LITEX - 打造消费级 Layer 2 应用框架

摘要

LITEX 是一整套面向消费级区块链应用的 Layer2 框架，整个框架主要分成两个部分：链上合约和链下协议。链上合约用于在共识层固定状态和逻辑，提供包括支付通道合约、业务验证合约等多种合约模板，是规则公示平台；链下协议用于处理链下数据的组织、传递和验证，提供数据公信力，提供数据协议和验证协议，是规则执行平台。

LITEX 真正地从终端用户的角度出发，为开发者提供了一套可验证、低门槛、用户友好、开发自由的产品技术方案。本文简述了 LITEX 的设计理念、系统架构、加密经济模型，以及在 LITEX 框架下开发区块链应用的最佳实践。

目录

愿景

区块链是一个高认知门槛的领域，诞生至今引发了很多社会实验，但是一直没有出现能够在主流用户群中普及的应用。究其原因，公链的设计目标在于达成尽量广泛的共识，而共识节点越多，性能就越低下，无法支撑大规模用户量的产品。在解决公链性能问题的方向上，分层设计的思想逐渐占据主流，催生了很多 Layer 2 解决方案，但是用户门槛依然高企，无法支撑消费级应用场景。

消费级产品是我们日常生活中接触最多的产品类型，它们目标是在满足主流消费者需求的前提下尽可能地降低价格成本和使用成本。与之相对的是工业级产品，它们一般需要满足较为严苛的需求设计，注重性能，而在成本、易用性等方面不会做过多的考量。举例来说，消费级路由器体积小、能耗低，配置引导人性化，还具有交换机和 AP 能力，价格只需几十元；相比之下，工业级路由器的路由能力强大，安全性高，但是体积庞大，能耗高，操作复杂（需要专业人员编写代码进行配置），价格从几万元到上百万元不等。不难发现，如果没有工业级路由器到消费级路由器的演化，互联网将很难像今天一样普及。

比特币作为最早的区块链应用，提供点对点的加密货币支付功能；以太坊则更进一步，提供去中心化的智能合约平台服务。作为底层公链，全球共识是它们的价值基础，共识越强越广泛就意味着全球有越多的节点参与数据的同步和校验，而这必将导致处理效率的降低，无法支撑消费级应用场景。与之相悖的，加密经济的发展离不开基础用户群体的扩充，为了吸引更多人加入，加密世界必须不断扩充场景，降低门槛，而这依赖于大量的消费级应用的出现。

消费级应用的诞生依赖于较高的 TPS，较低的转账手续费，较低的用户使用门槛，与此同时我们又不能完全舍弃区块链技术带来的去中心化和安全的属性。这个时候我们就遇到了区块链技术中常说的不可能三角问题，安全、去中心化、效率，三者不可兼得。这个时候如果我们还是希望通过不断加入新的功能、新的设计，在同一层上解决不可能三角问题，整个问题就会变得相当复杂，这不利于我们理解和剖析事物，分析出事物的内在规律。而且如果我们把所有的步骤、所有的功能都放到同一层处理的话，这一层会变得越来越复杂，耦合度非常高，今后的修改和升级都会非常困难，这对于实际存储价值的区块链是无法接受的。

任何问题到了某个复杂的阶段，如果当前方法不能解决，往往可以通过多加一层的思路来解决，在计算机中分层是一种非常常见的思想，TCP/IP 有四层结构，OSI 模型则有七层结构，而我们最常接触到的计算机存储也分成了一级缓存、二级缓存、内存和硬盘四层。

公链作为共识的载体，能否累积共识成为价值存储网络，最重要的两个因素就是安全和去中心化。安全性决定了公链能够承载多大的价值，一条公链无法沉淀高于其攻击成本的价值；而去中心化，决定了公链能不能成为一个更广泛的抗审查的价值网络，安全和去中心化是区块链的价值基础，我们应该让公链维持好这一点，而把性能、隐私等应用相关的问题放在上一层解决，只有这样才能做出基于区块链的消费级产品 —— 这就是区块链的分层思想。

为了解决底层公链（Layer 1）的性能问题，开发者们从分层的角度设计了一系列上层（Layer 2）的解决方案。Layer 2 是一种设计模式，它倡导把不需要全局共识的业务逻辑放到链下，只在需要结算或仲裁

的时候才提交到链上进行共识，闪电网络（Lightning Network）、状态通道（State Channel）、Plasma 等都属于 Layer 2 解决方案。

但是，这些方案的设计十分复杂，无论是开发者实现的难度还是普通用户使用的门槛都非常高，至今无法满足大规模消费级应用的需求。通过调研我们发现，当前 Layer 2 方案过于复杂的设计很大程度上是为了追求全面的安全、隐私、完全去中心化等目标，而对用户的使用成本并没有过多考量，这表明它们的定位仍然是「工业级」解决方案，而非面向「消费级」应用的支撑框架。

我们认为，加密经济需要消费级应用，Layer 2 方案的设计也需要从普通用户的角度出发进行取舍。因此我们设计了 LITEX，希望为开发者提供一套更加「接地气」的 Layer 2 解决方案，极大地降低普通用户的认知和使用门槛，催生更多消费级区块链应用，推动加密经济迎来蓬勃发展。

概述

LITEX 是一整套面向消费级区块链应用的 Layer 2 框架。基于 LITEX，开发者可以低门槛地产创建出大量用户友好的区块链应用，让用户既能够获得如互联网产品般简单易用的体验，又可以享受到区块链技术带来的资产安全、高流动性、公开透明等特性。

产品上，LITEX 将消费级区块链应用拆分为加密支付和业务逻辑两部分。加密支付涉及用户资产，需要密码学级别的安全保障，LITEX 将采用支付通道方案保证用户资产安全，还提供代币聚合、无感升级、交易可读，单双向通道可选等功能，用户在实际使用时，将无法感知加密支付与电子支付的差异。在业务逻辑部分，需要足够的灵活性和兼容性，以匹配不同业务复杂多样的逻辑需求，对此 LITEX 提出了链上验证、链外仲裁的设计模式，大幅降低开发者的开发难度和用户的使用门槛。

技术上，LITEX 对于加密支付和业务逻辑两部分，分别开发了支付通道合约和业务验证合约，目前合约的开发主要基于以太坊，未来可以扩展到任何支持智能合约的公链。其中支付通道合约已经支持在单个合约内同时开启 ETH 和所有 ERC-20 类型代币的支付通道；业务验证合约给出了游戏类应用的模板的设计，能够向用户展示易读、支持回放的链上验证结果，接下来 LITEX 还将在金融产品领域，Dapp 领域给出多个设计实例。

商业上，LITEX 始终坚信一款消费级应用的用户操作数据、用户活跃度、资金转移等数据对开发者和用户都具有极大的参考价值，有了这些数据才能够建立起用户和应用之间的正向反馈。为此，LITEX 采用了 pBFT 共识的许可链承载链下数据，让原本点对点、只有交易双

方确知的链下数据具有了公信力，让在此之上建立的商业生态更有活力。

在 LITEX 的帮助下，开发者可用自己熟悉的技术栈实现业务逻辑，只需要把有作恶风险的关键逻辑用验证合约的形式进行链上声明，就可以保证应用整体的公开透明，做到高效、可验证；支付层面上，用户既能够获得 Layer 2 技术加持下「提速降费」的支付体验，又可以随时通过关闭支付通道行使自己的资金所有权，无需担心未使用的资金被开发者扣留。基于 LITEX 框架的区块链应用在用户体验上比肩互联网应用，而且一旦对链下数据有疑议，用户可以方便地进行链上验证，这与很多打着区块链旗号却没有用到任何区块链特性的「伪区块链应用」有着本质区别。

