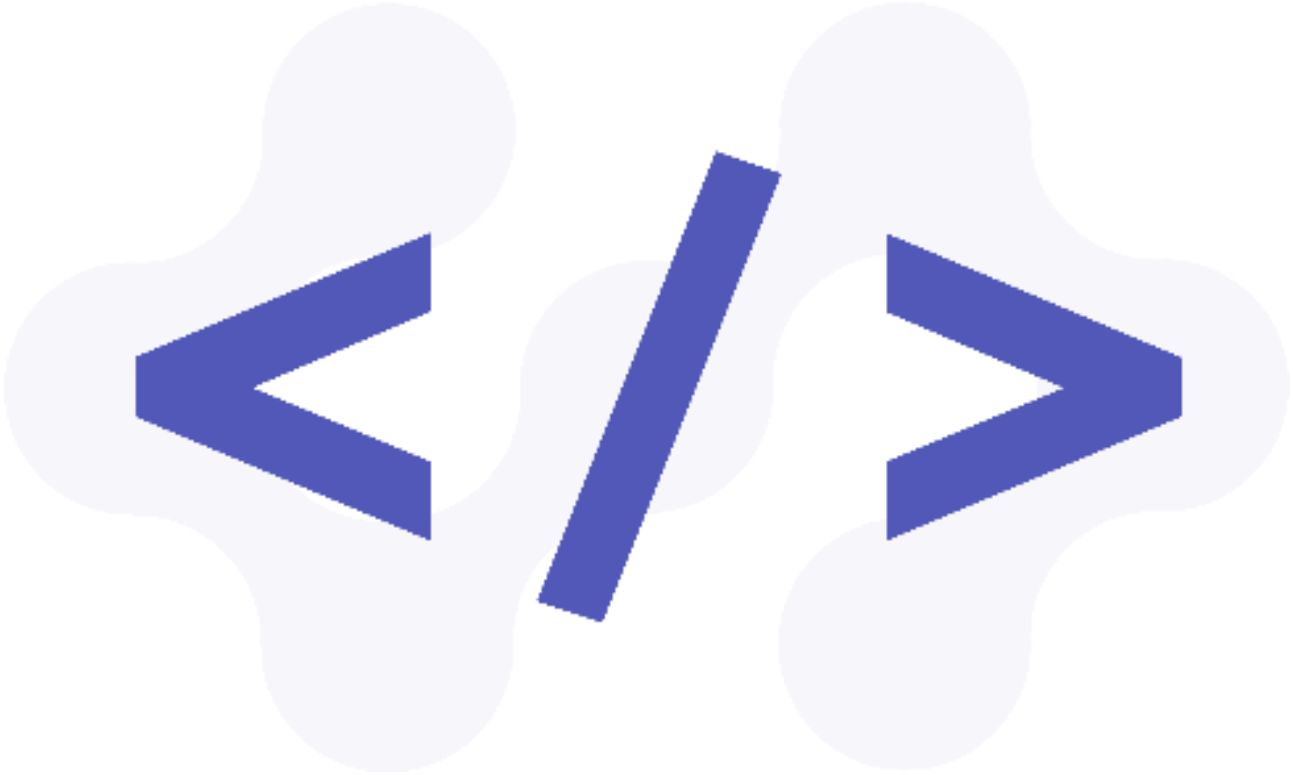


LemoChain

技术白皮书 v1.1

2018/05/10

目录

诞生背景

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 1800 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；**
- **吞吐量成为大型应用上链瓶颈，容易产生交易拥塞，无法承受爆款应用。**

我们致力于构建一个全新的区块链数据传输生态系统—LemoChain，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。

设计理念

1. 响应快速

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。我们可以看到当前主流网络之一的比特币网络平均每日确认 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。而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。

LemoChain 选择以响应速度高为特性的 DPoVP 技术来解决该问题。其参考了 DPoS 共识机制原理，能够提供接近 10000TPS 的交易吞吐量和小于 1 秒的确认速度，已经达到了 Visa 规模的交易处理能力，为 LemoChain 今后的发展状态提供了足够的成长空间。

