Luxalpa Chain · 艾尔链

基于DAG通用的

智能合约编程平台与区块链操作系统

白皮书 v1.0

2018 年 11 月

目　录

摘 要

继蒸汽机、电力、信息、互联网科技引发了一次次的社会变革之后，区块链技术由于它去中心化、可追踪、安全隐匿、不可篡改的特性被认为是第五个最有潜力引发颠覆性革命的核心技术。近年来，区块链成为了全世界关注的焦点，研究者从底层技术及基础设施层，通用应用及技术扩展层，垂直行业应用层多方面进行研究，在各国的不断探索下，区块链被逐渐的认识和认可，初步形成了行业生态链条。但是，区块链的发展仍旧面临着很多的挑战，要想实现“区块链+”的生态体系，迫切需要对区块链底层基础设施开展研发，进而为各类区块链应用提供可靠支撑。

LAC（LuxAlpa Chain）艾尔链是基于区块链 DAG 技术开发的主链，致力于为用户们提供可靠的智能合约编程平台与区块链操作系统。LAC 将针对现有实际中存在的问题，尤其是交易拥堵、交易确认时间长、交易匿名保护、存储中心化服务器不安全等问题，利用区块链技术在各个层面的协议和机制上更新改革，优化提升用户的使用体验，保证购物、交易、支付等功能的完全稳定运行，完善平台内的信任体系。

LAC 项目紧跟区块链 4.0 的技术趋势，结合自身需求和特点进行了多种技术创新。主要的包括：①**数据结构层面。**我们基于增强有向无圈图（DAG）构建了底层的数据结构。目标是解决传统区块链系统效率低下的痛点，从底层大幅提高 TPS，使整个链满足支付系统的巨大吞吐量。在 DAG 数据结构上，我们创建了全新的 Traw 架构，完整地定义了整个运行流程，保障了 LAC 在安全的基础上高效流畅运行。②在 Traw 架构上，LAC 提出了 **WAVE 并行异步拓展协议**，通过这种新的协议，LAC 打破了传统链式区块链单向拓展的方式，可以并行异步拓展，使得效率大幅提高，降低了单笔交易费率。③**在容错机制上**，我们定义了 Offline 离线处理容错机制。offline 给 LAC 链带来了更多应激性。使得整个链系统在网络不稳定、延时高的状态下依然能够运行，保证了 LAC 支付系统的稳定。④**在网络通信结构上**，LAC 构建了基于 P2P 的闪电通信网络，点对点（peer-to-peer）的通信结构充分实现了 LAC 的去中心化。基于该种通信架构，我们定义了 BLOOM 协议，采用了全分布式结构化的拓扑结构。并且 BLOOM 在使用了 DHT 散列哈希表组织节点。提高了通信系统的拓展性和容量。⑤**存储系统**，LAC 采用了基于 IPFS 的 T-IPFS 协议，形成了一个内容可寻址、版本化、点对点超媒体的分布式存储、传输系统。T-IPFS 的分片化处理大大地缩短了内容提取时间。通过 T-IPFS 的协议栈，实现了冗余和重复处理，节约了存储所需空间。⑥**在交易匿名保护**中，LAC 运用了零知识证明（zero-knowledge proof）和零币零钞协议（zero-cash protocol），能够提供完全私密化和加密化的虚拟货币转账。满足了不同场景的支付需求。

在分布式共识机制方面，采用了基于 DAG 技术的 RPOS 主侧链结合的安全

高效的共识机制，可异步并发地进行共识验证，大大提高了效率。主链采用的随机可信拜占庭共识是由 VRF（可证随机函数）与改进拜占庭算法结合而成，改进拜占庭算法利用阈值签名的方法保证了在少数节点出现故障时主链仍能稳定运行，提高了安全性。侧链采用的随机可信权益共识，在降低算力消耗的情况下，依旧保持着较高交易并发量。主侧链结合的方式在保证稳定性的情况下，提高了效率，可在更加复杂的场景中应用。

在智能合约与账户方面，采用简单的非图灵完备智能合约和更加复杂的高级图灵完备智能合约相结合的方式，平台为用户提供简易的操作模板，降低了编写智能合约的门槛，使受众范围扩大。平台同时支持具有一定程度编程能力的用户进行高级图灵完备智能合约的编写，增大了智能合约可应用范围，使其适用于更复杂的交易场景。

在 API 接口方面，平台为电商提供庞大的基础函数库。函数组以功能分类为模块，在实际操作时只需要调用功能模块，便可进行程序的设计，降低了电商信息接入的门槛。同时平台使用专业团队进行定期维护函数库，确保其可用性及安全性，并提供多方参与基础函数库的维护的应用程序，为函数库的维护拓宽了来源。

LAC 创新性的底层技术为其广泛的应用场景提供了坚实的技术基础。LAC 生态将会首先整合电商平台的流量优势和上游的供应商资源，以区块链支付作为突破口，打通场景、渠道和用户，适应新零售大背景下的消费方式变化，重新构建平台、消费者和商户三方的关系。进而提供与消费相关的泛金融服务，充分满足消费者的需要，丰富平台金融服务生态。

同时，LAC 也是一个具备强大社会责任的项目，让项目发展能够惠及社会上的每一个人是我们的宗旨。因此，我们设计了完备的慈善生态，用区块链技术推动慈善事业向着透明健康的方向发展。除了慈善生态，LAC 还会在众筹场景得到广泛应用，让拥有创新性想法但是却苦于资金支持的项目茁壮成长，赋能实体经济。

一、区块链技术背景

1.1 区块链介绍

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，本质上是一个去中心化的数据库。区块链采用非对称加密技术，能更好的保证交易的安全，保护数据隐私。

区块链技术经历了四次更新迭代。区块链 1.0 阶段主要是以区块链为底层技术的比特币以及其他虚拟货币的开发与发展；区块链 2.0 对应的是智能合约，与货币相结合,对金融领域提供了更加广泛的应用场景；区块链 3.0 则和经济社会的各行各业结合延伸到一切领域。区块链 4.0 关注的是生态体系的完善，进一步支撑区块链作为行业的基础设施。

1.2 区块链发展现状

全球区块链仍处于探索阶段，发展不成熟，处于一个逐渐被认识和认可的阶段。区块链市场规模飞速增长，预计 2018 年会达到 41.4 亿美元。国际标准化组织启动了区块链标准化相关工作，各大区块链联盟纷纷加速推进区块链标准的制定进程。来自于金融、物联网、医疗、知识产权、供应链等等的各行各业的企业纷纷加入到区块链的浪潮中。区块链研究在技术研究和应用的业务场景拓展方面不断发力，逐步从概念化“脱虚向实”形成了初步的行业生态链条。

对区块链技术的研究和探索主要集中在 3 个层面：第一个是在底层技术及基础设施层，主要包括区块链相关硬件与基础协议的研究。第二个在通用应用及技术扩展层，为行业垂直应用层提供服务和接口及相关技术服务。第三个在垂直行业应用层，在金融、物联网、供应链、数字货币、娱乐、医疗等垂直领域落地实施。

区块链的发展仍旧面临着很多的挑战，要想将这一颠覆性技术真正融入到现实经济社会中，迫切需要对区块链底层基础设施开展研发，进而为各类区块链应用提供可靠支撑。

1.3 区块链面临的困境

1.3.1 高成本与高门槛

区块链技术的使用成本较高，限制了需要灵活构建免费服务的开发人员，在一定程度上阻碍了其成为主流应用。目前区块链还未面向主流消费者，几乎所有的区块链应用都要求用户运行区块链全节点或轻节点，学习成本较高。

1.3.2 性能低

区块链技术对于传统行业的改造有利于解决行业当前遇到的痛点，但是由于技术的不成熟，在实际的落地当中却不尽人意。交易速度慢，交易费用高，都是阻碍区块链技术落地的障碍。比特币所使用的区块链每秒只能处理 7 笔交易，以太坊稍高一些，但是面对每天上千万笔交易的需求也力不从心，交易延迟会严重影响用户体验，极大地削减了区块链应用的竞争力。

1.3.3 能耗高

消耗资源获挖比特币是相对公平的分发初始比特币的方式，其消耗的资源数量巨大，据测算，2018 年 5 月 25 日全球比特币挖矿耗电 1.88 亿千瓦时，是 2017 年同期的 6 倍。全球比特币挖矿总耗电量相当于捷克一个国家的耗电量，占全球电力消费的 0.31%。目前比特币全年碳排放相当于 3385 万吨，平均每个比特币交易排放 474 公斤二氧化碳。巨大的能源消耗使得有一部分人对此广为诟病，认为这种消耗没有带来实质的价值。

1.3.4 安全风险

区块链技术在安全性能方面，仍旧存在部分风险，如 51%算力攻击，智能合约漏洞等等，并非无懈可击。

51%算力攻击是指当一个节点的算力达到足以篡改区块链记录时所造成的风险。在 POW 机制中，当节点接收到了从其他节点传来的更长的区块链时，会自动放弃当前的链，转而继续在新的主链上进行挖矿，这样一来拥有 51%算力的矿工，就能够撤销之前的交易记录。

除了算力攻击，攻击者还通过发布包含恶意代码的“智能合约”，控制区块链网络中的所有节点。从 The DAO，BEC，Social Chain，Hexagon 到 EOS 漏洞，“智能合约”已经成为区块链安全的重灾区。

二、LAC 艾尔链项目介绍

2.1 LAC 艾尔链项目介绍

LAC 采用了 DAG（Directed Acyclic Graph）有向无环图的技术，其异步并行延展的性质极大的提高了区块链的交易速度。其类网结构保障了良好的可拓展性，并且能够支持声明式的智能合约。在 DAG 的支持下，LAC 吞吐量大，可以满足多种场景下的复杂应用。用户可以通过 LAC 钱包，用在交易所用法币兑换 LAC，整个交易过程由 LAC 网络中的 Witness 节点和 Hub 节点的 DAG 共识完成；在数据存储上，我们利用了 IPFS 星际文件系统来进行文件管理，提高了速度，降低了损耗。同时，支付平台通过调用 LAC 的充值、提币等接口，可以实现支付平台交易的去中心化和高安全性。并且在交易过程中，我们利用零币零钞协议保障交易的去隐私化，保护了用户的敏感信息。

2.2 LAC 主链

LAC 艾尔链是运用 DAG 区块链技术搭建的主链，用以 LAC 代币的发行和流通。国际电商平台可通过 LAC 主链，实现产品与资产的上链，并按照 LAC 内完善的兑换体系，以一定比例进行兑换代币，同时将之对代币持有者公开，省掉代币交易的繁琐工作，交易可以做到接近实时的校验和确认、自动结算，同时监管者可以利用密码学的安全保证来审计不可篡改的日志记录。

LAC 主链具有以下特点：

- 最大限度的避免虚假信息，数据全局共享，满足合法需求的用户可以在链上访问和收益的所有数据。链上资金数据的安全性和完善性可得到根本保证，不会发生信用风险。
- 币值浮动与股价波动相关，发行的代币是有股票价值背书的数字资产。
- 随时可以完成代币的买入和卖出，对应着账户中代币所有权的转移，交易不可篡改。
- 明确记录了智能合约与用书面语言攥写的法律文件之间的关联。依靠智能合约自动执行，不需要第三方机构监督执行，省去人工成本，提高执行效率和正确率，环节众多，耗时较长，实现金融脱媒化。

2.3 LAC VISA 卡

LAC VISA 卡是通过 LAC 主链上的应用程序创建的匿名虚拟预付万事达卡。LAC 通过与国际主要金融公司合作，与万事达卡和 VISA 公司共同打造一个高效便捷的全球统一平台，帮助用户可以轻松方便地购买虚拟货币并将其存入预付卡中，为用户解决数字资产转移与跨境支付途中会遇到的问题。

LAC 艾尔链运用 DAG 技术打造钱包，利用保险机制，在绝对安全的基础上实现轻松、便捷、稳定的代币交易。用户的 LAC VISA 卡，对应着一个数字资产账户，后台显示用户拥有的代币数量、代币价格等信息。LAC VISA 卡通过整合区块链技术、移动互联网技术、快捷支付技术和生物识别技术，将支持基于 LAC 主链下发行的所有代币，不仅是跨境支付的输出口，也是数字经济价值的交换载体。

LAC VISA 卡具有以下特点：

- **安全**

  LAC VISA 卡采用密码学的 RSA 加密技术、离线冷存储、二次认证、生物信息识别等方式全方位地保证数字资产的安全。智能合约的使用也将有效避免双方交易违规，使得每一笔交易能正常进行而不至于用户数字资产受骗。同时 LAC VISA 卡将采用 IPFS 分布式存储技术将用户的个人信息以及交易数据进行分布式储存，以免不法分子有意窃取和篡改相应数据进而保护用户个人信息安全，避免在支付途中个人信息泄露。