区块链分层：Layer 2 设计思想

近年来，针对公链性能问题，业界提出了很多种扩容方案，主要分为链上扩容和链下扩容两大类。链上扩容方案试图通过直接修改共识协议达成扩容的效果，如增大区块、缩短出块间隔时间、更改共识算法、使用分片技术等，称为 Layer 1 层面的扩容方案；链下扩容方案则不谋求对底层公链的共识进行升级，而是通过链上合约与链下协议相配合的方式，将不必要全局共识的操作在链下完成，只在结算或需要仲裁的时候才提交到链上进行状态的共识，称为 Layer 2 扩容方案。

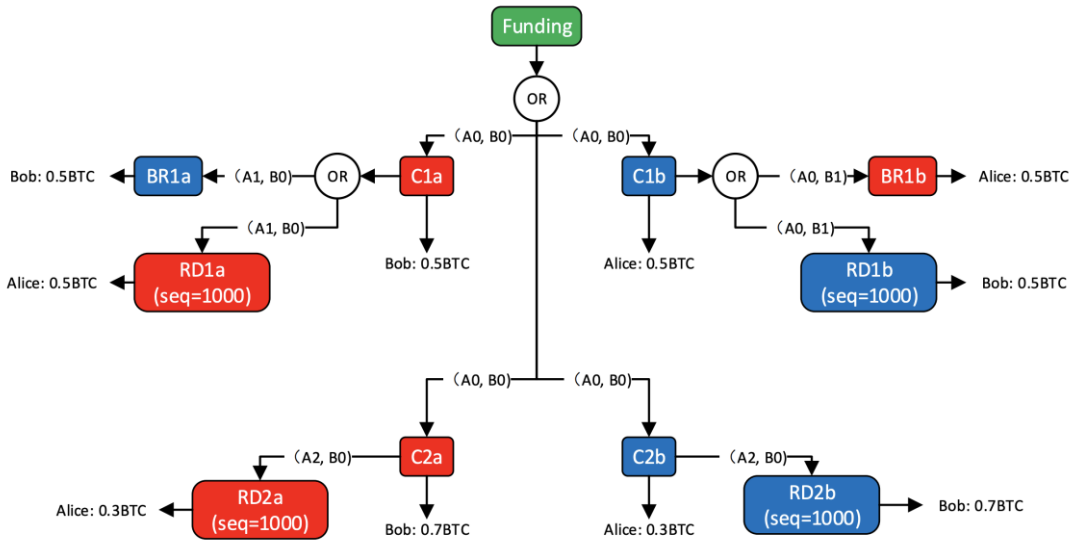
不难想到，Layer 1 扩容方案需要让全体参与者重新达成共识，新的共识也需要经历足够长期的检验，这无疑是非常艰难和缓慢的；即使最终能够达成共识，Layer 1 层面上的能购进行的改进也比较有限：要么提升节点吞吐量，要么提升并行程度。提升吞吐量势必对节点的硬件配置和网络带宽带来更高的要求，加剧中心化程度，而提升并行度需要借助的分片技术极为复杂，在去中心化的架构下更是容易出现各种问题，难度高、风险大、推进缓慢。

相对地，Layer 2 扩容方案认可 Layer 1 在全球范围内达成的共识价值，不期望修改共识，而是追求一种更加优化的方式来利用这种全局共识。同时，人们注意到不同的共识范围在安全和效率上拥有不同的平衡点，Layer 2 的设计者完全可以根据需求来限定共识范围，从而达成符合需求的扩容效果。例如小额支付场景下，收付双方对最终资金分配达成共识即可，共识范围限制在两者之间，效率极高，支付通道技术就是针对这种场景的解决方案。目前主流的 Layer 2 技术有如下几种：

闪电网络

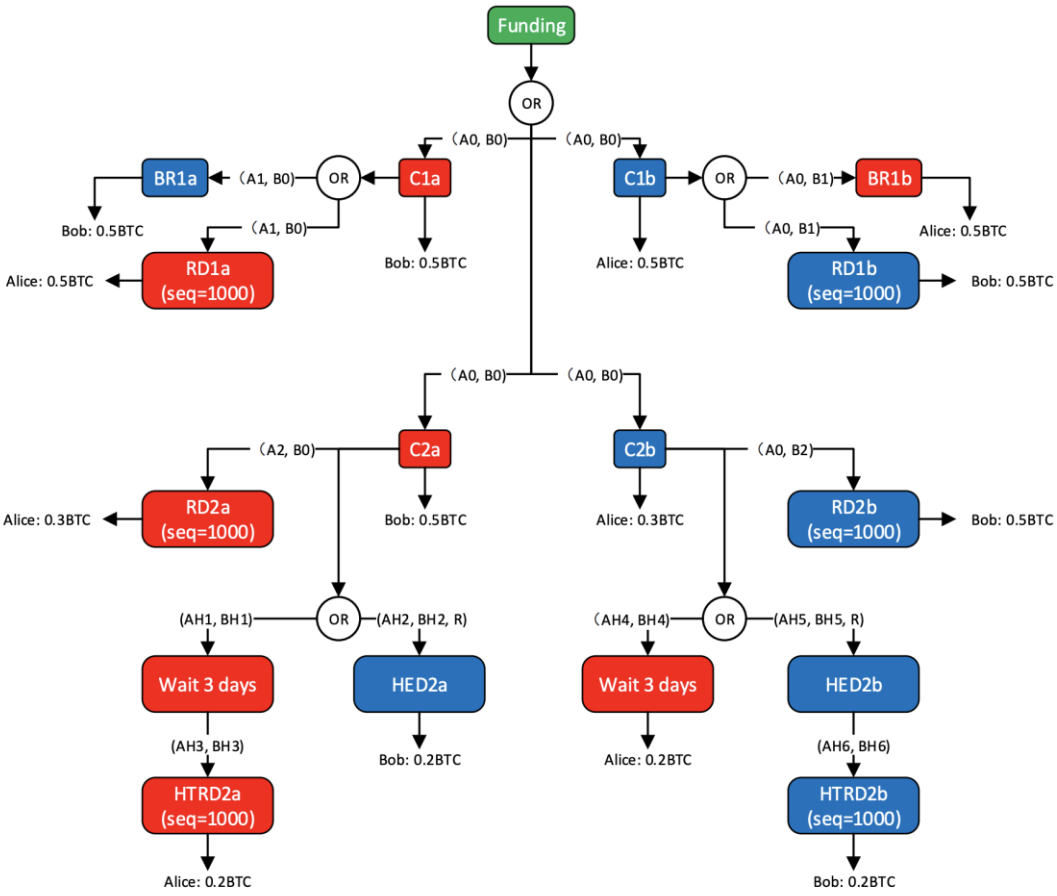
闪电网络是基于 BOLT 协议实现的比特币链下转账网络的统称。闪电网络是一个分布式网络，通过智能合约支持多方的即时、高密度的微支付，结合区块链技术消除将资金委托第三方可能带来的风险。闪电网络本质上是使用了序列到期可撤销合约（RSMC）和哈希时间锁定合约（HTLC）来安全地进行零确认交易的一种机制。需要开通支付通道的双方，共同预存一部分资金到支付通道内，之后双方进行交易时，不需要将每次交易提交到链上，仅需双方在链下对每笔交易进行签名确认即可。当需要关闭支付通道时，仅需将最终交易结果提交到区块链上，被最终确认即可，之前进行的多次链下交易将不再占用区块链资源，因此闪电网络上的交易具有速度快、成本低、即时确认的特点。

闪电网络主要由两部分组成，第一部分是双向支付通道的建立，即 RSMC（序列到期可撤销合约），RSMC 实现了两个人之间可以开通双向支付通道，并且可以在无第三方的情况下在链下完成安全的随时可终止的交易方案。



