Luther

lth.one

一个模块化的区块链基础设施

白皮书V1.0

目录

一、 区块链浪潮

有人说，区块链将引领第四次工业革命，第四次工业革命的重要组成包括人工智能、区块链、3D打印、智能制造等相关技术，其中区块链是连接各个技术的重要桥梁。区块链已经引发了世界性的关注，迅速地成为一场全球参与的竞逐场。

在区块链硬件领域，中国以及美国的相关公司具有绝对优势，全球大部分区块链硬件均由中国和美国的厂商生产。在算力的军备竞赛下，谁的区块链硬件算力更强，就能抢占更多的市场份额。芯片的设计和研发能力，是这场军备竞赛的决定性因素，因此，非常有力地促进了各国专用芯片设计产业的创新发展。

全球已经有超过数千家以区块链业务为主营业务的区块链公司，而且还在爆发式增长。

区块链技术不仅受到了创业企业的青睐，也受到了互联网巨头企业的广泛关注，互联网巨头企业纷纷拓展区块链业务，快速推动全球区块链产业发展。目前，微软、IBM、腾讯、阿里巴巴、百度、京东、微软等互联网行业巨头纷纷加入区块链技术的研究与场景应用中来。腾讯基于 Trust SQL 核心技术，打造领先的企业级区块链基础服务平台。目前，腾讯区块链已经落地供应链金融、医疗、数字资产、物流信息、法务存证、公益寻人等多个场景。例如，腾讯基于供应链场景下的真实交易数据， 通过区块链技术及运营资源，构建“区块链+供应链金融解决方案”，从根本上改善小微企业的融资困境，助力地方产业转型升级。阿里巴巴基于区块链技术去中心化、分布式存储及防篡改的特性已落地了多个应用场景，包括公益、正品追溯、租赁房源溯源、互助保险等，并且申请专利数量已达到 80 件左右。百度金融先后与华能信托、长安新生等落地了国内首单区块链技术支持证券化项目和区块链技术支持交易所 ABS 项目。京东运用区块链技术搭建“京东区块链防伪追溯平台”，从解决商品的信任痛点出发，精准追溯到商品的存在性证明特质，让所有生产、物流、销售和售后信息分享进来，共同铸建完整且流畅的信息流，并且也采用区块链技术来解决 ABS 参与各方的信

任问题，在区块链的系统架构上完成交易，确认资产的权属和资产的真实性。巨头涌入给全球区块链产业发展注入了新动能，产业蓄势待发， 并将借着新时代的东风快速崛起。

区块链技术虽然还处在发展的初级阶段，缺已经吸引大量的人才涌入区块链创业的浪潮中，很多著名的传统公司也早已开始布局区块链，区块链即是现在的热点所在。

第46届世界经济论坛达沃斯年会将区块链与人工智能、自动驾驶等一并列入“第四次工业革命”，显示出区块链技术的重大意义和极为广阔的发展空间。IBM公司CEO罗睿兰女士有一句著名的论断：“区块链对于可信交易的意义正如互联网对于通讯的意义”（What the internet did for communications, I think blockchain will do for trusted transactions）。

二、Luther 是什么

Luther 是一个模块化的高效率区块链基础设施，不仅是大家熟悉的公有链基础设施，它也是一个联盟链基础设施；所以Luther既可以服务于广大创业者建立公有链，又可以服务于企业、集团、银行甚至政府机构建立联盟链。

（1）公有链

公有链就是大家熟悉的BTC，ETHEREUM之类；公有链是对所有人开放，任何人都可以参与加入节点，同时所有数据默认公开;

目前在公有链领域，中国技术处于世界先进水平，已经诞生了很多国际性的公链，例如大家熟知的NEO，QTUM等。

（2）联盟链

联盟链是指若干个机构共同参与记账的区块链，即联盟成员之间通过对多中心的互信来达成共识。联盟链的数据只允许系统内的成员节点进行读写和发送交易，并且共同记录交易数据。

联盟链作为支持分布式商业的基础组件，更能满足分布式商业中的多方对等合作与合规有序发展要求。例如：联盟链会更适合组织机构间的交易和结算，类似于银行间的转账、支付，通过采用联盟链的形式，就能打造一个很好的内部生态系统来大幅提高效率。

联盟链和公链相比，在高可用、高性能、可编程，隐私保护上更有优势，它被认为是“部分去中心”或者是“多中心”的区块链。联盟链让节点数得到了精简，能够使得系统的运行效率更高、成本更低，在单位时间内能够确认的交易数量要比公链大很多，更容易在现实场景中落地。此外，联盟链相对于公有链非常重要的特点就是节点准入控制与国家安全标准支持，确保认证准入、制定监管规则符合监管要求， 在可信安全的基础上提高交易速度。

三、为什么会有 Luther

当前的区块链技术存在“不可能三角”，即无法同时达到“高效低能”、“去中心化”、以及“安全”这三个要求，具体来看：

（一）追求“去中心化”和“安全”则无法达到“高效低能” 比特币区块链技术便是一种极致追求“去中心化”和“安全”的技术组合。

从数据结构上看，它采用拥有时间戳的“区块+链”的结构，在可追溯、防篡改上具备安全优势，也易于分布式系统中的数据同步，但是若需要对信息进行查询、验证，则涉及到对链的遍历操作，而遍历是较为低效率的查询方式。在数据存储上，它的每一个节点都下载和存储所有数据包，利用强冗余性获得强容错、强纠错能力，使得网络可以民主自治，但同时也带来了巨大的校验成本和存储空间损耗。它并不像分布式数据库那样随着节点的增加可以通过分布式存储提高整体存储能力，而只是简单地增加副本。未来随着区块链技术所承载的内容增多，单个节点的存储空间将是个问题。

在并发处理上，比特币区块链技术最终只允许一个 “矿工”获得记账权建立一个交易区块，这种机制可以有效保证一个民主网络运行的安全和稳健，但其实质上是拥有所有数据的整个“链条”在进行串行的“写”操作。 相比关系数据库将数据分为若干表，仅仅根据操作涉及 的数据锁定若干表或表中的记录、其他表仍能并发处理 相比，比特币区块链技术的串行操作效率远低于普通数据库。

