

LITEX - 去中心化的数字货币即时支付解决方案

1. 摘要

小微支付 (Micropayment) 是比特币的一大难题，过长的确认时间、过高的手续费让比特币脱离了日常消费的支付场景，变成了一种价值囤积和大额结算的「数字黄金」。另一方面，针对区块链的追踪技术也日臻成熟，已经有多家相关公司与政府签订合同，共同研发监管比特币交易的技术，这让比特币网络的匿名特性受到了极大的冲击。

为了解决这些问题，技术界提出了多种升级方案，而社区各方的分歧也一度将比特币推到硬分叉的危机边缘。直到5个月前 (区块高度481,824) **隔离见证 (SegWit)** 的成功激活，标志着全网已经对软分叉已经达成共识，这不但缓解了比特币网络容量告急的问题，更重要的是让目前最有前景的升级方案——**闪电网络 (Lightning Network)** 得以更加顺利地部署。

一直以来，比特币在现实生活中的应用场景十分有限，普通商户在接受比特币支付上还存在很大的障碍。由于比特币应用的技术大都是高深的密码学、分布式计算等领域的知识，一般商户很难理解它的原理和优势；频繁大幅的币值波动也使得一旦接受比特币付款，商户将面临较大的损失风险。虽然有一些团队已经可以为商户提供法币结算的支付网关解决方案 (如目前最大的比特币商户支付网关 **BitPay**)，但其极度中心化的运作模式以及对主链交易的依赖导致其存在不亚于数字货币交易所的系统性风险 (如2014年当时最大的交易所Mt. Gox丢失85万枚BTC的「门头沟」事件)；而明星项目**TenX**虽然使用闪电网络技术实现了高效率的数字货币转账，却在向商户端的结算上完全依赖中心化的**VISA**，而且在解决数字货币向法币兑换的过程中也依赖于交易所模式。这些产品放弃了去中心化这一数字货币的核心价值，无法成为未来数字货币支付的主流解决方案。

LITEX是一种完全去中心化的数字货币支付落地解决方案，具有支持小微支付、即时到账、手续费极低等优势。**LITEX**以**易宝支付**明星产品——「**非银行卡支付**」业务模型为基础，基于**BOLT**协议实现了自己的「**复合决策闪电网络**」，通过上层决策网络匹配支付请求和法币兑换请求，再由下层闪电网络建立高效、安全的支付通路，最终通过各地支付收单方完成与商户的法币结算。由于法币提供的模式类似于**P2P**代付，全过程无任何中心化机构参与，避免了由于**Visa**等卡组织停止合作而导致的商业模式崩溃 (如**TenX**等先

例)，极大地保证了支付网络的安全稳定和持续发展。另一方面，上层网络的激励策略可以有效避免闪电网络的中心化倾向。

LITEX相比其他支付产品的优势有：

- **去中心化的法币供应模式**：系统中法币由购币者提供，相当于**P2P代付法币**，法币的获取不需要依赖交易所等中心化机构；
- **避免资金丢失等中心化风险**：使用闪电网络作为支付通道，没有自建资金池，即使受到攻击也不会有资金损失；
- **支付落地深入稳定**：团队现有资源可以迅速跟主流国家收单方建立合作，绕开银行卡组织等中心化机构，避免产生其他产品因VISA停止合作而无法落地、费率不可控等严重问题。

LITEX在以下几个方面大大优化了现有的比特币支付的体验：

- **小额支付**：可以支持**极其小额**的比特币支付，如0.00001 BTC的支付；
- **即时支付**：高达**每秒数百万笔**支付的并发处理能力（对比Visa目前峰值处理能力为80000笔/秒，比特币主网处理能力约7笔/秒），任意支付可以在秒级完成；
- **无手续费**：**LITEX**的链外交易能力避免了主链交易的高额手续费，使用LITEX向商户支付的消费者可以享受**交易0手续费**；
- **匿名交易**：得益于链外交易能力和**HTLC**智能合约，以及基于类似**Tor**的加密协议，可以保证网内的所有交易都无法被追溯；
- **商户无门槛接入**：在商户端，接入LITEX收款能力与接入现有的任何支付网关的流程完全一致，甚至可以获得**T+0**的法币实时入账服务；
- **多币种支持**：LITEX具备**跨链原子交换（Atomic Swaps）**能力，在LITEX上用户可以低成本、零风险地进行比特币（BTC）、以太坊（ETH）或者莱特币（LTC）以及其他数字货币之间的实时互转互通。

我们相信，数字货币体系终将完全变革现有的金融生态，实现全球范围的流通闭环；数字货币也将融入人们日常生活的方方面面，降低交易成本，提升交易安全。这个过程注定是漫长的，LITEX以技术为推动力，秉持去中心化的理念，致力于通过对数字货币支付效率和体验的提升迅速扩大数字货币的应用场景和持币人群，建立数字货币生态闭环。

摘要	1
项目背景	5
数字货币的现状	5
比特币的困境——小微支付 (Micropayment)	5
比特币的困境——伪匿名	7
比特币的曙光——闪电网络 (Lightning Network)	7
关键问题：如何落地	10
解决方案演变	12
阶段一：中心化解决方案——代表产品BitPay	12
阶段二：半中心化的解决方案——代表产品TenX	13
阶段三：去中心化的解决方案——LITEX	14
最终阶段：用数字货币完成交易闭环	15
去中心化的支付解决方案——LITEX	16
概念定义	16
核心价值	16
架构介绍	17
综述	17
LITEX主体架构	17
技术创新	19
复合决策闪电网络模型	19
匹配引擎	19
智能路由	20
完全匿名	20
轻节点	21
应用场景	22
日常消费场景	22
未来展望	23

代币系统设计	24
名称与设计目标	24
LXT体系	24
LXT的产生和消灭	24
价值体系和激励方案	24
LXT发行计划	25
项目规划	26
组织架构介绍	27
LITEX 社区基金会	27
核心团队	28
合作伙伴团队	28
基石投资人及顾问	29
风险声明	30
风险提示	30
免责声明	33

2. 项目背景

2.1. 数字货币的现状

据不完全统计，目前在各大交易所上市的数字货币已经超过1600种，而仅仅9年前，世界上第一种数字货币——比特币的概念才刚刚由中本聪提出。这些数字货币中有为了解决比特币的困境而出现的竞争币（如瑞波币），也有基于区块链技术诞生的应用平台代币（如以太坊，以及基于以太坊开发的DApp生成的各种Token），还有基于侧链等新技术的自定义币种。可以说，数字货币的繁荣很大程度上反映了技术界以及全社会对区块链技术的认可和期待。

然而，数字货币目前的应用场景却十分有限。由于种类繁多、币值不稳定，数字货币主要的交易都来自于币币交易以及法币兑换，相比流通货币而言，现在的数字货币更像是一种投资标的。毫无疑问，火热的投资市场让区块链技术为大众所熟知，这是有利于数字货币发展的，但这不会是未来的发展方向。数字货币终究要回归流通货币的本质，只有人们开始使用数字货币消费、商家使用数字货币结算，整个社会慢慢迁移到数字货币的流通体系上来，才能实现数字货币的最大价值。

数字货币的应用场景受到限制固然有社会各界认知不全面、传统利益集团阻碍等外部因素，但也有数字货币技术不完善、社区技术方案分歧较大等内部因素。而作为全球数字货币基石的比特币，也因其设计容量不足、处理速度慢、匿名性日渐降低等问题，基本无法作为流通货币使用，与大众的日常生活更是几乎没有关联。

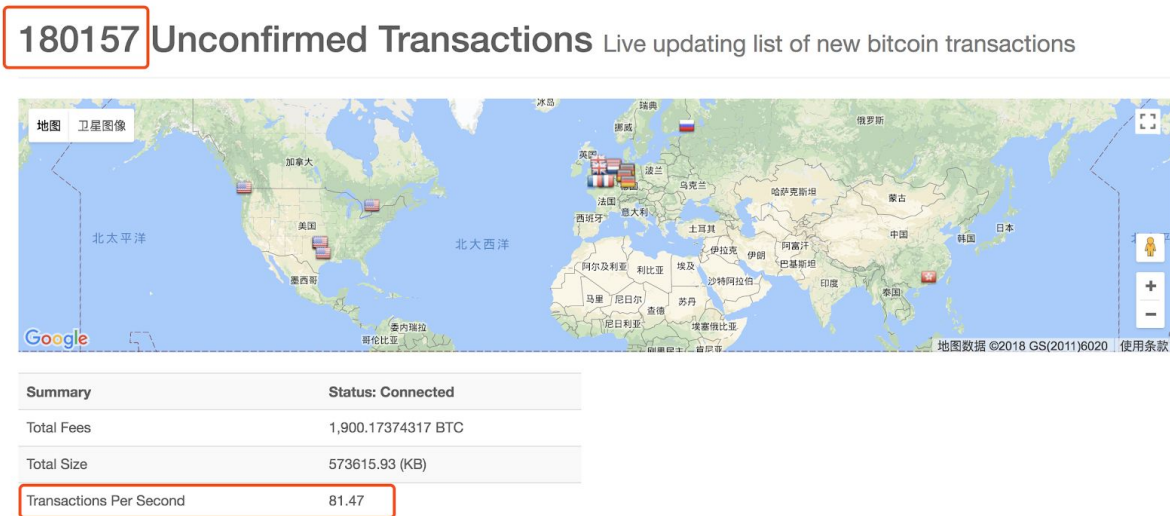
2.2. 比特币的困境——小微支付 (Micropayment)

