初链

——高性能混合共识公链

摘要

打造承载未来商用去中心化应用的公链，是时代的需求，也是初链的梦想。基于混合共识机制设计的初链，旨在为社会提供高速点对点通信、价值传输以及智能合约基础设施。

去中心化的最终目的，是打造自由平等的互信社会。经过以太坊等公链项目的努力，公链开发已取得显著进步，数字货币和智能合约的商业化使用成为可能。在此之前，部分私有链与联盟链已成功落地应用，让人们对公链开发者们产生了更大期望，希望商用公链的到来可以解决数字支付、智能合约等成本较高的现实问题。然而，公链之所以区别于私有链与联盟链，核心正在于其共识机制的设计需要保证互不相识、不断扩充的节点能通过技术手段彼此间建立信任，并集合算力完成任务，保障公链稳定、高效地运行。现有的共识机制设计大多难于在安全性与性能间实现良好平衡，正如分散决策与行政效率间的两难取舍，困扰住了公链开发者们。

初链希望在保持去中心化本质的同时，尽可能提升效率。POW 与 PBFT 相结合的混合共识机制设想的出现，为问题的解决带来了一丝曙光。

一、优势

支持无限节点进入

对于互联网电商、即时通讯软件、双边交易平台等大规模商业应用，支持大规模和不断增加的用户数目是公链承载它们的必备条件。PBFT 的通信复杂度决定了参与决策的节点只能保持在极有限的范围内。而利用 POW 可以接纳无限节点的特性与之结合可以弥补这一弱势。

安全性

PBFT 由于无法保证全体节点参与决策，所以存在比较强的道德风险及安全隐患。少量节点的不作为或宕机可能导致其他节点的数据被篡改或全链瘫痪。以 POW 为基础，选举产生 PBFT 主干节点的混合共识机制设计可以保证 PBFT 主干节点出现安全问题时及时进行重新选举，并对主干节点进行实时监督。

高性能

用户交易被及时记录是公链可用性及安全性的保障。PBFT 主干接点的通讯效率足以支持 10,000-100,000 TPS（每秒交易处理量）。可以保证多个智能合约或商业应用同时处理交易时全链通讯不受到阻塞，账本按时间先后顺序准确记录交易。

免费使用

无论是现在初步的测试网还是未来上线的主网 Stellar，初链将一直保持向所有用户免费开放的准则。初链始终认为，区块链公链是面向所有用户的基础设施，而非牟利工具。为每位用户提供更贴合需求、使用便捷、无成本的公链开发工具不只能为未来初链寻找合适盈利来源开拓空间，更有助于整个公链开发乃至区块链行业的长足发展。

二、技术架构

初链的技术架构分为三层，自下而上分别为：混合共识机制、智能合约、合约抽象。

混合共识机制

共识机制的设计是公链与私有链、联盟链的核心差别，其需要足够去中心化以实现安全性，又需要高运行速度以保证性能。行业已经基本形成认识——仅靠单一共识机制难以兼顾效率与去中心化本质。为弥补前两代公链比特币与以太坊 TPS 过低导致无法应用到实质商业应用开发的弊病，初链选择了将 PBFT 的高效与 POW 的去中心化相结合的混合共识机制。在保证去中心化本质的基础上，实现高性能、高可靠性的公链开发，以承载规模化商用 Dapp 运行的目标。

分布式协议的解决方式大致一分为二。一种是以比特币为代表的 POW 解决方案，已被证明在交易处理速度上难以更进一步；一种是以众多私有链、联盟链为代表的 PBFT 解决方案，可以高效处理大量交易。但 PBFT 解决方案要求参与记账的众多节点彼此信任，因此节点们最好在协议生效之前就相互认识。但将相互认识的主干节点对全链交易进行记录的构造应用到公链开发中无疑存在着巨大的道德风险。如何在公链中建立高效互信的共识机制，成为世界性的难题。

初链的解决方案各取二者所长。保留 PBFT 记录账本的机制不动，将超级节点的选取开放给公链，利用 POW 协议作为准系统支持超级节点的动态选取和协议达成，将主干节点社区的组建由私有链与联盟链性质转换为公有链性质。

智能合约

智能合约层是共识机制落地应用的关键一步。智能合约的运行必须依靠虚拟机完成，保证统一智能合约在不同环境下可以运算得到同一结果。初链继承了以太坊的虚拟机（EVM）的设计思路，在 PBFT 上推出 TVM。TVM 将植入每一个进行决策的主干结点，使得它们能根据单个需求进行调用请求。