- **便捷**

  与传统交易的中心化审核方式不同，LAC VISA 卡背靠区块链技术，利用智能合约可以实现 C2C 的自动交易。并且与实物相比，LAC VISA 卡更易安装、携带，也没有丢失的风险。并且 LAC VISA 卡将针对所有用户采取统一的支付标准与结算体系，使得交易最终结算简单快捷，有效降低交易成本与交集时长。同时，由于交易双方可能原本处于不同交易平台，LAC VISA 卡将起到一个统一平台的作用，交易双方的资金从原有平台出发，在 LAC VISA 卡平台实现交汇。LAC VISA 卡与用户各种原有平台都将建立长期稳定的合作关系，用户不必再支付跨平台转账交易产生的费用，而是由 LAC VISA 卡官方起到沟通作用，大大地降低了跨境跨平台转账的手续费用与耗时。

- **稳定**

  更重要的是，LAC VISA 卡采用 DAG 技术，以有向无环图为基础，再通过独特的技术优化，使得 LAC 能够拥有庞大的吞吐量，并辅以保险机制，多网点

多渠道同时进行转移支付，也有效避免了双花问题。同时 LAC 官方平台提供 LAC VISA 卡的长期技术维护，可支持同时在线用户数量超 5000 万，每秒 1000 次的代币交易，充分保证 LAC VISA 卡的稳健可用性，有效缩短了转账时间，达到即时转账的功能要求。同时，LAC VISA 卡将为 LAC VISA 卡持有者提供长期持有收益，佣金费用相对于比特币等传统数字货币转账也极低，大幅降低了转账所需费用。LAC VISA 卡在跨国跨境支付环境中有望做到与在国内支付环境下的微信与支付宝一样的方便快捷。

2.4 LAC 总体设计

2.4.1 LAC 网络设计

LAC 网络主要由 Trawl 网、Witness 节点 Hub 节点、LAC 钱包等核心功能模块组成。

- Trawl 网：Trawl 网为 LAC 网络的节点链接结构，用来进行节点的添加，认证，防止双花等核心功能。
- Witness 节点：Witness 节点为 LAC 网络的见证人节点，用来确认 LAC 网络的每笔交易。
- Hub 节点：Hub 节点为 LAC 网络的全节点，存储 LAC 网络所有区块信息。
- LAC 钱包：LAC 钱包既支持 windows 等电脑平台的全节点钱包，也支持 Android、IOS 等手机端的轻节点钱包。

在 LAC 网络中，所有的 Hub 节点都由 P2P 网络组织，其他节点的通信需要经由 Hub 节点。通过全网多个 Hub 节点的互联，整个网络的通信效率将大大提高。而用户在选择时，可以选择任意一个想接入的 Hub 节点。需要说明的是，网络中的 Relay 节点不提供端到端的信息加密服务，但它的功能与 Hub 节点有相似的地方。

在通信上，Hub 节点在全节点钱包基础上，提供了数据转发的功能。

在数据储存上，全节点钱包和见证人保存完整的账本数据，但仅供它们自己使用；而轻钱包是不保存完整的账本数据的；只有 Hub 节点保存完整的账本数据，并与其它的节点进行共享。

2.4.2 LAC 应用平台设计

LAC 应用平台为 LAC 支付提供底层架构支持，后端服务调用 LAC 网络的钱包接口，支持 LAC 的支付、充值等业务。

- LAC 应用 Server LAC 应用后端服务，支持 LAC 支付平台现有业务流程。
- LAC 钱包接口 主要包括生成 LAC 用户的充值地址接口、支付接口等。

2.4.3 LAC 用户

LAC 客户端为用户提供各种可操作界面，LAC 客户可以利用法币到交易所购买 LAC，向地址充值：

- LAC 客户端 LAC 客户端通过调用 LAC 应用 Server，为用户提供各种可操作界面。
- 交易所 LAC 客户可以利用法币到交易所购买 LAC ,向 LAC 钱包地址进行充值。

2.5 LAC 解决的问题

2.5.1 使用 IPFS 星际文件存储技术替代中心化服务器

IPFS(Inter Planetary File System)是颠覆 HTTP 协议的分布式存储系统，它整合了近几年最好的分布式系统思路。LAC 决定采用 IPFS 星际文件存储技术替代中心化服务器，为全球用户提供安全可信赖的信息存储空间。

IPFS 用基于内容的寻址替代传统的基于域名的寻址，用户不再需要依赖中心化服务器，更不用考虑文件存储的名字和路径。IPFS 也是通用目的的基础架构，基本不存在中心化服务器存储上限瓶颈的问题。LAC 可利用 IPFS 技术将用户的个人信息以及交易数据进行分布式储存。所有大文件会被切分成小的分块，下载和上传的时候可以从多个服务器同步进行。文件也不在以中心化的方式进行存储，而是分布式方式，以免黑客有意窃取和篡改数据。

2.5.2 LAC 作为第三方评级机构，建立完善的信用体系

LAC 艾尔链将作为用户与国际电商平台之间的第三方评级机构，利用 LAC 主链上智能合约，建立稳定可靠的平台，会将用户的分享记录、国际电商平台的产品信息上链，实时发布有利于双方的咨询信息，消除双方的信息不对称；还会保证 LAC 代币的稳定流通，利用区块链技术形成一整套的信用管理和应用体系，建立用户和国际电商平台之间完善的互信机制。这一机制将利用去中心化的运行方式，保证信息的公开透明，长期维持参与双方的信任与合作。

2.5.3 与金融机构合作，支持数字货币支付

LAC 将与国际电商所处地区的金融公司密切合作，打造出一套全新的支付体系与规则，打破跨境支付等限制。

LAC 将基金会通过提前购买好数字货币，为用户预留钱包中等值的数字货币，以“预购”的形式存在于每名用户的钱包中。当在国际电商平台产生即时交易时，用户只需要通过线上智能合约和电子签名的方式，直接调用钱包中“预购”形式的数字货币进行支付，免去场内外兑换数字货币的波动性风险以及法律顾问等工作。

2.4.4 电商平台上链

LAC 艾尔链包括主链与侧链，LAC TOKEN 将以主链技术为基础作为核心币发行；其他国际电商平台都将上链，以侧链技术发行各电商平台 TOKEN。当用户在国际电商平台产生跨境支付时，可随时以 LAC TOKEN 为核心，与各侧链上的平台 TOKEN 产生主链交互，进行价值兑换。这样用户将通过数字货币支付的方式，避免跨境支付时，实时汇率波动造成的不稳定因素。

2.4.5 采用去中心化社区运营体系

LAC 艾尔链将采用去中心化社区运营模式，把一个高度中心化的管理网络变成一个几乎无中心化的管理网络。

传统的社交网络中完全依赖于一个中心点 A，如果点 A 消失或者崩溃，整个网络将会完全消失。但是在 LAC 的去中心化网络中，A 即使仍是一个重要的中心节点，但却已经被其他节点建立起了联系，即便把 A 从网络中拿走，整个网络也仍可以保持较高的紧密度并继续运行下去。而图中的其他节点，就是 LAC 项目中的社区共同维护者们，LAC 项目就是 A。A 的目标就是制定项目的未来战略规划和能够被大家认可的普世价值观，并且建立起这样的一个信任网络；而节点们则负责补充完善和维系整个网络，等到未来根据各个节点的贡献程度，会在这个网络中担当一些重要的角色，比如精神领袖，话题发起者等。这时社区的生命力和可持续性就会得到加强。

三、区块链技术

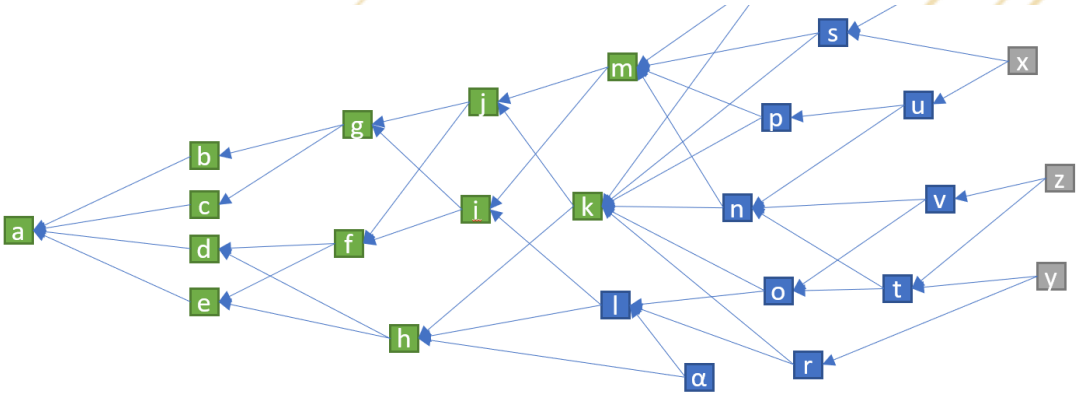
3.1 基于 DAG 的数据结构

自从诞生以来，区块链从比特币的区块链 1.0，到以太坊的区块链 2.0，最后到区块链 3.0，在不断向前发展。交易体系越来越成熟，也涌现出了很多不同的共识机制。但是区块链的本质依然是“链”，这种链式的数据结构是区块链的特点，但也成为了限制区块链交易速度的重要因素。比如比特币系统，只能够单链延伸，通过 pow 共识机制十分钟打包一个块，而确认交易要 6 个连在一起的块。整个过程需要 1 小时左右。低下的 TPS 根本无法满足实际应用。所以，突破传统的链式结构，是区块链技术走向繁荣的窗口。而 LAC 则是迈出这一步的先行者之一。LAC 的底层架构则是以 DAG（Directed Acyclic Graph）有向无环图为基础，再通过独特的技术优化，使得 LAC 能够拥有庞大的吞吐量，TPS 在理论上能突破十万一笔，能够满足跨国移动支付的带宽要求。

3.1.1 LAC 艾尔链的 Trawl 架构

基本结构

LAC 的基础数据结构叫做 Trawl。Trawl 是基于有向非循环图的结构。它不是一种按时间序列产生、连续延伸的链式架构，而基于有向非循环图的类网结构，能够异步并行拓展的类网结构。下面是 Trawl 的基本图示。



Trawl 由单元和有向边组成。单元是独立的一个节点，能够保存各种交易数据。而有向边表示的是两个单元之间的引用关系。

绿色部分表示已经入链的节点（node），他们具有完全认证性（complete legality）。而蓝色的部分是经过部分认证（low legality）的节点。他们虽然加入了 LAC 链，但是还需要进一步认证才能确保不被剔除（Eliminate）。而灰色

部分则是即将入链的新节点(cusp ,意为尖端)。而红色的节点则是“冲突节点”（ Conflicting ），在系统多重验证之后，可能被剔除。

图中 g 节点有两条有向边分别指向了 b 和 c，则称 b 和 c 为 g 的父节点（ Father Nodes)。g 为 b、c 的子节点(Son Node)。g 对 c、b 的引用称为为直接引用。j 又引用了 g，那么 j 就通过“间接引用”链接到了 b， b 则是 j 的祖先节点（ Ancestor node ），j 为 d 的子孙节点（ Descendant node)。图中有一个特殊的节点 a 没有父节点，它就是创世节点。

3.1.2 单个节点结构

每个节点由节点头和信息体组成。节点头的信息是由多串字典构成，主要包含下面的内容：

- **{ “ 节点版本 ” ： ****** }**
- **{ “ 创建时间戳” ： ****** }**
- **{ “ 节点创建者签名 ” ： 多重创建者签名}**
- **{ “ 父节点 HASH ” ： 所引用的多个父节点}**
- **{ “ 认证人列表 ” ： 认证该节点合法的其他节点群}**

信息体部分用于储存具体的交易信息，在 LAC 支付系统中，主要是支付流水，以及结算信息。如表 3-2 所示

version	**系统版本号**
time	produce_time：交易产生时间戳 legalize_time：交易确认时间戳
	• types_of_transaction：交易类型 如果该节点记录的是跨境交易，则字典值为“Cross-border payment” ，如果该节点记录的是本地交易，则记录“local payment” 。 • Terminal_code：交易终端串码，用于识别交易双方终端。保留一定信息作交易凭证 • payment_body：交易信息主体

message	--pay_in :代表了一笔交易的输入，由数据由一串数组构成。 -txid :该交易数字货币来源节点的 hash 值，只有当这个节点被系统认可了，该交易的资金输入才有效。 -scriptSig ：解锁密匙。用于解锁 txid 所指向的节点。使得该金额能够输出。 - index : 货币来源单元的消息索引 - out_index :pay_in 该货币来源单元输出索引 --pay_out : 输出货币的信息 -outtxid: 接受节点的地址 --out_num : 货币交易数量
creators	该节点创建者的地址和签名数组
Parent_node	该节点的父节点的 hash 数组值
Certifier	认证节点的 hash 数组值
*******	*******

