闪电比特币 白皮书

LIGHTNING BITCOIN WHITE PAPER

LIGHTNING BITCOIN

闪电比特币(LBTC)白皮书
Lightning Bitcoin(LBTC) Whitepaper

1 概要

LBTC（Lightning Bitcoin，闪电比特币）是去中心化的全球价值互联网传输协议，具体应用包括点对点支付以及去中心化数字资产交易等。任何接受 LBTC 协议的用户都可以几乎免费的使用 LBTC 来保证交易的实时性与安全性。

LBTC 是为了解决比特币存在的矿工中心化、网络拥堵、交易处理效率低等问题，由 Lightning 团队硬分叉比特币而形成的基于 DPOS（委托权益证明）共识机制的区块链；LBTC 是比特币实验的重要组成部分。

得益于 DPOS 共识机制出块时间短、高效、强健的特性，LBTC 可实现极为迅速的交易确认。Fast as Lightning，LBTC 正因其快如闪电而被命名。LBTC 是世界上最高效、最具有应用潜力的比特币协议分叉版本。借助于强大的网络吞吐能力，LBTC 可为快速点对点支付、去中心化交易平台、智能合约、链上 Oracle、链上治理等开发及使用需求提供充分性能支撑。

2 分叉方法论

2.1 点对点的电子现金系统

在 2008 年末中本聪提出的白皮书《比特币--一种点对点的电子现金系统》中，明确指出比特币是一个不依赖中心机构的、点对点的电子现金系统。

所谓电子现金，以当下的商业概念理解，它是一种支付方式（支付系统），但有别于常见的第三方支付系统，比特币实现了不依赖中心与中介的用户支付行为。同时，比特币也是一种通货商品；无论我们是否定义比特币为货币，其通货商品的属性是必然成立的，该属性亦赋予比特币具体的内含价值。

在目前版本的比特币方案之前，密码朋克运动的先驱者曾经有数次尝试，但都没有成功。中本聪的方案的精髓在于，他首先保证了去中心化的 P2P 网络是可以在技术上实现的，而后建立了强健的、长期可持续发展的经济系统。无数先例表明，倘若没有去中心化这一技术基础，任何电子现金系统的尝试最终都难以避免中心化机构的打击。

基于不对称加密体系和哈希函数，比特币构建了坚固的反破解系统，使得对比特币区块链数据的逆向结构在计算上不可能。比特币使用的 P2P 网络概念很早就已被应用，但是中本聪创造性地利用不对称加密函数和哈希函数的 trap-door 特性，建立了依赖私钥-公钥-地址的密码学构造、区块之间的哈希关系连接、可验证的电子签名交易脚本等一系列精巧机制，使得破坏比特币数据库所消耗的资源远远大于构建数据库所消耗的资源。

设计者的智慧更体现在他所引入的矿工奖励机制，即依赖矿工提供算力构筑比特币信任的城墙，进而通过不可逆地凝结算力这一方式，从无到有创造了一个全球性电子现金系统所需要的关键元素--信任。某种意义上来说，构建牢固且不断累积增长的信任，才是比特币协议设计思想核心的核心。

2.2 LBTC 的分叉方法论

LBTC 通过发起对原始比特币协议的硬分叉，成为了比特币的一个实现版本。因此，LBTC 可以被认为是对比特币协议的一种诠释方式，亦应当被认为是点对点电子现金系统的一个落地方案。

比特币分叉，广义上指比特币区块链在拓扑结构上的分裂，在较短的一段时间内形成两条链共存的情况；但在比特币共识机制的作用选择下，区块链最终会恢复到唯一链的共识状态。狭义的分叉一般指代人为导致协议变动带来的硬分叉，因共识的分裂造成比特币网络在多套不同的共识群体环境下运行，形成若干独立的区块链协议。

比特币至今已有多个仍在成功运行的分叉协议版本，不同的协议版本针对比特币存在的缺陷或局限提出了各有侧重的解决方案。在众多分叉版本中，LBTC 在全球范围内首次提出基于 UTXO 的 DPOS 共识机制，并在解决了一系列技术难题后取得了长期稳定的主网运行。

LBTC 认为，一个真正的点对点支付系统，需要满足以下条件：

1）必要的信息吞吐能力和交易处理速度，足以应对高频小额支付交易；

2）支持该支付系统的运行成本足够低廉，大大低于该系统功效所产生的社会总效用；

3）设计出使得系统得以长期稳定运行的经济系统，引入适当的角色以支持具备拓展潜力的系统功能、并平衡其中的利益关系；

4）有可行的方法进行协议的自我更新，使得系统能够不断进化、引入新的特性以适应环境。

LBTC 的分叉方法论：

1）LBTC 认可原始比特币协议的价值与地位，复用和借鉴了原始比特币协议所产生的数据以及部分重要设计思想；

2）LBTC 希望实现比特币点对点现金系统的设计初衷，通过改造比特币协议，建立一个技术上可行的、全球共享的点对点现金系统；

3）在点对点现金系统的基础上，要求协议能够承载一定的经济活动功能，简便、安全、人人可用；

4）LBTC 对比特币协议进行的上述改进和创新，既要在根本上解决构建点对点现金系统所必须面对的技术及经济问题，又要尽可能地引入已经被验证成熟的技术和模式，确保系统的稳定性、用户可接受性以及长期可持续性。

针对保证足够的信息吞吐能力以及控制运行成本的矛盾，LBTC 引入了高效的 DPOS 共识机制，并创新性地解决了比特币底层 UTXO 模型与 DPOS 账户系统不兼容的难题，成为唯一使用 DPOS 共识机制、也是唯一成功解决 UTXO+DPOS 技术问题的比特币分叉协议。LBTC 所使用的 DPOS 共识机制，保证 3 秒稳定出块、具备不可逆转块设计，不仅使得点对点支付得到技术性能上的支撑，也为内置 dApp、链上治理、智能合约等复杂链上行为和功能提供了充分可行性。

其次，针对协议的可维护性、可持续性以及长期创造性解决问题的能力要求，LBTC 构建了有自身特色的链上治理哲学，引入了兼顾民主与效率的 SGS 链上治理体系。该体系极大程度地鼓励了社区对链上事务的参与、促进了参与群体对环境变化的响应，因而协议能够快速更新迭代，成为能够自我运营、自我更新进化的比特币协议。

而针对协议功能对经济模型中复杂系统角色的需求，LBTC 的链上治理体系和 DEX 体系引入了节点、分享治理委员会、交易网关、承兑网关等经济行为角色，权力结构上实现了记

账权与治理权的两权分离，在链上治理的民主实践中迈出创造性的一步。

2.3 比特币路线对设计初衷的背离

虽然比特币在设计上保证了去中心化、点对点的电子现金系统的技术可行性，但这并不意味着比特币的发展路径完全符合白皮书的设计初衷。比特币暴露了作为点对点现金系统的诸多弊病，并且在市场影响下选择了偏向于储值资产的自我定位。

前文已经提及过，一个真正的点对点支付系统，需要：

1）必要的信息吞吐能力和交易处理速度，足以应对高频小额支付交易；

2）支持该支付系统的运行成本足够低廉，大大低于该系统功效所产生的社会总效用；

3）设计出使得系统得以长期稳定运行的经济系统，引入适当的角色以支持具备拓展潜力的系统功能、并平衡其中的利益关系；

4）有可行的方法进行协议的自我更新，使得系统能够不断进化、引入新的特性以适应环境。

而比特币面临的第一个问题就是信息吞吐量低下所导致的交易处理量和交易确认时间问题。这一问题的本质是由比特币 POW 机制、区块大小设计（2M）和出块时间（约 10 分钟）带来的。区块大小、出块时间都是在 POW 框架下保证了网络的去中心化程度这一根本目的而决定的，不能通过简单地参数调节来解决问题。闪电网络提供了链下拓展的解决方案，但仍面临一些争议，并不是一个本质的方案（导致中心化、中介化）。此外，任何基于 POW 机制的其他比特币分叉协议，亦无法在根本上解决这一问题，反而分化了 POW 算力、进而分化了信用构建所需的宝贵资源。

比特币面临的第二个问题是 POW 机制对资源的巨大消耗。POW 的长期运行固然可以积累价值不菲的信用护城河，但无法以足够低廉的成本支撑一个点对点电子现金系统。这使得比特币反而在市场的影响下调整了自身的定位，主动或被动地选择了线上储值资产的发展路径，试图将自己打造为电子版、线上版的黄金。对这一路线我们不做过多评价；但可以肯定的是，比特币协议已经背离了当初建立全球点对点现金系统的初衷。

第三个问题是，比特币虽然构建了可以持续运营的矿工体系，但是对于点对点支付系统这样偏向于实际应用、功能设计更为复杂的系统来说，矿工体系显得过于简单低级。而且目前主流论调普遍认为，可以从数学和经济原理上证明，在 POW 机制下矿工与用户、开发者的利益是不可协调的。比特币体系无法给出一种很好的可以让复杂的链上系统经济角色（例如网关）产生收入并平衡各方利益的解决方案，也无法做到记账权与治理权的两权分离，极大地阻碍了比特币适应复杂经济活动的能力。

此外，比特币的治理机制依赖的是最为原始的链下治理，治理内耗极为严重、无法实现快速响应，这应当是众所周知且一度影响比特币生死存亡的大难题。又因比特币对路线的选择，导致比特币开发组对协议的变动和升级极端保守化，这一切使得比特币并不适合作为点对点现金系统这样一个偏向于支付应用的系统。

总而言之，比特币目前所具备的特性（POW、出块时间长、块容量小、矿工一元经济体系、协议变更保守化）更加适合当前作为储值资产、电子黄金的定位，但同时也不可避免地背离了点对点现金系统的初衷。

2.4 LBTC 分叉详情

- 分叉时间：北京时间 2017 年 12 月 18 日；
- 分叉块高：499999；
- 共识机制：基于 UTXO 的 DPOS；
- 出块间隔：固定 3 秒，可动态调整；
- 设置不可逆转块；
- 块体积：2M，可动态调整；
- 不支持隔离验证；
- 添加重放保护；
- 支持 CPU 挖矿；
- 有拓展智能合约的能力；

3 LBTC 的技术架构

对照	BTC	LBTC	BCH	BTG	BCD	B2X	SBTC	BCHC	BTX
分叉时间	-	2017.12.18	2017.8.1	2017.10.25	2017.11月底	2017.11.16	2017.12.17 (试验)	2017.8.1	2017.4.24 (非分叉产生)
总发行量	2100万	7265926	2100万	2100万	2100万	2100万	2121万	2100万	2100万
分配方式	挖矿	挖矿	挖矿 分叉获得	挖矿 分叉获得	挖矿 分叉获得 可预挖 (4000万)	挖矿 分叉获得	挖矿 分叉获得 可预挖(21万)	挖矿 分叉获得	挖矿 空投 快照索赔
共识机制	PoW	DPoS	PoW	PoW	PoW	PoW	不明	PoW	PoW
算法	SHA256	-	SHA256	Equlhash	optimized x13	不明	不明	SHA256	Timetravel 10
挖矿设备	ASIC	CPU	ASIC	GPU	GPU	GPU	不明	ASIC	GPU
块大小(实际)	1M(2-4M)	2M	8M(8M)	1M(2-4M)	8M(8M)	2M(4-8M)	8M(8M)	8M(8M)	20M
块间隔	10分钟	3秒	10分钟	10分钟	10分钟	10分钟	不明	10分钟	2.5分钟
难度调整	2周	-	DAA	EDA	2周	DAA	不明	EDA	Diff64_15
SegWit	支持	不支持	不支持	支持	支持	支持	不明	不支持	支持
重放保护	-	支持	支持	支持	支持	支持	支持	支持	-
其他特征	-	链上治理SGS 去中心化交易有所	-	唯一地址格式	交易金额加密	-	智能合约 闪电网络 知识证明 移除动态 检查点保护	-	-
团队	Bitcoin Core	Lightning Team	BitcoinABC Bitcoin Unllmited BitcoinXT 等	Bitcoin Gold	Evey团队 007团队	BitcoinX团队	Super Bitcoin	团队未知 官网介绍 抄袭BCH	Bitcore