RSMC（Revocable Sequence Maturity Contract）

第二部分是 HTLC (哈希时间锁定合约)，HTLC 实现了两个尚未开通双向支付通道的人，可以经过多个中间方建立起一条支付通道来完成链下转账交易。这两个类型的合约进行组合构成了闪电网络，从而实现任意两个开通了闪电网络功能的人都可以在链下完成交易。

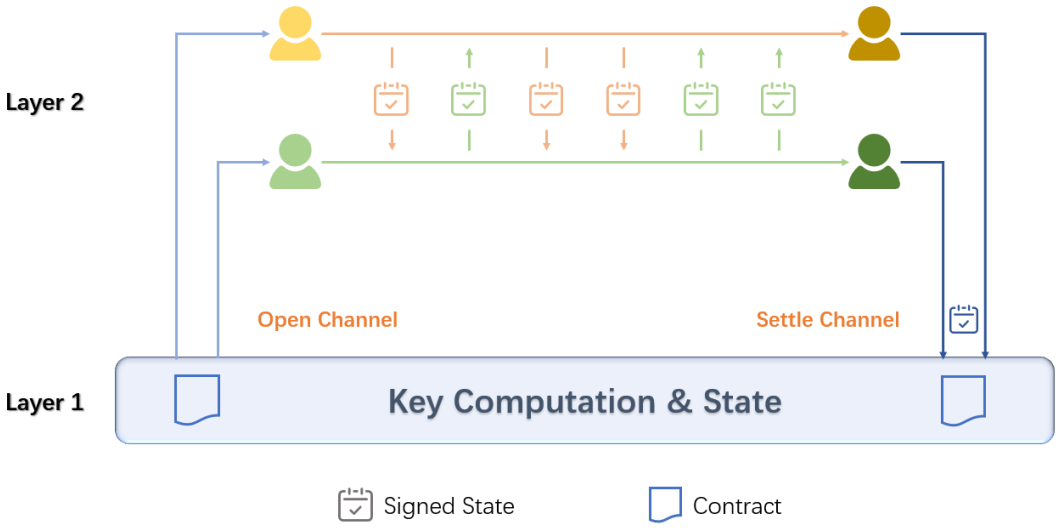


HTLC（Hashed Timelock Contract)

状态通道

状态通道是用于执行交易和其他状态更新的一种链下扩容技术，是支付通道的升级版，状态通道不仅可以用于支付，还可以用于区块链上进行的任意的状态更新。状态通道的本质是通过在不同的用户之

间或者用户和服务之间建立起一个双向的通道，在不同的实体之间提供状态维护的服务。



State Channel

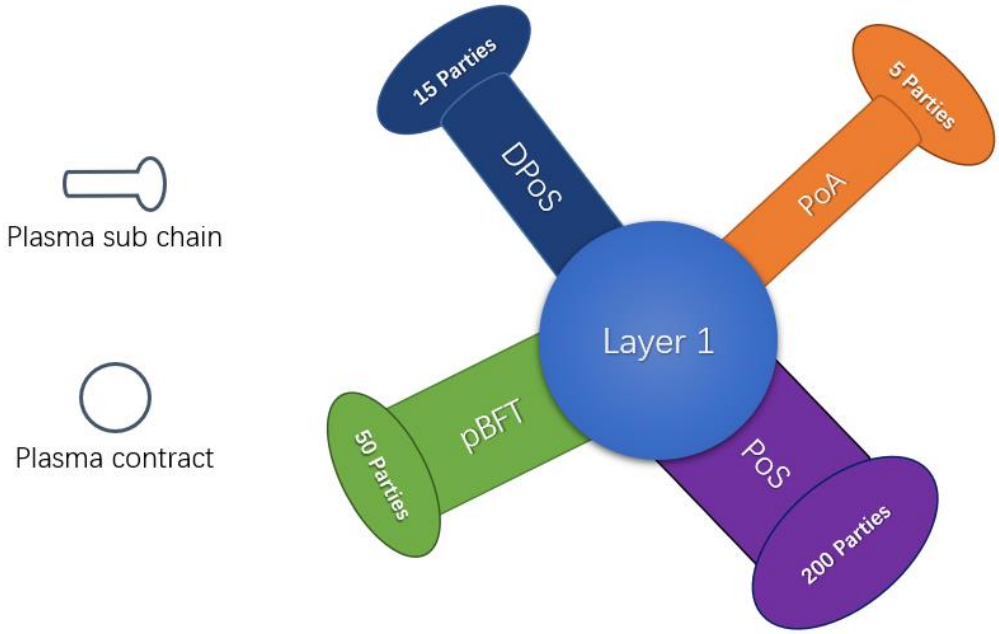
状态通道的使用流程和支付通道是比较一致的，主要包括：

- 打开通道，两个或者多个参与者需要就初始的状态达成一致，然后双方或者多方将某些状态或者一定数量的代币存入状态通道的托管合约内，然后状态通道即为开启。
- 使用通道，在开启状态通道的两者或者多个参与者间，用户之间可以在链下进行交易和状态的签名和转移，不需要将每一次状态更改都提交到链上。
- 关闭通道，当某一方需要关闭通道时，需要提交有效的状态更新到链上，然后会进入一段挑战期，在挑战期内状态通道的两边的参与者都可以随时提交序列号更高的状态更新，防止用户作恶。在挑战期结束后，具有最高序列号的有效状态即被确认为最终状态，被主链记录并结算。

状态通道允许用户将区块链上的许多操作转移到链外，用户只需在链下进行通讯签名即可不必再等待链上交易确认，待到链外操作完成多方签名确认后，提交最终的状态结果到主链上进行结算即可。

Plasma

Plasma 是由 Vitalik 和 Joseph Poon 于 2017 年 8 月发布的一种基于以太坊的链下扩容方案。Plasma 是一系列在根链上运行的自动智能合约，用户可以将自己在根链上的资产锁定在一个根链的智能合约中，然后将资产映射到对应的 Plasma 链上，Plasma 链会由一位或者多为验证者共同运行维护，根链上的合约会要求 Plasma 链将每一个区块的 Merkel Root 提交到根链上，作为欺诈证明，只有完成提交证明的 Plasma 区块才是确认有效的。

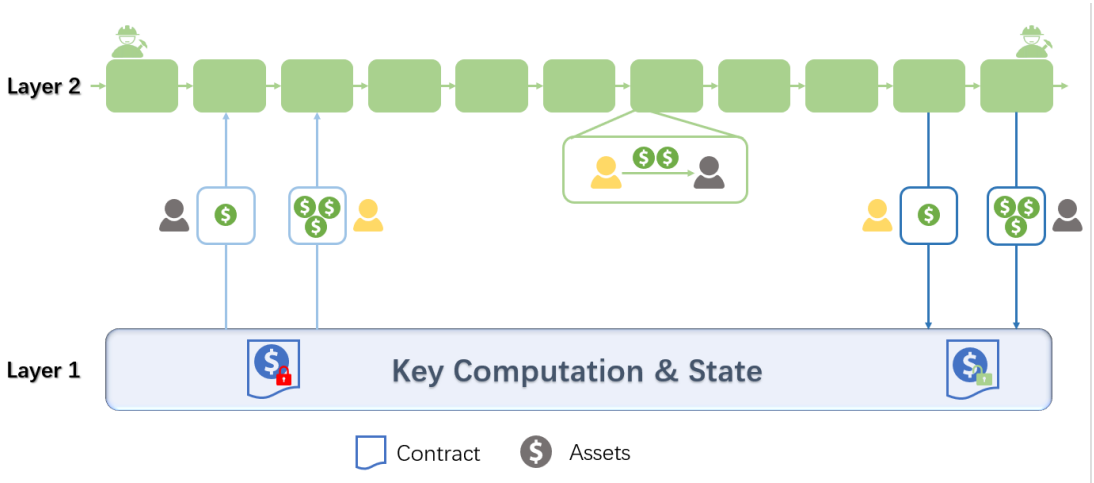


Plasma Overview

Plasma 上的用户可以通过保存的 Merkle Proof 来验证 Merkel Root 的有效性，确保子链运行的安全性，当用户想从 Plasma 链上退出时，只需要向根链提交合约证明，就可以将自己的资产从 Plasma 链上撤回到根链上去。并且为了保证 Plasma 链上的验证者不会作恶，验证者需要锁定一部分保证金在根链的智能合约中，一旦 Plasma 上出现仲裁，诚实的一方提交相关交易的有序历史的明确证明，作恶的 Plasma 验证者的保证金就会被扣除。

