如何实现Web3生态系统向以账户为中心转变？

加密货币生态系统大多采用链中心视角，这种设计理念主要是由于对区块链空间稀缺性的感知所驱动的，是安全性和去中心化与性能和扩展性之间的权衡。如今多链环境下，跨链交互需求越来越明显，而以链为中心的设计导致了交易效率低下和用户体验碎片化的问题。为了优化跨链操作，链抽象这一概念被提出，抽象出底层链的复杂性，实现不同区块链之间更加顺畅的交互。在这样的背景下，专注于 MEV 等话题的独立研究机构Frontier Research的研究员Stephane Gosselin和Ankit Chiplunkar提出名为「OneBalance」的新概念，通过构建一个以账户为中心的生态系统实现链抽象。

### OneBalance 框架的构成与功能

OneBalance是一个框架，用于创建和管理所谓的「可信账户」来整合用户在多链环境中的操作和资产。这些账户在可信承诺机上运行，通过资源锁定管理状态并可靠地请求状态转换，从而提供一个更安全、更高效的跨链交互方式。OneBalance 的目标是改变目区块链上的任何操作，都要依赖用户用私钥签名来发起的现状。

可信账户（Credible Accounts）是 OneBalance 框架中的核心组成部分，在可信承诺机上运行，以便实现跨链功能和高安全性。这种账户类型不仅管理用户在不同区块链上的资产和状态，而且能够确保这些状态的变更请求是可靠且安全的。可信账户抽象化了底层区块链的复杂性，简化跨链交易和资产管理。此外，可信账户还抽象化了交易费用，比如不同链上的 Gas 费，这样用户不用再关注不同链的费用结构。

可信承诺机（credible commitment machines）是实现可信账户功能的底层技术基础，通常是指可以执行并保障复杂操作安全性的硬件或软件环境，包括硬件安全模块（TEE），多方计算环境（MPC），或是智能合约账户等。它们的主要职责是确保账户的安全性，发出资源锁定，并验证这些锁的履行。通过可信承诺机，OneBalance 确保所有账户操作都是在一个高度安全和验证过的环境中进行，提升交易的可靠性和防篡改能力。

资源锁定（resource locks）是一种在可信账户中使用的机制，主要用于在满足特定条件之前锁定用户资产或状态。资源锁的设计目的是确保在跨链操作期间资产的安全性和一致性，防止用户在操作执行期间进行双重支出或其他类型的欺诈行为。例如，用户可以在一个链上锁定特定的代币，直到另一个链上的操作成功完成，从而保证这些代币只有在所有预定条件得到满足后才会被转移或释放。这种锁定机制提高了跨链交易的安全性，但并不意味着消除了对桥接的需求。

OneBalance 本身其实是不能保证完全的执行原子性，但它可以通过锁定机制来激励原子性。用户可以为锁定机制允许设置触发条件：一是必须满足的特定条件才会触发锁定；二是在完成特定交易之后才能解锁，也就是锁定的履行取决于一系列外部事件的发生。如果链间的部分操作未能如预期执行，执行这些操作的代理将无法从中获得经济利益，这样可以经济上保障操作的原子性。



### 与现有账户类型的对比

现有的两种主要账户类型：外部拥有账户（EOA）和智能合约账户（SCA）。EOA 是最基础的区块链账户类型，由公私钥对直接控制，不涉及任何智能合约的逻辑。由于链上没有机制确保用户提交的交易是其最终决定的交易，用户可以通过更改 nonce 提交新交易，从而抵消之前的交易，所以虽然 EOA 交易速度较快且成本较低，但它们无法提供可信承诺。SCA 是通过智能合约来管理和控制的账户，允许执行更复杂的逻辑和交易。但 SCA 不能主动发起交易，并且成本高。

相比现有的两种主要账户类型，OneBalance 通过资源锁定和可信承诺机提高了交易的安全性和不可抵消性，同时保持了交易的速度和成本效率。通过在可信计算环境中内部实现资源锁，无需消耗大量 Gas 或等待链上最终性，实现了成本和效率的平衡，同时OneBalance 支持使用现代的身份验证方法，如会话密钥和多因素认证（MFA），提供与智能合约账户类似的用户体验改进。

此外，OneBalance 可以兼容 EIP-4337 实现的账户系统，可以在需要时利用 EIP-4337 实现的智能合约逻辑来增强其跨链账户管理功能。但 OneBalance 不局限于使用账户抽象和 4337 的链，它是一个通用框架，应用范围更广。OneBalance 可以视为在 EIP-4337 的基础上，扩展了其理念并增加了跨链功能。

通过实施 OneBalance 框架，在多链环境中对用户账户和资产进行集中管理和操作，有望推动 Web3 生态系统向以账户为中心视角转变。OneBalance 提供了统一的账户接口，使得用户能够在不同区块链间无缝交易，无需关心各链之间的差异。这种集中式的账户管理还为用户提供了更高级的安全功能和自定义设置，增强了用户对资产的控制和保护。