一种合格的流通货币应该具备小额、即时支付能力，相比现金，电子货币在这方面有先天的优势。然而在主网 (mainnet) 已经成功运行了9年的今天，比特币系统却逐渐丧失了迅速处理小额支付的能力，变成了一种价值符号和大额资产转移的通道，一如当年的黄金。小微支付之所以会成为比特币的一大难题，是因为比特币为了确保分布式记账系统的一致性和稳定性，在架构上对效率做出了牺牲。

比特币设计之初，为了确保交易的不可撤销性、提升恶意节点的攻击成本，引入了一种分布式记账系统。它将数据封装打包后用链表结构承载，并通过一种叫做「工作量证明」 (Proof of Work, POW) 的机制保障全网的计算节点都自发一致地维护唯一的账目记录。而对于链条上每一个称作「区块」 (Block) 的数据包，引入了非对称加密算法，确

保其中记录的每一笔交易都不可更改。这就是我们今天熟知的「区块链」(Blockchain) 技术。

区块链技术现在已经成为各大巨头公司乃至各国政府都积极研究发展的前沿技术，价值潜力巨大，而比特币由于其货币属性，对自身区块链的能力进行了比较大的限制。一方面，为了保障系统的安全稳定和存储效率，比特币的区块大小被限制在1MB以内；另一方面，为了平衡矿工的收益，系统设计了一种动态难度机制，将系统的区块产出速度稳定在10分钟/个；而每笔交易的平均大小为226B。这些因素导致了比特币网络处理交易的速度是大致不变的，约为**7笔/秒**，而实际的交易大小往往能够达到500B，这时候系统处理能力下降为3笔/秒。随着比特币交易量的不断增长，比特币主网 (mainnet) 网络拥堵的情况也日益严重，下图为撰文时 (2018年01月16日) 从blockchain.info截取的实时数据：



可以看出全网平均每秒产生的交易笔数高达81.47笔，是处理速度的11倍多，而等待确认的交易数量超过了18万笔！即使立即停止所有交易，系统也需要6个小时以上才能处理完这些交易，可见比特币主网已经异常拥堵。

比特币主网的拥堵进一步加剧了小额支付到账延迟的情况。由于比特币转账手续费是固额收取而非按比例收取，小额支付者愿意付出的手续费无法跟大额支付者抗衡，而矿工会优先记录手续费高的交易以获取更高的收益，因此小额支付的记账优先级总是低于大额支付。事实上，目前一部分小额支付可能需要第二天才能到账。也就是说，如果你去星巴克买一杯大杯拿铁，并直接使用比特币支付，那么运气不好的话，很可能坐到咖啡店关门的时候你还没喝到那杯拿铁。

另外，比特币系统还对过小的支付金额做了限制。因为主网的不堪重负，比特币核心团队在2013年提交了一个功能来禁止一定金额以下的比特币交易，这被称为「除尘补丁」。目前这个灰尘阈值 (dust threshold) 是546聪 (5.46μBTC)，对应币值峰值时约

为14美分，而低于这个阈值的转账将会被直接丢弃（官方原文：won't be relayed, won't be mined）。鉴于全世界不同地区的物价水平不同，低于14美分的交易在实际生活中并不少见，而这些交易在比特币系统中属于不被支持的「不经济交易」（uneconomic dust）。

除了延迟到账问题，高昂的手续费也使得小额交易失去了意义。去年12月比特币的交易手续费一度达到1000聪/字节，按照226字节的交易大小和1 BTC≈15000 USD的时价来计算，一笔交易所需的手续费已经高达30美元，这不是一笔小额消费能够承受的手续费金额。

我们可以得出结论，比特币网络在处理小微支付时无法满足其小金额、低延迟、低手续费的固有要求，甚至可能把较小的支付金额直接过滤掉，这导致比特币无法将应用场景拓展到日常生活消费中来，极大的限制了数字货币的发展。

2.3. 比特币的困境——伪匿名

比特币受人追捧的一个重要原因是它的匿名交易特性：由于比特币地址是不记名、可随意创建的，比特币交易也无需第三方中介机构的参与，虽然每一笔比特币网络上的交易都被全部节点记录下来，但是无法确认交易双方的真实身份，从而保障了交易双方的隐私。然而随着数据挖掘技术的发展，以及各国政府对比特币交易监管的极大需求，有些技术公司（如Chainalysis和Elliptic都已跟政府签订了合同）已经在区块链交易追踪取证技术上获得了成果，这使得比特币交易匿名的含金量逐渐降低，而其交易记录全网公开、不可撤销的特性使得一旦一个地址的拥有者被锁定，他的全部历史交易都将被无争议地追溯出来，这将形成非常大的隐私风险。也就是说，今后主网上的比特币交易的匿名性很有可能无法达到现金交易的水平。

2.4. 比特币的曙光——闪电网络（Lightning Network）

从2015年比特币维护者加文·安德烈森（Gavin Andresen）指出主网扩容的迫切性以来，比特币核心团队和整个社区都在争论什么方案才是比特币的未来。其中一派的主要意见为直接扩大区块的容量（2MB、8MB甚至不设上限），而这将不可避免地导致比特币硬分叉，进而严重影响当前格局的稳定性；另一派主张保留1MB的区块大小，通过链外的方式更长久地解决容量和延展性问题，而且这种方式有可能通过软分叉就能解决。经过激烈的博弈，原定于2017年11月（区块高度494,784）的SegWit2x硬分叉计划终止，而3个月前成功激活的隔离见证作为软分叉解决方案被固定了下来，比特币最终选择了一条平稳而长远的道路。

隔离见证 (SegWit) 的原理是将区块中用于验证交易的见证信息 (占交易容量的40%左右) 在区块中的存储方式进行了调整, 使得节点验证区块大小时不计算这部分内容, 从而使得在逻辑上保持1MB容量限制的同时, 达到在实际上增加区块空间到约2MB的效果。隔离见证的另一个重要意义是解决了「交易延展性」(Transaction Malleability) 问题, 即一笔交易的ID (TxID) 有可能在最终确认前被第三方改变的问题。交易延展性虽然不会造成系统性的恶果, 但是它的解决为比特币最受期待的升级方案铺平了道路——闪电网络。

闪电网络 (Lightning Network) 可以说是万众期待的比特币网络「第二层」升级, 是比特币网络的「升维」操作。它的基本逻辑由两个智能合约 (**RSMC**和**HTLC**) 构成, 在保证链上支付一样的安全性的同时, 巧妙地实现了比特币支付的链外运行。闪电网络在解决比特币困境上具有以下优点:

- **资金安全**: 用户可随时关闭交易通道并申请提现, 这一过程由智能合约保证;
- **快速交易**: 交易双方只需在打开通道和关闭通道时各提交一笔主网交易, 期间双方在通道中的所有交易在链外进行, 每一笔交易无论金额大小都能在毫秒级时间完成, 系统处理速度可达每秒几百万笔;
- **低手续费**: 主网依赖专业矿工组织通过大规模计算进行交易维护, 而闪电网络中的每个节点都可以作为交易传递链路, 这种传递是全自动、极低成本的, 因此只需非常少量的手续费, 交易就能急速地在闪电网络中传递。
- **隐私保护**: 由于通道内的交易不会记录到主网, 而传导链路上的每个节点只能获知它的上下游节点信息和金额信息, 无法掌握交易全貌 (如发起人、支付人、交易总金额), 这使得交易双方的隐私得到了极大的保障。

另一方面, 闪电网络目前还停留在方案实现阶段, 距离闪大规模部署和使用还有一段距离。结合小微支付场景来看, 目前闪电网络还存在如下课题:

- **跨链通道**: 需要更多的主链对闪电网络加入支持;
- **智能路由**: 支付通道的限额由通道链路上最小的一环决定, 每笔交易都需要寻找一条限额高于自身金额的通路才能到达收款方;
- **完全匿名**: 需要借助额外的加密协议来实现;
- **轻节点**: 闪电网络设计中要求每一个节点都运行一个比特币网络全节点, 这无疑极大的限制了闪电网络的应用场景, 需要设计一种可以运行在移动设备上的轻节点才能适应日常支付场景的要求。
- **中心化倾向**: 由于闪电网络支付通道的开启和关闭都要消耗一定手续费, 而通道容量有大小, 因此有出现中心化大节点的风险。可以通过对协议进行自定义实现来加入一些反馈调节等机制, 从而依靠自适应算法维持一个健康的拓扑结构和去中心化