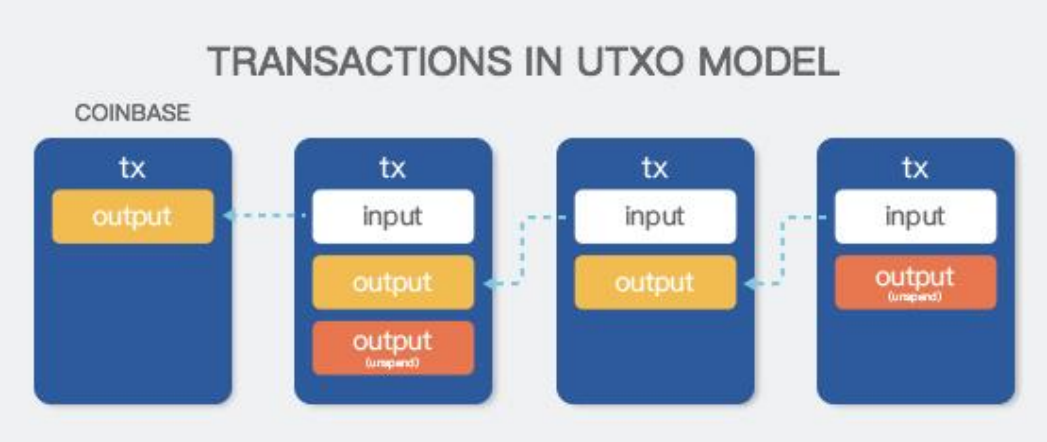
3.1 LBTC 是一个互联网价值传输协议

LBTC 是一个互联网价值传输协议（Internet of Value Protocol）。所谓价值传输，指在特定协议框架下可以实现的价值表达、传递和信用构建，以及基于此的所有经济金融活动，具体可能包括转账汇款、数字资产互换，法币-数字资产交换、信用背书的数字资产发行与交易、去中心化交易所、交易与承兑网关等一系列具备现实功能与社会效用的应用。

LBTC 协议的设计核心是，通过选用适当的技术架构去保证 LBTC 有足够的能力担当全球互联网价值传输的载体系统。LBTC 协议是实现价值传输的基本框架，即一切链上经济行为的母体。因此，我们对 LBTC 适用的技术架构以及各项内在细节提出了很高的要求，创造

性地建立了基于 UTXO 的 DPoS 共识机制，并设计了不可逆转块、时间戳共识、Cache 中间件等平衡了这一组合的性能与可靠性，实现了一个比原始比特币更为贴近点对点现金系统设计初衷的协议版本。

3.2 UTXO 模型：最安全的记账方式



在数据层，LBTC 沿用了比特币采用的 UTXO 模型，作为区块链账本记录的基础架构。UTXO 是 Unspent Transaction Output （未被花费的交易输出）的缩写，是中本聪最早在比特币交易数据结构设计中采用的技术方案，同时也是比特币协议为世界带来的一项极具创新性的数据结构概念。

UTXO 放在比特币协议的数据库中是这样的形式：在链上确认若干笔转账交易目的地指向用户 A，并且 A 尚未花费掉这些交易所指明的资产，所有协议参与者就认可 A 就拥有这些资产。

相较于 UTXO 模型，一般人更容易理解账户模型（Account Model）。账户模型是指在数据库中保存账户的 ID、所有者标识以及该账户中的资产余额；当发生转账交易时，这些账户的余额会依据交易进行调整变动，形成新的账户-余额的 Mapping 关系（即对应关系）。而在 UTXO 模型中，一个账户的余额并不是作为一个数字被储存起来的，而是用占有的

UTXO 的总和计算出来的。也就是说，UTXO 并没有所谓账户-余额的 Mapping 关系，它仅仅是一个对所有历史交易的忠实记录，简约但十分强健。

UTXO 模型具有以下优点：

UTXO 的可靠性

在一个区块结构体中，previousblockhash 和 merkleroot 是两个最重要的字段，都起到了防止交易信息被篡改的可能性。UTXO 模型的核心思想就是保证已经写入的数据不可变，链式的 UTXO 基于这一核心思想，通过哈希指针连接不同交易的输入和输出，保证所有交易的合法性，实现 UTXO 的可溯源性。

UTXO 的一次性

UTXO 模型中的每一笔交易都是由多个交易输入组成的，这些输入其实就是 UTXO + 签名。每一个交易输出（Transaction Output）只有两种状态，已花费和未花费。如此确保了每个 UTXO 仅能被花费一次，抗双花攻击能力极高。

UTXO 的隐匿性

对比起账户模型，UTXO 更加私密。前文已知，每个 UTXO 都是“一次性”的。用户要是每笔交易都换一个地址，那么就很难找到其中两个地址的相关性，保证了交易的隐匿性。如果还有需要进一步提高这种隐匿性，亦可以考虑使用环形交易签名对、交易要素混用等技术手段。

UTXO 的可并行性

UTXO 模型被公认具有潜在的可扩展性，因为 UTXO 允许交易的并行化处理。当一个交易发送者发送两笔独立的交易时，花费独立的 UTXO 也可使交易用任意次序处理。这样可以使一个人的资金分离，在保证隐私的同时具有并行处理交易的能力。

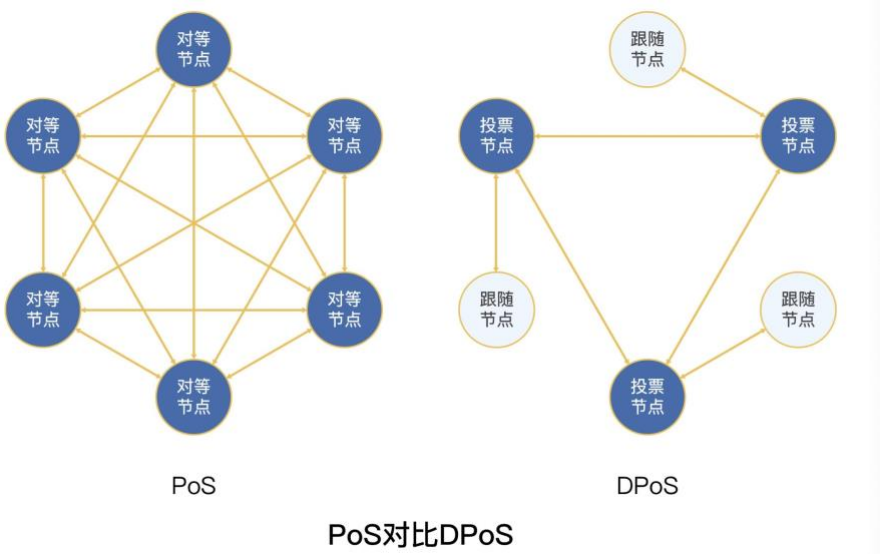
比特币的 UTXO 模型经过了多年较为稳定的运行和测试，性能和安全性都有较大的优势。LBTC 作为比特币的分叉币，采用 UTXO 模型，对于 LBTC 来说是对其底层技术的一种继承。LBTC 采用比特币核心代码为基础进行开发，也是较为谨慎的选择。UTXO 的安全性和并行交易特点也将给 LBTC 带来更高效率的可能。

3.3 DPoS 架构：最高效的共识机制

在共识协议上，LBTC 采用了委托权益证明（DPOS）的机制。DPoS 是基于 POW 及 POS 的基础上，出现的一种新型的保障数字货币网络安全的共识算法。它既能解决 POW 在挖矿过程中产生的大量能源过耗的问题，也能避免 POS 权益分配下可能产生的“信任天平”偏颇的问题。那么，DPoS 就能顺理成章成为在共识机制 3.0 中的代表性共识机制。

简单阐述 DPoS 共识机制，其原理是让每一个持币者进行投票，选出一定数量的持币者代表,或理解为一定数量的代表节点，并由这些代表节点来完成交易验证和区块生产的工作。持币者可以随时通过投票更换这些代表，以维系链上系统的“长久纯洁性”，保证该协议有充分的去中心化程度。

DPOS 是目前所有共识协议中最快，最有效，最分散，最灵活的共识模式。 DPOS 利用利益相关方批准投票的权力以公平和民主的方式解决共识问题。 所有网络参数，从简单的交易手续费标准、出块间隔、区块参数到更为复杂的链上治理规则，都可以通过选定的代表进行调整。



PoS对比DPoS

DPoS 共识机制具有以下优点：

DPos 的高效能：

更快的确认速度：以 LBTC 为例，每个区块的时间固定为 3 秒，一笔交易（在得到 6-10 个确认后）大约消耗 1 分钟，完整的区块生产周期仅需 5 分钟；每 1-2 个周期即可以生成作为确认点的不可逆块。而在 PoW 机制下，以比特币为例，产出一个区块需要约 10 分钟，而确认一笔交易（得到 6 个确认）至少需要 1 小时。

DPoS 的低功耗：

DPoS 机制将节点数量进一步减少的同时，将节点间的相互关系从竞争改为合作，避免了不必要的算力竞争和互相攻击等无谓的损耗，在保证网络安全的前提下，整个网络的能耗进一步降低，网络运行成本最低。

DPoS 的高效治理：

只要利益相关方批准，开发人员可以实施他们认为合适的任何更改。这项政策不仅可以保护开发者，同时它还可以保护利益相关者，并确保没有任何人单方面控制区块链网络或让区块链网络失控。硬分叉如同替换了 51%的见证者，因此利益相关者参与的越多，其对应的选举证人越多，那么整个系统的安全性就越高。

DPoS 的鲁棒性：

在整个过程中，任何人都可以通过观察见证人的参与率来监测网络健康状况。如果在某个时候见证人的参与程度都低于一定水平，那么整个区块链交易网络用户可以被允许用更多时间进行交易确认，而且还会提醒用户需要对他们的网络状况保持高度警惕，可以在出现问题后的 1 分钟内提醒用户区块链网络上可能存在潜在的问题。
DPoS 机制最早由 BM 应用在 BTS 项目中。BM 的其他明星项目 STEEM、EOS 同样沿用了这一共识机制。DPoS 自诞生以来一直都是高性能、高效率、高灵活性的代名词，众多项目的长期实践也证明了 DPoS 机制的这些优良特性。

3.4 UTXO+DPoS：惊人的奇妙组合

很多人可能会有一个错误的认知，认为 DPoS 只适合于账户模型，不能用于 UTXO 模型。但是实际上 UTXO 模型是存放记录的一种方式，用于交易存储、组织及验证；DPoS 是一种共识算法，用于保证在分布式网络中参与者也可以对交易数据取得一致认识。UTXO 和 DPoS 没有互斥性也没有相关性。
实际上 UTXO 和 DPoS 联合会有许多额外的优势。

更高的性能基础：

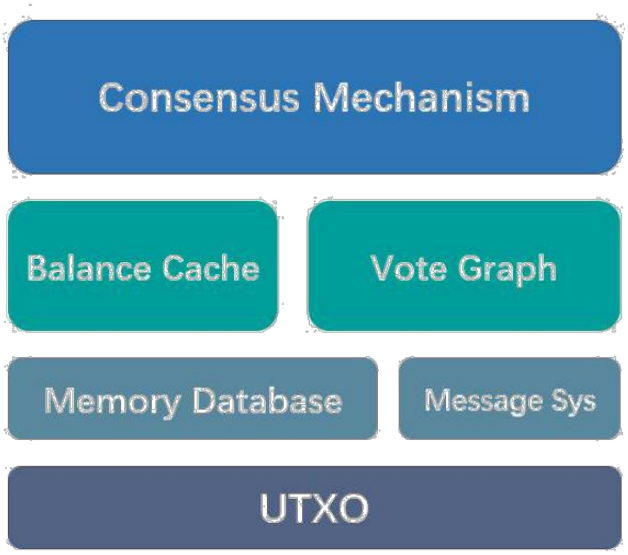
因为 UTXO 的分离操作，具有潜在的可并行性。配合 DPoS 的性能支持，使得 LBTC 具有极为优秀的性能基础。实际运行结果来看，LBTC 可以满足 2800TPS 运行要求。