2. 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，辅助开发者快速达成这一目标。

3. 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。

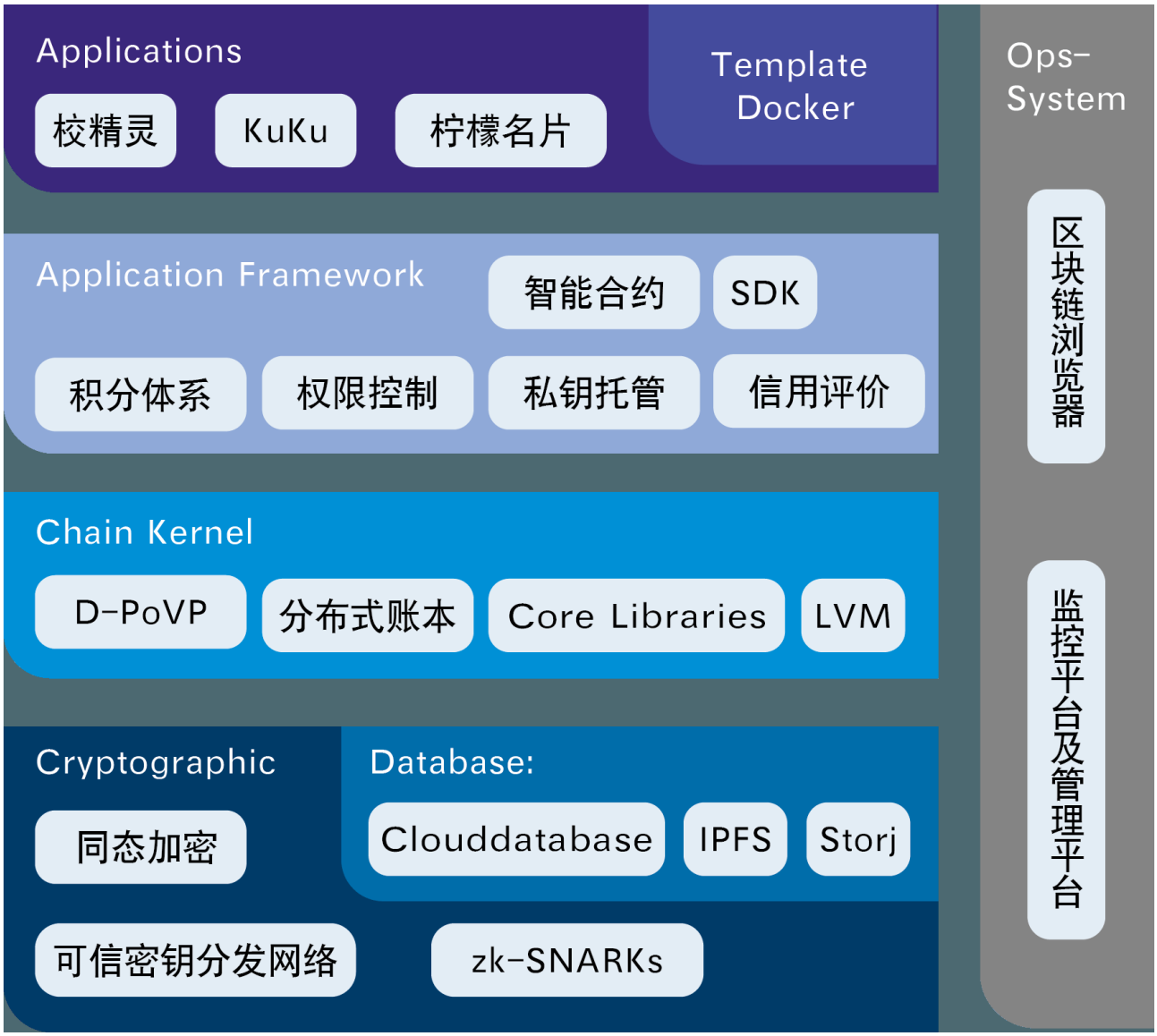
4. 安全与隐私

LemoChain 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 LemoChain 与专门的代码审计团队达成合作，以确保整套机制能够抵御恶意攻击。