在对内容的验证上，比特币区块链让每个节点都拥有所有的内容，同时对区块内的所有内容进行哈希，这增强了民主性和安全性。但是这种整体哈希的设计思路则意味着不能以地址引用的方式存储数据，否则由于所引用地址上所存储的信息由于并未进行哈希校验而可能存在篡改。因此，比特币区块链技术缺乏高效的可 扩展性，在对大型内容的处理上存在效率问题。

（二）追求“高效低能”和“安全”则无法完全 实现“去中心化”

从“共识机制”角度看，为了在确保“安全”的前提下解决比特币区块链技术所采用的工作量证明方式的低效性，权益证明（Proof of Stake）、股份授权证明（Delegated Proof of Stake）等机制被采用。但是无论是基于网络权益代表的权益证明，还是利用101 位受委托人通过投票实现的股份授权证明，实际上都是对“去中心化”的退让，形成了部分中心化。典型例子是EOS的21个超级节点，就是为了“高效低能”部分牺牲“去中心化”。

同样在区块链技术的演化上，除了以比特币为代表的公有链技术外，又衍生了联盟链技术和私有链技术。

联盟链技术只允许预设的节点进行记账，加入的节点都需要申请和身份验证，这种区块链技术实质上是在确保安全和效率的基础上进行的“部分去中心化”或“多中心化”的妥协。而私有链技术的区块建立则掌握在一个实体手中，且区块的读取权限可以选择性开放，它为了安全和效率已经完全演化成为一种“中心化”的技术。

（三）追求“高效低能”和“去中心化”则必须 牺牲“安全”

一个极端的案例便是基于 P2P（Peer-to-Peer）的视 频播放软件。以往当在线观看人数增多时，基于中央服务器设计的视频服务器会因承载压力变大而速度缓慢。为了提高效率，P2P 视频播放软件的设计使得一个节点在下载观看视频文件的同时也不断将数据传输给 别人，每个节点不仅是下载者同时也是服务器，资源的分享形成不再依赖于中央服务器的“去中心化”模式。

同时，由于视频一秒有24 帧，少量图片的局部数据损坏并不影响太多的视觉感官，但是用于数据校验而出现的图像延迟则是不可接受的。于是 P2P 视频

播放软件牺牲了“安全”性，允许传输的数据出现少量错误。在这种去中心化的网络中，参与的节点越多，数据的传播越快，传播的效率越高。当然这对于严谨的金融业来说，数据的错误是不可接受的，安全也是金融业所首要考虑的问题。

总之，从当前的技术条件来看尚无法实现“高效低能”、“去中心化”和“安全”三者皆得的区块链技术。但是若对其一个或若干个要求进行妥协，所产生的新技术集合由于更符合实际需求，有可能它对实际应用的吸引力反而增强。

现有的区块链基础设施中，没有一个是可以解决“不可能三角”问题的；ETHEREUM具有“去中心化”和“安全”属性，但是却无法满足“高效低能”；EOS则是牺牲了“去中心化”来换取效率提升的空间。

这些基础设施都有一个共同的局限性：他们的子链会继承他们的三角属性，造成用户分流，例如用户A的业务要求强“去中心化”，他们会选择ETHEREUM，用户B的业务要求“高效低能”，他们会选择EOS技术。

为了解决这些问题，Luther将打造模块化的区块链基础设施，由子链建造者自由选择模块组装，每一个子链建造者在不可能三角中的侧重点不一样，他们可以根据自己的业务特点灵活选择。

四、Luther 技术设计

Luther基于现有的区块链技术进行深度重构和优化，综合bitcoin、ethereum、bts石墨烯等技术优势，开发出我们自己的高性能、高拓展性、高度模块化的基础链，以满足不同落地业务场景的差异化需求。