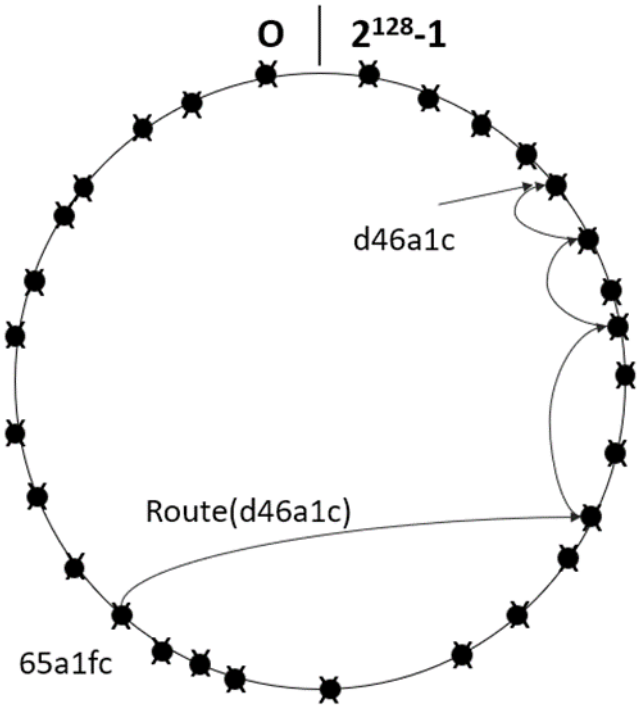
***由于跨境支付的复杂性，节点包含上述信息又不仅限于上诉信息**

3.2 基于 P2P 的 Hub 节点组织策略

p2p （peer-to-peer）点对点技术又称为对等网络技术。这种网路技术能够利用每个节点的计算能力和带宽来分散集中计算的需求，非常契合区块链分布式架构的特点。在纯 p2p 网络中，没有端（terminal）和服务器（server）的概念。每一个节点都要承担计算任务，也就是全网的计算和存储资源都分散了。信息的传输可以直接在节点之间进行，无需中间环节和服务器的参与。由于 LuxAlpa 的通信是依赖与 Hub 节点的互联，所以在组织 Hub 节点时，利用了 P2P 网络的优势，可以大幅提高通信速度，进而提升整个链的交易速度。

3.2.1 LAC 的 Hub 节点组织策略

LuxAlpa 采用的是**全分布式机构化拓扑结构**的 P2P 网络。融合了 LuxAlpa 本身的技术之后，我们构建了一套适用于 DAG 架构的 Hub 节点组织架构——“**LuxAlpa-Bloom**”。在 BLOOM 中我们使用了分布式散哈希列表 **DHT（Distributed Hash Table）**来组织我们的 Hub 节点。DHT 本质上是一个由大量广域范围内 Hub 节点共同管理维护的散列表。它被分成很多不连续的块，每个块会被分配一个属于自己的 Hub 节点。并且该 Hub 节点成为这个块的管理者。被哈希散列（Hash Function）函数加密之后，一个对象的 ID 被映射成 128 位的 HASH 串。在 LuxAlpa-Bloom 中，我们实现了一个高度容错和可拓展的 SDDS（Scalable Distribute Data Structures）集群。在这个集群中，DHT 结构能够适应 Hub 节点的动态加入和退出。而且利用重叠网络拓扑结构的确定性，DHT 能够提供精准发现。只要 Hub 节点存在于网络，DHT 总能发现它。



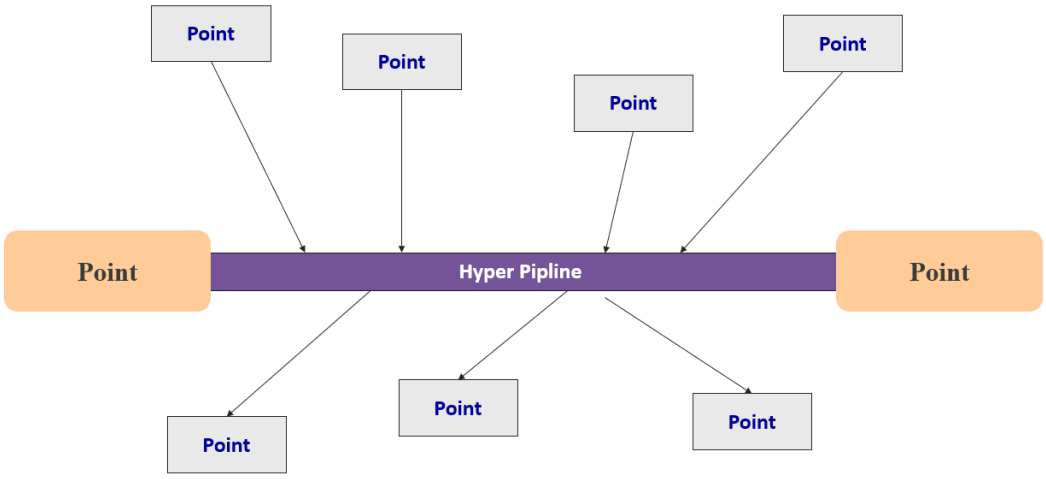
在 BLOOM 中，我们提出了一个对象定位和路由协议。通过 HASH 散列函数为每个节点分配了一个 128 位（可拓展）的标识符（nodeID）。所有的标识符构成了一个逻辑上的环形 nodeID 标签。节点 IP 地址以 HASH 的格式随机分配。

• **bloom 协议的优点**

分布式处理	将以中心计算节点为中心的服务分散到各个节点 ,避免出现中心化计算的性能瓶颈;
拓展性强	随着节点数目越来越多，bloom 的性能会不断得到提升和补充
稳定性高	局部网络出现问题不会造成大规模事故
节点自治	整个系统由节点自治，成本更低，可维护性高。
通信速度快	由 DHT 作索引，并且形成了 SDDS 结构，使得 Bloom 协议中节点查找交流速度非常快
容量高	索引地址由哈希散列生成 最低为 2^128 个，而且支持扩充。

3.2.2 基于 BLOOM 的高速支付通道

为了充分挖掘 P2P 闪电通信网络的性能 ,我们在 Bloom 中构建了叫做 **BTP**（Bloom Transaction Pipeline）交易管道的交易策略。通过 BTP，我们可以在节点之间建立点对点的高速支付通道。首先 BTP 会在交易频繁，或者交易量大的节点之间预设高速管道。当相关节点发出支付请求时，BTP 就能依托这些预设的管道济南高新多次、高频、双向的瞬间支付：



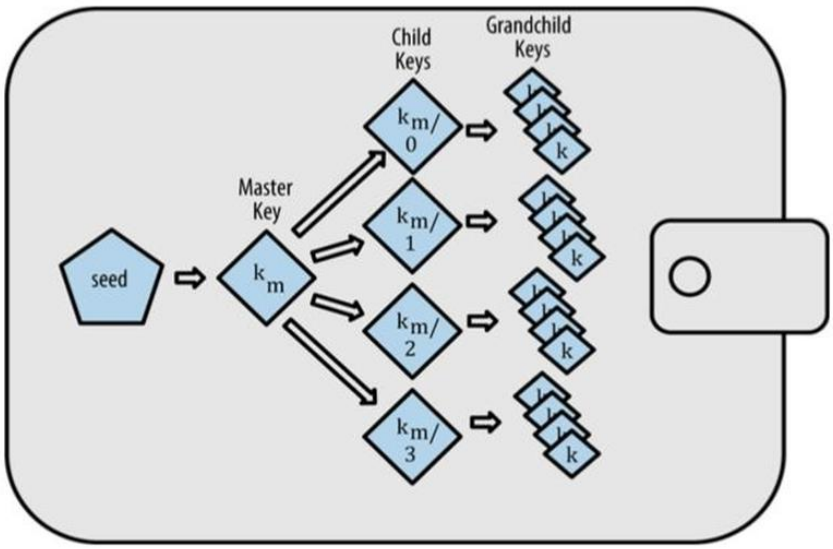
若双方之间没有直接的点对点支付通道。只要找到一条联通双方的、由多个支付通道构成的支付路径就能完成高速支付。LAC 利用 BTP 管道支付策略。可以显著地提高交易效率。

3.3 共识层

目前较为常见的共识机制如 POW，POS，DPOS 已经在各大区块链产品中得到了应用 ,但是随着区块链行业的发展 ,共识机制的许多弊端也已经暴露出来。最初的 POW 共识机制发展至今已经出现了造成了大量资源的浪费、挖矿集团的垄断等弊端，POS 共识也有着代币限于发行、节点需要长期在线等弊端。DPOS 共识机制下用户的参与积极性不高、安全性隐患等缺点。现在的区块链产品需要探求一种具有更好安全性，稳定性、公平性的共识机制。

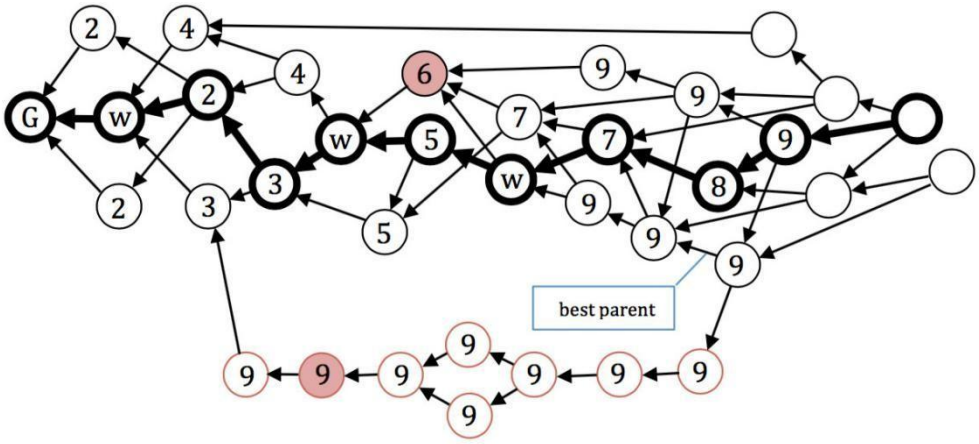
LAC 项目采用的是全新的 RPOS 共识机制。在 DAG 技术的基础上，RPOS 共识机制是随机可信拜占庭共识以及随机可信权益共识与阈值签名的结合 ,在防范双花问题上，利用 DAG 链技术特点，已经得到了很好的解决。RPOS 采用主侧链结合的多链架构体系 ,RPOS 共识机制在结合了传统共识机制的去中心化特点上，大大提高了资源利用的效率，提高了处理速度。相比于 POW 共识机制，RPOS 共识机制去除了挖矿这一需要消耗大量算力的工作 ,既保持了完全去中心化的网络，又杜绝了大量资源的浪费，在利用相对较少的算力情况下，能保持效率的极大提高。

LAC 具有类似于比特币的网络的 P2P 网络，节点在传播消息的时候，选择的节点是随机的 peer 节点。为了保证消息的准确性与真实性，原始发送者在发送之前需要利用私钥对消息进行签名 ,在其它节点进行转播之前 ,需要验证其真实性。节点对一个信息只会转发一次，以此来避免前向回环的的现象出现。钱包的地址由 LAC 节点通过随机种子生成分层确定，大大提高了钱包安全性。



3.3.1 主链

主链是可以把所有单元关联在一起的，由指定单元沿着由子单元到父单元进行回溯而形成的单链，因此从任意一个顶点开始都可以构建一条主链。两个不同的节点以相同的规则进行回溯的时候，如果在某一部分相交，那么在之后将会完全重合，而重合的这一部分就叫做稳定主链。在最极端的情况下，便是在创世单元上相交，因此，两个无序单元之间，总存在一部分的稳定主链，通过稳定主链，便能在这两个单元之间建立总序。



稳定主链的结构如图所示。为每一个位于稳定主链上的单元建立索引，建立索引的规则是，从创世单元为 0，其子单元为 1，以此类推的规则。对于不在稳定主链上的单元，索引采用的是第一个直接或间接引用该单元的稳定主链单元的索引。

因此每一个单元都拥有了一个主链索引，主链索引数较小的被认为是较早创立的单元。在主链索引相同的时候，便会比较单元的哈希值，哈希值较小的单元

则被认为有效。主链构建的过程本质是最优父单元选择的递归调用。在参与共识机制的时候，需要选择出公证单元，公正单元由见证人发出。见证人既可以是非匿名长期参与社区运营并拥有良好信誉的人，也可以是维护网络健康的组织。见证人虽然被认为是诚实守信的，但是仅仅选一个见证人显然是不合理的，因此见证人可以由多个。

3.3.1.1 随机可信拜占庭共识

随机可信拜占庭共识是 RPOS 主链采用的共识机制。随机可信拜占庭共识是基于 VRF 函数与改进拜占庭算法共识机制。通过 VRF 函数选取共识节点组，再利用拜占庭算法保证工作节点的公证性。主链采用随机可信拜占庭共识，可以极大提高资源的利用率，以及交易速度，在与 POW 同等完全级别下，在完全去中心化网络下，利用 POW 所需 1%的算力，即可提升 1000 倍 的性能，目前 TPS 可达 10 万笔每秒，确认交易的时间已经提升到了两秒以内。

