# LORA白皮书

**Part1.项目背景**

**1.1 区块链是继 IT、互联网后的新数字技术**

自互联网诞生以来，人类社会的信息传播成本得到极大的降低，信息传播效率的飞跃带来生产力的极大解放。然而传统互联网更关注信息的传输效率，却忽略了信息的确权与归属，导致‘数据裸奔’‘信息无主’等长期性结构性问题。而有些信息具有很强的价值属性，比如汇款转账信息，这些有价值信息的传递需要依赖第三方来“保驾护航”。因此，目前信息的价值传输成本依然高企。

区块链的诞生，带来了解决这个问题的曙光。由于区块链公开透明、难以篡改、不依赖中介机构的特点，区块链可以实现安全、高效、低成本的价值传输。人类有望基于区块链构建起一个可信、可编程的价值传输网络。在价值互联网中，价值传输成本将极大降低，生产力将又一次获得极大解放。区块链独特的优势，如数据的确权使用、价值的高效传输，可以广泛应用于很多行业，比如金融服务、合同契约、慈善公益、物联网等，区块链将在未来改变很多行业的面貌。因此，区块链绝非无足轻重的领域，而是国际上的兵家必争之地。正如 Android 操作系统奠定了智能移动生态的基础一样，区块链正在构筑下一代数字世界的技术根基。而古往今来可见一斑，区块链就好比一个底层的技术构架得以被认知。而接下来则开始走入到应用的阶段。“去中心化”是区块链的核心构架。“公平、公开、公正”是区块链所承载的核心价值观。

核心技术是国之重器。 区块链被认为是继互联网之后的下一个 IT 浪潮，眼下区块链应用在全球范围内正呈现从星火燎原向火爆方向加速发展的势头。

**1.2 区块链发展的瓶颈**

区块链已经发展至 3.0 阶段，具备支持大规模商业应用的可能，但数据处理能力有限，无法满足高频次、大规模应用需要。也就是说底层技术带来的限制，阻碍了上层应用的正常发挥，虽然有美好畅想，实现起来还需要很长时间。具体来讲，究其根本，区块链现存的问题是吞吐量和交易确权速度的问题。

为了解决这一问题，区块链行业在进行以下尝试 : 其一是大区块，即提升每一个区块的储存空间，此方法在比特币中曾有过试用，比特币一个区块大小仅有 1MB 储存空间，在 2017 年年底时 SegWit2x 将区块大小从1MB 提升至 2MB，但出于安全考虑，最终取消 SegWit2x 硬分叉 ; 其二是链下交易，即通过在主链之外构建闪电网络或侧链，以实现交易的链下处理。以太坊正积极推进此类解决方案，提前支付一些以太坊或比特币作为押金，之后在链下通过其他方法来跟其他人进行交易 ; 其三是代理人共识协议，即多人成为超级节点，形成小团体。EOS 在尝试用这种“议会制”共识产生区块，再将区块广播给整个网络，从而达成整个网络的共识。

然而这三种尝试方式都不能完美解决区块链的交易速度，去中心化和安全性的矛盾。LORA公有链正致力于构建一个具备高扩展性与兼容性的下一代区块链基础设施，推动行业从概念验证迈向大规模商业落地。

**1.3 区块链发展前景**

区块链被誉为继蒸汽机、电力与互联网之后的第四次底层技术革命。如果说蒸汽机与电力曾解放了人类的物理生产力，互联网重塑了信息传递方式，那么区块链则作为数字时代构建信任机制的核心引擎，有望重塑全球数字经济的生产关系结构。

在金融领域，尤其是跨境金融业务中，金融机构长期面临对账、清算和结算成本高企、流程繁琐等挑战。区块链技术凭借其“可追溯、不可篡改”的数据特性，能够显著降低机构间对账与争议解决成本，同时加速支付处理效率，为小额跨境交易打开通道。早在2017年12月，招商银行便完成了全球首笔基于区块链的跨境人民币同业清算业务，标志着区块链在金融实际应用中的可行性已初步验证。

区块链的核心价值在于解决数字时代的两大结构性难题：其一，资产流向的可视化；其二，信任机制的低成本构建。与传统经济体系中对实体货币流通“看不见、管不着”的痛点不同，区块链确保了每一次价值流转皆有“链”可循。而在无需信任中介的前提下完成信任确权，更是对现代信用体系的深刻重塑。

正如中国社科院知识产权中心研究员杨延超所言，区块链的最大意义在于构建了匿名网络环境下的信用基础，释放出前所未有的创新潜能。这一技术正加速渗透至医疗健康、教育、公益慈善、社会治理等多个领域。以文化产业为例，过去因复制成本低、维权难度高、举证复杂等问题，知识产权保护长期困扰从业者；而区块链提供的全流程确权与溯源机制，正在根本性重构内容产业的信任基础与商业模式。

综上所述，区块链作为面向未来的通用型技术基础设施，正展现出强劲的发展潜力与跨行业渗透能力，预计将在未来十年深刻影响全球经济格局与生产逻辑。

**Part2.LORA公链**

**2.1 LORA公链系统简介**

LORA是一条专为高并发商业应用设计的多链并行区块链网络，致力于突破现有公链在性能、兼容性和可扩展性上的瓶颈。它基于Tendermint跨链协议，优化了BFT共识机制，构建出一个集分布式存储、智能合约、安全通信于一体的高效底层架构。

相比传统公链，LORA不仅具备不可篡改、点对点传输等基础特性，还通过模块化设计将系统分为Token链、数据链等多个功能子链，并原生兼容以太坊虚拟机（EVM），大幅降低开发者迁移成本。其独有的并行计算架构，显著提升链上事务处理能力，有效缩短响应时间，实现高效稳定的运行环境，适用于DeFi、元宇宙、数字身份等多种高频应用场景。

