a16z：应用代币的新财务模型 如何产生现金流

基础设施代币——对应于第1层网络（或计算栈中的相邻部分，如第2层）——其经济模型已经发展成熟并被广泛理解，这些模型基于对区块空间的供需关系。但对于应用代币——在区块链之上部署服务的智能合约协议，它们传递了“分布式业务”中的权利——经济模型仍在解决之中。

应用代币的商业模式应该像其底层软件一样具有表现力。为此，我们引入了应用代币的现金流——这种方法使应用程序能够创建宽容、灵活的模型，用户可以选择他们如何因提供的价值而获得奖励。这种方法从不同司法管辖区的合法活动中创造费用，鼓励更大的合规性。同时，它还最大化了协议累积的价值，同时鼓励治理最小化。

我们在这里分享的原则适用于所有web3应用程序——从去中心化金融（DeFi）到去中心化社交应用程序、DePIN网络，以及两者之间的所有领域。

## 代币模型面临的挑战

基础设施代币受内嵌的供需关系影响：需求增加时，供应量减少，市场相应调整。许多基础设施代币的这种原生经济基础因以太坊改进提案1559（EIP-1559）而加速发展，该提案为所有以太坊交易实施了基础费用，这些费用将被燃烧。但尽管有零星的购买和燃烧模型尝试，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使用者，而非提供者，因此它们不能依赖于从使用它们区块空间的其他人那里收集的燃气费。这就是为什么它们需要开发自己的经济模型。

这里也存在一些法律挑战：基础设施代币的经济模型由于典型区块链交易的通用性质和它们使用的程序化机制，更少受到法律风险的影响。但对于应用代币的经济模型，涉及的应用程序可能依赖于受监管活动的促进，并可能需要治理代币持有者的中介——这使得经济更加复杂。一个促进在美国高度受监管的衍生品交易的去中心化交易所，与以太坊有很大的不同。

这些内在和外在挑战的结合意味着应用代币需要一种不同的经济模型。考虑到这一点，我们提出了一种可能的解决方案：一种设计协议的方法，以补偿应用代币持有者提供的服务，同时最大化协议收入，激励监管合规，并纳入治理最小化。我们的目标很简单：通过现金流，给予应用代币与许多基础设施代币已经拥有的相同的经济基础。

我们的解决方案专注于解决应用代币面临的三个问题：

治理方面的挑战

价值分配方面的挑战

受监管活动方面的挑战

# 1. 治理挑战

应用代币通常具有治理权，而分散自治组织（DAO）的存在可能引入了基础设施代币所没有的不确定性。对于在美国有重要业务的DAO，如果DAO对协议收入有控制权或中介协议的经济活动并使其程序化，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。对于无法这样做的DAO，怀俄明州的新分散非注册非营利协会（DUNA）提供了一个去中心化的法律实体，可能有助于减轻这些风险并遵守适用的税法。

# 2. 价值分配挑战

应用程序在设计向代币持有者分配价值的机制时也必须小心。结合投票权和经济权利可能会引起美国证券法的关注，特别是像按比例分配和代币购买销毁这样简单直接的机制。这些机制看起来类似于股息和股票回购，可能会破坏代币应该与股权有不同的监管框架的论点。

项目应该探索利益相关者资本主义——以一种有利于项目的方式奖励代币持有者对项目的贡献。许多项目鼓励积极的参与，包括运营前端（Liquity），参与协议（Goldfinch），以及作为安全模块的一部分质押抵押品（Aave）。这里的设计空间非常开放，但一个好的起点是列出项目中的所有利益相关者，确定应该鼓励他们哪些行为，并决定协议通过这种激励可以创造什么总体价值。

为了简化起见，在这篇文章中，我们将假设一个简单的补偿模型，即奖励代币持有者参与治理，尽管还存在其他方案。

# 3. 受监管活动的挑战

促进受监管活动的应用程序在设计代币持有者价值积累机制时也必须小心。如果这些机制从未经许可的前端或API中积累价值，而这些前端或API并未遵守适用法律，代币持有者可能从非法活动中获利。

大多数针对这个问题的提议解决方案都集中在限制价值积累到在美国被允许的活动中——例如，只对涉及某些资产的流动性池的协议费用进行激活。这使得项目受到监管方法的最低公共分母的限制，并破坏了全球自治软件协议的价值主张。这也直接破坏了治理最小化的努力。确定哪种费用策略从监管合规的角度来看是可行的，不是DAO的适当任务。

在一个理想的世界里，项目应该能够在任何活动被允许的司法管辖区收取费用，而不必依赖DAO来确定什么是被允许的。解决方案不是要求在协议层面遵守监管，而是确保只有当产生费用的前端或API在前端所在地遵守适用的法律和法规时，才会传递协议生成的费用。如果美国规定对某个应用程序促进的某种类型的交易收取费用是非法的，即使这种活动在世界上的任何其他国家都是完全被允许的，那可能会导致该应用的代币经济价值降至零。在费用积累和分配方面的灵活性最终等于面对监管压力时的韧性。

