LEMO

White Paper v2.2 Simplified Chinese

4-14-2018

195 Pearl's Hill Terrace #02-65 Singapore (168976)

LEMO

基于安全多方计算的数据流通链

为 B 端用户提供基于区块链的去中心化用户账户系统，数据流通协议，数字资产确权及流通，交易撮合和结算等服务，构建未来应用的数字资产生态体系。

IMPORTANT DISCLAIMER

There are risks, and uncertainties associated with Lemo and/or the Distributor and their respective businesses and operations, the LEMO tokens, the Lemo Initial Token Pre-sale and the Lemo Wallet (each as referred to in this Whitepaper). You can find a description of the risk related to the Token Pre-sale under the section Legal, which should be read carefully.

This Whitepaper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of Token Pre-sale or Initial Coin Offering like the one described in this Whitepaper is prohibited or restricted.

The LEMO tokens are not intended to constitute securities in any jurisdiction. LEMO tokens are utility token and cannot have a performance or a particular value outside the Lemo Platform. Therefore, this Whitepaper cannot constitute a prospectus or offer document for investment in securities.

This Whitepaper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by Lemo to purchase any LEMO tokens or give any help in any investment decision.

You are not eligible, and you are not to purchase any LEMO tokens in the Lemo Token Pre-sale (as referred to in this Whitepaper) if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a resident of the People's Republic of China.

Contents

执行摘要

LemoChain（简称 Lemo）的发起者们，致力于利用区块链技术，帮助解决行业中不同机构之间的数据确权问题，从而促进非竞品商家之间的数据共享，同时提高非精准流量的再利用；另一方面，Lemo 鼓励个体将个人信息和需求加密上链，精准匹配需求方与供应方。

由此形成一个去中心化的商务数据流转生态体系，实现点对点的价值转移，构建一个支持多个行业（包括教育、社交、招聘等）的去中心化商业生态，最大程度降低商家获客成本，扩展其商业模式和现金流。

长远来看，Lemo 的目标是打破不同商业体间的数据屏障，定义未来数据使用技术标准，支撑商业数据流通生态的建立。我们在未来会推动数据流通和使用领域的标准化建立，通过推出各种 API 和 SDK，甚至自有的编程语言，以达到使各行各业都可以方便、快捷的使用和共享数据的目的。同时基于 LEMO Token 的数据价值流转体系、信用体系的建立也会在生态的完整度上提供相应的支持。由于技术上的创新、生态治理架构的完善、应用范围广，LemoChain 将成为解决多个行业数据确权和流通问题的公有链。

从技术的角度分析，Lemo 通过引入成熟的技术体系，将实现首个基于 D-PoVP（Delegated Proof of Valuable Participation 价值参与权益证明）共识机制的智能合约平台，使其在合规性上符合不同行业的监管需求的同时，提升其商业应用场景的结合度。同时通过引入多方安全计算、零知识证明及同态加密等机制，Lemo 生态将确保数据在流转过程中的安全性、隐秘性和有效性，从而建立数据价值流转的底层信任机制。

从生态治理架构角度分析，Lemo 的发起者们于新加坡设立了 Lemo 基金会，致力于 LemoChain 的研发建设、治理透明化引导和推进整个生态的工作，促进整个生态的安全与和谐。整个生态治理基金会架构，分别从代码管理、团队管理、财务管理和公共关系等多个维度帮助管理整个开源社区的一切事宜，从而确保 Lemo 的可持续性、基金会内部管理有效性及众筹资金的安全性。

从应用角度分析，Lemo 将通过去中心化应用和服务提供商将链下因素引入，形成符合现实世界商业逻辑的区块链智能合约，支持多个行业。最终不仅实现走向移动端策略（Go Mobile），而是真正的走向服务和线下，为终端消费者提供切实的好处。在 LemoChain 整

个生态系统中，我们将会与第三方开发者站在一起，从技术架构的角度支持并提供服务，包括：

- **加密 Token 支持**（跨应用流通，无地理限制的加密 Token，随时为开发者和其用户提供数据和服务的交易工具）。
- **商业数据撮合交易系统**（提供基于多方安全计算的数据流通服务，帮助不同的应用搭建合规、透明的数据流通渠道）。
- **诚信系统**（用户信用体系，利益驱动，奖励优质用户，淘汰劣质用户，帮助开发者筛选目标用户，提升付费与转化）。
- **账户系统**（一个账户，用遍所有应用，提升应用转化率和流量来源）。
- **数字资产合约**（为开发者及其用户的数字资产确权，帮助其流通和变现，提升用户参与积极性）
- **数据加密存储和传输系统**（为 B 端用户和开发者提供完善的数据加密、存储和传输体系，确保数据在流转过程中的有效性、安全性及隐私保护）

我们同时将制定一个奖励计划，鼓励早期的第三方开发者加入我们，一起开发基于 LemoChain 的移动端服务，共同促进区块链世界的高效协同发展。

Lemo 的设计理念

为什么设计 Lemo

自从 2009 年比特币代码开源以来，比特币网络的价值从零开始，到今天已经成为一个价值约 1600 亿美金的点对点支付网络，整个区块链世界也出现了很多代币和区块链项目，包括致力于搭建通用智能合约平台和去中心化应用平台的以太坊项目。但是区块链行业不论是从技术角度，还是行业应用角度都还面临着很多挑战，主要问题如下：

- 缺乏与现实世界商业逻辑符合的智能合约平台。比特币生态和以太坊生态由于缺少与现实世界的连接，使各行各业的广泛应用受限；
- 共识机制本身缺乏灵活性，现有的共识机制对社会资源造成浪费；
- 现有区块链系统具有很大的封闭性。目前大多数智能合约仅接受链上数据作为触发条件，缺乏与现实世界的交互；

我们致力于可以构建一个全新的区块链数据传输生态系统—Lemo，作为未来去中心化应用世界通用的互联网数据价值传输协议，把数据价值数字化（Digitalize）与代币化（Tokenize），推动区块链技术应用于现实商业场景。

同时在传统的移动应用领域，中心化的体系和缺乏信用机制的客观环境导致互联网上充斥着虚假和无效的信息。作为有着多年移动互联网经验的开发者，Lemo 的发起者认为 Lemo 必需改变未来的数据流通体系，以解决传统中心化应用的几个普世问题：

- 作为应用的主要参与者，用户缺乏应用治理的话语权。中心化的平台方就像收割者一样获取流量和数据带来的价值；
- 用户的隐私得不到有效的保护。用户的隐私权只是得到了平台方的书面保护承诺，但是非公开的数据交易是行业常态；

- 用户产生的内容，参与应用治理，邀请新用户加入等贡献无法得到有效的奖励。用户推动社区成长的动力有限；
- 应用的开发者们普遍缺乏有效的盈利渠道。广告成为多数应用的唯一收入来源。而广告作为一种对用户打扰极大的方式，其被动的用户体验普遍不被用户所接受；
- 应用之间是封闭的。开放的不涉及隐私的数据无法互通，用户和开发者都耗费了大量的时间和资源去做重复的事情。

例如账户注册，填写信息，选择自己的喜好等。用户的体验和应用的转化率都面临着极大的挑战。

而无论在线上和线下的商业活动中，有效数据的获取和交换一直以来都是绝大多数商业模式成长的源动力。而传统商业数据流转过程中一直以来都存在着以下问题：

- 数据来源具有局限性。数据渠道不公开、不透明。数据拥有者和需求者之间的通道有限；
- 数据的有效性在使用前无法得到验证或者验证成本很高；
- 数据的权益没有一个公平公正的体系进行约定；
- 数据的流通和使用一直处于灰色地带，没有一个公开透明的监管体系对行为加以约束和管理；

- 数据的获取成本极高；
- 数据传输的安全性；
- 数据的使用和归属得不到有效保障，过程无法监管，不透明；
- 数据交易的双方信任成本普遍很高，直接导致了数据的流通性和产生的价值极其有限。

Lemo 的愿景

LemoChain 是未来应用和商业数据的价值传递链，以区块链技术驱动的价值传递生态。Lemo 基金会将致力于通过社区、第三方开发者和技术上的创新，打造一个在全球具有影响力的开源社区生态，最终目的是解决社交、教育、招聘等不同行业的数据价值流通问题。Lemo 是有兼容性的面向 B 端的生态社会，是一个信用系统，一个账户系统，一个数据的流通生态。

Lemo 的原则

针对未来应用领域的潜在需求，Lemo 网络的响应速度是第一要素，否则今后无法承载大型应用，建立生态的愿景也将毫无意义。我们可以看到 CryptoKitties 这一款应用就导致以太坊网络上 2 万笔交易订单被堵塞，迟迟得不到确认，并且耗去了全网 15% 的算力。而基于 DPoS 的石墨烯 /EOS 能够提供 10000TPS 的交易吞吐量和平均 1 秒的确认速度，已经达到了 Visa 规模的交易处理能力，为 Lemo 提供了足够的发展空间。

Lemo 在技术设计中将遵循以下几个原则：

1. 通用

LemoChain 作为一个通用的数据交易区块链，不会偏向某一具体场景。最大化地为各行业解决方案提供施展的舞台。同时 LemoChain 也会提供一定的开发套件和模板，以辅助开发者快速达成这一目标。

2. 易于升级

任何系统都无法避免 bug 和优化，即便是经受住了无数黑客和科学家分析考验的以太币网络，仍然存在升级的需求。然而比特币网络算力的中心化导致矿池拥有绝对的话语权，在比特币用户与矿池之间、甚至不同矿池之间出现利益冲突时比特币网络的进化就无法顺利进行。而另一大区块链技术代表以太坊，也曾因分叉时无法达成共识，导致 ETC 与 ETH 两条分叉链至今仍在并行发展。

经过最充分测试仍然无法避免少量 bug 的出现，LemoChain 必须确保能够简单而无歧义的快速修复这些 bug。

3. 安全、隐私

Lemo 从区块链核心代码到上层应用，都将以保护用户的数据、交易内容等隐私为重要目标。确保除了用户自己，无人能够获取到这些数据。涉及敏感信息的代码还将全部开源以接受用户的审查。同时我们会安排专门的代码审计，以确保整套机制能够抵御恶意攻击。