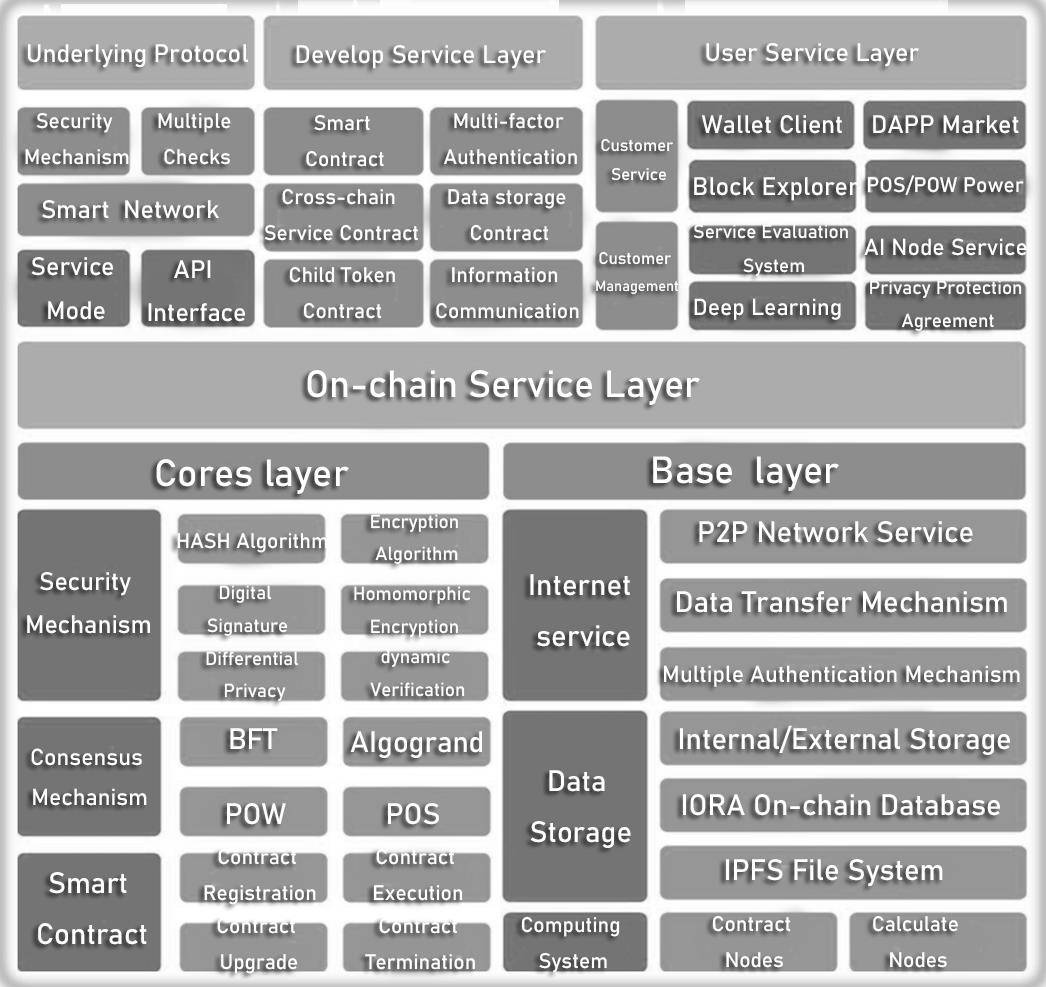
LORA的设计初衷是成为“下一代价值互联网的基础设施”，为全球去中心化应用提供一个更开放、更兼容、更可持续的运行平台。

**2.2 公链架构体系**

LORA针对大流量、高并发和跨区块链间数据、模型来优化建 立底层系统架构。LORA的平稳运行需要一个可靠、安全、可扩展、 易维护的应用系统平台做为支撑。

LORA将区块链系统分为以下几层 ：

1. 用户服务层
2. 开发服务层
3. 链上服务层
4. 底层协议层



**2.3 LORA项目设计理念**

LORA团队将构建企业级区块链应用的分布式、生产级开放生态，致力于推动将区块链技术与数据应用紧密关联起来，充分利用区块链技术的优势，解决应用系统实践中心化系统日益明显的成本与安全保障问题。

LORA采用 Tendermint跨链协议，采用 1+N平行链、静态账本、LRB时空证明、动态存储、多态节点、节点转移、节点淘汰和 POS 共识机制的模式，以商业应用系统需求为前提，提供开源IDE开发环境，构建真正的区块链3.0商业应用新生态。

Token链即公有链的加密通证，是去中心化、基于区块链作为支付技术的数字通证载体。加密数字LORAToken 系统实现了点对点的直接交易，从而避免了高昂的手续费、繁琐的流程等传统中心化支付的问题。所有交易须经过网络节点的认证，并永久记录在基于区块链技术的 Token 链公共分布式账本中。LORAToken 是实现 LORA价值传递最重要的工具。

**2.4 LORA技术特点**

区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了若干网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块，对于普通用户来说它是一个公有账本，记载所有的交易记录，对于开发者来说可以理解为一个分布式的数据库。区块链数据库的特点是去中心化、开放、自治、不可篡改，区块链与去中心化应用息息相关，非常适合为去中心化应用（DAPP）提供存储功能。

LORA的1+N多链结构，其核心本质是公有链+N个子链构成。公有链和子链属于业务逻辑和数据分区处理，不是物理隔离的公有链、私有链的区分。公链只有一条，子链理论上可以有无数条，而每条子链都可以运行一个或多个DAPP系统。子链是用最新的分片存储技术，支持多个交易并行处理，交易完成后，异步写入公链交易账本。是解决网络拥堵的最佳手段之一。

**2.5 Distributed Data System公链技术构架**

**2.5.1协议层**

所谓的协议层，就是指区块链最底层的技术。这个层次通常是一个完整的区块链产品，它维护着网络节点，仅提供 Api 供调用。通常官方会提供简单的客户端 ( 通称为钱包 )，这个客户端钱包只能建立地址、验证签名、转账支付、查看余额等。这个层次是一切的基础，构建了网络环境、搭建了交易信道、制定了节点奖励规则。 从技术来说，协议层主要包括网络编程、分布式算法、加密签名、数据存储技术等 4 个方面，其中网络编程能力是选择编程语言的主要考虑因素，因为分布式算法基本上属于业务逻辑上的实现，什么语言都可以做到，加密签名技术是直接简单的使用，数据库技术也主要在使用层面，只有点对点网络的实现和并发处理才是开发的难点。分布式算法、加密签名等都要在实现点对点网络的过程中加以使用。

**2.5.2 兼容 SOLIDITY 虚拟机拓展层**

SOLIDITY 扩展层智能合约是基于以太坊 EVM 的“可编程合约”，或者叫做“合约智能化”，其中的“智能”是执行上的智能，也就是说达到某个条件，合约自动执行，比如自动转移证券、自动付款等。扩展层使用的技术基本没有限制，分布式存储、机器学习、VR、物联网、大数据等等，都可以使用。编程语言的选择上，可以更加自由，因为可以与协议层完全分离，编程语言也可以与协议层使用的开发语言不相同。在开发上，除了在交易时与协议层进行交互之外，其他时候尽量不要与协议层的开发混在一起。这个层面与应用层更加接近，也可以理解为 B/S 架构的产品中的服务端(Server)。这样不仅在架构设计上更加科学，让区块链数据更小，网络更独立，同时也可以保证扩展层开发不受约束。

**2.5.3 应用层**

应用层是普通人可以真正直接使用的产品，也可以理解为 B/S 架构的产品中的浏览器端 (Browser)。这个层面可以让区块链技术快速走进寻常百姓，服务于大众。大家使用的各类轻钱包 ( 客户端 )，应该算作应用层最简单、最典型的应用。编程实现 :C++、JLORscript、Python、Go 等。

**2.5.4 共识层**

此层包含共识算法以及共识机制，能让高度分散的节点在去中心化的区块链网络中高效地针对区块数据的有效性达成共识，是区块链的核心技术之一，也是社群治理的有效机制。

LORA采用蜂巢节点网络和轮循中的混合共识机制，最终可实现的扩容效果将优于闪电网络。公链底层采用Token链+平行链的多层结构，满足 Web3.0时期 DAPP应用矩阵的高并发和高交互需求。Token链是基于POS+BFT最优算法、多链异构数据激励层和重要性证明机制搭建的平行链，数据链共识层是由按照不同业务需求的N条不同类型的共识机制共同组成的平行链，属于1+N类型的多链结构，从而解决了公链系统的性能和扩容问题。

