

# 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



## 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



# 为什么我们要开发 Phalcon 浏览器?

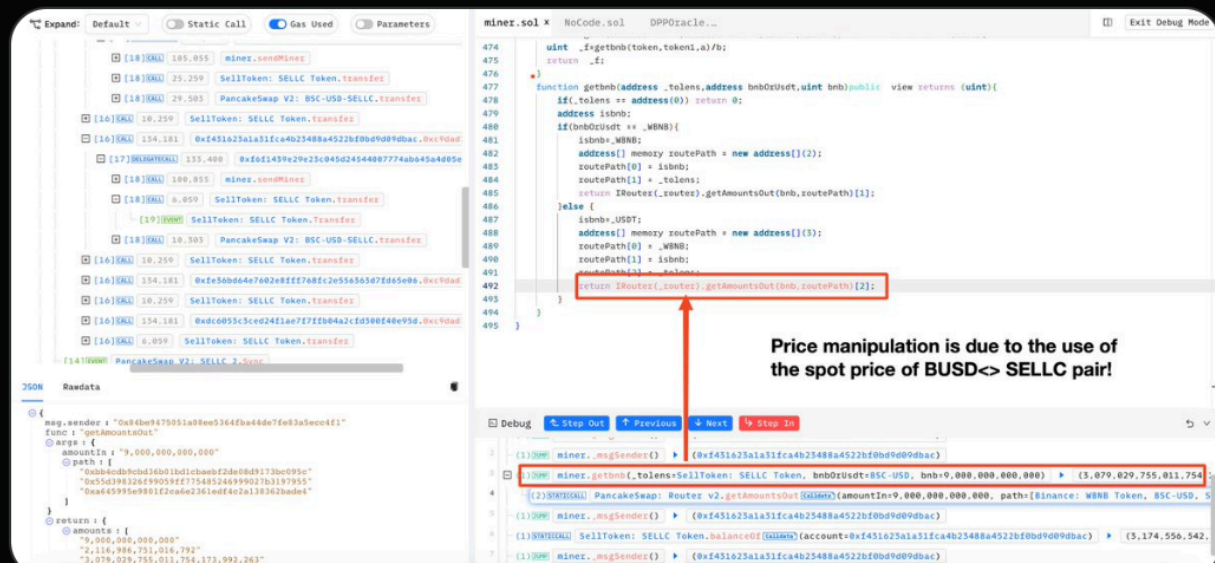
## 主流区块链浏览器的不足之处 (Etherscan-like)

- 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

**Phalcon** @Phalcon\_xyz · Jun 11


.@TrustTheTrident suffered a price manipulation attack. The exploit led to a loss of 446 WBNB (~\$100K). The root cause was a flaw in the spot price calculation for rewards.



3 5 24 3,703

**Phalcon** @Phalcon\_xyz · Jun 11

Here's the exploitation tx:



explorer.phalcon.xyz  
Phalcon Blockchain Transaction Explorer  
BSC transaction hash parse for txhash  
0xe968e648b2353cea06fc3da39714fb964b935...

7 418

## 示例交易

Overview Logs (64) Comments

Transaction Hash: 0xe968e648b2353cea06fc3da39714fb964b9354a1ee05750a3c5cc118da23444b [Phalcon](#) | [OpenChain](#) | [Tenderly](#)

Status: ✔ Success

Block: 29005755 86760 Block Confirmations

Timestamp: 3 days 27 mins ago (Jun-11-2023 10:37:49 AM +UTC)

From: 0x0060129430df7ea188be3d8818404a2d40896089

Interacted With (To): Contract 0x2cc392c0207d080aec0befe5272659d3bb8a7052 ✔ [TransparentUpgradeableProxy](#) ✔

Tokens Transferred: 39

- From ✔ DPPOracle To ✔ TransparentUpg... For 63.546255930376963663 (\$15,802.87) ⚡ Wrapped BNB (WBNB)
- From ✔ DPP To ✔ TransparentUpg... For 620.224049498839872504 (\$154,239.16) ⚡ Wrapped BNB (WBNB)
- From ✔ DPPAdvanced To ✔ TransparentUpg... For 85.234984372502128504 (\$21,196.49) ⚡ Wrapped BNB (WBNB)
- From ✔ TransparentUpg... To PancakeSwap V2:... For 630 (\$156,670.27) ⚡ Wrapped BNB (WBNB)
- From PancakeSwap V2:... To ✔ TransparentUpg... For 3,079,029.717807410649060316 🔗 SellToken (SELLC)
- From ✔ TransparentUpg... To PancakeSwap V2:... For 3,079,029.717807410649060316 🔗 SellToken (SELLC)
- From PancakeSwap V2:... To ✔ TransparentUpg... For 0.000552697188326803 (\$0.00) 💰 Binance-Peg ... (BSC-U...)
- From PancakeSwap V2:... To ✔ TransparentUpg... For 3,174,556.092237876693762871 🔗 SellToken (SELLC)
- From ✔ TransparentUpg... To 0x4fd94ebf7b5e5f... For 3,174,556.092237876693762871 🔗 SellToken (SELLC)
- From 0x84be9475051a0... To 0x4fd94ebf7b5e5f... For 3,079,029.755011754173992263 🔗 SellToken (SELLC)

