



目录

1. 摘要	2
2. 目标	3
3. 技术体系	4
3.1. 共识机制	4
3.2. 安全机制	5
3.3. 智能合约	6
3.4. 目录索引链	7
3.5. 网关与稳定币	8
4. 经济系统	9
4.1. 发行总额与分配模式	9
4.2. 挖矿机制	10
4.3. 生态合作应用场景激励	10
4.4. 经济生态模型	11
4.5. 生态可扩展性	12
5. 路线图	13
6. 核心团队	14



摘要

随着物联网、移动互联网的快速发展，全球数据迅猛增长，据国际数据公司（IDC）的监测数据显示，近几年全球大数据储量的增速每年都保持在40%，2016年、2017年和2018年全球数据储量分别为16.1ZB、21.6ZB和33.0ZB。数据与人们的生活息息相关，对政府、企业、组织和个人来说，数据的影响已远远超出了人们的预期。

在新技术、新业态、新模式乃至新概念层出不穷的时代，数据资产化成为一个必然趋势，LKBT泛化了数据资产的概念，将知识、算法和算力也看作是一种广义的数据资产。LKBT是为数据资产交易平台服务的金融基础设施，实现数据资产的可信交易和记账服务，可与各类知识计算化操作系统和数据资产交易系统无缝连接。



目标

LKBT是全球首个专门为数据资产（知识，算法，算力）可信交易及清算而设计的区块链基础设施，目标是明确地定义数据资产（知识，算法及算力）的质量标准，定价规则，交易清算体系及制度，完整地解决数字资产（知识，算法及算力）在交易中的合规难、定价难、算法计费难及清算难的问题。



技术体系

数据有不同的表现形式，如数字、文字、图像、声音等，它是信息的载体，它表现为数据库、文档、图片、视频等各种形式，并作为信息系统的输入和输出而存在。在大数据时代，数据是一种无比珍贵的资产，也称为数据资产，它是属于个人或组织的数字财产。狭义的数据资产为数据本身，广义的数据资产包括数据、知识、算法和算力，LKBT中的数据资产泛指广义数据资产。

知识（Knowledge）是符合文明方向的，人类对物质世界以及精神世界探索的结果总和。算法是（Algorithm）是解题方案的准确完整描述，是一系列解决问题的清晰指令，算法代表着用系统的方法描述解决问题的策略机制。也就是说，能够对一定规范的输入，在有限时间内获得所要求的输出。算力是指分布在不同地方的存储资源和计算资源。

LKBT为数据、知识、算法和算力等数据资产的全球流通提供基础平台，实现数据资产的可信交易和记账服务，可与LEBEN等各类知识计算化操作系统和数据资产交易系统无缝连接。

共识机制

区块链是一种去中心化的分布式账本系统，它可以用于登记和发行数字化资产、产权凭证、积分等，并以点对点的方式进行转账、支付和交易。区块链系统与传统的中心化账本系统相比，具有完全公开、不可篡改、防止多重支付等优点，并且不依赖于任何的可信第三方。

由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序不可能完全一致。因此区块链系统需要设计一种机制对在差不多时间内发生的事务的先后顺序进行共识。这种对一个时间窗口内的事务的先后顺序达成共识的算法被称为“共识机制”。

LKBT采用LkbtBFT共识协议的BFT机制来实现所有验证者节点就将要执行的交易及其执行顺序达成一致。LkbtBFT通过预先审核通过的权威节点来完成验证，通过预置的验证与投票者名单，可在很短的时间内对区块数据进行投票与验证，对区块数据达成共识。可降低区块链交易验证的复杂性和范围，提高区块链的信息处理能力，支持高吞吐处理能力的需求。LKBT共识协议能在高交易处理量、低延迟和更高能效之间达成一个平衡。

安全机制

区块链能构筑安全、可信的存储与交易网络的核心是其安全机制和密码算法，LKBT采用了可扩展哈希函数、可插拔公钥密码技术及环签名等智能合约隐私保护技术，从而提供一个安全高效的交易网络。