Token链和多层数据链根据业务逻辑和数据存储的不同分工和类型进行的分链处理，相互

之间通过SEC网关实现通讯交互。多链结构改变了传统区块链单链式结构存在的技术瓶颈和不

可能三角缺陷，极大提高交易确认速度，大大减少公链账本的资源占据，满足大规模数据响应

需求。

**2.5.4.1 验证人**

在经典的拜占庭容错算法中，每个节点有相同的权重。在Tendermint，节点有着不同数量（非负）的 投票权，而那些拥有相当数量投票权的节点称之为 验证人。验证人通过广播加密签名、投票或者对下一个区块表决同意来参与共识协议。

验证者的投票权是一开始就确定好了，或者根据应用程序由区块链来决定修改投票权。例如，在像Midas 枢纽的权益证明应用里，投票权可由绑定为押金的代币数量来决定。例如 ：像⅔和⅓这样的分数指的是占总投票权的分数，而不是总验证人，除非所有验证人拥有相同权重。而>⅔ 的意思是”超过⅔ “，≥⅓则是”⅓或者更多”的意思。

**2.5.4.2 Tendermint 共识**

Tendermint是部分同步运作的拜占庭容错共识协议，这种协议源自DLS共识算法。

Tendermint以简易性、高性能以及分叉问责制而著称。协议要求这组验证人固定且被熟知，并且每个验证人都有其公钥验证身份。这些验证人试图同时在一个区块上达成共识，这些区块是一系列的交易记录。每个区块的共识轮流进行，每一轮都会有个领头人，或者提议人，由他们来发起区块。之后验证人分阶段对是否接受该区块，或者是否进入下一轮做出投票。每轮的提议人会从验证人顺序列表中按照其投票权比例来选择确定。

Tendermint 采用了使用大多数投票（超过三分之二）和锁定机制的最优拜占庭容错，来确保其安全性。这类似于POS授权投票共识机制，而禁止这些能够保证：蓄意破坏者想要造成安全性问题，须有三分之一以上的投票权，并提交超过两份以上的值。

如果有一组验证人成功破坏了安全性，或者曾试图这么做，他们会被协议识别。 协议包括

对有冲突的区块进行投票和广播那些有问题的投票。

除了其超强的安全性外，Tendermint还具备杰出的性能 ，并支持 RUST 高性能编程语

言写入底层智能合约。以商用型云平台为例，Tendermint共识以分布在五大洲七个数据中

心的64位节点为基准，其每秒可以处理成千上万笔交易，订单提交延迟时间为1-2秒。而值

得关注的是，即使是在极其恶劣的敌对环境中，比如验证人崩溃了或者是广播恶意破坏的投

票，也能维持这种每秒超过千笔交易的较高性能。

**2.5.5 激励层**

此层使用拓展型链存储技术，将私钥所有者签名和基础数据存储在拓展链上。用户上传大型数据时，在链式数据存储网络自动搜寻节点，形成一种新型的点对点传输网络，在保证数据完整性的基础上进行数据确权，从而进一步提升了存储和访问的安全性。

**2.5.6 扩展 P2P 网络协议**

可扩展性的提出，为了解决区块链彼此不兼容的信息孤岛问题。首先，我们认为升级、分叉是网络进化的有效途径之一，分叉后形成一个主链和若干子链。主链和子链从技术角度看完全对等，只是基于小区的共识给它们设置不同的标识。每一条子链可根据不同的商业应用做适度化定制，通过在子链之间构建 VEP，其工作方式类似于网关，子链之间通过VEP 可交互信息和交换价值。通过这样的协作，可形成多应用的区块链生态。不仅如此，非区块链的在线数据也将纳入LORA生态，辅以智能合约，可对现实世界中的事件做出回应。

**2.5.7 同构跨链机制**

经典的区块链网络，如比特币网络、以太坊等都是采用单链结构，所有的事务和交易都是在一条链上进行。单链结构的优点是交易和共识流程比较简单，在区块链发展早期能够很好地满足用户需求。 但是随着区块链技术的发展和市场对区块链的需求不断增强，单链架构逐渐暴露出很多无法解决的痛点 : 整体吞吐量和性能存在瓶颈 : 比特币只有 7TPS 以及需要 6 个区块的确认机制，以太坊出块间隔也需要 10-20 秒，这些都严重阻碍了日益增长的区块链业务发展需求。

链内业务相互干扰 : 单链架构很容易由于个别业务的繁忙而造成整个系统拥堵，很多正常的交易都得不到及时处理和确认 ; 封闭的网络结构 : 无法实现不同链之间的跨链交互，无法满足多平台之间的业务交互需求。为了克服单链结构的局限性，LORA采取基于Tendermint共识的多链并行结构。

并行多主链机制:LORA可以引出多条主链，每条主链负责专门的业务领域，相互独立

又相互关联，主链之间耦合比较少，发挥并行处理的优势，对过程性区块，引入封存策略，

超期数据进行历史归档，提升系统处理效率。多链并行解决不同业务、不同形态链的功能

支持，同时提高性能。跨链共识实现数据审计和价值流通。由于现实世界的不同业务具有各种各样的特殊性，如前所述单链结构是很难完美的支撑多种异构业务的。在 LORA中，每一条链只服务于最小功能集合的业务，每个内聚型的业务运行在单独的链，这样既能做到有效的安也能实现计算和资源的有效利用最大价值，不同链之间通过跨链协议进行交互，实现价值交换。

LORA多链结构能满足现实世界各种不同类型的复杂业务需求，不同类型不同特性的业务在不同的子链运行，比如计算密集型、IO 密集型、混合型分别在不同链上良好地运行 ; 不同安全等级要求的业务也可以在不同层次运行，比领域，相互独立又相互关联，主链之间耦合比较少，发挥并行处理的优势，对过程如针对银行的业务需求，在数据的保密和安全以及事务的强一致性会有更高的要求，因此可以隔离在最安全的一层。

**2.5.8 异构 /中继柔性跨链机制**

LORA通过一系列有针对性的协同智能合约，及异步通讯、状态机和哈希锁定技术，实现一套通用的柔性跨链机制，打通各个区块链系统的通信瓶颈，让各种数字资产互联互通，适当的跨链协同机制有效保证内部各条并行链之间，以及与其他公链之间的共识和价值的有效和可靠传递。

柔性跨链包括两个部分 : 一个是 LORA与外部链的互联互通，LORA与其他链通过一个公共

的智能合约来实现，适配其他链的特征，基于状态机的异步操作，完成与其他链的交互。另外

一个就是基于 LORA平台的其他链之间的互通。LORA也提供一个更复杂的智能合约来支持其他链之间的互联互通，由于要支持两种不同类型的其他链，智能合约结合中继链完成不同类型链