Scroll for more ⌵

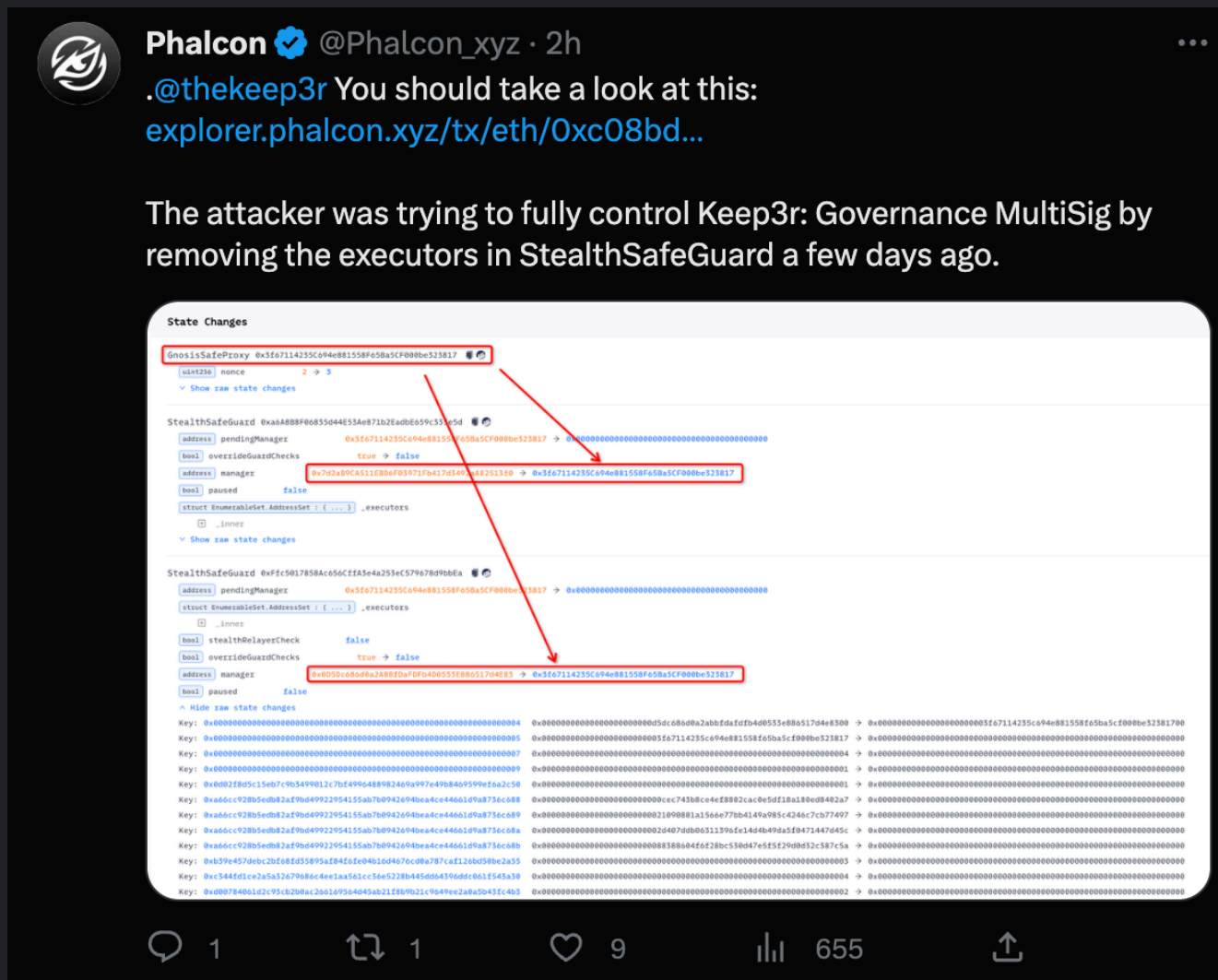
Value: 0 BNB (\$0.00)