# 一个核心问题：追踪费用

费用的可追溯性对于解决不合规前端可能带来的潜在风险至关重要，同时不引入审查风险或使协议需要许可。有了可追溯性，应用程序可以确保代币持有者累积的任何费用仅来自代币持有者所在司法管辖区合法合规的前端。如果费用不可追溯，将无法将代币持有者与从非合规前端（即，由非合规前端收集的费用）累积的价值隔离开来，这可能会使代币持有者面临风险。

为了使费用可追溯，协议可以使用一个两步应用程序代币质押系统设计。

步骤 1：确定产生费用的前端，

步骤 2：根据自定义逻辑将费用路由到不同的资金池。



# 映射前端

费用可追溯性要求将一个域名映射到一对公/私钥。如果没有这种映射，恶意前端可能会伪装交易，假装它们来自一个诚实的域名。密码学允许我们“注册”前端，将域名到公钥的映射不可变地记录下来，证明域名确实控制着那个公钥，并使用所说的私钥签署交易。这使我们能够将交易，因此也就是费用，归因于特定的域名。

# 路由费用



一旦费用来源可追溯，协议就可以决定如何分配这些费用，既能保护代币持有者不接收来自非法交易的费用，同时也不会增加DAO的去中心化治理负担。为了帮助说明这一点，可以想象一下应用代币质押的可能设计范围，从为每个前端提供一个质押池，到为所有前端提供一个质押池。

在其最简单的构建中，每个前端的费用可以被路由到一个特定的前端质押模块。通过选择质押给哪些前端，代币持有者将能够决定他们接收哪些费用，并避免任何可能使代币持有者处于法律风险之中的费用。例如，代币持有者可能只选择质押给与一个在欧洲获得了所有监管批准的前端相关联的模块。虽然这种设计听起来很简单，但实际上却相当复杂。如果有50个不同的前端，就可能存在50个质押池，费用的稀释可能对代币价值产生不利影响。



在设计谱系的另一端，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初衷。如果所有费用都被集中在一起，就无法区分合规前端和不合规前端的费用——一个坏苹果会毁了整桶。代币持有者将被迫在不接受任何费用和质押在一个他们将从其管辖区域内不合规前端的非法活动中受益的池子之间做出选择——这个选项可能会阻止许多代币持有者参与，或者可能导致系统回到当前次优设计，即DAO必须评估费用可以应用在哪里。



# 通过设定解决费用可追溯性问题

这些复杂性可以通过设定来解决。考虑一个任何人都可以为其创建前端，任何前端都可以拥有自己的质押模块的无需许可的智能合约协议应用程序。让我们将这个协议应用程序的一个前端称为app.xyz。

App.xyz 可以遵循其所在地司法管辖区的特定合规规则。从 app.xyz 起源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，或者质押给一个想要单独挑选他们认为合规的前端组合的设定人。这些代币质押者将以他们质押的前端集合的费用形式获得收益。如果一个前端产生了100美元的费用，并且有100个实体各自质押了1个代币，那么每个实体有权获得1美元。设定人最初可能会为他们的服务收费。将来，政府可能会对其司法管辖区中合规的前端进行链上认证，以帮助保护消费者，附带好处是自动化设定。

这种模型中一个潜在的风险是，不合规的前端可能因为缺乏合规前端的行政开销而更便宜地运营。它们还可能设计模式将前端费用回收给交易者，以进一步激励他们的规避行为。两个因素可以减轻这种风险。首先，大多数用户实际上希望前端遵守他们当地的法律和法规。这对于大型、受监管的机构尤其如此。其次，治理可以作为最后的手段或对一再违反规则并危及应用程序可行性的不合规前端的“否决权威”，从而抑制不良行为。

最后，所有不是通过注册前端启动的交易产生费用将被存入一个统一的质押模块，使协议能够捕获由机器人和其他直接与协议智能合约交互的交易产生的收入。

# 从理论到实践：将方法付诸实践

让我们更详细地重新审视应用代币堆栈。为了便于前端质押，协议需要建立一个注册智能合约，前端需要在此注册。

每个前端或API都可以在其域名的DNS记录中添加特殊的TXT记录，如ENS DNS集成。这个TXT记录包含前端生成的一对密钥的公钥，这个公钥一旦生成就被称为证书。

前端客户端随后可以调用一个 register() 函数，并证明它拥有其域名。将域名映射到证书公钥，反之亦然，这些信息被存储起来。

当通过客户端创建交易时，它还会使用其证书公钥签署交易负载。这些信息被捆绑在一起传递给应用程序的智能合约。

应用程序的智能合约验证证书，检查它是否对应正确的交易主体，并且已经注册。如果是，交易就会被处理。交易生成的费用随后被发送到一个 FeeCollector 合约，同时附带域名信息（来自注册表）。

FeeCollector 允许设定人、用户、验证者等直接对一个域名或一组域名质押代币。这些合约必须跟踪每个域名上质押的代币数量、每个地址在该质押中的份额，以及他们质押的时间长度。流行的流动性挖矿实现可以作为这个合约逻辑的起点。

