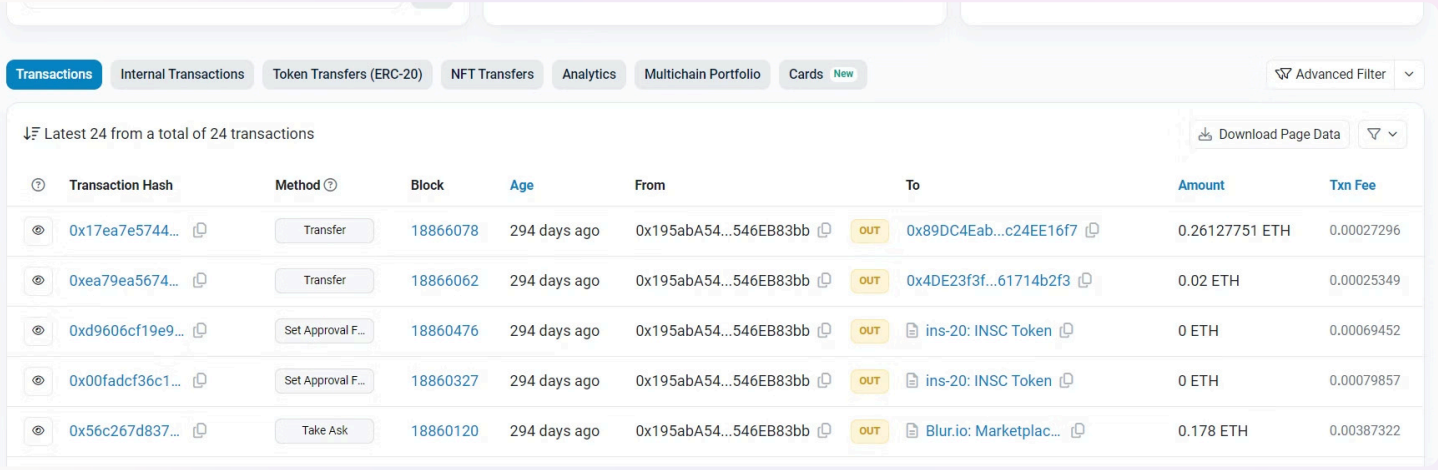
Dec-25-2023，一个圣诞节的冬天



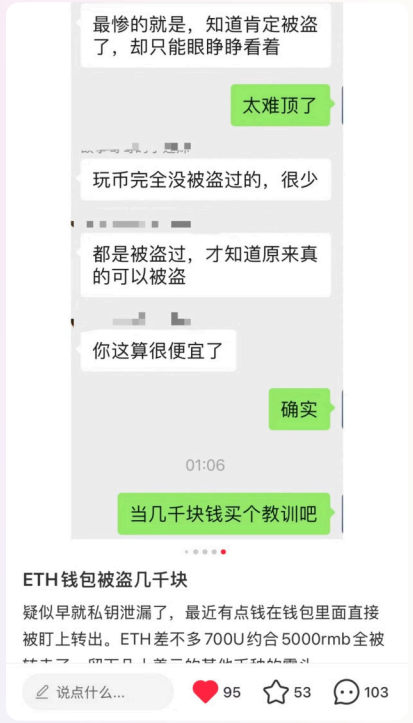
Transactions | Internal Transactions | Token Transfers (ERC-20) | NFT Transfers | Analytics | Multichain Portfolio | Cards New | Advanced Filter