侧链

侧链是一条独立的链，侧链和主链之间通过侧链协议，允许资产可以从主链安全地转移到侧链上，然后在侧链上完成一系列的交易转账，并最终可以安全地返回主链。侧链和 Plasma 之间的主要区别在于，Plasma 是非保管特性的侧链，在 Plasma 链上出现任何问题时，用户检测到错误，可以提交仲裁安全地退出 Plasma 链，将资产转移回主链。而侧链的安全性需要由侧链自身保证，用户转移到侧链上的资产在受到攻击时，无法安全地退回主链。



Side Chain

侧链和主链间主要通过双向锚定技术实现资产转移，即用户需要在主链上把一定的数字资产发送到一个特定地址，该笔数字会被锁定，同时，提交这笔资产锁定的证据，当侧链检查到这个证据的时候，侧链上就会释放等量的数字资产，然后用户就可以在侧链上进行交易转账了。双向锚定有多种实现方式，按照中心化到去中心化的排序依次有：单一托管模式，联盟托管模式，SPV 简单支付验证 等方式。

总结

这些常见的 Layer 2 方案看上去实现各不相同，设计也比较复杂难懂，但是如果我们在理解的基础上，深入挖掘一下它们背后的设计思想，就能够找到一些共性：

首先，它们的链下数据都是由参与方各自进行数字签名的方式进行密码学保真，保证没有人能伪造别人的链下数据；

其次，链下数据格式都由链上的合约进行定义，确保在提交链上结算或仲裁时能够被合约承认；

再次，无论是闪电网络和状态通道的松散存储、点对点传输，还是 Plasma 和侧链这样的链式存储、广播传输，本质上都是对链下数据进行不同形式的组织和传输，针对的是不同的应用场景；

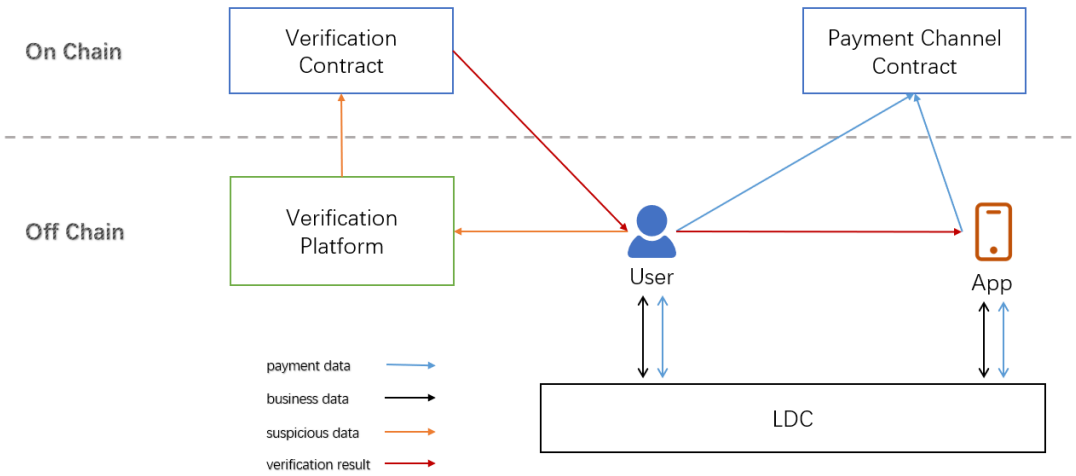
最后，在需要结算或仲裁的时候，它们的方式都是要求用户将对自身有利的链下数据提交给链上合约进行共识和固定，完成状态和资产的回归。

通过上面的共性分析不难得到这样的结论：Layer 2 其实是一种设计模式。这些方案在本质上都是将公链看做底层的共识载体，把对应用的支撑提升到上层实现，这就是区块链分层的思想。因此我们认为，

分层思想是区块链技术触达普通用户日常生活的最佳路径，也是最符合商业逻辑和用户认知的架构设计。

LITEX 架构

LITEX 结构上分为两大部分：链上合约和链下协议。链上合约包含支付通道合约、业务验证合约等，用于在共识层固定状态和逻辑；链下协议用于处理链下数据的组织、传递和验证，同时提供足够的数据公信力。此外，LITEX 还提供了方便普通用户进行数据查询、提交和链上验证的一系列工具，如 Layer 2 交易浏览器、业务验证平台、流程回放工具等。这些工具和协议的代码都将开源，任何个人或者团队都可以在此基础上搭建或者二次开发适合自己的数据查询和验证工具。



LITEX Overview

LITEX 作为 Layer 2 层应用框架，可以适配多种 Layer 1 层公链。为了方便理解，本文将统一使用以太坊作为基础链来描述 LITEX 的产品技术方案。

链上合约

支付通道合约

LITEX 的支付通道是在状态通道的基础上，根据消费级场景进行深度定制的一系列通道合约组合。功能上，除了基本的开关通道、充值提现和资产保全（强制关闭通道）等功能外，还具备代币聚合、无感升级、可读交易等独有的特点；类型上，根据场景不同，分为单向通道和双向通道两种，能够更好地满足不同的商业场景需求。

- **开关通道 / 充值提现 / 资产保全**

为了方便理解，我们把加密世界的资产体系映射到现实世界：

首先我们发现这个世界没有现金，所有资产都是数字化的，并且由一个可信的银行（公链）来记账，每个人的 ID（公链地址）对应一个账户余额（链上资产）。一开始，人们的资金往来必须去银行进行汇款（链上转账），手续费很高而且速度很慢；后来，银行推出了一种储值卡（支付通道），持卡人互相转账的手续费极低且速度飞快。用户开卡（开通道）时要预存一些资金到卡里，余额不足时可以从账户内转到卡里（充值），余额过多时可以从卡里转回账户（提现）；不需要这张卡时可以销卡（关通道），卡内没用完的资金会退回银行账户。

那么资产保全如何体现？在现实世界中，银行由国家背书，信用很高，既不会擅自动用你卡内的资金，也不会在销卡时扣留余额（当然，特殊情况除外）。在加密世界中，信任是由公链提供的，只要用户能够用私钥签名证明自己的身份，任何第三方都无法阻拦用户的提现或者退款操作，这就是强制关闭通道，它给予了支付通道对资产的保全能力，可以保证用户资产安全。

- **代币聚合**

LITEX 能够使用同一个合约承载以太坊原生代币 ETH 以及所有 ERC-20 代币的支付通道，这就是 LITEX 支付通道的代币聚合能力。代币聚合让 LITEX 的支付通道入口具有唯一性，这在商业环境中非常重要，因为用户可以非常轻松地判断出自己开通道的目标地址指向的是官方合约还是恶意的钓鱼合约，从而在资产安全上更加放心。借助 ENS 等去中心化的地址映射服务，LITEX 还可以将支付合约地址公示为类似 pay.litex.eth 这样更加易读易记的域名，进一步降低用户的使用门槛，提升安全感。