的网络。LITEX 就使用了双层网络的结构实现了复杂路由和网络健康程度的自我调节，从而最大限度地避免中心化风险。

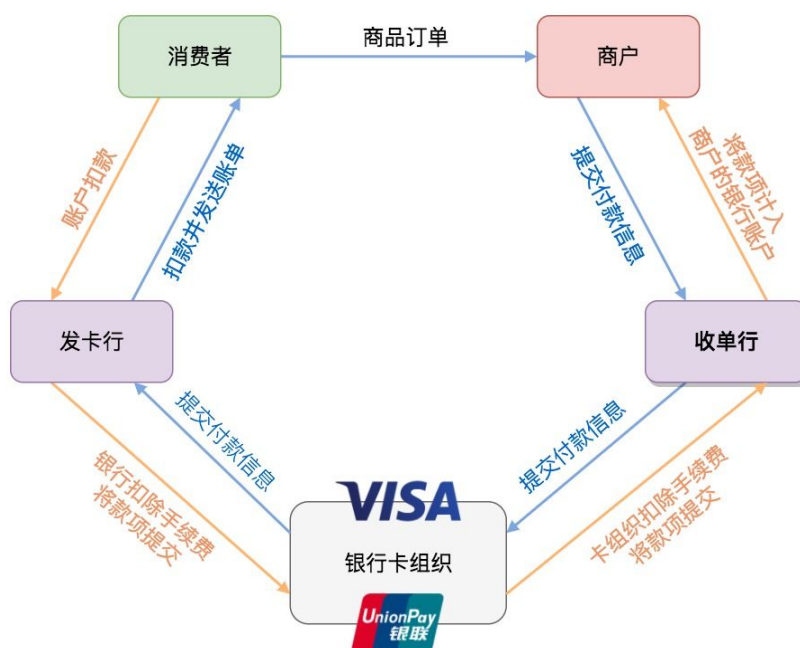
闪电网络是目前最有前景的升级方案，已经有一些科技公司投入到了闪电网络基础技术和应用场景的探索中。随着半个多月前Blockstream公司宣布闪电网络RC1在主网测试成功，我们可以预见更多的团队将会加入到完善数字货币生态的行列中来。

3. 关键问题：如何落地

在相当长一段时间内，商户对直接接受数字货币支付的认可度都不会太高：一方面接受数字货币需要相对较深的技术知识，商户没能力也没动力去学习；另一方面数字货币币值波动的频率和幅度还非常大，无法纳入商户的成本收益模型中。因此在数字货币支付的解决方案中，如何能够尽量低风险、高效率地完成数字货币到法币的兑换进而结算给商户，是无论如何也绕不开的问题。

首先是数字货币兑换。目前数字货币到法币的兑换主要是由交易所完成的，但是交易所是一个完全中心化的机构，资金被盗风险、交易时效性差都制约了将直接对接交易所API作为支付方案一环的可行性。一些解决方案采用了对接交易所的同时自建资金池进行缓冲的方式进行优化，但这也带来了新的问题，比如资金池的容量问题，以及运营方需要自担巨大的资金波动风险的问题等。只有尽量高效、安全地将数字货币兑换成法币，这一环才能满足消费场景支付的需要。

另一方面，也是最重要的一环：将法币结算给商户。虽然这件事情每天都在发生，但实际上的一笔法币的结算需要很多支付机构之间互相协调配合，这其中商户承担了全部的费用（国际上平均手续费为交易金额的2%~3%）。下图简要描述了各机构的协作过程：



在支付行业中，「收单行」其实代表了一个生态，主要由**收单银行**、**收单机构**、**服务商**三者构成。收单银行就是指在商户那里放置POS机的银行；收单机构指持有第三方支付牌照的专业公司，如易宝支付、微信支付、支付宝等，他们直接跟银行合作，完成快捷支

付等协议的对接以及风控等工作；服务提供商指协助收单方对商户提供软硬件系统的服务公司，如哆啦宝，主要涉及跟消费者和商户直接交互的软件系统，以及维护商户关系等。

回到法币结算问题上来，从上图可见最简单的方式是跟银行卡组织合作，因为他们已经在全球遍布了与发卡行、收单行的合作，但这有两个问题：一是卡组织手续费很高（2%以上），提升成本；更重要的是，数字货币的全球化属性跟卡组织跨境结算功能在一定程度上有直接竞争关系，卡组织很可能停止支持加密货币甚至封杀加密货币，而且这已经发生了——**Visa和MasterCard先后宣布停止旗下所有加密货币（即数字货币）联名卡的功能**，两方CEO也分别发表言论抨击比特币，表示不会承认比特币的货币属性，也不提供比特币支付和兑换的服务。由于这一服务从几年前开始提供，现有的大多数数字货币支付产品方案都采用了跟卡组织对接的方式完成支付落地，但是现在他们在商户端的这一出口已经被完全堵死了。

将支付落地方案完全依托于卡组织的解决方案是不稳定、不长久的，而且目前也是不可行的。LITEX 团队具有**深厚的支付行业背景**，未来将深入全球支付行业生态，由团队自主**建立与世界各国当地收单机构的合作关系**，在更深层次上做到数字货币支付落地的安全稳定，从而可以跟各银行卡组织进行名正言顺地竞争，并在数字货币大流通时代到来之时将他们淘汰出局。

4. 解决方案演变

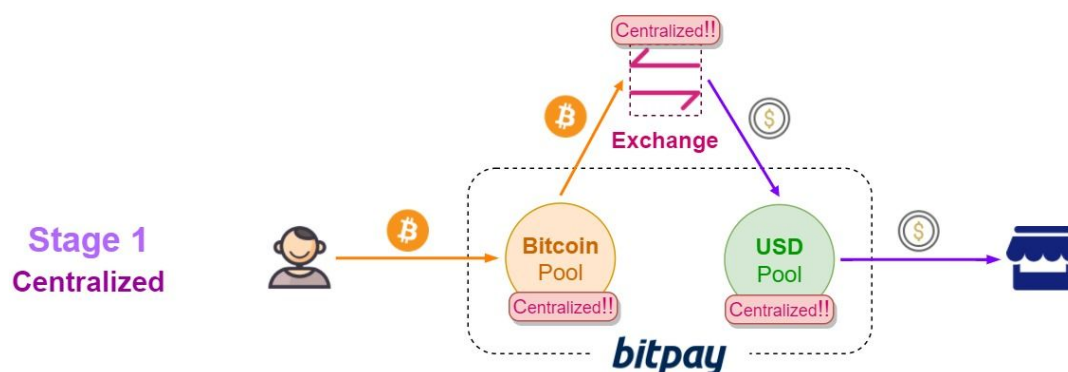
为了提高消费者和商户对交易中使用数字货币的接受程度，一个合格的产品要能解决这些基本问题：

- 支付到账慢
- 支付手续费高
- 接收数字货币的知识门槛高
- 数字货币币值波动大

应对前两个问题最好的方式是尽量避免在主链进行交易，但这也会带来一些安全问题；后两个问题则相对简单，只要为商户承担数字货币到法币的兑换工作，实现向商户直接结算法币，问题就解决了。然而在实现方式上，能否延续数字货币的**去中心化、匿名**等特性，在很大程度上决定了这种方案的生命力，因为只有完全去中心化的解决方案才能体现数字货币的核心价值，否则只能看作是一定阶段的权宜性产品。下面按照这个标准，我们把解决路径划分为三个阶段，分别为：**中心化、半中心化、去中心化**，以及在数字货币实现完全互通后，哪种方案更有生命力。

4.1. 阶段一：中心化解决方案——代表产品BitPay

BitPay是目前全球最大的数字货币（主要是比特币）支付解决方案提供商，被称为比特币界的PayPal。它通过向商户提供法币结算的方式，鼓励更多商户接入比特币支付方式。自2014年成立以来，BitPay已经在全球拥有了几万个合作商户。