1. 总体架构

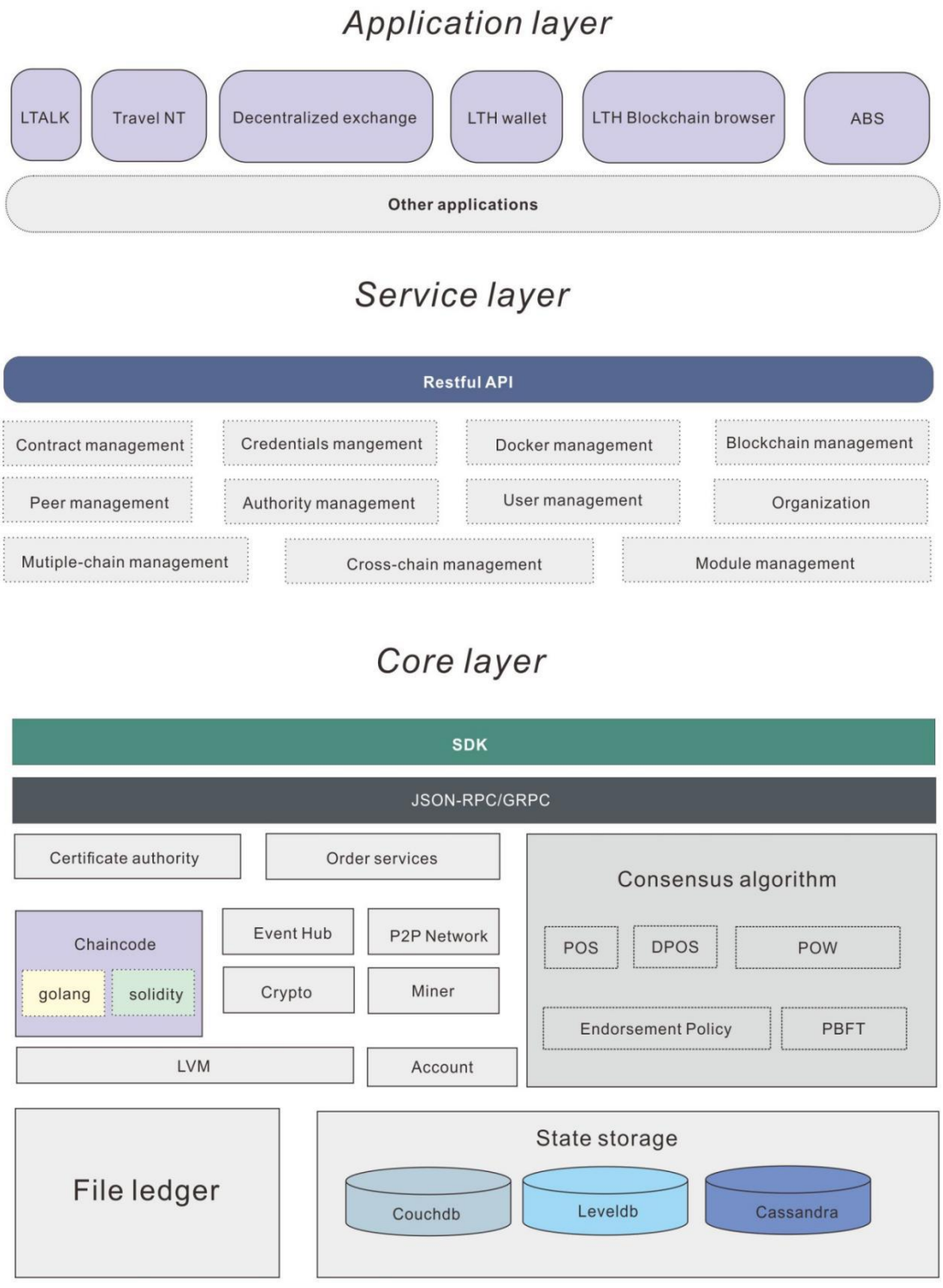

图1 LutherChain总体架构

2. 组件模块化

Luther将区块链所有的核心进行模块化，尤其是对共识算法模块化并以Luther标准的接口提供服务，使得Luther的子链开发者们能够根据自己的业务灵活选择积木方块组建自己的公有链、联盟链、私有链。

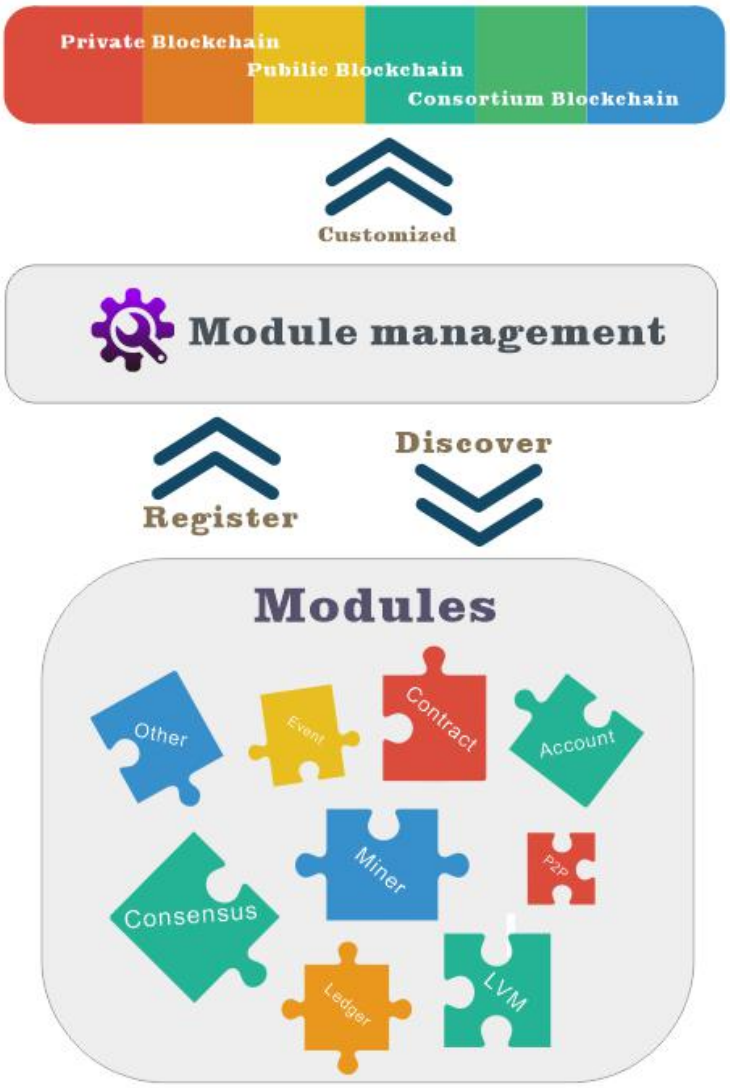

图2 LutherChain组建模块化

3. 更完善智能合约

据最新数据显示ethereum的DAPP数量已经达到561个，为了能够保证ethereum上的DAPP可以迁移到Luther上，LVM完美兼容solidity智能合约。除此之外Luther新增支持golang语言开发业务智能合约，部署到区块链上之后通过封装智能合约的标准GRPC接口对外提供服务以便进行业务处理。

