a16z：从代币模型挑战谈起，如何设计新经济模型解锁现金流和合规性

作者：a16z

编译：Felix, PANews

对于基础设施代币（如L1或L2），其经济模型已经得到充分的开发和理解，根源在于对区块空间的供需关系。但对于应用代币（在区块链上部署服务的智能合约协议）而言，经济模型仍在完善中。

应用代币的业务模型应该像其底层软件一样富有表现力。为此，本文引入了应用代币的现金流概念。这种方法使应用程序能够创建宽松、灵活的模型，用户可以选择如何为他们提供的价值获得奖励。这种方法能在不同司法管辖区的监管要求的合法活动中产生费用，从而鼓励更大程度的合规。此外，可以在鼓励最小化治理的同时最大化协议的价值。

本文所分享的原则适用于所有Web3应用程序——从DeFi到去中心化的社交应用程序、DePIN网络，以及介于两者之间的任何应用。

### 代币模型面临的挑战

基础设施代币受制于内在的供需关系：随着需求的增加，供应减少，市场也会相应调整。以太坊改进提案 1559 (EIP-1559) 加速了许多基础设施代币的这种原生经济基础，该提案实施了一项针对所有以太坊交易的销毁机制。尽管有零星尝试购买和销毁的模型，但应用代币并没有与 EIP-1559 类似的模型。

应用程序是区块空间的用户，而不是提供者，因此它们不能依赖于使用其区块空间的其他人那里收取gas费。这就是为什么他们需要开发自己的经济模型。

这里也存在一些法律挑战：由于典型区块链交易的通用性质及其使用的编程机制，基础设施代币经济模型更不受法律风险的影响。但对于应用代币经济模型，所涉及的应用程序可能依赖于监管活动，并可能需要治理代币持有者的中介——这使得经济更加复杂。例如，一个促进衍生品交易的去中心化交易所（在美国是一项受到严格监管的活动）与以太坊等完全不同。

这些内外挑战意味着应用代币需要不同的经济模型。考虑到这一点，本文提出了一种可能的解决方案：一种设计协议的方法，可在最大化协议收入、激励监管合规性并纳入治理最小化的同时，补偿应用程序代币持有者的服务。目标很简单：通过现金流为应用代币提供许多基础设施代币已经具备的同样的经济基础。

解决方案侧重于解决应用代币面临的三个问题：

#### 治理挑战

应用代币通常具有治理权，而DAO的存在可能会带来基础设施代币不会面临的不确定性。对于在美国有重大业务的DAO，如果DAO控制协议收入或充当协议经济活动的中介并使此类活动程序化，则可能会出现风险。为了避免这些风险，项目可以通过最小化治理来消除DAO的控制权。对于无法做到这一点的DAO，怀俄明州新成立的去中心化非法人非营利组织协会 (DUNA) 提供了一个去中心化的法律实体，可以帮助减轻这些风险并遵守适用的税法。

#### 价值分配挑战

应用程序必须谨慎设计向代币持有者分配价值的机制。根据美国证券法，将投票权和经济权结合起来可能会引起担忧，尤其是像按比例分配和代币买入并销毁这样的简单直接的机制。这些机制看起来类似于股息和股票回购，并且可能会削弱代币应该受到与股票不同的监管框架的论点。

项目应该探索利益相关者的模式——以有利于项目的方式奖励代币持有者的贡献。许多项目都在鼓励积极参与，包括运营前端（Liquity）、参与协议（Goldfinch）和作为安全模块的一部分质押抵押品（如Aave）。这里的设计空间是开放的 ，但一个好的起点是规划项目中的所有利益相关者，确定应该鼓励他们每个人采取哪些行为，并决定协议可以通过这种激励创造什么样的总体价值。