可扩展哈希函数

哈希（Hash）函数又称散列函数，它是一种单向密码体制，即一个从明文到密文的不可逆映射。Hash函数能够将任意长度的输入映射成固定长度的输出，即散列值。Hash函数的数学表述是 $h=H(m)$ ，其中 H 指Hash函数， m 是指任意长度的明文， h 是固定长度的Hash值。Hash函数对于不同的输入可以获得不同的Hash值，如果出现对于不同的输入获得了相同的Hash值则称为Hash碰撞。

可扩展哈希函数是可根据实际应用场景和性能需求进行自适应调整的哈希函数，LKBT通过制定策略来选择不同哈希函数的方法来实现。LKBT将可扩展哈希函数用于区块生成及链接，将根据实际具体需求，灵活选择 SHA、SCRYPT、BLAKE等哈希函数，从而保障其链上数据的不可篡改性，提升LKBT的安全性。

公钥密码技术

公开密钥体制是加密和解密使用不同的密钥。每个用户保存一对密钥，即公钥（PK）和私钥（SK），PK是公开信息，用作加密密钥，而SK需要由用户自己保存，用作解密密钥。加密算法和解密算法是公开的，虽然SK和PK是成对出现，但却不能根据PK计算出SK。公开密钥体制的优点是适用网络的开放性要求，与对称密钥体制相比，密钥管理要简单的多，尤其可以方便地实现数字签名和认证。

LGBT采用可插拔公钥密码技术来保障交易的完整性和可信度。LGBT根据用户需求，提供兼容不同国家或组织的公钥密码标准方法，包括但不限于基于椭圆曲线的公钥密码技术，从而提升LGBT的安全性和适用范围。

智能合约中的隐私保护技术

智能合约运行在区块链上，没有任何第三方进行信用背书，因此智能合约不同于传统合约的隐私保护。智能合约中的隐私威胁主要是攻击者对身份隐私和交易隐私的攻击，目前主要隐私威胁包括匿名性隐私威胁、访问控制隐私威胁和链上信息隐私威胁等。针对区块链数据全部上链并且公开透明的隐私保护问题，LGBT采用混币器和环签名技术来保障智能合约的安全性。

智能合约

智能合约作为区块链技术的核心架构之一（合约层），是一种可由事件驱动的、具有状态、运行在区块链上的计算机程序，以数字化方式传播、验证或执行合同，进而控制和管理区块链上的智能资产。

在区块链技术中，智能合约可看作一种嵌入式程序，能够内置于数据区块中，形成可编程控制的数字化系统。在部署智能合约之前，会预先制定好与合约相关的所有条款的逻辑流程，当预先编程好的条件被触发时，智能合约便会自动执行相应的合同条款，用户与智能合约的交互行为都需要严格遵守此前制

定的逻辑流程，以防止出现违约行为。

LGBT区块链兼容Solidity智能合约，并在此基础上加以扩展，支持私有智能合约。私有合约定义联盟，只在联盟内可见，合约数据只保存在私有DB上，不会把隐私数据全网分发。实现公开交易全网一致共识，私有交易局部共识，隐私数据得已保护。

目录索引链

目录索引链，是数据、知识、算法资产化的可信存储媒介，是资产形式化后的可信流通渠道，是可交换资产价值发掘的可信交易链条。

现代信息社会发展速度空前加速，海量数据被制造、传输和使用，互联网中数据无处不在；而蕴含于数据中的知识，是在信息的不断沉淀和应用交互过程中产生出来的，揭示未知的规律；算法是智慧的形式化，表现为知识的收集、加工、应用、传播能力，因而形成流程化的方法。从数据到知识，再到算法，蕴藏着巨大的发展机会和力量，数据、知识、算法的传播是人类迈向智能传播的必然过程。

数据走向资产化是大势所趋，在数据资产化的过程中，必须建立高效的数据交换机制，实现数据的互联互通、信息共享、业务协同，以成为整合信息资源，深度利用分散数据的有效途径。知识和算法具备类似特性，此类资产所具备的可复制、可共享、无限增长和供给的禀赋，成为数字经济时代发展的关键生产要素。