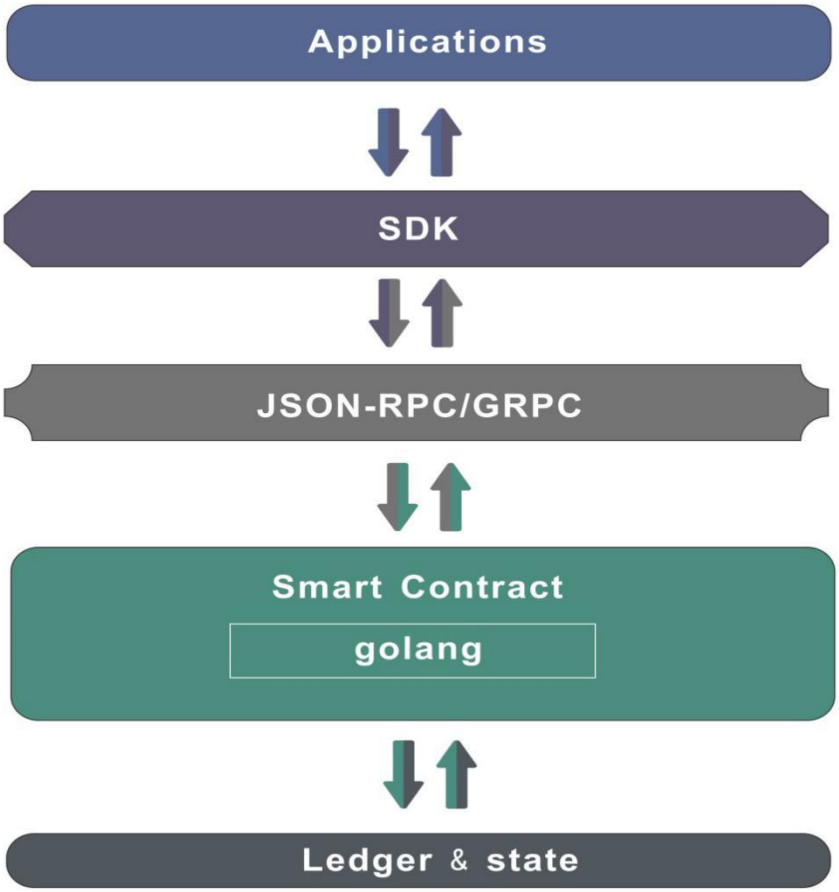

图3 LutherChain 智能合约

4. 可扩展存储

我们将把存储做成可拔插的组件，这样使得存储便于扩展；可以轻易扩展集群nosql数据库，以便支撑应用的庞大数据量；支持leveldb、couchdb和cassandra。

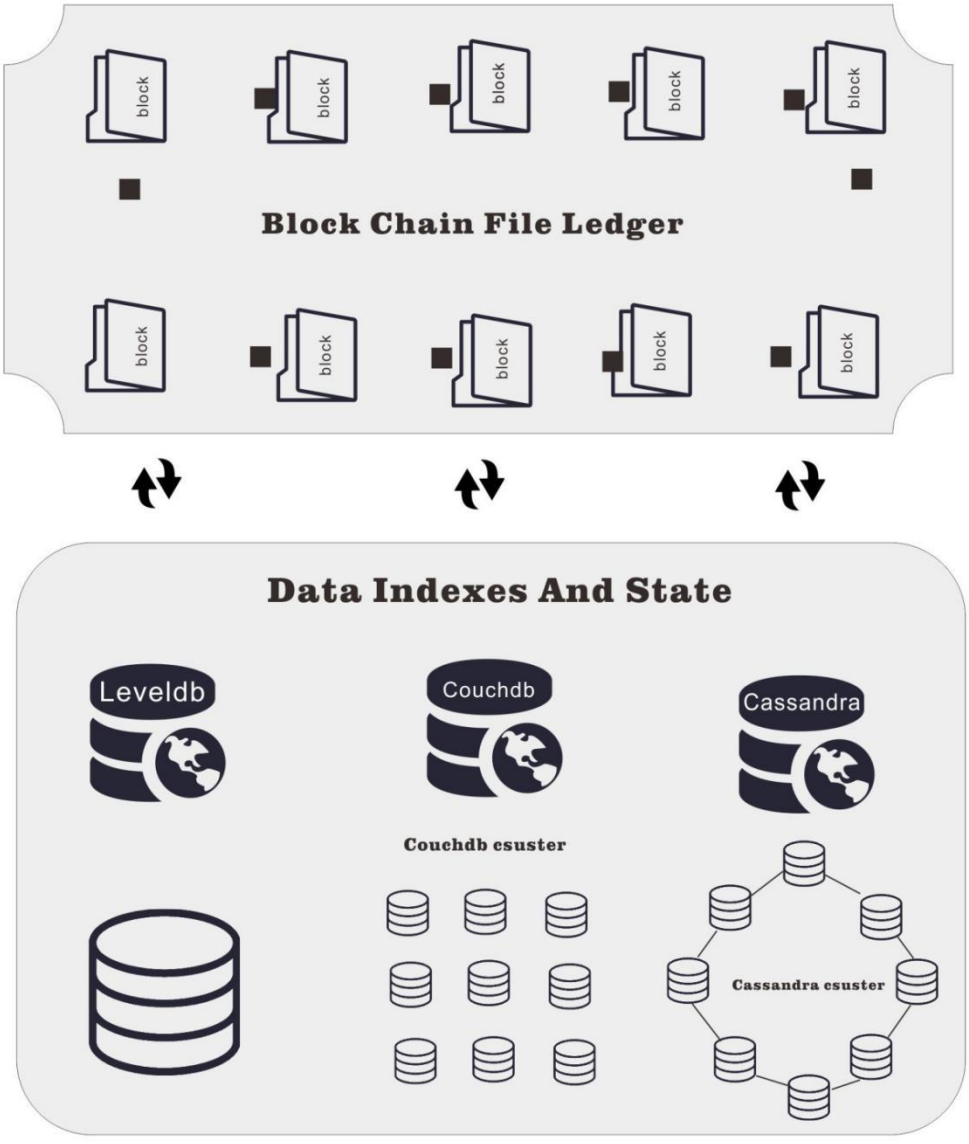

图4 LutherChain 可扩展存储

5. 多链并行

Multiple-chain是除了main-chain之外还可以有很多并行运行的sub-chain，peers可以加入到不同组织或联盟的sub-chain，peer和sub-chain是多对多关系；每一条sub-chain都有自己的数据访问权限，做到了多链数据隔离；这样可以满足企业的联盟链构建。

