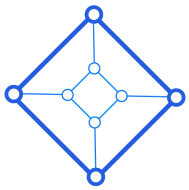

衔梯网络 白皮书

Ladder Network Whitepaper

目录

1.摘要

从互联网发展历程来看，互联网技术经历了 Web1.0、Web2.0，现在正在快速迈进以区块链、云计算、人工智能、大数据为核心的 Web3.0 时代，驱动新时期的商业社会形态、组织形态和治理关系变革。随着 5G 技术和万物万联时代的提前来临，金融、供应链、游戏、存储、溯源、内容等各行各业加速行业“链改”，新一轮科技革命和产业变革席卷全球。

但是，Web3.0 演进进程和区块网进化中，也存在诸多问题亟待解决：

- 存在着中心化、共享不充分、交易拥堵、交易费用昂贵等问题。
- 链与链之间缺乏互操作性，存在互通不畅问题。项目与项目之间无法进行价值沟通，孤岛问题仍然存在。
- 已有跨链技术关注资产转移而缺乏完善跨链基础设施，不利于异构架构整合。
- 链改开发难度高，部署极其复杂，现有区块链架构无法满足未来 5G 环境下多样复杂的应用场景需求。

为解决这些问题，衔梯网络 Ladder Network 应运而生。**衔梯网络 Ladder Network 是致力于成为“Web3.0 时代”的跨链领域基石网络，旨在建成区块链世界万链互通的领航者。**衔梯网络 Ladder Network 通过引入门限签名的见证人机制确保交易验证的有效性，首

创跨链投资模式，促进了跨链资产的畅通流动，引入预言机打通了链与现实世界的壁垒。

衔梯网络 Ladder Network 构建了分布式、去中心化、最安全及最大规模 POS 跨链网络，验证节点可达上千个，候选验证节点可达万级。利用跨链优势和万级以上的节点优势，衔梯网络 Ladder Network 重点部署的领域有：数据共享、安全及隐私保护、去中心化交易所和 Web3.0 电商等。通过与 ABMatrix 的战略合作，预计未来三年直接带来千万级的物联网用户流量。

衔梯网络 Ladder Network 可作为区块链第一层协议，可对接成千上万的第二层区块链协议，通过跨链技术构建覆盖更多范围内的企业多方协作的价值网络。衔梯网络 Ladder Network 瞄准千亿级规模的“万企上链”和“万链互通”市场，BAAS 区块链服务平台建成后，将全面支持金融、供应链、游戏、去中心存储等领域的敏捷发币，实现企业链改，满足 5G 时代高吞吐、低延迟、高并发、低功耗复杂应用场景需求，重塑行业的信用基石和商业形态。

2.行业背景

区块链的本质是一种去中心化的分布式账本，具备分布式数据存储、共识机制、加密算法、点对点传输等特点。2009 年 1 月 3 日中本聪挖出第一个区块开始，比特币不间断连续运行至今，用长达 10 年的不间断安全运行成果，比特币证明了区块链技术的可行性。这

10 年来，全球迎来了区块链概念大爆发，以太坊、ICO、稳定币、去中心化交易所、IEO、超级节点经济等概念正在颠覆着人们的想像。

2.1 区块链发展路径

对于未来区块链行业发展方向，我们有以下两个预判：

一是全球迎来了区块链最好的发展时期,各行各业有着极其迫切的上币链改需求，未来将驱使更多的 BAAS 区块链服务平台诞生。

在资本助力和技术驱动下，越来越多的公司、创业者开始涉足区块链，区块链项目呈井喷式增长。2018 年 10 月 10 日，IBM 宣布 IBM Food Trust 正式商用。2019 年 2 月，摩根银行宣布将发行银行系统稳定币 JPM，一个 JPM 瞄准一美金。2019 年 3 月，彭博社报道拥有 20 亿用户的 Facebook 正在战略转移区块链，研究利用 WhatsApp 推出一款稳定币，瞄准汇款市场。

区块链技术正在推动新一轮的商业模式变革，成为打造诚信社会体系的重要支撑。各行各业涌入区块链的方式有两种，一种是自主开发，内部培养区块链人才完成链改。另一种是使用现成的区块链平台服务。从节省成本、提高效率看，后者将是大多数公司完成业务币改的主要方式。未来将会诞生很多专业的区块链服务，即 BAAS 产品服务，这是一个巨大的产业、市场和技术需求。

二是区块链是属于所有人的，区块链的项目也应是分布式的，未来不会出现全球统一或少数统一的区块链框架、架构，未来一定是万链共存齐飞的世界。

万链共存多元化发展必然带来异构性、互操作性和复用低效等问

题，因此连接不同链的中间平台将应运而生，并催生链与链之间的协议、技术、架构 ，也即是跨链技术。

跨链技术如同计算机系统的中间件技术。互联网促使分布式系统和网络应用的诞生，中间件就是伴随网络技术的产生、发展而兴起的，由于不同的系统、不同的应用广泛存在，因此有了 IBM CICS 等著名的中间件存在。

因此，我们认为，万链共存、企业币改链改的过程中，链与链之间的协作、互操作将更加常见，跨链技术随之兴起和繁荣。

2.2 行业痛点

每条链都有自己的逻辑架构、区块结构、共识机制、挖矿模式和商业模式、经济模型、治理结构。万物万链世界首当其冲要考虑的问题是链与链之间的互操作。另外，由于应用场景的多样化，业务上链往往需要考虑与现有系统的整合问题，面临的挑战也很大。

在跨链资产交易方面，在去中心化技术不是很成熟的条件下，目前市场中心化交易所实现了资产转移以及不同资产互换，是一个相对折中的弱跨链方案。中心化系统的弊端是用户需要把资产转移到三方中介中，用户丧失资产所有权的同时也带来了安全隐患，那些聚集了大量用户资金的交易所也是黑客攻击的目标。交易所通过技术手段阻止了黑客攻击，但它也影响了正常的资金交易和提现，同时交易所还普遍存在内幕上币等不公平不公正的现象，这都促使人们寻找更好跨链方案。

在跨链信息协作方面，不同区块链的网络共识机制不同，跨链后经常出现信息不同步问题，比如比特币平均十分钟出一个块，EOS 是 1.5 秒，那么中间九分钟五十多秒的间隔，黑客就有可乘之机；其次区块链协议的复杂性，不同区块链经济体系不同，也是导致不同区块链网络之间通信协同困难的主要原因。

在链与现实部署方面，也存在许多问题：业务逻辑复杂导致上链难度大;现实世界无法与链上资产进行一一对应，导致链上数据失真，比如溯源供应链系统无法彻底解决上链前的真实性验证;上链实施开发周期长、技术难度大;等等。

2.3 现有跨链技术

现有去中心化跨链技术大致有三类： 公证人机制（Notary schemes），侧链/中继（Sidechains/relays），哈希锁定（Hash-locking）。

公证技术：早期瑞波实验室提出 Interledger 协议就是典型的公证人技术，它的目标是连接不同账本并实现它们之间的协同。Interledger 协议适用于所有记账系统、能够包容所有记账系统的差异性，该协议的目标是要打造全球统一支付标准，创建统一的网络金融传输的协议。它缺点是去中心化程度不够，由个别机构掌控。