目录索引链通过区块链技术真正实现数据资产化，从而为主体（个人、家庭、企业、政府、司法等）之间实现资产确权、完成资产的有效流转。随着区块链上数据的不断完整，数据资产的流转会越来越快，从而会吸引更多的参与者参与其中。目录索引链为专业人士打造了知识和算法产权撮合平台，在消费者、权益人、合作伙伴和投资人等主体间实现智能撮合，达成其间的可信交易。

网关与稳定币

稳定币是一种与另一种资产挂钩的加密货币（如黄金、白银、美元、欧元等），它是一种全球货币，不与中央银行挂钩，其价值较稳定。目前常见的稳定币可分为法币稳定币（Fiat Stablecoin）、加密稳定币（Crypto Stablecoin）、商品稳定币（Commodity Stablecoin）、主权稳定币（Sovereign Stablecoin）等类型。

法币稳定币以美元或欧元等货币（法定货币）挂钩或抵押，采用固定比率（1稳定币：1美元），如True USD（TUSD）、USD Tether（USDT）、Paxos Standard（PAX）、USD Coin（USDC）Center、Gemini Dollar（GUSD）和Bitcoin Air（USDAP）。加密稳定币是通过与其他虚拟货币挂钩或抵押，如Bitshares、BitUSD、MakerDAO等。商品稳定币是币的价格与商品挂钩或抵押，商品可以是金属（如金、银、铂和铜）、能源（如原油、天然气和汽油）、牲畜（如猪肚、活牛和饲养牛）或农产品（如玉米、大豆、小麦、大米、可可、咖啡、棉花和糖），如Digix Global和HelloGold是基于金属的稳定币。主权稳定币是由中央银行或监管机构支持并批准的币。LKBT可通过资产网关，对接各种稳定币。

一体化稳定币平台是LKBT构建互操作性经济生态系统的重要部分。将通过资产网关，对接已经存在的稳定币例如Libra、USDT、TUDS、Dai等，通过LKBT区块链来映射资产，与之共享数字经济成果。资产网关使运行在不同网络上的数字资产在平台上进行锁定和解锁，让数字资产能够访问并使用所有LKBT主网上的创新功能。一旦锁定，资产就将进入LKBT主网生态系统，并能有效在LKBT网络上与其他资产进行交互，用于支付。



经济系统

为促进LKBT生态建设，优化发行了独立数字货币LKBT，用于未来数据资本时代数据交易的支付工具。LEBEN是LKBT的第一个合作伙伴，后期LKBT将会为各种数据资产交换平台提供金融服务。