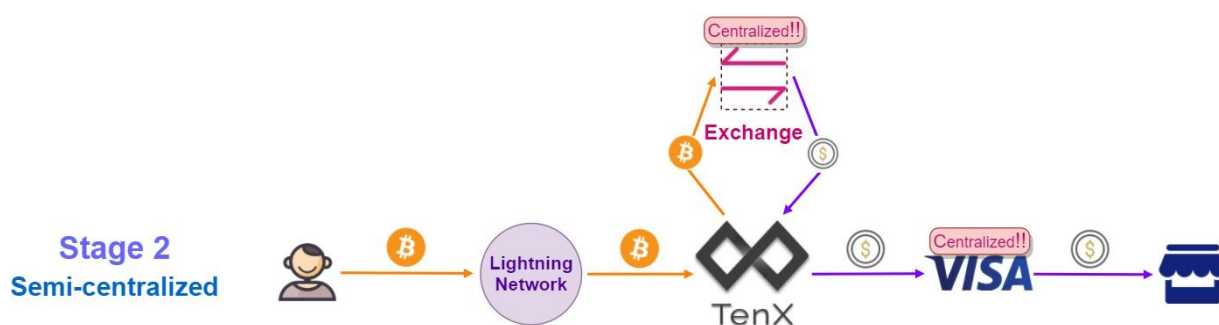


BitPay通过把用户转账过来的比特币帮商户兑换成法币的方式提供服务，然而这种服务模式已经逐渐脱离时代：日趋高昂的手续费让原本就不太多的比特币支付者变得更加稀

少，也迫使BitPay将商户的提现门槛提高到了100美元。另一方面，BitPay完全中心化的运作模式使得用户和商户的资金安全得不到保障：为了节省手续费，用户会倾向于每次向BitPay的钱包中转入较大金额的比特币，而商户端也有前述的提现门槛。如果BitPay因为遭遇攻击导致其官方账户中的比特币和现金受损，那么相应的用户和商户资金也就同样丢失了，这种情况已经在交易所被黑客攻击的事件中上演过多次了，很多用户血本无归而又无可奈何。

4.2. 阶段二：半中心化的解决方案——代表产品TenX

比特币社区对隔离见证达成共识后，闪电网络的前景也明朗起来，很多团队开始基于闪电网络构建解决方案。他们中的佼佼者——TenX在36小时内筹集到100,000枚ETH的成绩也侧面反映出了业界对这种解决方案寄予厚望。



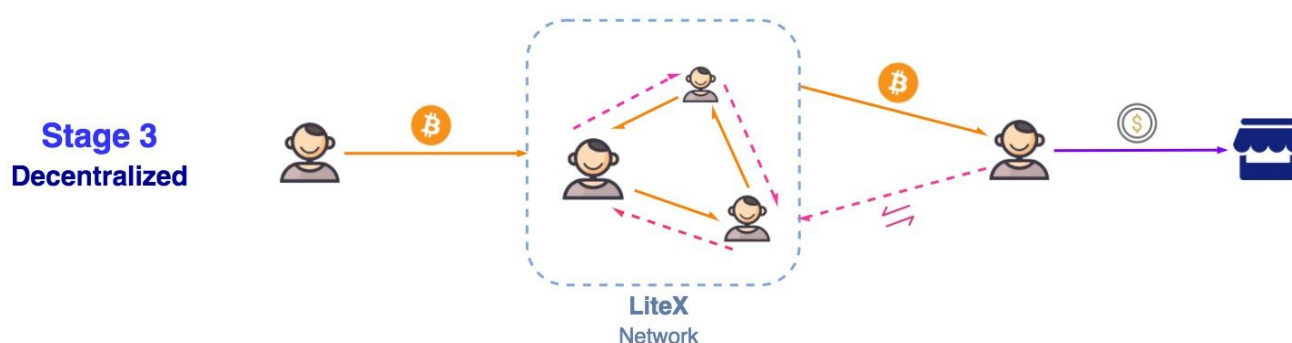
TenX的进步之处在于它通过闪电网络与用户进行数字货币转账，这就极大的规避了数字货币存储在官方账户内的中心化风险，因为即使TenX受到攻击，用户依然可以利用RSMC智能合约将自己的资金提回主链钱包内，不用担心被攻击者转走。但是这在支付流程中只能算是完成了一半，因为还需要将数字货币兑换成法币向商户结算，TenX在这一步选择了与Visa合作发行联名信用卡的方式解决问题。然而Visa官方曾明确表示，Visa并不涉及到将货币转换为法定货币的方式，这方面由发行人或其程序管理员通过一个加密的货币兑换来执行。也就是说Visa只是作为一个结算通道帮助TenX集成进商户的结算流程，其对数字货币消费的所谓支持也与用户使用信用卡积分进行消费非常类似，并不涉及数字货币兑换法币的业务，可见这一步骤只能由TenX借助交易所等方式中心化地完成。

另一方面，通过Visa等银行卡组织与商户结算相当于将自己核心商业模式的一半委托给合作方完成，而作为数字货币支付方式的TenX与代表传统货币支付网络的Visa在将来必然会发展为竞争关系，这是非常不稳定的。2018年的1月6日，Visa宣布与一家名为WaveCrest的借记卡供应商结束了合作，而正是这家公司发行了TenX、CryptoPay、Bitwala、Wirex等公司的数字货币联名卡，所以TenX与Visa联合发行的借记卡已经无法使

用。Visa的CEO阿尔弗雷德·凯利 (Alfred Kelly) 也在1月18日前后表示Visa不会支持比特币交易。

4.3. 阶段三：去中心化的解决方案——LITEX

无论BitPay还是TenX，都存在对Visa等卡组织的依赖和中心化的数字货币到法币的兑换方案，这些给他们的商业模式带来了隐患和打击。只有探索出一种完全去中心化的支付路径，才有可能长久地解决数字货币的支付问题，LITEX正是这样一种解决方案。



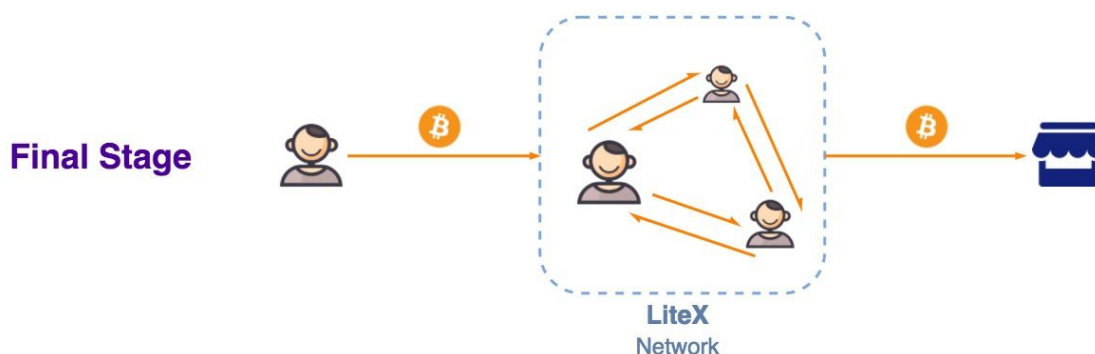
LITEX的架构中不存在任何中心化的节点，无论是数字货币的传递还是法币的结算都是由网络上的用户节点自主协调完成的，这是LITEX网络节点通过复杂的匹配模型和路由算法实现的。在这一过程中，消费者成功用数字货币完成了即时支付，即使支付金额非常小也不会受影响；商户实时地收到了对应金额（扣除一定手续费）的法币，免受提现门槛的困扰；购币者也低成本地换到了需要的数字货币，可以用于接下来的消费或任何目的。

LITEX不但低成本、高效率地解决了数字货币在支付场景中遇到的问题，还能最大限度地保障用户和商户的资金安全。在上述交易过程中，如果交易环节中有节点出现问题，交易都可以自动切换到其他路径继续进行；即使大部分节点瘫痪导致交易无法进行，用户的资金也会按照RSMC和HTLC协议自动提现到主链账户或退回法币账户，不会被窃取或丢失。

另外，LITEX网络中交易通道内的节点只能接触到相邻节点信息，由于没有中央节点的存在，以及协议中的多层次加密保障，用户在LITEX中的转账和交易都是完全匿名的，这是中心化或半中心化解决方案无法做到的隐私保障。

4.4. 最终阶段：用数字货币完成交易闭环

用户使用数字货币支付，商户使用数字货币结算，法币与数字货币互换的需求大幅减少甚至消失，这是我们期望看到的数字货币新生态。



LITeX在迈向这一生态的过程中无疑会发挥非常大的促进作用，但这并不意味着LITeX的价值仅存在于过渡阶段，即使在完全数字货币化的交易场景中，LITeX已经建立起的大规模、多联通的闪电网络结构仍然是效率最高、成本最低的支付通路，这一先发优势建立的壁垒将具有非常大的粘性，让LITeX成为用户支付的首选。