4. 开放

Lemo 将搭建区块链基础设施，提供便捷的操作接口以及开发套件，与行业伙伴优势共享，共同推动数据交易市场的发展，打造区块链的共赢生态。

更明确的，针对当前区块链技术和现实应用中的局限性和各种问题，Lemo 提出如下改进目标：

- 实现区块链技术对商业应用的兼容性；
- 灵活全面的共识机制；
- 解决现实商业场景中的信用成本与信用问题；
- 条件性释放智能合约与链上数据触发相结合，实现与现实世界的交互；
- 提供通用账户系统，消除应用间的界限；
- 明确所有参与者的权益；
- 帮助参与者将自己确权后的数字资产进行流通；
- 确保数据传输过程中间的安全性和有效性，保障数据所有者的权益。

基于这些目标，Lemo 最终将会为开发者和服务商提供一套包含五个主要模块的解决方案来完善未来的应用数据流通和服务体系：

1. **一个基于多方安全计算和智能合约的数据流通体系，帮助用户进行数据、数字资产的有效交换和流通；**
2. **一个基于区块链智能合约及同态加密技术构建的高速去中心化数据存储和传输体系，帮助开发者、服务提供者、以及用户安全的存储数据（数字资产），确保所有参与者的权益；**
3. **发行 Lemo 代币，作为数字资产的所有权量化证明和流通媒介；**
4. **一个账户系统，为体系内的所有参与者建立通用的账户，消除应用场景间的价值界限；**
5. **一个信用体系，以智能合约约定不同的社区行为带来的信用影响，以去中心化的方式维系社区的价值体系，奖励优质参与者，惩罚或者驱逐劣质的参与者；**

在保障安全性的前提下，将开发者和用户的对立关系，和同一领域不同开发者的竞争关系，转变为同属一个体系的合作者。在 LemoChain 架构上建立的去中心化应用中，用户和不同的开发者都属于参与者。通过贡献自己的产品、开发和运营能力，提供内容、数据、社区治理、流量、存储空间、资产等，获得社区的代币奖励。同时 LemoChain 提供一个数字资产和权益的变现和流通渠道，从而让体系中的所有参与者都能相互配合，并从中获益。

LemoChain 的生态和技术架构

参与者 Stakeholders

LemoChain 的参与者是构成 LemoChain 生态体系的机构或者自然人。从不同的维度加以定义后，我们将 Lemo 生态的参与者分为以下几类：

1. 用户

由 DApps 接入生态。通过创建账户，邀请其他用户加入，贡献内容和用户数据获取 Lemo 奖励。Lemo 同时可以用以支付 DApps 内的应用场景内的服务、存储节点的数据存储服务，或者由 Lemo 主链提供的跨应用确权和交易服务。

2. 开发者 / 应用方

通过在自己的应用中集成并使用 Lemo API 接入生态。通过搭建应用，获取用户，并以加密的方式贡献数据获得 Lemo 奖励。其贡献的数据经 Lemo 确权并报价后可进入数据流通链进行交易，提供给有数据需求的其他参与者，并获得 Lemo。开发者也可以在有数据需求（新的用户来源、商业分析用数据、用户行为等）时，对 LemoChain 链内进行广播。对于没有开发能力的应用方，LemoChain 也将为有限的应用场景提供基础的用户接口和界面，使其可以快速的享受 Lemo 生态带来的利益。

3. 储存节点

通过贡献自己的存储空间和算力接入生态。有限的存储服务器的拥有者可以以存储节点的身份加入到 Lemo 的生态中，通过为整个生态提供去中心化的存储和算力获得各方支付的 Lemo 代币。（由于当前去中心化分布式存储技术的不成熟，数据的安全性还得不到有效保障，LemoChain 生态早期将采用中心化的云存储体系为参与者提供服务，直至数据的去中心化安全性问题得到有效且可验证的解决。）

4. 投资人

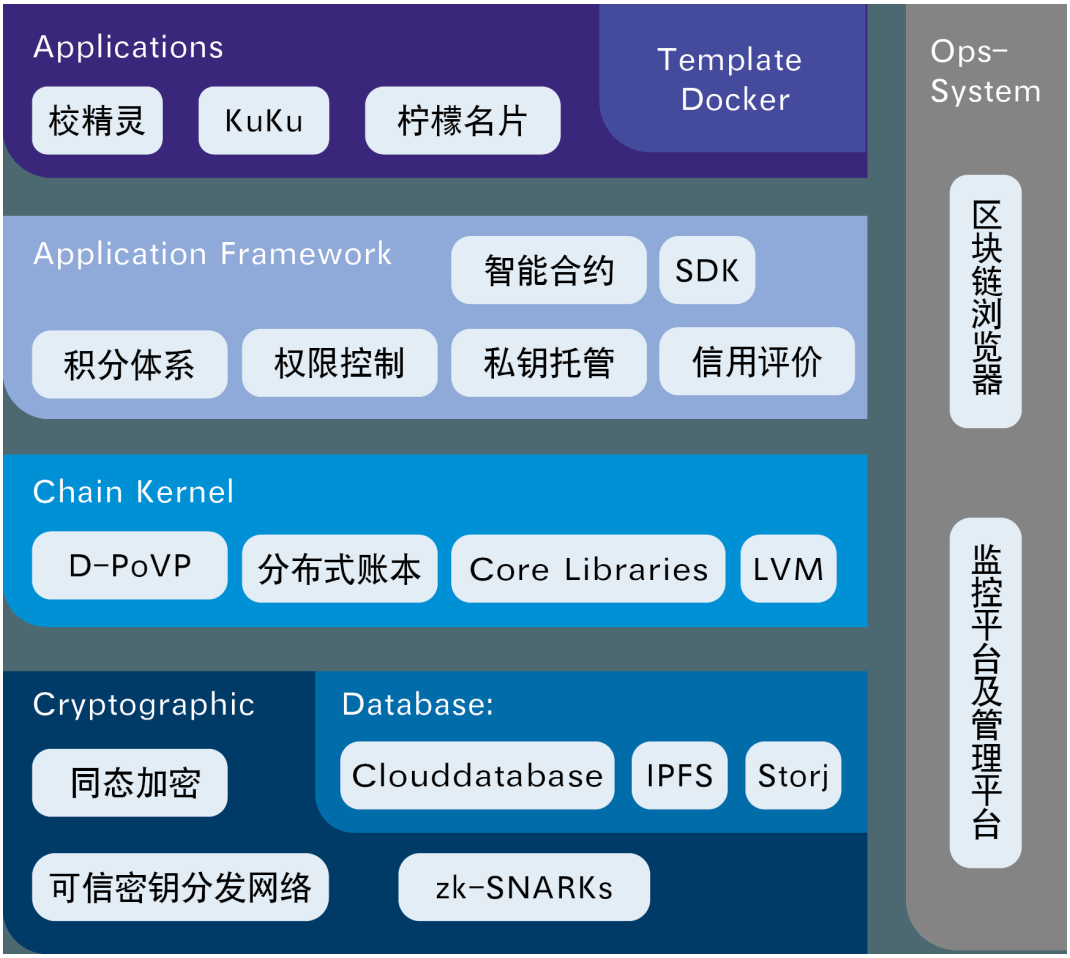
通过 Lemo 代币的预售渠道获得 Lemo 币的早期持有权。投资人是 LemoChain 生态的早期支持者，理念的传播者。通过投资人募集的资金将被用于 LemoChain 的开发，社区建设，市场推广及日常运营，为其他参与者的利益创造基础。

5. 意见领袖

意见领袖由 Lemo 基金会通过多个维度的评价，每 12 个月基于对社区的贡献来确定候选人，然后由社区的参与者投票选举产生。意见领袖可以发起 LemoChain 生态的发展意见，经基金会审核，参与者投票后决定 Lemo 生态未来的发展发向。意见领袖同时拥有 Lemo 基金会的投票权，有权参与所有跟 LemoChain 发展相关的决策，并可获得社区基于其贡献提供的 Lemo 奖励。

LemoChain 的生态对所有人的参与都是开源且免费的。只有当使用到具体的存储、数据等服务的时候才需要支付 Lemo 代币。Lemo 代币可以通过早期对 Lemo 基金会的投资，或者在生态中贡献自己的数据、流量、存储空间和算力、邀请新用户、参与社区治理等获得。

系统架构


Applications
校精灵
KuKu
柠檬名片
Template
Docker
Ops-
System
Application Framework
智能合约
SDK
积分体系
权限控制
私钥托管
信用评价
区块链浏览器
Chain Kernel
D-PoVP
分布式账本
Core Libraries
LVM
监控平台及管理平台
Cryptographic
同态加密
Database:
Clouddatabase
IPFS
Storj
可信密钥分发网络
zk-SNARKs

共识机制

共识机制一直是各区块链研究的热点，普遍的观点认为有效算法是必须符合拜占庭容错原则的。并且需要在尽可能短的时间内做到安全、明确及不可逆，便于提供一个最坚实且去中心化的系统。在实践中，该流程分为两个方面：选择一个独特的节点来产生一个区块，并使得交易总账不可逆。

拜占庭容错问题可以形象地表述为主要解决一个将军可信通信的问题。一群将军想要实现某一个目标（一致进攻或者撤退），单独行动无法完成，必须合作达成共识，但由于叛徒的存在，将军们不知道应该如何达到一致。这里“一致性”是拜占庭将军问题探讨的主要内容。目前解决了拜占庭将军问题的算法已经有很多，下面对比其中几种常见算法。

1. 实用拜占庭容错（PBFT）

PBFT 机制以 IMB HyperLedger fabric 为代表。其描述的一种解决方案核心是状态机副本复制算法。首先由一个主节点负责生产区块，将接收到的交易数据向全网广播。最终每个节点都保存了服务的状态副本。将所有的副本组成的集合总数用 N 表示，使用 0 到 |N|–1 来表示每一个副本，只要不可信的副本（类比于叛徒数）数量 f ⩽ (|N|–1)/3，那么这个系统可以正常运转。在此机制下所有节点最终会达成相同的共识，因而不会分叉。假如主节点离线，备份节点会触发超时机制，依据节点编号推选出下一个主节点。

PBFT 的工作前提是网络中的各节点事先已知，因而只适用于联盟链或私有链。工作在 PBFT 机制下的节点需要两两通信，网络通信复杂度是 O(n^2)，通信量会随节点数量增长而爆发式增长，在公链环境下会导致严重的广播风暴。