合约抽象

合约抽象层将抽象智能合约中的基本商业逻辑，简化开发者设置复杂智能合约的流程。

三、应用生态

保险

保险同样是初链可以发力的领域。区块链与保险业的融合可能真正推动保险向自动理赔的方向发展。区块链下的智能合约可以在触发条件达到时自动进行理赔，省却繁琐的理赔步骤，避免可能存在的道德风险。农业险种一直是保险难以涉足的领域，因为粮食产量受到诸多自然及认为因素影响，留存证据困难导致理赔困难，因而农民难以理解和接受农业险。如果利用传感器衡量温度、湿度、风速等天气情况，达到条件时即触发自动理赔，就利用智能合约自动完成、不可篡改的特性实现了低成本、快速、标准化理赔。同理可应用于飞机延误险。通过调用航空公司或机场公共接口，智能合约自行判断航班是否发生延误并确定延误原因，从而自动触发理赔行为。当航班延误，旅客看到自己账户的余额不断增加时，其激动的情绪也许就会平息许多，不会再爆发大规模围攻登机口的情况。

此外，传统保险业可能被新出现的互助保险模式所颠覆。互助保险与去中心化交易机制是完全互通的。各用户是完全平等的，而非现在较保险公司处于弱势地位。由于不再需要中介充当组织者建立资金池，用户间完全可以利用区块链共识机制的设计，依靠点对点互助的形式设立保险。每一笔保费的支付可追查、可溯源、公开透明而及时高效。结合初链的混合共识机制设计，互助保险也可以采用分层监督的方式保证道德风险的出现。

区块链技术让保险业得以重归匹配供需、计算风险的主业上，而非像今日一般如此注重资产管理能力。这本不该是保险的本意。

医疗

在医疗领域，区块链的匿名性、去中心化等特征可用于保护病人隐私，电子健康病例（EHR）、DNA 钱包、药品防伪等都是区块链技术可能的应用领域。

IBM 在 2017 年发布了一份医疗保健与区块链的报告，具体阐释了区块链技术在临床实验记录、监管合规性和医疗/健康监控记录领域可能发挥的巨大价值，以及健康管理、医疗设备数据记录、药物治疗、计费和理赔、不良事件安全性、医疗资产管理、医疗合同管理等方面的特殊优势。

在 EHR 方面，个体完整的健康历史记录，包含每个生命体征、高效准确地记

录服药、医生诊断、患者疾病和手术相关的所有信息，与医护人员、地点、事件相关的全盘历史数据对精准治疗和疾病预防有宝贵价值，区块链恰好能将个体乃至机构群体的数据进行实时存储与共享。

在初链体系中，每笔交易都有时间戳，成为永久性记录的一部分，且无法在事后进行篡改。在无权限限制的公链环境中，各节点均能查看所有记录。在有权限限制的公链环境中，各节点可以建立共识机制，确定节点对交易的查看权限，从而维持隐私性，并且在需要时掩盖各节点真实身份。通过这种方式，区块链实现了资产全生命周期的完整记录。在资产流经整个供应链时，无论是患者健康记录，还是一瓶药片，所有记录清晰可见。

IBM 调查了医疗高管对区块链的价值意义，高管们普遍认为区块链能最有效地消除医疗信息摩擦，包括信息不完善、信息风险和信息无法访问等。比如计算机记录能保证信息输入的准确无误，而区块链自身的属性，如挑选最快最好的信息纳入数据库以及高度保密的安全性，将冲破以往医疗信息化的藩篱，最大限度地尽其所长。

区块链应用中智能合约的标准化是关键一环，在医疗行为的监管中有重大价值。当出现非合规事件，智能合约会自主跟踪合规情况、实时向相关方发送通知，有效去除检查环节，简化执行流程，降低监管成本。

在数据保密且质量可靠的基础上，各组织、机构、企业都能加入该系统、利用数据开展合作。采用个人健康数据、医疗设备数据、医护人员采集的数据，开发新的医疗应用或提供服务，实施健康管理并创建新的数据源，由此构成更大的区块链生态，形成良性循环。

在计费和理赔方面，区块链还能有效阻止骗保等不当行为，减少医疗资源浪费。企业 PokitDok、Capital One 和 Gem 提出一种由区块链支持的平台，旨在帮助患者在接受治疗前，提前确定自付费用金额，也能提供预付款等服务，避免造成患者意料之外的成本，医疗机构也能减少未收款项。

