优罗链项目白皮书

EULOGIAN WHITEPAPER FOR PROJECT LAUNCH

www.eulo.io

目 录

“优罗链（**EULO**），区块链**3.0**时代的标志性公链，良好的匿名性和即时交易秒结算的特性，使得优罗链能够在大规模商用**DAPP**中提供良好客户体验度，而独具特色的链上世界银行使得资产能够增值保值。”

EULO对区块链的理解

区块链，最早在中本聪的白皮书《比特币：一种点对点的电子现金系统》中提出，是分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用。虽然以技术的面目诞生，但是其所带来的已经远远超越技术范畴本身，正如互联网技术给我们带来的一样。

在 EULO 看来，区块链不仅仅是一项技术、一个工具，更是一种思想：开放、共享、去中心化。区块链的这些核心精神与互联网不谋而合，而与互联网不同的是，区块链把这样的思想从信息的传递进一步拓展到价值的传输，即从信息互联网到价值互联网。信息互联网使得信息传输的成本趋于零，深刻地改变了社会的经济格局，影响了每个人的生活。当未来市场交易成本趋于零的时代到来，以区块链为基础的价值互联网可能会对整个世界的经济格局及社会结构带来新的变化。

随着社会飞速发展，科技进步，生活节奏几何倍增，信息不可靠、信用资源缺失的情况愈发严重，政府、企业、个人之间的信任体系愈发脆弱，沟通和交易成本增加。 在这个经济快速发展的时代，EULO 认为区块链技术以其去中心化， 防篡改，高度透明等特性，会成为继 PC 互联网、移动互联网后又一个革新人类社会的技术，将会使社会各种关系的信任变得更加简单。

目前区块链技术仍处于较初级的发展阶段，各种形态的公链、共识机制、扩展方案和跨链策略不断被提出。EULO 致力于解决当前主流公链存在的问题，并提出一种新的产品-去中心化链上世界银行（下文称：世界银行），解决数字货币市场波动较大的问题，降低传统投资人的进入门槛。

EULO

公链行业分析

1.公链行业背景

公链是区块链的底层协议，是区块链世界的“操作系统”，为各种应用开发提供基础技术支撑，是未来区块链技术落地应用的核心基础。经历了公链 1.0 比特币和公链 2.0 以太坊的探索，公链 3.0 正着眼于解决系统的扩展性、安全性和监管兼容性问题，以承载大规模的商业应用。同时，公链 3.0 仍需保留区块链的开放、自治等特性。与互联网的架构不同，区块链底层协议的价值远远超过应用层，底层公链仍将是现阶段区块链行业的攻关重点，各公链在可扩展性、应用性、共识哲学，以及应用生态搭建上的角逐将长期延续。

1.1 公链1.0-比特币

比特币在设计之初定位为支付工具，只能进行价值传输。中本聪因此大幅删减了许多脚本指令，所以其安全性极高。但比特币的脚本语言是图灵不完备的，不能执行循环语句，可扩展性差，许多高级应用无法建立在比特币脚本之上。

1.2 公链2.0-以太坊

以太坊是一个具备图灵完备脚本的公共区块链平台，被称为“世界计算机”。除进行价值传递外，开发者还能够在以太坊上创建任意的智能合约。以太坊通过智能合约的方式，拓展了区块链商用渠道，比如众多区块链项目的代币发行，智能合约开发，以及去中心化DAPP 的开发，目前基于以太坊的DAPP 已经超过1000 个。然而，当前的以太坊网络存在扩展性不足、安全性差、开发难度高以及过度依赖手续费等问题，区块链的大规模商用遭遇了发展瓶颈。

1.3 公链3.0-大规模商用

公链 3.0 定位于能大规模商用，与实际资产和真实价值相关联，推动实体经济发展。目前正在竞争区块链 3.0 的公链项目有 EOS，Cardano 等，但这些公链项目多数处于理论论证及测试阶段，少数主链完成开发的项目也仍处于早期探索阶段。而技术储备充足、财力雄厚的公链 2.0 代表以太坊仍在不断地自我迭代，准备采用 Plasma、Sharding 和 Casper 等技术大幅度提高以太坊的处理性能。

公链是未来一切区块链商业应用的基础设施，在已有的技术中，涉及到共识机制、智能合约、跨链技术、侧链技术、兼容性和扩展性等，在这些技术的组合影响下，直接决定着公链的基本性能，包括维护公链正常运行的节点数量、交易处理速度及应用开发的难易程度等。区块链底层平台技术开发具有技术结构复杂、开发难度大、开发周期长及争议较大等特点。

围绕着公链这些底层技术，又形成包括区块链钱包、区块链浏览器、节点竞选、矿机、矿池、开发组件、开发模块、技术社区及项目社群等一系列的生态系统，这些生态系统的完善程度直接决定着公链的使用效率和效果。

目前市场上整体生态系统比较成熟的项目包括 ETH、NEO 等，但这些项目尚不能支撑起高频的商业应用，所以市场一直在探索符合商用的公链。

区块链底层技术平台尚处于不断创新，逐渐完善的阶段，以目前的技术水平尚不足以对现实世界产生巨大影响并进入到实际的大规模商用阶段。在目前的区块链底层平台的研发过程中，对共识机制、中心化与去中心化、交易处理速度和安全等问题最为关注，讨论也最为激烈，但对于未来如何实现高效、安全和去中心化的平台大家还尚未形成共识。

2. 公链的核心要素

互联网世界里的核心资源要素包括存储资源、传输资源、运算资源三个方面， 区块链技术作为互联网技术的延伸，其核心资源要素与互联网有很大的相关性。同时，区块链是信任的机器，在互联网传递信息的功能之外，还承载着价值传输的使命，因而区块链世界的核心资源要素可归结为存储资源、传输资源、运算资源和共识机制所产生的信任资源四个方面。

业界通常将区块链的架构分为五个层面，分别为数据层、网络层、共识层、合约层和应用层，我们将其中的核心技术要素提炼成五个维度，包括可扩展性和传输技术、系统安全、分布式存储、监管兼容性和共识机制。公链的核心技术要素和核心资源要素如图 2-1 所示。