发行总额与分配模式

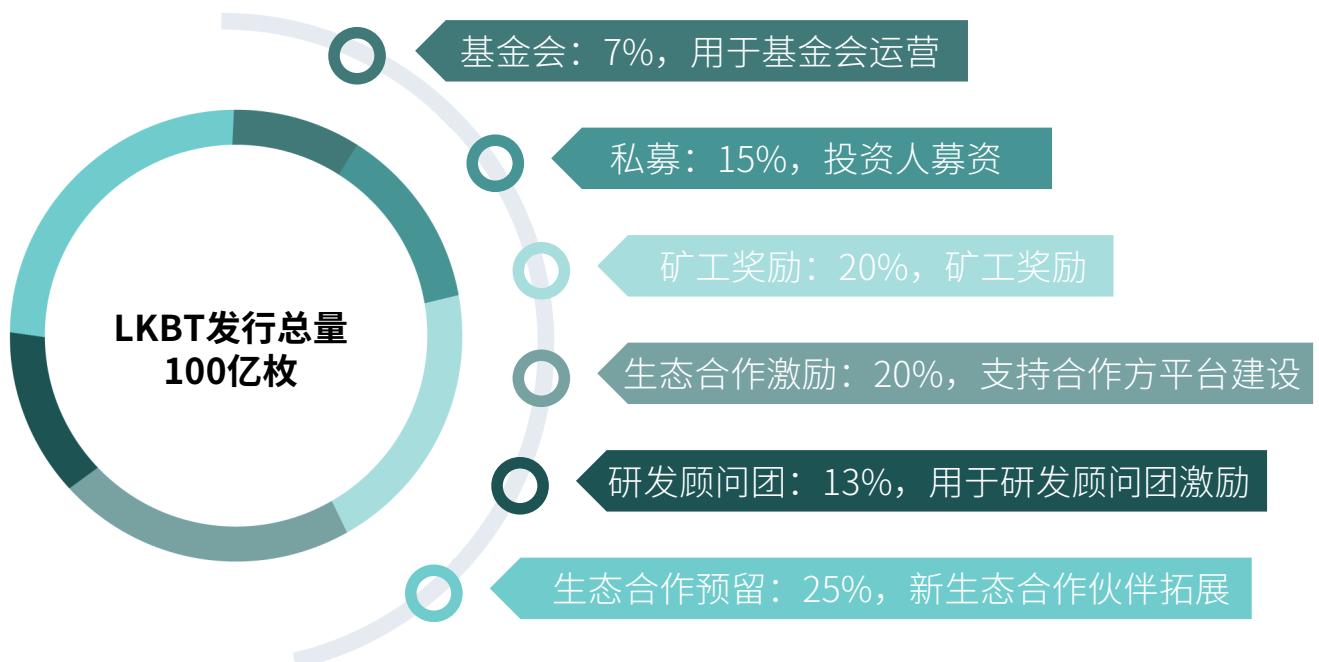


图1：分配模式

挖矿机制

- **挖矿模式：**LGBT挖矿模式为POS挖矿模式。
- **超级节点：**全球范围内筛选重要算力合作伙伴作为超级节点。
- **衰减模式：**每2年减半。

生态合作应用场景激励

LGBT选择了LEBEN作为第一个支持的应用场景，并且提供最大力度支持。我们将提供20%的LGBT用于LEBEN生态建设。

激励对象：用于激励合作方LEBEN系统生态中的数据供给方、知识供给方、渠道服务方、数据审核方以及平台参与者。

通过LGBT的激励作用，促进合作方平台发展，扩大LGBT实用价值。

经济生态模型

LKBT为数据交易和支付而生，LKBT服务的对象是拥有实际应用场景的产业生态合作伙伴。LKBT与合作伙伴共同建设LKBT的经济系统。

LKBT经济系统运行模式

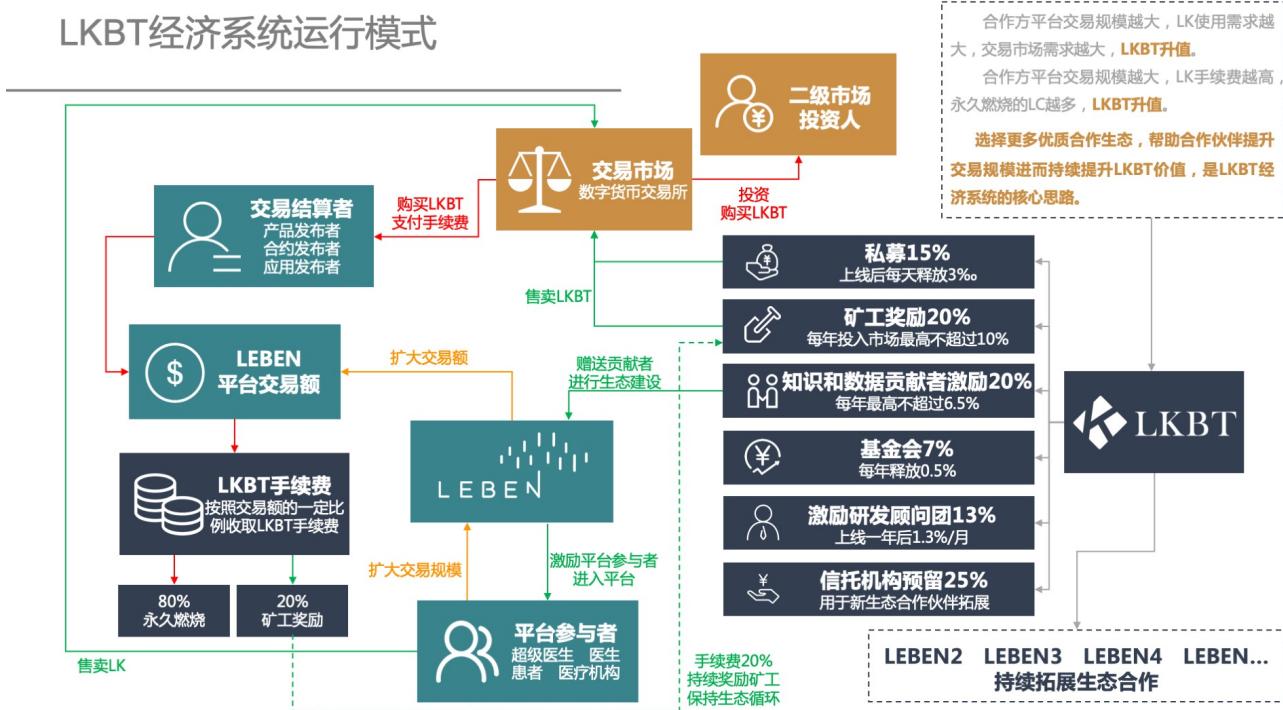


图2：经济系统运行模式

LKBT经济系统运行的核心

1. LKBT的实用价值

LKBT首个实用场景就是与LEBEN平台的交易深度绑定，在LEBEN平台上每完成一次交易，都需要按照交易额度的一定比例支付对应价值的LKBT作为交易计算手续费。LKBT的价值与LEBEN平台的价值高度绑定，LEBEN平台规模越大，交易额越大，LKBT的价值越高。

2. LKBT的燃烧机制