2. 工作量证明（Proof of Work，PoW）

PoW 是中本聪 2008 年在一个隐秘的密码学讨论组上贴出了一篇研究报告，报告阐述了他对电子货币的新构想，提出来的比特币共识算法。整个系统中每个节点为整个系统提供计算能力（简称算力），通过一个竞争机制，让计算工作完成最出色的节点获得系统的奖励，也就是完成新生成货币的分配。简单稳定，在吸引了各种黑客和科学家的广泛关注后，仍然经受住了各种攻击。

中本聪试图完成的最大限度的民主和去中心化。因为他设计 POW 的前提是，节点和算

力是均匀分布的，因为通过CPU来进行投票，拥有钱包（节点）数和算力值应该是大致匹配的。随着人们将 CPU 挖矿逐渐升级到 GPU、FPGA，直至 ASIC 矿机挖矿，这条路已经和原来的去中心化、算力均匀分布的初衷渐行渐远。这违背了数字货币的设计理念，导致比特币的用户分裂为持币者和矿工两个人群。他们的利益相互冲突，并且容易遭受算力攻击。

3. 股权证明（Proof of Stake，PoS）

POS 机制可以被描述为一种虚拟挖矿。鉴于 POW 主要依赖于计算机硬件的稀缺性来防止女巫攻击，POS 则主要依赖于区块链自身里的代币。持币人将手中的代币当作押金放入 POS 机制中，这样他们就成为了验证者。PoS 算法会在这些验证者中随机选取一个，给他们权利产生下一个区块。选取的依据是他们投入代币的多少，以及持有代币的时间长短。如果在一定时间内，这个验证者没有产生一个区块，则会重新选出一个验证者来代替来产生新的区块。类似于根据持有代币的量和时间发放利息的一种制度。实际的 PoS 实现还会有一些出块后清空币龄，币龄衰减等机制。POS 机制会带来无法进行算力攻击的优势，因为发起攻击的人需要持有总币量的 51%，攻击导致币值下跌后，自己将会是总币值受损最严重的人。

PoS 机制下一些持币人会长期、大额持有代币以获得更大的投票权重。因此整个网络中的流通代币会减少，价格也更易受到波动。由于可能会存在少量大户或矿池持有整个网络中大多数代币的情况，整个网络有可能会随着运行时间的增长而越来越趋向于中心化。

4. 股份授权证明机制（Delegate Proof of Stake，DPoS）

DPoS 共识机制在 PoS 的基础上牺牲了一定去中心化的特性，大大加速了交易确认的耗时。其主要原理是在所有节点中随机选出数量有限的代理人节点，由这些节点轮流记账，以代理人的共识作为全网共识。新区块奖励由代理人和投票人共同分享。为了避免恶意节点成为代理人后对区块链造成不良影响，DPoS 机制需要在一定时间后重新选举代理人。

DPoS 目前已经具有成熟稳定、吞吐量高的优点。只需代理节点达成共识即可确认交易，其交易频次甚至可以达到中心化的 Visa 结算规模。

5. 价值参与权益证明（Delegated Proof of Valuable Participation，DPoVP）

为了促进 Lemo 平台中各应用生态的发展，促进用户更多地贡献价值，Lemo 以 DPoS 共识机制为基础发展出了全新的 DPoVP 机制。这一技术的代表性特征是定义了多种，而不仅仅是以租售闲置计算机资源的模式获取代币 / 积分体系。支持多种维度，可将用户的行为数值化。累加求和后作为用户对平台忠诚度、贡献度的衡量依据，同时可以作为激励用户的

一种运营手段。防刷，且各业务可定制。所有参与者都将基于自己对整个生态体系的贡献获得 Token，将传统的‘挖矿’方式从算力和存储等技术角度延伸到现实的商业价值领域。

吞吐量

如何提高区块链网络的吞吐能力是一个非常现实的问题。目前比特币网络的出块时间为 10 分钟，平均每日确认 30 万笔交易，交易确认时间最少为 1 个小时，远远达不到一个金融工具的结算能力要求。以太币网络的平均确认时间约为 14 秒，面对现象级应用，容易出现网络拥堵，长期不能恢复，无法承载大型应用。因此 LemoChain 选择以响应速度高为特性的 DPoVP 技术来解决该问题。

DPoVP 基于 DPoS 做了大量优化，采用顺序出块的规则，一旦上个见证人出的块收到三分之二节点的确认，就可以立即开始生产下一个区块。相当于出块的时间间隔仅仅受限于网络传输速度，在通常情况下能够达到小于 1s 的平均确认速度和平均 8000TPS 的数据吞吐量。

2.1 投票

为了保持功能的独立性和扩展性，Lemo 采用智能合约来实现投票功能。节点通过该合约注册为候选人，接受用户投票。最终根据投票结果选出前 21 个节点作为见证人。

2.2 调度

见证人按照地址的字典序依次出块。在自己出块或收到新块后需要重新计算自己的出块倒计时，时间归零后直接在当前链上出新的块。倒计时计算公式如下：

$$
\mathrm{T}=\begin{cases} t_w & ,d\left(I_{me},\ I_{receive}\right)=1 \\ \left(d\left(I_{me},I_{header}\right)-1\right)*t_o & ,d\left(I_{me},\ I_{receive}\right)>1 \\ T & ,d\left(I_{receive},I_{header}\right)<0\cup d\left(I_{receive},I_{header}\right)>1 \end{cases}
$$

其中 d 表示两个出块序号的距离：

$$d(a, b) = \left(\left(I_a - I_b \right) + C \right) mod\, C)$$

t_w 表示轮到当前节点出块时的等待时间。这是为了防止出块过快，导致早期交易少时链上全是空块；

I_{me} 表示当前节点的出块序号；

I_{header} 表示当前 *header* 区块的出块者的序号；

$I_{receive}$ 表示收到区块的出块者的序号；

C 表示节点数量；

t_o 表示轮到该节点出块后的最大可出块时间，超过这个时间则下一个节点应该立即出块；

T 公式的最后一行表示出块倒计时无需重新计算。

当生产出一个新的区块后，会首先在见证人之间进行广播，三分之二的见证人节点确认后，我们就认为这个区块进入了“最终确认状态”。此时才会向全网进行广播。因此广播出来的区块一定是完成了共识的，不会分叉。普通节点收到广播的区块并通过校验后，即可放心地将该区块保存下来。

影响交易确认速度的因素仅仅取决于两个部分，见证人节点之间达成共识的耗时，交易和最终区块在普通节点和见证人节点之间传播的耗时。为了进一步提高交易确认速度，见证人节点将会辅助其它见证节点广播确认信息。这样能够更快地将确认信息广播到所有见证节点，提升恶劣网络环境下达成共识的速度。

2.3 同时出块风险的应对能力

假设某时刻通信正常，A 节点正在出块，B 节点应在 10 秒时出块，C 节点应在 20 秒时出块。

A 迅速出块并广播，但没能同步到 B 节点，只同步到了 C 节点。C 节点重 新计算出块时间可能在 10.3 秒。这导致 B、C 节点在非常近的时间内相继出块，并广播到其它见证节点，导致分叉，无法达成三分之二共识。

按照时间计算公式，见证节点收到不连续的块时不会重新计算（缩短）出块时间，并且会辅助广播其它节点的确认信息。各节点尽量收齐所有分支上的块后才做决策。

分叉的选择规则是：优先选择最长链，相同长度时优先选择根部连续的链。如：

$$A \leftarrow C \leftarrow D \leftarrow E > A \leftarrow B \leftarrow D > A \leftarrow C \leftarrow E$$

所有节点按照同样的规则选择分叉链，达到三分之二共识后该链上所有块进入“最终确认状态”，向普通节点广播。由于分叉发生在共识节点上，对于只接收进入“最终确认状态”区块的普通节点没有任何影响。

2.4 共识网络分裂风险的应对能力

假设 21 个共识节点有 11 个在中国，10 个在美国。由于光缆中断等特殊情况导致网络被分裂为两个无法互通的部分，各自产生一条分叉链。这里将两个网络命名为 C 和 A。

各节点会持续计算倒计时并出块，但永远无法收到超过三分之二的节点共识。见证人不再向普通节点广播区块。

以 C 网络为例，忽略出块时间和网络传输耗时的情况下，各节点循环一轮（生成 C_C 个块）的时间与 A 网络节点数线性相关，即 $C_A \times t_o$，因此平均出块间隔为：

$$\frac{C_A \times t_o}{C_C}$$

显然同样时间下见证节点多的一边会产出更多的区块。光缆恢复后见证人网络连通，新区块能够广播到所有节点，各节点顺着父块 hash 拉取到完整的分叉链，根据最长链原则，选出最终链。于是该链上的各区块达成三分之二共识，开始向普通节点广播。

这种情况下确认出块的过程将会停滞一段时间，但对于链上交易并没有安全风险。

数据储存

LemoChain 旨在打造一个去中心化的数据确权和流通平台，参与者数据的安全存储、加密传输、版权归属至关重要。而区块链的安全性很大程度上取决于它被大量节点镜像复制并且 100%可用，在链上存储大型的易变的文件将会带来超高的成本消耗。例如，存在一款每秒处理 100 万交易的高性能区块链应用，每笔交易产生 100 个字节的记录，则消耗的存储空间将会以超过 100MB/s 的速度增长。为了保持实用性，需要定期截断区块链上的交易记录并且保存区块链状态快照。然而，完整的交易记录仍会被复制到每一个节点，造成了不必要的备份开销。因此将大尺寸的数据保存在区块链中是一个既不实用的也不可扩展的分散文件存储解决方案。

