队无能力且无义务告知参与者 OA 在开发中的每个技术细节，因此信息披露的不充分是不可避免且合乎情理的。

市场竞争产生的风险：区块链是一个竞争异常激烈的领域，有数千个团队正在计划并着手开发不同的项目，竞争将是残酷的，但在这个时代，任何好的概念，创业公司甚至是成熟的公司都会面临这种竞争的风险。但对我们来讲，这些竞争都是发展过程中的动力。

法律政策风险：OA 项目可能被各个不同国家的主管机构所监管，且由于加密货币的发行具有极大的创新性，在全球范围内的绝大多数国家均具有法律空白，行业存在极大的法律及政策不确定性。

价格波动风险：若在公开市场上交易，加密通证通常价格波动剧烈。短期内价格震荡经常发生。该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。OA 项目的开发和运营团队对任何二级市场的通证交易不承担责任。OA 币交易价格所涉风险需由交易者自行承担。