图2-1 公链的核心要素

3. 共识机制的优劣

主流公链采用的共识机制有：PoW、PoS、DPoS 以及 PBFT，简单介绍如下：

工作量证明机制 Proof of Work（PoW）

是指获得多少代币，取决于主体挖矿贡献的工作量，一般来说，电脑性能越好， 分给矿工的矿就会越多。代表币种：BTC、LTC 和现阶段的 ETH。

权益证明 Proof of Stake（PoS）:类似于财产储存在银行，这种模式会根据你持有代币的量和时间，分配给你相应的利息。简单来说，就是指谁拥有的币多（需要钱包在线），谁就有发言权， 所以 PoS 就是根据在线钱包的持币比例来证明谁有发言权。

授权权益证明Delegated Proof of Stake（DPoS）：让每一个持有某种资产的人进行投票，由此产生一定数量的代表 ,再由选举产生的代表按照某种机制出块。从某种角度来看 ,DPoS有点像是议会制度 ,如果代表不能

共识机制	特 性	
	优 势	劣 势
PoW	1、参与度高，节点自由度高 2、节点系统开放 3、公平公正	1、去中心化程度低，容易引起51%攻击 2、能源耗费多，造成浪费 3、安全性较低 4、扩展性弱，性能低 5、没有最终性 6、造成硬件设备浪费
PoS	1、安全性高 2、能源耗费少 3、去中心化程度高 4、节点系统开放	1、公平度低 2、没有最终性 3、大众认知度低
DPoS	1、能源耗费少 2、性能高 3、具备最终性	去中心化程度低，节点系统相对封闭
PBFT	1、性能较高 2、具备最终性 3、安全性好	1、去中心化程度低，节点系统相对封闭 2、容错率低

图 2-2 主流共识机制的特性分析

履行他们的职责（比如出现作弊等情况，他们会被除名，网络会选出新的节点来取代他们。代表币种：EOS。

实用拜占庭容错算法 PBFT Practical Byzantine Fault Tolerance（PBFT）：

PBFT 是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。将所有的副本组成的集合使用大写字母 R 表示，使用 0 到|R|-1 的整数表示每一个副本。为了描述方便，假设|R|=3f+1，这里 f 是有可能失效的副本的最大个数。尽

表币种：NEO。

除了以上共识机制之外，还有各种改进型的共识机制，包括租用共识机制 LPoS（通过这一机制，代币持有者可以将他们的代币借给全网节点的矿工，并获得分红收益）、动态权益的共识协议（DSC，通过动态选举若干记账人，然后在所有记账人中采用PBFT 方式进行交易共识）、FBA 联邦拜占庭共识、OCE(基于 DBFT 共识协议和可验证随机函数VRF 的增强版本共识引擎，实现了近乎无限的可扩展性，只需很少的计算量，生产几乎不会分叉的区块链网络，OCE 支持可插拔验证者、在线协议修复/升级）等。

主流共识机制的特性优劣分析如图 2-2 所示：

4. 痛点分析

4.1 单独PoW和PoS都存在问题

对于 PoW 共识机制 :由于专业矿工和矿机的存在，最终算力过度集中让社区趋向中心化发展，矿霸事件频出，容易遭受 51%攻击造成交易回滚，用户损失资产；同时扩展性较弱，性能较低，此外，大量重复计算产生的高能耗也是 PoW 被诟病的原因之一；

对于 PoS 和 DPoS，这种不需要消耗太多算力即可达成共识的机制对 PoW 的上述缺陷有所弥补，但依靠代币数量获得出块又形成了新的中心化趋势，而且实现过程复杂容易分叉，需要运行大量的节点保证公链网络正常，这样会造成网络流量压力大，中间步骤存在安全漏洞。

4.1.1 区块确认时间较长

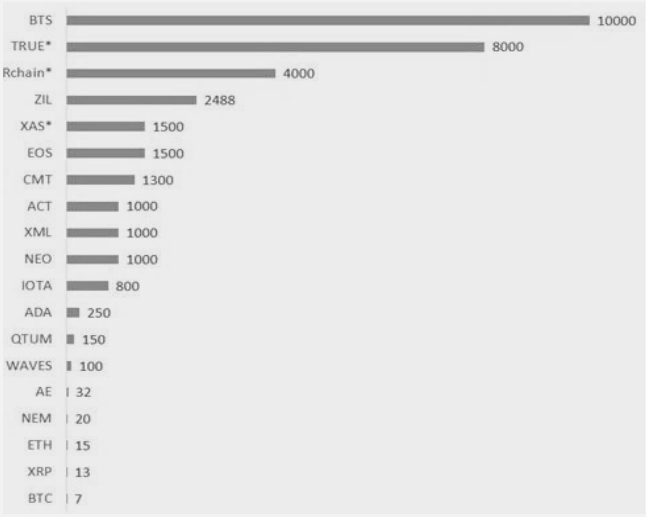


图 2-3 主流区块链项目的 TPS 情况

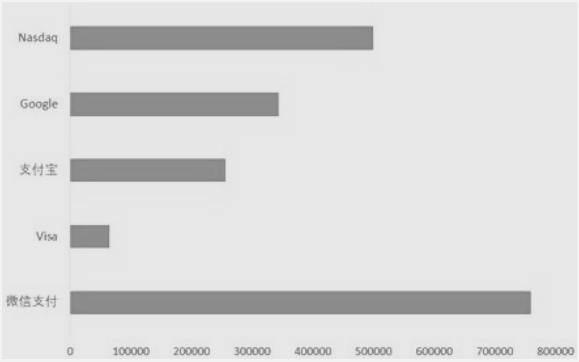


图 2-4 传统互联网应用的 TPS

比特币平均 10 分钟出一个块，大致需要 6 个区块确认，区块确认时间约为60 分钟；以太坊平均 15 秒出一个块，大致需要 12 个区块确认，区块确认时间约为 3 分钟。区块确认完成才代表当前交易处理已完成，全网已记录，按照此种方式计算，比特币的 TPS(每秒处理事务数) 约为 7，以太坊的 TPS 约为 15。主流区块链项目的 TPS 情况如图 2-3 所示。

根据目前传统商用应用的处理速度来看，现有区块链平台项目的交易处理速度尚不能支撑起大规模的商用应用，虽然在不断探索和开发，但区块链要真正的进入的商用应用，还需要很长的路要走。传统互联网应用的 TPS 情况如图 2-4 所示。

4.12 币价随市场波动较大

从数字货币出现伊始，人们就一直在诟病它疯狂的价格波动，近半年 BTC 的价格波动就超过 300%，ETH 的波动超过 400%，某些小币种的波动甚至超过1500%。相比其他金融资产和法币，数字货币价格波动较大的主要原因有三个：