区块链的可追溯性，还包括医疗事故的追溯以及药品的回溯与监管。比如建立药物一致性的物流配送与管理体系，对假冒药品构成致命打击。因为区块链的数据是即时更新、广泛共享的，药店、厂商、买家、监管部门等多方都能实时观察数据流动，包括药品制造和分销信息，从而加强药品监管，阻止假药进入市场。

据悉，英国 Blockverify 就是开展药品来源试点项目的组织之一，帮医疗人员通过扫描药品验证真伪。

区块链能杜绝不良安全事件，如解决医疗设备尤其是连网的健康设备的安全问题。2016 年强生公司曾警告患者，其“OneTouch Ping”胰岛素泵很容易受到黑客攻击，无独有偶，FDA 曾报告圣犹大医学心脏设备中存在网络安全漏洞。所以与网络相连的医疗设备的运转正常非常重要，维护网络安全也是区块链在医疗场景中的重要应用。

游戏

本处所指的区块链与游戏的结合并非如以太坊养猫、以太水浒、以太三国等是在区块链上创造出虚拟资产以供收藏，玩家通过新玩家的资金贡献与虚拟资产的流转获得利润的伪“区块链”游戏，而是指区跨链技术应用于游戏产业为产业带来的升级改造。

就目前发展而言，区块链重点可以应用于游戏的虚拟资产流通与博彩平台。绝大多数游戏的用户黏性并不牢靠，用户体验过 A 公司的游戏后可能迅速流失，因为其在 A 公司游戏中的所获并不能转化成其玩 A 公司其他游戏的动力。通过区块链技术保证虚拟资产的可溯源、便捷流转、交易成本低，可以极大提高老玩家的忠诚度，打通 A 公司不同游戏之间的生态，延长用户生命周期。小游戏厂商甚至可以联合起来，将虚拟资产在同一链上交易，以降低用户导流成本，增强用户依存度。

大型游戏往往都举办众多友谊赛、联赛，其间博彩的商机不可谓不大。利用区块链智能合约，解决及时交付与透明性等问题。当接口调用获得游戏结果时，代码自动运行完成博彩交付。

公益

公益是当今时代的主旋律之一。截止 2017 年 7 月，我国 7000 多万贫困人口中，因病致贫的占近 3000 万，如何让公益以更高效、更公平、更透明的方式开展，是每一个公益人的心愿。

捐款者出于社会责任或者是个人爱心，向公益慈善组织捐赠财物，用来帮助陷于困境的群体或者改善社会问题，那么这些钱财到底用在了哪里？可能在每位捐款者心里都会打上一个问号，慈善公益部门也常常会遭到质疑，如何证明已经把善款送到了灾区？如何证明医院真正把捐款用在了患者身上？双方常常会产生诸多矛盾纠纷，就像此前壹基金被怀疑“贪污捐款三亿”、杨六斤 500 万善款事件、红会文家碧贪污事件等等，伤的不仅是钱，更是捐赠者的感情。

将区块链技术应用到公益慈善事业中，将改变传统的公益慈善捐款信息传递模式，区块链作为一项分布式账本技术，具有信息不可篡改、公开透明、可追溯等特点，能够完美解决公益慈善事业存在的痛点，当用户的善款进入区块链系统后，将被自动记录在区块链上，并盖上时间戳，这个记录不可被篡改，每一笔捐款和支持都像“快递”一样有迹可循。

诸多区块链与慈善相结合的项目已尝试落地。

2016 年 7 月，蚂蚁区块链公益正式上线，“让听障儿童重获新声”成为蚂蚁金服与中华社会救助基金会的小规模试水项目。2016 年 12 月上线了新版本，增加了中国红十字基金会的首个区块链公益项目“和听障说分手”和壹基金区块链公益项目“照亮星星的孩子”，实现了实时账目公示，有助于解决公益财务透明的“痛点”。2017 年 3 月 16 日，支付宝上所有爱心捐赠项目已经接入到蚂蚁区块链平台。统计数据显示，截止 2018 年 1 月 30 日，已经有 37 家公益机构，超过 300 个公益项目，接入蚂蚁区块链平台，捐赠人次超过 937 万，捐赠总金额超过 4800 万元。