5. 去中心化的支付解决方案——LITEX

5.1. 概念定义

- **LITEX Network, LTXN** : LITEX的支付和兑换网络系统, 是一种基于BOLT协议的, 针对数字货币支付、兑换以及法币结算等场景进行定制实现的复合型去中心化网络, 由**决策网络**和**执行网络**(闪电网络)结合构成;
- **LTXN节点** : 每一个参与LTXN的用户或机构都是一个LTXN节点:
 - **消费者 (Customer)** : 使用数字货币进行消费支付的用户;
 - **商户 (Merchant)** : 接受数字货币支付并提供产品服务的用户;
 - **购币者 (Exchanger)** : 使用法币兑换数字货币的用户;
- **匹配引擎 (Matching Engine)** : 通过复杂策略匹配和路由网络中的数字货币支付请求与货币兑换请求;
- **最后一跳 (Last Hop)** : 在LTXN支付通道中最后链接到商户的一环。

5.2. 核心价值

LITEX建立了一套去中心化的数字货币支付系统。项目立足于最前沿的比特币网络升级技术, 结合易宝支付「非银行卡支付」体系中的多方匹配策略和支付网关的合作模式, 将用户和商户接入数字货币支付的成本降到最低, 同时保证交易的完全匿名。LITEX生态还会把系统产生的收益回馈给参与建设生态的所有角色, 形成正向激励的健康发展模式, 不断扩大数字货币支付的应用场景。

从日常消费场景来看:

- **消费者** : 支付结果实时确认, 无手续费; 通道内的数字货币的随时提现 (指通过主网交易回到自己的比特币钱包) 由智能合约保障, 无中心化风险; 且交易完全匿名, 隐私得到保障;
- **商户** : 无需了解数字货币, 接入和使用流程与现存支付网关高度一致; 支持法币入账, 支持实时到账, 规避币值波动风险和结算风险;
- **购币者** : 法币兑换数字货币将变得非常简单、快速, 用户可以无知识、零余额加入LTXN, 并随时通过法币兑换到需要的数字货币以供使用。

从满足多级需求上来看:

- **消费者** : 既可以满足本国法币结算的日常消费支付需求, 也可以满足跨国法币结算的出境购物支付需求, 还可以满足全球的线上购物支付需求;

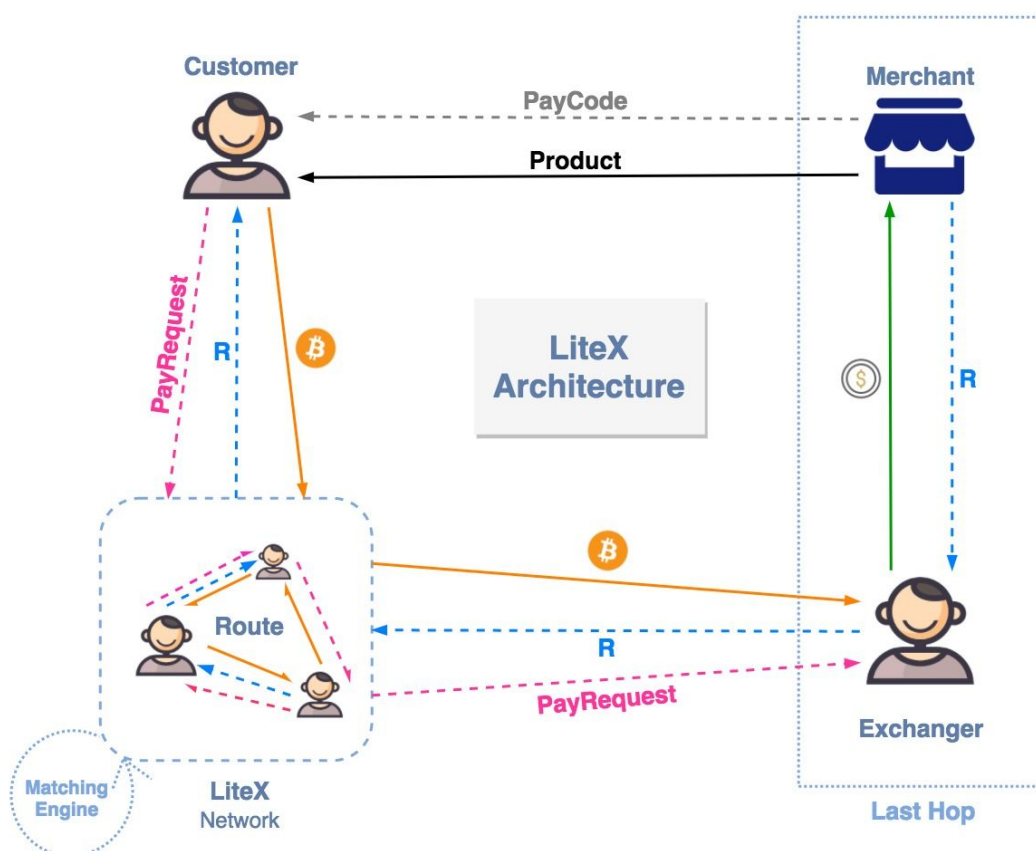
- **商户**：对数字货币接受度低的情况下，可以选择法币实时结算；未来了解并接受数字货币后，可以无缝切换成数字货币结算，并且可以直接享受到LTXN已经建立的闪电网络体系所带来的高效率、低成本收款体验；
- **购币者**：既可以满足普通个人用户兑换需求，也可以接入交易所等机构的兑换需求，既可以满足较高成本的快速兑换需求，也可以满足较低成本的挂单性质的兑换需求，未来还可以通过跨链原子交易直接满足数字货币之间的兑换需求。

5.3. 架构介绍

5.3.1. 综述

LITEX的主要应用场景为数字货币小微支付消费场景，这一场景的参与者为消费者和商户。由于商户对数字货币的接受度还比较低，我们引入了另一个应用场景——货币兑换，实现了在最后一跳中通过智能合约将法币交易纳入整个支付通道链路，避免了中心化风险的发生。这两个应用场景相辅相成，共同完成系统的业务闭环。

5.3.2. LITEX主体架构



上图为LITEX解决方案的总体架构图。实线箭头代表的是货币和产品等现实交易要素的流向，虚线代表的是LITEX系统中的数据和控制信息的流向，其中的 R 可以先简单理解为一个暗语，拿到暗语的人可以向他的上游索取数字货币，这是HTLC智能合约中用以保障整个链条自动进行交易传递的机制。

LTXN网络的运转主要由两个流程驱动，主流程是消费者使用数字货币消费的过程，基本按照上图中逆时针方向运行；副流程是购币者将法币换成数字货币的过程，基本按照上图中顺时针方向运行——除了在最后一跳（Last Hop）中购币者付现给商户的环节。两个流程通过**决策网络**和**匹配引擎**（Matching Engine）的协调得到最优化的配置和联动，共同完成多种支付场景和兑换场景的需求。

在主流程中，消费者获得商户的**收款码**（包含通道地址、收款鉴权码等信息）后，通过LITEX的钱包App（轻节点）发起一笔支付请求（PayRequest），这一请求被广播到LTXN上，通过匹配引擎得到一个支付路由（PayRoute），这一路由将消费者的付款请求发送给匹配程度最高的购币者（进入副流程），并由购币者用法币支付给商户，商户确认收款后，会发送一个暗语 R 给购币者，购币者将 R 发送回LPTN后就能立即获得对应金额的数字货币，最后 R 经LTXN中的节点链路反馈给消费者，消费者验证 R 与收款鉴权码匹配后，将数字货币支付给LTXN中对应节点，整个交易过程结束。

系统设计中满足各需求的优先级如下：

- **资金安全**

确保交易资金安全是链外交易的前提，只有通过技术方案规避中心化的信任风险才是一个合格的链外交易解决方案。LTXN基于闪电网络技术，可以通过RSMC和HTLC两种智能合约确保资金安全。无论LITEX的官方节点是否受到攻击而掉线，LTXN都可以自发地完成交易、提现等操作；即便是网络节点大规模故障导致网络无法连通，在一定时间后用户的数字资产也会被智能合约自动提交到主链进行提现，安全地回到用户的数字钱包里。