以一个金融业务场景说明多链并行的应用场景：

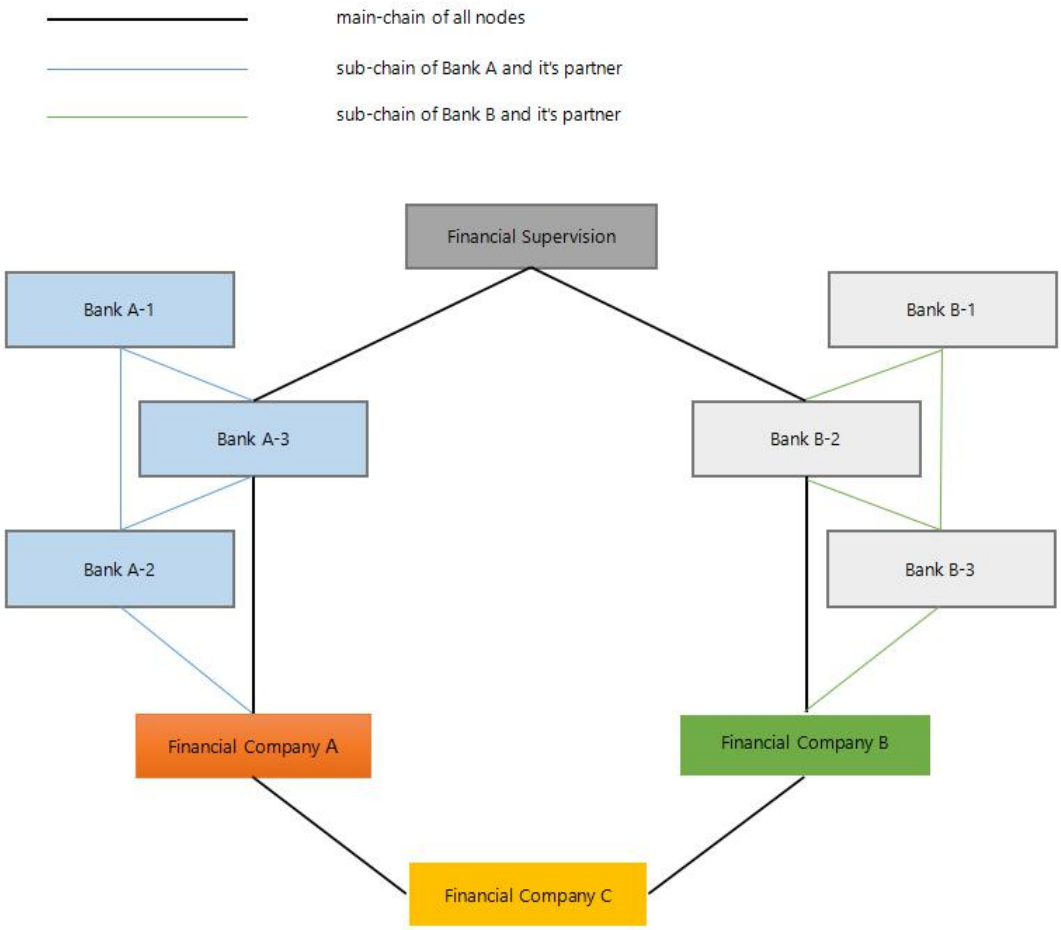

图5 LutherChain 多链并行

1. 在这场景中区块链的参与角色可以分为：银行、金融服务商、监管部门；他们全部参与到main-chain中；进行数据共享、交易共识。

2. 然而在参与者中各角色之间可能存在竞争关系，同时存在数据隐私的需求；所以在同一银行的各分行之间可以建立sub-chain；其他节点如果得到了sub-chain的允许也可以动态加入到这条sub-chain中进行数据共享。

3. 通过main-chain和sub-chain的设计，各参与角色既能够通过区块链进行账本共享、交易共识；又能够进行权限控制，核心数据隔离；使得各方数据得以权限保护，只共享每个角色想要共享的数据；在保证自己核心竞争力的同时进行数据互通，达到共赢。

4. 比如ethereum，任何人都可以参与进区块链中，作为全账本节点，节点拥有整个区块链的所有数据，并且可以任意查阅，因此无法存放敏感隐私数据和机密数据。

5. Luther的数据权限控制也是模块化的，使用者可以按照自己的业务需求选择。

6. 跨链协议

跨链，顾名思义，就是通过一个技术，能让价值跨过链和链之间的障碍，进行直接的流通。

区块链是分布式总账的一种。一条区块链就是一个独立的账本，两条不同的链，就是两个不同的独立的账本，两个账本没有关联。本质上价值没有办法在账本间转移，但是对于具体的某个用户，用户在一条区块链上存储的价值，能够变成另一条链上的价值，这就是价值的流通。

如果说共识机制是区块链的灵魂核心，那么对于区块链特别是联盟链及私链来看，跨链技术就是实现价值网络的关键，它是把联盟链从分散单独的孤岛中拯救出来的良药，是区块链向外拓展和连接的桥梁。

由于LutherChain的模块化和多链并行特性，将来会有大量公有链、联盟链、私有链基于LutherChain技术实现，所以LutherChain内置垮链协议模块，开发者可以简单轻松的运用垮链协议打通多链生态圈。