已经对设定人质押（或直接对费用管理合约本身质押）的用户随后可以根据质押到域名的应用代币数量提取相应的费用份额。这种架构可能类似于 MetaMorpho/Morpho Blue。



这种方法可以在不增加应用程序DAO治理负担的情况下引入。实际上，治理责任可能会减少，因为费用开关可以对协议所促进的所有交易永久开启，从而消除DAO对协议经济模型的控制。

# 基于应用程序类型的额外考虑

虽然这些原则广泛适用于应用程序代币经济模型，但根据应用程序的类型，也可能有其他的费用考虑：建立在第1层或第2层的应用程序、应用链，以及使用rollups构建的应用程序。

# L1/L2应用程序的考量

在第1层（Layer 1）或第2层（Layer 2）区块链上的应用程序直接在链上部署智能合约。当用户与应用程序的智能合约交互时，会收取费用。这通常通过一个易于使用的前端（如应用程序或网站）发生，前端作为零售用户和底层智能合约之间的接口。在这种情况下，任何费用都将源于该前端。上面关于app.xyz的例子说明了对于第1层应用程序，费用系统可以如何运作。

应用程序可以不依赖策展人来筛选前端费用，也可以对贡献网络费用的前端采取白名单或黑名单方法。这里的目的仍然是确保代币持有者和整个协议不会因为非法活动而获利或受益，并且遵守特定于司法管辖区的法律和法规。

在白名单方法中，应用程序将为前端发布一套规则，创建一个遵守规则的前端注册表，向选择加入的前端发放证书，并要求前端质押代币以接收应用程序费用的一部分。如果前端不遵守这些规则，它们将被削减，并取消其费用贡献的证书。

在黑名单方法中，应用程序不必创建任何规则，但启动应用程序的前端将不是无需许可的。相反，应用程序将要求任何前端在启用前端使用应用程序之前，提供法律事务所的意见，证明前端符合其司法管辖区的合规性。一旦收到意见，应用程序将向前端发放费用贡献的证书，只有在应用程序收到监管机构通知前端不合规的情况下才会被撤销。

费用路径将反映前几节提供的例子。

这两种方法都显著增加了去中心化治理的负担，要求DAO要么建立和维护一套规则，要么评估关于合规性的法律意见。在某些情况下，这可能是可以接受的，但在大多数情况下，将这种合规负担外包给设定人会更可取。

# 应用链的考虑因素

应用链是针对特定应用的区块链，其验证者仅针对该应用工作。

作为工作的回报，这些验证者会收到付款。与第1层区块链不同，那里的验证者通常基于代币的通胀发行获得奖励，一些应用链（如dYdX）则将客户费用传递给验证者。

在这种模式下，代币持有者必须质押给验证者才能获得奖励。验证者成为经过设定的质押模块。

这项工作设置与第1层验证者不同。应用链验证者解决特定应用的特定交易。由于这种差异，应用链验证者可能承受与其促进的基础活动相关的更高程度的法律风险。因此，协议应该给予验证者根据其司法管辖区的法律和他们自己的舒适度执行工作自由。重要的是，如果其验证者集合在地理上是分散的，这可以在不危及应用链的无需许可性或使其面临重大审查风险的情况下完成。

希望利用费用可追溯性好处的应用链的架构将与第1层应用程序类似，直到费用通道。但验证者将能够使用前端映射来确定他们希望处理来自哪些前端的交易。任何给定交易的费用随后将流向活跃的验证者集合，而选择不参与的不活跃验证者将错过这些费用。从费用的角度来看，验证者执行与上文讨论的质押模块设定人相同的功能，而对这些验证者的质押者可以确保他们没有从任何非法活动中获得收入。验证者也可以选举一个策展人来确定哪些前端在每个司法管辖区合规。

# 应用程序汇总注意事项

Rollups拥有自己的区块空间，但可以继承另一条链的安全性。如今大多rollups都有一个单一的序列生成者，负责排序和包含交易，尽管交易可以通过一个称为“强制包含”的过程直接提交给第1层。

如果这些rollups是特定于应用的，并将它们的序列生成者确立为唯一的验证者，那么由该序列生成者包含的交易所生成的费用可以基于合规前端的设定集分配给质押者，或者作为一个通用池。

如果rollups去中心化它们的序列生成者集合，序列生成者就成为了事实上的设定质押模块，费用管道将反映应用链的情况。序列生成者取代验证者进行费用分配，每个序列生成者可以自行决定接受哪些前端的费用。

尽管应用代币有许多可能的模型，提供策展质押池是一条向前发展的路径，有助于解决应用所独有的外在挑战。通过认识到应用面临的内在和外在挑战，创始人可以更好地从头开始为他们的项目设计应用代币模型。

致谢：我们要感谢Porter Smith启动了这个项目。

这里表达的观点是个别AH Capital Management, L.L.C.（“a16z”）人员的个人观点，并非a16z或其附属公司的观点。