侧链/中继链：区块链系统本身可以读取链的事件和状态，即支持 SPV（Simple Payment Verificaiton），能够验证块上 Header、merkle tree 的信息。本质特点是必须关注所跨链的结构和共识特性

等。一般来说，主链不知道侧链的存在，而侧链必须要知道主链的存在；双链也不知道中继的存在，而中继必须要知道两条链。

哈希锁定：Lightning network 闪电网络提供了一个可扩展的 bitcoin 微支付通道网络，它极大提升了比特币网络链外的交易处理能力。交易双方若在区块链上预先设有支付通道，就可以多次、高频、双向地实现快速确认的微支付；双方若无直接的点对点支付通道，只要网络中存在一条连通双方的、由多个支付通道构成的支付路径，闪电网络也可以利用这条支付路径实现资金在双方之间的可靠转移。

公证人机制、侧链/中继或哈希锁定是实现跨链操作性的一种理论上的框架技术。目前比较火的 Cosmos、Polkadot 即是实现某种跨链技术的产品。在跨链技术上，衔梯网络 Ladder Network 和 Cosmos、Polkadot 一样，是典型的中继链模式，衔梯网络基于 Substrate 框架开发，这一点又和 Polkadot 类似。

3.解决方案

3.1 项目愿景

衔梯网络 Ladder Network 致力于打造全球最分布式、最安全和最大规模 POS 跨链网络，构建区块链平行世界的可信跨链平台，搭建链与链之间的信任桥梁，打破一链一孤岛的局面，实现链与链之间的自由流通、资产互操作、价值互通。

衔梯网络 Ladder Network 通过可操作性、可配置化的模块设计，

提供敏捷发币功能，助力企业完成业务链改，实现业务价值增值，最终为“万企上链”和“万链互通”提供最安全、最可靠、可插拔的区块链基础服务，为全球区块链世界革命贡献力量。

3.2 设计目标

为了实现上述愿景，衔梯网络 Ladder Network 技术需求主要来自于跨链技术和区块链支撑服务两个方面。其设计目标：

• 实现互操作性(Realize interopera)

互操作性是跨链的最基础需求。造成互操作性不好的原因，主要是各个项目的底层协议不统一，异构性导致链与链之间成为孤岛。衔梯网络 Ladder Network 将提供标准的通信机制、网络协议、资产通讯、服务语义，促成不同平行链互操作性的达成。

• 屏蔽异构性（Hiding heterogeneity of system）

参照 TCP/IP 协议分层思想，在衔梯网络 Ladder Network 架构设计上建立逻辑分层，将处理功能相同的模块建立层级，层与层之间通过服务语言通讯，跨层级不能直接通讯，从而屏蔽异构性，屏蔽共识算法、治理架构、区块结构等差异。

• 可信隔离（Trusted isolation）

清晰制定链内最小安全设施可信计算模块，建立安全边界（security perimeter），划分可信与不可信的边界。明确统一安全

接口，使用引用监控器（reference monitor），保证安全最大化，访问路径可确认、可验证，达到安全、可信。

• 共性凝练和复用（Common Condensation and Reuse）

相同领域的区块链服务之间许多基础功能和结构是有相似性的，每次开发系统都从零开始绝对不是一种好的方法，也是对质量和效率的很大的伤害。因此，衔梯网络 Ladder Network 应按照不同的应用场景领域划分不同的模块处理，建成复用性高的区块链服务平台,达到区块链服务面向用户，服务参数化管理，功能支持可配置的目标。

3.3 生态协同

衔梯网络 Ladder Network 是基于 Substrate 开发框架协议开发。目前 Polkadot 项目也使用 Substrate 框架。Substrate 是类似于 Express 或其他 Web 应用程序的框架，主要用于构建分布式或去中心化系统的框架，例如加密货币项目或消息总线系统。衔梯网络 Ladder Network 使用 Substrate 的目的，一是能使项目继承 Substrate 的功能、安全性和可扩展性优势。二是能将团队的主要精力集中在跨链平台和区块链商业服务的研发上。正如大多数 WEB 应用程序不需要重新实现自己的 HTTP 协议一样，使用了 Substrate 后，每一个团队创建新链时，不需要从头开始一步步实现网络和共识等代码。

衔梯网络 Ladder Network 使用 Substrate，结合了三种技术:La_WebAssembly、La_Libp2p 和 La_GRANDPA 共识协议，通过快速构建新的区块链的库，应用区块链客户端的关键框架，能够同步到任

何基于 Substrate 技术开发的链。通过使用 Substrate，衔梯网络 Ladder Network 将直接继承以下优势：

- 实现区块链共识算法、最终确定性和区块投票逻辑。
- 具有能够进行节点发现、数据同步和复制等功能的 P2P 网络库。
- 通过高效、确定、沙箱化的 WebAssembly 运行机制，可以用来运行智能契约，甚至运行其他基于 Substrate 开发的项目。
- 能够在浏览器中无缝运行一个节点，该节点可以与任何桌面或云节点通信。
- 跨平台的数据库/文件存储抽象。
- 无缝的客户端更新。快速安全的部署本地版本的代码，无需担心出现硬分叉和其他共识问题。

3.4 技术架构

衔梯网络 Ladder Network 提供了异构链间资产转移通道的基础设施，是一个通过跨链协议实现与不同区块链网络互联互通、完整记录跨链交易、维护链内交易明细的分布式系统。

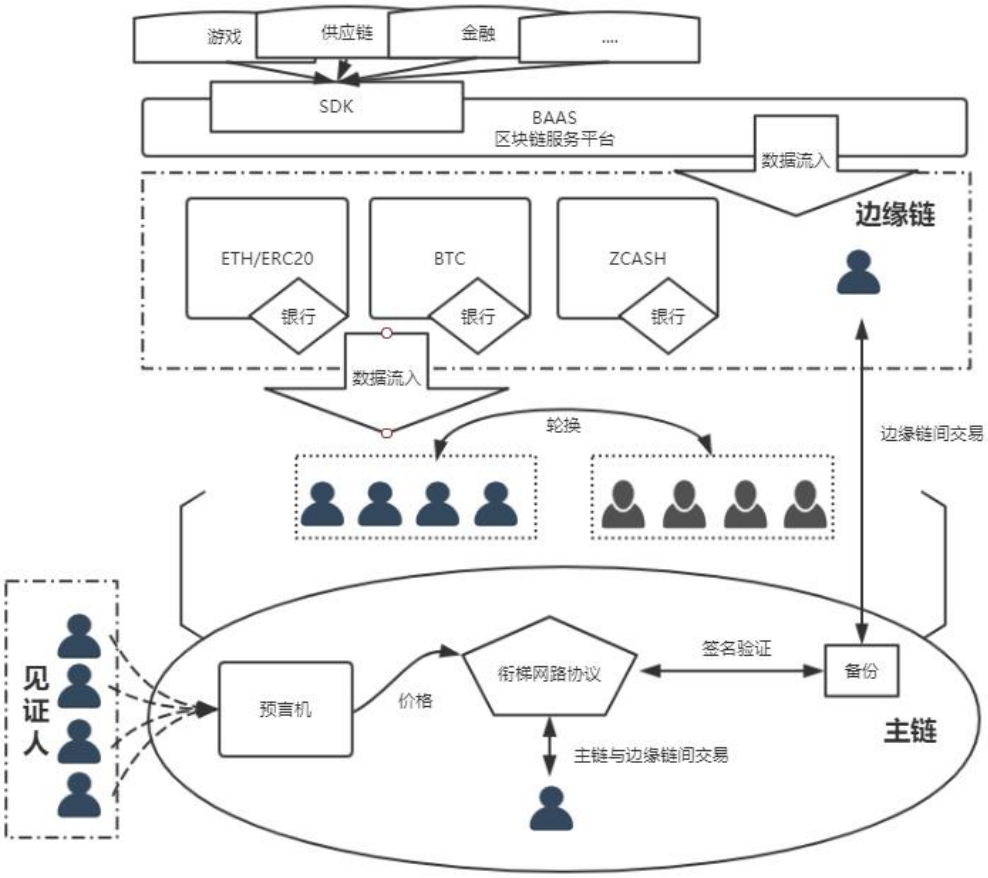

图 1：架构图

边缘链是指搭载了衔梯网络协议的链，例如以太坊、比特币、EOS、溯源链等等。**主链**是衔梯网络 Ladder Network 核心链，它可以独立运行，也可以充当桥链。