①VRF 函数

VRF 函数即 Verifiable Random Function，可证随机函数。该函数可通过协议给定的随机数利用哈希算法得出一个可以被公众用户验证的结果，该结果用于验证交易数据的合法性。由于传统的非对称加密算法在通过哈希函数时生成的结果在验证时需要用户提供交易私钥，这在一定程度上降低了交易区块数据的安全性，VRF 函数在利用哈希函数的基础上，消除了验证结果需要利用私钥这一条件。通过 VRF 函数生成验证结果的步骤如下：

- 利用给定的随机数与某种标志变量相结合。标志变量可以是代表轮次等意义的变量。这里的随机数一般为前一个区块产生时通过全网去中心化的算法生成的随机数，而最初的随机数由协议提供。
- 将结合后的数字组合使用私钥进行数字签名，生成后的数字此处称作 info。此处私钥（sk）是交易区块产生时通过哈希算法得出的非堆成加密密钥，数字签名保证交易与最后生成验证结果的匹配性。
- 通过哈希算法，将进行数字签名过后的一串随机数字进行哈希映射，生成具有某一固定位数的验证结果 result。
- 通过另一函数再次将数字签名后的随机数字进行映射，得到验证结果所需的 proof。此处 proof 是作为私钥替代品的形式出现的，由于 proof 是由私钥和随机数字映射得来，因此可以保证 proof 的唯一性。

- 在生成 result 与 proof 之后，验证节点利用特定的函数验证能否由私钥生成的 proof 映射到 result。若不能，则该 proof 无法验证成功；若能，则进入下一步。
- 之后只需要计算节点将随机数 info 与交易公钥即 pk 提供给验证节点，验证节点通过特定算法验证 pk,proof,result 是否匹配，若匹配，则操作成功；反之，则不成功。

通过上述流程可以得出，通过 VRF 函数生成的验证结果既避免了用户提供私钥的调节，也提高了验证结果的安全性，降低了结果的可操纵性。

共识机制在进行新一轮共识节点组选举的时候，通过 VRF 函数生成验证结果之后进行广播，用户在收到广播之后将得到的返回值再次进行哈希映射。若得到的映射值处于协议给定的返回当中，用户便可以判断出自己被选作共识节点，并参与之后的交易区块的生成打包。由于被选作共识节点的用户是通过接受广播的返回值，并自己通过哈希映射与自己所持有的私钥来进行判断自己是否成为共识节点，因此在不进行广播的情况下，哪些节点被选作共识节点无法被互相知晓，这在一定程度上保证了共识节点选举的公平性。

② 拜占庭算法

在共识节点选取成功之后，共识节点组利用阈值签名的方法达成对区块生成的共识。针对一个共识节点组，组内会根据哈希算法生成一队组私钥和组公钥。每一个节点都会拥有按节点个数均分的组私钥片，用于对区块进行签名，而组公钥则用于对由该组产生的区块进行验证。对于特定的共识节点组，系统按照一定比例预设相应数目的阈值。在进行打包一个区块时，需要参与的节点进行数字签名，而进行数字签名则需要节点拥有的组私钥片。只有当组私钥片的个数达到预设的阈值时，数字签名才能完成，此时达成共识。在打包完成之后，通过一定的算法，发送区块并向全网进行广播。

其他拥有组公钥的节点可以利用一定的函数对该区块进行验证，验证该区块是否由本组打包并发送。在验证该区块属于本组打包并发送之后，想解锁该区块，查看进一步的信息时，依旧需要一定量的节点利用私钥片进行数字签名，完成即可打开。

该拜占庭算法利用阈值签名的特点，保证了在少数节点故障的情况下，依旧能进行数字区块的打包，并且在少数节点试图对非法区块进行数字签名时，因为数量的不足而无法完成数字签名，从而防止了少数节点的恶意操作。

3.3.2 随机可信权益共识

RPOS 侧链采用的是随机可信权益共识，由于侧链的所需交易并发量低于主链，因此采用这种少量节点完成出块操作的共识。相比与 POW 的交易量及交易速度，该种共识方式依然有着较大的提升幅度，目前 TPS 已经达到了 3 万笔每秒，交易确认时间在 5 秒以内。

该共识机制依旧是利用 VRF 函数进行共识节点组的选取，每一个共识节点组会生成一对组私钥和组公钥，在需要进行区块的打包生成时，需要在共识节点组里选出出块节点。出块节点的选取，需要节点根据自己的私钥利用哈希映射出随机数，随机数最小的即为出块节点。出块节点完成打包出块的工作，其余节点作为见证节点，完成对区块的数字签名。签名完成之后，发送到全网，并进行广播。同时，各节点也可以利用组公钥对交易区块进行验证，要查看区块信息，需要一定数量的组私钥片。

相比于 POW 共识机制，RPOS 共识机制去除了挖矿这一需要消耗大量算力的工作，既保持了完全去中心化的网络，又杜绝了大量资源的浪费，在利用相对较少的算力情况下，能保持效率的极大提高。

3.3.3 交易确认

在新单元创立时，每一个节点会回溯自身的当前主链，因为当前所有的不存在子单元的单元都有可能以此构造新单元。由于非稳定主链上的单元会不同，不同节点回溯的主链也可能会不同。然而，随着新单元的产生，存在时间足够长的稳定主链会保持不变。

随着时间推移，未来节点进行主链回溯时，所有的主链将会汇集于某个单元，这个单元及之前的单元都是稳定单元，不会再因为新单元的产生而发生变化。因此，创世单元必然是一个稳定节点。若是基于当前的非稳定节点集合构造一条当前主链，并且该主链上存在一些之前已认定稳定的节点，未来的主链都会在这些点或早于这些点汇集，然后就是相同部分的稳定主链。存在一种方法，把这个稳定点向远离创世单元的方向推进，就可以根据数学归纳法证明这个稳定点存在。而被这个稳定点所引用的单元将获得确定的 MCI，包含在这些单元中的所有消息也将被确认。

3.4 基于 IPFS 的分布式存储

在 LAC 中我们的数据储存采用了 IPFS（InterPlanetary File System）协议。IPFS 是一种全新的文件协议，与传统的 HTTP 协议完全不同。HTTP 协议使用域名来映射数据。这种数据处理方式高度依赖中心服务器，稳定性得不到保障，还存在数据大量丢失的风险。同时，依赖于 HTTP 多的传统的数据存储方案成本相对高。

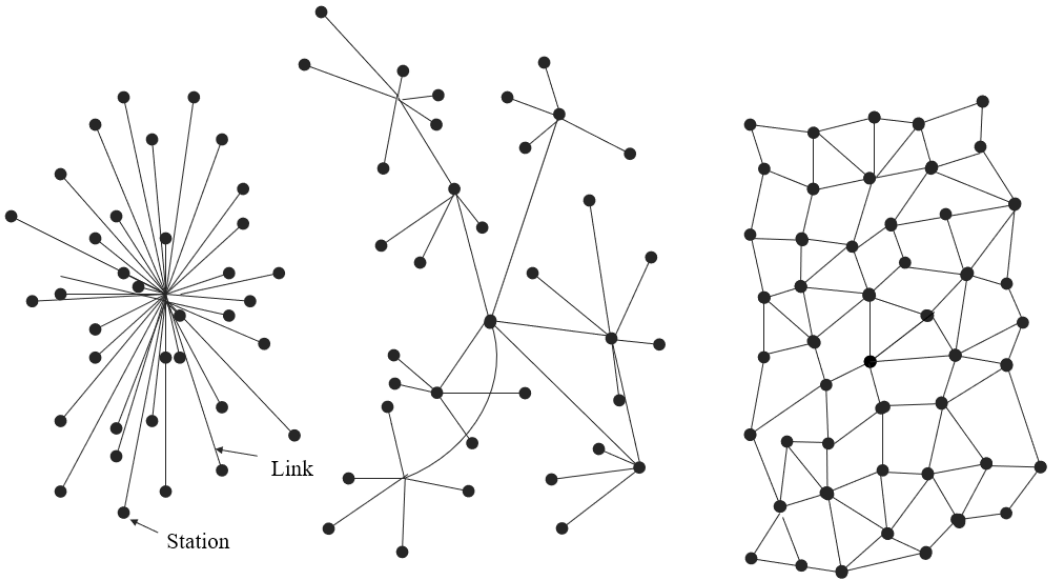
IPFS 本质上是一种内容可寻址、版本化、点对点超媒体的分布式存储、传输协议。同样作为超文本协议，它却比 HTTP 更快、更安全、更自由。IPFS 的内容寻址会通过唯一标识访问数据，可以提前知道这个标识是否重复，如果该数据已经被存储过，IPFS 就能从其他节点直接读取所需的相同的数据，节约了时间和空间。

3.4.1 LAC 的 T-IPFS 协议

在 Filecoin 的 IPFS 基础上，我们融入 LAC 的技术特点，形成了一套适合 LAC 的分布式存储协议 T-IPFS。

在 T-IPFS 中，我们利用 Mutiformats 算法集来对文件进行 HASH 加密和描述。（它包含 SHA1\SHA256 \SHA512\Blake3B 等主流的 HASH 算法。每一类算法生成的 HASH 串都有各自的数据特点，我们可以根据 HASH 码，看出是执行了哪一类算法。)每一个超文本的文件在 Mutiformats 的作用下会生成一串独一无二的 nodeID，以及 hash 指纹。而这个 nodeID 的作用就相当于 HTTP 中的 IP 地址，T-IPFS 就根据这些 nodeID 来存储数据和寻址。

其实在形成 nodeID 之前，T-IPFS 会对数据进行分片处理。将大的数据块切分成适当的大小（如：1M），再进行后续处理。一个超文本数据集中有效数据其实不多。根据 T-IPFS 的内容描述算法，冗余的数据就生成一串相同的 hash 值。再进行存储时有效数据占比可以提升很多。大大节约带宽和空间。



数据分片处理后，T-IPFS 将用 LAC 借用中的 bloom 协议，进行 P2P 的分布式存储。之后，每个节点既成为资源使用者，也可以是资源提供者。有节点当发起数据请求之后 ,系统根据 nodeID 寻址 ,将数据分片拼凑成一份完整的数据。这种分布式存储方式提高了效率，降低成本。

3.4.2 T-IPFS 协议栈

nodeID	S/Kademlia 生成 对等节点省份信息生成
Network	任意传输层协议 ICE NET & NAT 穿透
routing	DSHT -分散式松散 hash 列表 定位对等点和存储对象需要的信息
switch	管理区块分布
object	Merkle-DAG 内容寻址的不可篡改、去冗余对象链接
file	文件版本管理系统 类似 Git

name	自我认证 SFS（self-Certified Filesystems） DAG 命名对象可变
application	在 IPFS 上运行应用利用附近节点， 提升效率，降低成本

八个层面的子协议栈，相互协同，共同支持整个 T-IPFS 协议

在整个栈中，通过 Kademlia 算法我们可以生成对等信息节点，并且制定出路由(routing)规则。同时，Distributed Hash Table （DHT）也是由 KAD 协议构建。每个加入 DHT-HASH 散列表的节点都要生成自己的 ID 信息。系统根据每个不同的 ID 存储网络中的数据，并与其他节点建立联系通道。

在 Network 层，T-IPFS 使用了 LibP2P 以支持任意传输层协议，实现 ICE NET&NAT 穿透，使得重要信息在调用时能够在网络间极速传输。

switch 协议层里部署了部分中心服务器，使得系统可以将相同的资源请求形成集群 **swarm**，而不是单个处理，使得数据请求效率大大提高。

在 file 协议中，T-IPFS 使用了类似于 Git 版本的控制文件系统，使得每个节点能保存不同版本的所有数据。保障了数据的可追溯性和永久保留。

object 协议保证大多数数据都是以 MerkleGag 的结构存在。这种结构可以提升内容寻址的效率，并且高效去重。

name 层协议是指，在用户获取对象时，使用 HASH 指纹进行验证。检查其公钥和 Nodeld 是否匹配。在确定了用户真实与否的情况下，也得到了可变状态。加入了 IPNS 之后，可读性也增强了。

最后的 **application 协议**允许 LAC 的应用在成本很低的带宽下获得数据，从而提高整个系统的效率。

3.4.3 T-IPFS 切分结构化数据

在 LAC 支付系统中，支付信息都是结构化的数据。包含交易号，交易双方信息，交易金额等结构规律的数据。于是我们就可以在 T-IPFS 中利用数据分片技术，将数据切分为单个字段。在传统的数据处理方案中，这些包含交易信息的数据字段会被打包在一起，存储在中心服务器上。这中集中储存的方式既不利于

数据安全，也不利于防止数据丢失。

而在 T-IPFS 中，我们将这些相关的字段分发到不同的节点当中。形成多个子 HASH 串。利用分布式存储的特点，加强数据安全。在需要取用数据时，T-IPFS 根据子 HASH 串进行索引，将数据分片拼接成完整的交易数据。

