**一文了解 DeFi 时代的 ZK KYC：合规方向的有力竞争者**

[[](https://foresightnews.pro/column/detail/200)](https://foresightnews.pro/column/detail/200)

**[Cabin VC](https://foresightnews.pro/column/detail/200)**

**[2022-11-22 15:29](https://foresightnews.pro/column/detail/200)**

来源链接

订阅此专栏

收藏此文章

长久以来，KYC 领域的项目在「用户隐私」与「用户认证」两难选择中寻找平衡。

**原文标题：《Weekly Brief | ZK-KYC：合规方向的有力竞争者》**

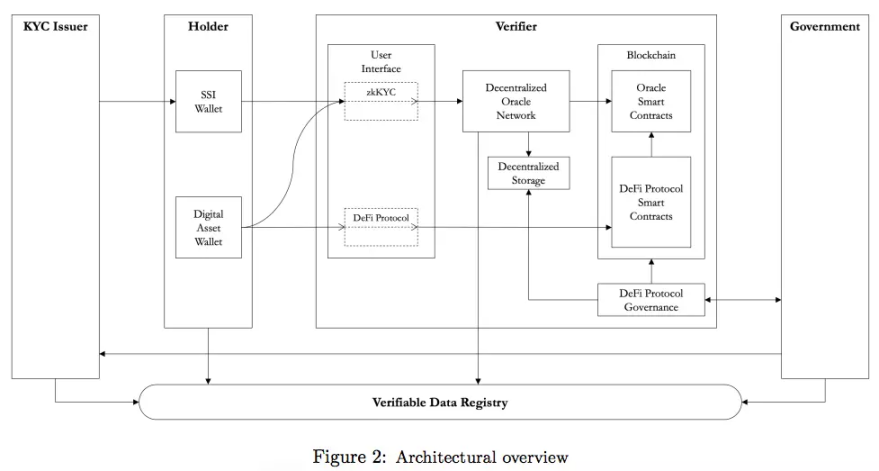
**撰文：Cabin VC**

在大量 Web2 传统机构向 Web3 过渡的过程中，合规是一个重要话题。传统金融市场体量庞大，但链上市场的安全与信任基础设施仍未准备好。

链上 DApp 的 KYC 赛道正在扩展，KYC 对于传统机构大规模的资金来说，是其安全、顺利地进入 Crypto 领域的必经之路，通过 KYC 的机构和个人们可在这个新兴领域共同释放流动性。

Tornado cash 监管等事件给 Crypto 市场带来的思考，基于 KYC 服务的项目也在更新迭代。长久以来，KYC 领域的项目在「用户隐私」与「用户认证」两难选择中寻找平衡。而随着零知识证明的成熟度提升、技术普适性增强，ZK-KYC 这一 ZK 细分领域正在受到更多关注。

2021 年 9 月，《zkKYC in DeFi》论文中概括了在 DeFi 中实现 ZK-KYC 解决方案的生态体系：

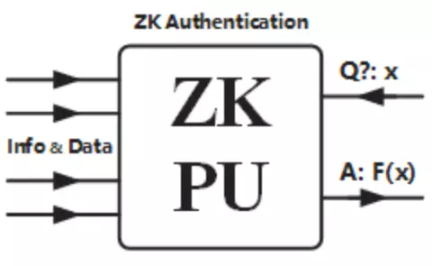
*（https://eprint.iacr.org/2022/321）*

出于监管透明的目的，DeFi 中的 ZK-KYC 不要求与 DeFi 协议共享任何个人身份信息。zkKYC 解决方案通过 DID 及零知识证明，引入 KYC 发行方和去中心化 Oracle 网络 (DON) 作为关键组件。「KYC 发行方」在不接触用户数字资产钱包信息（或 DeFi 活动）的情况下验证个人身份；而 DeFi 协议在不知道用户身份的情况下，与用户数字钱包交互。在某些情况下，仅指定的治理实体（图中为政府机构）才能触及受怀疑的用户身份。

《ZK-KYC and ZK Authentication Process》对 ZK-KYC 进行了更准确的定义：在不知道客户的任何直接信息下做出对该客户的认证判断过程，叫做零知识了解你的客户，即 ZK-KYC (Zero Knowledge-Know Your Customer)。

*（\* 其他相关的定义还有：其中在零知识的情况下做出判断的技术，称为 ZK 认证技术 ( Authentication Technology)，使用 ZK 认证技术完成对客户、资产、事件等认证的过程，称为 ZK 认证过程 (Authentication Process)。*

该论文进一步阐释了 ZK 认证过程如何实现：



零知识认证处理器 ZKPU（Zero Knowledge Processing Unit）需要对输入信息进行处理，并与既定的表针 Protocol 进行核对，增加用户于基础公钥的数据维度，以 ZK 认证的方式实现用户关联资产增信、信用核实等信息的各项工作。

该核心环节往往设计复杂，可能使用到的技术包括但不限于：边缘计算、区块链协议、ZK 认证算法、加密算法、异步计算等等，ZKPU 的形态根据应用场景也非常多样，如算法函数、链上节点、预言机等等。

ZKPU 的设计需要做到：

1. 证明其认证问题的有效性，并且保证
2. 不会对外泄露或被攻破获取实际数据

ZK-KYC 最终的呈现形式将是能够包括个人隐私、满足监管需要、为 DeFi 协议营造合规环境，例如：用户利用自己的信息在链下通过自己的设备以 ZK 生成 ZK Proof，随后通过 Proof 即可验证是否为白名单的用户。随后，某一 DeFi 协议与 KYC 发行方（或服务商）合作，以用户出示的 zk proof 证明其符合监管，并允许用户使用该协议。这种方式也易于 Web2 机构方接受。

近段时间，币安公布了入选币安孵化器第五季孵化计划的 12 个项目，其中就包括了 zkDID 赛道的隐私去中心化 KYC 解决方案 zkPass。zkPass 旨在通过 MPC 用于防止欺诈（用户伪造数据），并使用 ZKP 保护用户隐私。

此外，该赛道中值得关注的还有：去中心化 KYC NFT 提供商 IdentDeFi、链上零知识证明身份平台 0xHolonym 等。

<https://foresightnews.pro/article/detail/19586>