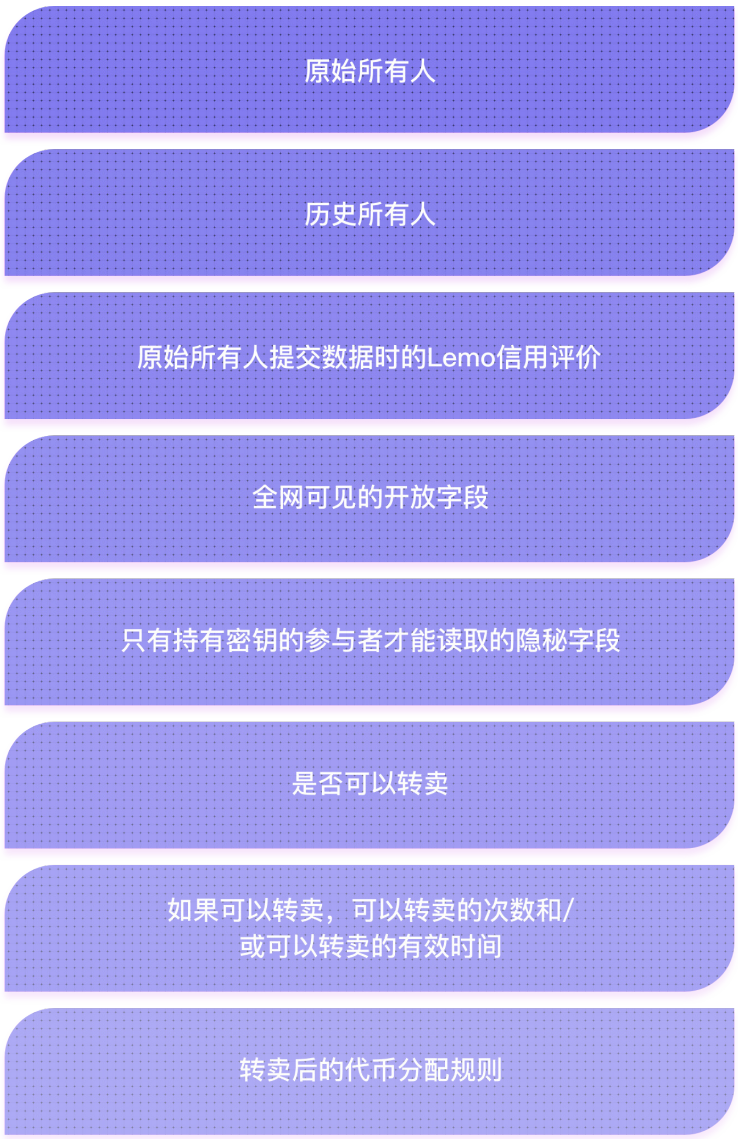
为了解决这个问题，LemoChain 将数据层分离，进行链外存储。只在链上记录数据的摘要信息，大大降低了区块链的存储压力。按照不同的场景，综合考虑了应用业务可能会用到的各种字段，抽象出统一的对外接口。支持灵活对接去中心化的 IPFS、storj 文件系统，中心化的云数据库等方案。也为用户提供了更多样化的选择。为了进一步简化应用平台接口对接的工作，LemoChain 配套提供了存储系统适配 SDK，封装了公私钥对生成、地址生成、签名、验签、加密、解密等函数，屏蔽较为复杂的签名生成规则、编码转换问题，以及多种底层错误码处理逻辑。在接口上可选择引入用户身份管理模块和私钥存储模块，降低业务应用的公私钥管理负担。方便业务开发者直接使用。

IPFS 是一个面向全球的、点对点的分布式版本文件系统，具备传统文件存储系统无法比拟的确定性和不可篡改性。也降低了数据中心故障造成的数据丢失风险。IPFS 的 p2p 网络使用的是 DHT 技术，用基于内容的地址替代基于域名的地址。用户依据文件内容进行文件寻址而不是文件路径，读取时也不再需要对进行身份验证，只需要验证文件内容的哈希。LemoChain 会将用户的数据加密后存储到 IPFS 系统中，任何人可以根据交易获得的私钥自行获取数据，无需依赖中心化的应用。这类文件系统为了保证文件冗余可靠，需要用户支付代币以激励提供存储服务的节点长期在线。否则一旦过多节点离线，将会导致文件的部分碎片无法取回。

中心化的云数据库将建立在世界级的大型云服务供应商的体系之上，具有稳定、可靠、低成本的特点。能够提供 99.99999999% 的数据可靠性，99.9% 的可用性，高达 200gbps 的吞吐和低至 1ms 的延时性能。Lemo 会加密保存用户数据，并开源代码，以取得用户的信任，

确保用户数据的隐私不受侵犯。

在 Lemo 网络中流通的所有数据都将是包含了使用条款的加密数据包。使用条款由经 LemoChain 价值链确权的原始所有人确定后，由包含了数据流通智能合约的 Lemo 代币帮助其进行流通和交易。LemoChain 将帮助参与者定义数据的以下信息和流通机制：



撮合交易

传统的私有数据撮合交易场景中，交易双方的数据需要互相披露，或交由可信任的第三方进行匹配。在目前多变和充满恶意的环境中，这是极具风险的。第三方在交易中的话语权过大，存在泄漏、篡改、隐瞒双方数据的可能。因此，可以支持联合计算并保护参与者私密的协议变得日益重要。LemoChain 致力于引入安全多方计算 (Secure Multi-party Computation，SMC) 来解决该问题。

安全多方计算是解决一组互不信任的参与方之间保护隐私的协同计算问题，SMC 需要确保输入的独立性、计算正确性，同时各输入值也不泄露给参与方。通常，一个安全多方计算问题在一个分布网络上计算基于任何输入的任何概率函数，每个输入方在这个分布网络上都拥有一个输入，而这个分布网络要确保输入的独立性，计算的正确性，而且除了各自的输入外，不透露其他任何可用于推导其他输入和输出的信息。

以婚恋网站配对为例，将用户的条件与特征映射为 t 维空间中的点。

$$P = (x_1, x_2, \cdots, x_t), x_i \in [0, 1]$$

设需求方期望的目标为 a，数据提供方的数据为 $B=b_1, b_2, \ldots, b_n$, 满足

$$a, b_i \in P$$

撮合交易算法可归纳为 t 维空间上的最近邻算法 NN，即求出 满足 a、b 间的距离 d 最小。

$$b` = NN(a, B) = \min_{i=1,\cdots,n} d(a, b_i)$$

为了保护 B 数据隐私不泄漏，区块链中的计算节点需要与数据 a、b 隔离，只能获取到加密后的数据。因此 LemoChain 引入全同态加密算法（Full Homomorphic Encryption）来进行数据匹配计算处理。全同态加密能够在没有解密密钥的条件下，对加密数据进行任意复

杂的操作，以实现安全的明文计算。

设加密算法为 $E(x)=c_X$ ，解密算法为 $D(x)=p_X$ ，有：

$$b` = NN(a, B) = D\left(NN\left(c_a, c_B\right)\right)$$

受同态加密算法的性能限制，LemoChain 选取欧氏距离的平方来进行匹配度计算。则最优匹配计算公式为：

$$b` = NN(a, B) = D\left(\min_{i=1,\cdots,n} d\left(c_a, c_{b_i}\right)\right) = D\left(\min_{i=1,\cdots,n} \sum_{j=1}^{t} \left(c_{a_j} - c_{b_{ij}}\right)^2\right)$$

经由上式计算出 b` 后，查询方获得了最佳匹配目标。整个匹配过程中代理计算节点和查询方无法接触到加密前的其它用户数据，用户数据的私密性得到保障。

智能合约

智能合约是传统合约的数字化版本，一旦编写好就可以被用户信赖，合约条款不能被改变，具备不可更改性。该理念早在 1994 年由密码学家尼克萨博（Nick Szabo）提出，直到区块链技术出现后才得以实现。从本质上讲，智能合约是在区块链数据库上运行的计算机程序，可由预先编好的条件触发自行执行。区块链技术带来了一个去中心化的，不可篡改的，高可靠性的系统。在这种环境下，智能合约才大有用武之地。智能合约是区块链最重要的特性之一，也是区块链能够被称为颠覆性技术的主要原因。它正使我们的社会结构发生日新月异的变革。

LemoChain 智能合约支持 Java，C/C++，Python 等多种语言，所有智能合约源码被编译成字节码在虚拟机中运行。并利用沙盒（Sandbox）技术实现了对事务彻底的隔离以及限制对计算资源的访问，达到性能与安全的最大化。

LemoChain 的智能合约虚拟机建立在以 LLVM(Low Level Virtual Machine) 为基础的编译器架构上。LLVM 支持 JIT(Just-In-Time Compilation) 技术，可根据需要，动态编译并执行生成的机器码，能够大幅提升动态语言的执行速度，最大化地发挥硬件性能。基于 LLVM 强大的三段式设计，未来 LemoChain 智能合约还将支持 JavaScript 等更多语言，将最大程度方便不同技术背景的开发者进行智能合约的开发工作。

智能合约包括合约的注册、触发、执行以及注销四个部分。

合约注册

合约注册是将用户编写好的合约安全检查处理之后，共识存储到区块链的过程。用户注册一个合约时需要依据代码量消耗 gas。

合约触发

合约触发是在合约注册之后，通过外部条件来触发合约执行的过程，支持定时触发、事件触发、交易触发和其他合约触发的方式。定时触发是指满足合约中预设的时间之后，节点就触发时间共识之后，自动触发合约调用的过程。事件、交易和其他合约调用都是一次新的请求，在共识过程中触发合约执行。

合约执行

合约执行是合约代码在独立的环境中运行的完整过程，包括对合约构造镜像环境、代码执行、执行代码中状态修改的共识以及共识的异常处理。其中存在一种特殊的消息调用，叫做代理调用。除了目标地址的代码在调用方的上下文环境中被执行，其他都和消息调用一样。这就意味着合约可以在运行时动态地加载其他地址的代码。只有代码是从被调用方中获取。这就使得我们可以方便地将代码封装成库，在其它合约中复用。比如为了实现复杂的数据结构，可重用的代码可以应用于合约存储中。

合约注销

是对已经执行过、过期作废或者业务需求变更不再需要的合约进行转存，清理。清理的过程需要多节点共识之后才能完成。区块链中移除代码的唯一方法是合约在它的地址上执行了 selfdestruct 操作。这个账号下剩余的余额会发送给指定的目标，存储和代码从栈中删除。

LemoChain 提供了一部分标准合约实现。包括资产一致性检查、自动撮合成交、多重签名、到期自动清算等逻辑相对简单的合约。用户可调用或对这些合约进行改造，以适配自身业务需求。也可以完全自己实现。

应用层服务

LemoChain 在应用层提供了丰富的应用开发框架和灵活的部署方式，方便不同类型的开发者快速接入，构建应用。

账户系统

在去中心化的区块链世界中，用户的财产只有自己可以掌握，任何人和机构都无法盗用，也不存在被服务器黑客攻破导致账号被盗的可能。但事实上大部分用户无法妥善管理好自己的账户私钥。据德勤（Deloitte）公司统计，至少有 37% 的用户登陆网站的时候会忘记密码，从而使用“找回密码”的功能。在区块链上忘记私钥则会导致财产直接消失，没有任何途径可以找回来。到目前为止因此消失的比特币已达 400 万个，占总币量 23%。用户对私钥安全托管的需求非常强烈。

