使用 Phalcon 浏览器分析和调试交易

Raymond

Jun 2023

About BlockSec

Building blockchain ***security infrastructure***

- 2021年由顶级的学者和安全专家成立
- 提供安全审计服务，开发先进安全工具，服务行业头部机构
- 行业第一个并且至今仍是唯一完成线上攻击阻断并挽救了超过 1400 万美元

  e.g.：Paraspce、Saddle Finance

BlockSec 旗下代表性产品

Phalcon

为开发者和 DeFi 团队服务
的安全开发套件

MetaDock

为 DeFi 和 NFT 用户提升区
块链浏览器易用性的插件

MetaSleuth

可视化加密资金分析
和追踪工具

BlockSec Phalcon

为开发者和 DeFi 团队服务的安全开发套件

- Explorer: 浏览和分析交易
- Debugger: 在线调试交易
- Simulator: 在线模拟和预执行
- Fork: 保留主网状态创建自己的私有测试链

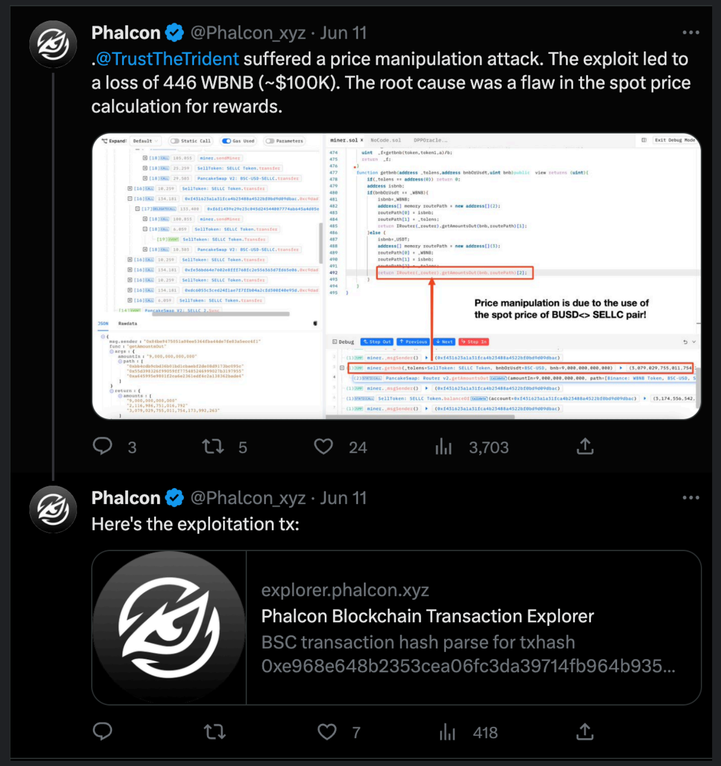
phalcon.xyz

为什么我们要开发 Phalcon 浏览器?