2016 年 12 月，网络互助平台众托帮在上海举行了“心链”发布会，而“心链”是众托帮依托区块链技术，专门针对公益行业开发的产品，依托区块链技术，所有的爱心将被记录在“心链”上，捐助金额、资金流向等信息公开透明，使公益资金非法挪用成为不可能，这也让个人的爱心行为成为一笔客观的“数字资产”。截止 2017 年 10 月，平台捐赠笔数突破 1 亿，已发行爱心资产近 20 亿。

如此众多，不胜枚举，可以显示区块链与慈善深度融合的未来趋势。

资产证券化

数字货币的延伸在于代币。资产可以变成代币，代币可以转化为资产使用权

的证明。资产变成货币实质是一种证券化。如果节点间能建立一个账本，将资产证券化池子中的资产全部挪到这个账本上，基础资产的各种特征都做好标记，不断循环，按交易时间更新区块，不可篡改，定期跟踪，就能够实现资产证券化与区块链的有效结合。

数字广告行业

由 Facebook、阿里巴巴、谷歌、百度等互联网巨头公司垄断的数字广告行业存在诸多行业痛点。中小型广告媒体受制于互联网巨头公司的体量，被迫与其结成“流量联盟”，议价能力弱。对于广告主而言，可修改的用户点击数据、难以测量的覆盖群体使得数字广告主们面临着严重的信息不对称。广告主们往往为失真的用户点击量和覆盖面支付了高昂的广告费用，而达不到预期效果。

众多广告交易平台的存在一定程度上为广告主们提供了替代解决方案，但双方的信任问题仍未消除。一方面，部分广告平台依靠开发机器人、增加广告点击量来骗取广告费用；另一方面，部分广告主拒绝在广告媒体发布之前支付广告费用。因此，实际上中小广告交易平台与互联网广告平台相比，其效率更低，互信度亦不足。

归根结底，数字广告行业的症结在于信任机制。面对花费高价信任互联网巨头与花费较少但面临欺诈风险的两难境地，广告主们最希望的就是低成本互信广告交易平台的出现。区块链技术的商用使得这种希冀成为不远的现实。

由于区块链的去中心化、匿名性、公开性、自治性、交易记录不可逆等特性，区块链技术得以为其承载的广告主们提供透明互信的交易平台。其主要可以实现：

（1）数据真实传达至受众，并且可统计；

（2）广告主与广告媒体资金往来安全；

（3）各方交易透明化。

利用智能合约，交易双方可以建立安全可靠的交易机制，并使得广告效果可测量，同时降低交易成本。参与到广告交易的用户亦进入了初链的经济生态，其可在初链生态中获取或创造更高的附加价值。

小额支付

在诸多情境下，人们过多地占用了公共资源或造成了负外部性却并未给付相应报酬。如当后车从左方超越前车时，实际占用了快车道这一道路交通资源。拥有路权的前车为让后车超过需要减速避让。在不远的自动驾驶时代，如果后车产生超越前车的需求时，主动向前车发出从左侧超越的请求并支付很小一笔费用，前车接收后自动避让。既能保障超车行为的完成，又能使前车获得放弃路权的收益，安全而公平。

再比如解决垃圾邮件、垃圾短信的困扰。如果每次邮件、短信的发送都需要向对方支付一笔小额费用，对于正常沟通交流的人而言，由于一来一往支付相抵，交流成本并未有显著提高；但对于大量群发垃圾邮件或垃圾短信的人，则会面临巨大的成本，从而遏制大规模单向发送垃圾信息的可能。

小额支付的实现必须由不收取手续费的区块链完成。提供高性能、稳定交易环境的初链正适合这样的落地场景。

价值传输

尽管区块链技术距离真正成熟仍有一段时光，但可以看到其在金融领域的应用已是必然。不仅仅是货币创造，区块链能给金融业带来的真正改变在于价值传输与公共账户，国内外不少机构同时在支付结算、资产登记与资产转让等方面做着积极探索。由于区块链是一个公开、同名、可追溯、不可篡改的分布式总账系统，可以有效降低支付、清算、结算步骤的错误率，同时监控资金每一步的流入流出情况，推动诚信社会建立且有利于金融监管。随着区块链技术不断走向成熟，资产的真实性会得到进一步的保证。