更高的安全性：

在 DPoS 的架构中，节点按照给定的顺序出块，且时间间隔很短。如果使用账户模型，数据库会膨胀的很快，而且极短时间的数据库同步面临网络异常的时候会有许多问题。而采用 UTXO 模型，不仅可以保持数据库的大小，也可以根据特定算法生成锻造周期表，保持全网节点根据相同数据计算出的锻造周期表是一致的，此时全网节点达成共识。当锻造节点出现宕机、网络分区等情况，全网会根据“事务提交”的原则，以最长链为主链自行切换覆盖，保证一致性。

时间戳共识：

UTXO 和 DPoS 结合的一大难点在于时间戳，DPoS 共识基于时间，会严格检查区块时间。全节点系统时间必须设置为和标准时间一样，否则共识一致性会出现问题。而 UTXO 本身也记录了时间戳的功能，但时间戳并不基于标准时间。在 LBTC 里将时间戳统一成标准时间协议，以保证区块的正常运行。当存在作恶节点或者时间不同步的区块时，出块被作为异常块处理，出块节点被作为异常节点处理。



数据快照和投票：

在比特币采用的 UTXO 模型中，并不支持查询地址余额的功能。在比特币中，可以通过全局遍历 UTXO 数据，实时计算地址余额。实时计算的工作量相当巨大，计算时间以小时为单位，现实中不具备可行性。但是比特币不采用 DPoS 共识，并不需要节点注册、投票等功能。

而在 LBTC 系统中，为了 DPoS 算法的需要，LBTC 中新增地址余额计算、节点注册、节点投票新功能。考虑到共识算法的高性能要求、注册节点数目的有限性，把地址余额、节点注册及投票信息保存在内存中，程序退出时，把数据回写磁盘。通过数据库和地址余额、投票信息来链接 UTXO 记账信息和 DPoS 共识机制：

• 注册、投票的信息由比特币底层协议负责传输。

• 把注册、投票信息保存在内存数据库中。

• DPoS 共识模块查看注册、投票信息，完成共识。

4 LBTC 链上治理

4.1 链上治理的内涵和外延

4.1.1 区块链：自我进化的类生命体

自中本聪于 2009 年提出的一份 9 页白皮书，并给出最初版本的代码实现后，比特币协议在近 10 年的时间中经过不断完善和更新，已经形成最高市值超过 3000 亿美元、消耗超过全球 1%电力资源的庞大网络协议。

值得注意的是，如果考虑到中本聪本人仅仅提供了初始协议版本的设计，那么比特币事实上是在完全缺乏单一领导以及中心化组织结构的状况下，带来足以对现实世界产生深刻变革的影响。

区块链项目被广泛接受为一种新型的社会实验形式，本质上是在实验去中心化的社会组织模式是否能够有效汇聚群体（社区）的智慧与力量，以及该组织模式是否能够在外界环境变化中表现强大的生命力与适应性。这意味着，区块链项目并不能仅仅被看作一种松散的社会组织结构，而是接近于具有生命活性、自适应与自我进化能力的类生命体。

在生命演化的历史长河中，单细胞原核生物在长期的偶发变异、自然选择的作用下，形成了极为丰富的物种分支，最终诞生了有脊椎动物这一高级多细胞生命形式。自然演化的奇迹充分说明：生命的原始设计固然重要，精确的设计能更高效率精准地解决问题，但从更

长远的视角来看，生命体具有的持续自我进化并适应环境变化的能力，才是生命得以持续繁荣的客观基础。自我进化适应环境的能力，实际上是一种对没有出现过的刺激的反馈能力，或者对更宽范围的变化作出调整的能力。这就需要摒弃固定的模式，用进化的思路来设计整个系统。

4.1.2 治理是区块链自我进化的制度基础

区块链协议的本质是网络协议、交易协议、共识协议的结合。

- 网络协议：发现与广播交易；
- 交易协议：定义有效的交易；
- 共识协议：定义并形成唯一的链。

共识协议是区块链协议的灵魂，因为共识协议清晰定义了看似松散的去中心化组织如何形成意见基础与权利义务基础。

区块链的治理（governance）是形成与维护共识协议的客观基础和制度保证；同时，治理也为参与各方达成共识提供了主观的意见路线。治理涉及的领域可能包括：

- 现有协议的更改；
- 追溯更改区块链的状态；
- 利益与补贴的分配；
- 以及其他任何利益相关事项。

由此可见，区块链治理的根本目的是保证共识协议的形成、维护和持续进化；因此我们可以认为，区块链治理从顶层设计上为区块链的自我进化提供了制度性基础。

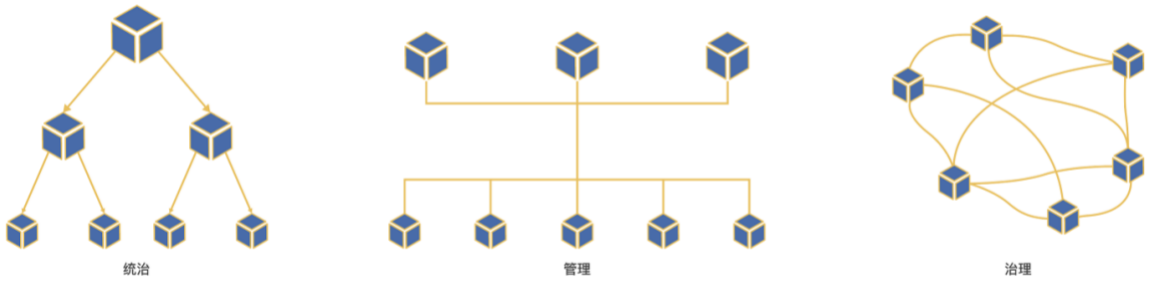
此外，区块链作为去中心化组织方式的伟大尝试，区块链的治理也很可能是人类文明史上最为先进的群体行为范式。群体性的系统可以将个体的进化性传递给整个系统。同时因为

区块链治理是一个多参与者的系统，因此天然具有很好的强健性，可以抵御不可预见的各种风险。

4.1.3 管理、统治与治理

理解区块链治理的内涵，应当辨析管理、统治与治理的概念，明确治理既不同于统治、亦不同于管理。

	管理	统治	治理
诉求差异：	管理者通过协调被管理者的活动，以便收到个人单独活动所不能达到的效果或经济收益。	组织内部上层运用自身权威，单方向对更下层成员进行管理。	在一定范围内引导、控制和规范组织内部的活动，以最大限度地增进组织内部所有公众利益。
运行方向差异：	管理方到被管理方单向	组织内自上而下单向执行	双向、互动
形成的客观基础与行为方式差异：	·强调获取更大的组织效用，即施加管理后的个人效用之和大于施加管理前的个人效用之和； ·主要内容为协调人的关系、激发个体活动的积极性；	·制定和实施政策以形成对组织内公共事务的单向管理；	·建立于市场原则、公共利益的合作； ·强调行为基于组织内的共同目标；



从管理、统治到治理，其背后是生产力对生产关系、经济基础对上层建筑的必然要求。如果我们可以认为区块链技术革新了生产关系，那么也必然伴随新型链上治理相对于传统治理方式的革新。

区块链是一种去中心化的技术模式，链上治理也是一种去中心化的治理模式。这种观念的根本逻辑在于，自由和权利是激发人创造力的源泉，也是维持秩序的力量。中心化的管理者虽然一定程度上可以帮助保护部分个体的权利，但是相对于中心化管理者对个体的权利和自由造成的损害和侵蚀，帮助显得很微弱。

链上治理同时也是一种自底向上的治理理念，没有预先设计的前进方向和运行模式，每个参与者在他们的位置上，按照自己的选择行动，整个系统就会朝着所有参与者的意愿向前。在这样的秩序中，理性的个体都按照自己利益最大化的方向行进。整个系统的决策不依照中心化管理者的喜好，而是出于最多数人的最大化利益的根本要求向前发展。公共话题因为牵扯到多数人而被多数人推进，只牵扯到少数人利益的事务变得不那么公众，用个体的自由和理性来推动系统的发展。

4.1.4 LBTC 定义的治理

1）治理活动的核心：角色

角色可能包括：用户、受托权利人、委托权利人、开发者等

2）治理的基本要素：激励（inventive）、协作机制（cooperation mechanics）：

- 激励：决定组织（社区）形成的结构基础与运行驱动力。
- 协作机制：决定组织（社区）运作的效率。

3）治理的具体表现领域：Consensus、Voter、Voting Area、协议升级与变动：

- Consensus：决定参与记账和出块的权利义务、决定 Block reward 利益的分配、是形成链上权责的客观基础。
- Voter：决定谁有权利参与与影响治理活动
- Voting Area：决定链上治理涉及的领域，哪些事务可以被投票决定
- 协议升级与变动：如何决定协议的升级与变动，以及协议如何进行更新

4.1.5 区块链治理的发展历程：从链下到链上

区块链治理的发展，总体上经历了从链下到链上的发展过程。伴随着治理链上化，区块链系统内部角色身份也产表现出一定的模糊化趋势。

下文将会结合 LBTC 提出的治理观，简述代表性项目在治理层面的概况和发展逻辑线。

1）比特币(Bitcoin)

比特币生态中的角色可以分为：矿工、用户、开发者。矿工得到所有经济激励（来自于 Block Reward 和交易手续费），并对协议的升级有投票权；开发者和用户没有直接经济激励。

这一激励制度的安排可以从理论上解释比特币历史上曾出现的社区矛盾的逻辑根源，并且揭示了另一部分显著性稍低的隐患。比特币的激励制度决定了以下现象会必然出现：1.矿工垄断经济利益和投票权利，会趋向于中心化；2.开发者没有直接经济激励，会趋向于保守化、小团体化，并且有被第三方营利组织过度干预的风险。3.矿工总体权利的绝对优势导致矿工和用户的分裂。

从激励（incentive）的角度，比特币协议的机制较为原始，但是对比特币来说却有一定的健壮性。比特币的定位已经从点对点支付网络转型为储值型资产，因此开发的保守化是可以接受、甚至是有利的；这是比特币独有的特征，并不适用于其他项目。

2）以太坊(Ethereum)

由于以太坊在目前阶段以 POW 为主，因此其激励机制与系统角色与比特币大同小异的。但以太坊在以下两点有其独特之处：1.以太坊有社区领导人（Vitalik Buterin），这导致以太坊社区的凝聚力和运行效率更高，但同时面临过度捆绑的风险；2.以太坊可能在未来全面转向 POS，将会一定程度缓解挖矿中心化和角色对立化的问题。

3）TEZOS

Tezos 是较早提出并尝试链上治理的项目。在协作方式（cooperation mechanics）上，比特币和以太坊都是链下治理：比特币开发者在线下沟通并提出 BIPs，以太坊在 GitHub 收集协议升级提案，两者都把治理过程转移到链下。而 Tezos 强调将治理过程程式化，通过链上投票的形式进行新开发者提案测试与主链融合的决策。

这一机制的本质是，把治理权力从开发者小团体和矿工手里剥离出来并分散到每个用户手中，同时又使得真正的开发者有经济激励去推进协议的更新，因此较难出现比特币开发者保守化的问题。

4.1.6 区块链治理的待解决问题

1）消极贡献问题：

此处所讨论的贡献积极性包括开发的积极性与投票的积极性。积极性与激励直接相关，尤其是经济激励与权力激励；在相应激励缺失的情况下，积极性问题是大概率出现、且非常难以解决。在历史上，某些积极性问题被行业爆发的整体环境带来的心理冲击所掩盖；而在区块链项目竞争加剧的未来，这一问题很可能大规模爆发。