- **无感升级**

智能合约具有不可篡改的特性，这产生了信任，但也埋下了隐患。没有开发人员能保证自己的代码不出问题，也没有产品经理敢断言自己的设计能够满足未来的所有需求，因此可维护、易维护是消费级产品必备的基本功。如果产品升级需要所有用户付出较大的时间成本和金钱成本，甚至影响到合作伙伴的业务运行，那么它的设计无疑是失败的。

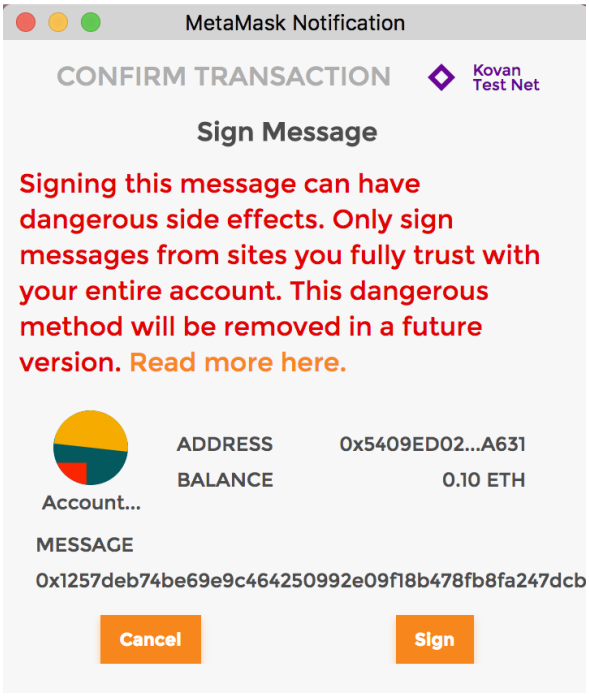
LITEX 的支付通道合约采用了代理（Delegate Call）技术，能够在不改变合约地址的情况下对合约逻辑进行升级，升级后老版本的用户仍然可以正常使用，直至业务流程中出现通道的自然关闭，之后再次开启通道时，用户流程即可无缝切换到新的合约逻辑。

支付合约地址的稳定性让开发者无需担心合约升级造成的业务中断和用户丢失，可以更加放心地将新功能集成到自己的产品中去，也不用担心合约出现了问题无法修复的情况；新老合约的无缝切换可以

让用户体验达到对区块链技术「无感」的最佳境界，避免了因为频繁要求用户配合而导致的用户流失。

- **可读交易**

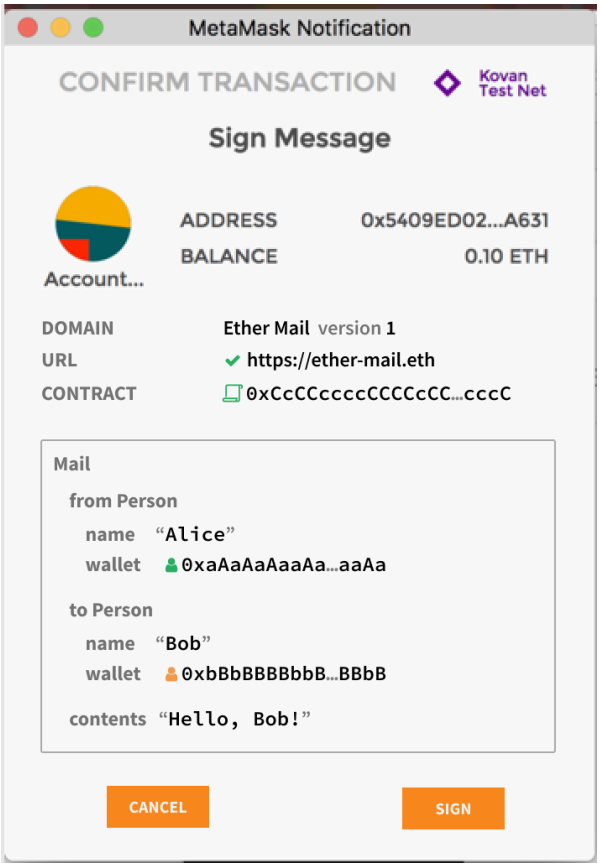
区块链的用户早已习惯了一串串乱码 —— 无论是公钥、私钥还是钱包地址，都是由一堆字母和数字组成的毫无意义的字符串，似乎只有长度的区别，数字签名也是如此。如果只是转账操作，这些乱码往往不影响用户使用，因为只要核对好金额和收款地址就不会出太大问题；但是如果涉及到合约调用，用户签名时是无法得知具体内容的。这就像有人要跟你签合同，但是你却无法看懂合同内容一样，这样的操作模式会存在很大的风险。



Signing non-typed data

以太坊的 EIP 712 规定了一种新的签名标准，如果钱包和合约都按照这一标准进行签名，用户可以在签名之前看到可读的字段，从而

得知将要签署的具体内容，这一操作称为 signTypedData —— 格式化数据签名。



Signing typed data

LITEX 支付合约完全支持 EIP 712 规范，开发者可以自定义发起支付请求时需要用户确认的信息（如币种、金额、订单号、商品信息等），用户在确认付款时也能够完全了解自己签发的是哪一笔订单对应的付款请求，极大地提升了用户体验。

- **单向通道**

在消费场景下，商家为用户提供商品或者服务，用户向商家支付资金，商家将收到的资金用于消费或者再生产。但是在支付通道的限制下，商家收到的资金仍然锁定在通道中，需要进行一笔链上交易才能从支付合约中提到链上地址里。但是这一操作执行起来比较复杂，

因为状态通道的设计默认是双向的，在双向支付通道中，通道两端是对等关系，而且互有资金往来。如果一方想要提现或者关闭通道，为了防止其作恶，必须等待另一方对这一操作进行签名授权；如果对方长时间不在线或者不同意，那么发起方必须向链上提交强制关闭通道的请求，在对方也提交了链下交易或者等时间窗口过去之后才能拿到资金。这个流程非常复杂、耗时，还会中断商户与用户的通道（再次开启还需要用户主动操作、支付手续费），如果商户每次需要提现时都要与多个用户执行上面的流程，相信双方都会放弃这一支付产品。

但是，实际场景中的支付行为绝大多数情况下是单向的：资金从消费者转移到商家。一旦按照单向的思路重新设计支付通道，让资金只能从一端流向另一端，我们就会得到一种既符合实际使用场景，又能够极大简化提现流程的设计方案。在单向通道中，只存在用户到商家的付款凭证，因此商家在提现时不需要征求用户的同意：因为通道中的用户付款资金本来就归商家所有；而且商家因为无法掌握用户私钥，所以无法伪造更多的用户付款凭证。商家可以在不打扰用户的前提下单方面提取资金，只需要提交一笔链上交易即可完成提现甚至关闭重开通道等操作。单向通道将在保证用户资金的前提下，极大地便利商家对于通道中资金的支配权力。

单向通道是 LITEX 将技术方案与实际场景结合，对产品方案进行综合优化的成果之一，它在解决实际问题的同时简化了技术实现，很好地体现了 LITEX 作为消费级区块链应用框架的设计理念。

业务验证合约

- **传统 Layer 2 合约：链上司法 + 链上执法**

如果了解过目前的 Layer 2 方案就会发现，难度最大的部分是链上的合约的编写。Layer 2 的链上合约相当于一个自动运行的法庭，需要对业务中出现的所有可能的情形进行覆盖，在出现仲裁请求的时候能够给出结果，并自动执行。这种合约的目标非常理想，但是现实中实现起来的复杂度很高，尤其是在底层公链对合约支持能力有限的情况下。