- **支付和收款体验**

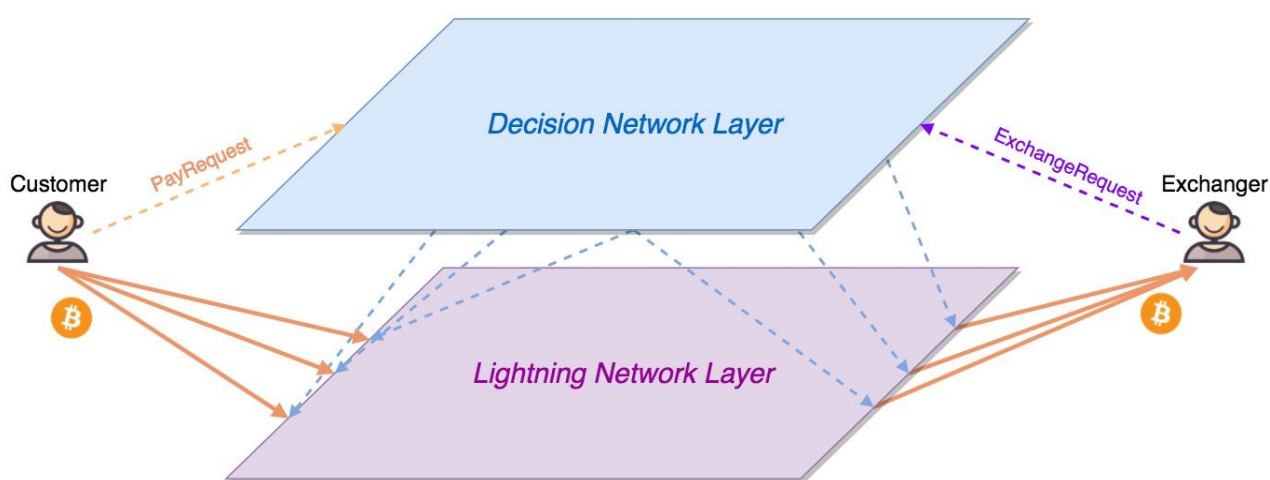
小额及时支付场景要求消费者能够快速、顺畅地完成支付，而商户可以方便地确认收款情况。由于数字货币价值的波动性，如果使用数字货币进行标价，消费者和商户都会陷入商品价格时刻变化的灾难中。LITEX的客户端支持输入**以法币为单位的**价格，在匹配引擎的辅助下确定对应的数字货币价格，消费者只需了解自己通过数字货币支付了特定法币价格的金额即可；在商户端，商户可以选择法币实时入账，因此使用体验与其他支付网关（如Visa）并无区别，甚至在到账时间上更有优势。

- 兑换效率

系统可以对不同的兑换需求提供相应的产品方案，而具体选用哪种方案由购币者自由选择。如果购币者有稳定的兑币需求，对时效性要求不高（如可以延迟一天甚至一周到账，并可以承受币值波动带来的风险），系统可以以比较低的手续费满足这一需求；如果购币者有非常迫切地的兑币需求，系统也可以通过匹配引擎最快速度地为其匹配相应的订单，而此时购币者可能需要付出稍高的手续费。

5.4. 技术创新

5.4.1. 复合决策闪电网络模型



闪电网络是基于BOLT协议实现的分布式网络的统称，最基础的闪电网络只能实现数字货币的链外点对点交易以及传递交易，一旦涉及到法币交易的匹配就无能为力了。我们设计的「**复合决策闪电网络**」是通过将一个决策层网络和一个执行层闪电网络融合到同一套分布式系统中，共用节点的同时可以做到深度联动，让闪电网络更智能，从而实现兑换请求与支付请求的匹配等高级路由功能，同时还可以通过规则设计和反馈系统让整个网络拓扑保持高效和分散化，避免出现中心化节点。

5.4.2. 匹配引擎

匹配引擎是一系列分布式智能算法集合，是LTXN最复杂的核心部件。限于篇幅，以下的描述大都基于系统中最简单的业务类别进行举例，不涉及具体的数据结构，也不讨论核心策略集——「非银行卡支付」业务逻辑如何应用于复杂业务处理和提升系统稳定性等细节。

LTXN系统中同时存在很多支付请求和兑换请求，其中支付请求一般有金额相对较小、即时性要求非常高的特点，兑换请求则视情况而定：有些用户为了获得较低的兑换成本，可以承受即时性比较低的兑换过程，甚至可以只设定一个上限，而在兑换的过程中按照需求随时结束兑换；另一些用户为了马上获得数字货币，可以选择支付较高的兑换手续费从而能够在很短的时间内兑换完成。实际设计中，用户需求的**时效/成本**比值可能介于前述两种情况之间的任意位置，我们将其用一定方式量化以作为入节点的自适应匹配决策的参考数据。

除了时效/成本的匹配，两方金额的匹配也是非常重要的一环。常见的情况是兑换请求的金额大于支付请求，LTXN各节点需要在全网匹配出复数个满足要求的请求组成最优解，需要考量的因素包括但不限于币种、金额、通道时间成本、通道传递损耗等。如果支付请求大于兑换请求，这种情况下支付额度较大，此时需要权衡的除了上述因素外，还应将主链通道的时效性和成本综合考虑，如果金额过大则建议用户进行主网支付。

最后，匹配策略同样需要考量联通性成本，如果收付两方位于互不联通的两个网络中，还需要建立网间通道的成本，这部分放在下面的路由部分进行讨论。

5.4.3. 智能路由

闪电网络通道的建立和关闭都需要进行链上交易，会产生比较高的时间和金钱成本，因此多数情况下消费者与购币者之间不存在直接通道，而是根据HTLC合约通过中间节点进行交易传导。中间节点可能是单个节点，也可能是首尾直连的多个节点。为了能够迅速的找到最短（或者代价最低）的路径，LTXN各节点都有一套自主协商算法和节点信息缓存同步策略，以便在需求出现时以最快速度找到通路，完成交易。

闪电网络的提现操作需要关闭支付通道，这使得全网的拓扑结构时刻处于变化状态：一方面，随时都可能有旧的通道被关闭，新的通道被打开，原本合法的通路可能因为没有及时通过而关闭，这时候就需要立即寻找新的通路；另一方面，由于每笔支付需求不同，各节点间的通道容量（可以理解为通道的直径）也会不同，除了在最初路由时将通道容量考虑在内之外，路由过程中有可能需要实时对支付进行拆分、合并操作，这些超越传统路由算法问题模型的业务逻辑需要更加细致的策略实现。

5.4.4. 完全匿名

为了增加闪电网络的隐私性和安全性，我们选择了一种基于Sphinx的用于掩盖所有来自中介路由数据的解决方案。参与闪电网络的节点只能看到与自己建立通道节点的相关交

易，对于闪电网络中的其他交易是完全无法感知的。同时在闪电网络的节点之间使用身份验证机制，防止中间人攻击。

5.4.5. 轻节点

按照BOLT协议，闪电网络的节点被设计为一个完整的比特币网络节点，这意味着加入网络的用户必须维护一个体积达几十GB的完整数据备份，这在实际使用中是不现实的。我们基于简易支付验证 (Simplified Payment Verification , SPV) 来设计LTXN的节点，并在此基础上添加了一些业务需要的数据记录，这样LTXN的节点不需要维护一个完整节点，也不需要存储整个网络中的全部用户交易，只需要存储与该节点建立通道的用户的相关交易即可。一旦通道关闭，交易在区块链主链得到确认，通道两端节点的余额就会写回主链，此时用户可以选择删除之前的交易数据来优化存储空间。优化后的LTXN节点不会占用太多的存储空间，一般的智能手机完全可以支持。

6. 应用场景

6.1. 日常消费场景

首先在不引入LITEX的情况下，我们讨论数字货币的消费场景是怎样的：

假设Alice只持有比特币，并且想从咖啡店老板Bob这里买到一杯咖啡。如果Bob只是一个对技术不太了解、不追新潮的普通商人，那么他拥有一个比特币钱包的概率几乎为0，这意味着Alice必须先把比特币兑换成法币，然后才能支付给Bob。Alice可以登录到一个数字货币交易所出售她的比特币，而为了尽快获得法币（Bob可能已经开始磨咖啡豆了），她需要以比较低的价格挂出，并支付相对不算低的交易费用。由于交易额度较小，即使Alice成功售出了比特币，交易到账时间也有可能长达数小时，而这时候咖啡已经凉透了。

经过上次失败的交易后，Bob对比特币有了一定的了解，他欣赏比特币的理念，但同时又不想因为接受比特币支付而承担币值波动风险，于是他接入了一家比特币支付网关提供商，这样一来虽然接受的是比特币支付，但最终到账的是支付网关兑换后的法币，看上去正常多了。Alice为了方便支付，也已经向这家支付网关进行了预充值（主网交易，需要较高手续费和较长的时间），所以这次比特币支付体验不错，Alice很快拿到了刚做好的咖啡。Bob登录到网关后台，打算把刚刚这笔5美元的交易提现，结果发现由于比特币主网交易手续费过高，支付网关将提现门槛改成了100美元！无奈中Bob只能等Alice买够20杯咖啡后才能提现了，这要等上至少20天——如果Alice每天都来的话。就在第19天的时候，Bob发现这家支付网关由于受到黑客的攻击丢失了大量的比特币和现金，宣告破产（中心化风险），自己的未提现95美元也成为泡影，这时Alice也向Bob抱怨说自己还没消费完的比特币也一并在这次事件中被黑客转走。

