

# 使用 Phalcon 交易模拟器和 Fork

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



## 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

Q phalcon.xyz



# Phalcon 交易模拟器

## Simulator

# 典型使用场景

交易员, DeFi 用户

## 预执行交易

Pre-execution

昂贵的试错成本

开发者

## 参数调试

Debug

效率低, 不够真实细致

安全研究员

## 回放历史交易

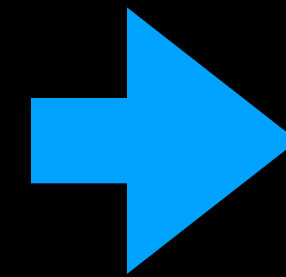
Playback

复杂情况回放成本高

# 传统工具不足之处

## 现状

- 需要配置本地环境
- 需要归档节点
- 性能比较差
- 新人容易踩坑



## 问题

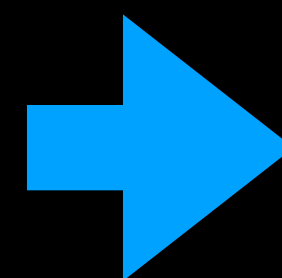
- 门槛高
- 成本高
- 效率低
- 不友好



# Phalcon 交易模拟器

## 传统解决方案

- 需要本地安装环境
- 需要归档节点
- 性能比较差
- 新人容易踩坑



## Phalcon

- 无需配置本地环境
- 无需归档节点
- 行业领先的性能
- 1 分钟上手



# Simulator 实战演示

示例一

示例二

# 总结

- 支持自动获取 ABI，填写参数进行模拟
- 支持使用本地 ABI，模拟没有开源的合约
- 支持直接修改链上交易进行模拟
- 提供准确和详细的模拟交易分析能力
- 无需节点和配置本地环境
- 行业领先的模拟速度
- 1 分钟上手



# Phalcon Fork

保留主网状态创建自己的私有测试链

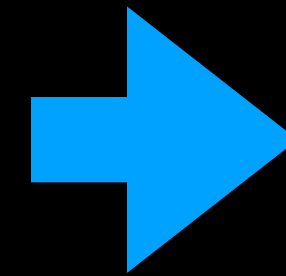
\*目前支持 ETH/BSC/Polygon, 更多公链陆续支持中

# 本地开发到主网运营存在巨大 Gap

## 真实案例

- Akutar ~\$34M
- Wintermute ~2M \$OP
- zkSync Transfer ~\$1.7M
- Nomad Bridge ~\$154M
- Aave 更新

...



## 测试面临严重挑战

- 环节缺失
- 严重受限
- 多链环境复杂
- 成本高昂

# Fork 核心能力和特性

镜像，可控，高效，兼容，协作，私有，安全

- 从主网上的任意区块和位置创建 Fork，保留主网状态
- 完全控制该 Fork (BlockHeader)
- 灵活多样的使用方式 (MetaMask、RPC、Dashboard)
- 兼容 Hardhat 和 Truffle 的 Debug Method
- 提供水龙头和 Scan 等一系列工具
- 支持多用户协作，团队内部开放，对外保持私密性
- 无缝集成其他 Phalcon 安全工具