（一）Luther的垮链协议将支持bitcoin，ethereum，EOS以及Luther的子链。

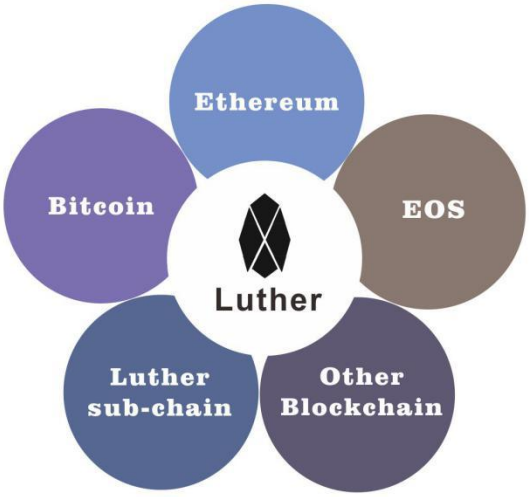

图6 LutherChain 垮链协议

（二）Ethereum和Luther垮链流程

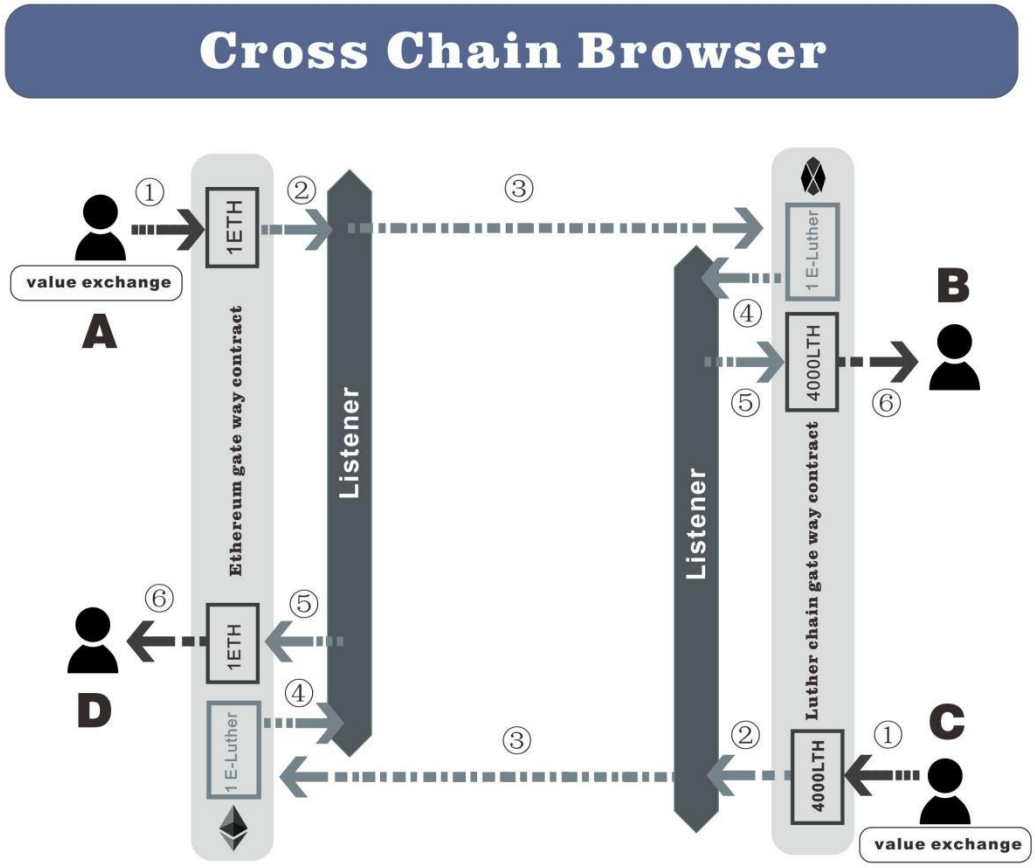

图7 LutherChain 和 Ethereum垮链流程

- 在ethereum和LutherChain上分别发布锚定代币E-luther，L-ether；
- 在ethereum和LutherChain上分别部署gateway contract；
- 在ethereum和LutherChain两侧都部署区块和交易监听；
- 以用户A转账给用户B为例，价值从ethereum网络传递到LutherChain网络中，用户A发送1个ETH给用户B；
- 步骤①，用户A发起转账，会预先通过value exchange 做实时的价值转换，然后调用Ethereum gateway contract进行转账，参数包含：ETH数量，折算目标链资产LTH的数量，目标链用户B的地址等。

- 步骤②，步骤①的交易被Listener监听。
- 步骤③，由Listener模块自动触发调用LutherChain gateway contract，从Listener地址转账1个L-ether到LutherChain gateway contract的被监听的池地址；真正的ETH留在Ethereum gateway contract内作为准备金。
- 步骤④，Listener监听到L-ether的转账交易。
- 步骤⑤，由Listener触发调用LutherChain gateway contract。
- 步骤⑥，合约转账给用户B 4000个LTH。
- 从LutherChain到ethereum的转账流程一样。
- 整个垮链转账过程，用户都可以在cross chain browser中查询跟踪。

7. 共识机制

POW

提供标准的POW算法作为模块组件，支持CPU和GPU挖矿。

POS/DPOS

提供标准的POS/DPOS 算法作为模块组件。

POS：也称股权证明，类似于财产储存在银行，这种模式会根据你持有数字货币的量和时间，分配给你相应的利息。

简单来说，就是一个根据你持有货币的量和时间，给你发利息的一个制度，在股权证明POS模式下，有一个名词叫币龄，每个币每天产生1币龄，比如你持有100个币，总共持有了30天，那么，此时你的币龄就为3000，这个时候，如果你发现了一个POS区块，你的币龄就会被清空为0。你每被清空365币龄，你将会从区块中获得0.05个币的利息(假定利息可理解为年利率5%)，那么在这个案例中，利息 = 3000 * 5% / 365 = 0.41个币，这下就很有意思了，持币有利

息。

比特股的DPoS机制，中文名叫做股份授权证明机制（又称受托人机制），它的原理是让每一个持有比特股的人进行投票，由此产生101位代表，我们可以将其理解为101个超级节点或者矿池，而这101个超级节点彼此的权利是完全相等的。从某种角度来看，DPOS有点像是议会制度或人民代表大会制度。如果代表不能履行他们的职责（当轮到他们时，没能生成区块），他们会被除名，网络会选出新的超级节点来取代他们。

PBFT

PBFT： Practical Byzantine Fault Tolerance，实用拜占庭容错算法。 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。尽管可以存在多于3f+1个副本，但是额外的副本除了降低性能之外不能提高可靠性。