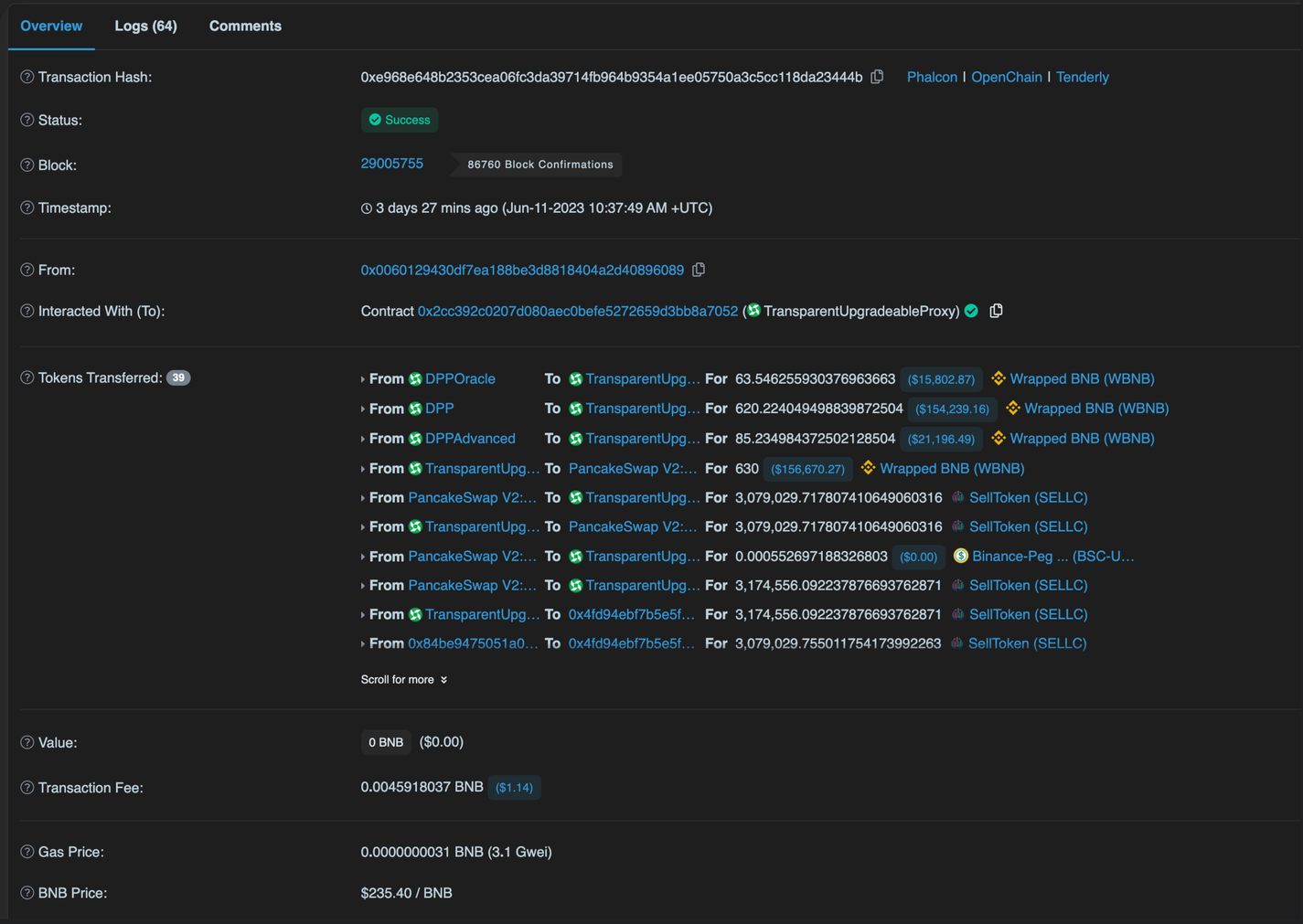
主流区块链浏览器的不足之处（Etherscan-like）

- 缺乏结构化 Trace，无法理解复杂交易
- 缺乏细粒度的交易变化，无法查看细微但重要的变化
- 只有静态数据，无法动态的捕捉变化过程和中间结果

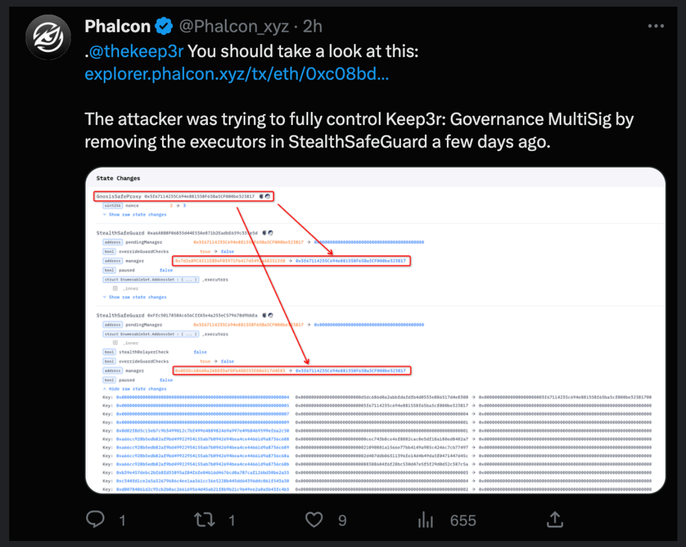
不足一：缺乏结构化 Trace，无法理解复杂交易



示例交易



不足二：缺乏细粒度的交易变化，无法理解交易变化的结果



示例交易

Value:	0 ETH ($0.00)
Transaction Fee:	0.0061445472927740398 ETH $10.74
Gas Price:	35.790074106 Gwei (0.000000035790074106 ETH)
Ether Price:	$1,739.25 / ETH
Gas Limit & Usage by Txn:	218,027 | 171,683 (78.74%)
Gas Fees:	Base: 34.290074106 Gwei | Max: 40 Gwei | Max Priority: 1.5 Gwei
Burnt & Txn Savings Fees:	Burnt: 0.005887022792740398 ETH ($10.29) Txn Savings: 0.000722772707259602 ETH ($1.26)
Other Attributes:	Txn Type: 2 (EIP-1559) Nonce: 6 Position In Block: 75

Input Data:

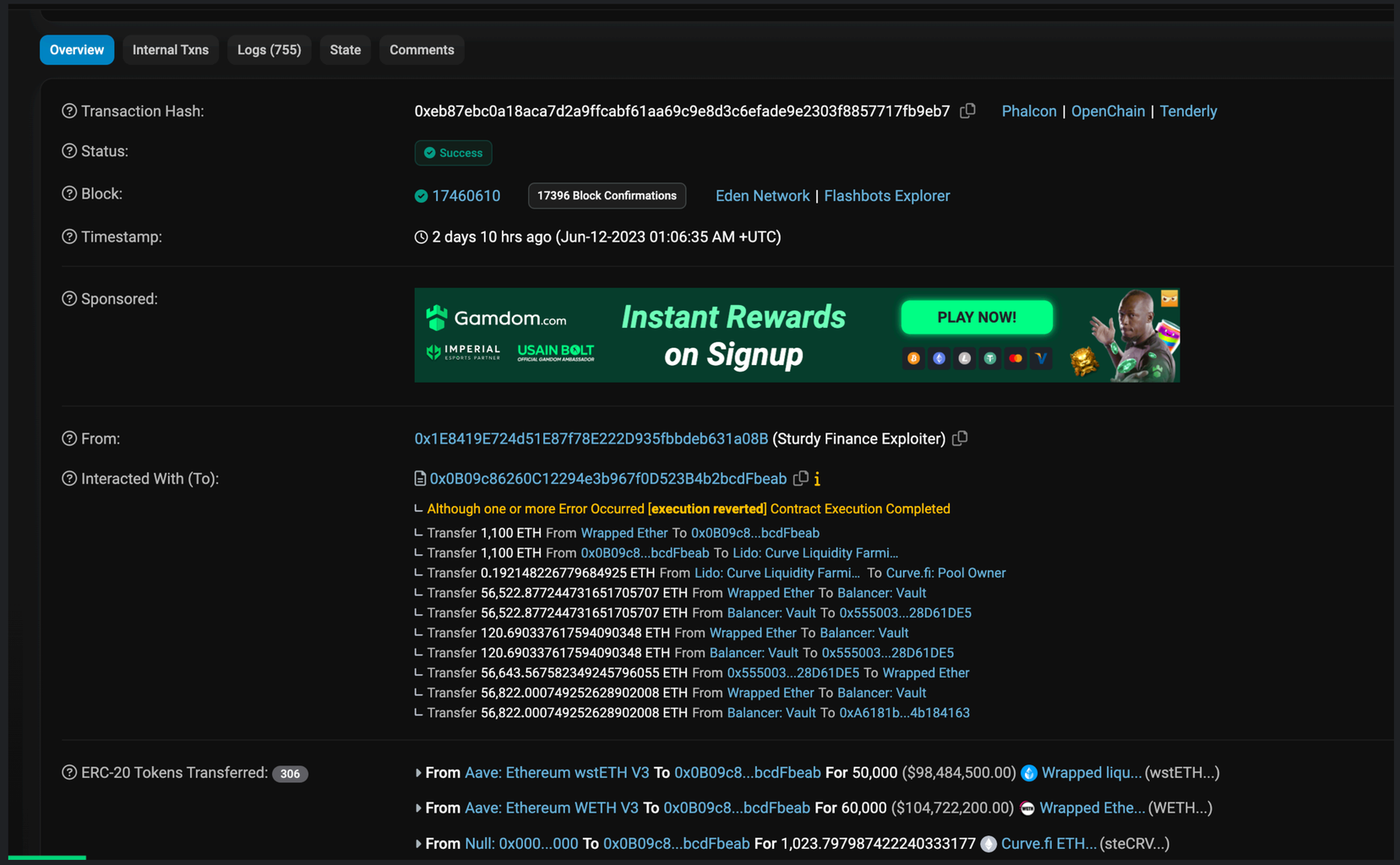
```
Function: execTransaction(address to, uint256 value, bytes data, uint8 operation, uint256 safeTxGas, uint256
baseGas, uint256 gasPrice, address gasToken, address refundReceiver, bytes signatures)

MethodID: 0x6a761202
[0]:  000000000000000000000000040a2accbd92bca938b02010e17a5b8929b49130d
[1]:  0000000000000000000000000000000000000000000000000000000000000000
[2]:  0000000000000000000000000000000000000000000000000000000000000140
[3]:  0000000000000000000000000000000000000000000000000000000000000001
```