理想状态下，业务逻辑可以描述为一个有限状态机（FSM），所有结果都能够由一些确定的操作和一个全局的状态集合描述。每一步操作都会通过状态机改变当前的全局状态，然后参与方对全局状态签名并互换，作为最终提交到链上合约的证据。实际场景中，一个完整的业务逻辑很难完全由一个 FSM 来描述，其中的一些步骤可能依赖于前面某几步的中间结果，甚至有可能需要对之前的输入进行回溯。另一方面，为了处理多步逻辑，链上合约需要具备让参与方在任意一步将业务从链下转到链上继续进行的能力，这不但大大提升了开发难度，也让用户在遇到这样的情况时产生了两难的抉择：要么放弃继续进行业务，承担相应的违约资金损失；要么继续链上进行业务，承担后续的所有链上交易成本。

现实世界中，法律条文只有对逻辑的表述，针对每一个具体案例都是由司法体系判定结论，然后交由执法部门执行。链上部署的开源合约经过全球共识，其逻辑和执行是确定性的，即使是合约部署者也无法修改，这就是区块链界崇尚的「Code is Law」。不难发现，智能合约不仅仅是「法律（Law）」，因为对于确定的输入其执行结果是确定的，事实上涵盖了「司法」和「执法」的范畴。对于支付通道这种较为简单的场景，「一站式」的流程确实能够提升效率，达到去信任化的效果。但是真正的用户场景往往是非常复杂的，我们很难提前把司法乃至执法所需要的全部边界考虑清楚；即使规则已经打磨到比较完备的地步，

把判断和执行的逻辑用代码全部放在链上合约中又是一件复杂度极高的工作，复杂的代码让合约的安全性、可读性都大打折扣，很难真正商用。

我们认为，在消费级场景中，链上合约只需要承担公示规则的职能，无需考虑「执法」。这就是业务验证合约提现的「链上验证，链外仲裁」的思想。

- **业务验证合约：链上司法 + 链下执法**

业务验证合约是 LITEX 框架下的一种独特的合约形式，一方面，它让开发者在充分利用公链共识价值的同时，极大地降低了编写 Layer 2 合约的难度。另一方面，业务验证合约的使用成本非常低，无需发送链上交易，只需使用全节点的查询接口就能实时地获得验证结果，这使得无论是用户自己验证还是第三方平台辅助验证都不需要付出任何额外的资金成本。

从开发者角度来看：开发者在编写业务验证合约时，不需要在合约中实现全部业务流程，尤其是避免了目前 Layer 2 合约中极为复杂的异常流程和链上流程的处理，而只需要把业务中最关键的、需要对用户公示的逻辑在合约中体现即可。在这一指导思想下，开发者在设计业务逻辑时就可以有的放矢地把关键流程模块化，定义好它们与其他业务流程的数据接口，接下来就可以用任何需要的技术栈来完成其他的业务逻辑。这样一来，不仅开发效率得到了提高，产品的可维护性也大大增强了，因为原来需要在合约中实现的很多业务逻辑可以用传统的互联网后端来实现，随时可以进行维护，无需重新部署合约。

从用户角度看：用户如果在应用的使用过程中对结果产生任何异议，用户自己可以非常方便地利用 LITEX 链下协议提供的数据提取工具查询对应的链下数据，并按照自己的技术能力选择使用可信任的第

三方数据平台（如 etherscan.io 等）或者自己使用工具调用验证合约的查询接口，传入链下数据，从而获得清晰易读的验证结果，甚至可以将整个业务流程回放一遍。LITEX 的业务验证合约让用户能够简单直接地体验到「可验证」这一区块链重要特性的价值，有助于加深用户对区块链应用的认识，培养起关注数据合法性的好习惯。

链下协议

链上合约就像一个个锚点，它们规定了什么样的状态是合法的，以及如何提交这些状态。有了合约的保障，链下协议就可以设计得非常灵活，能够根据实际需求呈现出各种形式。举个极端点的例子，两个懂合约的人可以通过互相发送包含链下数据的电子邮件来达成一种简陋的链下协议；基于同样的合约，另外两个人甚至可以把签名数据转换成二维码打印出来，包在信封里邮寄给对方来达成更加原始的链下协议。总而言之，只要链下的数据符合链上合约的要求，同时又能被参与的各方理解、生成和传递，就是一种合格的链下协议。

然而，链下协议设计有一个大前提 —— 用户需要拥有很强的区块链技术基础知识。一直以来，区块链面向的都是技术人员，普通互联网用户连概念都很难理解，更不用说实际操作了。而 Layer 2 的产品结构理解起来比链上合约更为困难，如果链下协议和用户产品不做针对性地进行优化，那么一个合格的用户就必须：

- 理解 Layer 2 的设计模式
- 理解链上合约的逻辑
- 能够发现链下数据的异常
- 能够向合约提交链下数据来保全自己的资产

这些要求远远超出了一般用户群的能力，是典型的工业级导向设计。为了支撑消费级的应用，LITEX 在设计链下协议时必须破除对用户能力的过高假设，真正站在普通用户角度看待问题，并进行针对性的优化，从而降低用户理解和使用区块链产品的门槛。

存在的问题

● 普通用户无法掌控自己的数据

链下数据是用户保障自己权益的唯一凭证。一般来说，用户是有责任管理好自己的数据的，就像加密账户的私钥也必须由用户自己负责保存一样，一旦丢失，只能自己承受损失。然而，对于连数据库是什么都无法理解的普通用户而言，链下数据看不见摸不着，自己根本无法掌控，只能寄希望于开发者提供界面展示出来。这就产生了极大的不对等，因为事实上开发者管理了双方的链下数据，一旦出现问题，用户很难保障自己的权益 —— 如果开发者不提供接口，用户甚至无法导出自己的链下数据。

● 普通用户无法处理掉线问题

除了数据掌控力的问题之外，Layer 2 体系本身还存在一个大问题 —— 掉线问题。假设 Alice 与 Bob 之间有一条通道。正常情况下，Alice 要关闭通道时，如果 Bob 在线并且同意，那么他们可以通过协商合作的方式关闭通道，这是最理想的情况。如果 Bob 不同意，Alice 可以向合约提交强制关闭通道的请求，合约会给 Bob 留一个足够长的时间窗口来提交自己的链下数据，以防 Alice 故意只提交对自己有利的数据，导致 Bob 蒙受损失。那么如果 Alice 故意在 Bob 可能长时间不在线的时候提起强制关闭通道请求，就很有可能侵占 Bob 在通道内的

资产，这就是掉线问题所描述的情况。这一问题业内目前的解决方法是，专门为此搭建一个「守护者」网络，让用户花钱雇佣他们替自己在掉线的时候提交链下数据。事实上，用户连掉线问题是什么都很难理解的情况下，说服他们花钱购买这种服务是非常困难的，这反过来也会导致提供这一服务的节点很难收回成本，很难真正建立起这样的网络。

- **链下数据的公信力不足**

从开发者角度来看，传统的链下协议还有数据公信力不足的问题。链下数据类似聊天信息，总是点对点发送，这导致除了开发者之外的其他人都无法掌握数据的全貌。但是在消费级领域，一个产品的用户数、活跃度、收入流水等信息又是极其重要的衡量指标，好的产品是非常希望向市场公开这些数据的。因此，链下数据公信力过低的现状也给开发者们带来了很大的困扰。

为了解决以上问题，LITEX 选择使用许可链方案作为链下协议的基础，称为 LITEX Data Chain，简称 LDC。与侧链方案不同，LDC 在 LITEX 的架构中只承担对链下数据进行组织、存储和传递的职责，并不涉及资产的转移。可以说，LDC 是 LITEX 框架下所有应用和用户共享的一个分布式公共数据库，LDC 的节点则是这些数据库的维护者，也是链下数据的验证者、用户的守护者，这一设计让上面列出的问题得到了很好的解决。