1）监管漏洞较大

数字货币存在着很大的监管漏洞，这是造成其价格波动不稳的主要原因。每一个新兴科技产品，都存在技术层面和道德层面两方面的使用伦理。从技术层面来看，任何一个使用者，只要没有破坏技术层面的准则和规范，都属于正常使用。但是从道德层面来看，将技术应用于非法目的，显然是任何一个国家与合法组织都不能接受的。

因此，一些研究区块链的学者和程序员，希望可以在技术层面上保持区块链的“去中心化”和“匿名化”特性；而在道德层面上与政府、司法部门合作，达到必要的监管目的。

2）投机心态弥漫

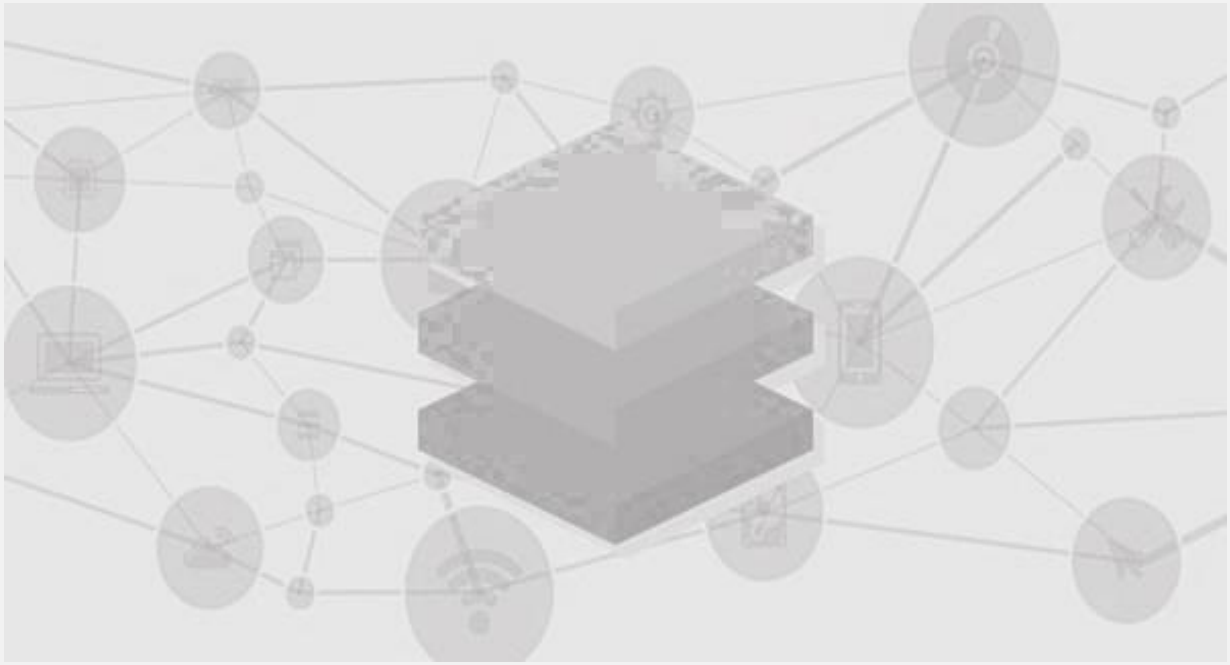
以比特币、以太坊为代表的数字货币并非一些人所想象的“庞氏骗局”、“郁金香热”，而是具有技术价值和金融实践价值的数字资产；但几乎没有门槛的 ICO 使得五花八门的区块链项目被拼凑了出来，其中充斥着许多毫无实质内容的空壳。有些 ICO 项目直接把国外的开源项目代码搬来，稍稍改变几个参数，就上线圈钱了。这样的项目，引来了大量投机者。

某些投机者购买某 ICO 代币，短时间内翻60 倍，而他的本金只有 10 万。这种规模的回报率，已经远远超出合理范围。

3）自身技术尚不成熟

公有区块链目前存在很多的问题。区块预设容量太小，扩容方案又多有瑕疵；转账交易速度慢，大量搁置交易；通过对特定网络端口的攻击可以破坏区块链正常确认工作；大量中心化的矿场、交易所逐渐占据全网超过半数的算力，一旦这些平台被黑，整个区块链网络可能面临生死考验；诸如此类，不一而足。技术不成熟，就意味着区块链网络可能面临攻击，其市场价格也就容易产生较大波动。

综上所述，监管漏洞大往往会让价格迅速上升，因为众多非法交易一直在助推价格走势；投机气氛浓厚是数字货币价格呈现过山车走势的重要原因，但凡有坏消息流出，价格便会应声回落或踟蹰不前；技术不成熟，令价格无法稳定在合理区间内，价格的涨跌幅度较大。



4.1.3 特殊场景下隐私无法得到保护

当中本聪于 2009 年发明比特币时，他提供了一种方式供无条件信赖彼此的参与者们协作维护规范且防篡改的交易和电子信息纪录。后面的区块链公有链都参照了这种方式，每一个参与者都能够获得完整的数据备份，所有交易数据都是公开和透明的。这是区块链的优势特点，但另一方面，对于很多区块链应用方来说， 这个特点又是致命的。因为很多时候，不仅仅用户本身希望他的帐户隐私和交易信息被保护，就商业机构来说，很多帐户和交易信息更是这些机构的重要资产和商业机密，不希望公开分享給同行。

比特币对隐私保护的解决思路是，通过隔断交易地址和地址持有人真实身份的关联，来达到匿名的效果。所以虽然能够看到每一笔转账记录的发送方和接受方的地址，但无法对应到现实世界中的具体某个人。但这样的保护是很弱的，通过观察和跟踪区块链的信息，通过地址 ID、IP 信息等还是可以追查到帐户和交易的关联性。

EULO的解决方案

1. 解决方案

EULO 基于 PoW+PoS 算法，采用主节点+超级节点构建的双层网络，使用零知识证明，同时对区块链传输层协议进行优化，实现快速支付和匿名场景下的交易。另外，EULO 还加入了预言机的设计，打造去中心化的链上世界银行，减少加密货币市场价格波动对传统投资人的影响。