Latest 24 from a total of 24 transactions | Download Page Data

Transaction Hash	Method	Block	Age	From		To	Amount	Txn Fee
0x17ea7e5744...	Transfer	18866078	294 days ago	0x195abA54...546EB83bb	OUT	0x89DC4Eab...c24EE16f7	0.26127751 ETH	0.00027296
0xea79ea5674...	Transfer	18866062	294 days ago	0x195abA54...546EB83bb	OUT	0x4DE23f3f...61714b2f3	0.02 ETH	0.00025349
0xd9606cf19e9...	Set Approval F...	18860476	294 days ago	0x195abA54...546EB83bb	OUT	ins-20: INSC Token	0 ETH	0.00069452
0x00fadcf36c1...	Set Approval F...	18860327	294 days ago	0x195abA54...546EB83bb	OUT	ins-20: INSC Token	0 ETH	0.00079857
0x56c267d837...	Take Ask	18860120	294 days ago	0x195abA54...546EB83bb	OUT	Blur.io: Marketplac...	0.178 ETH	0.00387322

被盗0.28ETH

很可能与打ETH铭文这种新资产有关



香港科大（广州）
区块链协会

Night's Watcher -

以太坊早期交互风险守望者

没头脑与不高兴队

Jupiter

权利的游戏 - 链与链的纷争

	Ethereum 1.0	Ethereum 2.0	Polkadot	Cosmos	Avalanche	NEAR	Solana	BSC
Architecture 区块链架构	单链结构 (同步) Single-chain (synchronous)	多链结构 (分片) Multi-chain (shards)	多链结构 (平行链) Multi-chain (parachains)	多链结构 (IBC-可兼容) Multi-chain (IBC-compatible)	多链结构 (子网络) Multi-chain (subnets)	多链结构 (分片) Multi-chain (shards)	单链结构 (同步) Single-chain (synchronous)	单链结构 (同步) Single-chain (synchronous)
Security 安全性	Global 全局安全性	Shared 共享安全性	Shared (if parachain connected)共享安全性	Blockchain-specific 每条链负责自身的安全性	Shared (validators choose subnets) 共享安全性	Shared 共享安全性	Global 全局安全性	Global 全局安全性
Consensus 共识机制	Proof-of-Work PoW 工作量证明	Casper Proof-of-Stake Casper 权益证明	Nominated Proof-of-Stake NPoS (提名权益证明)	Tendermint Proof-of-Stake Tendermint 权益证明	Avalanche Proof-of-Stake Avalanche 权益证明	Nightshade Proof-of-Stake Nightshade 权益证明	Proof-of-History (PoS) 历史时间证明	Proof-of-Authority 权威证明
VM/ Development 虚拟机/开发	EVM (Solidity, Vyper)	EVM (Solidity, Vyper)	WebAssembly, Substrate	WebAssembly/EVM Cosmos SDK	AVM (Go), Athereum (EVM)	WASM, Aurora (EVM)	Sealevel (Rust)	EVM (Solidity, Vyper)
Validators (today) 验证者数量 (撰文时)	6,000 (nodes)	160,000	300	125	960	60	600	21
Economics 经济学	Variable transaction fees 交易费多变	Variable transaction fees 交易费多变	Market cost for parachain slot 平行链插槽的市场成本	Variable transaction fees 交易费多变	Fixed transaction fees by type 同一类型的交易，交易费是固定的	Variable transaction fees 交易费多变	Variable transaction fees 交易费多变	Variable transaction fees 交易费多变
Governance 治理模式	Off-chain 链下治理	Off-chain 链下治理	On-chain 链上治理	On-chain 链上治理	On-chain 链上治理	On-chain 链上治理	On-chain 链上治理	On-chain 链上治理