LemoChain 的账户体系主要解决用户身份到区块链地址的映射关系、用户隐私的保密性以及监管审计的可追踪性问题。允许用户使用易于记忆的用户名和密码进行访问，并提供了 OAuth2.0 认证机制。取得用户授权的第三方应用可以方便地获取用户基本信息，而不需要自行实现和维护用户账号的管理逻辑。最终只需短短几行代码即可接入 LemoChain 生态。

基于账号系统，LemoChain 在 SDK 中实现了一些常用的业务单元插件，开发者可以根据自身业务需求，快速集成到自己的 DApp 应用中。极大地缩短了项目的开发周期。

- 线上保险箱。将私钥加密后托管备份在线上，只能由用户自己取回。
- 通讯录。管理维护用户持有的众多代币地址，以及近期交易对象的地址信息。
- 积分体系。支持多种维度，可将用户的行为数值化。累加求和后作为用户对平台忠诚度、贡献度的衡量依据，同时可以作为激励用户的一种运营手段。
- 信用评价。通过一些基础的实名身份认证服务对用户初始信用进行评估，再根据用户的后期表现不断修正评估结果。整个评估结果都会作为信用记录写入区块链中，可以为数据交易软件的买卖双方提供强有力的信用依据。
- 权限配置。允许在账号与账号、账号与应用之间建立授权关系。通过权限与许可机制建立更为高阶的数据流转控制逻辑。

线上保险箱

线上保险箱是 LemoChain 提供的用户私钥安全托管的功能，旨在减轻用户的安全负担。首先在本地客户端对用户的私钥进行加密，然后上传到 LemoChain 的私钥保险箱中。当用户私钥丢失后，可以通过提供认证信息将加密后的私钥取回，并在本地进行解密。整个过程中私钥和密码的明文都不会出现在互联网上，也不会出现在 LemoChain 服务器中，私钥安全得到了保障。只有用户自己才能解密保存在网络上的私有数据。

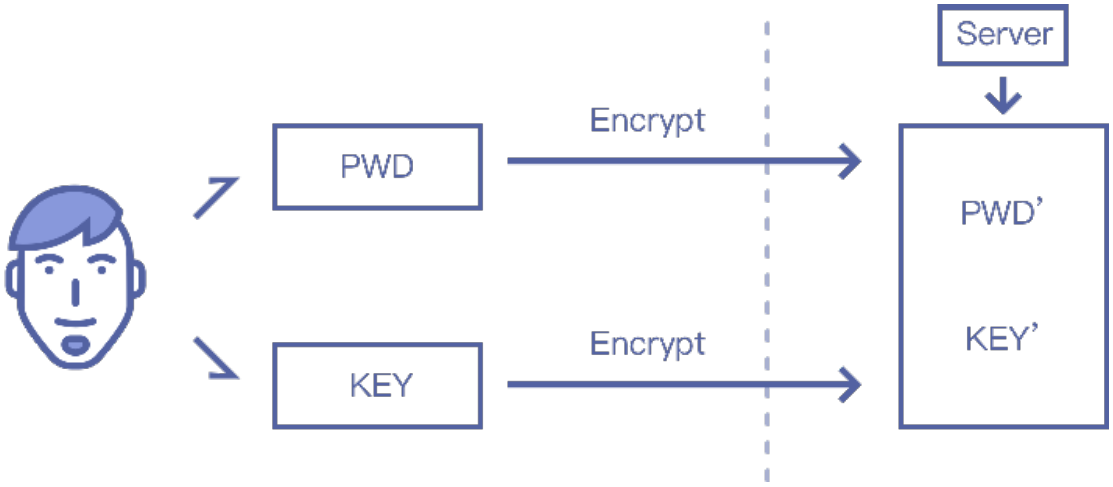


图 1 托管私钥

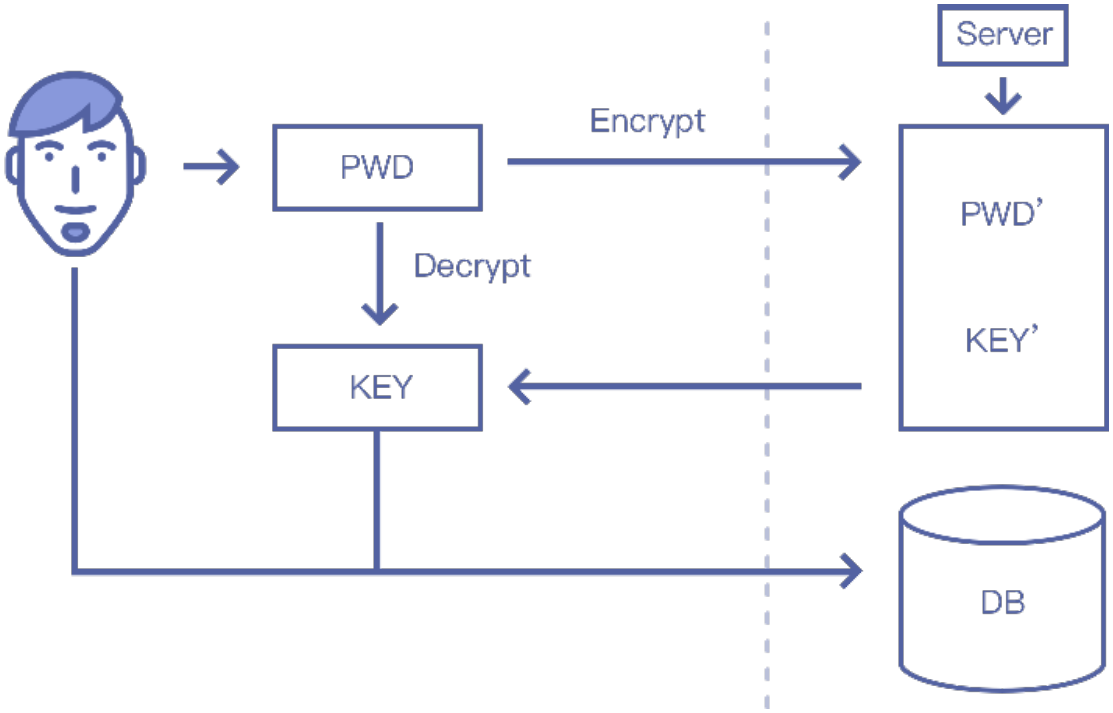


图 2 找回私钥

为避免可能的恶意攻击造成服务器数据库数据泄漏造成损失。线上保险箱的秘钥存储将采用三方加密技术，将数据交由隔离的第三方服务器加密处理后再进行存储。即便加密后的私钥数据被盗，也无法还原出任何可利用的真实信息。

数据交易所模版

为了帮助开发者更快地实现各自行业的数据交易功能，LemoChain 基于婚恋交友场景实现了一套去中心化的数据交易系统的应用示例。

将所有的匹配需求作为交易数据在链上挂单，通过智能合约进行自动撮合交易。当匹配成功时双方互相发送数据解密私钥，确保用户的隐私只有匹配双方才可以见到。整个交易过程公开透明，隐私信息不会泄漏给第三者，交易所也无法做到欺诈隐瞒。解决了传统数据交易所安全、信任的问题。

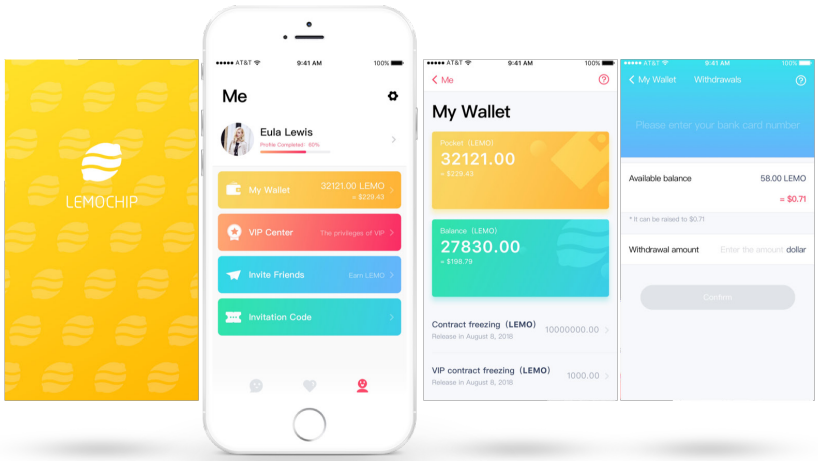
这套应用向开发者展示了 LemoChain 的智能合约，以及各项服务的使用方法，是最佳的开发者入门学习资料。并且可以作为模板衍生出其它领域的数据交易应用。

钱包工具

为方便 Lemo 代币持有者方便的查看自己的余额、查询和追踪交易记录、奖励记录，并接受 LemoChain 社区的相关资讯，我们开发了 Lemo 的钱包应用。目前针对 iOS 和微信小程序两个平台进行了开发。其中小程序应用已经可以通过搜索 LemoWallet 获得。

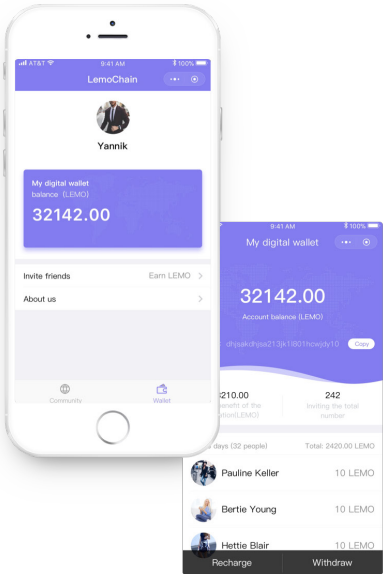
iOS App

LemoChip



Mini Program

LemoChain



基于 LemoChain 的应用前景

LemoChain 基于去中心化的区块链网络打造了一个足以支持每日数以千万级的活跃用户的平台。依托于去中心化、标准化的数据存储机制，降低各方面的参与成本。

LemoChain 的生态架构如下：

- 对于开发者：我们开放数据交换 API，统计分析 API，深度学习 API
- 对于企业：数据交易、算法交易、企业 DApp
- 对于开源社区：区块链技术研发成果数据交易