1.1 解决单纯的PoW+PoS 共识机制的问题。

EULO 的共识机制采用 PoW+PoS 算法。PoW 用于产生和分发 EULO。EULO 的总量恒定，为 210 亿，采用 PoW 挖矿，类似比特币网络挖矿。比特币网络运行近 10 年，没有出过明显问题，其 PoW 共识机制和基于此的经济模型会比其他共识机制更加稳健。

PoS 共识机制用于打包 EULO 交易，其处理交易更快。EULO 的产生和交易打包分离后也会更加安全。若因算力集中出现 51%攻击，只能影响后续 EULO 的产生，无法篡改历史交易，确保用户账户资产安全。

1.2 解决区块确认时间较长的问题。

EULO 构建了交易确认的双层网络，修改了底层网络传输协议来缩短区块确认时间。普通交易确认的双层网络是指以普通 pos 节点(简称普通节点)+主节点（包含超级节点）组成的网络，普通节点负责打包交易，打包完毕后广播给该主节点所链接的超级节点和其他主节点；超级节点类似传统互联网领域的 CDN 节点，主要解决数据同步问题，在共识上无其他特权；如果客户采取 InstantSend 模式发起即时转账交易，该交易的输入会被锁定到对应的特定交易去，该交易在主节点网络达成锁定的共识，所有与之冲突的交易和区块将被永远拒绝，除非它们能匹配当时锁定的交易对应 ID。而目前全网交易

锁定的时间大约是 1 秒;因此采用InstantSend 的快速交易可以实现安全的 1 秒到账，我们称之为秒到。

EULO 还修改了底层的网络传输协议，一是使普通网络的信息传输确认更快， 二是使跨境网络的传输可以突破某些限制，解决网络环境复杂场景下的跨境支付问题，这个主要对底层网络传输协议栈做修改，使得在普通节点在主节点的协议下可以高速互换信息，这种模式对超级节点所处的网络环境有较高的要求。

1.3 解决数字货币市场波动对投资人的影响问题。

EULO 加入了去中心化的预言机设计，在此基础上打造了一个去中心化世界银行，投资人可以使用世界银行的换汇功能获得对稳定币BCK的等值价值兑换。减少数字货币市场剧烈波动对投资人的影响，风险更小更可控， 也降低了传统投资人的参与门槛。

世界银行本质来说，是一个通过智能合约实现的 DAPP，它可以在链上实现传统金融领域的锁汇、储蓄等功能。使区块链更好的服务于传统实体经济。主要流程分为：价格获取；以当前价格存入世界银行一定 EULO 的数量进行锁汇；然后一定周期后可以自动转回链上银行兑换，获取原来总价值对应现在的币数。除此之外预言机配合智能还能衍生更多的 DAPP 运用，可广泛运用在各种竞彩、游戏行业。

1.4 解决隐私泄漏的问题。

EULO 使用零知识证明来解决隐私保护的问题。零知识证明是指既能充分证明自己是某种权益的合法拥有者，又不把有关的信息泄漏出去——即给外界的“知识”为“零”。

EULO 可以交易匿名，为 EULO 上的数据隐私提供保护。在数据为个人所有的情况下，可以不暴露隐私，对个人的信息进行有效的使用和交换。这方面 EULO 可扩展使用的场景有：加密通讯和数据隔离等。

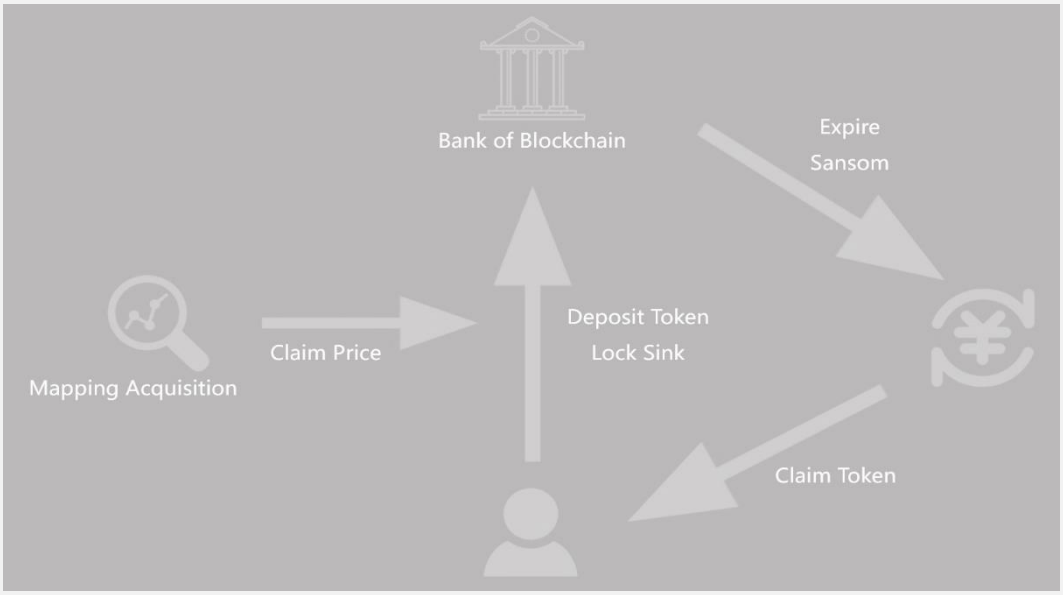


图 3-1 世界银行运作流程

2 .去中心化的链上世界银行

通过EULO的智能合约机制，可以在EULO主链上发行稳定币。EULO上发行的第一个稳定币是BCK(简称：刀币),BCK在智能合约下按照算法运行,去中心化的信任机制解决了以往稳定币需中心化背书和难以监管的超发问题。BCK跟美元进行等值挂钩，在智能合约下EULO跟BCK能够自动进行兑换，所以称EULO主链上这个具有换汇功能的智能合约为链上世界银行。

EULO使用预言机获取链外EULO市场行情等数据信息作为区块链资产间兑换的基础。

将一定数量的EULO转入链上银行的智能合约地址，智能合约在预言机机制下产生即时汇率，自动汇兑相应数量的稳定币BCK。

其流程示意图如图 3-1 所示：

链上银行汇兑手续费是3%，即转入市值100美金的EULO(假如此时EULO价格是1美金，数量是100) 进链上银行，可以获得的BCK市值是：$100×（1-3%）=$97。

通过链上银行兑换获得的稳定币BCK，两个月后也可以转入链上银行自动换回EULO ，免收手续费，即转入100美金的BCK，可以即可兑换到价值100美金的EULO。如果此时EULO价格上涨到2美元，则价值100美金的EULO数量是50个，如EULO价格下跌到0.5美元，则价值100美金的EULO数量是200个。