但是...用户正面临着前所未有的风险

必须有人做区块链世界的守夜人

Night's Watcher - 以太坊全境捍卫者

守夜人游骑兵

少样本异常账户检测模型（BERT-based）

应对早期和新型风险，如新账户、新交互、新合约

焚烧尸体不留隐患

异常账户污点名单

对所有异常账户部署、交互的合约和地址进行黑灰名单标注

修建巩固长城

Certora形式化验证

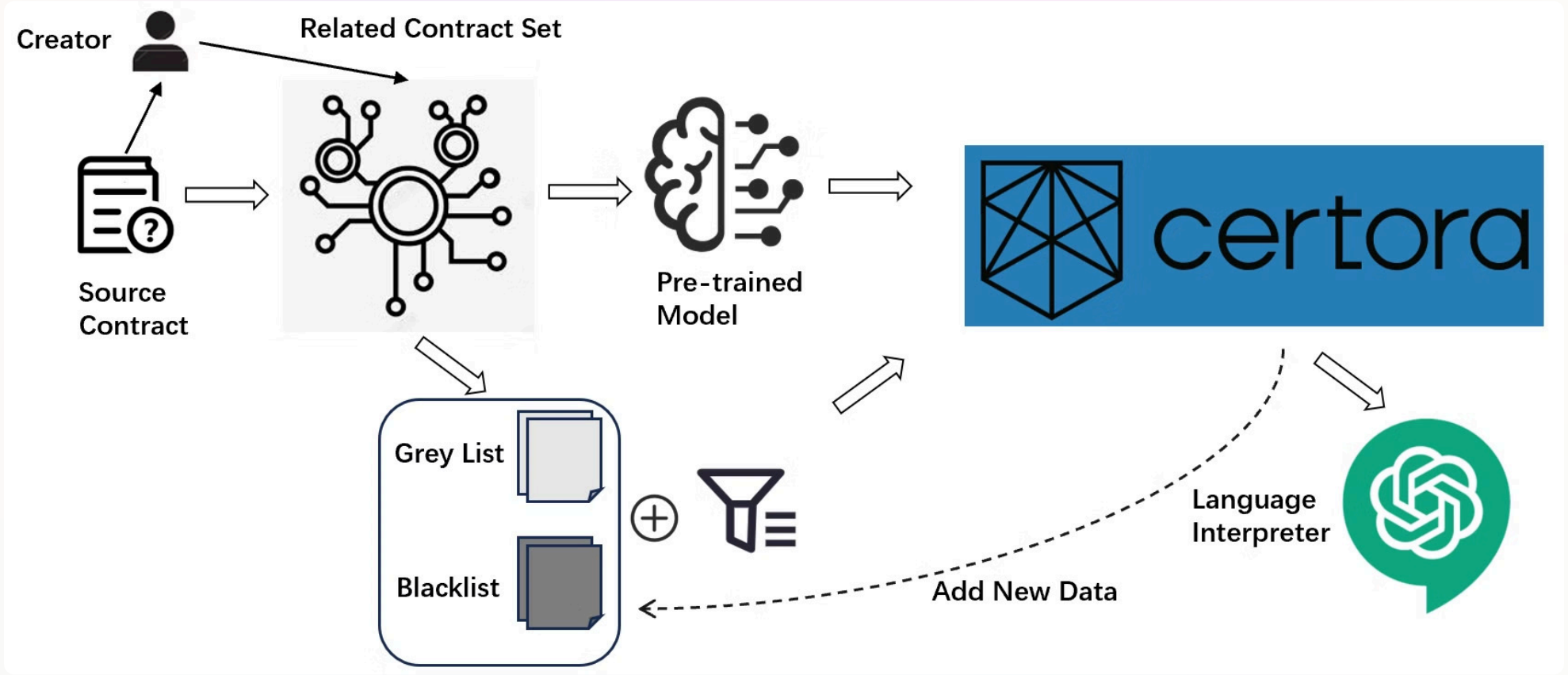
使用形式化规则对合约进行安全性验证

派送渡鸦通知全境

报告生成和用户教育

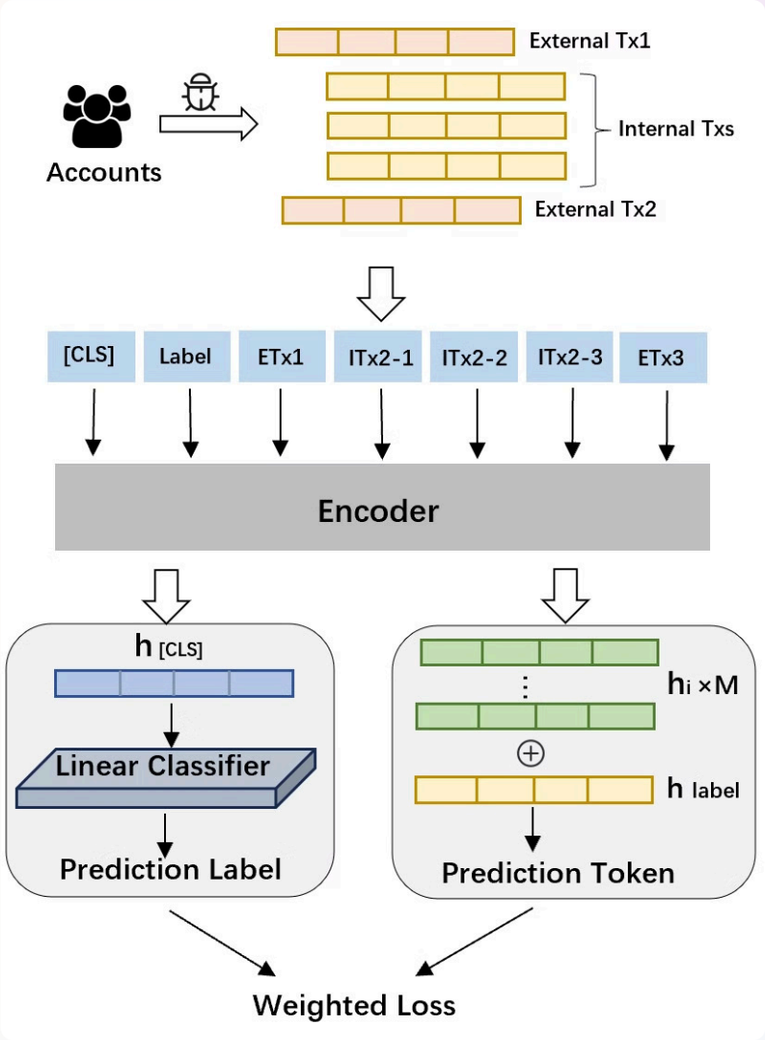
对发现的风险、安全问题进行自然语言标注和提示，减少用户交互风险

可解释的防御系统框架

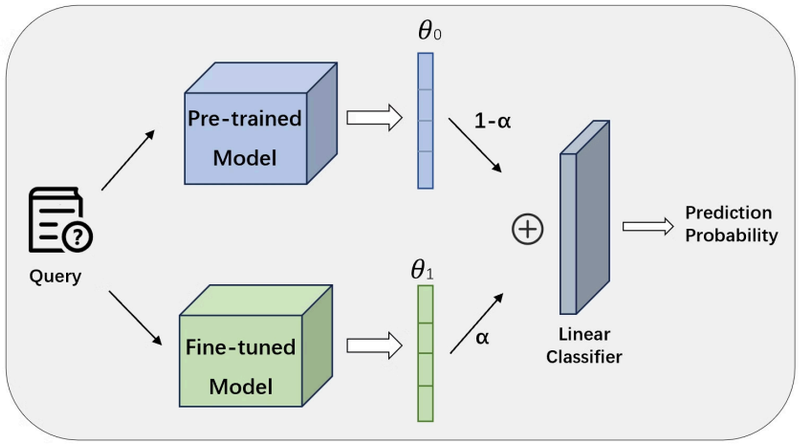