的互联互通。

跨链交易是区块链网络之间的去信任消息，这是一个关键的基础设施组件，用于链路间通信。跨链交易最初是在源块上创建的，然后在最终到达目标区块链之前通过桥梁和连接网络进行处理和转发。如前所述，跨链交易的创建者必须使用LRB作为通信支付交易费用，从而激励每个交叉点的参与者。LORA跨链通信通过适配器来实现，适配器会创建一个兼容的区块头。

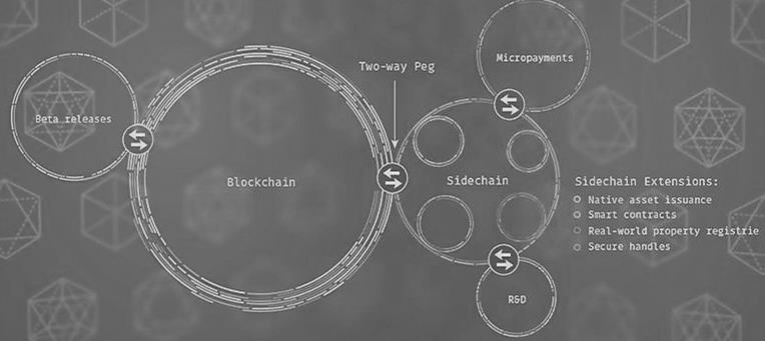
LORA设计了层级侧链机制来解决跨链交易匹配不同链区块生成速度的问题，根据链的区块生成

速度把链划分到不同的层，然后为每一层提供一个专有的适配链或者适配模块来带动同层的跨

链交易。

**2.5.9 LORA 侧链结构**

**側鏈（SideChain）**



楔入式侧链技术（ Pegged Sidechains），它能够实现数字资产在多个区块链间的转移，这就意味着用户们在使用其已有资产和现有应用的情况下，就可访问新的加密货币系统。

侧链是一种特殊的区块链，它使用“SPV 楔入”技术实现与其他区块链之间的资产转移，这使得用户能用已有的资产来使用新的加密货币系统。人们不必再担心激励层Token难于采纳创新和适应新需求，只要创造一个侧链，然后对接到原有系统中即可，通过继承和复用原生区块链，还避免了新货币的流动性短缺和市场波动等问题。并且由于侧链是一个独立的、相对隔离的系统，侧链中出现的严重问题只会影响侧链本身，这极大地降低了系统风险和成本。

**侧链起源：**

侧链（SideChains）实质上不是特指某个区块链，而是指遵守侧链协议的所有区块链，该

名词是相对于原生主链来说的。

**侧链协议是指：**

可以让主链Token安全地从原生主链转移到其他区块链，又可以从其他区块链安全地返回原

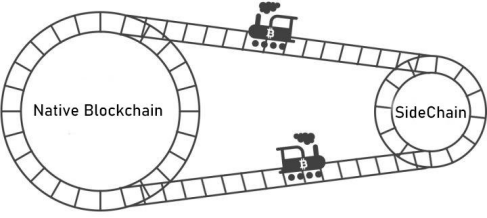
生主链的一种协议。

显然，只需符合侧链协议，所有现存的区块链，如以太坊等竞争区块链都可以成为侧链。

侧链协议具有重大意义，它意味着原生Token不仅可以在原生区块链上流通，还可以在其他不同类型的区块链上流通，其应用范围和应用前景会更加广泛；有创意的人们会研发出各种应用让侧链协议与原生主链对接，使得基于原生链的地位越牢固。

**楔侧链协议：**

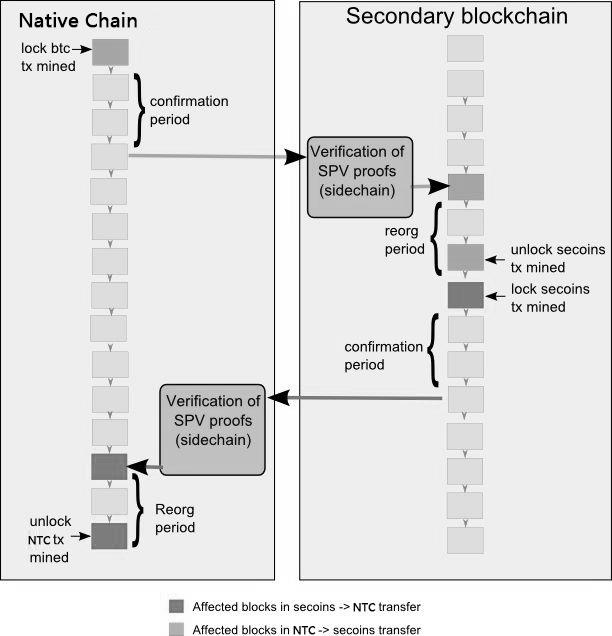
侧链协议目的是实现双向锚定（Two-Way Peg），使得原生Token可以在主链和侧链中互转（图）。



**双向锚定分为以下几个阶段：**

发送锁定交易，把 原生交易数据 锁定在主链上。

由原生通证持有者操作，发送一个特殊交易，把Token锁定在区块链上。



双向锚定示意图

**楔侧链协议：**

➢ 等待一个确认期

确认期的作用是等待锁定交易被更多区块确认，可防止假冒锁定交易和拒绝服攻击，典型

的等待时间是1-2天。

➢ 在侧链上赎回原生Token

确认期结束后，用户在侧链上创建一个交易花掉锁定交易的输出，并且提供一个SPV工作

量证明，输出到自己在侧链上的地址中去。该交易称为赎回交易，SPV工作量证明是指赎回交

易所在区块的工作量证明。

➢ 等待一个竞争期

竞争期的作用是防止双花。在此期间（1）赎回交易不会被打包到区块（2）新传输到侧链的比特币不能使用（3）如果有工作量更大的工作证明出现，即该赎回交易包括了比特币主链更

大难度的SPV证明，则上一个赎回交易将被替换。

**侧链的作用:**

侧链可以让区块链实现更好的表现和隐私保护。它们也可以扩展来支持各种资产，例如股票、债券、真实世界或虚拟世界中的货币，也可以增加智能合约、安全处理和真实世界财产登记注册之类的功能。侧链还可以拥有用于微支付的其它侧链。它们可用于未来侧链的预发布版本的实验，或者比特币测试版本的实验。

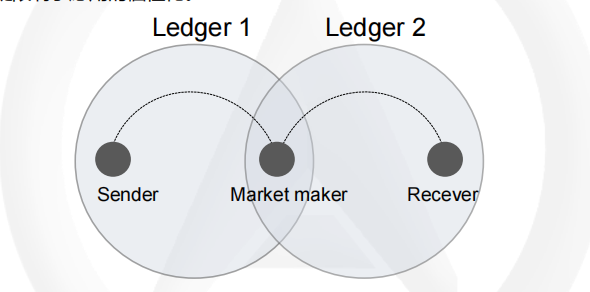
**技术现状：完整脚本VS侧链**

大型公有链系统为人称道的一个设计上的亮点就是脚本引擎。基于完备的脚本引擎，不但可以实现普通的转账功能，还可以实现多方签名、抵押担保、博彩数据等智能合约应用。 但是出于安全和当时实现难度的考虑，第一代区块链系统的脚本系统设计的较为简陋，做了非常多的限制，譬如并不支持循环、脚本长度受限、只支持几种标准的的交易类型。