# Fork 真机演示

# 典型场景和需求

NFT 等待公售

提前开启公售 -> Mint -> 白名单机制、评估 Gas 消耗和成本

DeFi Staking Claim 收益

Staking -> 批量模拟交易 -> 评估 Claim 成本和收益

DAO 提案或合约升级

提交 Proposal -> Vote -> 推后时间 -> 执行提案 -> 冒烟测试

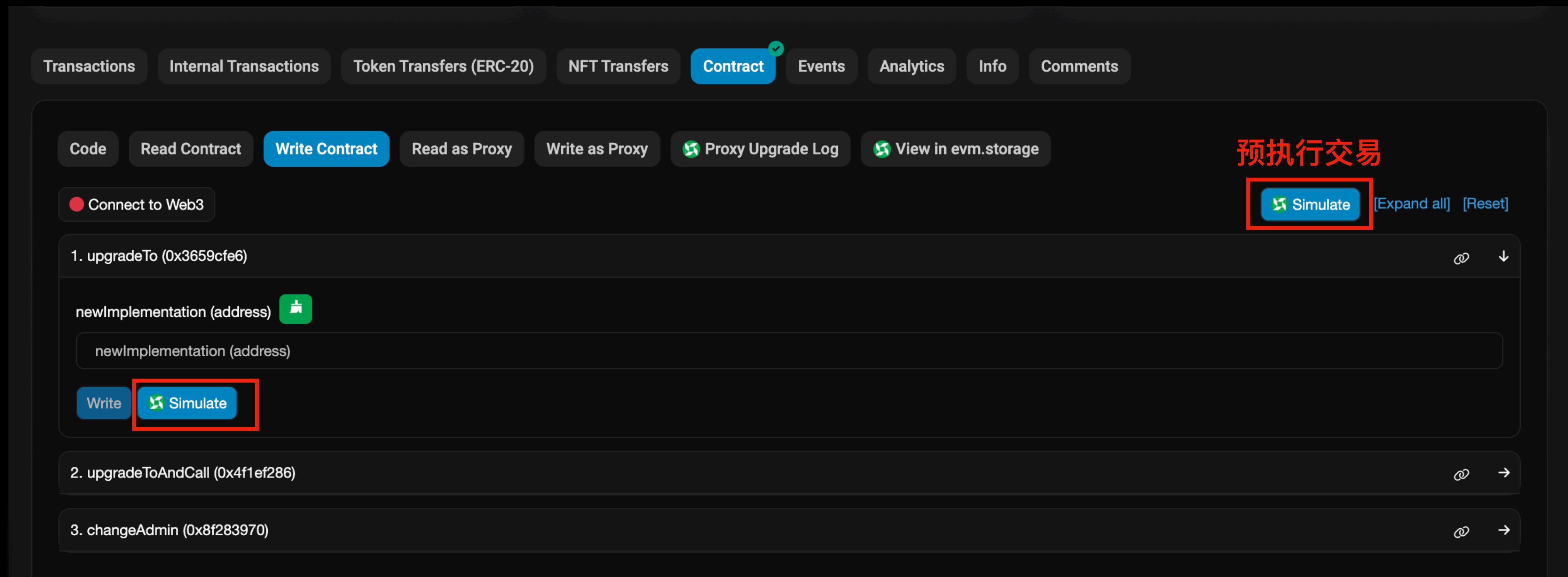
历史事件研究和回放

Fork 高度 -> 布置环境( Header/ Time) -> 回放测试



- **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



The screenshot shows the MetaDock interface with the 'Contract' tab selected. The interface includes a navigation bar with tabs for Transactions, Internal Transactions, Token Transfers (ERC-20), NFT Transfers, Contract, Events, Analytics, Info, and Comments. Below the navigation bar, there are buttons for Code, Read Contract, Write Contract, Read as Proxy, Write as Proxy, Proxy Upgrade Log, and View in evm.storage. A 'Connect to Web3' button is visible. The main content area displays a list of transactions, with the first transaction '1. upgradeTo (0x3659cfe6)' selected. The transaction details show a 'newImplementation (address)' field with a 'Write' button and a 'Simulate' button highlighted in red. The 'Simulate' button is also highlighted in red in the top right corner of the interface, with the text '预执行交易' (Pre-execute transaction) next to it. The 'Simulate' button has a tooltip that says '[Expand all] [Reset]'.

# Building Blockchain Security Infrastructure

Phalcon: <https://Phalcon.xyz>

**Twitter:**

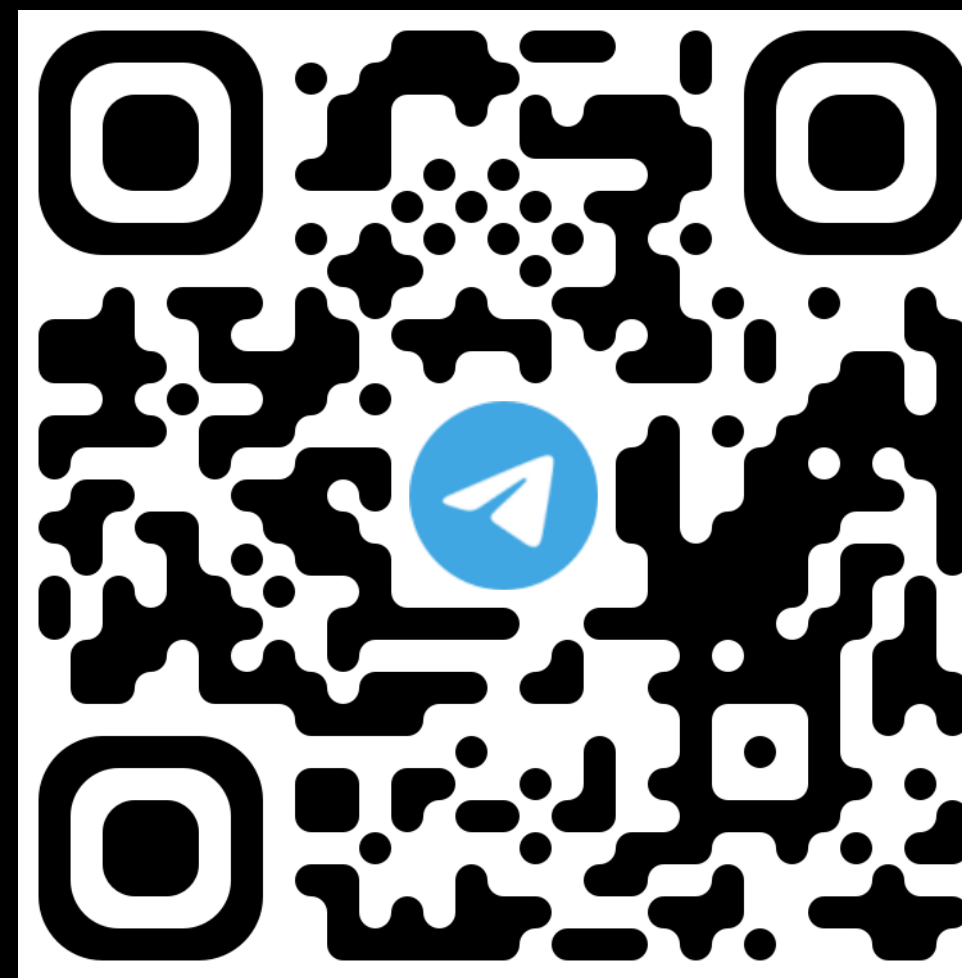
[@BlockSecTeam](https://twitter.com/BlockSecTeam)