View Input As · Decode Input Data

不足三：只有静态数据，无法动态的捕捉变化和中间结果

示例交易



Phalcon Explorer

核心功能

- 调用树
- 调试器
- 模拟器
- 资产变动统计表
- 资金流向图
- 状态变化统计
- Gas 火焰图

目标用户

开发者

- 在线分析和调试
- Gas 分析和优化

安全研究员

- 安全事件分析
- POC 撰写

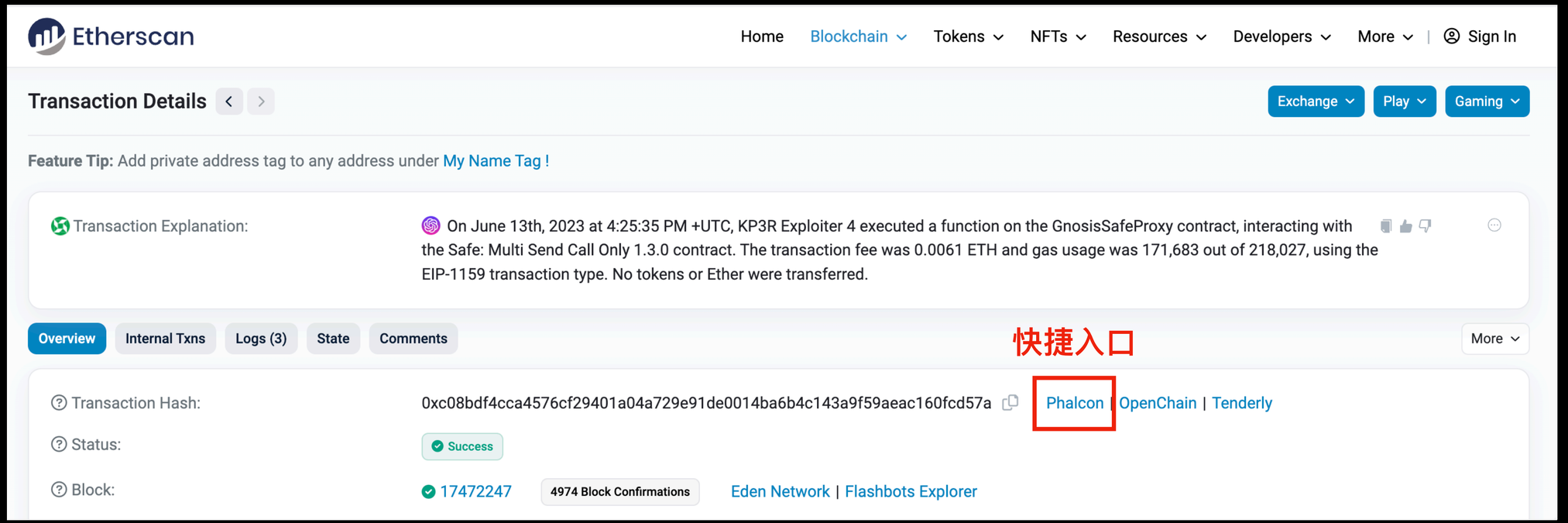
DeFi 用户

- 读懂交易

Phalcon 实战演示

- **MetaDock**: 专为 Web3 开发者、安全研究员和活跃用户设计的插件

  完全开源，完全免费，无广告，插件不收集任何数据



Building Blockchain Security Infrastructure

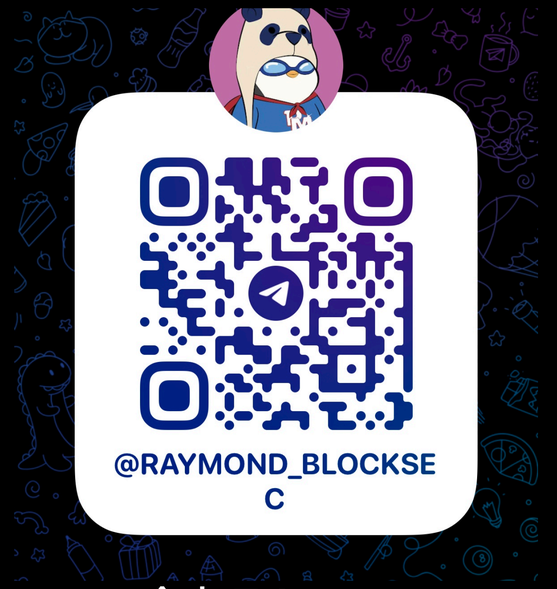
Phalcon: https://Phalcon.xyz

Twitter:

- @BlockSecTeam
- @phalcon_xyz
- @MetaDockTeam
- @MetaSleuth

官网: https://blocksec.com

技术和安全事件讨论群组
(仅限英文)



个人 Telegram
(中英文)