5. 开放

LemoChain 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。

6. 分层架构



LemoChain 将区块链细节屏蔽在系统底层，通过稳定的接口和 SDK 向上层应用提供服务。各模块松散耦合，支持替换和升级，上层应用无需进行任何改动。

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。

1. 常见共识机制

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。

1.1 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。

1.2 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。

1.3 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。

1.4 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。

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

LemoChain 综合 BFT 和 DPoS 共识机制，并将用户贡献价值纳入激励机制考虑范围，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， 通过多种维度的积分体系将用户的行为量化，作为用户对平台贡献度、忠诚度的衡量依据。一方面提供了鉴别高质量用户的标准，另一方面也可以作为平台激励用户的一种运营手段。平台通过对用户贡献的奖赏，促进了 LemoChain 上各应用生态的繁荣发展，进一步吸引更多流量来到平台。这种良性循环机制成为 LemoChain 上应用迅速发展的一大助力。

DPoVP 共识机制的基础综合了 BFT 快速共识不会分叉的优点和 DPoS 的吞吐能力，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 记账权的归属

记账权主要解决是否该自己出块，什么时候出块的问题。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，时间归零后直接出新的块。

首先我们定义 I 表示出块者序号。有：

I_{me} 表示当前节点的出块序号；
I_{new} 自己生产的，或收到的并通过验证的区块的出块者序号。高度为当前链的高度 +1；
I_{last} 确认新块之前，上一个已确认过的区块的出块者序号；

其中 d 表示两个出块序号的距离：

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

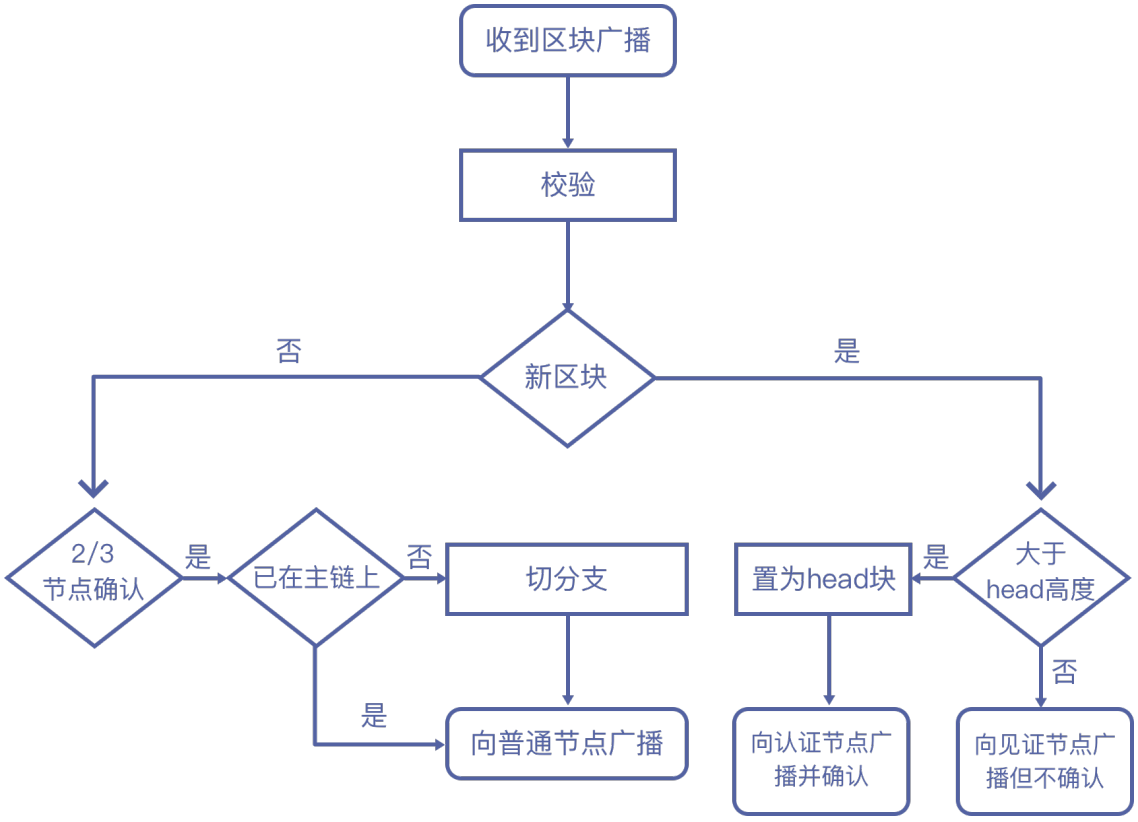
其中 C 是共识节点数量。
触发重新计算倒计时之前需要验证新块的合法性。倒计时计算公式如下：