以以太坊为代表的第二代区块链系统为例，其最大特色是构建了扩展智能合约层，极大完善了脚本引擎的功能，加入了读取区块链、计费、跳转等新指令，还解除了栈内存、函数调用深度以及脚本长度限制等。其脚本语言基本达到了图灵完备，利用这样的脚本，开发者可以实现几乎任何可以用数学方式表述的功能。

自以太坊以来，扩展脚本成为了一种实现去中心化开发平台的流行方式，但该方式的一个很大的缺点就是，应用代码本身及应用产生的数据都存在同一个区块链中，造成了区块链的快速膨胀。以太坊试图通过优化和压缩区块和交易本身来延缓这种膨胀，也只是一种治标不治本的方法。

此外，基于脚本实现的应用之间是共享同一个账本的，像区块产生时间等参数是无法被定制的，这无疑限制了应用的个性化。



侧链机制是通过另一个维度实现扩展性的，每个侧链运行在不同的分布式节点网络中，有独立的受众、投资人和开发团队。这种天然的分片解决方案，不但解决了区块链的膨胀问题，而且每个应用都拥有一套个性化的账本，其共识机制、区块参数、交易类型都是可以被定制的，所以我们认为侧链与完备交易脚本相比，是一种成本更低、更加灵活、也更加易用的解决方案。

**2.5.10 灵活支持商业应用**

LORA通过两方面来实现易用性。一是提供区块链即服务系统 BaaS (BlockchainasaService)

来降低企业及个人的使用门坎。通过网络分叉、数据定制、智能合约发布和升级、资产交易监

控等并辅以可视化功能，让区块链应用变得简单易用。并提供多种语言支持，从 Lua、C++ 到

JLOR，让不同平台的开发者都可以便捷地开发。

**2.5.11 开源 Graphene 技术**

针对以太坊低效的传输速度及公链之间存在的信息孤岛，各公链都提出了自己的扩容和跨链方案，但实际落地却不甚理想。很多公链都没有如期上线，2018 年最火的公链 EOS 当时号称 TPS可达百万，可实际运行中的TPS只有 3000 左右。但是LORA实际运行的 TPS达到了39000+，特别是在将来可以成倍增长，LORA是怎么做到的?LORA基于优秀的开源 Graphene 技术和 BFT 优化算法，把对交易行为的确认转变为对算法证明的确认，因此理论上能提升 20倍效率，能直接从 Graphene 继承成熟的架构、性能等技术优势。Graphene 主要的技术优势包括 : 能支持 10,000+TPS 的交易吞吐能力，每笔交易确认时延平均可达秒级。

**2.5.12 分片技术**

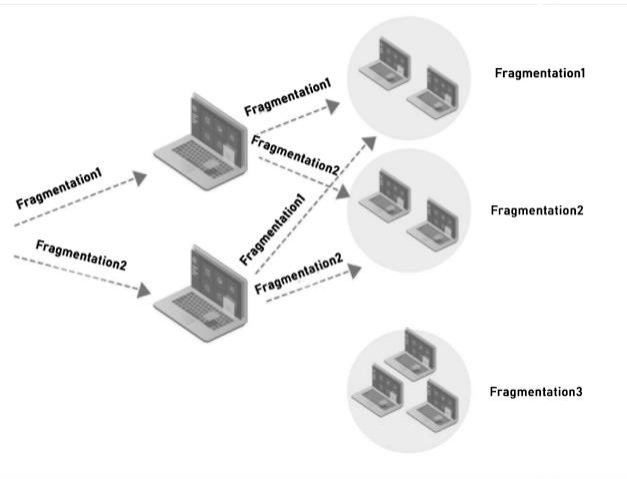
LORA引入了 (Sharding) 分片技术，支持水平扩展，采用网络分片和交易分片相结合的分

片技术 ; 同时提供 BaaS(BlockchainasaService) 服务，为开发者提供丰富的 BaaSAPI、数据交易API、原生 API开发区块链应用。

LORA通过采用 POS 共识协议，结合先进的开源 Graphene 方案和分片技术，实现了扩容

和跨链目标，在目前大多数运行环境中TPS达到了39000+。

LORA提供了一个先进稳定的跨链底层公链，物联网和SWAP是LORA上的首批应用。



**Part3.LORA技术与网络的安全防护**

**3.1 区块链本身具备的安全优势**

如今黑客可以破坏整个网络、篡改数据或诱导粗心的用户落入安全陷阱。他们窃取盗用身份信息，并通过对中心化数据库的攻击及单点故障引发其他安全威胁。但区块链技术中的数据存储和共享数据的模式，与目前信息安全是截然不同的做法。比特币和以太坊都使用相同的密码学技术来保障安全交易，但现在也能够作为一种防范安全攻击和安全威胁的工具。区块链在信息安全上的的优势主要在于以下几个方面 :

· 利用高冗余的数据库保障信息的数据完整性

· 利用密码学原理进行数据验证，保证不可篡改

· 权限管理方面，运用了多私钥规则进行访问权限控制

· 区块链上的交易数据全部都附有交易者的数字签名，不可伪造。

· 利用区块链的安全优势可以进行多重安全应用的开发。

由MIT开发的CertCoin可能是第一个应用基于区块链的 PKI。PKI 是一种常见形式的公钥密码可以用来保护邮件，消息应用，网站和其他形式的通讯。然而由于多数 PKI 接口需要依赖中心化的，受信任的第三方认证机构(CA)来发行、吊销、和为每个参与者保存钥匙对，黑客能够通过冒用用户的身份进入加密通讯中获取信息。而 CertCoin 移除了中心化的权利机构，使用区块链作为分布式账本分发公钥，能够有效降低黑客单点侵入的风险。

而在认证领域，同样也有很多例子，如公政通Factom系统。它基于区块链建立链式结构的存储，将认证分解成存在性证明、过程性证明和可审计证明三部分。对于任何数字资产的认证处理，都可以按照这三个步骤实现数据记录的安全性和监督合规。

**3.2 LORA安全防护**

**3.2.1 以身份验证保护边界设备安全**

正如 IT 关注数据和连接向“智能”边界设备的迁移，安全同样关心这种转变。毕竟，网络的扩展可能会提升IT 效率、生产力并降低耗电量，但也给 CISO、CIO 和整个公司带来了安全挑战。很多公司因而寻求应用区块链来保护 IoT 及工业 IoT(IIoT) 设备安全的方法——因为区块链技术可增强身份验证，改善数据溯源和流动性，并辅助记录管理。

**3.2.2 提升机密性和数据完整性**

尽管区块链最初创建时是没有特定的访问控制机制的 ( 源于其公开分发的属性 )，有些区块链实现如今却在解决调制解调器密性和访问控制问题。在当今数据极易被篡改或伪造的时代，确保调制解调器密性和完整性问题无疑是巨大的挑战。但区块链数据的完全加密特质确保了这些数据不会被非授权方染指，但又仍具有流动性 ( 中间人攻击几乎没有成功的可能 )。