为简单起见，在本文将假设一个简单的补偿模型，奖励代币持有者参与治理。

#### 监管挑战

在为代币持有者设计价值增值机制时，促进受监管活动的应用程序也必须谨慎。如果此类机制从不符合适用法律的前端或API中获得价值，代币持有者可能会从非法活动中获利。

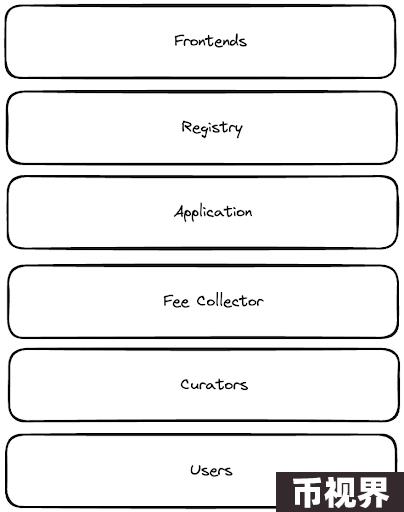
针对此问题提出的大多数解决方案都集中在将价值增值限制在美国允许的活动中——例如，仅对涉及某些资产的流动性池收取协议费用。这使项目受到监管方法的影响，并破坏了全球自主软件协议的价值主张。它还直接破坏了最小化治理的努力。对于DAO来说，从监管合规角度确定哪种费用策略有效并不适宜。

在理想情况下，项目将能够在任何允许此类活动的司法管辖区收取费用，而不必依赖DAO来确定什么是允许的。解决方案不是要求在协议层面遵守法规，而是确保只有在前端或产生这些费用的API遵守了前端所在地区的适用法律和法规的情况下，协议产生的费用才会被传递。如果美国禁止对应用程序促成的某种交易收取费用，那么即使这种活动在世界上其他国家都是允许的，也可能使该应用代币的经济价值降至零。在费用累积和分配方面的灵活性最终等于在监管压力面前的弹性。

### 一个核心问题：追溯费用

费用的可追溯性对于在不引入审查风险或协议被许可的情况下解决不合规前端产生的潜在风险至关重要。有了可追溯性，应用程序可以确保代币持有者获得的任何费用仅来自代币持有者管辖范围内合法合规的前端。如果费用无法追踪，就无法保护代币持有者免受不合规前端累积价值的影响，这可能会使代币持有者面临风险。

为了使费用可追溯，协议可以通过两个步骤设计：

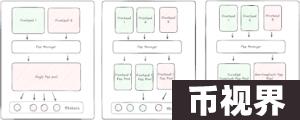


### 映射前端

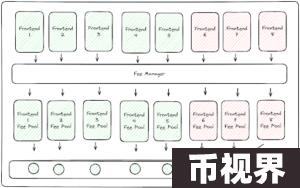
费用可追溯性需要从域到公钥/私钥对的一对一映射。如果没有这种映射，恶意前端可能会伪造交易并假装是从诚实的域提交的。密码学允许“注册”前端，不可变地记录域到公钥的映射，证明域实际上控制该公钥，并使用所述私钥签署交易。这使我们能够将交易（从而将费用）归为给定域。

### 路由费用

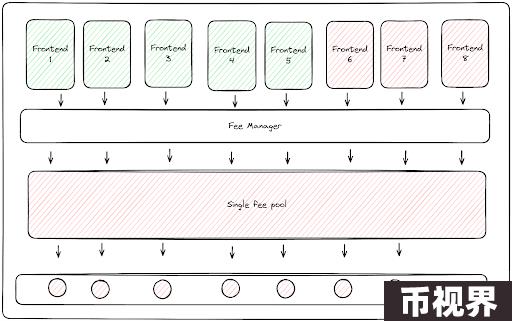
一旦费用来源可追溯，协议就可以确定如何分配这些费用，以使代币持有者免于从非法交易中收取费用，而且也不会增加DAO的去中心化治理负担。为了帮助说明这一点，我们可以考虑应用代币质押的各种可能设计，从每个前端一个质押池到所有前端共用一个质押池。