LDC - LITEX Data Chains

● 概述

LDC 采用许可链集群来实现，单链共识节点数量不超过 100 个，出块时间不高于 0.5 s，实际运行 TPS 不低于 10000，多链综合 TPS 可达百万以上，足以满足当前大部分商业产品的需求。LDC 的共识机制、密码学原语、底层数据库和虚拟机均为可插拔设计，目前可兼容以太坊的地址格式、签名算法和所有开发工具，未来随着 LITEX 在多条底层公链上的拓展，对于异构链的支持也可以不断添加到 LDC 中。LDC 具有基于角色的权限控制能力，其性能和隐私保护等能力也可以随着技术的升级而不断优化。

● 共识与节点

LDC 目前采用 pBFT 共识算法，在 N 个节点组成的单链共识网络中，能够在保证可用性（liveness）和安全性（safety）的前提下提供 (N - 1) / 3 的容错性。考虑到性能和延迟受节点数量影响较大，N 设定为不超过 100。LDC 具有即时确定性。

LDC 的节点分为共识节点和验证节点两种，前者为全节点，后者为轻节点。共识节点有打包区块和参与治理的权限，验证节点只有接收交易的权限。节点的加入需要通过网络的准入检查，如果身份验证失败，即使能够在数据网络层面与其他节点连接成功，也无法获取到任何交易数据。

共识节点需要通过投票选出，获得票数最高的 N 个节点自动获得出块权限和治理权限，享受出块收益和治理激励。将 LITEX Token 通过底层公链上的投票入口合约锁定后，即可在 LDC 上获得相应的投票权证，用于给一个或多个节点投票。如果要撤回投票，需经过 72 小

时的解锁期才能将底层链上的 LITEX Token 解锁。参与投票的地址可以得到由生态基金给出的治理激励，具体激励方式在经济模型部分给出。

作为许可链，LDC 可以支持对共识节点的出块权重进行动态调节，每个 epoch 调节一次，通过权重调节可以将节点的质押情况或者得票情况与出块收益进行匹配，也可以对服务响应差、掉线频繁的节点进行降权。出块激励的具体信息会在经济模型部分详细说明。

● 账户与权限

LDC 的账户分为普通账户和合约账户，前者是拥有私钥和公钥、能够签发交易的账户，后者是拥有代码逻辑和数据存储的账户。与公链的不同是，LDC 的账户可以进行分组（Group），方便进行权限管理。组是通过合约实现的，每一个组都包含账户以及子组的列表，同时记录父组的标识，形成树形结构。

作为许可链，LDC 具备基于角色的权限管理能力。权限系统基于合约实现，既可以对单个账户的权限直接进行设置，也可以创建角色进行统一管理。常见的权限包括发送交易、创建合约、节点增删等等，还可以根据业务的需求自定义其他的权限。

LDC 默认拥有一个 Super Admin —— 超级管理员权限账户，能够对 LDC 进行最高权限的操作，例如共识节点的增删、角色权限的管理等。然而，作为一个应用框架的底层设施，LDC 的数据需要保持公信力，治理权限也需要交由生态执行，因此链上治理机制是必不可少的功能模块。

- **链上治理**

链上治理是指在区块链的运行过程中能够根据条件自动执行的管理规则，例如节点权限的授予和撤销、手续费率的动态调整等等。相对的，链下治理是指通过管理委员会的方式进行决策，然后由统一的管理员权限对链上规则进行调整的方式。不难发现，链上治理规则透明，执行效率高，没有中心化风险，是区块链首选的治理方式。

LDC 将超级管理员权限分散为多个子权限，每个权限都可以由一个或多个治理合约进行控制。这种机制使得链上治理的实施变得公开透明，如共识节点的投票选举结果即可通过这种方式自动生效，与底层公链的数据同步也可以自动核验。在业务的发展中，链上治理规则可以不断修正和增补，像现实世界的法律一样，与时俱进地维护 LITEX 加密经济体系的安全。

- **隐私保护**

链下数据的公信力对开发者有很大的意义，但是支付数据的隐私性也是用户非常看重的一个方面。相对于中心化架构的服务，LDC 的数据不依赖于中央服务器的存储，因此可以避免单点故障造成的数据丢失或数据泄露；P2P 的组网方式可以将 ip 等信息的暴露范围降到最低；用户账户基于密码学创建，与实际身份不需要进行对应。这些都是 LDC 作为区块链架构在数据隐私保护上的优势。

然而，区块链并非没有隐私方面的劣势。为了迅速达成共识以及追溯交易，链上数据是公开透明的，任何人都可以看到从创世块开始至今的所有数据，追踪所有交易。虽然交易内的地址信息并不对应任何现实信息，但是在实际使用场景中，用户在现实生活中的信息会不

可避免地出现暴露，这就让链上地址与链下身份出现了对应的可能；再加上区块链交易可追溯的特点，更容易造成用户行为隐私的泄露。

针对这一问题，LDC 准备了两种方案。第一种是密码学方案，能够使用零知识证明技术对交易数据进行隐私保护。开启后，发送方用户的地址信息和交易内容不必周知，只需要提供相关的证明信息即可。这一方案能够很好地保护收发双方的地址信息以及交易细节，但是会对性能产生一定影响，适合在比较关键的业务场景（如支付场景）使用。另一种是数据隔离方案，即将敏感数据利用侧链甚至链外存储的方式进行隔离，只将需要参与共识的见证信息放在 LDC 上公开运行，这一方案的性能较好，也比较容易与现有场景结合。

- **掉线守护**

LDC 可以很好地解决 Layer 2 方案中的掉线问题。LDC 节点是生态的维护者和受益者，每一笔交易都会经过节点的处理，节点也因此获得了手续费收益，因此节点有责任和能力在出现掉线风险的时候帮助用户提交链上证据。此外，手续费收益会留出一部分专门用于奖励成功帮助用户提交链下数据的节点，提升节点帮助用户守护资产的意愿。

用户在签署链下数据时，会自动签发一个授权，使得所有获得这个数据的节点都有向合约提交数据的能力；另一方面，链上合约的规定强制关闭通道的申请方必须由本人提交，不能由其他地址代为提交。在这一前提下，节点无法恶意代替用户进行强关操作，只能在对手方发起强关时帮助用户提交链下数据，充分保障了用户的资产安全。

LDC 的优势

- **提升数据公信力**

作为许可链，LDC 上存储的链下数据具有公开可查和难以篡改的特性，开发者很难随意更改 LDC 上的数据。由于链下数据以 LDC 上查询到的信息为准，开发者无法像在其他 Layer 2 方案中那样虚报数据；因为无法获取用户的私钥，开发者也无法伪造用户主地址签名的链下数据（即支付数据）；因此 LDC 上的数据很大程度上真实地反映了用户的实际操作情况，是具有公信力的统计数据，未来也可以作为 LITEX 生态中应用的评价指标。

此外，LDC 也是抗女巫攻击的，鉴于 LITEX 的支付通道是单向通道，开发者无法通过自建账户来回收付的方式制造虚假的交易量，一旦通道内资金耗尽，只能通过链上交易进行资金追加或者开辟新的支付通道，而这与在链上合约直接伪造交易量的手续费和时间成本相同。而对于其他采用点对点和双向通道的 Layer 2 方案来说，制造虚假交易量易如反掌，但由于它们的链下数据本就不具备公信力，因此直接虚报数据可能是成本更低的方式。

- **保障数据安全**

链下数据是 Layer 2 应用中最重要的部分，用户的资产安全完全依赖于对链下数据的保存和管理。相比用户自己存储和维护链下数据的方式，LDC 用许可链的形式对链下数据进行统一管理会更加安全，不会出现用户因为清空缓存或者误删应用而导致的数据丢失，也不会因为开发者服务器出现单点故障而导致应用数据损坏。