贡献积极性是关乎区块链项目生死存亡的问题。例如比特币的开发者保守化问题，导致比特币社区旷日持久的大争论（有关扩容等）；EOS 的投票积极性问题导致 EOS 主网推迟上线。如何重构区块链的激励机制，平衡系统关键角色的权责义务，是区块链项目面对的至关重要的问题。

2）角色对立问题：

角色对立问题从某种意义上与消极贡献问题是同源的，皆可归因于激励（incentive）这一治理要素。

在区块链生态中，普通用户、开发者、矿工，甚至与更复杂的委托权益人、受托权益人等，其权利义务存在较强的不对等性。例如在常见生态中，开发者与普通用户往往都不享有直接经济激励，只能从 Token 价格的上升中获取收益，但是开发者承担的责任缺远远大于普通用户；理性的治理机制不可能指望开发者仅仅出于兴趣或责任来完成开发工作，因此开发者有可能选择淡出社区或成为普通用户。

以上例子是一个权责不对等的情形，往往不至于导致角色严重对立；若考虑到利益冲突的情形，就更易引发直接的对立。例如在常见的 POW 生态中，矿工有提高交易手续费率、提高 Token 价值的动机，而用户有降低交易手续费率、降低 Token 价值的动机（需注意：用

户不一定是持币人），两者将完全处于对立面。历史上多次出现 POW 矿工恶意打包空交易、引发网络堵塞的案例，印证了利益冲突引发角色对立的逻辑。

3）Token 流动性匹配问题

Token 流动性匹配问题是指在区块链生态体系中，Token 的分配、锁定、发行等影响流通量的环节出现了失衡，导致 Token 价值的不正常波动，以及利益相关方受损的情形。
Token 流动性匹配问题的本质是供需关系失衡。

例如增发量过大的 Token 系统，可能引起系统内通胀、减损早期用户积极性的问题；
Token 过度锁定与抵押的系统，可能引起价格失真、货币供给不足的问题。长期来看，经济模型设计以及供需关系调节机制存在瑕疵的 Token 系统，尤其是整体平衡性弱、政策极端的系统，极易被自身的设计所反噬。

4.2 LBTC 的链上治理体系

4.2.1 LBTC 治理思想：记账权与议事权的『两权分离』

作为基于 DPOS 的去中心化系统，LBTC 在主网以及协议的维护环节采用了权利代理（Delegate）的组织原则。权利代理，指自然意义上的权利人将自身权利通过一定形式的意思表达，委托或授权给代理人行使的过程；LBTC 所采用的 DPOS 即是一种主网的记账权利人通过投票将记账权委托给股东数量的 受托人的共识机制。

代理机制在当今或历史上曾出现的组织治理结构中并不罕见。事实上，代理机制扩张了组织中不同权利人角色的行为能力，形成更集中和高效的治理行为模式，例如辖区选民将投票权委托给议员、再由议员代表选民行使投票，决定事关选民利益的重要辖区政策。在一个区块链系统，可能也存在某种意义上的权利代理行为。

但是需要特别强调的是，区块链系统的权利代理行为，根据所代理权利的性质，可以总结为：

1）记账权的代理；

2）议事权的代理。

在区块链系统中，记账权与议事权可能同时存在，且在技术上两者表现出一定的独立性。例如在比特币系统中，记账权通过 POW 的开放竞争获得、而议事权以矿工投票方式完成决策。以比特币为代表的早期区块链项目，呈现较强的记账权与议事权重合的现象，而这一现象很可能导致系统治理权利的中心化与架空化，使得普通用户与社区成员难以获取相对应于其持有经济利益的权利。在治理机制较为完善的项目中，记账权与议事权（后简称两权）出现了一定的分离，提高了系统内角色参与治理活动的效率和可行性。

LBTC 首次提出了两权分离的治理理念。LBTC 团队认为：

1）在机能较为复杂的区块链系统中，适当程度的两权分离是有必要的。

2）应当在不同权利领域单独设计权利代理机制，实现适当程度的两权分离。

两权分离是区块链系统议事行为复杂化、角色多样化的必然要求。根本原因在于议事行为所需要的能力与资质，同记账行为所需要的能力与资质有非常巨大的差异：协议往往通过 Staking（抵押）、激励或反向激励约束并组织记账权利人的恶意行为；而在议事行为中社区必须充分考虑议事权利受托人的获得意见基础、治理意愿与治理能力，两者完全不在同一层次。如果简单地混同两权的表达，则必然导致议事行为（即治理行为）的无效化。

4.2.2 LBTC 治理思想：代议民主与直接民主的『混合治理』

卢梭在《社会契约论》中认为，理想的社会建立于人与人的契约关系、理想的政府治理建立于被统治者认可统治者的权力。因此，社会治理应当是完全由所有社会成员的公共意志所决定，且这些公共意志有利于全社会。

但是，卢梭并没有提出切实可行的方案，来构造理想社会治理的制度基础，它更多地停留在思辨的层面。直接民主是原始的、理想化的，其效率和公正性很大程度上受到制度设计者对实现民主的单元（Unit）的影响。例如，如果在极为原始的直接民主体系中奉行「一人一票」原则定义了个人作为实现民主的基本单元；采用 POS 的区块链系统定义了 Token 作为实现民主的基本单元。

历史经验表明，无论如何构造实现民主的单元的定义，直接民主也难以逾越其低效性的固有缺陷；治理的网络规模越大、这种低效性表现的越为明显。因此，对于天然需要良好拓展性（scalability）的区块链网络协议，直接民主可能成为对链上治理效能的掣肘。

代议制民主是近代发展完善的治理机制，体现了公正性与高效性的良好平衡。代议制要求系统成员（民众）让渡权力给有能力且能够代表其意愿的人，因此成员事实上通过间接的方式表达了对系统的最终控制权。在代议制民主下，选举自然成为分配系统权力结构的关键行为，这也是基于 DPOS 的区块链系统应当关注并谨慎设计选举机制的原因。

	直接民主	代议民主
民主的实质	治理是民众公共意志的体现。	民众将治理权利让渡给有能力且能够代表其意愿的人，实现间接控制。
实现民主的关键行为	对民主单元（Unit）的定义	选举与投票规则
特点	公平、简单直接、普适性强	高效率、分工结构合理

LBTC 作为同样基于 DPOS 的比特币协议，需要充分权衡代议民主的效率性与直接民主的公平性与普适性。LBTC 采用了结合理事会治理与社区治理的双层治理结构，并在治理层次

之间设计了精巧的沟通反馈机制，使得理事会与社区能够分别关注到各自应当关注且有能力进行决策的事务。在这一混合治理机制下，权力的配置以及传达体现得更为灵活和高效。

4.2.3 系统角色定义

• 用户：

分为 LBTC 用户、LBTC 上建生态用户。原则上，凡持有 LBTC 的用户，都可以通过 LBTC 行使社区治理权利。

• 受托权利人：

记账权的受托权利人是出块节点；议事权的受托权利人是理事。
LBTC 的节点与理事分别代表系统的记账权、议事权，是 LBTC 实现高效治理的核心。LBTC 的节点与理事通过不同的方式进行选举，两者没有必然身份联系。

• 委托权利人：

LBTC 社区是一个由 Token 控制并实施治理的系统；因此，LBTC 的委托权利人是所有 LBTC 持有者。LBTC 持有者是 LBTC 治理系统里面最基本、最广泛存在的参与者，也是 LBTC 治理的最终目的。持有者参与 LBTC 治理系统的方法很简单，但是当众多持有者参与治理的时候，他们的意愿会变成最终的行动指南。
持有者可以将他们的投票权代理给节点。持有者选择他们信任的、理念相同的节点，将自己的权限交由他们使用，大量持有者推选出的节点来执行用户的意志。持有者也可以选择喜欢的钱包、矿池直接托管自己的代币，获取自己的收益。持有者可以将自己的议事权代理给理事会，来参与到 LBTC 未来发展的共同规划中。

• **开发者：**

开发者是 LBTC 生态的基石；LBTC 将把对开发者的奖励纳入 LBTC 链上治理体系，直接提升到协议层面的高度。LBTC 系统就其形式来说是一个代码维持的程序，代码的质量决定了系统的性能，代码更新进度决定了它进化的速度。开发者是维护系统程序最重要的力量，程序的开发和维护因为特有的技术门槛，所以不需要也不可能由全员来共同完成。所以需要特定的开发者团队来完成开发和维护工作，并因此得到奖励——这样才能更好地激励开发者的工作效率。

• **链上 Oracle：**

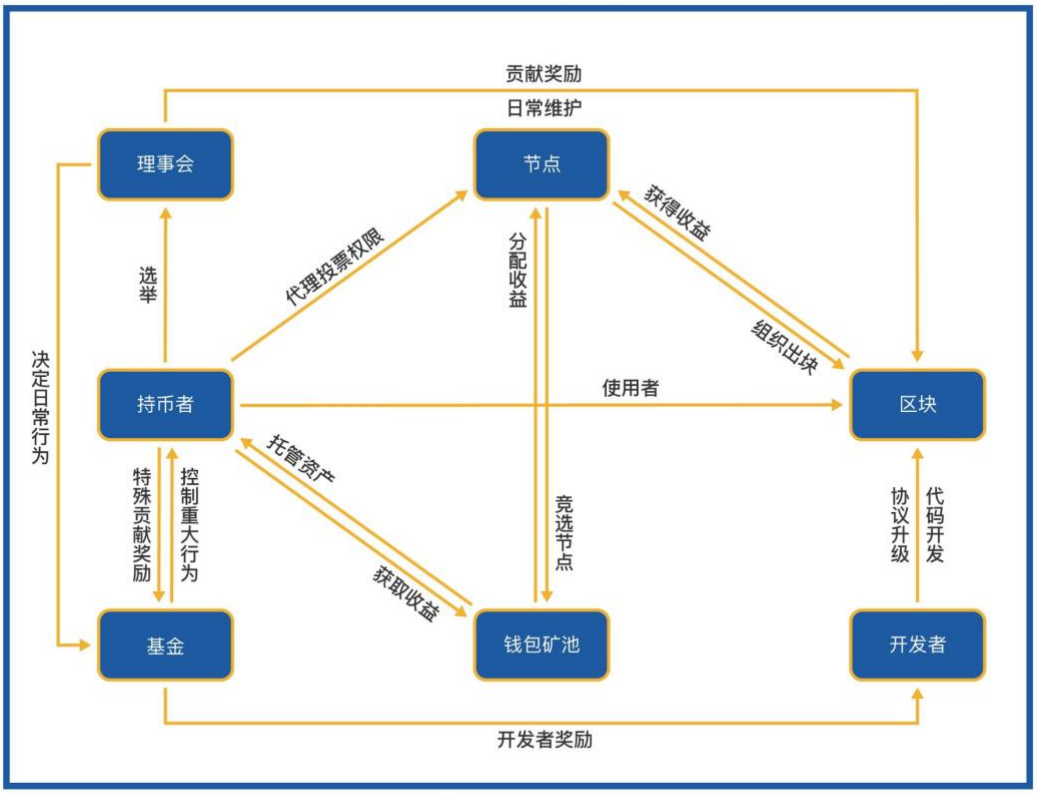
在 LBTC 生态系统中，链上 Oracle 将成为链上网关、去中心化交易所的重要角色。链上 Oracle 也属于 LBTC 用户，但不同于普通用户的是，链上 Oracle 会以服务提供方、资产承兑方等功能性角色的形式存在。

• **钱包和矿池：**

钱包和矿池是由社区或者其他第三方做的应用，方便用户托管和使用他们的代币。它们可以用用户的代币来竞选节点和获取收益，但这些权力本身是属于原本的用户的，钱包和矿池必须将这些权力再归还给用户，将获取的收益分给用户，按照用户的意愿进行投票。钱包和矿池帮助用户实现他们应有的投票权，仅此而已。