$$\mathrm{T} = \begin{cases} (C-1)t_o & ,d(I_{me}, I_{new}) = 0 \\ 0 & ,d(I_{me}, I_{new}) = 1 \cap t_{now} - t_{new} \geq t_w \\ t_w - (t_{now} - t_{new}) & ,d(I_{me}, I_{new}) = 1 \cap t_{now} - t_{new} < t_w \\ \left(d(I_{me}, I_{new}) - 1 \right) t_o - (t_{now} - t_{new}) & ,d(I_{me},\ I_{new}) > 1 \end{cases}$$

t_{now} 当前时间；
t_{new} 收到的区块头中的时间戳；
t_W 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；
t_O 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。

2.3 共识

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，这个区块会进入“最终确认状态”。此时见证节点向全网广播该块。对于普通节点来说，接收到的区块一定是完成了共识的，永远不会分叉。只要收到的区块能够通过校验，就可以放心地保存下来。



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，交易和最终共识区块在普通节点和见证人节点之间传播的耗时。见证人节点相互确认和同步的过程加速了区块的广播扩散，能够进一步提升恶劣网络环境下达成共识的速度。

3. 风险应对能力

在 LemoChain 需要三分之二的见证人确认才可共识一个区块，因此能够容忍的作恶节点数不能超过总人数的三分之一。实际上某些情况下只要有一个诚实节点存在，就可以保证 LemoChain 的正常运行。以下分析几种典型的风险场景。

3.1 无利害关系 (Nothing At Stake) 攻击

在 DPoVP 网络中出块无需工作量证明，所以运算量很低。见证人可以在所有分叉上确认和出块，无论哪条分叉获胜，都能获得收益。出块程序根本不对导致分叉的区块做验证，或旨在发动双花攻击。这种方式不需要额外的算力等成本，相当于对区块链的分叉无动于衷。

在 DPoS 中需要达成 2/3 节点共识才会向普通节点广播，因此只要在所有分叉上出块的见证节点不超过 1/3，就不会在异常区块上达成共识。如果这些见证节点只是随意选择一个分支进行确认和出块，则会降低共识效率，导致没有任何分支能够达成共识。实际上这种情况下只要有一个诚实的见证人节点，就可以在该节点出块后得到更长的区块链，因而迅速收敛并达成共识。

3.2 同时出块风险

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分叉处区块 hash 的字典序更靠前的链。

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。

3.3 共识网络分裂

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。

3.4 提前共识攻击

恶意见证节点可以将未达成共识的区块广播给普通节点。这将会导致普通节点在短期内分叉。在恶意见证节点不超过 1/3 的情况下普通节点需要等待 1/3 节点出块后即可根据最长链原则甄别出正确的链。在 21 个见证节点，超时时间为 10 秒的情况下，分叉时间只能持续 3.5 到 70 秒。随后恶意见证节点将暴露自身并被投票出局。

4. 数据储存

LemoChain 旨在打造一个去中心化的数据交易平台，用户数据的安全存储、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，中心化的云存储服务等方案。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 基于 DHT 技术搭建 p2p 网络，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。得益于去中心化网络的优势，用户上传及取回数据均可通过最近的节点来完成，大大提升了传输速率。

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。LemoChain 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。LemoChain 将会为每个用户提供一定的免费空间，适合对数据安全没有绝对要求的场景。