数字版权

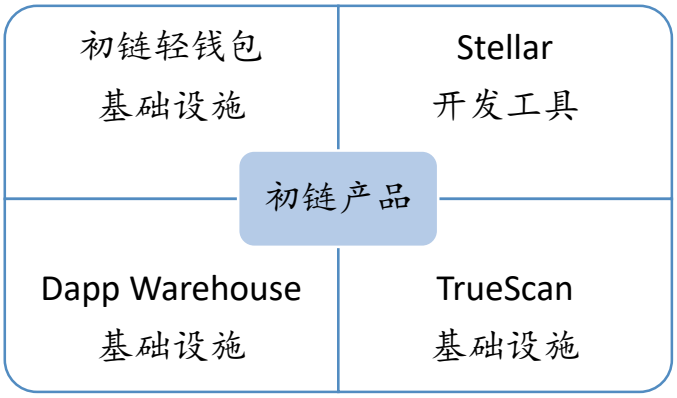
瑞士一家区块链公司 DECENT 希望利用区块链技术完善数字版权管理。通过数字视频指纹识别，即将视频的运动变化、颜色及关键帧等特征记录抽象出独特的“指纹”，利用这一指纹来跟踪保护网络上的视频内容。由于目前区块链数据存储中广泛使用的哈希编码具有唯一性和不可逆性，因此每一文件的编码都不会相同。数字指纹识别技术可以系统地使用文件详细特征来区分正版和盗版内容，并追查盗版来源。

其他应用场景

初链利用其节点的可扩充性与共识机制的高效性、安全性，可以更多地应用到移动数字汇票平台、证券交易等金融业态及物联网、供应链管理、产权追踪、数字证书等领域。

四、产品矩阵

初链的产品矩阵如下：



初链轻钱包为节点提供接收、发送、管理全部初链数字资产等服务。

Stellar 为商用 Dapp 开发者提供便捷、稳定、高效率的智能合约开发平台，开发者可以对合约进行全生命周期的管理。

Dapp Warehouse 为面向用户的 Dapp 下载平台。

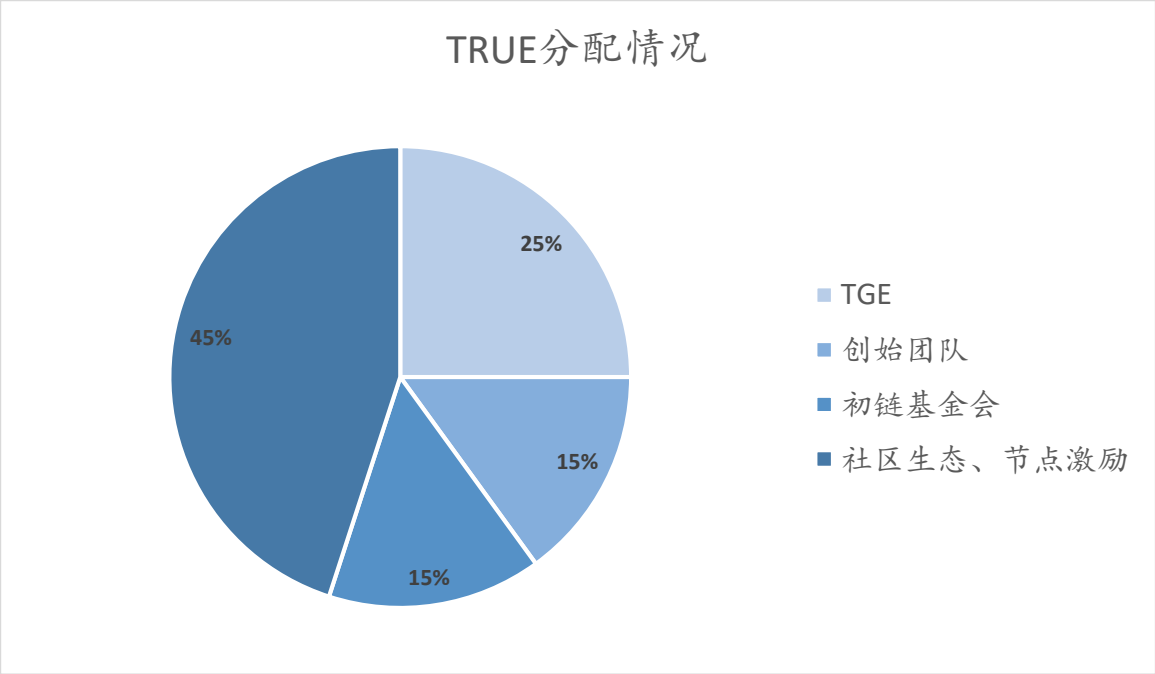
TrueScan 作为初链的区块链浏览器，为节点提供合约监控、交易统计、账本查询、隐私保护等服务。