• **LBTC DAO 基金：**

基金是由 LBTC 社区领导者组建的，由理事会代为管理的，用以维护 LBTC 系统发展的组织。



4.2.4 节点要求以及选举规则

节点是 LBTC 治理系统里最重要的一个环节，是直接参与 LBTC 治理的代理者。节点的主要任务是负责产生、确认、记录区块信息，忠诚的节点会得到区块奖励，而作恶的节点会失去奖励。但是想要成为节点，不仅需要有足够性能的设备支持一个节点服务，保证产生区块的准确率，同时还需要获得广大代币持有者的支持。

节点由用户选举产生，代表着选举他们的用户。节点在参与 LBTC 链上治理的时候可以投出重要的一票，但是如果违背了多数用户的意见，节点就会逐渐失去他的选票，并最终失去成为节点的资格。

每个节点可以在自己的主页展示自己的技术、团队、理念等信息，吸引代币持有者的投票。作为最普遍存在的代币持有者，他们有权选出心中合格的，符合自己诉求的节点，然后给他们投票。每个代币持有者可以给信任的节点投票，最多可以选择 51 个节点，每一个节

点都会获得这个代币持有者所有的投票。每个周期系统会自动统计选票数，选出获得投票数前 101 的节点候选人成为节点。

4.2.5 LBTC 理事会(LBTC Council)细则

1.理事与理事会的定义

LBTC 理事会（简称理事会）是 LBTC 社区执行议事职能的专设机构。理事会负责主网协议参数维护更新与日常社区事务管理。
LBTC 理事（简称理事）是代表 LBTC 社区行使议事权职能并处理事务的人员，同时也是 LBTC 协议以程式化形式法定的链上职能角色。

2.两权分原则

理事会与 DPOS 记账节点独立，不对记账以及记账节点的选举行为负责。

3.理事资质

任何 LBTC 地址持有人可以成为节点。
理事需要通过 KYC 认证，为有完全行为能力的自然人或组织团体。
LBTC 理事会初期设立 5 个理事名额；随着社区规模扩大，可以适当增加理事会规模，但不得低于 5 人。因为理事会特殊的重要程度和贡献度，理事会不仅需要有足够的技术水准，还需要有有一定的社区支持，了解社区的现状与民意。所以理事会的 5 名成员中暂定的 3 名由 LBTC 开发者社区推选出来，两名由社区内部竞选选举出。理事要求至少持有 20,000 个 LBTC，理事也可以同时兼任节点。

4.选举方式

理事通过链上理事选举决定。该选举活动是一项独立的、不同于 DPOS 节点选举活动的行为，于每季度举行一次。

任何 LBTC 持有人都可以在钱包内委托选票给理事候选人。选举结束后，根据委托选票的数量决定前 5 名候选人正式成为理事。

在选举前，理事候选人应当正式在社区平台公开自身信息、治理计划等，已获得社区的公开支持。

5.理事的职能与权力

1）决定 LBTC 主网的可变参数；
2）审核并讨论社区意见提案与开发者提案；
3）讨论涉及主网协议更新的事项；
4）讨论并组织社区事务；
5）讨论并决定当期 DAO 基金会划拨款项以及其他公共资金的安排；
6）讨论 LBTC 治理体系涉及的规则条款的变更。

6.经济激励

LBTC 将在基金会中划拨特定数量的款项到理事会激励基金，作为对理事的经济补偿。

（开发者奖励机制，推广运营活动奖励）

7.理事会决策机制

理事会的决策以理事会决议为单位进行组织管理。

针对理事会讨论的问题，经全体理事投票表决后，通过的事项正式被认定为理事会决议，并以《LBTC 理事会决议第*号》并附以决议时间为标题对社区公开展示。

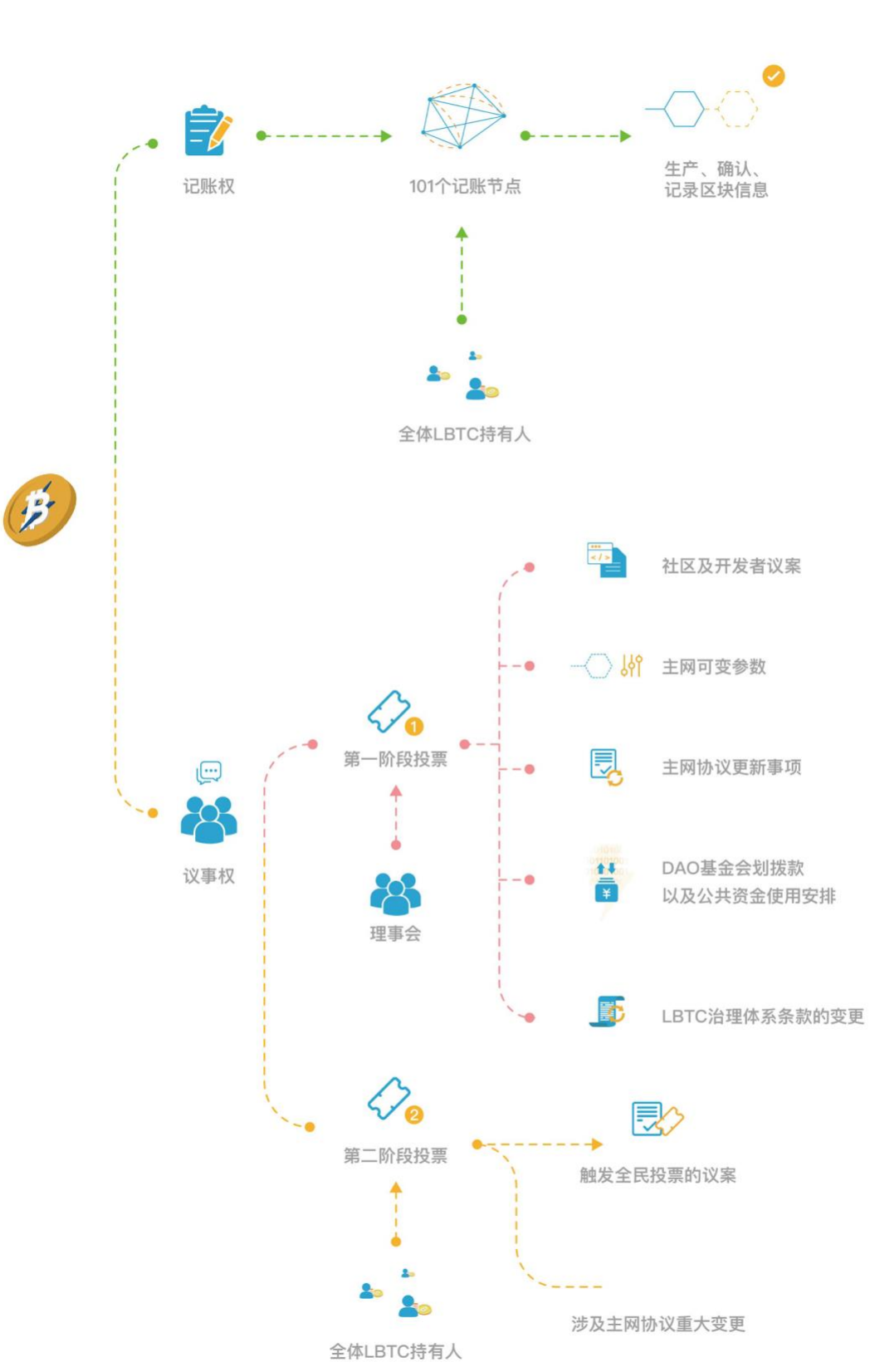
理事会决议通过后，原则上在公示三天后生效，除非该决议触发了社区全员投票。

理事会的内部决议投票，按照理事被委托的 LBTC 数量决定投票权重；但是单个理事的权重不得超过 40%且不得低于 10%。

8.社区全员投票机制

所谓社区全员投票，是指针对某项理事会决议，要求社区全体成员以 LBTC 进行投票，并根据投票结果进行最终的民主式决议。

社区全员投票是特定情况触发的，而非法定发生。理事会决议对社区公开后，社区成员可以在 LBTC 钱包或项目主页中对决议进行反馈投票（即可以以自身 LBTC 投票，表达反对）；如果某项决议获得 LBTC 流通总量 1/5 以上选票反对，就自动触发社区全员投票。社区全员投票需经参与投票的 LBTC 数量 67%以上支持方可通过；对于触发了社区全员投票且没有得到通过的理事会决议，当即自动失效。


记账权
101个记账节点
生产、确认、
记录区块信息
全体LBTC持有人
议事权
第一阶段投票
理事会
社区及开发者议案
主网可变参数
主网协议更新事项
DAO基金会划拨款
以及公共资金使用安排
LBTC治理体系条款的变更
第二阶段投票
触发全民投票的议案
涉及主网协议重大变更
全体LBTC持有人

4.2.6 LBTC DAO基金

基金是由LBTC社区领导者组建的，由理事会代为管理的，用以维护LBTC系统发展的组织。由于整个LBTC的发展更像是一种公共事业，系统升级能惠及每一个参与者，然而每个个体都不愿意为此付费——如果其他使用者可以免费地搭便车的话。这样就需要一个组织，他们向所有参与者收取费用（并不是直接收取，而是从其他的代币中收取部分比例），用来支持系统的升级维护。基金的角色在整个治理中是极为重要的，但并不是统治性的，基金会同样只是用户权利的代行者，帮助整个系统维持进化。

我们将从长期无人确权的LBTC池中拿出一部分，分批释放给基金会。基金会负责奖励对LBTC生态系统做出贡献的人，增加所有系统参与者的贡献动力，使得整个生态系统形成一个闭环。基金会属于整个LBTC社区，日常任务由LBTC理事会代为管理，重大事项则由所有参与者共同决定。基金会将负责下列具体事由的奖励发放：

- 理事会奖励：为理事会作出的日常管理工作给予的奖励
- 开发者奖励：奖励开发者做出的代码升级或者新协议的开发
- 社区贡献：奖励社区成员给出的议案、资源或者其他贡献
- 其它奖励

