DOI: 10.7544/issn1000-1239.ps20240201
61(2): 273−273, 2024

区块链去中心化平台与代币的转账信息不一致问题的发掘与检测

苏　洲

（西安交通大学网络空间安全学院　西安　710049）

随着区块链去中心化平台的经济体量逐年攀高，对区块链去中心化平台和区块链代币的代码审查已经愈加趋于严谨，出现了大量基于去中心化平台或代币的研究. 然而，鲜有针对去中心化平台和代币的交互问题进行研究，尤其是代币的实际转移与去中心化平台所期望的转移被默认为一致. 根据可见的攻击实例，这一类交互问题实际上大量存在且造成了巨大的经济损失. 文章将该类交互问题总结为“去中心化平台预期代币转移与代币本身的转移之间的不一致问题”. 针对这样一个长久以来被忽视的安全问题基本处于黑盒的状态，这篇文章对该问题进行了研究，提出了有效的检测方法以及对结果进行了剖析.

1. 该论文通过研究去中心化平台的合约中记录代币转移信息的数据结构、该数据结构改变量和代币合约中的数据结构改变量之间的关系来探索未发现的安全问题或财产风险，探究了合约攻击的可能性和隐藏的漏洞.

2. 该论文提出了一种自动化方法，针对区块链去中心化平台与代币间存在的不一致问题进行深入研究. 通过这一方法，作者成功开发了一个名为 DEALS 的工具. DEALS 不仅具备自动化特性，而且具有出色的性能和准确度，专门针对转账信息的潜在问题进行监测和分析，结合了智能合约的静态和动态分析技术，从而确保对转账信息问题全面和深入地检测.

3. 该工作梳理了为去中心化平台提供核心功能的函数，这些函数是去中心化平台运作的基石. 作者分析了去中心化平台的记账模式并从中总结了 3 种去中心化平台常用于存储代币转账信息的数据结构类型，揭示了去中心化平台存储转账信息的本质.

4. 该论文使用 DEALS 工具对多个主流的去中心化平台和代币合约进行了深入的实验检测. 这些实验的目标是识别实际运营环境中存在的不一致问题，验证 DEALS 工具的准确性和有效性，并发现了大量去中心化平台与代币的转账信息存在问题的交易，为区块链安全领域提供了大量可供研究的对象和数据.

5. 该论文揭示了 10 类导致不一致问题的原因，每一种原因不仅都得到了详细的描述，而且对原因都进行了深入的解析，从而揭示了其中的根本性机制和可能导致的后果.

该论文的工作让区块链去中心化平台与代币之间的交互更加透明可信，使区块链安全的可解释性得到了进一步的提升，因此在区块链领域具备可喜的科学价值. 我相信该项研究方向具备继续深入研究的科学价值，并期待它在区块链安全领域带来更多的创新与突破.

评述专家



苏洲，西安交通大学网络空间安全学院教授. 主要研究方向包括通信网络安全、物联网安全、信息物理融合系统安全等.

亮点论文

姜人楷，宋书玮，罗夏朴，陈厅，罗瑞杰，王炳森，乔翱. DEALS——追踪代币转账信息不一致 [J]. 计算机研究与发展，2024, 61(2): 274−288. DOI: 10.7544/issn1000-1239.202330613