这种数据完整性也扩展到了IoT和IIoT。 比如说，IBM就在其WatsonIoT平台上提供了以私有区块链账本管理IoT数据的选项，该功能已集成到了IBM的云服务中。爱立信的区块链数据完整性服务，可为在通用电气司 PredixPaaS平台上工作的App开发人员提供完全可审计、符合规定且可信的数据。

**3.2.3 保护隐私消息**

LORA正用区块链保护实时聊天工具和社交媒体上流转的隐私信息。WhatsApp和iMessage之类App所用端到端加密不同，LORA使用区块链来保护用户的元数据。因为元数据是账本中随机分发，不存在单一的收集点，所以不会被黑。

**Part4.LORA优势介绍**

**4.1 LORA优势**

**4.1.1 技术优势**

LORA是一个面向大数据时代的区块链数据价值生态体系，其核心目标是建立一个可以高效、安全、激励正向强化的数据交换与数据价值挖掘的区块链网络。当前数据交易中最为显著的四大痛点分别是:数据资源浪费、数据孤岛、数据沉淀与数据供需不匹配。而LORA通过构建一个需求导向、奖励数据贡献、分包实现数据结构化的社群网络，打造一个安全、高效、可溯源、无数据沉淀、可再深度开发的数据交易平台，通过数据竞赛和数据去中心化交易来系统化地解决上述痛点。结合区块链网络与数据价值发掘、交换的需求，LORA的构架设计遵循如下基本原则 :

✓ 交易可信事务历史记录进入区块链并永久存证，交易双方低成本信任交易网络，这要求网络兼具可靠性与私密性，同时规避数据沉淀等中介问题。

✓ 激励兼容经济体系设计促进网络节点发布数据，基于数据开发衍生价值发掘功能，同时参与整个生态开发促进数据价值发掘、交换成本不断下降。

✓ 精细化交易模式通过网络机制设计促进数据资产交易更趋性细化。

✓ 市场化数据定价通过网络机制设计保证市场化数据定价更细致化。

✓ 支持高并发交易支持高并发量数据交换，实验室网络环境可达百万级，实际网络环境可达 39523TPS，成为未来海量人工智能、物联网、机器人进行大规模数据采集、交换、边缘计算结果交换等能力的基础设施。

✓ 支持数据质量验证支持对数据进行采样、交叉比对、格式比对、类型识别、范围识别等自动化验证手段，在保障交易安全的同时，默认提供多种数据质量验证的能力设置。

✓ 支持衍生数据服务支持对数据进行可编程模型计算的功能，支持开发者采用通用语言编制更复杂的数据分析工具并接入LORA，支持接入预言机 (Oracle) 网络提升智能合约功能范围。

✓ 支持跨链区块链服务支持在数据存储、计算能力方面具有成熟解决方案的区块链服务接入

**4.1.2 提升、替代 PKI**

公钥基础设施 (PKI) 是保护电子邮件、消息应用、网站和其他通信形式的公钥加密体制。然而，大多数 PKI实现依赖中心化的第三方证书颁发机构 (CA) 来颁发、撤销和存储密钥对，这就给网络罪犯留下了窥探加密通信和假冒身份的机会。而在区块链上发布密钥则在理论上可杜绝虚假密钥传播，并可令应用具备验证通信对象身份的功能。

LORA是首个基于区块链的 PKI 实现。该项目整体摒弃了中心证书颁发机构，使用区块链作为域名及其公钥的分发账本。另外，LORA还提供不带单点故障的，可审计的公开 PKI。LORA区块链技术，我们就可以用公民生成的身份来签名交易了。

**4.1.3 网络层访问控制**

LORA公有链允许节点自由进出网络，且区块链的网络层没有登记用户身份。金融行业的风险和安全性相对更高，未登记身份的节点自由进出网络为系统安全带来很多不可控性。

LORA区块链技术在金融行业应用时，应结合业务需求，分析必要使用公有链，并登记网络中节点的身份。此外，还应采用VPN专网、防火墙、物理隔离等技术对节点，特别是矿工节点的物理网络和主机进行保护。

**4.1.4 LORA 网络传输安全**

在LORA的网络传输的安全性更多的体现在是否有良好的对抗中间人攻击的能力上。

中间人攻击 ( 英语 :Man-in-the-middleattack，缩写 :MITM) 是指攻击者与通讯的两端分别创建独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。

安全的数字钱包需要能够对终端里面全部的数字证书的合法性进行扫描、对网络传输过程中的代理设置进行检查并能够保障基础的网络通讯环境的安全性。

**4.1.5 高吞吐量**

区块链的本质是一种分布式共享记账的技术，其分布式特征主要体现在分布式一致性而非分布式并发处理。例如比特币网络每秒只能处理 7 个交易，以太坊每秒处理15个交易。

当前所有的公有链网络都面临系统的扩展性问题，为保证数据的一致性，防止拜占庭将军

问题，某些特定环节只能串行执行，而无法并行。通过长期的测试与优化实践，AurumOxProtocol 的 BOE 技术能让 AurumOxProtocol 可以在链外直接多次、高频、双向地通过轧差方式实现瞬间确认，AurumOxProtocol 拥有全球顶尖并发速度，每秒可处理39000笔交易，比EOS快10倍以上, 与现有的区块链系统相比，AurumOxProtocol有更快更稳定的交易确认，并且提供够足够的灵活性设计。AurumOxProtocol 的 BOE技术让处理性能已经能满足万级 TPS 的需求。如果再引入Off-Chain 等机制，还能进一步大幅提高交易吞吐量。

**4.2 LORA技术分析**

以区块链的思路去研发企业应用，必须跳出区块链现有的框架设定，从底层架构入手，以

企业应用需求为导向，不用过于关注现有的公有链、联盟链等基础概念的界限划分，大胆突破

创新改革，将区块链技术优质特性与企业应用结合，方能从根本上解决问题。

**4.2.1 LORA技术深度剖析**

LORA将集多种前沿区块链技术和自主研发的独家技术架构于一身，目标是打造大型商业

数据应用系统，未来区块链技术的先驱者和引领者代表。LORA使用了1+N多链结构、POS共识、CSL账本与动态存储技术、多态节点、多共识并行机制、安全沙箱机制、国产化IDE等多种前沿技术内涵。

**4.2.2 1+N平行跨链结构**

LORA的平行跨链结构，其核心本质是公有链+平行链+子链构成。公有链和子链属于业务逻辑和数据分区处理，不是物理隔离的公有链、私有链的区分。公链只有一条，平行链和子链理论上可以有无数条，而每条链都可以运行一个或多个DAPP系统。平行链用最新的分片存储技术，支持多个交易并行处理，交易完成后，异步写入公链交易账本，是解决网络拥堵的最佳手段之一。

**4.2.3 DAG(有向无环图）**

这是LORA基础数据结构的重要技术之一，DAG改变了传统区块链式结构的技术瓶颈和缺陷，可有效提高交易确认速度，减少公链账本占据资源。 LORA采用Chain结构+DAG结构兼容的方式，适用于公链和子链。