Transaction Fee: 0.0045918037 BNB (\$1.14)

Gas Price: 0.0000000031 BNB (3.1 Gwei)

BNB Price: \$235.40 / BNB

# 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: 0.006144547292740398 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]: 0000000000000000000000000040a2accbd92bca938b02010e17a5b8929b49130d

[1]: 00

[2]: 00140

[3]: 0001

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


Overview Internal Txns Logs (755) State Comments

Transaction Hash: 0xeb87ebc0a18aca7d2a9ffcabf61aa69c9e8d3c6efade9e2303f8857717fb9eb7 [Phalcon](#) | [OpenChain](#) | [Tenderly](#)

Status: Success

Block: 17460610 17396 Block Confirmations [Eden Network](#) | [Flashbots Explorer](#)

Timestamp: 2 days 10 hrs ago (Jun-12-2023 01:06:35 AM +UTC)

Sponsored: 

From: 0x1E8419E724d51E87f78E222D935fbbdeb631a08B (Sturdy Finance Exploiter)

Interacted With (To): 0x0B09c86260C12294e3b967f0D523B4b2bcdFbeab [i](#)

- Although one or more Error Occurred [execution reverted] Contract Execution Completed
- Transfer 1,100 ETH From Wrapped Ether To 0x0B09c8...bcdFbeab
- Transfer 1,100 ETH From 0x0B09c8...bcdFbeab To Lido: Curve Liquidity Farmi...
- Transfer 0.192148226779684925 ETH From Lido: Curve Liquidity Farmi... To Curve.fi: Pool Owner
- Transfer 56,522.877244731651705707 ETH From Wrapped Ether To Balancer: Vault
- Transfer 56,522.877244731651705707 ETH From Balancer: Vault To 0x555003...28D61DE5
- Transfer 120.690337617594090348 ETH From Wrapped Ether To Balancer: Vault
- Transfer 120.690337617594090348 ETH From Balancer: Vault To 0x555003...28D61DE5
- Transfer 56,643.567582349245796055 ETH From 0x555003...28D61DE5 To Wrapped Ether
- Transfer 56,822.000749252628902008 ETH From Wrapped Ether To Balancer: Vault
- Transfer 56,822.000749252628902008 ETH From Balancer: Vault To 0xA6181b...4b184163

ERC-20 Tokens Transferred: 306

- From Aave: Ethereum wstETH V3 To 0x0B09c8...bcdFbeab For 50,000 (\$98,484,500.00) [W](#) Wrapped liqu... (wstETH...)
- From Aave: Ethereum WETH V3 To 0x0B09c8...bcdFbeab For 60,000 (\$104,722,200.00) [W](#) Wrapped Ethe... (WETH...)
- From Null: 0x000...000 To 0x0B09c8...bcdFbeab For 1,023.797987422240333177 [W](#) Curve.fi ETH... (steCRV...)