[@phalcon\\_xyz](https://twitter.com/phalcon_xyz)

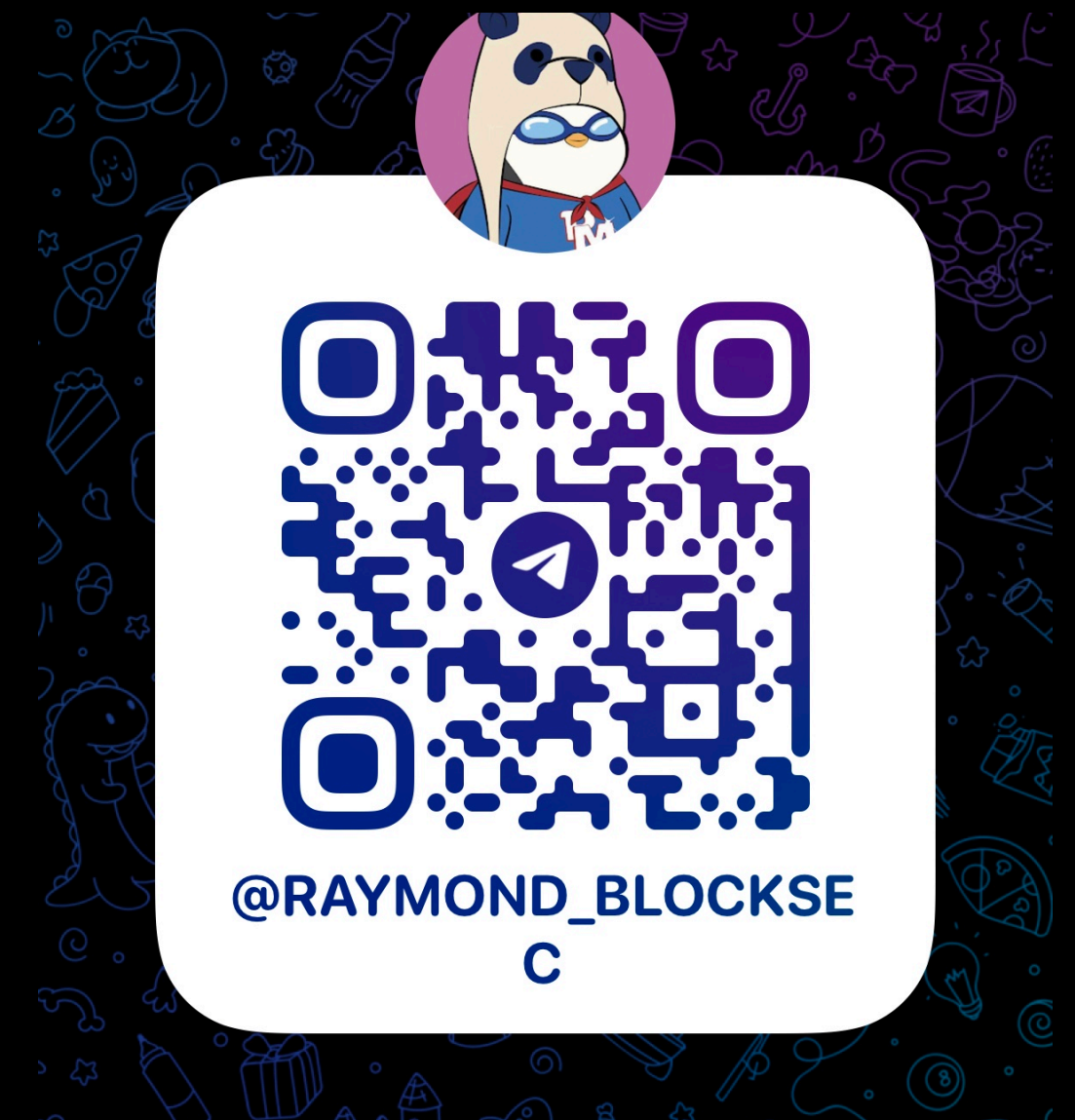
[@MetaDockTeam](https://twitter.com/MetaDockTeam)

[@MetaSleuth](https://twitter.com/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)