持有稳定币BCK，避免了价值的大幅波动外，还可以获得链上银行的收益分红。每年链上银行将收益的60%EULO,按照BCK登记日的锁仓数量直接进行利润分红。

链上银行的收益主要分为：1. 在链上银行，EULO兑换稳定币BUC，智能合约自动扣除的手续费3%。2. 通过链上银行所得稳定币BCK换回EULO时，如果EULO价格增长，则链上银行又赚到更多的EULO。

技术实现

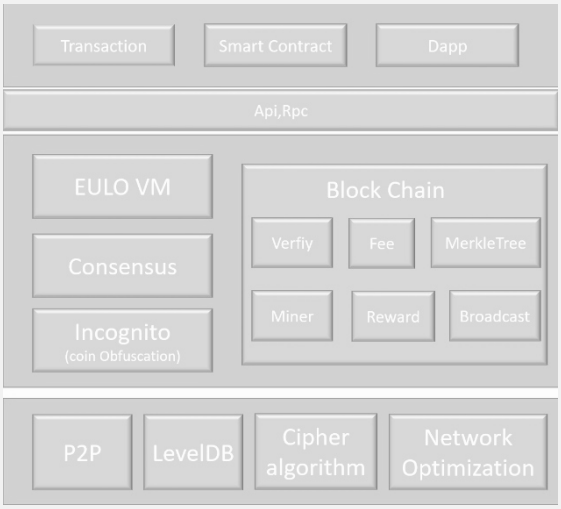


图 4-1 EULO 的技术架

1. EULO 的技术架构

EULO 架构在三元悖论中侧重于安全、去中心化，采用分布式网络架构，合理分配算力，并且让生态中各参与方，快速获取跨链数据服务，并保障服务不受第三方干扰。

2. 功能模块

一般区块链由数据层、网络层、共识层、激励层、合约层、应用层 6 层结构组成，数据层主要对信息数据进行记录、存储，通过时间戳、链式结构、哈希函数、Merkle 树、非对称加密等技术整合起来；共识层封装了网络节点的共识算法机制，目前共识算法主要有 PoW、PoS、DPoS 等等；网络层封装了 P2P 网络、传播机制和验证机制；激励层主要针对将经济因素集成到区块链体系的情况，一般为经济激励的发行机制和分配机制；合约层主要封装了区块链的各类可编程脚本、算法机制和智能合约；应用层是对区块链的应用场景扩展。

EULO 将六个层级进行重新的排序和定义，我们将其综合为三个层级(图-4)， 按功能或者结构从上到下可以分为三个层级，顶层应用层(合约层，应用层)，包括转账，智能合约，Dapp，应用层通过 rpc 或者 api 与下面的核心层进行数据传输交互;中间层为核心层（共识层，激励层, 数据层）,包括 EULO VM、区块核心、共识算法、以及隐私核心的混币算法零知识证明; 最下面为支撑层(数据层，网络层)，涉及 P2P 网络，数据存储，密钥算法，以及网络优化;

1)　支撑层

支撑层：主要涉及到各种广播消息，节点的同步，网络节点的发现以及网络传输的优化改进，以及区块打包时代各种安全算法。

2)　核心层

a)　EULO VM

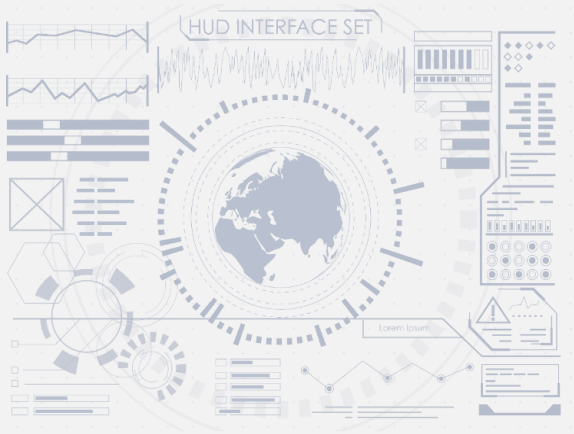
EULO 是可编程的区块链。它并不是给用户一系列预先设定好的操作（例如常见的币币交易），而是允许用户按照自己的意愿创建复杂的操作。这样一来，它就可以作为多种类型去中心化区块链应用的平台，包括加密货币在内但并不仅限于此。它的核心是虚拟机，可以执行任意复杂算法的编码。因此 EULO 是"图灵完备的"。开发者能够使用现有的编程语言为基础的编程语言创建出在其上运行的应用。

和其他区块链一样，EULO 也是一个点对点网络协议。EULO 区块链数据库由众多连接到网络的节点来维护和更新。每个网络节点都运行着 EULO 虚拟机并执行相同的指令。因此这能保证在所有节点的验证，输出结果的一致性，保持了整个区块链的一致性。而且去中心化的一致性使 EULO 具有极高的故障容错性，保证零停机，而且可以使存储在区块链上的数据保持永远不变且无法篡改。

b）　共识算法。

EULO 共识算法被设计成为了混合模式 POW+POS，在前期的采用单一 POS 方式实现快速交易功能，然后在 6 个月后实现的 POW 挖矿+POS 打包确认。

POS 记账采用 POS3.0 模型，避免传统 POS 的币龄攻击；POW 采用变种的 CryptoNight 算法，该算法 GPU 和 CPU 效率差距不明显，可在保证去中性化的同时保证较低的能源消耗。



c)零知识证明。

它指的是证明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。比如证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。

在 EULO 中给用户提供了高隐私性可匿名的交易可选，由于传统零知识证明交易体积很大，我们将在正式版本中采用全新的 bulletproof 算法，该算法能将交易体积从现在的 20K 减小到 1.5K 左右。同时无需设定可信任的初始设置（zec 需要），使交易更匿名更隐私。

3) 应用层

a) 交易

EULO 交易分为 Coin 转账交易以及 Stake 权益转让：

EULO Coin 转账交易。账户体系采用了 UTXO 模式，在转账的方式上提供了独有的方式（快速、匿名模式）进行转账交易。当选择快速模式时，将以最大的 Fee 进行转帐；当以匿名模式转帐时，EULO VM 会采用零知识证明算法（详见区块链核心中阐述）进行匿名模式的交易。转账函数定义如图 4-2 所示。

```
bool CWallet::CreateTransaction(const vector<pair<CScript, CAmount> >& vecSend, CWalletTx& wtxNew,
    CReserveKey& reservekey, CAmount&
    nFeeRet, std::string& strFailReason,
    const CCoinControl* coinControl,
    AvailableCoinsType coin_type, bool
    useIX,
    CAmount nFeePay)
```