每一次释放到基金会之前，会由基金会预先提起议案，确定释放代币的数量和时间，并由理事会投票，获得赞同后推行方案。

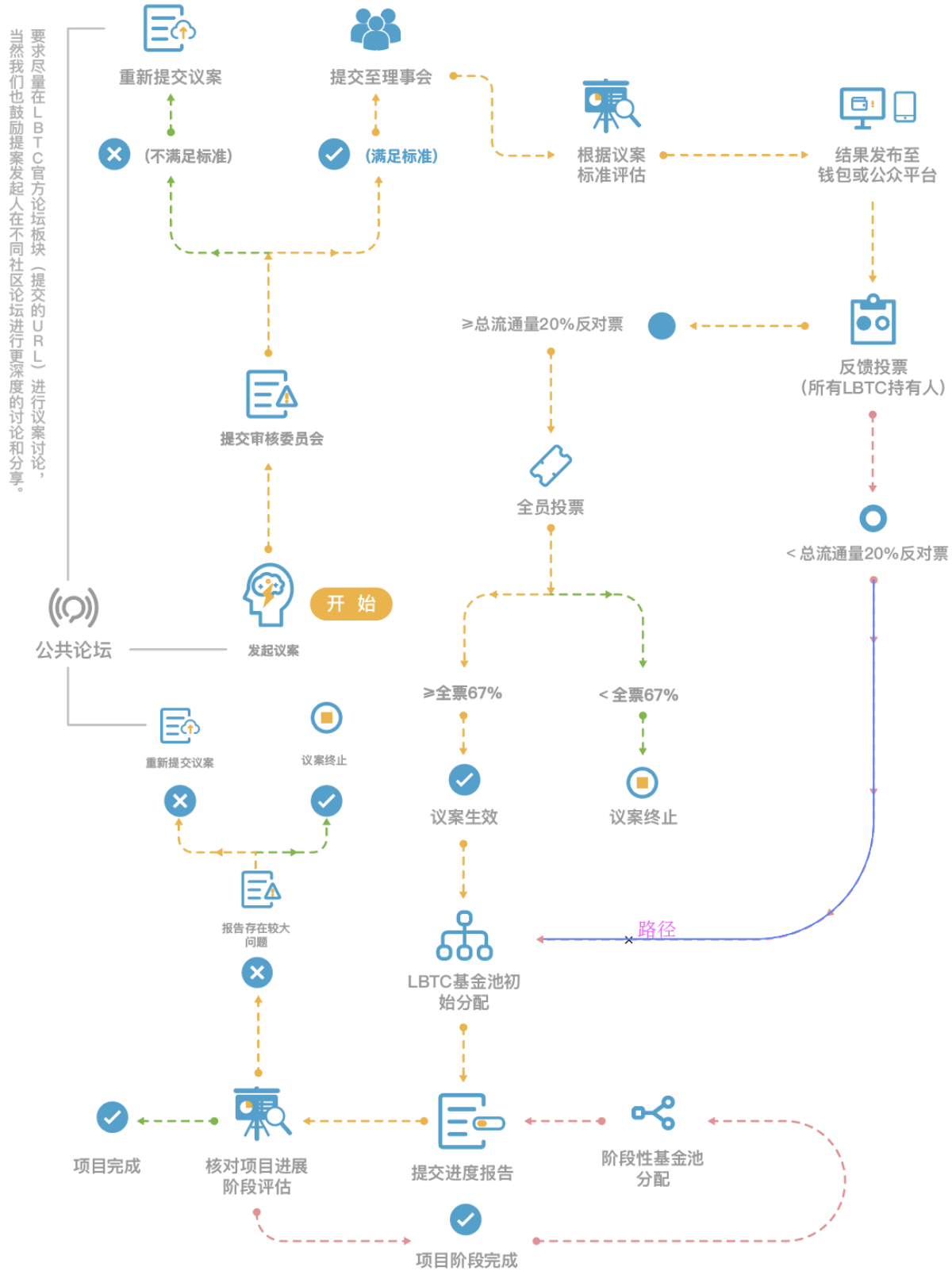
4.2.7 LBTC协议的自我进化

LBTC协议是一个自我进化的协议，在现行版本的基础上，由所有参与者共同决策共同推行升级。社区的成员可以将想法提交给理事会，可以是管理体系的改动，可以是未来发展路线，甚至是一个简单的建议。只要提出想法，理事会将考虑是否为好的建议，是否值得升级，然后在将建议反馈给开发者社区。

开发者社区根据理事会建议形成代码升级标准化的闪电比特币改进建议（Lightning Bitcoin improvement proposals，LBIP），想法也可以直接来自于开发者社区，形成的 LBIP 再由理事会评估。

理事会如果认可这个 LBIP，会直接推行协议升级，并在官网、钱包中公布这次改动的代码、细节和影响。所有代币持有者可以发表自己的看法，或者发表反对意见。当反对意见超过设定阈值的时候，会开启一次全民公投。如果升级的 LBIP 是极为重要的、底层的、革命性的，那么会跳过预先推行的步骤，直接开启全民公投。

SGS 链上治理系统：


要求尽量在LBTC官方论坛板块（提交的URL）进行议案讨论，
当然我们也鼓励提案发起人在不同社区论坛进行更深度的讨论和分享。
重新提交议案
提交至理事会
（不满足标准）
（满足标准）
根据议案
标准评估
结果发布至
钱包或公众平台
≥总流通量20%反对票
反馈投票
（所有LBTC持有人）
提交审核委员会
全员投票
< 总流通量20%反对票
开 始
公共论坛
发起议案
≥全票67%
< 全票67%
重新提交议案
议案终止
议案生效
议案终止
报告存在较大
问题
路径
LBTC基金池初
始分配
项目完成
核对项目进展
阶段评估
提交进度报告
阶段性基金池
分配
项目阶段完成

5 LBTC 去中心化交易平台

5.1 DEX 与代币化的未来

5.1.1 DEX 是交易所的未来

DEX，即 Decentralized Exchange（去中心化交易所），指在区块链上通过智能合约或内置功能控制的 token 交易所。与 DEX 相对应的是中心化模型管理、公司制运营的交易所。DEX 将会成为未来交易所生态的重要组成形式，与传统中心化交易所形成明确的分工。DEX 的不可替代性在于：

1）在 DEX 中用户可以完全控制链上资产，不存在用户对传统中心化交易所的信任风险问题。DEX 不会出现交易所非法冻结、挪用、卷跑用户资金的行为。

2）DEX 不需要 KYC 以及 AML 流程，用户不会暴露额外信息给交易所；中心化交易所占有大量用户信息，并且有可能非法使用这些信息。

3）DEX 可以伴随主链的存在而永久保持运行，不会出现因交易所人为因素回滚、宕机或关闭的问题。

4）DEX 完全依赖链上行为，因此天然是全球性且不受限的，链上资产的流动具有很强的自由度。

但是我们清晰地认识到，目前 DEX 存在一些对大规模应用形成阻碍的问题：

1）DEX 的性能受限于主链性能，交易确认较慢，不适合高频操作以及需要快速反馈的操作。

2）市场上绝大多数 DEX 没有清晰明确的产品定位，与中心化交易所形成重复竞争、而非错位竞争。DEX 不应否认中心化交易所的固有优势进行盲目的竞争。

3）在交易大类别资产、标准化程度较高的资产，如 BTC、ETH、ERC 20 Token，DEX 并不具有太多优势。中心化交易所可以提供很优秀的深度与交易体验，以及灵活多样化的衍生交易品种，DEX 在这方面是弱项。

5.1.2 代币化运动的必然性

在过去的数年间，数字加密资产更多表现为纯粹的链上资产，即基于区块链的原生 Token、以及基于 Token 衍生的 Token。但在可预见的未来，数字加密资产会体现更大的泛用性和普及性，并且与真实世界的资产和信用体系相连接，更由此催生数字加密资产的发行、交易、托管、承兑以及其他周边需求。

我们可以预见，Tokenization（代币化）是区块链技术走向大规模应用的重要路径；一个与真实世界保持完全的隔离的链上世界难以称为支持广泛 Tokenization 的基础设施。更值得注意的一点是，Tokenization 可以被进一步解释为 Asset Tokenization（资产代币化）以及 Security Tokenization（证券代币化），尽管外界普遍认为证券代币化是广义的代币化的本质：例如将股权、债权、非标准收益权以及衍生证券进行代币化，以代币的形式在链上确权并流转。这一理解却并未脱离传统金融的范畴；我们认为，代币化运动可能引发更为全面的资产代币化，而非狭义地框定在传统证券的范畴。

因此我们需要进一步解释资产与证券的差异，并说明为何 LBTC 希望通过打造去中心化交易平台以及引入链上 Oracle 来支持未来将会发生的全面的资产代币化。按照定义，证券是经济权利凭证，是财产权利凭证、流通权利凭证、收益权利凭证的集合体；而资产是一种广义的资源，并且该资源可以在未来带来某种不仅限于经济利益的权益或权利。区块链将会引发的革命，绝不可能局限于将传统证券的形式由链下账簿转移到链上账簿这一记账载体的转变，而是创造多种新型的、非传统和非标准的资产类型。技术上，借助于区块链

的记账体系以及引入链上 Oracle，我们可以建立一个承载任何形式资产的发行、流通、托管与承兑平台，这些资产可以指代任意形式的权利，其含义远比金融证券更为庞大。

5.1.3 非标准非传统资产

非传统资产，是指在传统世界中尚未或者无法被证券化的资产、甚至是未能被归属于资产定义的权益或权利。非标准资产，是指可能在任意环节被个性化、差异化定制的资产，它可以包括但不限于在底层权益、发行方式、权利责任关系、承载形式等方面有别于传统资产特点的创新性资产。LBTC 去中心化交易所生态将会非常重视非标准、非传统资产（双非资产）这一类有巨大市场需求、但是尚未得到大规模发展的链上新资产类型。

由此，LBTC 去中心化交易所将重新定义双非资产代币化的内涵。此类资产的代币化可以覆盖最近已经出现或仍处于萌芽期的资产类型，例如：

- STO（证券化代币发行）；
- FOF（Fund-of-Funds）；
- 小规模募集的 crypto 二级市场基金；
- 矿池份额；
- 特定权益份额二次分发；
- 发行可承兑的 IOU；

例如，一个社区的意见领袖（KOL）想向社区成员推荐并预售自己看好的项目，即使这个项目还未上线、还未发行正式进行代币发售，社区领袖一样可以在 LBTC 上发行这份数字资产、向社区成员发售，并且可以允许成员之间自由交易；在代币发行之后，所有持有这一份数字资产的人可以经由资产发行人兑换代币。

需要注意的是在此例中，代币发行人实际上是作为网关（gateway）或链上 Oracle，以自身信用或抵押品为基础发售了代币。这种模式是 LBTC 认为未来将大有可为的链上新经济模式。网关的本质是一种提供中介服务的链上 Oracle，它在技术意义上是去中心化的，

但在经济意义上是信用化的。在纯粹的去中心化经济体系下，真实世界资产与链上资产是隔离的，这是原子世界与数字世界逻辑上自然隔离的结果；而 LBTC 一贯于明确自身称为连接原子世界与数字世界中介的作用，将会服务于真实世界资产的链上化运动，培养适合链上 Oracle 生长的土壤。

当然，用户也可以在 LBTC 支持的 DEX 发行自定义非标化产品，比如一份比特币价格的保险、一份量化基金的份额、一份矿池的算力。任何人都可以交易这种权益，并最终在发行者处获得兑付。甚至传统意义上的证券也可以经由链上 Oracle 的发售与承兑、以数字资产的形式在 DEX 中交易。理论上，只要是可定义、可量化、可分割的权益，都可以实现个性化定制，并在 LBTC 支持的 DEX 中流通交易。

5.2 LBTC 上建 DEX 与 Oracle 生态

5.2.1 LBTC 对 DEX 的天然适配性

LBTC 是去中心化的全球价值互联网传输协议，而在庞大的数字加密资产世界中点对点支付功能能够覆盖的使用场景非常受限。因此对去中心化价值的传输以及数字资产的交易功能的支持是 LBTC 使用者的必然需求。LBTC 天然适合 DEX、适合链上 Oracle 以及双非资产平台生态的构建与生长。

LBTC 使用了基于 UTXO 的 DPOS 共识机制，具备出块时间短、网络吞吐量大、网络运行稳定强健的特性，天然适合去中心化的数字资产交易活动。LBTC 本身是已经成熟运行的点对点支付网络，DPOS 的机制使得交易确认时间控制在 3s 左右，甚至足以满足企业级应用的性能要求。此外，LBTC 上建 DEX 可以采用模块化技术架构，对外开放功能组件与 API，对第三方交易平台与链上 Oracle 赋予很高的终端灵活度。

众所周知，数字资产和现实资产的流通问题一直是一个棘手的问题，随着各国的监管日趋严格，公开合规地承接法币通道变得越来越困难，而 LBTC 上建 DEX 刚好可以解决这一问题。DEX 可以将法币通道问题同样进行去中心化处理，任何在平台上参与网络的人都可以成为网关，承接法币和数字资产的兑换，也可以发行代表各国法币的数字资产来流通。网

关无需拿到法币通道的许可牌照就可以运行交易所，亦无须考虑未来政策变化的风险。在目前主流市场的监管体系下，承兑商做为网关提供交易和兑换服务，无论承兑商本身还是对手方都是合规的。因此 LBTC 使得现实世界与虚拟世界简单而又合法地连接在一起。
在 LBTC 上发行自定义的数字资产，用户不需要考虑任何技术上的问题，包括服务器的搭建、技术团队的组建、代码的编写维护与升级；LBTC 上建 DEX 可以提供所有必需的技术解决方案。只需要打开 LBTC 客户端或网页，按照自己的需求来定制代币的参数（以后甚至可以尝试不设定代币的总额，建立一个通胀或者通缩的代币经济体系）。用户可以按照规则将这些资产证明的代币分发给客户，并允许他们在 LBTC 上自由交易。整个过程并不需要资产发行者亲自参与任何技术环节。