3.5 交易匿名保护

在数字货币的交易中，匿名交易和隐私保护是非常重要的，这也是数字货币的重要特性之一。

在大多数区块链系统中，隔断交易地址和持有人身份的联系是保护交易匿名的主要手段。但是这种方式在大数据技术下显得捉襟见肘。通过跟踪区块链信息，大量收集地址 ID、IP，进行大数据分析。在一定程度上可以在交易与持有人之间建立映射关系。所以 LAC 使用改变了思路，开始从交易的无关联性（Unlinkability）和不可追踪性(Untraceability)对交易进行保护。

LAC 主要运用了零知识证明（zero-knowledge proof）和零币、零钞协议（zero-cash protocol）来对交易匿名性作保障，能够提供完全隐私化和加密化的虚拟货币转账

3.5.1 基于零知识证明的——Tzks 协议

零知识证明（Zero-Knowledge Proof）是由 S.Goldwasser、S.Micali 以及 C.Rackoff 在 20 世纪 80 年代初提出的。它指的是证明者（被验证者）能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

在 LAC 中我们借鉴了 Hawk 中的 zksnake 构建了适合于 LAC 的一套基于零知识证明的匿名协议——**Tzks** 。我们以示证者（prover）向验证者(verifier)证明，他知道有两个数使 a 和 b 使得 a+b = 9，在证明过程中示证者（prover）不能透露 a 和 b 的值。

我们会选择一个特殊的加密函数 Q(x)，它有如下性质：

- 单射函数，且函数单调。变量不同函数值不同
- 逆向困难，从函数值反推自变量困难
- 给定 Q(a) Q(b) 我们可以计算出某些关联函数值

验证过程：

- 通过随机函数，验证者(verifier)通过随机点 s 产生随机函数 k，并且发送加密函数值数组**[Q(1), Q(s), Q(s2), ..., Q(sd)], [Q(k), Q(ks), Q(ks2), ..., Q(ksd)]**
- 示证者产生一个偏移多项式 R(x)，然后根据验证者的加密函数值数组计算出**Q(P(s)+R(s))、Q(kP(s)+kR(s))**发送给验证者。
- 验证者(verifier)验证接受到函数值 E(P(s)+R(s))是否满足应有的性质。并且验证收到的另一个函数值是不是 E(kP(s)+kR(s))

在 Tzks 中，我们在系统中会预制一个信息称为 Common Reference，验证者发送给示证者的信息跟据这个不变量生成，不需要再向示证者发送其他信息。并且后面的验证过程也可以重复使用 Common Reference 参数。

然后为了使随机点 s 和随机参数 k 保密 ,我们在 Tzks 中设置了 **String**(CSR，共同参考字符串)。CSR 实质上为 s 和 k 的加密值数组。CSR 明文则由特殊形式保护。

使用 Tzks 协议之后 LAC 能够使得示证者(prover)和验证者(verifier)之间不需要交换过多的信息，保障了匿名性。同时验证过程只需要少量计算即可完成，这种少量信息交换节省了验证工作计算量，并且为通信层节约了大量成本。

3.5.2 零币零钞协议

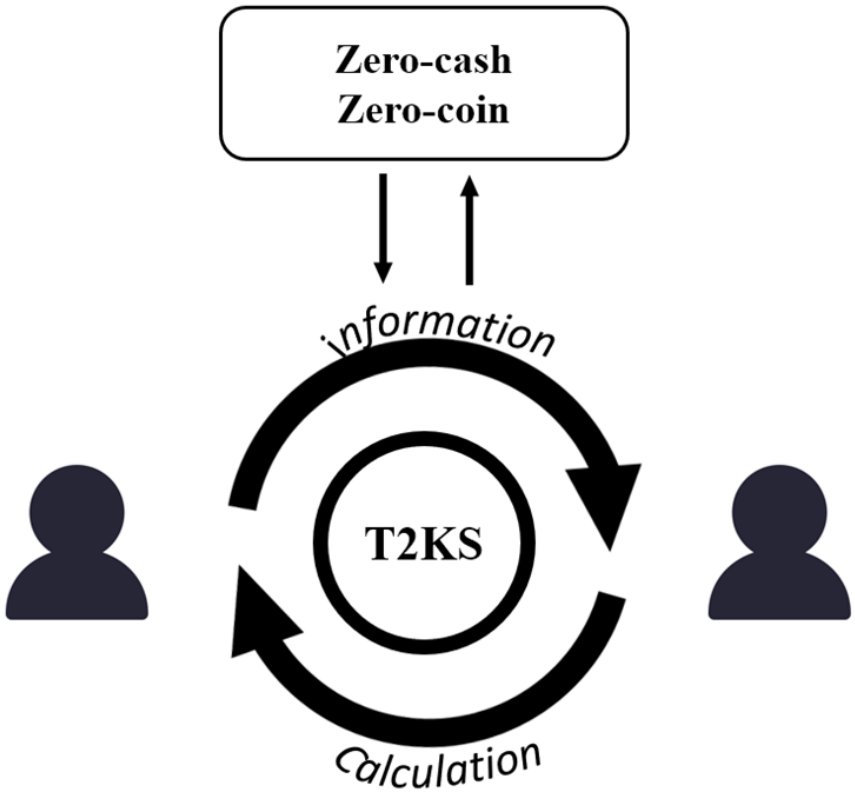
零币协议（zero-coin）是指零知识验证用于零币铸造和赎回过程，可以隐藏交易双方的信息；

零钞协议（zero-cash）可以将交易中的验证内容转换成多项式乘积，并且在隐藏交易金额的同时验证交易。

所以采用零币零钞协议之后，在验证交易过程中，可以隐藏交易金额，唯一公开的交易信息就是“交易存在与否”

在验证时，首先需要把验证过程分成一个个的验证步骤，并且将步骤再分解转化为包含简单运算的算法电路。算法电路再经过数字化转化为多项式乘积如：$g(x)h(x) = z(x)y(x)$ ；

当验证结果正确时，等式成立。在这个过程中验证者会选择检查点，来查看当前等式是否成立。同时 LAC 会加入动态加密算法，保障第三方验证者无法得出等式的实际输出值。在过程最后，多项式的两边同时乘上保密参数 M，以隐藏 $g(x)h(x) = z(x)y(x)$中各式的具体数值。



LAC 的交易匿名处理

LAC 艾尔链采用了基于零知识证明的 Tzsk 协议和零币零钞证明后，我们就可以在保证效率的情况下，证明交易过程的完备性，交易双方的真实性，交易的合法性。并且在整个过程中充分实现匿名交易。

3.6 智能合约账户与交易

智能合约是一种通过信息化方式被传递，验证以及执行的计算机协议，智能合约是信息化时代的产物。相比于传统合约，智能合约具有更高的有效性以及可执行性。基于区块链技术的信息存储具有分布式存储，不可篡改，可追溯等特点，正是这些特点，才让区块链环境下的智能合约有了更好的发挥空间。在 LAC 项目中，基于 DAG 技术的区块链提高了打包交易区块的速度，为智能合约部署速率的提高打下了基础。

3.6.1 智能合约的账户

类似于以太坊，本平台拥有两种账户：外部账户和合约账户。外部账户是用户拥有的较为固定的账户，该类账户通过私钥进行控制，在智能合约中主要进行消息的发送及合约的部署。合约账户是在部署智能合约时生成的，由部署合约的代码进行控制，一般将合约的地址作为区块的合约账户。在交易进行的时候，通常需要外部账户对合约账户发出一系列操作指令，这样合约账户才能进行一系列的操作。

项目平台为智能合约提供储存及运行的底层环境，外部账户拥有着可以通过项目平台提供的客户端进行智能合约代码的实现，目前市面上主流的语言系统如C++，java 等语言均能进行代码的撰写。对于常用的智能合约及较为简单的合约，我们会提供相应的代码模板，账户只需要提供相应的数据之后，再进行编译，便能进行合约部署。

合约账户与一份份智能合约相匹配，由存储在区块链上的代码数据控制，在接收到来自外部账户的消息之后，开始进行一系列的操作，合约便开始在平台中运行。

3.6.2 智能合约的部署与交易

外部账户进行代码实现之后，由客户端进行编译，之后需要将编译后的合约打包发送至区块链。区块链上的工作节点在接收到信息之后，运用共识机制将信息存储至区块链之中，只有当合约成功上链之后，才算部署成功，之后的合约才能有效执行。合约部署成功之后，当满足触发条件之后便会自动执行。

在智能合约执行的过程中需要注意的是，合约的内容如果由双方共同签订，只有在双方账户都同意并提供各自的私钥的情况下，才能进行合约的修改，即合约中的双方并不能单方面的实现合约的修改，并且在满足触发条件时，便会自动触发，不需要合约双方进行再次操作。若是一方账户想提前履约，便需要发送消息至合约账户，进行一系列操作，当履约程度满足了双方合约中所确定的条件，智能合约将视为交易完成，并自动生成交易数据出块，并向全网广播，此时交易数据由全网共同见证，完成分布式存储，并不再被篡改。

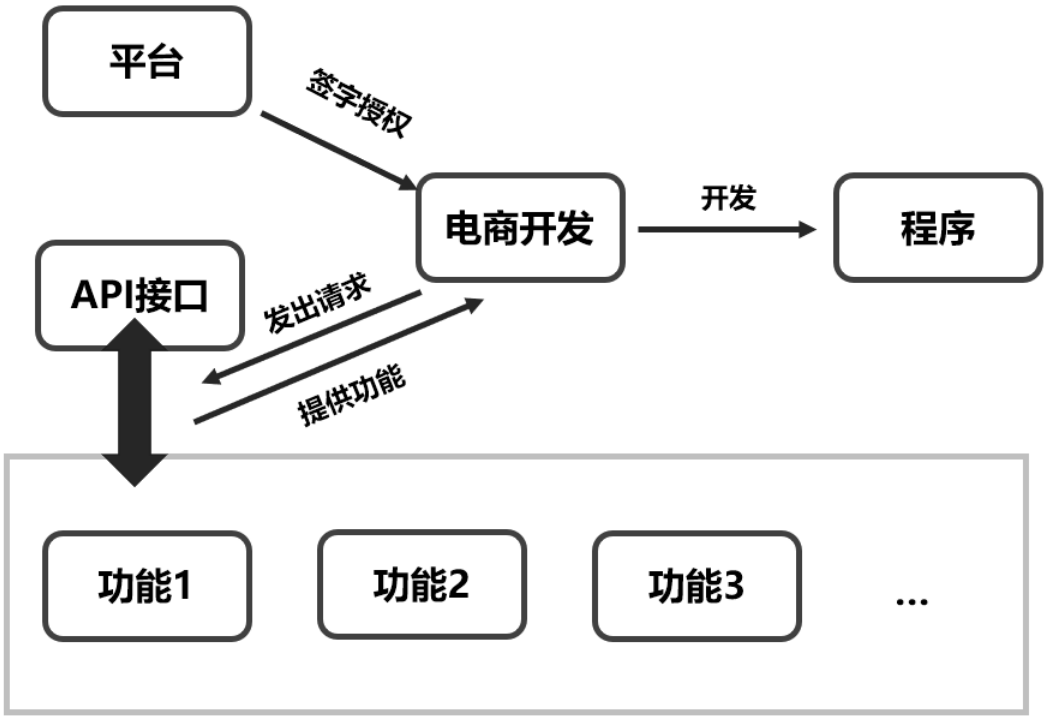
智能合约的部署和交易需要耗费一定的算力，平台将根据所耗算力的多少进行服务费的收取。在本平台中，服务手续费的收取主要是两个依据，一是完成交易时交易中所含的数据字节数，二是根据交易过程中程序被执行的次数所决定。若交易为一次性打包出块完成，便根据交易数据大小收取一定量的代币费用，若交易分为多次执行，则每次执行都会根据程序的复杂程度进行收费，即一个交易很可能进行多次收费。因此在进行智能合约的部署时，为防止所需手续费不足导

致合约中断，应该预存一定量的代币用于合约的执行。

3.7 API 接口

API 接口即 Application Program Interface,应用程序接口，是为开发程序的人员提供的访问一组例程的接口，API 可实现在程序员不必知道其源代码的情况下进行功能的调用。LAC 项目打造的 API 项目接口将为各电商开发人员提供便利的模块化程序，以提高开发人员的效率，使程序更加便于维护。

3.7.1 模块化功能



一个程序系统是由许多个复杂的函数组合而成的，而根据功能将这些函数进行分组则能很大程度上降低开发难度。LAC 项目程序开发客户端将创建类似于函数库的程序组，该程序组包含上千种副程序，该副程序是以模块化形式存在，即实现某种功能的代码已经被封装，只需要通过调用副程序便能实现常用功能。该程序组为各大电商平台开发人员提供能够访问 API 接口的权限，通过 API 接口，他们将能够直接使用其中预存的功能函数，而不必知道源代码以及其中工作的细节。由于开发者不必再重复性的对某种常用功能进行代码的实现，这将大大