# 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

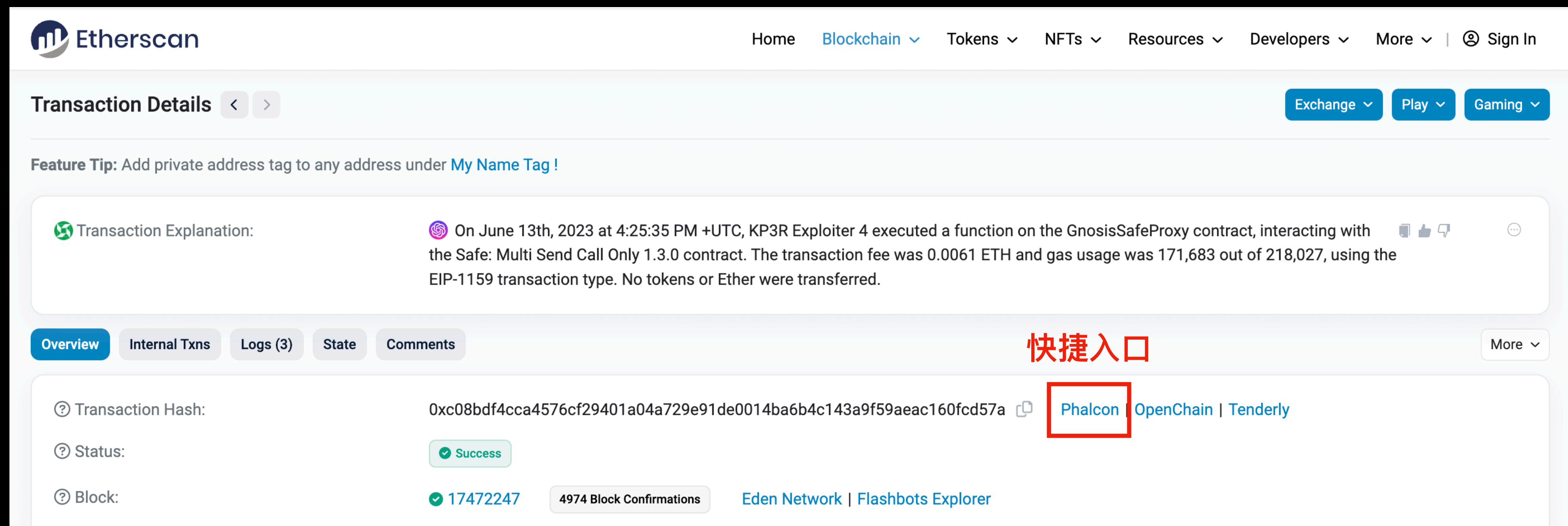


DeFi 用户

- 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



Etherscan Home Blockchain Tokens NFTs Resources Developers More | Sign In

Transaction Details < > Exchange Play Gaming

Feature Tip: Add private address tag to any address under [My Name Tag](#) !

Transaction Explanation: On June 13th, 2023 at 4:25:35 PM +UTC, KP3R Exploiter 4 executed a function on the GnosisSafeProxy contract, interacting with the Safe: Multi Send Call Only 1.3.0 contract. The transaction fee was 0.0061 ETH and gas usage was 171,683 out of 218,027, using the EIP-1159 transaction type. No tokens or Ether were transferred.

Overview Internal Txns Logs (3) State Comments More

Transaction Hash: 0xc08bdf4cca4576cf29401a04a729e91de0014ba6b4c143a9f59aeac160fcd57a [Phalcon](#) OpenChain | Tenderly

Status: Success

Block: 17472247 4974 Block Confirmations Eden Network | Flashbots Explorer

# Building Blockchain Security Infrastructure

Phalcon: <https://Phalcon.xyz>

**Twitter:**

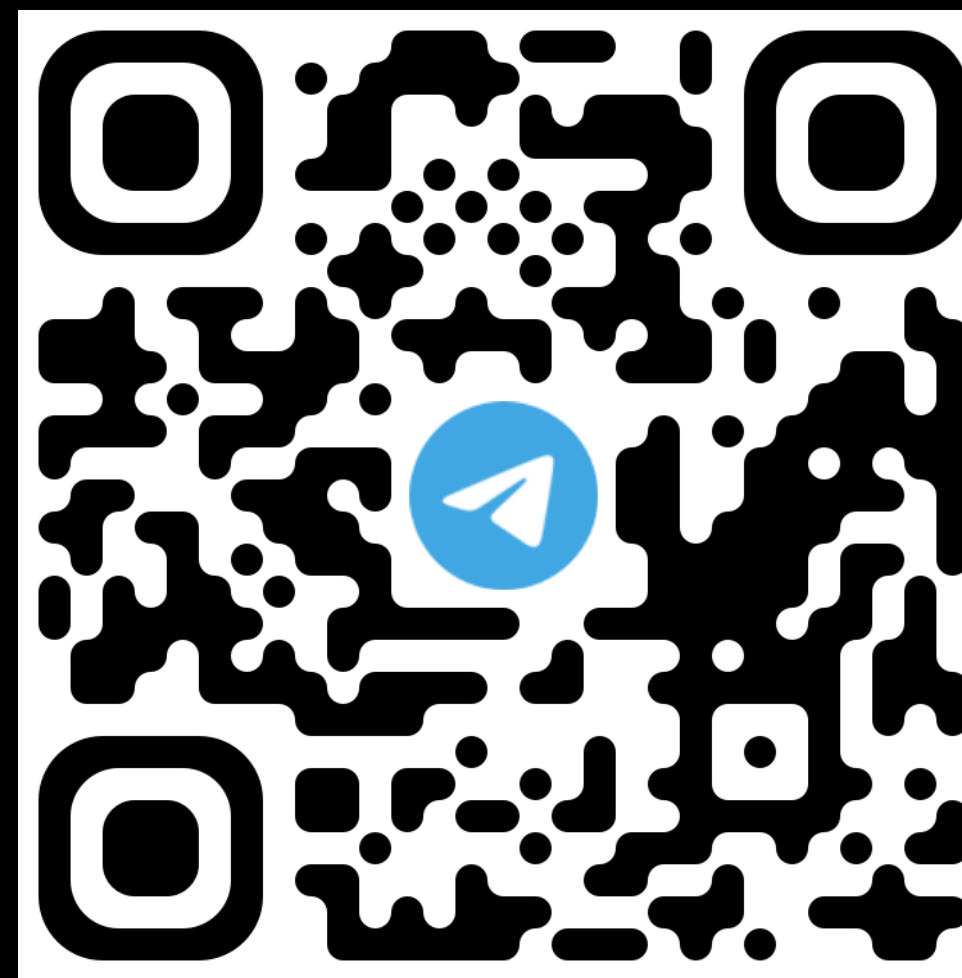
[@BlockSecTeam](https://twitter.com/BlockSecTeam)