衔梯网络 Ladder Network 主链提供注册模块。名称在主链注册模块上进行登记，经规则 Rule-Audit 即可正式加入衔梯网络 Ladder Network 成为合法的边缘链，共享衔梯网络 Ladder Network 的跨链服务。

每个边缘链都对应一个 64 位的地址空间，为了避免开发者、用户使用人员识别繁杂难记的地址，衔梯网络 Ladder Network 提供链名服务 CNS(Chain Name Serives)。CNS 负责将地址空间与项目名进行

双向映射，比如 BTC 边缘链在网络中的名称为 Ladder_BTC。

区块链系统之间相对独立，信息在单个区块链系统内流转是可信的，而在链之间流动需要通过桥接中断方式加以证明，所以边缘链中的消息通过主链存储和校验后，再由主链转发到目标边缘链上，从而确保链与链之间信息的可信流通。

跨链运行简单的流程：用户在边缘链 A 发起的到 B 链的转账操作，用户 A 首先通过 CNS 获得 B 链的项目名，再通过 Request—Resposey 方式查询是否有冲突，如没有冲突，即由证明用户从边缘链获取转账证明，并提交转账信息到主链上，主链对信息校验后发送到边缘链 B 上，至此完成一个信息跨链操作。

未来，衔梯网络 Ladder Network 还将提供 BAAS 模块，为企业、创业者上链提供一键发币功能，BAAS 模块提供了参数化、配置化的区块链服务，根据业务领域开发金融 SDK、供应链 SDK、游戏 SDK、存储 SDK 等构件接口，企业将能以零编程方式接入 BAAS，共享主链服务，为企业链改币改提供商业生态。

3.4.1.共识

衔梯网络 Ladder Network 使用 POS 为基础的 BABE + Grandpa 共识算法，在出块人选择上，BABE + Grandpa 则是基于 VRF 算法随机选择出块人，这保证了公平性。

在衔梯网络 Ladder Network 上有三类节点：权威节点，预言机证明节点，普通验证节点。权威节点是抵押大量保证金的节点，保证金

越多，出块的权益越大，如果不出块，或者作假，其保证金将被扣除。预言机证明节点是抵押了一定保证金的节点，通过随机算法选出一组节点，它们从边缘链上获取数据并签名后发送到主链，获取汇率。如果发送了虚假交易或者不发送交易，衔梯网络 Ladder Network 会扣除保证金，并剥夺其跨链交易证明节点的名额。只有掌控了足够权益才能成为普通验证节点，它对前两类节点行为进行验证，发送作假行为。

3.4.2 跨链原子交易

为保证交易的原子性，我们设计如下协议：

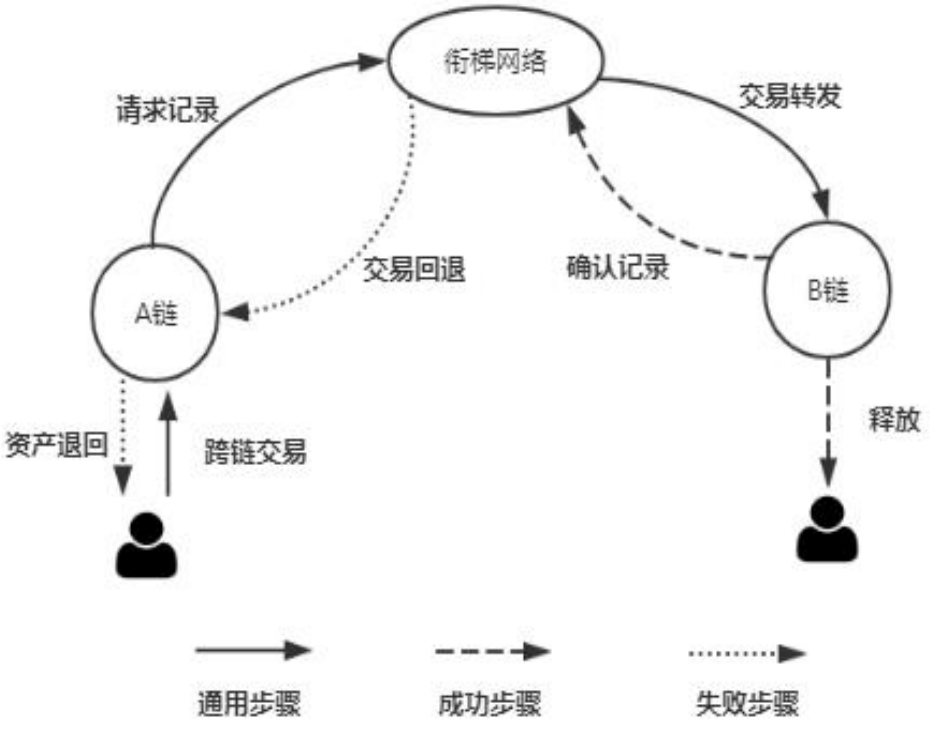

图 2：原子交易协议

用户在边缘链 A 上发起一笔跨链交易，主链自动监听 A 链的交易事件并记录（因为采用多签见证人方式，交易记录存在冗余，后续会介绍如何处理改进问题）。 主链对 A 链上的事件进行校验，并转发到边缘链 B 上，因为在 B 链上释放需要足够的资金，这时就存在有两种情况，资金充足能达到释放标准，那么这笔交易成功，并记录到主链上；资金不够无法释放，这笔交易失败，主链将把用户在 A 链上发起的交易资产返回给用户，即发起一笔回退交易。

在整个交易流程中，用户资产会在边缘链上锁定一段时间。如果交易失败，会在边缘链上返还资产；交易成功，则把这部分资产放入资金池，用于释放从其他链发起的交易。

每秒交易量（TPS）

TPS = Sb / St / tb

Sb 是块的大小，主链块大小为 4M。

St 表示交易的大小，通常交易为 250 字节。

tb 表示出块时间，默认 3 秒。

交易延时

为保证交易的安全性，所有交易需要在衔梯网络 Ladder Network 上记录，其时间为 Ta（可视为出块时间），边缘链的出块时间分别为 T1 和 T2，防止双花的块确认数 D。