LKBT设定了持续性燃烧机制，LEBEN平台的使用者所支付的LKBT总额中80%的额度会作为燃料货币直接燃烧。LEBEN平台的交易额越大，LKBT的交易计算手续费额度也就越大，燃烧掉的LKBT也就越多。

生态可扩展性

LKBT预留了25%的份额用于扩大应用生态合作，在未来LKBT会选择更多类似LEBEN这样拥有实际应用落地场景的合作伙伴进行合作，不断扩大LKBT的应用范围。



路线图

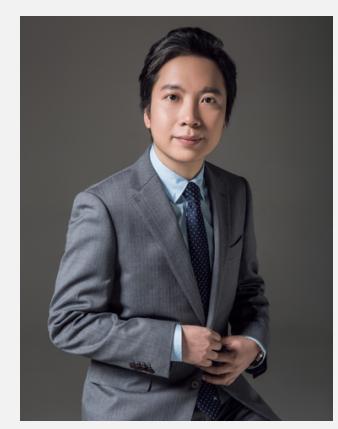




核心团队

Amos Lang, LKBT创始人

硕士，曾就读于清华大学、中国科学院，拥有15年以上互联网产品运营、开发、市场推广经验，自2016年开始，涉足于大型基础设施的PPP投融资与“互联网+”信息化建设。擅长将区块链技术落实到实体产业实际运转并真实解决产业应用的问题。



Justin博士, LKBT首席科学家

博士，毕业于清华大学精密仪器系，16年以上IT平台设计开发经验，先后服务于贝尔实验室，IBM中国研究院等著名公司，擅长人工智能分析、数据平台的设计及开发，2014年进入国内著名对冲基金专注于大数据交易平台的设计及人工智能的引入，2018年进入区块链行业，擅长区块链中的共识算法，多方安全计算，联邦学习等算法逻辑及体系架构，并有多项专利正在申请中。



Evan, LKBT首席营销官

18年以上互联网营销推广经验，曾就职第九城市、完美世界等知名互联网企业，历任营销总监、发行副总裁等职务。2018年进入区块链行业，擅长对应用于产业方面的区块链项目进行推广与宣传。