- **方便用户提取**

在传统的 Layer 2 应用模型下，普通用户由于没有技术能力，无法理解自己的链下数据具体在什么位置，也不可能靠自己的力量将其提取出来用于链上仲裁，只能依靠开发者提供相应的接口查询和提取链下数据，本质上是由一方管控双方的链下数据，这让普通用户处于非常弱势和被动的地位。

LDC 上存储的链下数据完全公开透明，用户可以使用官方提供的区块链浏览器进行数据查询，还可以根据应用种类，交互过程，使用时间等方式对数据进行分组筛选，方便用户迅速辨认出自己想要仲裁或者验证的链下数据，然后可以一键提交链上验证。LDC 的区块链浏览器、验证平台等技术将会完全开源，任何第三方都可以自行搭建和定制符合 LDC 数据协议的数据查询和验证平台，服务对应的用户。

LITEX 经济模型

作为一个多角色共同参与的 Layer 2 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，并将生态产生的价值回馈给全体参与者。为此 LITEX 设计了一种加密代币 LITEX Token（符号为 LXT）来承载这一功能。

LXT 是发行在 Ethereum 公链上的 ERC-20 协议代币，总量 20 亿个，不可增发，不可销毁。随着 LITEX 对更多底层公链的支持，LXT 有能力按需求进行部分跨链迁移，迁移的过程中全网总量不会上升。LXT 的发行分布见附录一。

价值捕获

LXT 作为 LITEX 生态系统中的代币，需要具备捕获整个生态价值的能力，因为 LITEX 从产品上主要分成加密支付和业务逻辑两个部分，这两个部分涉及到的资源消耗和主要参与者是不同的，因此需要制定对应的价值捕获方式，兼顾到 LITEX 生态中的各个角色，努力保障各方利益一致性。另外，为了激励节点在生态早期加入进来，LITEX 还会拿出一部分代币作为出块奖励，按照实际的出块情况分配给所有共识节点。

- **加密支付部分**

用户能够在 LITEX 网络中通过支付通道实现安全、快速地支付，是与 LDC 共识节点的付出分不开的。为了维护 LITEX 网络的安全性、稳定性和处理效率，共识节点们需要投入大量的资金和精力维持节点

软件的运行，因此理应从支付的总额中获得一定比例的手续费的收益。而 LITEX 网络的验证节点作为用户交易安全性的最后守护者，监控着链上每一笔交易的准确完成，确保全网共识节点不会作恶，因此也应当获得一部分手续费收益。

用户在 LITEX 网络中进行支付时，根据实际使用的支付代币种类，需要缴纳一定比例的支付手续费。支付手续费会按照共识节点和验证节点进行一次划分，然后按照各自类型节点抵押的 LXT 数量进行等比例的分配。具体分配规则会在价值分配部分进行说明。

- **业务逻辑部分**

开发者在 LITEX 上做项目开发时，需要对 LDC 的资源占用支付一定的费用，LDC 提供的资源主要包括：计算资源、网络带宽资源、存储资源等，其中计算资源和网络带宽资源属于短期消耗资源，会实时刷新，而存储资源属于长期消耗资源，需要共识节点付出长期的存储成本。因此在经济模型设计中，前期不再计算开发者对于计算资源和网络带宽的消耗，这一部分已经在出块奖励中补贴给共识节点了，但是开发者需要为不可再生的存储资源付出一定的成本。

LDC 会给开发者一定的初始存储空间，这部分空间是免费的，但是随着数据的增长，如果这些空间在相当的时间内没有任何更新，这部分空间有可能会被快照后回收，其内容以只读的形式存放在存档服务器中。为了获得更多持续可用的存储空间，开发者需要根据应用的实际情况，通过抵押 LXT 的方式获取在 LDC 网络中的存储空间。因为 LXT 是一个非通胀模型，开发者并没有实际的资金损失，只是通过锁定 LXT 流动性的方式获得了来自 LDC 网络提供的有限的存储空间。

- **出块奖励部分**

前面所描述的价值都依赖于 LITEX 生态的发展，生态繁荣之后，这些价值能够给所有节点带来可观的收益，但是早期却很难覆盖节点们维护网络所需要付出的成本。因此，LITEX 会拿出一部分 LXT 作为出块激励，用于在前期激励参与到网络建设中来的共识节点。

价值分配

- **支付手续费分配**

节点类型	分配比例	分配方式
共识节点	70%	按照获得票数的比例分配
验证节点	30%	按照所投票数的比例分配

- **LDC 空间抵押费率**

空间类型	空间大小	抵押率	永久存储
初始空间	100 MB / 合约	0	否
生产空间	总量 10 TB	10 LXT / MB	是

- **出块奖励**

总量	单块奖励	产出规则	奖励来源
3 亿 LXT	2 LXT	每 2 年单块收益减半	生态建设预留

价值统一

共识节点:共识节点作为网络的主要资源成本付出方,获得了来自系统的生态奖励,还可以获得一部分用户支付交易手续费;而对于开发者需要抵押一定的 LXT 才能获得一定比例的存储空间,保障了共识节点不需要无上限地增加硬件成本。

验证节点:验证节点作为整个网络的安全守护者,验证节点可以获得一部分来自系统的生态奖励,还可以通过抵押 LXT 获得一部分交易手续费的分红权,除此之外,当验证节点发现网络中存在错误交易或者共识节点作恶等情况,验证节点可以提交仲裁,如果证实交易错误或者节点作恶,验证节点还可以获得额外的验证收益。

用户:用户主要是希望获得安全的高效的交易转账服务,而 LDC 单链设置的 100 个共识节点,在一定意义上确保了节点的去中心化属性,降低了共识节点作恶的可能性,并且采用了高效的支付通道,提供 10000 以上的 TPS 能力,用户可以获得安全的高效的低成本的交易转账体验。

开发者:LITEX 会为开发者提供完整的技术解决方案,帮助传统开发者便捷的利用区块链技术搭建属于自己的区块链应用,并且会为开发项目对接区块链圈内的生态基础设施,帮助开发者的产品迅速成长。

LITEX 生态:在 LITEX 整个生态中,共识节点、验证节点、开发者都需要锁定一定的 LXT 以获得对应的交易手续费的分红权或者是所需要的开发资源,整个经济模型充分平衡生态体系中的各方利益,确保各方利益的一致性。

组织架构

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。

LITEX Lab

- **Guanghong Xu - CEO**

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 (Bradcom) 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。

- **Leo Wang - COO**

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。

- **Johnson Zhang - CTO**

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，LTXN 设计者，曾就职于 IBM、新浪微博等平台担任高级研发工程师。

- **Frank - CPO**

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。

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。

- **Jeffrey Wernick** - 顾问

芝加哥大学经济学与金融学博士，比特币早期参与者，Uber 及 airbnb 的早期投资人。

- **丛林** - 顾问

华尔街区块链联盟成员，String Labs 顾问，现任芝加哥大学金融专业教授、博士生导师、东亚研究中心教授，Summa Cum Laude 和 Phi Beta Kappa 奖得主。

- **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。

投资机构

- 星耀资本

- 节点资本

- 双花资本

- JLAB

附录一、LITEX Token（LXT）分布

数量	比例	用途	说明
700,000,000	35%	预售	面向机构投资者等，用于 LITEX 项目后续开发、人才招募、市场推广等。此部分资金的使用需要定期公示。
300,000,000	15%	生态建设	用于空投、Node 激励等生态启动需求。
600,000,000	30%	发展基金	用于发展合作伙伴、团队建设等。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	回报创始团队在加密货币领域的探索和开发以及今后维护 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%	顾问及合作机构	面向需要合作的各种机构以及顾问等。

附录二、LDC 共识节点参考配置表

类型	CPU	内存	存储	带宽	平均延迟
体验配置	2 核	4G	30G	10M	≤10ms
生产配置	4 核	8G	200G	100M	≤10ms
推荐配置	16 核	64G	500G	100M	≤10ms