这个过程中，生态对用户数据进行确权。

多个行业的支持

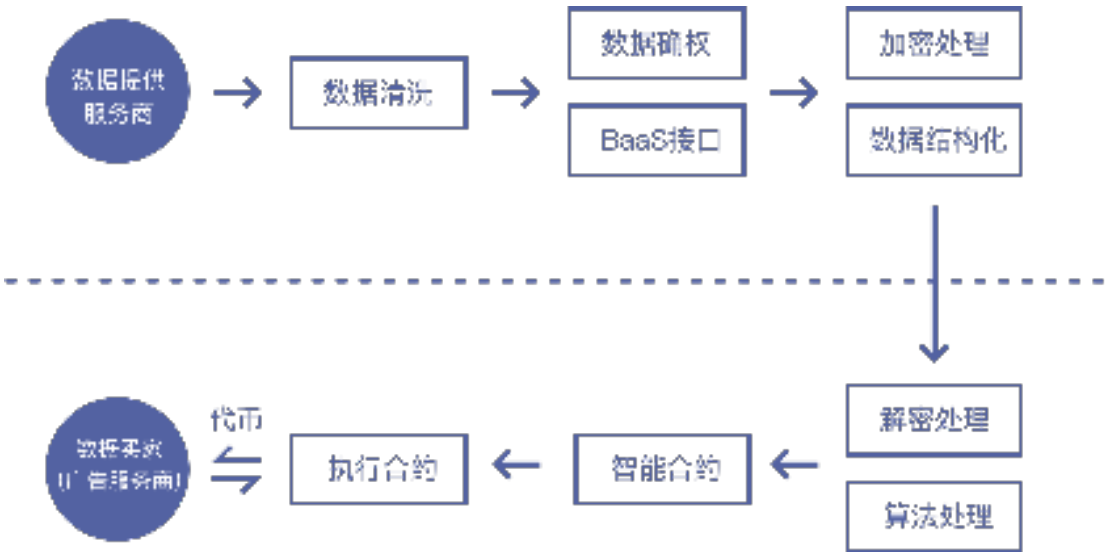
在 LemoChain 的生态中我们将引入更多行业共识机制并满足其监管的需求，可以支持多个有信用缺陷和数据价值传递缺陷的行业，并提供相应的技术支持。例如：社交、教育、招聘、金融等。另外基于 LemoChain 的数据流通智能合约和信用体系，通过图灵完备的编程语言，可以实现更复杂商业逻辑的支持。

应用场景

Lemo 是做社交起家，早在 2016 年，Lemo 团队就曾经尝试在自有的几个社交产品之间进行数据交换，提升过剩流量的复用率，由此大大增加了各个 APP 的盈收。当时我们的整体付费率从 6.5% 提升到了 11.5%，几个月的时间营业额翻了接近一倍。

仅仅几个 APP 之间的数据共享，就可以达到这样的效果，那么假设更多商家可以加入，为商家带来的收益可想而知。

但是在我们尝试邀请更多其他社交 APP 参与其中时，信任问题成为最大的障碍。这让我们意识到目前商家对于数据共享的强烈需求，以及面临的巨大困难。而区块链去中心化存储的特点及数据确权技术，以及背后的经济价值体系完美解决这一问题，Lemo 的诞生就是为了解决这些问题。



应用场景一：区块链技术应用于婚恋社交

用户通过婚恋交友 DApp，提交个人的数据及其交友需求， 个人可以将自己的社交数据加密存储，然后数字资产确权，上传至可获收益平台，并能获取代币。广告商、及其其他婚恋交友平台商需要支付代币来获取此数据，可以用于交友精准匹配、广告精准投放，流量共享等应用场景。

应用场景二：健康医疗数据 DAPP

通过健康数据 DAPP，实现个人健康数据的安全保护、数据共享、方便使用等。个人将自己的健康数据上传至可获利数据平台，并能获取代币。医疗服务商、药厂等数据买家需要时直接从可获利数据链上调取即可，在新药研发、测试、精准 医疗等方向有巨大的应用场景。

应用场景三：区块链技术应用于教育与人力资源领域

教育育培训行业中会有各种语言培训机构、素质教育培训机构，这些机构之间其实不是竞争关系，完全可以资源共享，互通有无。但是现在的情况是，这些机构各自花费了大量的人力、财力以及时间成本，获取市场资源（其中还总是有一些资源属于无效资源）。如果通过 Lemo 解决机构间的信任和生源确权问题，可以通过共同招生的形式资源共享，增加生源，降低获客成本，增加盈收。

而一种以区块链技术为基础的教育，技能，与职业经历信息平台。基于区块链技术的不可篡改性和时间戳功能，为用人机构提供一个可认证的学历，技能，与职业经历信息源，从而为企业在招聘过程中节省大量用于背景调查的人力和财力。此技术系统还可广泛应用于公证，金融，银行等行业的文书认证，具有广泛的应用前景。

区块链技术从根本上解决数据流通的信任问题，然后在其基础上实现去中心化。而LemoChain生态将致力于从技术层面全面支持去中心化应用，开发不同的模块如: 账户系统，信用系统，数据流通协议等，提供适用于不同开发者和服务商的开发平台和接口，节约开发成本，从而帮助他们快速迭代，增加盈利手段。另外通过激励策略，吸引更多的开发者加入LemoChain，将 DApp 想法产品化，使普通互联网用户享受区块链技术带来的价值。

Lemo 代币的发行

创始代币

LemoChain 已经创建了 LemoChain 的创始代币 Lemo，这是一种在公开预售之前发行的 ERC-20 代币，并且在预售结束且主链上线之后可以 1 比 1 兑换成基于 LemoChain 网络的代币。

Lemo 即将向 LemoChain 社区成员和投资者发行。他们将与 LemoChain 一起并肩前行，与 LemoChain 有着共同的愿景一起去创造价值，改变数据流通的未来。在 LemoChain 的漫长发展中，这些早期参与者将是社区讨论、提供反馈和建议的主力，会帮助 LemoChain 变得更完善，并通过社区推广来支持 LemoChain 的发展。

Lemo 是基于以太坊创建的代币合约，是在以太坊网络发行的去中心化区块链数字资产，Lemo 发行总量为 16 亿，（“矿前”总量），并会以不超过 25,000,000 Lemos / 年的速度产生新的代币。新代币的产生将在 LemoChain 的主链上遵循 D-PoVP 的机制， 通过贡献数据、存储空间和算力、社区贡献等获得。挖矿的模型和算法还在设计之中，可挖总量将在挖矿规则和节点部署等问题解决后确定。但未来总量将一定不会超过 25 亿枚代币。

Lemo 预售方案

LemoChain 将发行矿前总共 16 亿 Lemo，25%（4 亿）的 Lemo 代币将以每 1 个 ETH 换得 9000 个 Lemo 的比例，在预售时期分私募和公募两个阶段分配给参与者，总募集硬顶 20000 个 ETH，软顶 2000 个 ETH。预售将分阶段从 2018 年 3 月开始分阶段释放给不同的参与者，并会根据参与者的贡献在私募阶段给予不超过 20% 的赠送额度。预售持续至 2018 年 5 月中下旬，或在触及到硬顶上限之后 24 小时内停止。

预售期结束后，后续的投资者也将可以通过各大加密货币交易所以合规的方式获得 Lemo 代币。Lemo 将在 6 月初开始逐步上线全球范围的加密货币交易所。

Lemo 代币是数据价值传递的载体，在 Lemo 生态内具有量化数据价值的属性， 但不会以任何方式参与 Lemo 生态以外的流通。

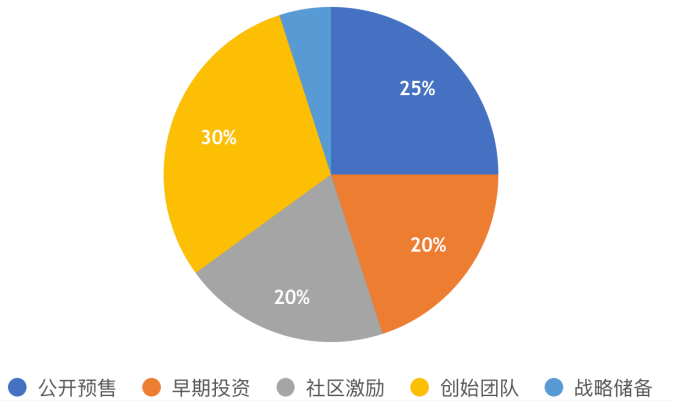
概况

Lemo代币预售方案

描述	币量
矿前总量	1,600,000,000 Lemo (100%)
预售量	400,000,000 Lemo (25%)

- 25% 的矿前 Lemo 代币会在预售期将被创造并发送至的预售参与者的智能合约地址。参与者可以通过由 LemoChain 提供的钱包应用，或者于以太坊网络上查看和管理；
- 20% 的矿前 Lemo 代币将被创造对有影响力投资人非公开预售，锁仓并配币回馈他们在项目早期对 LemoChain 的支持；
- 20% 的矿前 Lemo 代币被用于早期社区激励，将持续奖励用户，开发者等参与者加入 LemoChain 生态、参与社区的建设；
- 30% 的矿前 Lemo 代币将被创造并分配给 LemoChain 核心开发者、创始人和团队，并被锁定在一个为期 48 个月的期权智能合约中，每 6 个月行权一次；
- 5% 的 Lemo 代币储备将被锁定至少 12 个月，作为战略储备，并且周期性的逐步分配给新的贡献者。其前提是对整个 Lemo 社区的成长有益。否则，这些储备将被销毁。

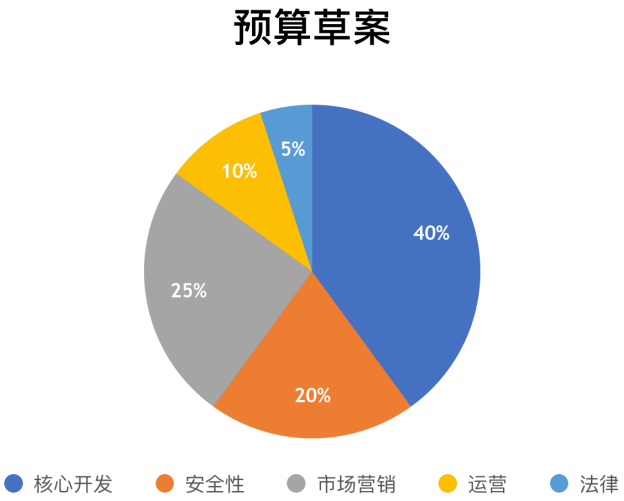
矿前代币分配



预售

在预售期间募集到的资金将只用于对 LemoChain 生态的开发和利益有帮助的方向。LemoChain 的技术研究表明了这些技术可以在相关领域的可行性，但是也认识到 Lemo 社区的工作任重而道远。