一次成功的跨链交易，至少需要有四笔交易，两条边缘链上各一笔交易，主链上两笔交易，分别为请求和确认交易 ，那么我们可以给出如下公式：

$$L = Ta * 2 + T1 * D + T2 * D$$

失败处理

跨链抵押在衔梯网络 Ladder Network 上验证失败或在 B 链上释放失败的时候，都会对 A 链的资产进行回溯，实现原子操作，避免 A 链资产的丢失。

首先是在衔梯网络 Ladder Network 上的多签验证阶段失败，衔梯网络 Ladder Network 会直接返回验证失败，如果验证节点在一段时间内收不到资产抵押验证成功的回复信息，就会将该笔交易记录为删除，同时把资产返回给 A 链。

多签验证的存储结构：

交易 <=> [签名，是否发送]

交易 <=> 是否验证通过

衔梯网络 Ladder Network 上接受验证节点监听获取的跨链抵押交易，当签名数量达到一定的数量的时候就会确认该笔抵押请求并存储该交易。失败就会直接删除该交易存储，同时通过参数进行配置修改，

防止因网络延迟导致的重复交易干扰。

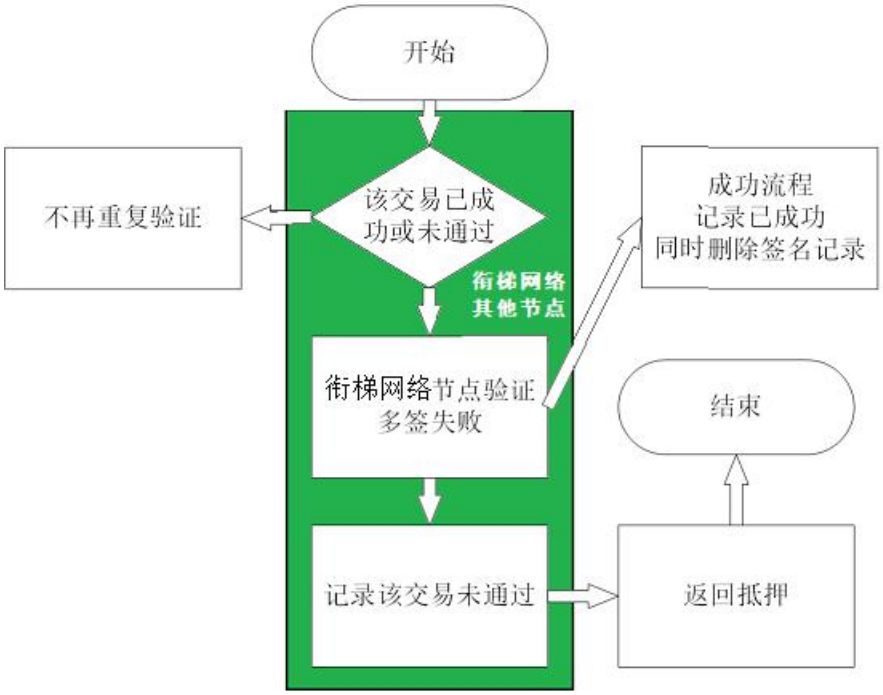

图 3：原子操作对都验证失败的时候资产返回流程

3.4.3 银行模块

通常跨链是通过资产映射方式，例如中心化交易所，用户需要三步操作才能转换资产。我们的目的是简化资产转移所需步骤，仅通过一次包含目标链以及账户地址的操作，就能实现资产转移。

考虑到资产总量对转换实时性的影响，我们引入银行模块来解决流动性问题，在边缘链上该模块通过合约管理用户的投资资产，并且在一定时间后能在主链上获取收益。

在链上用户可以随时取出资产，我们不会做任何锁定。投资人可在边缘链上操作，将资产的投资给跨链提供流动性，作为回报获得主链上的投资收益，因此该投资操作近似银行存款。同时该操作设计多个不同的链和不同分工的节点，以以太坊为例，其主要流程和分布图

如下：

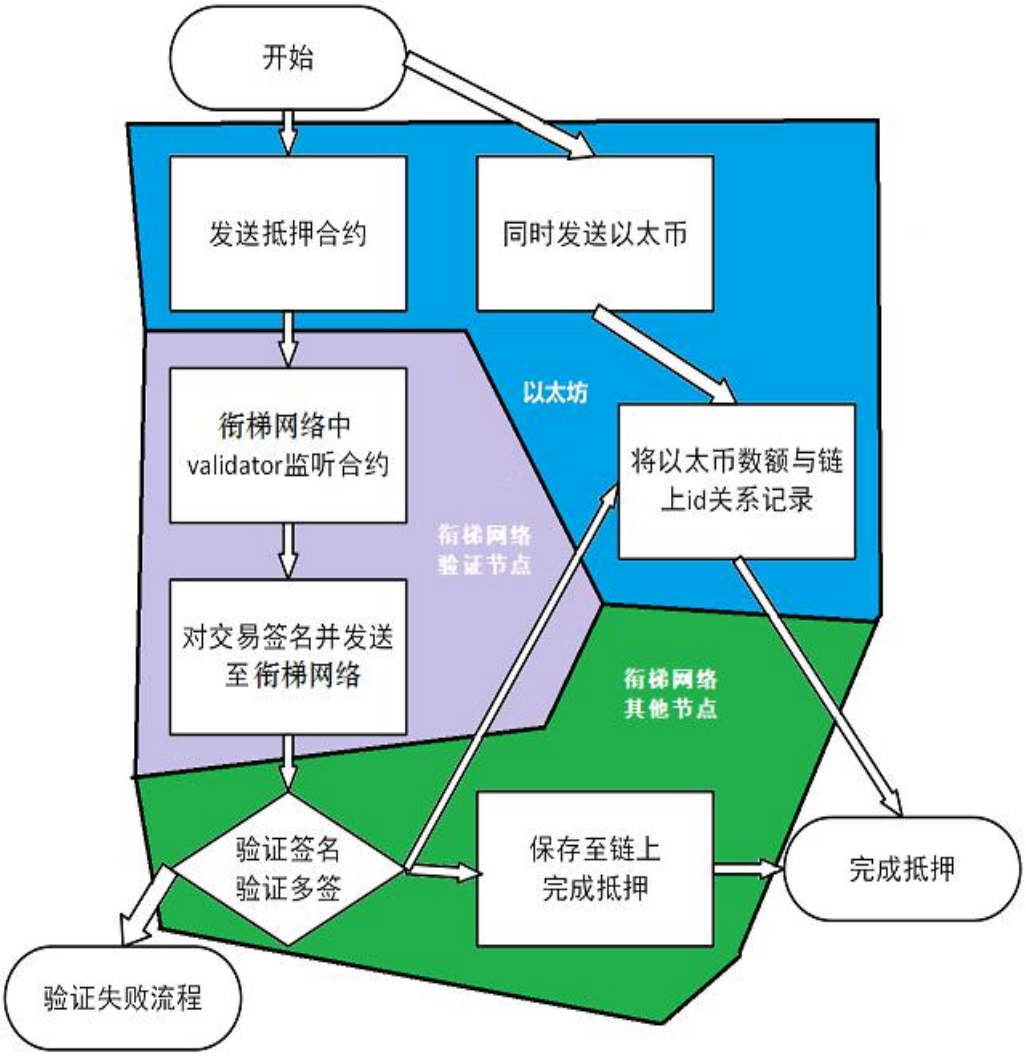

图 4：衔梯网络 Ladder Network 抵押操作节点分工以及流程

银行模块系统流程可以分解成 5 个部分，以下流程以太坊为例，以太坊上操作产生一个抵押的交易 T，Ladder Network 上的相关验证节点监听到这个信息后，完成签名并转发上链进行验证。