4-2 转账行数

转账函数流程为：

i. 判断 useIX 是否(真)，并且最小使用支付费用是否小于 CENT(1000000)=0.01 Coin ，如果费用小于该值则设定最小 Fee 为CENT；

ii. 检测转账金额是否为正数，并计算总的转账金额；

iii. 将该交易(CmerkeleTx)绑定到本地钱包，并设置 fTimeReceivedIsTxTime=true；

iv. 加锁本地钱包 cs_wallet；

v. 判断转账模式并根据 payees 构造 CtxOut，然后按照千字节计算费用；最小费用为 10000 duffs KB，并判断转账金额是否小于转账最低手续费；

vi. 从本地钱包选择属于自己的 Coin(CtxOut)且未 spend 的进行组合累计转出金额数量，并判断是否有足额的金额进行本次交易；

vii. 根据转账设置项判断是否进行匿名等操作，并进行相关操作的的设置；

viii. 最后对转出进行 sign，本次转账构建完成。

权益转账。权益转账函数流程为：

i. 获取本地 Coin 的余额；

ii. 获取本次权益转让后返回的本金，如果本金小于或者等于本次余额

iii. 则本次交易不能构建；

iv. 计算币龄（计算公式：）

v. 兑现相应的权益，构建对应的 CtxOut；

vi. 对交易进行签名，本次权益转让构建完成。

b) 去中心化的 oracle

EULO 的主节点网络在去中心化的前提下完成了现实世界到区块链的完美映射，解决了以往公链oracle 系统采集节点单一（公信度低）、实时性低（出块间隔太长）、采集不稳定的

问题。是 Oracle 系统的最完美解决方案。

c)智能合约及 DAPP

- **智能合约。**

智能合约是 EULO 生态系统不可或缺的一种机制。技术上是由事件驱动的、具有状态的、获得多方承认的、运行在一个可信、共享的区块链账本之上的、且能够根据预设条件自动处理账本上资产的程序。EULO 智能合约借鉴并移植了目前拥有强大社区及生态链网络的以太坊的合约机制，使其能轻易的满足现实社会各种合约场景需要，特别是金融类，比如金融类合约产品、差价合约、代币系统（token system）、作物保险、多重签名智能合约、储蓄钱包以及 EULO 独有的世界银行系统（详情见后面阐述）。

- **DAPP。**

Dapp 是运行在智能合约的机制上的一个应用或者程序，它和智能合约都需要运行在 EULO VM 上，其运行流程图如图 4-3:

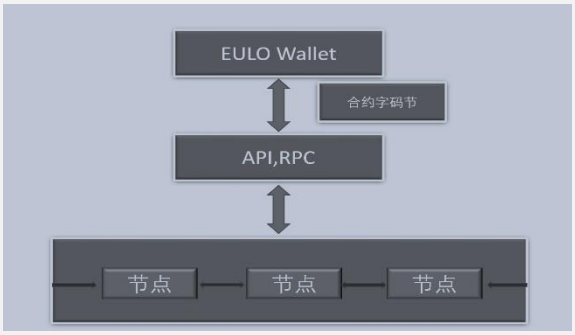


图4-3 智能合约执行

3. 网络结构

3.1 网络结构描述

EULO 整体网络在去中心化的基础上，采用通过添加了引入主节点（主节点需要 100W 个币）和超级节点（需要 1000W 个币，投票权利和主节点完全平等，主要工作是解决跨国环境下的区块同步和分发问题）协议分层构架；配合弹性区块大小机制；并且在主节点、超级节点的操作系统底层在通信协议栈机制上进行一定的协议优化（这是目前全世界研究的热点，优化 TCP 协议，优化并发性能），完美解决了在跨国通信线路高延时、高丢包的通信效率问题，通过对网络传输的优化， 以及EULO 整体项目架构的优点，目前实验室测

测试 TPS 性能超过 6000，且在目前转账能保证交易的准时时性(秒级支付)，而在后面的规划中，EULO 网络将通过分片方式实现百万级的 TPS 性能。

1）网络节点类型

- 超级节点：超级节点主要承担跨地区、跨境网络交易快速确认，打包以及网络流量快速分发、区块快速同步；
- 主节点: 节点主要承担交易快速确认，网络同步；
- 普通节点： 交易接收，分发，打包，并与超级节点，主节点同步区块。

2） 网络优化

- 目前问题：

a) 节点网络资源参差不齐，而又当跨境跨地区时，网络节点间交易的快速确认，区块的快速同步是一个巨大的问题。

b) 目前区块链网络主要采用 tcp 协议进行数据传输，而 tcp 是可靠的传输协议，除了建立连接时的各种握手包之外，在传输数据时会有各种机制保证网络的可靠传输，比如确认机制、重传机制、拥塞控制机制等都会消耗大量的时

```
CTxIn vin;
CService addr;
CPubKey pubKeyCollateralAddress;
CPubKey pubKeyMasternode;
CPubKey pubKeyCollateralAddress1;
CPubKey pubKeyMasternode1;
std::vector<unsigned char> sig;
int activeState;
int64_t sigTime; //mnb message time
int cacheInputAge;
int cacheInputAgeBlock;
bool unitTest;
bool allowFreeTx;
int protocolVersion;
int nActiveState;
int64_t nLastDsq; //the dsq count from the last dsq broadcast of this node
int nScanningErrorCount;
int nLastScanningErrorBlockHeight;
CMasternodePing lastPing;

int64_t nLastDsee;  // temporary, do not save. Remove after migration to v12
int64_t nLastDseep; // temporary, do not save. Remove after migration to v12
```

图 4-4 网络节点类型定义

间，当网络出现质量问题时，这种耗时更将成倍增长，而且要在每个节点上维护所有的传输连接，每个连接都会占用一定系统资源。当网络不稳定时这种机制更不利于区块的快速同步 交易的快速确认。

