零信任协议（ZTP）的工作原理及重要性

作者：wallet 来源：dWallet Labs 翻译：善欧巴，本站

零信任架构是一种安全模型，需要持续验证每个操作，消除固有的信任，从而实现跨整个 Web3 的安全、本机交互。

### 零信任 vs 城堡和护城河

零信任架构是一种现代的网络安全方法，强调验证一切和不信任任何事物。该模型确保每个操作、访问请求和互动都经过彻底的身份验证和授权，消除固有信任。

城堡和护城河模型是一种较旧的网络安全方法。在这种模型中，在受信任的内部网络（城堡）周围建立一个安全的边界（护城河）。一旦进入这个边界，实体就可以获得广泛的访问权限而无需进一步审查。虽然这种模型在较简单的网络环境中有效，但在处理当今复杂和互联的数字环境时却显得力不从心。这种方法的主要弱点在于依赖于“护城河”的不可渗透性，并假设威胁总是外部的，忽略了内部漏洞或被盗用的凭证的可能性。

零信任的开发是为了应对城堡和护城河模型的漏洞。在零信任中，无论网络内外的每个实体，除非被证明可信，否则都被视为不可信。这意味着每个操作、访问请求和互动都必须经过严格的身份验证和授权过程。

### 零信任在Web3中的自然契合

零信任在Web3中并不新鲜。自比特币诞生以来，区块链技术一直采用零信任方法。在区块链网络中，没有任何实体被信任。相反，每个用户都可以独立验证每笔交易，从头到尾确保协议被正确遵循。这个验证过程消除了对任何权威，包括运行网络的节点的信任需求。



在一个假设场景中，想象一个名为Castleum的区块链，它采用城堡和护城河模型。在这里，验证者处理交易并更新区块链状态而无需用户验证，如果共识机制被破坏，就会产生潜在的漏洞。相比之下，以太坊的零信任架构要求用户签署交易，验证者在验证其真实性后才将其包含在区块中，而这种真实性是由每个用户验证的。



### 主权和蜜罐问题

随着Web3的发展，许多区块链网络应运而生，每个网络都在其自身的领域内运作。虽然这些网络在其边界内保持零信任，但在需要不同区块链之间的互操作性时会出现挑战。传统的连接这些网络的方法涉及到牺牲零信任原则，回归城堡和护城河模型。

“主权问题”源于连接独立区块链网络的需求，需要信任第三方来管理跨链交互。这个受信任的实体（或实体）成为单点故障，牺牲了零信任模型。此外，这些解决方案会成为攻击者的诱饵，称为“蜜罐问题”。控制的资产越多，恶意行为者突破其防御的动机就越大。

### 孤立的ZTPs

ZTPs（零信任协议）是采用零信任架构的Web3协议。它们需要对每个操作进行持续验证，确保没有任何实体被固有地信任。在一个孤立的网络中，ZTPs是Web3的标准，通过确保仅涉及该网络的原生资产来保持零信任模型。这意味着在像以太坊这样的单一区块链中，可以为涉及该链的原生资产的交易保持零信任，从而实现“孤立的ZTPs”。

以Uniswap为例，这是以太坊上的一个流行的去中心化交易所。当用户想要交换两个以太坊原生资产，如UNI和ETH时，Uniswap作为一个零信任协议运行。该协议继承了以太坊的零信任架构，确保每笔交易都可由所有用户验证。



与 wBTC 交互时，Siled ZTP（Uniswap）作为 CMP 运行。wBTC/ETH 是目前 Uniswap 上最大的矿池。

然而，如果用户想要交换ETH和wBTC（Wrapped Bitcoin），情况就会改变。wBTC是依赖于中心化托管人（BitGo）的BTC衍生品。在这种情况下，Uniswap失去了其零信任性质，因为wBTC的安全性依赖于BitGo的城堡和护城河架构，需要用户信任BitGo而不是独立验证交易。这使得Uniswap作为一个城堡和护城河协议（或CMP）运行。

由于用户不能在Uniswap内直接与其他网络（如BTC或SOL）的代币进行交互，他们必须依赖依赖于城堡和护城河架构的衍生包装资产，使得Uniswap成为一个孤立的ZTP。这通常包括传统的跨链解决方案，如桥接、跨链消息传递、联合MPC。



### 2PC-MPC：ZTPs的未来

为了创建不局限于其部署网络的ZTPs，dWallet网络使用高级加密方法来保持不同网络之间的零信任。dWallet网络的2PC-MPC加密协议使ZTPs可以在各种区块链生态系统中运行而不妥协其零信任原则。通过加密地要求用户参与，dWallet确保每个操作都是可验证的，没有任何实体被信任。

2PC-MPC是一种加密方案，允许两方（在本例中为用户和dWallet网络）共同生成对任何网络的签名，涉及数百到数千个去中心化节点，形成一个非串通和大规模去中心化的系统。用户的参与确保了零信任，而dWallet网络的参与通过协议强制执行逻辑，创建了ZTPs的基础设施。



### ZTPs的工作原理

用户和网络参与：任何交易或操作要被验证，用户和dWallet网络都必须参与。用户的参与对生成必要的加密签名至关重要。

去中心化验证：dWallet网络由大量节点组成，共同验证用户输入和交易细节。这个去中心化验证过程确保没有单一实体可以控制或操纵交易。

跨链交互：ZTPs允许在不同区块链网络之间进行安全交互。例如，用户可以与以太坊和比特币上的资产进行交互而不妥协零信任模型。dWallet网络确保所有操作在这些网络之间都经过验证和认证。



### ZTPs的实际应用

Vitalik Buterin已经表达了对跨链应用的怀疑，主要是由于区块链之间的桥接固有的安全限制，特别是在面对对安全性较弱的链上的51%攻击时，强调了这些连接的城堡和护城河架构的风险，特别是在面临51%攻击时，会危及安全性较强的链上的原生资产。



ZTPs对于一个不依赖城堡和护城河架构的多链世界是必要的。提供去中心化托管、多链DeFi和非托管钱包解决方案。

### 结论

零信任协议（ZTPs）对于维护多链Web3的安全性和完整性至关重要。通过要求持续验证和消除固有信任，ZTPs确保不同区块链网络之间的交互是安全和有韧性的。使跨任何区块链的安全交互成为可能，为创新的去中心化应用铺平了道路。

随着我们继续探索区块链技术的潜力，通过ZTPs拥抱零信任原则将对构建安全和互操作的Web3生态系统至关重要。