过程 1　欲抵押者发送一笔交易，每个验证节点监听包含链上账户，抵押金额的交易

Txn n=1,2,3,4,5,……

过程 2 验证节点捕获并对每个交易进行签名

Tsn = sign(Txn) n=1,2,3,4,5,……

过程 3 封装同时将数据上传至衔梯网络 Ladder Network 上

∑Tx(Tsn, data) n=1,2,3,4,5,……

过程 4 衔梯网络 Ladder Network 的各个节点参与验证签名有效性，以及数据有效性（通过多签判断数据是否是被不合谋的验证节点分别上传的）该验证过程是由签名的模块提供保证。

Check（∑Txn） n=1,2,3,4,5,……

过程 5 验证通过就将数据保存至链上，完成抵押过程

Prase_update(T,data)

3.4.4 汇率模块

为了实现不同资产快速兑换，这就涉及资产定价。但区块链是一个确定性的、封闭的系统环境，目前只能获得链内的资产数据，区块链与现实世界是割裂的，不能获取到链外真实世界的数据。

为解决这个问题，我们在链上部署预言机合约。主链的汇率模块以轮换方式周期性的将各资产价格推送至预言机合约，预言机合约通

过链下的 API 接口获得外部数据。技术实现的流程是，外部数据发送数据给链上预言机合约，预言机合约把数据传送给汇率模块。

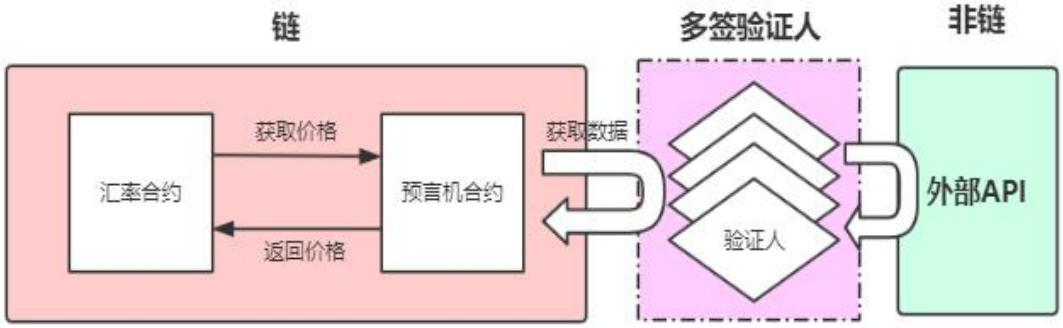

图 5：汇率模块

汇率模块的验证节点通过多签的方式实时获取外部加密资产的实时汇率，且该信息经加密签名处理，不可篡改。通过实时汇率，A 链和 B 链完成跨链资产转换,这类似于中心化的交易所。其过程如下：

步骤 1 判断当前账户是否是预言机节点的关联账户 id

Is_validator(id)

步骤 2 如果是的话，就调用外部 API 获取实时交易所各种加密货币汇率

Tx = http_get(url)

步骤 3 将汇率签名后发送至多签验证模块

Txsn = ∑Sign(Txn) n = 1,2,3,4,5,……

步骤 4 多签验证通过，则记录该汇率

Check_save(Txsn) n = 1,2,3,4,5,……

3.4.5 风险控制模块

在上述跨链协议中，有一个问题需要重点考虑，即是流动性不足引发的交易回退问题。如果该系统流动性较好，有足够的投资人和用户，理论上不会发生交易回退。但我们的系统将考虑一切可能发生的情况，包括初始、极端等边界情况，如在系统早期资金支持极少，用户体验不佳；另一方面，在边缘链上的投资人对资产存入与赎回操作都会影响流动性，因此引入风险控制模块来处理此问题。

AI 风险控制模块的作用：

- 通过利率保证边缘链上资金充足。
- 确保跨链交易的成功，减少无用操作。
- 保证系统的流动性。

AI 风险控制模块的影响：

- 控制银行模块利率变化
- 控制跨链交易的浮动费用。
- 控制边缘链资产价格稳定。

通过监控主链上的交易以及边缘链上的资金余额，我们可以推算

出某笔交易未来能否成功，从而减少交易回退现象，进而减轻系统压力。

允许最大跨链交易金额 Vmax 计算公式如下：

入资金均值：

$Vi = \sum(Vt / St) / n / L,\ n = 1,2,3,4,5,\cdots\cdots n < 100$

出资金均值：

$Vo = \sum(Vt / St) / n / L,\ n = 1,2,3,4,5,\cdots\cdots n < 100$

$Vmax = R - Vi + Vo$

T ：单笔交易

L ：交易延迟时间，单位秒

Vt ：T 交易发送的值

St ：T 交易从发送到当前时刻的间隔，单位秒

R ：当前边缘链上的余额

3.4.6 Plasma arbitration 协议

Plasma 最初设计目的是，为以太坊扩容问题，以链链结合的方式减轻主链的负担。 Plasma 的特色是提供了一个资产退回基本保证，即你始终都可以将你的资产和资金退回到主链上。

对于如何保证资产退回的问题，Plasma 包含了欺诈证明机制，即

用户提交资产冻结证据到主链，任何人都可以提交一份“欺诈证明”，质疑资产退回。 但是，资产退回本来就有风险，其中一个问题就是子链的用户同时向主链提交资产退回请求，会导致主链没有足够的容量来处理质疑期内的交易，还是有可能丢失资金。

我们把用户博弈部分放在性能高的衔梯网络上，再引入委会机制保证仲裁的公证性，这样避免主链因性能问题导致资金丢失。如下结构：

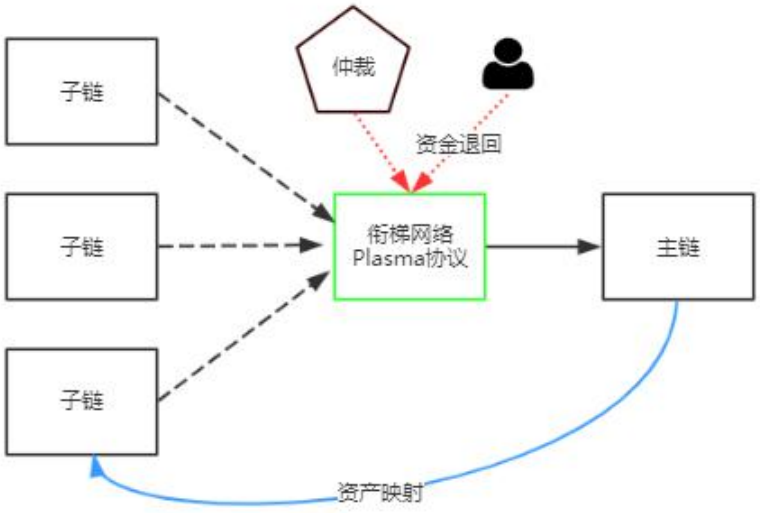

图 6：衔梯网络 Ladder Network Plasma 结构

使用流程如下：

第一步：供应商在衔梯网络上注册并开通映射通道。

第二步：用户在主链上映射资产，衔梯网络记录操作。

第三步：衔梯网络在子链上释放资产。

第四步：用户在子链上发起资金退回申请，衔梯网络仲裁。

第五步：衔梯网络在主链上释放资产。

4.安全性保证

4.1 基于 VRF 算法的门限签名协议

单见证人模式的主要缺点是安全性不足，以及去中心化程度不高，因此我们采用 VRF 算法的门限签名见证人方式弥补缺陷。在链上我们会周期性地通过 VRF 算法随机选举出新的签名组，并将其重新设置在各边缘链，也就说主链上的多签和主链上的多签是同步更新的。通过这种方式可以保证安全同步。