由于PBFT算法随着节点数的增多，其性能将下降，而公有链节点数量大多庞大，所以PBFT算法作为组件，供联盟链选用；作为企业级联盟链，PBFT算法有其独特的优势。

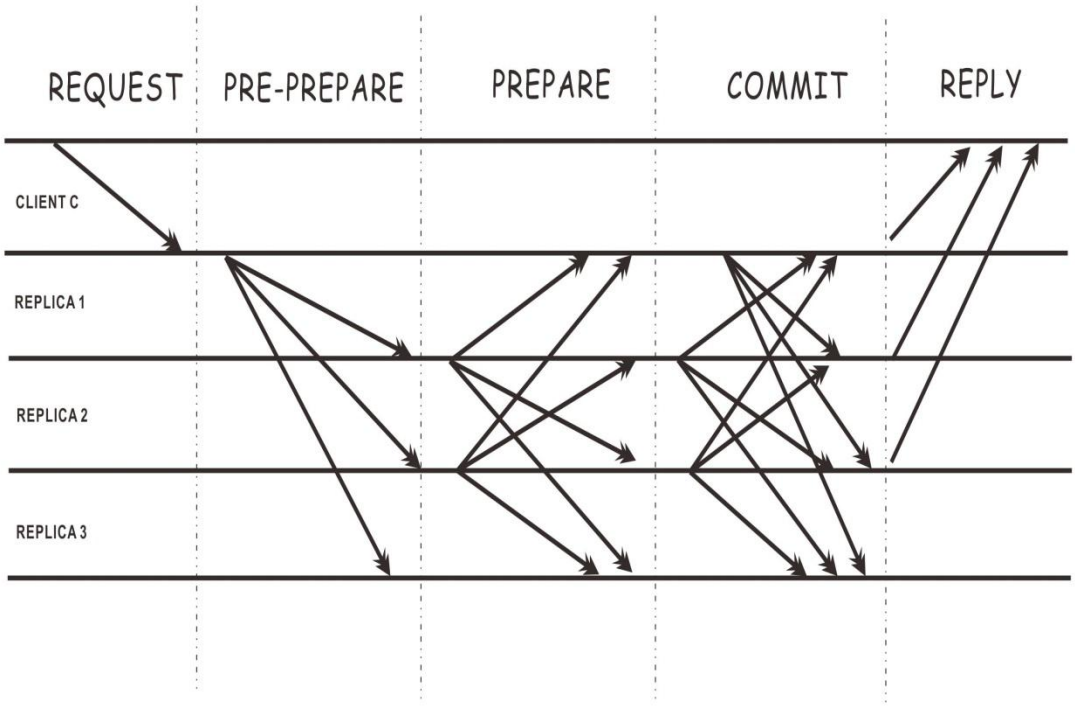

图8 LutherChain PBFT

背书策略

背书策略模式，和PBFT一样，作为联盟链共识选项，用户自定义标准格式的背书策略和智能合约一起发布到区块链网络上；背书策略根据链内的组织架构灵活配置。

举例：

在一个商户联盟中，商户A拥有20个节点，商户B拥有30个节点，商户C拥有40个节点，商户D拥有50个节点，共同组成一条链；

背书策略定义为：

(18 of A & 20 of B & 10 of C & 1 of D) or (15 of A & 22 of B & 38 of C & 40 of D)

对于一个交易，每一个节点都会执行智能合约并对结果进行背书签名，在

背书策略验证模块，只要达到了背书策略公式所描述的节点数量通过了验证，则共识达成，即视为交易有效，否则就判定为失败交易。

背书策略的权重，是在联盟组建时由联盟成员自由商榷后确定的。

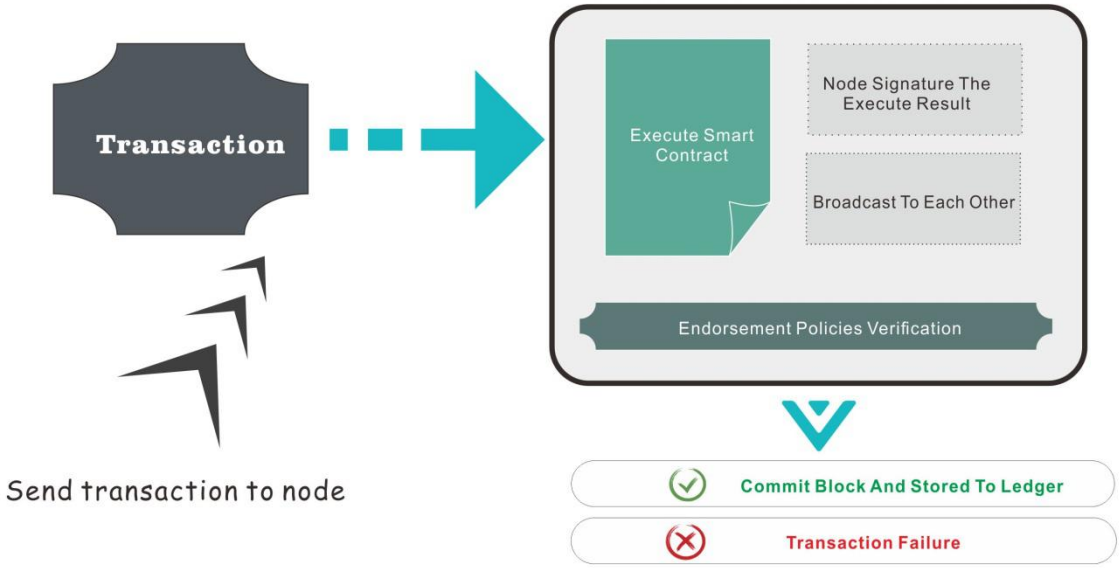

图9 LutherChain 背书策略验证

五、Luther 的经济模型

Luther 系统中内置的系统代币代码为 LTH，系统内置代币是整个系统生态的驱动剂，将用于支持应用发展、支付应用消耗费用、支持子链数字资产智能兑换、参与共识奖励、支付交易手续费等。