提高开发人员的效率，降低开发的难度。而将程序组内各个程序模块化，将使得当程序出现 BUG 时，维护起来更加的便捷。

3.7.2 电商信息接入

在与各大电商平台签订协议的同时，平台将允许电商平台创建程序以构造各自的应用平台，与此同时，各大电商平台将认可本平台发行的代币。本平台代币将成为可以进行跨国交易的代币，具体的代币汇率将根据市值进行变化。电商信息上链之后，可以通过授权 API 自主开发应用程序，拥有自己的个性化电商平台。基于 DAG 主链的区块链结合了区块链 4.0 的特点，为电商信息的保护提供了有效的保障。

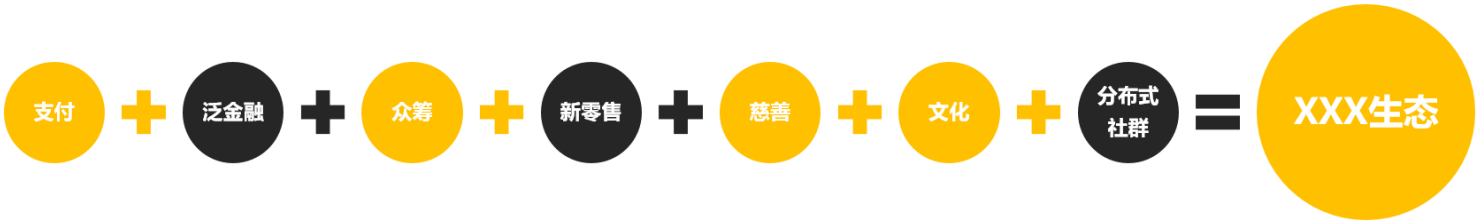
电商信息接入之后，便可以通过平台进行商品的交易。每一笔交易的进行依旧需要工作节点对交易数据进行打包出块，而依据打包出块交易的数据大小，我们将收取一定的手续费用。

3.7.3 运营与维护

随着区块链技术的发展，API 接口所连接的程序组也应该进行不断的维护与更新。为使更多的区块链爱好者投身于区块链的发展当中，平台将建立单向的程序组维护客户端。在这个客户端里，具有一定代码基础的区块链爱好者可以根据自己对区块链的理解，进行程序组里的副程序的编写，通过这个平台进行模拟测试。根据测试结果为我们提供有效的建议将会受到相应程度的奖励。

同时，平台将会由专业的团队定期对 API 接口的安全性进行检查，防止非法节点通过 API 节点进入程序组存储空间篡改程序组，导致开发应用出现故障。程序组的更新与维护也将由专业团队进行。

四、LAC 生态

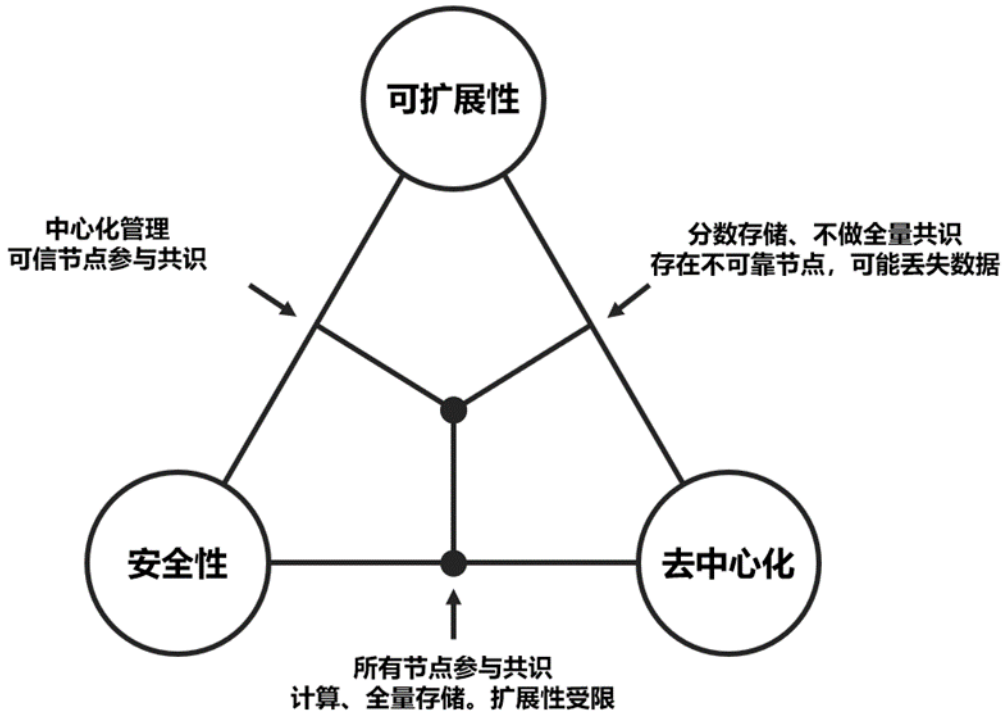


4.1 数字货币支付生态

4.1.1 传统支付存在的问题

自数字货币诞生以来，支付领域便被认为是数字货币与传统金融的主战场，是同时最能够发挥数字货币自身“货币”功能的领域。无论是现金、刷卡还是电子支付，传统支付领域都存在各自的问题。例如，现金支付只能适用于数额较小的交易，且完全不能满足目前电子支付的需要。同时，我们也看到电子支付，特别是现在使用最为广泛的手机扫码支付，存在种种安全隐患，并且支付门槛相对较低，人人都可以参与。二维码容易造假，并且很多商贩都有自己的二维码，假如二维码被偷换了，很容易造成用户财产损失。电子支付模式引入了支付宝、微信等大型第三方机构，极大地对支付效率进行了提高，也建立了用户的对支付渠道的信任。然而中心化的支付方式存在自己的显著问题，一是中心化的服务器容易瘫痪，并且需要持续投入人力物力进行长期维护工作，对社会资源和自然资源造成了巨大的浪费；中心化服务器无法避免人为作恶或者错误操作产生的严重后果，用户账户的安全性与消费行为的安全无法完全得到保障。

针对传统支付出现的乱象，我们需要寻找一个方案来解决。数字货币基于区块链技术，具有去中心化、匿名性等优势，可以保证支付安全透明，点对点交易，交易速度快。但是目前单纯使用区块链支付也存在自己的问题。去中心化(Decentralization)，安全性(Security)和可扩展性(Scalability)这三个属性，区块链系统无法同时满足，最多只能三选其二。



这就是区块链的“三角悖论”——在保证去中心化和安全性的前提下，无法大幅度的提高扩展性，导致难以商业化运用(如下如所示)。在区块链中交易时，不同的交易按序列排好等待，只有当上一个用户完成交易后下一个交易才能开始行动，通过这样的方式来保证整个区块链的一致性和贯彻性。但也严重影响了网络的通畅性。

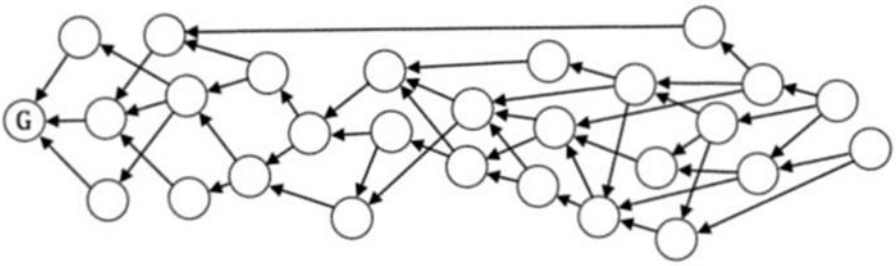
对于支付这一与个人生活和财产安全息息相关的特殊领域而言，安全性是其一切功能的基础，去中心化是区块链金融的本质属性和愿景使命，可拓展性决定了支付的适用领域和承载能力。区块链要实际应用，要真正深入我们的实际生活，切入万亿级的消费市场，就必须解决“三角悖论”的问题。以比特币为例，在闪电网络落地之前，比特币每秒只能处理 7-8 笔交易，完全无法满足商用需要。即使是区块链 2.0 的以太坊，网络拥堵和拓展性较差也已经是它的顽疾，网络升级失败，分片技术无法实现完整应用也为以太坊的未来蒙上了一层阴影。

4.1.2 DAG 技术与创新支付

而 DAG 技术在理论状态下（在网络足够稳定而且强大的前提下）可以将去中心化、安全性和可拓展性完美结合。采用 DAG 技术的分布式数据库，起步就可以把 TPS 做到 10 万+，还能把交易费用做到极低。

出于加快交易处理速率的考虑，节省用户在等待交易时耗费的时间，DAG 的设计能实现这样性能的优化。对于等待交易的用户，LAC 不考虑他们的他们的交

易类型，不再进行分类，使他们分成不同的队列等待，而是加速去为他们处理交易。如果发生交易冲突，LAC 链会先记录在案，在处理完所有用户的交易后再对出现的冲突进行处置，从整体上加快整批用户的交易速率。LAC 通过这样的安排来取代传统排序方式的区块链，并在支付时使用。

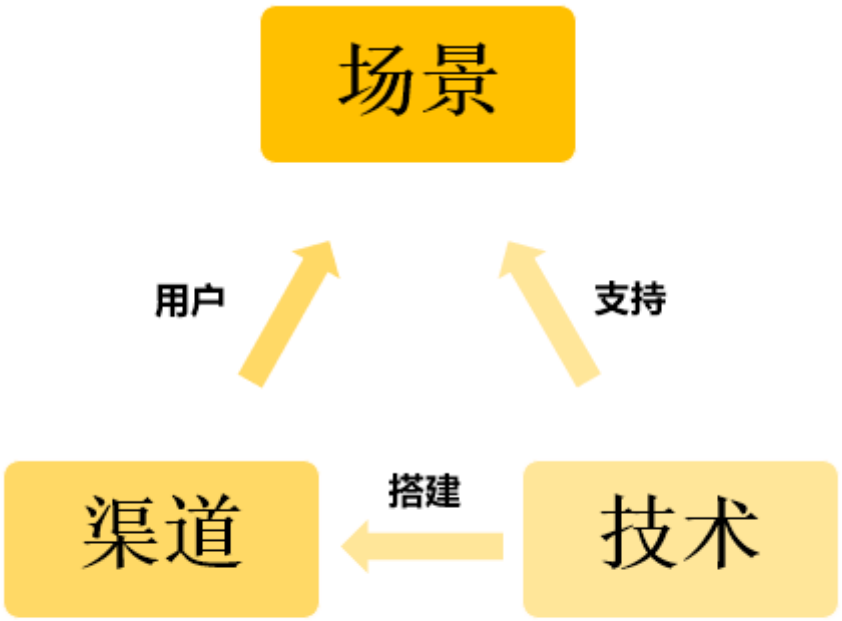


除了 DAG 技术，主链也将会是 LAC 的支付功能的重要保证。LAC 艾尔链是完全去中心化的，LAC 技术保证了高 TPS，低交易费用和高扩展性。有向无环图技术和主链技术从两个角度全力保障支付的高效、安全和便捷。LAC 的主链将会为支付和 Dapp 铺平道路，为 LAC 带来强大的后劲。

毫不夸张地说，基于 DAG 技术的 LAC 是一条完美的支付链，在 LAC 链的背后，是万亿级的支付市场和新一轮的支付革命。

4.1.3 LAC 的支付生态

除了技术上的巨大革新，LAC 要颠覆支付模式必须依托巨大得到用户群体。消费者在 LAC 的电商平台下单商品之后，将会直接使用 LAC 支付，收获信息上链后电商会立即收到 LAC 通证。LAC 通证可以实现线上线下支付的联动，线上支付与线下支付相结合，为用户提供更加完善的服务。



LAC艾尔链支付生态

4.1.3.1 支付激励模式

使用 LAC 支付的用户，可以获得相应的一定额度的积分奖励，积分除了是 LAC 的权益凭证。使用 LAC 交易的数额越大，获得积分奖励越多。与众多网络电商平台相似，积分可以用来消费抽奖、购买优惠券、抵扣消费金额、兑换消费奖品、参加线下活动。除了 LAC 链上的众多电商平台，LAC 也将与连锁便利店、电影院、餐厅等消费场景展开广泛的合作和联动。