**4.2.4 CSL账本与动态存储技术**

CSL即Classified Static Ledger(分类静态账本），将LORA账本分成资产账本、交易账本、应用账本、日志账本等不同类型。公链和子链均拥有不同的账本，其中资产账本、交易账本、日志账本为不可篡改的数据，应用账本可根据POS等共识机制完成更新、升级（即动态存储）。

**4.2.5 数据层存储技术**

账本存储技术可考虑采用类IPFS分布式文件系统方式实现，IPFS是集合多种前沿互联网技术的下一代分布式存储和共享技术，核心是内容可寻址的对等超媒体分发协议，它在IPFS节点（LORA数据节点）中构成分布式文件系统。

IPFS通过维护分布式哈希表来实现对LORA账本的统一存储和分发，这种基于点对点的超媒体协议，可以让LORA网络更快、更安全、更开放。IPFS支持高并发、大规模同时执行多种交易，然后通过共识更新到资产账本和日志账本。

**4.2.6 POS股权证明机制**

POW是基于链的共识，POS是基于块的共识，两者如何结合，有待深入研究，就目前看，最适合的可能是POS。但要实现大规模商业应用，还有待改进。数据行业的主链，即使只是处理一些小数据流，也需要高IO的操作，如果采用POS机制，节点的计算能力不是考虑的瓶颈，网络的承载能力往往反而成为了瓶颈，如果节点的带宽上下行都是100M（bit/s），如果一笔交易的数据控制在100个字节，考虑到接收与同步，需要双倍的数据，每秒能承载100\*1024\*1024/100/16=65536笔，1G的带宽是65万笔/秒，10G的带宽是650万笔/秒。目前大数据中心最大吞吐量是万兆级，因此，采用POS机制，理论上能实现百万级别的TPS。

**4.2.7 多态节点**

根据跨多链架构、CSL账本、LORA技术的设计要求，在LORA网络中采用多态节点的方式，可以有效地快速完成区块交易共识，降低成本费用。多态节点机制将LORA网络的节点分为共识节点、数据节点、普通节点。

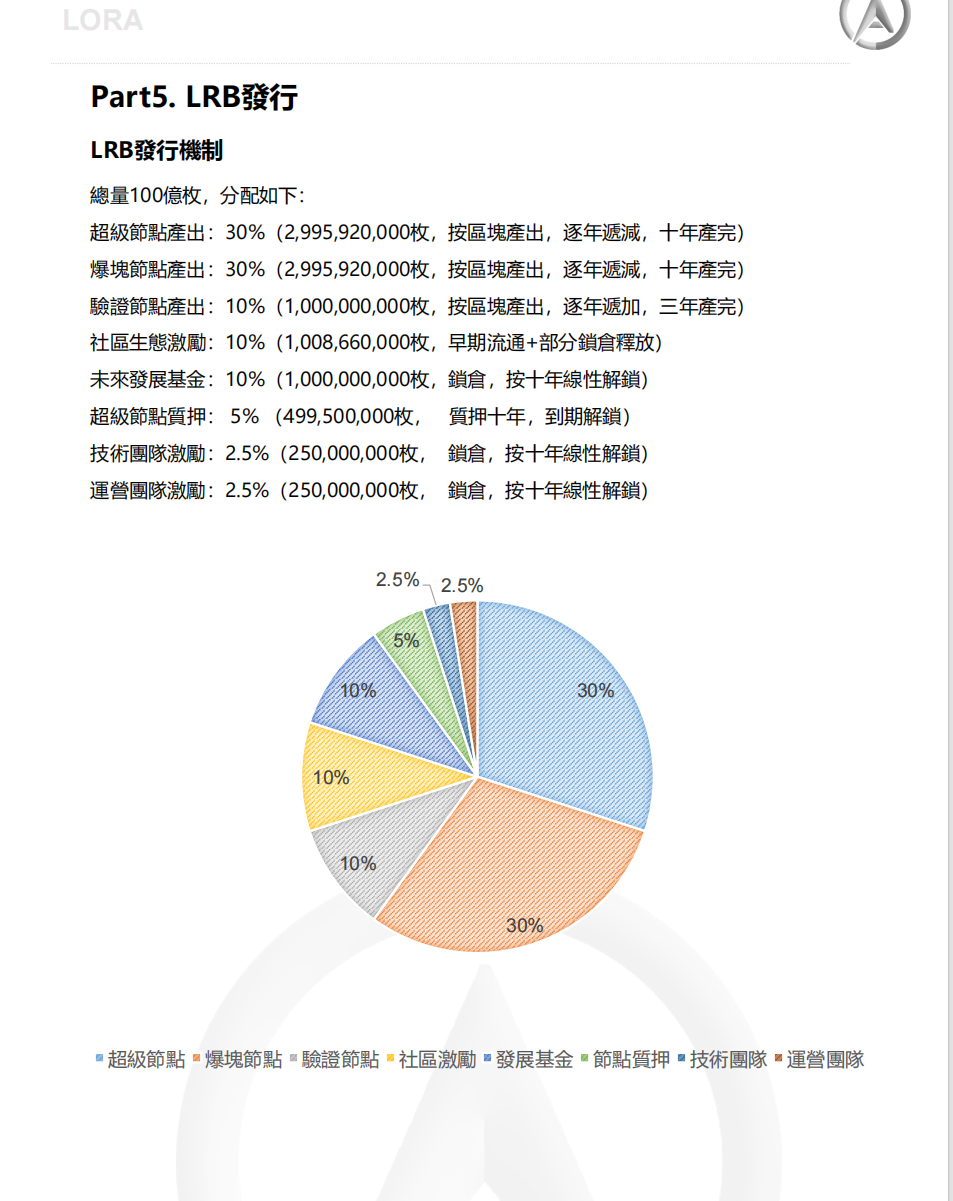
**4.2.8 闪电网络**

考虑到普通用户节点的效能问题，高速公链若要支持百万TPS级别，那么在使用POS的机制上，需要建立相对独立的网络模型或者通道，譬如1+N多链结构。主链上面要承载尽量多的数据种类和数据数量，为保证互通性，统一主链代币互通，但不同数据的内部每笔交易，需建立单独网络模型，如可路由的闪电网络。

譬如，链上运行一款区块链游戏，如果每一笔操作都进行交易的话，会造成网络的负担；而将每一组行为做成多通道，最开始发起一笔交易，结束后再发起一笔交易，中间部分由中间件快速处理。因此，在主链上只处理头和尾的两笔交易数据，剩余的工作交由平行链或子链进行，类似的这种模式会是一个极好的处理模式。闪电网络本身能处理十万级别的交易量，而平行链的承载是十万级别，主链的吞吐量在1+N多链结构下理论可达百万TPS。