4.2 动态多签

所有验证节点合计抵押必须超过 x%的衔梯网络 Ladder Network 的总发行量，假设没有一个人能控制 x%发行量，根据这个 x%来实时决定链上多签验证通过一笔交易所需的签名数量。

5.应用领域

衔梯网络 Ladder Network 利用跨链优势和万级以上的节点优势重点部署的领域有：数据共享、安全及隐私保护、去中心化交易所、Web3.0 电商。最终，衔梯网络 Ladder Network 建成 BAAS 区块链服务平台后，将提供多种领域的 SDK 组件，包括金融、供应链、游戏、去中心存储等平台，满足 5G 时代高吞吐、低延迟、高并发、低功耗复杂应用场景需要。

5.1 数据共享、安全及隐私保护

数据共享、安全及隐私保护是区块链重要的应用领域，数据类的项目一般属于这个领域。在这方面，衔梯网络 Ladder Network 具有成熟的解决方案。一方面，通过共享闲置资源把跨链验证节点集成到一体机，可以节省部署衔梯网络 Ladder Network 验证节点所需的费用，并且做到节点足够的分散和稳定性，该部分节点共享模型已获得国家知识产权局的发明专利；另一方面通过和边缘计算技术相结合，做到更好的保护企业数据安全及隐私，并且实现数据价值的共享和交换，做到价值流转可追溯、可验证、可量化和可清结算。

目前，衔梯网络 Ladder Network 和 ABMatrix 达成战略合作协议，双方合作帮助企业构建基于物联网技术与区块链技术的企业多方协作的数据价值网络。通过合作，衔梯网络 Ladder Network 将能深入到最广泛应用的数据共享、安全及隐私保护领域。与 ABMatrix 的战略合作，预计未来三年在物联网领域直接带来千万级的用户流量。

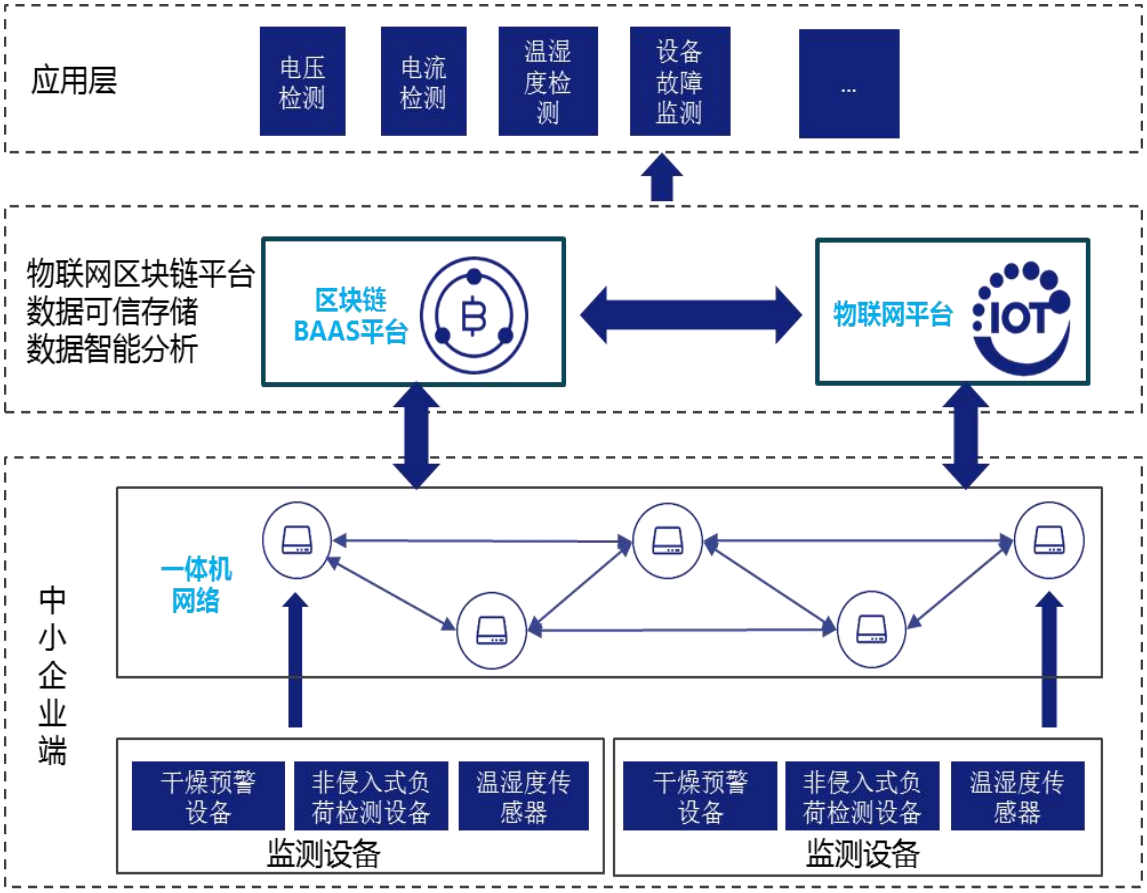

图 7：衔梯网络 Ladder Network 工业互联网架构案例

ABMatrix 由浙大系技术开发者和计算机科研实验室团队联合创立，是一家专注于前沿科技和产业升级的工业互联网平台厂商，其产品覆盖工业设备、边缘计算、物联网、区块链、大数据以及云计算等，为国际知名企业提供包括故障诊断、故障分析和预测、可靠性分析、产线优化乃至产能提升等全方位解决方案，覆盖百余家工业企业。

5.2 去中心化交易所

去中心化交易所是未来交易所的趋势。币安、火币都已布局这一领域，币安去中心化交易所 dex 即是使用基于 cosmos 的公链，未

来具有项目方资源的公链将会实现去中心化交易功能。

本质上,去中心化交易就是一种典型的跨链应用。衔梯网络Ladder Network 通过去中心化的方式将链间资产进行统一转化，任何链只要建立与衔梯网络 Ladder Network 的连接，就可以与所有链进行资产互通，并且支持隐私保护功能。衔梯网络 Ladder Network 的钱包很快将集成这一功能。

一旦主网上线后，衔梯网络 Ladder Network 的去中心化交易协议将能正式使用，衔梯网络 Ladder Network 将正式为中心化的交易所提供技术支撑平台，LAD 可作为平台币。由于有 gas 燃烧和通缩的机制，如果越多交易所使用衔梯网络 Ladder Network 平台，将对 LAD 的价值有着强大的支撑。