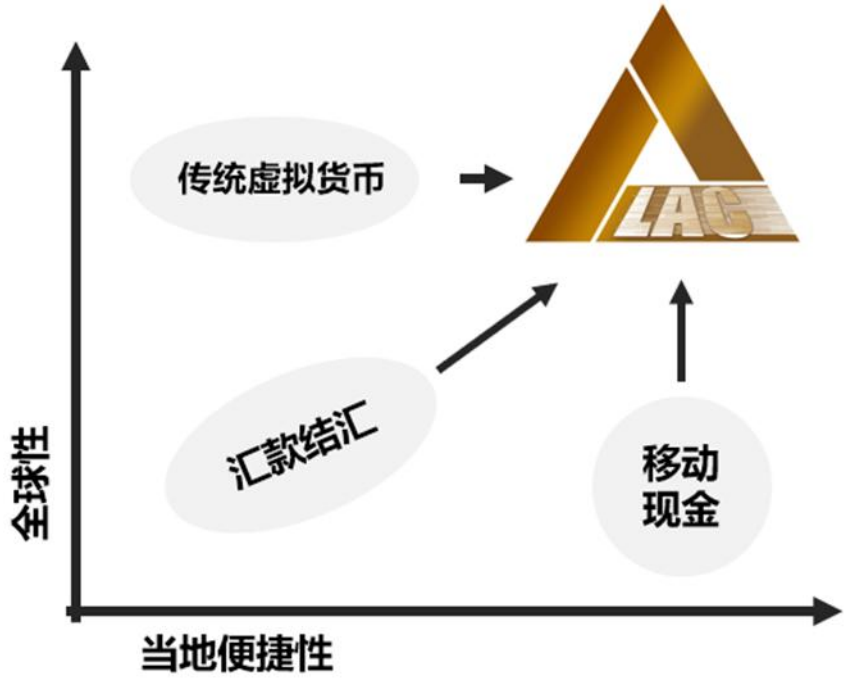
除了使用 LAC 支付，为了鼓励用户使用 LAC 消费，提高 LAC 的流通量和流通程度，用户将法币兑换为 LAC，在跨平台使用 LAC 支付时都将获得一定的积分奖励。

4.1.3.2 跨境支付

跨境支付时数字货币去中心化应用的重要领域。在目前国际金融以国家中心化的大背景下，交易费用高，交易限制多，交易时间长，交易效率低下，让跨境支付理论上与境内支付无异。支付只需要知道对方的地址即可完成，相比目前中心化金融机构，交易手续费用大大下降，交易时间大大缩短。真正实现区块链去除中间环节的作用。

随着跨国电商平台的发展，支付不局限在一国之内，跨国支付功能的不完善逐渐显现。全球每年通过银行进行的跨境支付交易超过 100 亿笔，规模超过 25 万亿，各国之间由于汇率不同，支付结算的手续特别繁琐，一笔跨境支付交易通常需至少 24 小时才能完成，且手续费高昂，平均每个汇款人所承担的手续费率达 7.68%，严重影响了国际电商的发展。

跨境支付时数字货币去中心化应用的重要领域。数字货币支付只需要知道对方的地址即可完成，相比目前中心化金融机构，交易手续费用大大下降，交易时间大大缩短。真正实现区块链去除中间环节的作用。当使用数字货币支付时，跨境支付与境内支付无异。



用户出境旅游时，只要当地有网络即可实现 LAC 的实时兑换，省去了换汇的环节，不必在身上携带大数额的法币，让旅游过程更加轻松、安全。

4.2 国际电商生态

4.2.1 国际电商

4.2.1.1 国际零售电商行业现状

2017 年，全球零售电子商务销售额达到 2.3 万亿美元，同比增长 24.8%。

2021 年，电商零售收入预计增长至 4.88 万亿美元。2017 年全球排名前三的网店收入达 1000 亿美元。全球已有七个国家网购用户数量过亿，预计未来亚洲地区网购人数将占全球一半，而从增长速度上来看，未来几年用户增长速度最快的将是中东和非洲。

国际零售电商市场在快速增长的同时也面临着一系列的转型，表现为从粗放式扩张转向精细化发展、从边界明显转向无界化态势、从发达地区转向新兴市场、从资源驱动转向技术驱动。

4.2.2 LAC 艾尔链重构国际电商格局

4.2.2.1 数据存储安全性

国际电商在推动全球经济一体化，促进零售业发展的同时，也面临着与日俱增的交易数据以及海量的个人信息、支付信息所带来的风险。传统电商是中心化的，所有数据都存储在中心化的服务器里，存在黑客入侵系统的风险，运营商也可能会不经用户同意就擅自盗用信息，用户的隐私难以保护。

艾尔链上的电商交易数据都将会进行去中心化储存，并且在落地商用之前将会进行严格的代码审计，确保代码的安全性。未经用户同意，用户的隐私数据将会进行非对称加密，确保用户个人隐私不被泄露。

4.2.2.2 电商平台信用体系

电商平台在发展过程中注重网站建设和在线支付等硬件因素，但是对于背后的信用体系等软件因素的关注却不够，虽然很多大型电商建立了信用评价制度和信用体系，但是一些信用问题，例如刷单、交易评价盗用、产品图盗用等问题却频频出现，电商平台尚未形成完善的信用体系。信用体系天生的行业特性导致了信息库的分隔，缺乏第三方评级机构，在一定程度上阻碍了电商平台的发展。

艾尔链将会最大程度地发挥区块链去中介化的作用。利用智能合约解决消费者、电商平台和商家之间缺乏信任的问题。不需要第三方的信任背书即可建立交易信任。另一方面，刷单、评价盗用等问题也将影响商家的信任评分。

4.2.2.3 制度规定缺乏

国际电商在迅速的扩张，但是配套的法律法规并未跟上步伐。电商中的刷单、刷好评、恶意差评行为层出不穷，却难以被界定是否违规。因为不同的案例根据不同量级，不同性质难以定性。海量数据归属权难以界定，用户作为数据的拥有者，却没有享受到数据所带来的收益。

艾尔链将联合链上电商进行行业自律，制定行业标准，重新塑造和改善电商行业的经营环境，从制度层面解决电商平台的困局。

4.2.2.4 提高交易过程透明度

传统国际电商的交易透明度较差，影响了用户与商户之间，用户与用户之间的信任程度。而对于零售电商平台而言，商家愿意为消费者的分享付费，消费者也愿意通过分享获得收益，可以形成一个良性互惠的生态圈。但是，由于交易过程不够透明，数据无法溯源，主体之间缺乏信任，商家无法监控消费者的分享频率以及效果，消费者也就失去了分享的动力。

艾尔链建立了一整套的激励措施，消费者无论是分享、在线还是消费都将获得不菲的通证奖励。消费者的行为指标都将会记录在链上，作为奖励的标准。商业也可以随时掌握当前产品的分享情况，以此解决消费分享过程中的信任问题。

4.1.4.5 产品信息不对称

电商平台售卖假货一直是一个备受关注的问题，由于商品难以溯源，消费者对于购买的商品缺乏信任。消费者其实愿意为优质产品买单，但是让消费者确信的成本却非常高，传统电商曾经尝试过用直播的方式来取信于消费者，但是依旧难以取得消费者的完全信任，阻碍了传统电商的品质升级。国际电商竞争激烈，消费者在选择的时候更加注重产品的品质，如果产品能够溯源，证明自身品质将会提升国际电商的竞争力。

产品的供应链全部会利用区块链进行溯源，结合物联网技术，全程记录产品从原料到生产到物流运输的全过程。杜绝假冒伪劣产品在各种电商平台野蛮生长的情况出现。消费者只需简单的操作即可掌握产品的全部信息，艾尔链将会致力于解决产品信息不对称的沉疴。

4.3 分布式社群生态

LAC 完整的生态需要依托巨大的社群体系，这个体系中有链上的电商、消费者和上游的供应商。LAC 的目标是让电商和消费者在这一生态中互利共生，合作共赢。LAC 使用创新技术的同时，也进行模式创新，让 LAC 的生态建设者在 LAC 的发展中获得红利。

4.3.1 电商

在传统的电商平台，商户与平台权利不对等，商户相对平台属于弱势方，平台掌握了流量和信息的这两个核心资源，商户只能依附于平台存在，对于平台提出的各种要求选择被迫接受。而 LAC 将会整合众多的电商平台，共享流量资源，众多的电商将不再有准入门槛和入驻费用。

LAC 整合了流量及信息资源，大大降低了电商的获客成本。目前平台上的电商获客成本极高，为了获取高质量的客源，投入了巨大的营销成本在广告投放，媒体营销上。在 LAC 平台上，电商可以以 LAC 的形式，用极低的价格投放广告。整合了多个电商平台后，资源将会高度集中在 LAC 上，为消费者提供一站式服务。

4.3.2 消费者

原有消费者的维护，新的消费者不断增加，是平台持续发展的必要条件。目前的区块链平台大多增量用户不足，缺乏发展动力。LAC 将会构建完整的会员体系，根据消费者的消费额、消费频率、在线活跃度（在线时间，浏览频率）加权，消费者分为三级会员制度，其中一级最高，三级最低。一级会员和二级会员将会在每个月初获得不同额度消费红包，每个月将会重新加权分级，激励平台用户在 LAC 上进行消费。

4.3.3 社区化分布式治理

LAC 将采取“TheDAO”——分布式的自治组织。分布式的自治组织是通过智能合约运行的实体，是一种通过智能合约将个体与个体、个人与组织、或组织与组织联系在一起的新型组织形式。

LAC 将把治理的权利交给社区，用技术让决策民主和管理高效实现兼容。采取社区化分布式治理意味着要尽可能把社区成员的积极性调动起来，让社区

成员能够共享权利，在 LAC 中真正获得归属感，在 LAC 的高速发展中获得红利。

4.4 泛金融生态

区块链已被广泛认为是未来二十年重构整个金融体系的变革性技术，在银行贷款、证券、保险、大数据征信等主要金融服务领域都将会得到广泛应用。除了消费，LAC 还可以为平台用户提供了诸如零押金分期，小额贷款等完善的金融服务。为了满足用户的消费需求，LAC 提供小额贷款业务。根据用户在平台的消费情况和信用记录，可以获得不等额度的 LAC 通证，用户只需在完全还清前每月支付利息即可。

对于消费能力不足以购买金额较大的商品的群体，LAC 可以允许分期付款。对于超过一定金额的商品，用户可以自由选择分不同期限支付，每期除了额定还款只需支付额外的少量手续费。如果到期未还款，平台将会下调用户的会员等级和信用评分。

对于一部分信用等级较高的一级会员，在数据分析充分评估风险的前提下，LAC 会为他们提供高杠杆借贷服务，保证会员使用大额度资金时资金量充足。

4.5 慈善生态

在目前的大多数非盈利组织中，善款的去向都是不透明的，即使公开也得不到有效监管，造成这些机构“既当运动员，也当裁判员”的情况发生。钱款的募集和使用过程难以透明公开，项目方可以轻松违规挪用款项，甚至项目造假。公益款项先进入中心机构账户，再由机构进行操作处理，多层级操作增加了项目成本。这是对捐款人和对捐款受益人的不负责，也不利于社会公益事业的发展。

区块链技术以不可篡改和可溯源性著称，如果使用分布式账本机制，将每一笔支出向捐款人公开，捐款人对于自己每一笔捐助的善款，通过区块链技术进行追踪，可确保自己捐助的资金最终应用到被需要的地方。

LAC 将会支持公益信息上链，利用区块链的总账技术进行记账，把线上善款募集、资金划拨、部分的线上支付数据记录在区块链上，解决捐款过程中的信息不对称的问题。

除了在链上记录信息，有了支付生态和智能合约的支持，LAC 也能实现数字资产的捐献通过智能合约实现，省去人工拨付等其他中间环中间机构，杜绝善款捐献中的作恶行为。

LAC 的主链系统也将为慈善生态提供支持，由于 LAC 主链通常是“完全去中心化”的，因为没有任何个人或者机构可以控制或篡改其中数据的读写。因此捐助者和受助者都可以完全信任 LAC 链上信息。

借助完备的金融服务体系和支付生态，LAC 在记账过程中，通过区块链去全盘透明公益基金的所有财务体系，将公益基金会专业化，扁平化和去中介化。逐步扩展区块链的记账节点，将捐款人、慈善组织、资金渠道、上游采购与专业援助服务提供方、受捐人或项目被有机地整合到 LAC 的公益区块链生态里。

4.6 电商众筹

众筹是指用团购+预购的形式，向网友募集项目资金的模式，可以为有创造能力但缺乏资金的人提供有力的资金支持。

目前的众筹平台作为第三方中心，为投资人和发起人提供了连接的纽带，强化了双方的合作，但是并没有承担起监督资金按计划使用的责任，无法为投资人的权益提供保护。众筹被认为是区块链除了支付以外最完美的落地场景之一，它解决了投资人和发起人之间的信任问题，用智能合约完成众筹中的权责落实，并且还可以记录发起人项目进展和各项开支。

例如，A 在 LAC 上发布一个众筹项目，B 投入一定的 LAC 参加众筹，A 拿到首批资金后启动项目，在项目运行过程中，B 要将大项支出信息记录在链上公开，重要决策也要及时在链上披露，当 B 完成项目原定的目标时，智能合约将会把后续资金持续打进 A 的地址。

此外，众筹发起者还可以直接在 LAC 主链上开发 Dapp 项目，用众筹所得的 LAC TOKEN 直接用于项目开发，或者借助 LAC 泛金融生态作为抵押获得启动资金，省去中间环节，降低项目开发成本。