以下是一份预算草案：



40% 核心开发

核心开发包括 LemoChain 的核心技术开发以及智能合约和去中心化场景开发。该预算的很大一部部分将用于基础架构的构建，优化终端用户的用户体验和实现新功能。

20% 安全性

LemoChain 正在建造的基础依赖于 LemoChain 区块链的安全性。LemoChain 正在计划一系列的安全审计，每一个新的主要功能的引入都需要进行额外的审计，然后才考虑在主网络上的部署。

25% 市场营销

考虑到 Lemo 早期奖励引擎的设计，LemoChain 将奖励和支持优质开发者的早期贡献，

并奖励其用户去邀请更多的用户加入，一起维持社区的繁荣。

10% 运营

为了确保在整个组织发展过程中的日常运营能够顺利地进行，Lemo 基金会将会对社区的运营和管理给予更大的关注，并且需要获取更多的全球运营资源。

5% 法律

合规性是 LemoChain 生态长期成功的关键，LemoChain 将把预算分配到法律成本中，将确保 LemoChain 在进入全球任何市场的时候都将符合各类监管的要求。

早期代币持有者的解锁计划

为保障 LemoChain 整个社区的持续繁荣，早期的代币持有者的 Lemo 代币将会有一定的锁定期。以下为相关细节：

创始团队

创始团队所持有的 Lemo 代币只能分阶段的逐步解冻。并且每次解冻都需要得到基金会决策委员会的支持。

	时间	比例
第一次	2019.01	10%
第二次	2019.07	10%
第三次	2020.01	10%
第四次	2020.07	10%
第五次	2021.01	10%
第六次	2021.07	10%
第七次	2022.01	10%
第八次	2022.07	10%
第九次	2023.01	10%
第十次	2023.07	10%

早期机构投资者

预售结束以后，早期投资者持有的 Lemo 代币溢价的部分将被锁定，并将分四次解锁。自上交易所 30 天后为第一次解锁，间隔 30 天后第二次解锁，之后每隔 45 天分两次，一共四次每次解锁 25%。锁定的代币将会在解锁条件触发后由系统直接发送至持有人提供的加密货币钱包地址。

LemoChain 的治理生态架构

为实现 LemoChain 的可持续发展，避免散沙式的发展结构和底层架构分化，Lemo Foundation LTD（Lemo 基金会），一个注册地为新加坡的非盈利性组织，会负责监督生态系统的公平和生产性增长，同时将制定完善的治理架构，成立常务委员会，对代码管理、财务管理、薪酬管理、更新迭代管理和特权操作范围等事务进行管理。同时，常务委员会跟随着基金会和社区的发展不断更新，并引入监察和监督机制，规则制定和变更控制管理等。最终，Lemo 基金会将促进整个生态系统向完全去中心化和自主网络过渡。 Lemo Foundation LTD 将通过与合作伙伴的全力合作，将政府、企业、技术、商业、大学等多个方面的资源进行整合，最大化的实现资源共享，高效的利用资源，实现社会协同发展。

与此同时，Lemo Foundation LTD 还将提供透明化的财务管理，全面的代码管理、技术研发、市场营销、安全性研发等的管理，帮助 LemoChain 进行商业推广。同时基金会将积极倡导高标准的道德和诚信的商业行为，遵守相关的法律法规。此外，Lemo Foundation LTD 将聘用第三方的权威机构通过相关工作的审计报告，合规的监管和监督 LemoChain 的发展。

Lemo Foundation LTD

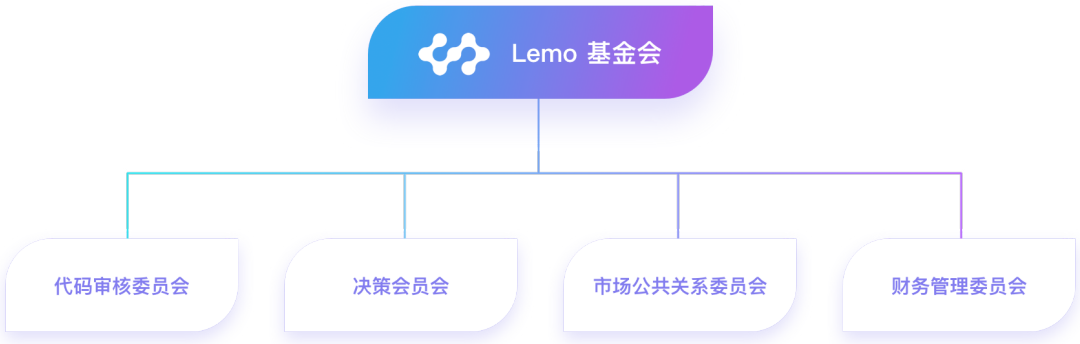
Lemo Foundation LTD（以下简称“Lemo 基金会”）将致力于促进 LemoChain 的研发建设和治理及推进工作，驱动整个 LemoChain 开源生态体系的安全与和谐发展，将公开、公正且透明的不以盈利为目的地运营 LemoChain。

Lemo Foundation LTD 是将由新加坡会计与企业管理区（ACRA）批准建立的非盈利组织（Non-Profit Entity），受新加坡公司法监管。该基金会由具备受该基金会受托资格的自然人或者法人组成的受托董事会或管理委员会（即下文中的决策委员会）独立管理运营。依照新加坡法律，Lemo 基金会是为支持或参与公共或私人利益活动，而不具任何商业利益的合法成立的组织。其所获的“利润”被称为盈余，将被继续保留作为其它活动的经费，而不在其参与者中进行分配。

Lemo 基金会会在不同国家开展活动的过程中，建立符合当地法规的内容审查和运营委员会，以保证其全球范围的合规性。

比特币与以太坊的多次分叉，使得人们对以太坊或者区块链的去中心化理念产生质疑。为避面出现分叉的局面，Lemo 基金会将制定良好的治理架构，帮助与推动整个社区的和谐发展。

Lemo 基金会的成立，是为了保证整个社区及其开源项目的可持续性、募集资金的安全性及其社区的管理。基金会成立初期将由创始团队组成，组织架构由决策委员会、研发代码审核委员会、财物及人事委员会和市场公共关系委员会组成。决策委员会由基金会首任主席 Andrew、LemoChain 核心研发人员和早期投资人组成，每任期两年。未来的决策委员会席位也将在组织架构和参与者数量的增加后，开放给更多的参与者。



LemoChain 创始团队

LemoChain 团队由来自硅谷、新加坡、伦敦、中国等地的高科技人士组成，融合了硅谷的技术创新、新加坡的高效能、伦敦的金融数据能力和腾讯，360 等公司的研发高品质。团队拥有多年海量用户数据构建和处理经验，致力于利用区块链技术提升现实生活与商业效率。“面向移动端”的战略将会促进区块链技术的产品化并提高区块链技术的行业易用性，用区块链搭建现实商业社会数据交互的桥梁：

当前团队核心成员

请参考官网最新信息：www.lemochain.com

Lemo 顾问团队

请参考官网最新信息：www.lemochain.com

Lemo 的部分战略合作伙伴

教育领域，LemoChain 与中国主流智能教育管理平台校精灵合作，基于 LemoChain 开发，区块链模块上线后，将覆盖上千万的用户量

将于 2018 年 8 月推出基于 LemoChain 的链上教育互动 Dapp，为国内上百家教育机构和近百万家长提高更加公开，合理的教育资源流通服务。

LemoChain 与中国成都会众科技有限公司达成战略合作，9 月份使用 Lemo 的区块链技术为其 500 万用户提供服务

2018 年 7 月份柠檬名片将基于 LemoChain 发布侧链，用区块链技术现实社会商业交易信任问题，为传统行业的商业交易提供信任保障，目前柠檬片已上线微信小程序和 App Store，8 月份将上线 App store，为全球用户提供区块链交易服务。

LemoChain 携手中国熊猫驾信开启智能合约服务的新篇章，熊猫驾信已经拥有 800 万的用户量

基于现有的产品线，加入 Lemo 区块链技术的模块，使用同态加密及其 IPFS 数据存储等技术来保障驾信的信息安全，来促进整个行业的发展。

社交领域，LemoChain 与美国社交公司 Inspiration 达成战略合作，DApp 上线区块链功能后，为其 600 万用户提供服务

2018 年 6 月份 Kuku 将基于 LemoChain 改造完善产品，用区块链技术解决酒托、饭托、婚托等现实问题。

由于保密条款的约束，关于更多顾问，战略合作伙伴及投资者信息将在提出信息请求后，签署保密协议的前提下告知。联系邮箱： foundation@lemochain.com

Lemo 的执行和迭代

时间表

Lemo 预售计划

LemoChain 的用户及其开发者通过消耗持有的 Lemo 来获取 LemoChain 的功能，尤其是在 LemoChain 运行分布式应用需支付和消耗一定量的 Lemo 代币。同时在 LemoChain 网络中进行的所有数字资产交易都将以 Lemo 代币进行结算。

LemoChain 矿前代币将会在 LemoChain 发布时产生，由 LEMOCHAIN 基金会持有。早期持有者持有的 ERC-20 Lemo 代币可以在此时进行 1 比 1 的兑换。

Lemo 公开预售的具体规则和信息将会通过 LemoChain 官网和 Lemo 钱包应用及公众号进行公布，请及时关注。

参与 Lemo Foundation 发起的 Lemo 代币预售不是零风险的。详细风险内容，请参阅 Lemo 的免责与风险说明。

Lemo 迭代规划

作为新兴技术的早期应用尝试，区块链技术会面临各种挑战和机遇。LemoChain 的未来迭代方向：

- 一是底层架构代码迭代；
- 二是建立在 LemoChain 主链上的商业应用迭代。

LemoChain 底层架构的迭代

当 LemoChain 架构代码本身出现漏洞，通常采用系统升级的方式进行迭代。出现漏洞需要经过代码审核委员会分析，测试和审核，提交至决策委员会报备，以下是重大漏洞的定义：