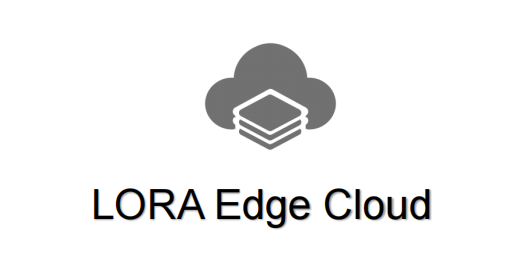
**4.2.9 LORA代码层架构设计**

LORA代码层设计主要分为：共识客户端、安全沙箱、状态机、LORA服务节点、TDataBase系统、LORAAPI、LORAScan Brower、LORAWallet、Dapp Client、LORAGateWay、UBMiddleWare 、LORAStudio、LORAOnline、LORASDK、LORAModule List等多种应用组件。



**Part6.LORA全加密生态系统**

**◆ LORA边缘云**



LORA边缘云包含区块链、神经网络引擎、人工智能深度学习和物联网技术，融合云计算、雾计算、边缘计算三大技术框架，构建出一个智能、自治、安全的边缘数字生态系统。边缘云的设计旨在将计算和存储资源从中心数据中心推向网络边缘，以支持低延迟的本地处理和智能决策，特别适用于对实时性要求极高的IoT场景。

LORA边缘云的区块链支系由以下三部分构成：

* LORA Chain —— 提供去中心化计算与存储基础设施，作为整个生态的核心主链，承载治理与价值传输职能；
* Distributed IOT —— 面向物联网领域的底层区块链框架，提供设备标识、安全通信、数据确权与设备互操作标准；
* Distributed AI —— 面向私域人工智能数据处理的区块链模块，实现AI模型的去中心化训练、验证和部署，提升数据隐私性、安全性与使用效率。

该边缘云系统实现从链上数据采集、加密处理、分布式训练到结果回传的完整闭环，极大拓展了区块链在边缘智能与物联网领域的落地空间。

**◆ LORA数据价值网络（L-DVN）**

LORA数据价值网络（LORA Data Value Network，简称L-DVN）是构建在LORA主链与子链结构之上的去中心化数据流通与定价平台，旨在解决数据供需错配、价值沉淀和确权难题。

该网络基于以下核心组件：

* 数据确权机制：借助区块链的不可篡改特性，对数据源与数据拥有者进行确权认证，防止数据被篡改、盗用；
* 智能合约定价模型：允许供需双方设定算法定价逻辑，基于数据质量、稀缺性、实时性等因素自动匹配价格；
* 激励机制：数据提供者可通过上传高质量数据获得LORA Token奖励，同时可选择是否开放AI训练使用；
* 数据验证模块：引入AI模型对数据进行格式、类型、范围等多重比对校验，保障数据可用性与安全性。

L-DVN作为LORA生态的数据中枢，将支撑物联网设备、金融系统、AI平台等上层应用的数据需求，构建一个可拓展的“数据即资产”网络。

**◆ LORA多链协同生态系统**

为突破单链架构的性能与兼容性瓶颈，LORA设计了“1+N”多链架构，通过主链+多子链的结构实现业务并发处理与数据隔离，并辅以灵活的跨链机制，实现生态模块之间的高效协同。

主要特性包括：

* 同构跨链：适用于LORA生态内部链（如LORA主链与AI子链之间）之间的数据与资产自由流通；
* 异构跨链：通过中继机制与智能合约适配，支持与Ethereum、Polkadot等主流链之间的互操作性；
* 层级侧链：将业务特性强烈差异的模块分配至不同的子链，如游戏链、医疗链、供应链等，互不干扰，提高系统处理能力；
* 安全沙箱机制：每条子链运行在逻辑隔离的执行环境中，支持个性化共识机制与运行逻辑，降低整体风险。

通过多链协同，LORA可以灵活扩展各类Web3场景，从元宇宙资产到金融结算，从AI训练到智能制造，构建跨场景、跨行业的通用型区块链基础设施。

**◆ LORA去中心化身份与隐私网络（L-DID）**

随着数据主权意识增强，LORA引入去中心化身份系统（Decentralized Identity, DID），为用户在数据生态中提供唯一、可验证且私密的身份凭证。

功能亮点包括：

* 链上身份注册与签名机制：确保每一个数据行为（上传、调用、授权等）都可被追溯到唯一身份；
* 零知识证明技术：支持用户在不泄露原始数据的情况下完成身份验证与授权；
* 隐私智能合约：合约仅可在用户授权条件下调用数据内容，防止隐私泄露；
* 与LORA钱包集成：用户可使用身份模块管理数据权限、绑定设备、参与投票治理等行为，提升用户控制力与透明度。

该模块将推动医疗、教育、金融等领域的数据共享，兼顾隐私与效率。

**◆ LORA生态金融系统（L-FIN）**

为了支持整个生态的运转和价值交换，LORA构建了完整的区块链金融系统，提供底层Token功能、治理机制、流动性支持与基础DeFi协议，核心组件包括：

* LORAToken：用于支付手续费、数据交易结算、跨链交易费用与生态激励；
* 链上治理系统：支持用户通过LORA Token参与投票，决定系统参数调整、社区资金去向等；
* 去中心化交易协议（L-SWAP）：为Token之间的自由兑换提供高流动性环境；
* 生态基金池：支持DApp开发者、数据提供方、节点运营商等的补贴与奖励。

未来，LORA金融系统还将引入稳定币、保险、抵押借贷等模块，构建自循环金融生态，推动整个系统自增长。

**Part7. LORA未来五年路线图（2025–2029）**

**2025年：生态启动与技术落地**

* 完成LORA主网部署与主链稳定性测试；
* 搭建LORA开发者社区，发布IDE工具与API文档；
* 发布LORA边缘云测试版本，启动首批AI与IoT接入；
* 启动跨链桥服务，实现与以太坊/BNB链的资产互通；

2026年：多链协同与数据经济建设

* 推出“1+N”多链架构正式版，开放子链接入；
* 启动数据交易测试市场，完成第一批数据确权流通。
* 发布LORA Data Value Network（L-DVN）V1.0版本；
* 推出链上身份系统（L-DID），支持医疗、教育场景试点。

2027年：行业级应用突破与AI集成

* 完成Distributed AI链部署，实现链上AI模型训练与调用；
* 发布AI+智能合约平台，开放AI模型定价与调用机制；
* 推出行业级应用包（金融、能源、供应链），推动LORA生态商业化；
* 实现部分国家与地区的政府级/大型企业数据合作落地。

2028年：生态金融体系成熟化

* 推出L-FIN DeFi生态，包括去中心化交易、借贷、保险、稳定币系统；
* 完善LORA治理模型，提升社区自治与Token赋能效率；
* 扩展侧链数量至100+，形成应用专链矩阵
* 建成全球多数据中心支持的边缘云网络。

2029年：全球化生态与基础设施标准化

* 完成LORA全球化部署，进入亚太、北美、欧洲多个国家基础服务市场；
* 推动LORA成为数据主权与去中心化标准的开源基础设施；
* 推出生态基金平台，支持全球DApp与数据创业者；
* LORA成为链上数据市场、智能边缘应用、Web3 AI平台三位一体的综合型基础设施网络。

**Part8.免责与风险声明（略）**