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

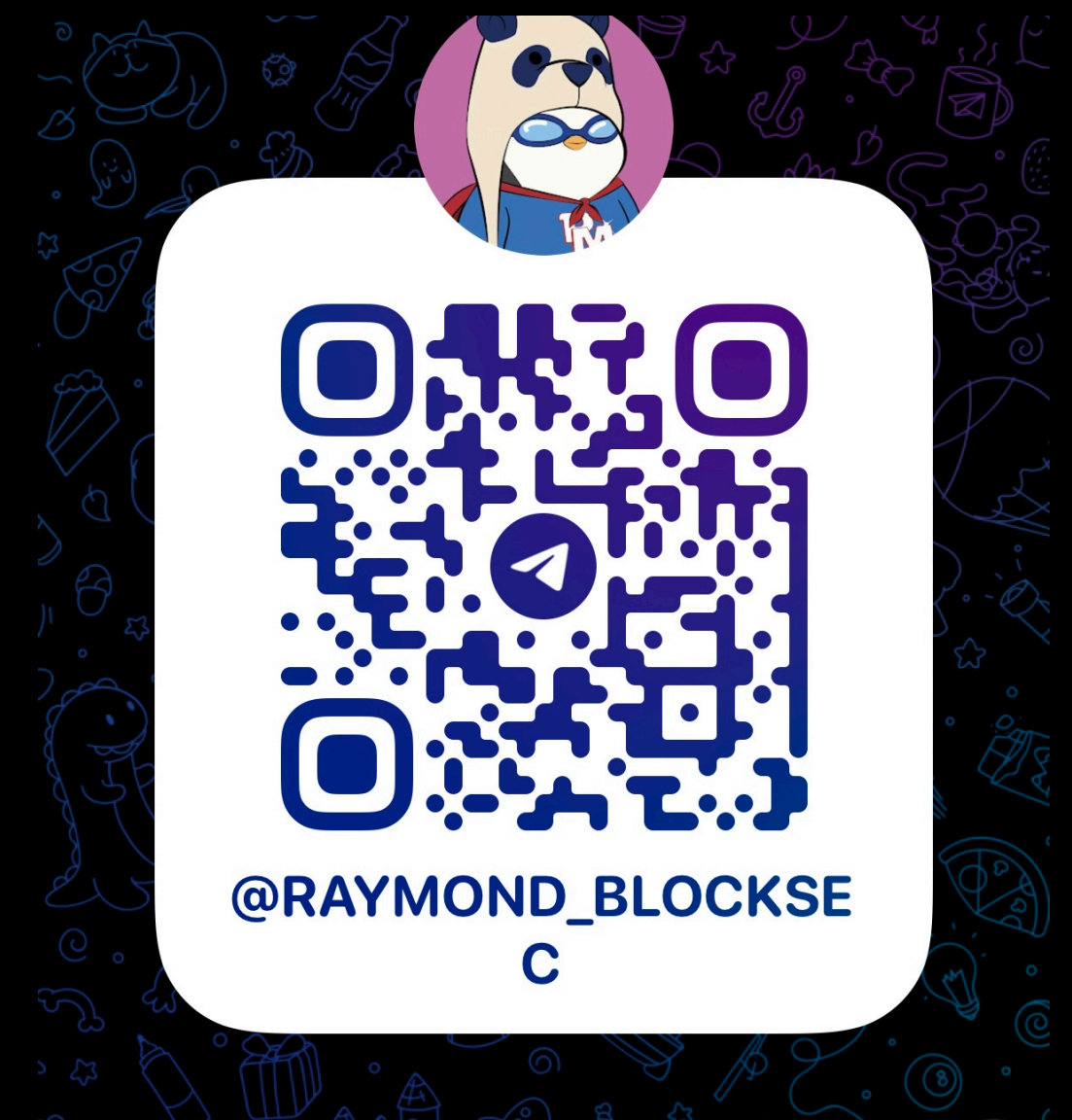
[@MetaDockTeam](https://twitter.com/MetaDockTeam)

[@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)