在其最简单的构造中，每个前端的费用都可以路由到单独的特定于前端的质押模块。通过选择质押到哪个前端，代币持有者将能够决定其收取哪些费用，并避免任何使自己陷入法律风险的费用。例如，代币持有者可以仅质押到与已获得欧洲所有监管部门批准的前端相关的模块。虽然这种设计听起来很简单，但实际上相当复杂。50 个不同的前端可能有 50 个质押池，费用的稀释可能会对代币价值产生不利影响。



另一方面，每个前端的费用可以集中在一起——但这违背了费用可追溯性的目的。如果所有费用都集中在一起，就无法区分合规前端和不合规前端的费用。代币持有者将被迫在不收取任何费用和将资金池中持有股份之间做出选择，在这个池子里，他们将从其管辖范围内不合规前端的非法活动中获益——这种选择可能会阻止许多代币持有者参与，也可能使系统恢复到当前是次优设计，即DAO需要评估费用可以应用于哪些领域。



### 通过管理解决费用可追溯性问题

这些复杂性可以通过管理解决。考虑一个具有费用和代币的无许可智能合约协议应用程序，任何人都可以为该应用程序创建前端，并且任何前端都可以拥有自己的质押模块，将此协议的一个前端称为App.xyz。

App.xyz可以遵循其所在司法管辖区的特定合规规则。源自 app.xyz 的应用程序活动会产生协议费用。App.xyz 有自己的质押模块，代币持有者可以直接将他们的代币质押到该模块，也可以质押给想要单独挑选一篮子他们认为合规的前端的管理人。这些代币质押者将从他们质押的一组前端中获得费用形式的收益。如果一个前端产生 100 美元的费用，并且 100 个实体每个质押 1 个代币，那么每个实体都有权获得 1 美元。管理人最初可以收取服务费。未来，政府可以在链上证明其管辖范围内的前端是否合规，以帮助保护消费者，附带的好处是实现管理自动化。

此模型的一个潜在风险是，不合规前端的运营成本可能更低，因为它们没有合规前端的管理开销。他们还可以设计模型将前端费用回收给交易者。有两个因素可以减轻这种风险。首先，大多数用户实际上希望合规前端遵守当地法律法规，尤其适用于大型受监管的机构。其次，对于反复违反规则、危及应用可行性的不合规前端，治理可以作为最后的手段或发挥“否决权”，从而阻止不良行为。

最后，所有未通过注册前端发起的交易费用都将存入一个单一的综合质押模块中，使协议能够从机器人发起的交易和与协议智能合约的其他直接交互中获取收入。

### 从理论到实施：将方法付诸实践

详细地回顾一下应用代币堆栈。对于促进前端质押的协议，它需要建立一个前端需要注册的注册智能合约。

每个前端或 API 都可以将特殊的TXT记录添加到其域的DNS记录中，例如ENS DNS集成。此TXT记录包含前端一次生成的密钥对的公钥，称为证书。



然后，前端客户端可以调用 register() 函数并证明它拥有其域名。系统将存储域与证书公钥的映射，反之亦然。

当通过客户端创建交易时，它还会使用其证书公钥对交易有效负载进行签名。这些将以捆绑包的形式传递给应用程序的智能合约。

应用程序的智能合约会验证证书，检查是否与正确的tx主体相对应，并且已注册。如果是，则处理交易。然后，交易产生的费用将与域名（来自注册表）一起发送到FeeCollector合约。

FeeCollector允许管理人、用户、验证者等将代币直接质押到单个域或域集。这些合约必须跟踪每个域上质押的代币数量、每个地址的质押份额以及质押时间。流动性挖矿的流行实现可以用作此合约逻辑的起点。

那些已向管理人（或直接向费用管理合约本身）质押的用户可以根据质押到域中的应用代币数量提取相应比例的费用。该架构可能类似于MetaMorpho / Morpho Blue。