5.3 WEB3.0 电商

传统零售时代，“中心化电商”是商家联网的主要方式，一个电商平台集中了所有商家和眼球/流量，成为消费者购物的第一入口。但是在注重用户流量的新零售时代,零售商家逐渐意识到自有流量的重要性,拥有独立的电商平台、“去中心化电商”成为商家的新诉求。

衔梯网络 Ladder Network 能够满足这方面诉求。在衔梯网络 Ladder Network 中，用户浏览电商 DAPP，选择了某件商品并下单，电商 DAPP 通过跨链网络去请求用户身份信息，核实通过之后，并向支付链发起支付请求，支付成功后，再将订单信息同步到物流链，物流链获取订单信息后，去商家仓库取件再将物品投递到用户手中，这

一切链下信息通过物联网实时同步到物流链上（如图 7 所示）。

通过衔梯网络 Ladder Network 的改造，电商平台用户的所有信息，包括请求信息、支付信息、物流信息和资金流信息，都在可信的网络中流转，用户的隐私和数据由用户自己掌控，避免了中心化电商的垄断、诈骗、造假等问题。

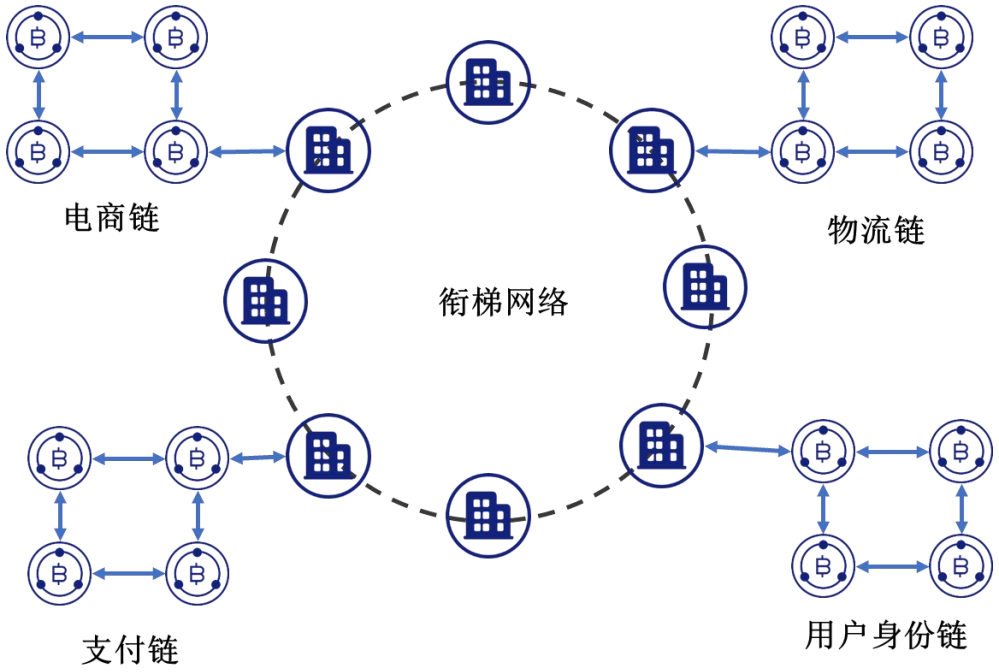

图 8：衔梯网络 Ladder Network 电商案例

6. 通证模型

衔梯网络 Ladder Network 代币为 LAD，总量 10 亿，不增发，矿池部分每 2 年减半的模式发行。用户通过跨链系统进入衔梯网络 Ladder Network 的各类资产，将根据每日均价自动折合成 LAD 市值，根据持有资产的总市值分配发行的衔梯网络 Ladder Network。

通证互换：15%

含早期通证互换参与者，和交易所上线的通证互换激励计划

开发团队：10%

LAD上线交易所后，每年解锁2%用于运维支出和可持续开发

基金会：10%

前期2%用于早期战略布局和高度合作，后面每年解锁2%

生态建设：15%

前期3%用于早期生态建设和资源引入，后面每年解锁3%

矿池预留 50%

每两年减半的模式进行发行，接入网络的节点和矿机进行激励和生态流通

用户挖矿所得的 LAD 可以用于：

- 支付矿工费用。
- 抵押成为节点。
- 投票选举节点。
- 作为兑换某些小众资产的中间货币。
- BAAS 平台接入锁定的代币。

边缘链的加入、用户交易、BAAS 平台接入项目的增加，都会消耗 LAD，在 LAD 总量一定的情况下，LAD 的价值将增加。

7.路线图

1.2018 年 7 月，衔梯网络 Ladder Network 立项。

2.2018 年 9 月，衔梯网络 Ladder Network 多个技术路线提出，白皮书 1.0 发布。

3.2018 年 12 月，衔梯网络 Ladder Network 项目技术路线优化，生态建设方向确立。

4.2019 年 5 月，衔梯网络 Ladder Network 测试网上线，实现以太坊和 ABOS 链等的跨链互联。

5.2019 年 9 月，实现和主流主网如 BTC、ETH、EOS 等链接；衔梯网络整体开源；启动跨链生态大航海计划。

6.2019 年 12 月，衔梯网络 Ladder Network 主网正式上线，启动 BPOS 挖矿机制，并开启节点竞选计划。

7.2020 年 3 月，BAAS 平台建成，提供大量基础 SDK 模块。

8.2020 年 6 月，供应链模块、游戏模块接入 BAAS，共享衔梯网络 Ladder Network 跨链服务。

9.2020 年 7 月，跨链生态大航海计划全面发力。

10.2020 年 9 月，Ladder Network 去中心化交易所 1.0 版本上线，实现跨链资产与信息自由流通，LAD 成为平台流通通证。

11.2020 年 12 月，实现社区节点去中心化自治。

8.治理机构

8.1 基金会设立

作为致力于打造全球最分散、最安全及最大规模的POS跨链网络，衔梯网络 Ladder Network 将设立基金会，基金会致力于衔梯网络 Ladder Network 的开发建设和运营推动，推动项目去中心化、透明化管理，促进开源生态社会的安全和和谐发展，为区块链发展贡献力量。

基金会首期决策委员会由 8 名成员构成，其中团队代表 5 人，早期投资人代表 3 人。期满后由社区投票重新选出。决策委员会任期届满后根据社区内投票评选出 10 个代表，由早期委员会成员根据社区成员贡献度选出 8 名决策委员会核心组成人员。新任成员需通过战略决策委员会成员全票通过，方可通过任职评选。

对于资金使用情况，基金会将会选择国际审计机构进行正规的财务审计，将定期公布审计结果，使投资者、生态参与者和使用者了解各项工作和资金使用的进度。

8.2 委员会职能分布

- 执行委员会

研究和拟定长期短期规划，制定章程和管理制度，制定项目规划和策略方向，协助拓展媒体关系，管理日常运营，负责推动基金会工

作平稳有效进行。

- **运营管理委员会**

根据基金会发展目标，负责项目清晰定位，制定发展策略，把握用户需求，制定运营模式和运营方向。

- **薪酬和人事委员会**

拟定和修改薪酬激励方案，调配机构设置及岗位设置，进行人员的聘请。

- **审计与合规委员会**

负责项目的监测和评估，包括运营审计、财务审计、代码审计及Token 应用审核等工作，保证项目的合规性和支出规范，提高资金使用效率。

9. 免责声明与风险提示

LAD 通证在任何管辖区域内都不构成证券。本白皮书不构成任何类型的招股说明书或要约文件，也不构成对任何司法管辖区证券或招揽投资证券的约。本白皮书不构成或成为任何有关出售建议的意见或