- 影响用户资产安全
- 重大安全事件
- 系统安全性问题
- 系统运行逻辑与设计不符

当 Lemo 生态无法满足参与者的商业和用户需求的时候，通常采用由意见领袖代表社区利益提出方案，决策委员会决策通过后组织开发者进行开发，开发完成提交代码委员会分析，测试和审核，再报备决策委员会的方式进行迭代。

商业应用迭代

Lemo 是全球开源项目，通过技术上的创新、理念上的创新将区块链与现实世界连接起来。关于商业应用的迭代，基金会会选择合适的第三方合作，进行行业及应用的迭代，由第三方开发者主导，Lemo 提供技术支持。

Lemo 的免责与风险声明

免责声明

除本白皮书所明确载明的之外，Lemo Foundation LTD 及其各地的合作机构和个人不会对 LemoChain 或 Lemo 代币作任何陈述或保证（尤其是对其适销性和特定功能）。任何人参与 Lemo 代币的预售计划及购买 Lemo 代币的行为均基于自己本身对 LemoChain 以及 Lemo 代币的了解。在无损于前述内容的普适性前提下，所有参与者将在 LemoChain 项目启动之后按现状接受 Lemo 代币，无论其技术规格、参数、性能或者功能等。

LemoChain 在此明确不予承认和拒绝承担下述责任：

- 任何人在购买 Lemo 代币时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；
- 任何人在参与 Lemo 代币预售时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法付款或无法提取 Lemo 代币；
- 由于任何原因 Lemo 代币的预售计划被放弃；
- LemoChain 的开发失败、推迟或延期，以及因此导致的无法交付 Lemo 代币或延迟交付；
- 相关区块链源代码的漏洞、错误、瑕疵、崩溃、回滚或硬分叉等技术问题引起的平台故障；
- 对预售所募集资金的使用；
- 任何参与者泄露、丢失或损毁了数字加密货币或代币的钱包私钥；
- Lemo 代币预售的第三方平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、 解散或歇业；
- 任何人对 Lemo 代币的交易或投机行为；
- Lemo 代币在任何交易所的上市交易或退市；
- Lemo 代币被任何政府、主管当局或公共机构归类或视为是一种货币、证券、商业票据、

流通票据、投资品或其他事物，以至于收到禁止、监管或法律限制；

- 本白皮书披露的任何风险因素，以及与该等风险因素有关、因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。

风险声明

LemoChain 开发和运营团队相信，在 LemoChain 的开发、维护和运营过程中存在着无数风险，这其中很多都超出了 LemoChain 当前开发和运营团队的控制。除本白皮书所述的其他内容外，每个 Lemo 代币预售参与者还均应细读、理解并仔细考虑下述风险，之后才决定是否参与本次预售计划。

每个 Lemo 代币的购买者应特别注意这一事实：尽管 LemoChain 开发和运营的管理主体是在新加坡设立的，但 LemoChain 和 Lemo 代币均只存在于网络虚空间内，不具有任何有形存在，因此不属于或涉及任何特定国家。

参加本次预售应当是一个深思熟虑后决策的行动，将视为参与者已充分知晓并同意接受了下述风险：

1）预售计划的终止

本次 Lemo 代币预售计划可能会被提前终止，此时参与者可能由于比特币 / 以太币的价格波动以及 LemoChain 开发和运营团队的支出而仅被部分退还其支付的金额。

2）不充分的信息提供

截止到本白皮书发布日，LemoChain 仍在开发阶段，其哲学理念、共识机制、算法、代码和其他技术细节和参数可能经常且频繁地更新和变化。尽管本白皮书包含了 LemoChain 最新的关键信息，其并不绝对完整，且仍会被 LemoChain 开发和运营团队为了特定目的而不时进行调整和更新。LemoChain 开发和运营团队无能力、且无义务随时告知参与者 LemoChain 开发中的每个细节（包括其进度和预期里程碑，无论是否推迟），因此并不必然会让预售参与者及时且充分地接触到 LemoChain 开发中不时产生的信息。信息披露的不充分是不可避免且合乎情理的。

3）监管措施

加密代币正在被或可能被各个不同国家的主管机关所监管。LemoChain 开发和运营

团队可能会不时收到来自于 1 个或多个主管机关的询问、通知、警告、命令或裁定，甚至可能被勒令暂停或终止任何关于本次预售计划、LemoChain 开发或 Lemo 代币的行动。LemoChain 的开发、营销、宣传或其它方面以及本次预售计划均因此可能受到严重影响、阻碍或被终结。由于监管政策随时可能变化， 任何国家之中现有的对于 LemoChain 或本次预售计划的监管许可或容忍可能只是暂时的。在各个不同国家，Lemo 代币可能随时被定义为虚拟商品、数字资产甚至是证券或货币，因此在某些国家之中按当地监管要求，Lemo 代币可能被禁止交易或持有。

4）密码学

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步（例如密码破解）或者技术进步（例如量子计算机的发明）可能给基于密码学的系统（包括 LemoChain）带来危险。这可能导致任何被持有的 Lemo 代币被盗、失窃、消失、毁灭或贬值。在合理范围内，LemoChain 开发和运营团队将自我准备采取预防或补救措施， 升级 LemoChain 的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。密码学和安全创新的未来是无法预见的，LemoChain 开发和运营团队将尽力迎合密码学和安全领域的不断变化。

5）开发失败或放弃

LemoChain 仍在开发阶段，而非已准备就绪随时发布的成品。由于 LemoChain 系统的技术复杂性，LemoChain 开发和运营团队可能不时会面临无法预测和 / 或无法克服的困难。因此，LemoChain 的开发可能会由于任何原因而在任何时候失败或放弃（例如由于缺乏资金）、开发失败或放弃将导致 Lemo 代币无法交付给本次预售计划的任何参与者。

6）众筹资金的失窃

可能会有人企图盗窃 LemoChain 平台所收到的公开预售所获加密货币。该等盗窃或盗窃企图可能会影响 LemoChain 开发和运营团队为 LemoChain 开发提供资金的能力。尽管 LemoChain 开发和运营团队将会采取最尖端的技术方案保护预售资金的安全，某些网络盗窃仍很难被彻底阻止。

7）源代码瑕疵

无人能保证 LemoChain 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能使得用户无法使用特定功能，暴露用户的信息或产生其他问题。如果确有此类瑕疵，

将损害 LemoChain 的可用性、稳定性或安全性，并因此对 Lemo 代币的价值造成负面影响。

8） 安全弱点

LemoChain 区块链是开源代码。尽管 LemoChain 开发和运营团队努力维护 LemoChain 系统安全，任何人均有可能故意或无意地将弱点或缺陷带入 LemoChain 的核心基础设施要素之中，对这些弱点或缺陷，LemoChain 开发和运营团队无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的 Lemo 代币或其他数字代币丢失。

9）“分布式拒绝服务”攻击

发布创始代币的以太坊设计为公开且无准入许可的账本。因此，以太坊可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使 Lemo 代币系统遭受负面影响、停滞或瘫痪，并因此导致在此之上的交易被延迟写入或记入以太坊区块链的区块之中，或甚至暂时无法执行。

10）处理能力不足

LemoChain 的快速发展将伴随着交易量的陡增及对处理能力的需求。 若处理能力的需求超过区块链网络内届时节点所能提供的负 载，则 LemoChain 网络可能会瘫痪或停滞，且可能会产生诸如“双重花费”的欺诈或错误交易。在最坏情况下，任何人持有的 Lemo 代币可能会丢失，以太坊区块链回滚或甚至硬分叉可能会被触发。这些事 件的余波将损害 LemoChain 的可使用性、稳定性和安全性以及 Lemo 代币的价值 。

11）未经授权认领待售 Lemo 代币

任何通过解密或破解 Lemo 代币持有者密码而获得持有者注册邮箱或账号访问权限的人士，将能够恶意获取 Lemo 代币持有者获得的预售 Lemo 代币。据此，持有者所获得的 Lemo 代币可能会被错误发送至通过持有者注册邮箱或注册账号认领 Lemo 代币的任何人士，而这种发送是不可撤销、不可逆转的。每位 Lemo 代币预售参与者应当采取诸如以下的措施妥善维护其注册邮箱或注册账号的安全性：

(i) 使用高安全性密码；
(ii) 不打开或回复任何欺诈邮件；
(iii) 严格保密其机密或个人信息。

12）Lemo 代币钱包私钥

获取 Lemo 代币所必需的私钥丢失或毁损是不可逆转的。只有通过本地或在线 Lemo 代币钱包拥有唯一的公钥和私钥才可以操控 Lemo 代币。每位预售参与者应当妥善保管其 Lemo 代币钱包私钥。若 Lemo 代币持有者的该等私钥丢失、遗失、泄露、毁损或被盗，LemoChain 开发和运营团队或任何其他人士均无法帮助该持有者获取或取回相关 Lemo 代币。

13）普及度

Lemo 代币的价值很大程度上取决于 LemoChain 平台的普及度。LemoChain 并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏情况下，LemoChain 甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大部分 Lemo 代币需求可能具有投机性质。缺乏用户可能导致 Lemo 代币市场价格波动增大从而影响 LemoChain 的長期发展。出现这种价格波动时，LemoChain 开发和运营团队不会（也没有责任）稳定或影响 Lemo 代币的市场价格。

14）价格波动

若在公开市场上交易，加密代币通常价格波动剧烈。短期内价格震荡经常发生。该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 Lemo 代币交易的二级市场，LemoChain 开发和运营团队对任何二级市场的 Lemo 代币交易不承担责任。 因此，LemoChain 开发和运营团队没有义务稳定 Lemo 代币的价格波动。Lemo 代币交易价格所涉风险需由 Lemo 代币持有者自行承担。

* 由于保密条款的约束，关于早期投资人的信息将在提出信息请求后，签署保密协议的前提下告知。联系邮箱： foundation@lemochain.com

* 此白皮书仅代表截止 2018 年 4 月 14 日 LemoChain 项目的进展和状态，版本号 2.2 持续更新中

- https://cryptovest.com/news/cryptokitties-burn-up-15-of-ethereums-gas/
- https://bitshares.org/technology/industrial-performance-and-scalability/
- https://blockchain.info/charts/n-transactions
- https://etherscan.io/chart/bloktime
- https://news.bitcoin.com/ethereum-blockchain-congested-cats/
- GENTRY C. Fully Homomorphic Encryption Using Ideal Lattices[C]//STOC '09. [s.l.]: ACM, 2009: 178