未来，初链将继续完善智能合约开发工具包，并拓展基础设施的产品丰富度，满足新一代公链使用者开发个性化、复杂化智能合约的需求。

五、代币经济

初链以初链币（TRUE）作为代币，可以实现价值储存、支付手段、价值尺度等职能，共计发行 1 亿。

初链币分配比例如下：



分配给初链团队的 TRUE 将受到长期归权时间表的制约，具体接触制约规则如下：

A. 20%，即 3,000,000 初链币（TRUE）在代币分发后 3 个月后解除制约；

B. 25%，即 3,750,000 初链币（TRUE）在代币分发后 12 个月后解除制约；

C. 25%，即 3,750,000 初链币（TRUE）在代币分发后 24 个月后解除制约；

D. 30%，即 4,500,000 初链币（TRUE）在代币分发后 36 个月后解除制约。

至此，分配给初链团队的初链币全部解除制约。

六、团队介绍

技术、研究及产品

Archit Sharma (Ren X) 初链工程负责人，分布式系统专家，操作系统和性能工程专家，同时主责工程团队管理。Ren X 曾于 Red Hat 和 CERN 就职，从事大规模云服务的规模化及分布式系统的设计与开发。Ren X 是多个重要开源项目的贡献者，以及多个 Docker Hackathon 的冠军。

Eric Zhang 初链创始人及 CEO。中国顶尖的极客平台 TopHacker Group 创始人，连接技术极客与各行业的问题。TopHacker 帮助多个区块链企业解决了核心和应用层的技术问题。

Felix Cai 前端产品负责人，前端极客，毕业于西安交通大学少年班。

Home Chen 移动端产品负责人，从事 IT 工作 20 年，有丰富的互联网产品设计研发、软件项目管理经验。曾是财火火公司的技术合伙人，负责新产品的研发工作，服务器集群和高并发处理。

Jesper L 初链共识研究，应用密码学，密码协议，分布式系统共识专家，毕业于清华大学。

Richard Wang 初链中国技术社区负责人，拥有全国 4000+互联网技术高管资源，300+作者与 400+一线将是资源。担任过多家互联网公司 CTO 及 CEO，深度操盘过多个传统企业互联网转型项目，机械工业出版社技术作者，曾出席国内各大技术峰会担任嘉宾将是，出品人，嘉宾评委。

Seay（法师） 初链安全顾问，《代码审计：企业版 web 代码安全架构》一书作者，Seay 源代码安全审计系统作者，知名安全博客 cnseay.com 博主，曾任阿里巴巴安全转机，阿里攻防实验室负责人，Sobug 技术合伙人，拥有十年安全攻防经验，服务过众多知名企业。

商业和运营

James Cheng 初链创始人，首席战略官，全球公关、机构投资者关系负责人，连续创业者，长安俱乐部会员；黑马会副会长（2015-2016 届）；长城会会员。

Yan Liu 运营总监，负责初链产品和商业运营，以及初链社区建设和运营工作，初链官方社区运营微信号将由“悟空”改为“白 龙 马”。未来将继续加强服务精神。

Larry Lin 初链创始人，新零售与区块链研究院院长，互联网营销与社区运营专家，曾负责中国最大内容共建社区“百度百科”的运营工作，拥有超过 10 年的数字广告和互联网行业从业经验，著有畅销书《微信营销与运营攻略》、《微机四伏-微博与微信营销实战兵法》

James Cooper 初链海外投资者及媒体关系负责人，全球法务合规负责人，全球知识产权法律专家，California Western School of Law 国际法学教授，Proyecto ACCESO 基金会项目主席，曾任美国国务院、美洲发展银行、美国专利和商标局顾问，世界知识产权组织美国代表。

顾问团队

魏先华 中科院教授、博士生导师，中国科学院虚拟经济与数据科学研究中心副主任，中和园-路透金融风险管理联合实验室执行主任。

程浩然 中国最早的数字广告交易所之一——互动通投资人。

周景龙 全球最大互联网组织长城会前合伙人，拥有广泛的全球互联网人脉和各地政府组织资源。

邹均 畅销书《区块链技术指南》的作者，中关村区块链产业联盟专家，服务合约（Service Contract）方向博士，曾任 IBM 澳洲金融行业首席软件架构师，在国际会议期刊 IEEE 上发表论文 200 余篇，其中区块链相关论文获 2016 年 IEEE ICWS 佳博士论文奖。

李雄 联想财经创始人