引入该功能不会增加应用程序DAO的治理负担。事实上，治理责任可以减少，因为可以为协议促成的所有交易永久开启费用开关，从而消除DAO对协议经济模型的任何控制。

### 基于应用程序类型的其他考虑因素

虽然这些原则广泛应用于应用代币经济模型，但根据应用程序类型，还可以考虑其他费用：基于L2或L2构建的应用程序、应用程序链和使用rollups构建的应用程序。

#### L1/L2应用

L1/L2区块链上的应用程序将智能合约直接部署在链上。当用户与应用程序的智能合约交互时收取费用。通常，这通过一个易于使用的前端（如应用程序或网站）发生，该前端充当散户和底层智能合约之间的接口。在这种情况下，任何费用都将源自该前端。上面关于 app.xyz 的示例说明了费用系统如何适用于L1应用程序。

除了依赖管理人来过滤前端费用外，应用程序还可以采用白名单或黑名单方法来过滤增加网络费用的前端。同样，这里的目的是确保代币持有者和整个协议不会从非法活动中获利，并遵守特定司法管辖区的法律法规。

在白名单方法中，应用程序将发布一组针对前端的规则，创建遵守规则的前端的注册表，向选择加入的前端颁发证书，并要求前端质押代币以收取部分应用程序费用。 如果前端不遵守规则将被削减，并且其费用贡献证书将被删除。

在黑名单方法中，应用程序不必创建任何规则，但应用程序前端的启动并非无需许可。相反，该应用程序将要求任何前端在允许前端使用该应用程序之前，提供律师事务所的意见，证明该前端符合其管辖范围。一旦收到意见，应用程序将向前端颁发费用贡献证书，只有当应用程序收到监管机构通知前端不合规时，证书才会被删除。

费用渠道与前几节中提供的例子类似。

这两种方法都大大增加了去中心化治理的负担，要求DAO建立和维护一套规则或评估有关合规性的法律意见。在某些情况下，这可能是可以接受的，但在大多数情况下，最好将这种合规负担外包给管理者。

#### 应用链

应用链是特定于应用程序的区块链，其验证者仅适用于该应用程序。

作为对其工作的回报，这些验证者会收到报酬。与验证者通常通过通货膨胀发行代币获得奖励的L1区块链不同，一些应用链 (dYdX) 则将客户费用转给验证者。

在此模型中，代币持有者必须质押给验证者才能获得奖励。验证者成为策划的质押模块。

此工作集与L1验证者不同。应用链验证者处理来自特定应用程序的特定交易。由于这种差异，应用链验证者可能承担更大程度的法律风险，这些风险与它们正在促进的底层活动有关。因此，协议应授予验证者自由，使其能够根据其管辖范围内的法律和自己的意愿执行他们可以执行的工作。重要的是，只要其验证者集在地理上是分散的，就可以做到这一点，不会危及应用链的无许可性或使其面临重大审查风险。

希望利用费用可追溯性优势的应用链的架构将类似于L1应用程序。但是验证者将能够使用前端映射来确定他们希望从哪个前端处理事务。任何给定交易的费用都将转到活跃验证者集，而选择不参与的非活跃验证者将错失此类费用。从费用的角度来看，验证者执行的功能与上面讨论的质押模块管理人相同，并且这些验证者的质押者可以确保他们不会从任何非法活动中获得收入。验证者还可以选举一名管理人来确定每个司法管辖区哪些前端符合规定。

#### Rollups

Rollups具有自己的区块空间，但可以继承另一条链的安全性。当今大多数Rollups都有单一的排序器。如果这些Rollups是特定于应用程序的，并将其排序器作为唯一验证者，则该排序器所包含的交易产生的费用可以根据精选的合规前端集或作为一般池分配给质押者。

如果Rollups将其排序器集去中心化，则排序器将成为事实上的精选质押模块，收费渠道将与应用链相同。排序器取代验证器进行费用分配，每个排序器都可以自行决定从哪个前端接受费用。

虽然应用代币有许多可能的模型，但提供精选的质押池有助于解决应用程序独有的外部挑战。通过认识到应用程序面临的内外挑战，创始人可以更好地为他们的项目从头开始设计应用代币模型。

相关阅读：专访1kx研究员： Web3代币设计的正确打开方式