现在我们引入LITEX，感受去中心化的支付网络带来的便捷与安全。

Bob遭受了损失，但他并没有放弃比特币，于是他接入了新的技术方案LITEX。接入过程与其他支付网关（如Visa等）并没有什么不同，十分顺利，于是Bob通知Alice他又可以接受比特币支付了。Alice为了避免上次遭受的中心化风险，也成为了LITEX的用户，建立了属于自己的支付通道。于是她打开LITEX的客户端扫描了Bob的收款二维码，并直接输入咖啡的法币金额5美元，点击支付——1秒钟后，Bob的收银台提示收到一笔5美元的支付，Bob点击确认收款，发现5美金直接打到了他的账户里；Alice的手机此时也提示支付完成，等值5美元的比特币已从通道余额中扣除，手续费为0。在LITEX的帮助下，Alice非常便捷地使用比特币买到了一杯咖啡，并且没有付出任何手续费；Bob则实时地收到了比特币转换而来的法币，终于可以放心地继续接受比特币支付了。事实上，即使这时

LITEX收到攻击而损失部分节点，已经建立起的LTXN仍能完成Alice的支付需求；即使多数节点被破坏而导致支付失败，Alice和Bob的既有资产也都不会遭受损失。

6.2. 未来展望

由于通道的开启和关闭都需要成本，而保持通道开启会获得手续费收益，用户有很大意愿保持通道的开启，一方面这对整个网络联通性十分有益，另一方面也造成了用户的「资金沉淀」。如果基于智能合约的区块链理财项目蓬勃发展，我们就可以通过LITEX钱包向用户展示优质的理财项目，让用户的闲置资金产生额外收益，同时进一步提升用户保持通道开启的意愿，让网络更加健康。

7. 代币系统设计

7.1. 名称与设计目标

作为一个多角色共建的生态系统，LITEX需要一系列激励规则来确保系统的健康运转和快速发展，并将生态产生的全部价值回馈给全体参与者。为此LITEX设计了一种加密代币**LITEX Token**（简称**LXT**）来承载这一功能。

7.2. LXT体系

7.2.1. LXT的产生和消灭

LXT 基于以太坊智能合约 ERC20 标准生成，总数量为**20亿（2,000,000,000）**枚，由系统一次性配置完成，永不增发。LXT没有消灭机制。

7.2.2. 价值体系和激励方案

LXT 以 LITEX 生态中产生的交易手续费为价值基础。

设定支付交易额为P，兑换交易额为E，手续费计算函数为F，那么

- 商户手续费： $F_M = P * 2.5\%$
- 兑换手续费： $F_E = E * 1\%$

由于生态中的兑换总额跟支付总额一致（即P的总额与E的总额相等，记为T），因此LITEX 生态价值的计算公式为：

$$V = F_M + F_E = T * 3.5\%$$

LXT 作为系统激励按照生态中各方的贡献进行分配。

沿用上述设定并增加激励计算函数B（含义为其计算结果的等值 LXT 数额）以及通道流量FL，那么

- 消费激励： $B_C = P * 0.1\%$
- 收单方激励： $B_A = P * 1.5\%$
- 服务商激励： $B_{SP} = P * 1.0\%$
- 通道激励： $B_{CH} = FL * 0.2\%$
- 兑换激励： $B_E = E * 0.7\%$

由于生态中P、E和FL总额一致，依然统一记为T，因此 LITEX 的生态激励总额的计算公式为：

$$B = B_C + B_A + B_{SP} + B_{CH} + B_E = T * 3.5\%$$

可以计算出 LITEX 将生态价值的**100%** (B/V) 用于生态激励，LITEX 运营方定期将手续费用于从持币用户手中回购 LXT，重新注入 LITEX 生态。

7.3. LXT发行计划

数量	比例	用途	说明
700,000,000	35%	预售	面向早期投资人等，用于 LITEX 项目后续开发、人才招聘、市场推广等。 此部分资金的使用需要定期公示。
500,000,000	25%	用户激励	用于激励生态参与者下载、使用、推广 LITEX 钱包下载、以及生态内的支付、转账等行为。
400,000,000	20%	发展基金	用于 LITEX 生态建设，在各国发展合作伙伴等。 此部分资金的使用需要基金会决议，并提前公示。
300,000,000	15%	创始团队	回报创始团队在数字货币领域的探索 and 开发以及今后维护 LITEX 等产品技术和运营发展作出的努力。 代币发行时此部分将被智能合约锁定，1个月后解锁，每月解锁此部分的1/36，分36个月解锁完成。
100,000,000	5%	合作机构	用于回报现有合作机构以及建立相关企业的合作。 代币发行时被智能合约锁定，上交易所后第一个月开始，每月解锁此部分的20%，分5个月解锁完成。

8. 项目规划

步骤	时间	计划
第一阶段	2017Q4	系统架构设计； BOLT协议基础功能实现与测试； 收单方接洽
第二阶段	2018Q1-2018Q2	LITEX 支付APP上线； LTXN 架构完成； 收单方、服务商接入测试
第三阶段	2018Q3-2018Q4	LTXN Alpha版本上线测试； LITEX 支付App接入跨链能力； 商户接入测试； 拓展合作收单方； 交易试运行
第四阶段	2019Q1-2019Q2	LTXN Beta版本上线，完成安全测试； LITEX 支付App 全能力开放； 进一步拓展收单方
第五阶段	2019Q3-2019Q4	APP与LTXN持续迭代； 商户大规模接入； 持续拓展收单合作，增强收单服务的稳定性

9. 组织架构介绍

9.1. LITEX 社区基金会

LITEX 社区基金会设立于新加坡，该机构是 LITEX 社区的法律主体，负责 LITEX 的技术研发、业务运营和市场推广，同时承担所有对 LITEX 的法律责任。

LITEX 基金会设立有决策委员会作为最高决策机构行使管理和约束基金会各执行机构的权利。决策委员会任期 3 年，任期满后将由 LITEX 社区选举产生。

下属各执行部门：

- 技术部

主要负责 LITEX 社区开源项目的技术路线制定、方案选型、架构设计、项目研发和管理、Github 代码库更新和维护等工作。

- 运营部

主要负责 LITEX 用户社区的运营和管理，包括社区活动策划、活动执行和社区激励计划的执行等工作。

- 市场部

主要负责社区品牌传播和商业拓展，完善社区生态建设。

- 人事财务部

主要负责 LITEX 基金会志愿者招募，管理基金会成员日常财务相关事务管理。

9.2. 核心团队

- **Guanghong Xu**

毕业于北京大学数学系密码学专业、伊州理工应用数学和电脑科学专业，研究方向为PKI加密体系。曾在VeriSign做数字认证相关工作、在Deloitte德勤任风险策略和信息安全顾问，参与过VISA在美国IPO时的支付信息加密合规认证，以及苹果、艺电(EA)、博通(Broadcom)等企业的信息加密和数字认证体系等顶级全球项目，现任Kaiser企业风险战略总监，具有丰富的密码学和商业应用经验。

9.3. 合作伙伴团队

- **王硕斌**

北京大学计算机系本科 (2003-2007) 硕士 (2007-2010)，全球最大的去中心化支付产品——易宝「非银行卡支付」产品运营负责人，连续创业者，北京大学CEO俱乐部执行理事，区块链技术信仰者和实践者。

- **张化强**

北京大学计算机系本科 (2003-2007) 硕士 (2007-2010)，区块链专家，网络安全专家，全栈工程师，「复合决策闪电网络」模型设计者，曾就职于IBM、新浪微博等平台担任高级研发工程师。

- **娄焕庆**

北京大学计算机系本科 (2007-2011) 硕士 (2011-2014)，区块链专家，项目架构师，全栈工程师，有丰富的项目经验，擅长结合产品需求和前沿技术设计解决方案。

- **褚天舒**

哆啦宝创始合伙人兼产品副总裁，原易宝支付非银行卡项目高级产品运营，曾任百度身边创始团队产品经理。北京航空航天大学计算机科学与技术专业学士，硕士。

哆啦宝是国内领先的线下支付营销企业，排名前三的微信支付服务商。每天支付成交超过200万笔。

9.4. 基石投资人及顾问

- **余晨** - 投资人

易宝支付联合创始人、总裁。毕业于北京大学计算机系，在互联网、电子商务和软件领域有20年的经验，曾荣获『中国手机圈影响力金英奖100人』荣誉榜单以及eWorld 2013电子商务世界『2013年度EC100中国电商营销百人风云会风云人物』。畅销书《看见未来：改变互联网世界的人们》作者。

- **常大维** - 投资人

哆啦宝创始人兼CEO，原易宝支付创始人兼CTO，曾任硅谷Riverside公司高级软件工程师。北京大学物理学学士，马里兰大学计算机工程硕士，美国硅谷华人工程师协会会员。

- **陈斌** - 顾问

前PayPal资深架构师。1989年获得吉林大学硕士学位，曾任日立美国系统集成总监、Abacus首席架构师、Nokia美国互联网应用首席工程师，丰富的海外经历，多年的支付行业架构经验。曾翻译出版《架构及未来》、《架构真经》和《数据即未来-大数据王者之道》，是最前沿技术的实践者和布道者。