5.2.2 LBTC 上建 DEX 服务概览

LBTC 上建 DEX 平台重点定位于服务新型链上 Oracle 或传统意义上的网关（gateway），发行、托管、流转并承兑各类数字资产，尤其将重点支持非标准非传统数字资产大类。非标准非传统数字资产是在区块链技术出现以前难以被大规模确权、托管和流转的资产类别；去中心化基础设施与链上 Oracle 的结合则提供了充分解放生产力，帮助双非资产走向大规模应用。这将是区块链革命最具潜力和颠覆性的创新产品。

LBTC 上建 DEX 平台为各类角色（资产发行方、承兑商、担保人、交易者、自建交易所等）提供完整的、可定制的技术解决方案，便捷地实现数字资产的自定义、发行、托管、流转与承兑活动。用户可以以多种角色或身份参与 LBTC DEX 平台。

LBTC DEX 生态定义了丰富的平台角色，实现差异化定制化需求：

• 资产发行方：

资产发行方可以自定义资产类型与参数，发售属于自己的 Token。例如：1）某社区 KOL 发行投资项目的预售额度，并将该额度包装为 Token 发行在 DEX 中，社区 KOL 自带流量可

以直接为 DEX 带来用户；2）某矿池可以发行矿池份额，将发售 token 定义为矿池的 shares，并负责承兑该 token。非矿池用户无需经矿池的注册或认证亦可在 DEX 中购买 shares。

·承兑商：

承兑商通过向市场认可自身的承兑义务，提供承兑服务；一般来说，承兑商也可以是自定义资产的发行方。例如，某承兑商在 DEX 中发行锚定 BTC 的稳定 token，并承担该 token 兑换 BTC 的责任。

·担保人：

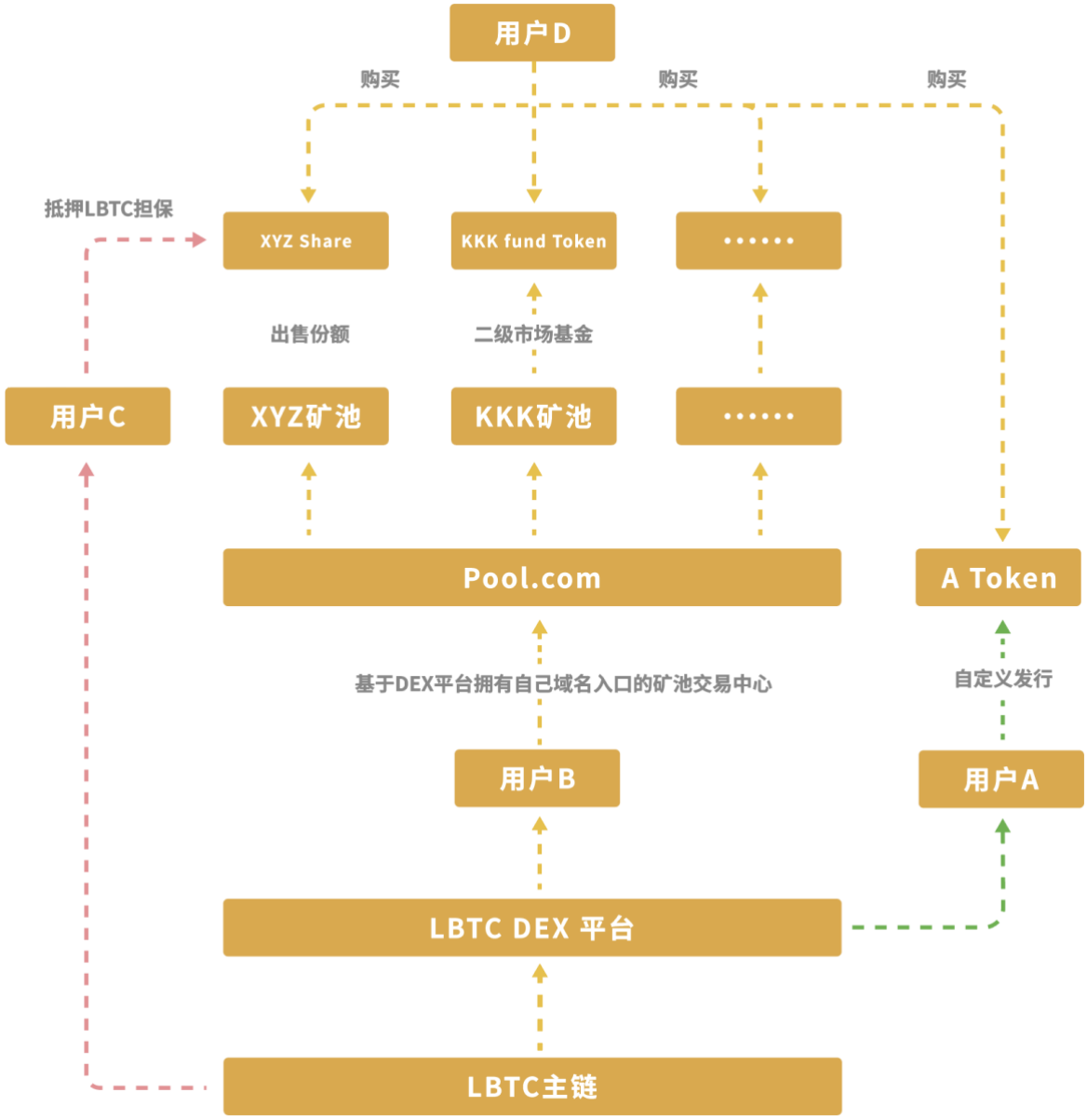
DEX 允许对自定义发售的资产进行担保，担保物可以是 LBTC 或其他 DEX 注册的数字资产。

·交易者：

指从事简单交易活动的参与方。由于 LBTC 建立于 DPOS 共识机制，因此提供极低的交易手续费水平，以提供支持高频次大深度的交易模式。

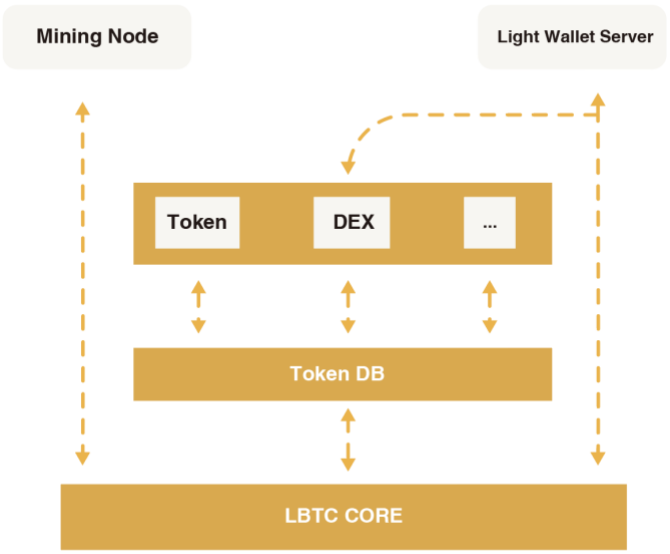
·自建交易所：

用户可以以自有名义（包括提供自有域名以及交易所 UI 界面等）基于 LBTC DEX 技术架构建立去中心化的个性交易所。例如，某矿池资深运营商可以建立具有独立域名的矿池份额交易平台，并自定义上线资产的发行与审核标准，甚至可以在 LBTC DEX 上基于此项现金流资产发售代表交易所 shares 的 token。


用户D
购买
购买
购买
抵押LBTC担保
XYZ Share
KKK fund Token
••••••
出售份额
二级市场基金
用户C
XYZ矿池
KKK矿池
••••••
Pool.com
A Token
基于DEX平台拥有自己域名入口的矿池交易中心
自定义发行
用户B
用户A
LBTC DEX 平台
LBTC主链

5.3 技术实现

5.3.1 系统架构总览



整个 LBTC 上建 DEX 架构可以被解析为四个层次。

• LBTC Core（LBTC 主链协议层）：

主链负责 DEX 链上交易的验证、打包出块以及形成共识的过程；同时，主链也作为 DEX 所交易的资产的承载介质。交易数据上链确保了 DEX 交易的去中心化特性，比传统中心化交易所更安全、透明、可靠。

• Token DB（Token 数据库）：

Token DB 是抽象出的存储介质。Token 是有别于 LBTC 主链上原生资产（即 LBTC）、可被用户自定义的链上资产。Token DB 是一个独立的链上存储系统，负责组织管理用户 Token 余额以及全局状态信息。

• 应用模块层（Token 模块、DEX 模块等）：

该层包含不同功能的 AppModule，如 Token 发行与转账、Token 交易等。AppModule 建立在 Token DB 上层，可以发起交易直接操作 Token DB、控制用户余额信息。

• 其他辅助性角色：

包括挖矿节点、轻钱包服务器等。这些辅助性角色可以参与 DEX 的运行过程，但不是直接相关的角色。例如，全节点钱包可以自行选择是否支持 DEX 模块。如果一个全节点钱包支持接入 DEX，则用户可以在钱包中直接调用 Token 的发行以及交易功能，此时钱包可以被认为是一个 DEX 客户端。

5.3.2 Token DB

• Token DB 是从架构中抽象出的存储介质。Token DB 用以保存 Token 定义信息、用户 Token 余额、地址和 ID 的 Mapping 信息。

• Token DB 是一个内存数据库，具有高效性。App 会在启动时从磁盘加载数据，并在退出时写回数据到磁盘以持久化数据。

• Token DB 是一个 KV 数据库，具有易用性，对用户和开发者友好。

• Token DB 实现了基于内存的回滚操作，可在极端情况下进行状态回滚，保护用户资产与交易记录。在状态回滚中，对应的 AppModule 仅处理业务逻辑，与状态相分离，简易高效。以下代码简单解释了基于内存进行状态回滚的逻辑片段：

```
OP(blockheight, key, value)
        Undo(key) = Balance(key)
        Undos(blockheight).push_back(Undo(key))
        Balance(key) = value

Rollback(blockheight)
         For item : Undos(blockheight)
                Balance(key) = Undo(key)
                Delete Undos(blockheight)

Commit(blockheight)
        Delete Undos(blockheight)
```

5.3.3 Token 模块

• Token 模块是一个应用类模块，基于 AppModule 形式加载在 DEX 架构上层，该 AppModule 可以保持更新。

• Token 模块赋予用户创建 Token、定义 Token 参数、发行、转账、锁定或解锁 Token 的功能。

Token 转账实现逻辑如下：

```
TransferToken(blockheight, data, fee)
        CheckFee(fee)
        (fromAddress, dstAddress, tokenId, amount) = Analysis(data)
        CheckBalance(fromAddress, tokenId, amount)
        fromAddressId = GetAddressID(fromAddress)
        dstAddressId = GetAddressID(dstAddress)
        OP(blockheight, fromAddressId ,Balance(key) - amount)
        OP(blockheight, dstAddressId ,Balance(key) + amount)
```

5.3.4 DEX 模块概览

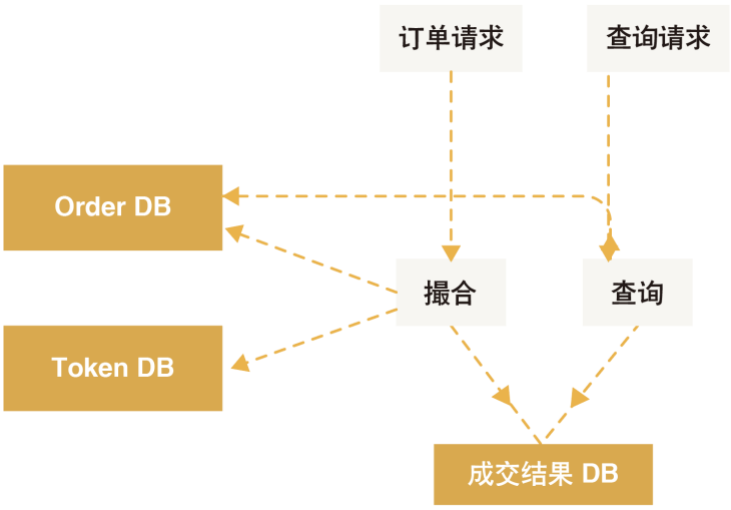
• DEX 模块也是一个应用类模块，基于 AppModule 形式加载在 DEX 架构上层，该 AppModule 可以保持更新。DEX 模块需要依赖于 Token 模块，并适配相应的 Token 标准。