对于电商平台而言，LAC 上的电商可以通过智能合约筹集项目资金，投资者也可关注项目进展并随时获取最新信息。电商众筹避免了传统电商众筹平台的信息不对称问题，极大地降低了电商发起人的启动成本，扩展 LAC 平台上的电商生态，支持“大众创业，万众创新”，让资本与创业有机结合。

4.7 直播生态

经过几年野蛮生长和流量大战，直播行业今年已经进入发展的瓶颈期，增量主播，增量用户严重不足，平台之间相互高薪聘请对方主播，恶性竞争不足为奇。长此以往，既无法让主播专心于自己的直播，也不利于行业发展。简言之，直播行业亟待新的增长点。区块链技术能够给直播行业注入新的动力，区块链直播主张的核心是内容至上，LAC 将会依托巨大的流量和社群资源自建直播平台。除了区块链技术，LAC 直播平台将提供基于人工智能和大数据的一站式广告投放方案，让正确的人看到正确的广告，用最少的钱实现最好的广告效果，充分对广告主负责。

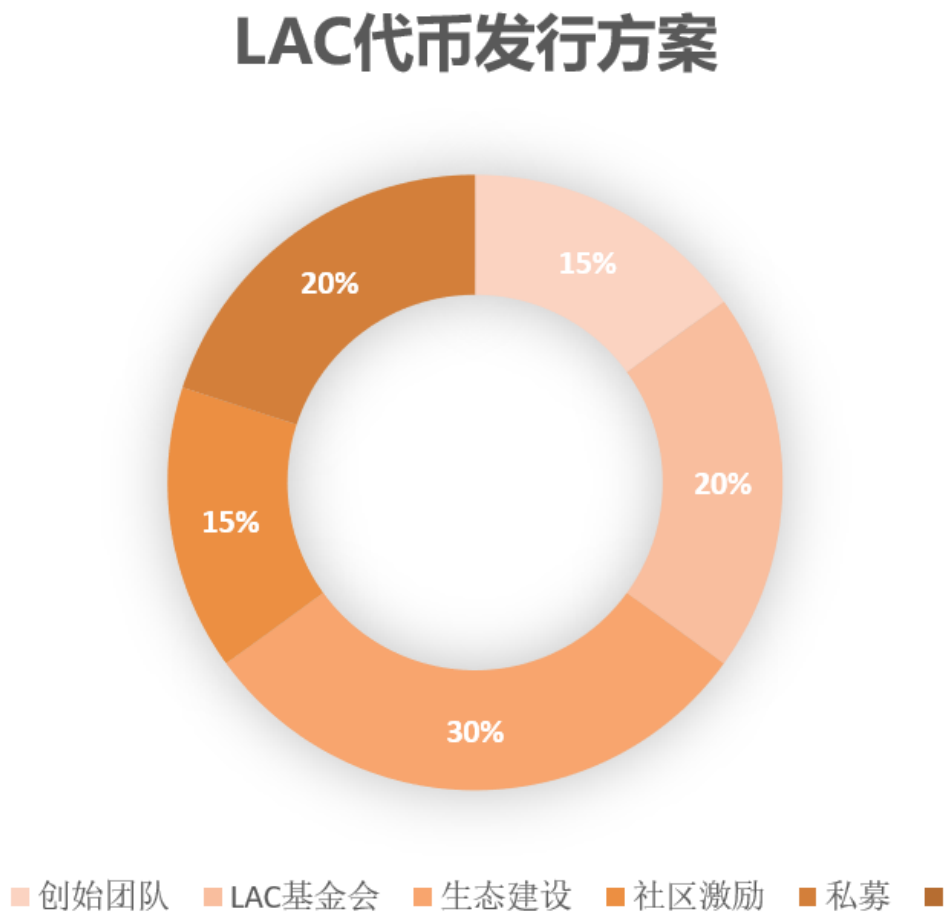
通过高效的机器学习算法的应用，LAC 社区实现了在视频的图像识别与短时间内为海量内容的标签化，可以高效甄别和发布直播内容，对内容进行快速鉴定，对于违规内容快速处理，让更多重视优质内容的“网红”可以收获更多的收益。LAC 设计的通证经济模式，也让观看视频的用户充分收益，共享直播平台发展的红利，根据观看时长，聊天频率，送礼物的次数计算用户活跃度，发放不同数量的 TOKEN 进行激励，实现社区价值的打造。

直播应用也将通过 LAC 主链的 Dapp 实现，除了直播以外，LAC 平台还将会开发多款满足用户各项不同需求的 Dapp，同时将会对优质 Dapp 的开发者给予高额度的奖励。各种 Dapp 将会使 LAC 生态进一步完善，成为 LAC 在更多领域落地，深入大众生活，赋能实体经济的内生动力。

LAC 去除了平台限制和手续费分成，鼓励用户成为优质内容创造者，将渠道、内容和用户三者紧密结合在一起，提高了平台内容的多样性，让生态结构更加完整。

五、代币发行方案

LAC 既是平台消费的通证，也是平台多项权益的价值凭证。LAC 生态的完善，通证不可或缺，LAC 发行总量为 77 亿。LAC 初始分配比例如下



- **创始团队 15%**

  共计 11.55 亿，即 15%的 LAC token 将用于创始团队激励，后期的技术开发和平台维护。该部分 LAC 会设置一年的锁仓期，一年后将按照每年 1%释放，16 年内释放完毕。

- **LAC 基金会 20%**

  共计 15.4 亿，即 20%的 LAC 会由基金会预留，基金会将统筹整个项目的进程，为项目发展提供建议和支持。该部分 LAC 锁仓期为半年，半年后将按照每年 1%释放，21 年内释放完毕。

- **生态建设 30%**

  共计 23.1 亿，用于 LAC 平台的运营，包括开发、运营、市场、人才招募、法务、财务、投资、商业拓展及后续发展等各个方面，每两年释放 1%，60 年内释放完毕。

- **社区激励 15%**

  共计 11.55 亿，15%的 LAC 将用于社区建设。作为一站式社群服务平台，社区建设将是 LAC 生态闭环形成的关键，该部分的 token 将用于社区生态激励和社群运营。

- **私募 20%**

  私募投资对象为天使投资人、机构、战略合作伙伴，主要为 LAC 的早期发展提供全球资源对接合作的支持。天使投资阶段获得的 LAC 币将锁定 8 个月。

六、基金会

LAC Fund (LAC 基金会，以下简称“基金会”)，致力于 LAC 生态建设、技术开发、商业推广，同时承担所有 LAC 的法律责任，在基金会下设立有

- **LAC 董事会**

  统筹整个项目的开发进度、运行情况、财务状况。LAC 首席执行官直接对 LAC 董事会负责，负责管理下属的市场部、技术部、投行部和风控部。完善 LAC 的区块链全产业线布局。

- **LAC 科技有限公司**

  LAC 科技有限公司主要负责 LAC 平台前期的技术开发、资讯消息管理、项目发行、上线交易所和后期的市值管理。

七、LAC 项目实施及路径规划

八、团队介绍

Christian Dal Santo
Back-End Developer
Created successful crypto applications(100,000 users).B.S in computer Science from UCLA. Worked @Microsoft and Amazon .

Faraz Amir
Lead Developer
Computer science from Stanford University. Has 6 years leading development teams in fintech applications.

Jacob Voyles
User Interface&Product
Founder of CryptoAnon.Has 5+years experiences in user interface design and front-end development in silicone valley.

Forest McDaniel
Full Stack Developer
8 years of experiences in full stack development & UI/UX design. Worked @Fantasy and TriNet

Paul Cruz
Full Stack Developer
5 years of experiences working on crypto & block-chain applications. B.S in Computer Science from UC Davis.

オウ アユウ
Project consultant
Bachelor of Economics, Osaka International University, Japan. Profound research on emerging economies, earlier exposure to the block chain industry, has invested in and participated in a number of financial sectors of the block chain projects.

九、免责声明与风险提示

免责声明

本文档是有关 LAC 的主要官方信息来源，目的是提供用于传达信息的特定对象的信息要求，仅作为传达信息之用，文档内容仅供参考，并且 LAC 基金会保留有对文档更改和编辑的权利。在作出相关决定之前，您应确保已阅读和理解白皮书的最新版本内容。

本文档只做参考交流之用，目的是提供用于传达信息和特定对象的信息要求，和向未来 LAC 潜在用户介绍 LAC 及其相关产品解决方案，以便他们决策是否深度参与项目与使用 LAC 提供的相关服务。本文档不构成在 LAC 及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。

本文档内容不得被解释为强迫参与 ICO。任何与本白皮书相关的行为均不得视为参与 ICO，包括要求获取本白皮书的副本或向他人分享本白皮书。 本文档只做参考交流之用，目的是提供用于传达信息和特定对象的信息要求，和向未来 LAC 潜在用户介绍 LAC 及其相关产品解决方案，以便他们决策是否深度参与项目与使用 LAC 提供的相关服务。本文档不构成在 LAC 及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。

LAC 团队将结合最新的开发进度，实时确保白皮书内容信息的真实准确性。开发过程中，项目将进行更新，包括但不限于：区块链技术更新迭代、生态模式的方向修改、通证及其分配机制等情况。因此本文可能会随着项目的开发情况进行内容调整，LAC 团队会及时在网站上以公告的形式，提示用户白皮书有内容进行更改。所以请务必实时关注官网，以获取最新版本的白皮书，并根据更新内容及时调整战略决策。LAC 团队明确表示，一律不承担因参与者过度依赖白皮书内容、本文信息不准确而导致的任何经济损失行为。

风险提示

LAC 作为 LAC 的官方代币，是平台发生效能的重要工具，并不是一种投资品。拥有 LAC 不代表授予其拥有者 LAC 平台的所有权、控制权、决策权。LAC 作为在 LAC 中使用的加密代币，均不属于以下类别：(a)任何种类的货币；(b)证券；(c)法律实体的股权；(d)股票、债券、票据、认股权证、证书或其他授与任何权利的文书。

LAC 代币不可用于本白皮书所提到之外的任何目的，包括但不限于任何形式的投资、投机行为。LAC 也不应因其信仰，假设或可能增值的其他价值项目而被交易。LAC 的增值与否取决于市场规律以及应用落地后的市场需求，我们无法保证 LAC 一定会增值，LAC 基金会以及团队不对其增值做出承诺，并对其可能造成的后果概不负责。

参考文献

[1]卜振兴.货币政策透明度影响因素研究——基于 DAG-SVAR 模型[J].财经论丛.2018

[2]李佳.基于区块链的电子支付变革及展望[J].中国流通经济.2018

[3]范广阔.公开透明是网络众筹平台自律的核心[N].中国商报.2018

[4]贾宏伟，邓修权.浅谈区块链在社会应急救助中的应用前景 Proceedings of 2018 2nd International Conference on Education, Management and Applied Social Science(EMASS 2018).[R].2018

[5]蔡维德； 郁莲； 王荣； 刘娜； 邓恩艳.基于区块链的应用系统开发方法研究.软件学报.2017.

[6]邵奇峰；金澈清；张召；钱卫宁；周傲英. 区块链技术:架构及进展.计算机学报.2017

魏尚北； 牛超. 密码学的区块链技术在电子货币交易中的应用研究.科技创新与生产力.2016

[7]杨宝华.《区块链：原理、设计与应用》.机械工业出版社.2016

[8]Andreas M. Antonopoulos. Mastering Bitcoin: Programming the Open Blockchain. O'Reilly.2017

[9]Joseph J. Bambara ;Paul R. Allen; Kedar Iyer. Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions.2018

[10]Jeff Reed. Blockchain: Blockchain, Smart Contracts, Investing in Ethereum, Fintech.2016

[11]周邺飞. 区块链核心技术演进之路——共识机制演进(1)[J]. 《计算机教育》.2017.

[12]王晓光. 区块链技术共识算法综述[J]. 《信息与电脑(理论版)》. 2017.

[13]韩璇，刘亚敏. 区块链技术中的共识机制研究[J]. 《信息网络安全》.2017.

[14]段希楠，延志伟，耿光刚，阎保平. 区块链共识算法研究与趋势分析[J]. 《科研信息化技术与应用》. 2017.

[15]刘肖飞. 基于动态授权的拜占庭容错共识算法的区块链性能改进研究[J]. 《浙江大学》,.2017.

[16]平健，陈思捷，张宁，严正，姚良忠. 基于智能合约的配电网去中心化交易机制[J].《中国电机工程学报》. 2017.

[17]刘德林. 区块链智能合约技术在金融领域的研发应用现状、问题及建议[J]. 《海南金融》.2016.

[18]臧磊. API 接口浅析[J]. 《电信网技术》.2004.

[19]李余琨， 杨平， 朱燊权. 支持开放的 API 接口的增强型业务[J]. 《计算机工程与应用》. 2004.

[20]李琪等.基于区块链技术的慈善应用模式与平台[J].计算机技术.2017

[21]乔一洛.区块链技术在泛金融领域的应用[J]。2018