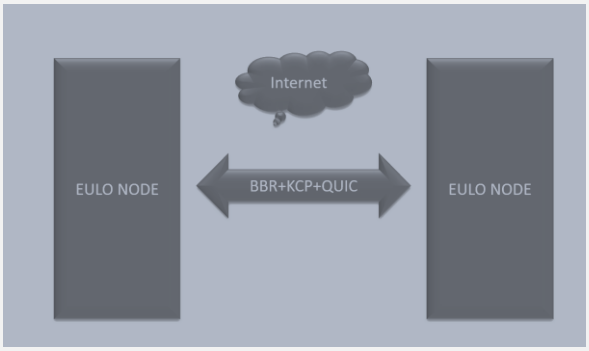


图4-5 BBR+KCP+QUIC网络优化

- **解决方案：**

a) 我们引入了超级节点进行跨境跨地区交易快速确认，区块快速同步。超级节点将拥有足够网络资源，以及超强的计算处理能力来满足EULO 项目的快速，高效，稳定的发展，以及更好的适应现实生活的各种及时交易场景。

b) 采用 BBR+KCP+QUIC 三重机制优化 IP 协议栈进而保证各网络区块的快速同步,交易的快速确认。BBR+KCP+QUIC 网络优化如图 4-5 所示。

团队介绍

1. 核心团队

江均勇，创始人&CEO

北京航空航天大学硕士，国内知名云安全专家，全球云安全联盟大中华区协调顾问、云安全联盟理事、中国云体系联盟常务理事、浦东软件园产业研究院特聘专家等职务，拥有近二十项全国技术发明专利。拥有丰富的大型公有云项目开发管理经验经验。

Benjamin Larson，CTO & Co-Founder

经济学，计算机硕士双学位。参与著名银行行跨行结算中心项目搭建和实施。对现金处理自动化系统、银行信息交换系统相关应用有着丰富的经验。

Debbie Otegen，CFO

曾就职于著名投资银行，负责金融信用衍生品开发工作。 拥有20年金融投资风控经验。擅长风险控制、、估值模型的搭建和实际应用。

Milan · Developer

具有11年经验的IT开发专家，擅长银行、金融交易等相关软件Web/移动端应用程序的架构和开发。

2. 项目顾问及投资机构

2.1 项目顾问

Brad Smith

管理顾问 ，从事IT管理咨询工作10多年。评估过100多个IT系统（包含选举、铁路、保险银行等）。对于企业管理有着丰富经验。

Anna Gavin

运营顾问，4A高级运营总监，擅长品牌推广及营销。对于新媒体及用户社区搭建也有着独到的见解和经验。

2.2 投资机构

AUEX 澳交所、LKDE、UKEX.com 英交所、BITALONG 比特龙、泰岳梧桐基金、青创投。

EULO分发机制

1. EULO 分发机制

20%的 EULO 由机构统一认购，20%用于市场拓展和社区建设，10%用于初期的技术研发，剩下 50%将在未来的 30 年内由 POW+POS+主节点共同挖出。

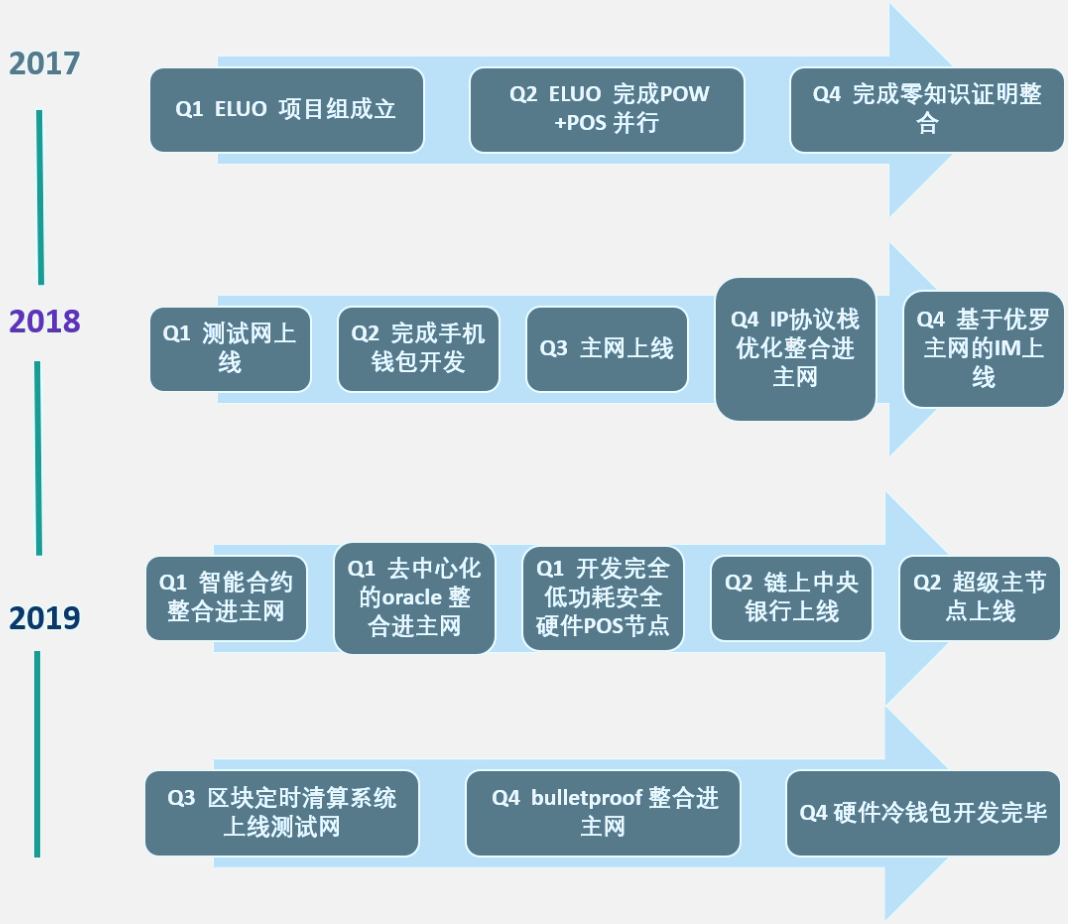
2. EULO 的使用场景

跨国跨银行结算时间和经济成本高，有时候需要长达一周甚至更长的时间。尤其在一些银行系统普及率低的地区和国家，嗜待一条实用高性能公链来实现链上交易清算，而目前大家所熟知的一些公链，要么交易确认速度慢，要么手续费高， 对交易结算双方安全隐私也没有很好的保护，以至于目前都没有哪一条公链实现了大面积的商业场景的应用。