5. 安全交易

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。

6. 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。

6.1 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。

6.2 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。

6.3 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。

6.4 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。

1. 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。

2. 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。

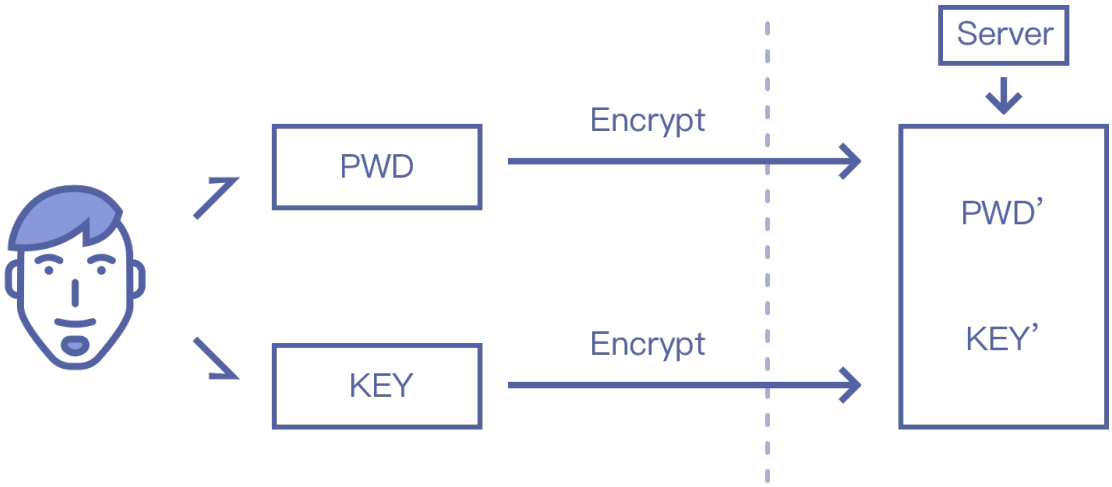


图 1 托管私钥

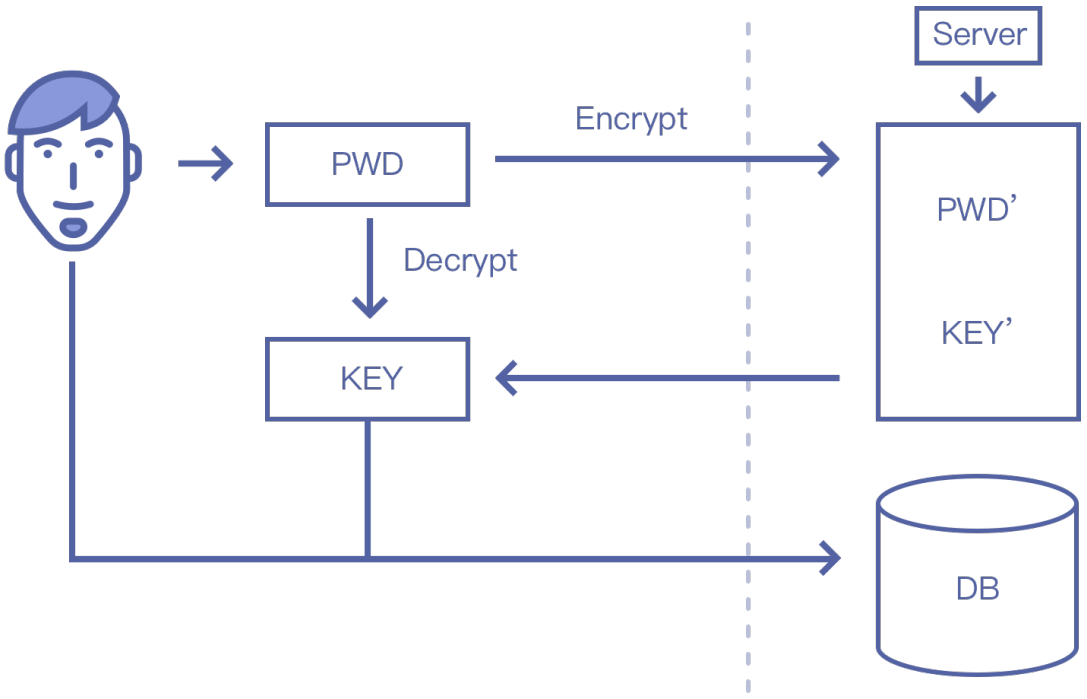


图 2 找回私钥

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。

3. 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。

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。

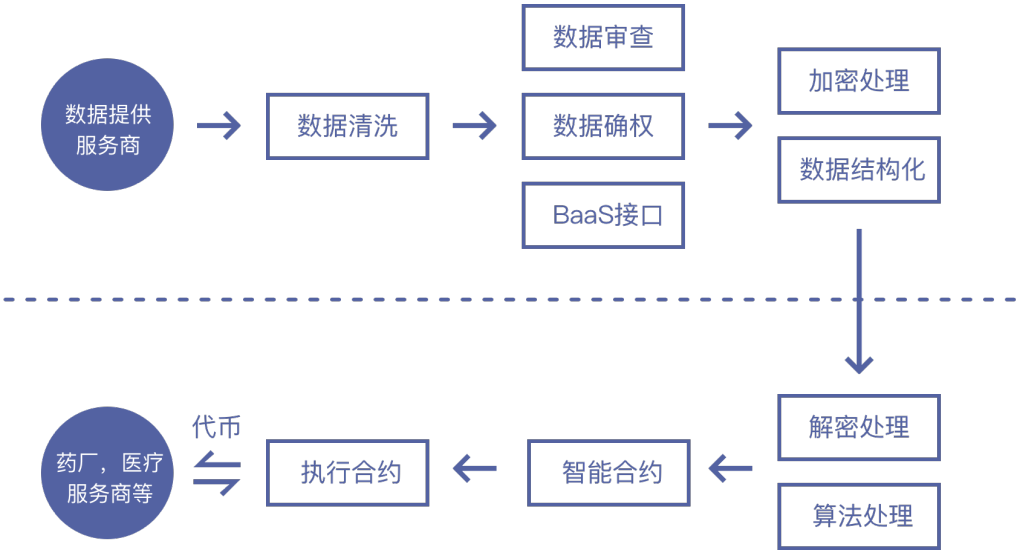
LemoChain 的生态架构如下：

- 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。

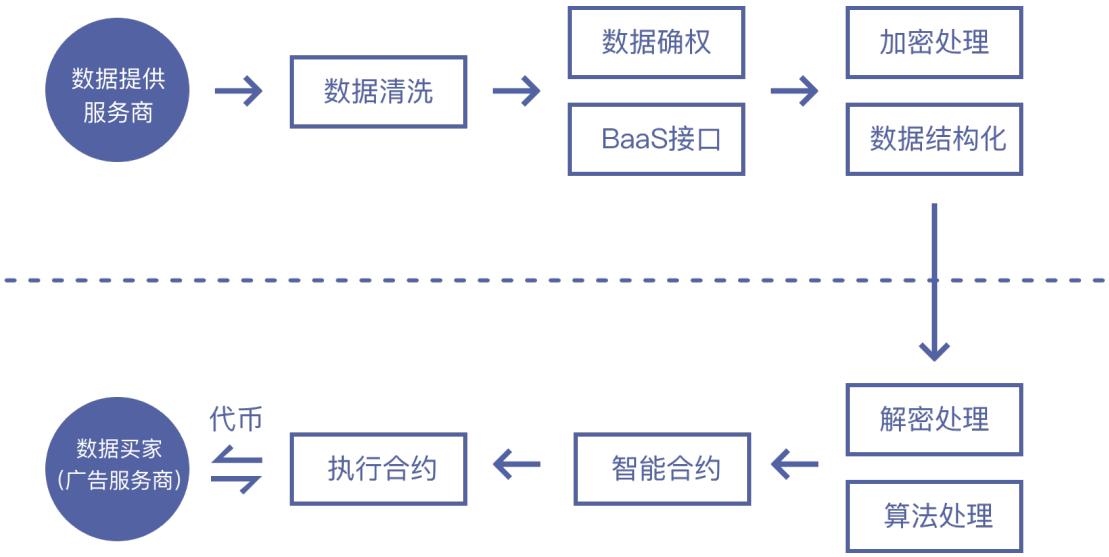
1. 应用场景一：健康医疗数据 DAPP

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。



2. 应用场景二：婚恋交友

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、广告精准投放等应用场景。



技术路线

为了持续推动 LemoChain 的应用和生态的建立，基金会做出了如下技术时间规划：

2017.06
LemoChain正式启动

2017.09
LemoChain Demo开发完成

2017.12
LemoChain
（LEMO代币）公开预售启动

2018.02
基金会成立，代币预售结束

2018.04
公开LemoChain测试网络源码

2018.08
上线基于测试网络的数据交易平台

2018.11
LemoChain公开测试
完成3个月的安全审查

2018.12
LemoChain上线发布会
上线主干网络

参考文献

1. https://cryptovest.com/news/cryptokitties-burn-up-15-of-ethereums-gas/
2. https://bitshares.org/technology/industrial-performance-and-scalability/
3. https://blockchain.info/charts/n-transactions
4. https://etherscan.io/chart/bloktime
5. https://news.bitcoin.com/ethereum-blockchain-congested-cats/
6. GENTRY C. Fully Homomorphic Encryption Using Ideal Lattices[C]//STOC '09. [s.l.]: ACM，2009：178
7. http://fortune.com/2017/11/25/lost-bitcoins/