（一）代币发行分布

LTH初始发行 10亿，其划分为六大部分，具体比例如下：

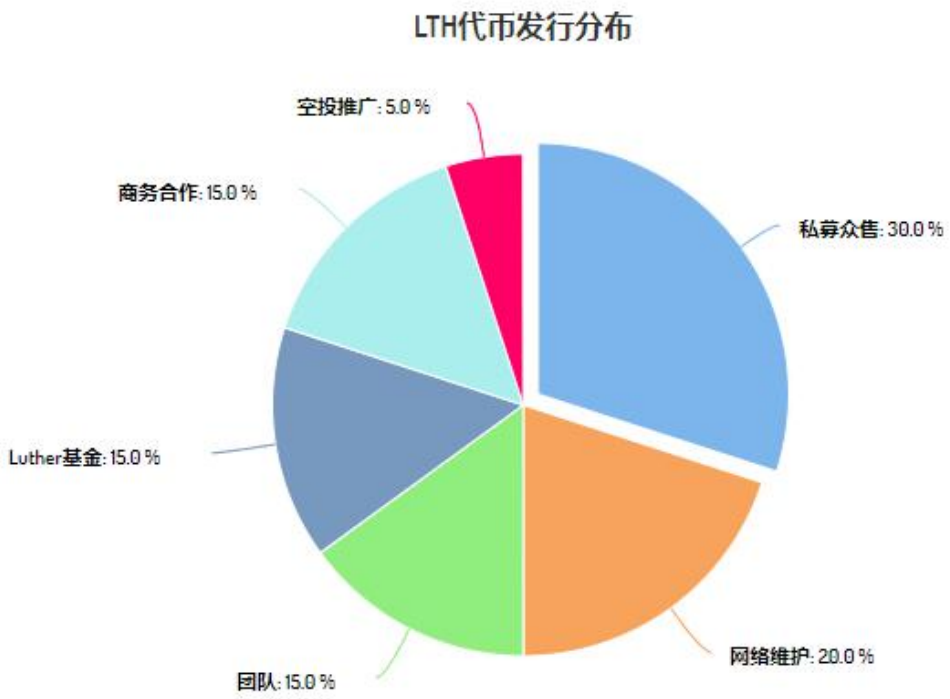

图10 LutherChain 代币分布

1、网络维护，占比 20%，共 2亿，主网上线后由矿工挖矿逐步产出。主网上线前处于锁仓状态。

2、私募众售，占比 30%，共 3亿。

3、团队，占比 15%。共 1.5亿，团队的部分会锁仓，上线后分 20 个月线性解锁，每月解锁 5%。

4、Luther基金，占比 15%，共 1.5亿，用于社区生态建设。

5、商务合作， 占比 15%，共 1.5亿，用于上交易所，商务合作等。

6、空投推广， 占比 5%，共 5000万。用于空投给主流token的社区成员地址。

（二）区块链网络维护

和BTC一样LTH总量恒定，不会通胀。

代币总量的20%将由挖矿产出，并逢2年减半。挖矿产出细则将在主网上线前公布。

（三）LTH价值体现

1. LTH代币作为链上交易的燃料。
2. 智能合约部署和执行将消耗一定的LTH。
3. 在未来，任何Luther的子链资产都将会对LTH代币持有者进行一定比例的空投。
4. 可以享受所有Luther基金会旗下区块链应用收益的30%分红。分红以LTH持有量为依据按比例分发。

5.Luther将作为Luther上第一个应用ltalk（链链）以及未来所有基于Luther生态应用的的生态资产。

六、Luther 发展路线图

2018年Q1

开始Luther的第一个应用ltalk的设计，ltalk是全球首个区块链行业社交及信息共享平台。

开始Luther主链技术设计。

2018年Q2

发行ethereum的ERC20代币LTH，在Luther主网上线后进行置换。

完成ltalk研发，发行内测版。

资源对接。

2018年Q3

ltalk正式版发布，上线android和ios应用市场。
市场部进行应用推广。
社区建设，建立中文社区，英文社区。
LTH上线三家知名海外交易所。

2018年Q4

全力展开Luther主链研发工作。
进行Luther生态圈的布局。
持续推广ltalk，持续迭代新版本。
扩大社区规模。
LTH上线更多主流交易所，提高流通性。

2019年Q2

发布主链内测版本以供社区头号玩家测试。
LTH上线更多主流交易所，提高流通性。
建立Luther生态圈。

2019年Q3

上线主网并进行主网代币置换。
Luther轻钱包app发布。
发布区块链浏览器。
LTH上线更多主流交易所，提高流通性。
公布下一个发展阶段的路线图和战略方向。

2019年Q4

Luther基金会成立专项基金用于扶持在Luther链上的应用、dapps以及以LutherChain技术为基础建立的子链。
持续公布和扶持多个Luther生态圈项目。
LTH上线更多主流交易所，提高流通性。

2019

2019年底，将Italk发展为千万级用户的全球区块链生态app；计划发展扶持LutherChain链上应用及Dapp100个以上；计划发展扶持LutherChain子链项目20个以上。

七、团队

盛永春
联合创始人兼首席执行官

惠得航
联合创始人兼首席运营官

孙茂杨
联合创始人兼首席信息官

莫尔斯贝尔
联合创始人兼首席技术官

赵杰
联合创始人兼首席财务官

艾萨克 坎贝尔
区块链底层开发工程师

哈该 沃克
区块链底层开发工程师

向云文
核心开发工程师

瓦特 艾迪
开发工程师

凯佩尔 罗德尼
开发工程师

蜜尔娜 雪莱
开发工程师

泰勒格雷戈
开发工程师

乔安娜 珀西
美术工程师

巴塞洛缪 乔伊斯
美术工程师

康纳加西亚
营运经理

琼 刘易斯
营运经理

八、完结

Luther团队将以务实和创新来驱动区块链技术落地和独角兽应用的诞生，引领第四次工业革命。

Luther 官 网： lth.one