对 LAD 通证（“合作商”）的合作商/供应商提出的购买任何 LAD 通证的任何要约的任何意见的一部分，也不应该全部或部分及其呈现的事实构成任何合同或投资决定的基础或依赖于任何合同或投资决定。任何人都不得就销售和购买 LAD 通证签订任何合同或具有约束力的法律承诺，并且不会在本白皮书的基础上接受加密货币或其他付款方式。任何合作商与您作为购买者之间的任何协议以及有关任何买卖 LAD 通证（本白皮书中提及的）的协议仅受单独文件的约束，该文件中列出了条款和条件（“条款与条件”）。条款和条件与本白皮书有任何不一致之处，以前者为准。

本白皮书中列出的任何信息并没有经过监管机构审查或批准。根据任何司法管辖区的法律，监管要求或规则，也没有或将要采取这样的行动。本白皮书的发布，分发或传播并不意味着已遵守适用法律，监管要求或规则。

- **免责声明**

在适用法律，法规和规则允许的最大范围内，LAD 和/或合作商不承担任何形式的，侵权，合同或其他方面的任何间接，特殊，附带，间接或其他损失（包括但不限于收入或利润的损失，以及使用或数据的丢失），起于您认可或依赖本白皮书或其任何部分而产生或与之有关。

- **风险和不确定性**

LAD 通证的潜在购买者（如本白皮书所述）应仔细考虑并评估与 LAD，合作商及其各自的业务和运营，LAD 通证和首次通证发行相关的所有风险和不确定性，在购买 LAD 通证之前所有信息集都在本白皮书和条款与条件中列出。 如果任何此类风险和不确定因素发展为实际事件，LAD 和/或合作商的业务，财务状况，经营业绩和前景可能会受到重大不利影响。 在这种情况下，您可能会损失 LAD 通证的全部或部分价值。

- **关于前瞻性陈述的警戒性声明**

本白皮书中包含的所有声明，在新闻稿中或在任何可由公众查阅的地方发表的声明以及 LAD 和/或合作商或其各自的负责人，执行团队和代表 LAD 和/或合作商（视情况而定）的员工可能做出的口头声明并非历史事实陈述。

有关 LAD 和/或合作商的财务状况，业务战略，计划和前景以及 LAD 和/或合作商所在行业的未来前景的所有声明均为前瞻性声明。这些前瞻性声明，包括但不限于关于 LAD 和/或合作商的收入和盈利能力，前景，未来计划，其他预期行业趋势以及本白皮书中关于 LAD 和/或合作商讨论的其他事项的声明均不是历史事实，而只是预测。

这些前瞻性声明涉及已知和未知的风险，不确定性和其他因素，可能会导致 LAD 和/或合作商的实际预期结果，业绩或成绩与预期结果，预期的业绩或成绩，表现或这些前瞻性表述暗示。这些因素包括：

（1）政治，社会，经济和股票或加密货币市场状况的变化，以

及 LAD 和/或合作商开展其各自业务和运营的国家的监管环境;

（2）LAD 和/或合作商可能无法执行各自的业务战略和未来计划的风险;

(3)预期增长战略的变化以及 LAD 和/或合作商的预期内部增长;

（4）在与各自的业务和运营有关的情况下，向 LAD 和/或合作商支付的可行性和费用的变化;

（5）LAD 和/或合作商经营其各自业务和运营所需的员工的实用性和薪酬的变化;

（6）LAD 和/或合作商的客户偏好的变化;

(7)LAD 和/或合作商运营的竞争条件的变化以及 LAD 和/或合作商在此类条件下竞争的能力;

（8）LAD 和/或合作商未来资金需求的变化以及满足这些需求的融资和资金的可用性;

（9）战争或恐怖主义行为;

(10)发生影响 LAD 和/或合作商的业务和/或运营的灾难性事件和自然灾害;

（11）LAD 和/或合作商无法控制的其他因素;

（12）与 LAD 和/或合作商及其业务和运营，LAD 通证和 LAD 初始通证销售相关的任何风险和不确定性。

所有由 LAD 和/或合作商或代表 LAD 和/或合作商的人员作出或归属的所有前瞻性陈述均由此类因素明确限制。鉴于可能导致 LAD 和/或合作商的实际预期结果，业绩或成绩与本白皮书前瞻性声明所表达

或暗示的预期有重大差异的风险和不确定因素，不应过度依赖这些陈述。这些前瞻性声明仅适用于自本白皮书的日期起。 LAD，合作方或任何其他人均不代表，保证和/或承诺，LAD 和/或合作方的实际预期结果，业绩或成绩将在前瞻性声明中讨论。

LAD 和/或合作方的实际结果，业绩或成就可能与这些前瞻性陈述中预期的结果有极大的区别。

参考文献：

[1]Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. The honey badger of bft protocols. Technical report, Cryptology ePrint Archive 2016/199, 2016.

[2]Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Ti- mon, and Pieter Wuille. Enabling blockchain innovations with
pegged sidechains. 2014.

[3]Dagher, Gaby G.; Mohler, Jordan; Milojkovic, Matea. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. SUSTAINABLE CITIES AND SOCIETY, 2018, 39, pp. 283-297.

[4]Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In 2014 IEEE Symposium on Security and Privacy, pages 459 – 474. IEEE, 2014.

[5]Gavin Wood. Devp2p wire protocol. https://github.com/ethereum/wiki/wiki/libp2p-Whitepaper, 2014.

[7]Gavin Wood. Yellow paper committee. https://github.com/gavofyork/curly-engine, 2016.

[7]Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II, 2014, pp. 486 – 505.

[8]Laplante, Phillip A.; Amaba, Ben. Blockchain and the Internet of Things in the Industrial Sector. IT PROFESSIONAL, 2018, 20(3), pp.15-18.

[9]L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016, 2016, pp. 17 - 30.

[10]Parity. Parity ethereum client. https://parity.io, 2016.

[11]Petar Maymounkov and David Mazi`eres. Kademlia: A peer-to-peer information system based on the xor metric. In IPTPS ’01 Revised Papers from the First International Workshop on Peer-to-Peer Systems, pages 53 - 65, 2002.

[12]P. Mohassel, S. S. Sadeghian, and N. P. Smart, “Actively Secure Private Function Evaluation,” in Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and

[13]Smetana, Sergiy; Seebold, Christian; Heinz, Volker. Neural network, blockchain, and modular complex system: The evolution of cyber-physical systems for material flow analysis and life cycle assessment. RESOURCES CONSERVATION AND RECYCLING, 2018, 133, pp. 220-232.

[14]S. Micali, K. Ohta, and L. Reyzin, “Accountable-subgroup Multisignatures: Extended Abstract,” in Proceedings of the 8th ACM Conference on Computer and Communications Security, ser. CCS ’01. New York, NY, USA: ACM, 2001, pp. 240 - 254.

[15]Vitalik Buterin. Serenity poc2. 2016.

[16]Vitalik Buterin. Ethereum 2.0 mauve paper. 2016.

[17]Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper, 2013.