• DEX 模块在调用 TokenTransfer 等基本功能的基础上，实现了一个共享深度订单池、Skylark 撮合引擎以及可定制 UI 界面的功能组合。

• 理论上，任何 LBTC 用户都可以基于 DEX 模块这一 AppModule，建立属于自己的 DEX。用户可以定义 DEX 的手续费水平、交易的 Token 品类、用户界面以及 Web 入口。这一功能将会极大地促进基于 LBTC 上建 DEX 生态的外部拓展。

• 所有基于 LBTC 的 DEX 都可以共享订单池，进而共享订单池提供的交易深度。订单池可以对不同 DEX 的订单实现无差别对待，以及快速精确的订单接入。同时，DEX 也可以保留使用独立订单深度的权利。

5.3.5 DEX 技术架构



• OrderDB：用于保存用户未成交的买单/卖单信息。

• TransactionDB：成交单数据库，用于保存用户已成交的买单/卖单信息，即用户在 DEX 的交易历史记录。

• TokenDB：用于保存用户 token 余额信息，表现为一个维护 Virtual Account-Token Balance 的 Mapping 关系。

• OrderHistroyDB：用于保存买卖交易的历史记录。

• 撮合：接受到用户新的买卖单，查询 OrderDB 中是否有价格匹配的订单，如果有则成交，并在 TokenDB 更新成交相关用户的余额信息、把成交结果相关信息保存在 OrderHistroyDB 中。

• 查询：负责查询当前的订单队列以及成交历史记录。

另需要提及的是，OrderDB 以及 TokenDB 都属于基于内存实现的数据库，而

OrderHistroyDB 由于数据量较大保存在磁盘中。由于 LBTC 上建的 DEX 是一个链上数据系统，结合 LBTC 出块时间特性，OrderHistoryDB 将在每一个 Block 产生时完成批量写入。

5.3.6 DEX 性能问题

DEX 作为一个面向用户的链上应用类产品，用户必然十分关心 DEX 系统的性能，因为系统的性能基础直接影响到用户的主观使用体验、以及客观上帮助平滑达成交易的能力。LBTC 上建 DEX 已经从不同角度分别考虑了系统性能问题以及对应的性能提升解决方案。

①考虑 DEX 性能与 LBTC 主链性能的关系：

本质上 DEX 是基于区块链这一数据库形式实现的应用，DEX 的性能直接受到区块链数据吞吐能力以及事件处理速度的影响。事实上，DEX 处理交易能力的瓶颈在于其基于的区块链数据库的数据吞吐能力，因此具备高 TPS 的底层区块链将有助于 DEX 订单行为以及其他交易行为的处理。LBTC 使用基于 UTXO 的 DPOS 共识机制、平均 3 秒出块，给 DEX 提供了极好的底层技术性能保证；在这一点上，LBTC 上建 DEX 更优于以太坊上建的 DEX，将为用户提供更强大的交易性能以及平滑的使用体验。

②DEX 的撮合性能：

• LBTC 使用自行研制和优化的 Skylark 交易撮合引擎。

• Skylark 交易撮合引擎主要基于一系列内存数据库操作，具备远优于磁盘数据库的 I/O 性能，且该 I/O 性能也远优于 LBTC 区块链的 TPS 瓶颈。

• Skylark 交易撮合引擎不处理用户的签名验证等具有计算复杂性的操作，主要以在内存数据库中查询订单为资源消耗项主体，其查找订单实现~log(n)的复杂度，因此可以实现极高的撮合效率。相比之下，基于以太坊的 DEX 只能退而求其次，采取链下的服务器撮合

方式，才能在撮合能力的数量级别抗衡 Skylark 交易撮合引擎。

③DEX 的查询性能：

DEX 查询分为订单（Order）查询和历史（Order History）成交查询；

订单查询通过 OrderDB 这一内存数据库实现，速度较快；

历史成交查询通过 OrderHistoryDB 实现，由于该数据库运行并非基于内存，且考虑到查询逻辑比较复杂，速度明显劣于订单查询。

需要考虑到，在现实使用场景中，用户可能发起查询操作的数量很可能不低于、甚至在数量级上也可能高于进行具体订单的操作行为（例如下单、撤单），因此我们必须解决非基于内存数据库查询的效率问题。如果 Skylark 仅按照标准的处理逻辑实现以上查询任务，有可能导致 LBTC 上建 DEX 针对查询行为的处理能力尚不能突破 LBTC 本身处理链上数据的 TPS 瓶颈，这样将会导致 DEX 无法利用 LBTC 主链的性能优势，削弱 LBTC 上建 DEX 这一生态的优势。

基于以上理由，DEX 技术开发团队考虑了以下潜在解决方案：

方案一：拓展为分布式查询

分布式查询的实现基础是存在大规模、大力度支持 DEX 运行的节点。当用户发起查询操作的数量达到一定阈值时，系统将分派查询任务并请求不同的节点。这意味着节点可以分布式地处理 DEX 中的查询任务（查询操作本身不改变链上状态，因此分布式的实现方式完全是可行且可被信任的）。

这一方案的困难在于，需要有大规模、大力度支持 DEX 运行的节点存在，否则技术上不可能实现分布式查询。成熟的技术解决方案决不可能仅仅单纯地基于理论上可行的构想去解决现实性能问题，因此我们必须考虑这一条件（节点对 DEX 运行的大力支持）不具备的情况下可行的解决方案。

方案二：剥离查询服务器或建立查询服务器群

我们已经在前文论述过，由于 DEX 中的查询操作本身不改变链上状态，因此查询行为的实现完全可以针对性能考虑实现方式上的变通。除了考虑分布式查询以外，我们还可以将查询服务器这一功能模块单独剥离，通过实体中心化的服务器来完成，甚至成立单独的服务器集群来提供高并发用户查询支持。

这一方案好比我们使用 etherscan 去查询以太坊的链上数据和状态。虽然 etherscan.io 本身是由中心化服务器运行的网页，但这并不妨碍以太坊本身的去中心化特性，这正是由于 etherscan 提供的是查询性质的服务，而查询操作不改写区块链的链上状态。LBTC 上建 DEX 可以根据用户实际需求，同时支持以上所讨论的两种优化方案。

④DEX 的数据吞吐量问题：

前文已经提及，DEX 的订单信息的构建通过一系列基于内存操作的数据库实现，而内存资源在特定时间内往往是有限的、无法随意拓展。

我们可以计算出，单一订单消耗的内存，进而计算处理订单信息的数据吞吐能力上限：

MaxOrderNumber = MaxMemory / MemoryPerOrder

这意味着我们会对运行 DEX 的节点提出硬件层面上的要求，并根据现实内存的大小，确定当下系统可支持的最大订单数量，实现一个灵活的订单的动态限额管理机制（Dynamic Order System Management），可见下文描述。

当订单处理需求达到系统上限时，分以下情况讨论：

第一、当订单总数量大于系统设置最大订单数时，则撤消固定数量（或固定比例）的不合理订单。不合理订单，定义为在一个交易对中，离可能成交的价格较远的交易，可通过一个动态参数调整。

第二、当交易对数量大于最大交易对个数时，撤消具有最新交易量的交易对中的所有订单。第三、设置可调节的强制处理限额（类似于一个 Hard Cap），确保即使极端情况出现，或需求短期内高度波动，也可以支持 DEX 的正常运行以及订单的可控，进而有效避免因订单挤压引起的服务器崩溃。

6 展望

在数字货币领域中，许多用户经常遇到灾难性的损失，通常发生在那些专门用来存放和保管用户资产的交易所里。跨链原子交换(atomic swaps)就此诞生。从技术概念而言即是允许加密货币在不同的区块链上进行直接的点对点转移，以此代替当前投资者所使用的易受攻击的交易所。作为区块链行业的技术先行者，LBTC 自然不会放过跨链原子交换这一新兴技术风口，运用跨链原子技术的 DEX，将能实现多币种的转换及交易，未来，许多大型客户资金库将会被代码所淘汰。跨链技术的实现对于跨链平台而言，还需要具有可扩展性的区块链，基于 DPOS 共识机制的 LBTC 正是满足了跨链技术对于可扩展性的需求，拥有足够的空间开发原子交换所需搭建基础架构。

未来 lbtc 将支持跨链技术，从而实现链之间的价值交换。我们认为未来的区块链将会是一个多经济系统、多链的架构。比特币定位为全球价值互联网传输协议，进一步拓展跨链功能从而链和链之间的交互的问题是很有必要的。第一个需要解决的问题场景就是跨链资产的转移问题，目前主流方法是通过中心化的交易所进行跨链资产转移，使用去中心化的多种弊端在上文多处均已提及。在 LBTC 去中心化交易所中采用跨链技术后，我们未来可以通过 LBTC 去中心化交易所直接实现链上资产的转移。下一个我们将探究的技术可能会是跨链的预言机，所谓跨链的预言机指当我们在某条链上执行一个动作时，可以自动触发另一条链上的特定事件，从而去执行指定的条款，具体的应用场景可以执行跨链的合约，例如在链 a 和链 b 之间发生资产转移时，就会用到跨链合约中的某些功能支付利息、支付资产等。

而智能合约也是近年来区块链行业逐渐兴起与不断发展成熟的技术，同时一并纳入了LBTC 的发展规划之中。智能合约系统根据事件描述信息中包含的触发条件，当触发条件满足时，从智能合约自动发出预设的数据资源，以及包括触发条件的事件。智能合约只是一个事务处理模块和状态机构成的系统，它不产生智能合约，也不会修改智能合约。智能合约可以让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志，正确执行，从而实现区块链中“去中心化”的最大特性。智能合约上线后，可大大提高 LBTC 的可扩展性，许多基于 LBTC 的 Dapp 即可上线。凭借着高 TPS，支持热门应用将不会出现网络拥堵的问题。同时，零知识证明已被列入了规划，因此可以想到，未来发展成熟的 LBTC 还将具有匿名及兼容多应用的特性，随着技术开发及生态建设的成熟，LBTC 具备的功能将更加强大和复杂。

在 LBTC 的未来规划的宏图中，LBTC 几乎创建了一个属于自己的帝国。安全可靠的技术的支持为帝国的建设打下了坚固的地基，链上治理的规划搭起了帝国的框架，而网关协议、去中心化交易所、智能合约则是上层建筑的血肉。从迄今为止的发展路线可以看出，LBTC 从不愿意走“大众”路线，DPOS+UTXO 机制、链上治理 SGS、去中心化交易所，无一不是区块链行业中的新兴实践。LBTC 在一步一个脚印地稳步前进，此时，分叉币已不再是它的唯一标签。LBTC 的“DPOS+UTXO+智能合约”三者的结合，是前无仅有全新实验，究竟能碰撞出怎样的火花，让我们共同期待。

7 参考文献

[1]Satoshi Nakamoto,Bitcoin:A Peer-to-Peer Electronic Cash System[M],2009.

[2]Ethereum:A Next-Generation Smart Contract and Decentralized Application Platform[M],2017.

[3]Ripple Labs,The Ripple Protocol Consensus Algorithm[M],2014.

[4]Bitshares,A PeertoPeer Polymorphic Digital Asset Exchange[M],2013.

[5]Steem,An incentivized,blockchain-based,public content platform[M],2017.

[6]Kevin Kelly,Out of Control: The New Biology of Machines, Social Systems, and the Economic World,2010.

[7]Jean-Jacques Rousseau，Du Contrat Socia，1762.