10. 风险声明

10.1. 风险提示

LITEX 基金会认为，在 LITEX 的开发、维护和运营过程中存在众多风险，这其中很多都超出了 LITEX 基金会的控制。每个 LXT 代币参与者应仔细阅读、理解并考虑下述风险，慎重决定是否参与代币互换计划。若参与到 LXT 代币互换计划则将视参与者已充分知晓并同意接受下述风险：

- 法律政策和监管风险

加密货币正在被或可能被各个不同国家的主管机关所监管。在各个不同国家，LXT 可能随时被定义为虚拟商品、数字资产或甚至是证券或货币，因此在某些国家之中按当地监管要求，LXT 可能被禁止交易或持有。如果监管主体出台相关规定，LITEX 基金会可能被勒令暂停或终止任何关于本次代币互换计划。LITEX 的开发、营销、宣传或其他方面也可能受到严重影响、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 LITEX 或本次公开售卖计划的监管许可或容忍可能只是暂时的。本次 LXT 公开互换计划若被提前终止，此时持有者可能由于以太币的价格波动以及 LITEX 基金会的支出而仅被部分退还其支付的金额。

- 项目团队风险

当前区块链技术领域团队、项目众多，竞争激烈，存在较强的市场竞争和项目运营压力。LITEX 项目能否在诸多优秀项目中突围，受到广泛认可，既与自身团队能力、愿景规划等相关，也受到市场竞争影响，包括可能面临恶性竞争。LITEX 社区核心成员拥有多年的保险行业及区块链技术积累，可以凝聚起更多在区块链技术领域和保险领域的人才加入社区，但也不能排除会有社区核心人员离开、内部发生冲突等导致 LITEX 项目整体受到负面影响的可能性。

- 技术风险

计算机技术正在不断发展，密码学正在不断进步，无法保证任何时候绝对的安全性，这可能导致持有人的 LXT 被盗、失窃、消失、毁灭或贬值。尽管 LITEX 基金会会努力维护 LITEX 网络的安全，但并不能保证 LITEX 不存在弱点或权限，且任何人均有可能故意或无意地将弱点或缺陷带入 LITEX 的核心基础设施要素之中，对这些弱点或缺陷 LITEX 基金会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 LXT 或其他数字代币丢失。此外，LITEX 的源代码可能存在某些瑕疵、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

LITEX 的可用性、稳定性和/或安全性，并因此对 LXT 的价值造成负面影响。公开的源代码以透明为根本，以促进源自于社区的对代码的鉴定和问题解决。LITEX 基金会将与 LITEX 社区紧密合作，今后持续改进、优化和完善 LITEX 的源代码。LITEX 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网络内届时节点所能提供的负载，则 LITEX 网络可能会瘫痪或停滞，且可能会产生错误交易。在最坏情况下，任何人持有的 LXT 可能会丢失。这些事件将可能损害 LITEX 的可使用性、稳定性和安全性以及 LXT 的价值。此外 LITEX 仍在开发阶段，由于 LITEX 系统的技术复杂性，LITEX 基金会可能不时会面临无法预测或无法克服的困难。因此，LITEX 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 LXT 无法交付给本次互换计划的参与者。

- 安全风险

来自外部的攻击将可能使 LITEX 系统遭受负面影响、停滞、瘫痪甚至计算错误，并因此导致在此之上的交易被延迟甚至暂时无法执行，也可能造成数据错误、崩溃或丢失，损害 LITEX 的可用性、可靠性、安全性以及 LXT 的价值。此外，可能会有人企图盗窃 LITEX 基金会所收到的公开售卖所获资金(包括已转换成法币的部分)。该类盗窃或盗窃企图可能会影响 LITEX 基金会为 LITEX 开发提供资金的能力。尽管 LITEX 基金会将会采取措施保护众筹资金的安全，但盗窃仍很难被彻底阻止。

- 其他可能的风险

- 源代码升级风险

LITEX 的源代码是开源的且可能被 LITEX 社区任何成员不时升级、修正、修改或更改。任何人均无法预料或保证某项升级、修正、修改或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料或非预期的结果，从而对 LITEX 的运行或 LXT 的价值造成重大不利影响。

- 未经授权认领 LXT 的风险

任何通过解密或破解 LXT 持有者密码而获得注册邮箱或注册账号访问权限的人士，将能够恶意获取 LXT 持有者的 LXT 代币。据此，持有者的 LXT 代币可能会被发送至其他人的 LXT 地址，而这种发送是不可撤销、不可逆转的。每个 LXT 持有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)使复杂、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以及其他相关安全措施。

- 市场风险:

LXT 的价值很大程度上取决于 LITEX 平台的市场发展和用户接受程度。LITEX 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，LITEX 甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大一部分 LXT 需求可能具有投机性质。缺乏用户可能导致 LXT 市场价格波动增大从而影响 LITEX 的长期发展。出现这种价格波动时，LITEX 不会也没有责任稳定或影响 LXT 的市场价格。

- 流动性风险

LXT 既不是任何个人、实体、中央银行或国家组织发行的货币，也没有任何硬资产或被其他信用所支持。LXT 在市场上的流通和交易并不是 LITEX 基金会的职责或追求。LXT 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 LXT 持有者处兑换任何 LXT，也没有任何人士能够在任何程度上保证任何时刻 LXT 的流通性或市场价格。LXT 持有者若要转让 LXT，该 LXT 持有者需寻找一名或多名有意人士进行互换。该过程可能花费甚巨、耗时长并且最终可能并不成功。此外，可能没有加密货币交易所或其他市场上线 LXT 供公开交易。

- 价格波动风险

若在公开市场上交易，加密货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、以太坊、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它客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 LXT 交易的二级市场，LITEX 基金会对任何二级市场的 LXT 交易不承担责任也没有义务稳定 LXT 的价格波动，且对此也并不关心。LXT 交易价格所涉风险需由 LXT 交易者自行承担。

- 竞争风险

LITEX 的底层协议是基于开源电脑软件。没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用 LITEX 的源代码或底层协议，以开发具有竞争性的协议、软件、系统、虚拟平台、虚拟机或智能合约从而与 LITEX 竞争，或甚至赶超或取代 LITEX，LITEX 基金会对此无法控制。LITEX 基金会在任何情况下均不可能消除、防止、限制或降低这种旨在与 LITEX 竞争或取代 LITEX 的竞争性努力。

- 信息披露不足风险

截止到本白皮书发布日，LITEX 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 LITEX 最新的关键信息，其并不绝对完整，且仍会被 LITEX 基金会为了特定目的而不时进行调整和更新。LITEX 基金会无能力且无义务随时告知参与者 LITEX 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)，因此必然会让持有者未能及时且充分地接触到 LITEX 开发中新产生的信息。信息披露的充分是可避免且合乎情理的。

10.2. 免责声明

本白皮书仅作为传达信息之用，文档内容仅供参考，不构成出售数字商品、股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。本文档内容不得被解释为强迫参与互换。任何与本白皮书相关的行为均不得视为参与互换，包括要求获取本白皮书的副本或向他人分享本白皮书。参与互换则代表参与者已达到年龄标准，具备完整的民事行为能力，与 LITEX 基金会签订的合同是真实有效的。所有参与者均为自愿签订合同，并在签订合同之前对 LITEX 进行了清晰必要的了解。

LITEX 基金会将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，LITEX 基金会将通过在网站上发布公告或新版白皮书等方式，将更新内容公布于众。请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。LITEX 基金会概不承担参与者因：(i)依赖本文档内容、(ii)本文信息不准确之处，以及(iii)本文导致的任何行为而造成的损失。LITEX 基金会将不遗余力实现文档中所提及的目标，然而基于不可抗力力的存在，LITEX 基金会不能完全做出完成承诺。

LXT 是平台发生效能的重要工具，并不是一种投资品。拥有 LXT 不代表授予其拥有者对 LITEX 平台的所有权、控制权、决策权。LXT 作为一种加密代币不属于以下类别：(a)任何种类的货币；(b)证券；(c)法律实体的股权；(d)股票、债券、票据、认股权证、证书或其他授予任何权利的文书。

LXT 的增值与否取决于市场规律以及应用落地后的需求，其可能不具备任何价值，LITEX 基金会不对其增值做出承诺，并对其因价值增减所造成的后果概不负责。在适用法律允许的最大范围内，对因参与互换所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其它经济损失，LITEX 基金会不承担责

任。LITEX 平台遵守任何有利于行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时，参与者披露用以完成此类检查的所有信息必须完整准确。LITEX 平台明确向参与者传达了可能的风险，参与者一旦参与互换，代表其已确认理解并认可细则中的各项条款说明，接受本平台的潜在风险，后果自担。