使用 EULO 交易，交易手续费极低，同时交易确认速度快，可以达到秒级交易确认速度，同时可以实现选择性隐私交易结算，基于这些特点，EULO 主要定位于跨境交易支付领域，尤其是在一些银行系统普及率低的地区和国家，EULO 的普及将极大地满足人们对商业场景秒级交易支付的需求，改善人们的交易支付体验，提升跨国经济结算清算的流转效率。

EULO

发展路线


2017
Q1 ELUO 项目组成立
Q2 ELUO 完成POW +POS 并行
Q4 完成零知识证明整合
2018
Q1 测试网上线
Q2 完成手机钱包开发
Q3 主网上线
Q4 IP协议栈优化整合进主网
Q4 基于优罗主网的IM上线
2019
Q1 智能合约整合进主网
Q1 去中心化的oracle 整合进主网
Q1 开发完全低功耗安全硬件POS节点
Q2 链上中央银行上线
Q2 超级主节点上线
Q3 区块定时清算系统上线测试网
Q4 bulletproof 整合进主网
Q4 硬件冷钱包开发完毕

社区治理

1. EULO 社区治理架构

治理是人们在主观问题上达成共识的过程，而这些问题不可能完全被软件算法所捕获。直观的理解，就是共识算法不能完全解决的问题，也就是不能通过软件完全自动解决的问题，而需要人的参与，通过投票等方式表达意愿，行使权力的过程。

首先，少数的区块生产者是授予了权力，可以进行一系列执行。这是一种执行集中制，是为了高效。但为了保证执行集中制的正义，是民主的集中制，必须对集中制进行充分的监督。治理的权力来源并最终属于 token 的拥有者。也就是， 区块生产者进行操作，而 token 持有者对操作进行反馈的闭环过程，有效地影响区块生产者。

而 EULO 主节点承担了即时支付、隐私支付、对提案项目投票等功能，因此， 主节点数量越多，分布越广泛，EULO 网络就越稳定。

2. 如何防止主节点被攻击

那么，承担工作的 10 个主节点又是如何挑选出来的。10 个主节点是通过哈希算法在主节点排序靠前的 10%中挑选出来的，将前 100 个区块和 10%的主节点都进行哈希，最后将哈希最接近的 10 个主节点挑选出来。而我们知道，每一个主节点、前 100 个区块都是随机和变化的，相当于一个算力工具，由于作恶成本太高，从而有效地防止了攻击。

主节点网络作为最重要的基础设施，当然也设计了完善的社区激励机制。一个主节点的建立需要抵押 1000000 个 EULO，所有的主节点可以得到 45%的全网挖矿收益。站在安全和效率的角度来综合考虑，主节点会是承载应用的一个很好的点。

3. 分布式投票机制促进社区建设

提案对社区的建设具有非常重要的意义，EULO 为此设置了一个分布式投票机制。

每个节点都有提案的权利，提案需要消耗 5 个 EULO，是否通过由主节点用户投票决定。每一个主节点有一个投票权，投票权可以行使于预算提案或影响 EULO的重要决定。任何提案至少要获得 10%的网络主节点的同意，到月底将会创建一系列的"超级块"，向已批准的提案支付 EULO，用于资助那些对 EULO 社区发展有帮助的推广项目或研发项目。

目前，大部分的区块链项目均由一个团队负责运营，和传统的以社区创办者、管理员或明星用

风险说明

1. 政策性风险

目前国家对于区块链项目以及互换方式融资的监管政策不明确，存在一定的因政策原因而造成的参与者损失的可能性；在市场风险中，若虚拟物品市场整体价值被高估，那么投资者风险将会增加。

2. 监管风险

包括 EULO 在内的数字资产交易具有极高不确定性，由于数字货币领域目前尚缺乏有力的监管，故而数字货币存在暴涨暴跌的风险，个人参与者若缺乏经验，可能难以抵御市场不稳定所带来的资产冲击与心理压力。

3. 竞争风险

区块链项目众多，竞争十分激烈，存在较强的市场竞争和项目运营压力， EULO 未来在众多项目中获得众多用户，成为主流平台产品，受到广泛认可，存在一定的风险。

4. 技术项目风险

密码学的加速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给 EULO 开放平台，这可能导致 EULO 的丢失。项目更新过程中会不断修复漏洞，但不能保证不造成影响。

5. 目前未知风险

除了以上提出的风险，还存在一些团队暂时尚未预料的风险，请参与者在做出决策之前，充分了解团队和项目，理性参与。

免责申明

这是一份概念性文件（“白皮书”），用来说明我们提出的 EULO 公链与 EULO Token。这份白皮书可能会随时受到修改或置换。然而，我们没有义务随时更新这份白皮书，或提供读者任何额外资讯的通道。读者请注意下列事项：

并非适用所有人：EULO 和 EULO 并非开放给所有人。参与可能需要完成一系列的步骤，其中包括提供特定资讯与文件。

在任何司法管辖区内不提供受管制产品：EULO（如本白皮书所述）无意构成任何司法管辖区内的证券或任何其他受管制产品。本白皮书不构成招股说明书或任何形式的要约档，也无意构成任何司法管辖区内的证券或任何受管制产品的要约或招揽。本白皮书并未经过任何司法管辖区的监管机构审查。

不提供任何建议：本白皮书并不构成关于您是否应参与 EULO 公链或购买任何 EULO 的建议，也不应作为任何合约或购买决定的依据。

不代表任何声明或保证：对本白皮书中描述的讯息、声明、意见或其他事项的准确性或完整性，或以其他方式传达与计划相关的讯息，我们不给予任何声明或保证。在没有限制的情况下，我们不对任何前瞻性或概念性陈述的成就或合理性给予任何声明或保证。本白皮书中的任何内容，均不得作为对未来的承诺或陈述之依据。

在适用法律所允许的最大范围内，尽管有任何疏忽、违约或缺乏关注， 任何因本白皮书的任何相关人员或任何方面而产生或与之有关的任何损失（无论是否可预见），其所有责任均免除。可能受限但无法完全免除的责任范围，仅限于适用法律所允许的最大限度。

以中文版本为准：本白皮书为官方简体中文版本，任何英文翻译文件仅供参考， 不经任何人认证。如果本白皮书的英文翻译与中文版有任何不一致之处，请以中文版本为准。

WWW.EULO.IO