少样本异常账户检测模型

预训练架构



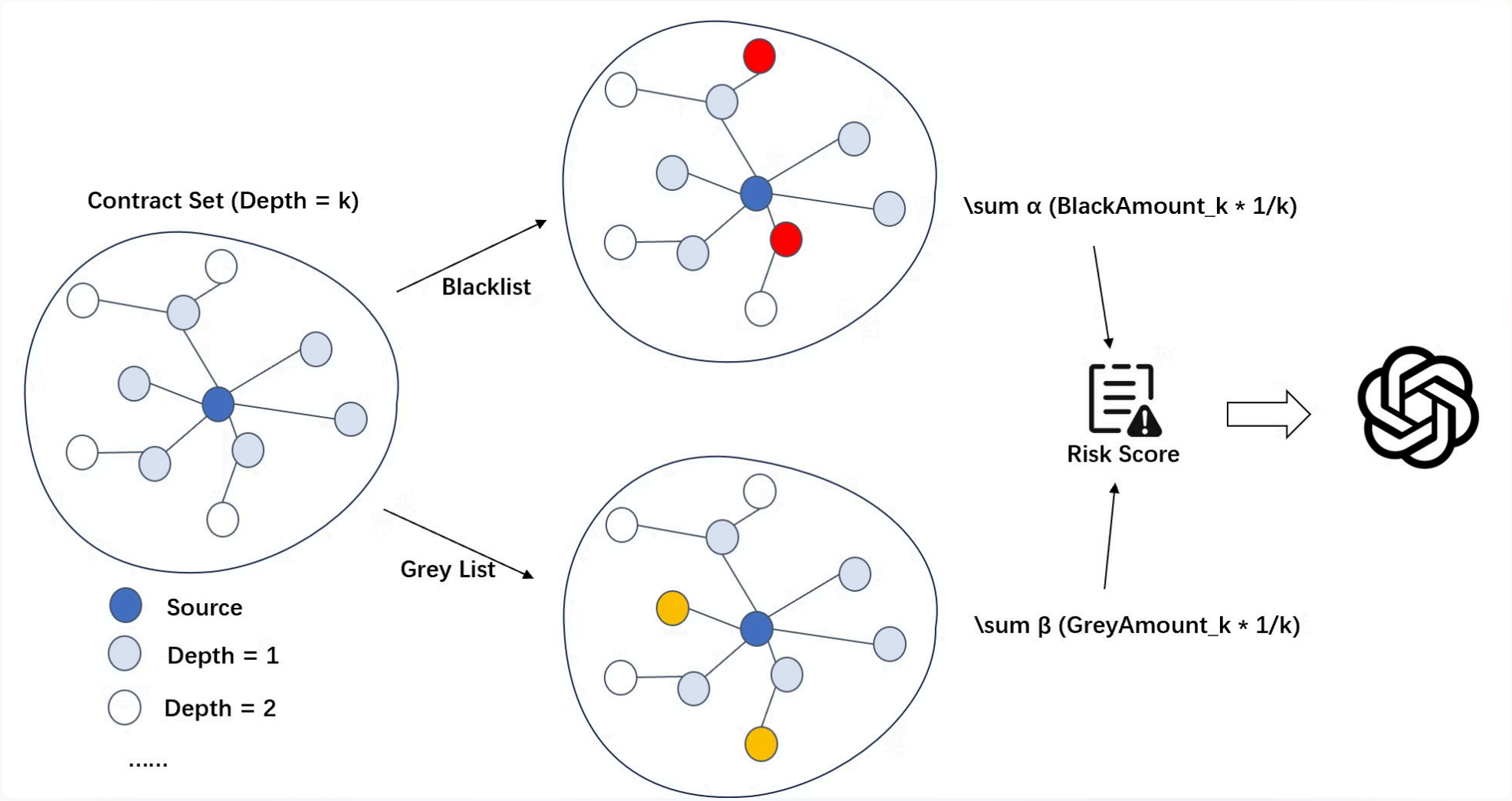
少样本微调策略



检测效果（30-shot）

	标签集	精确度	recall	F1
phisher	5634	0.7129	0.7208	0.7168
Ponzi	314	0.5918	0.6719	0.6294
mevbot	1679	0.8727	0.7385	0.8000
airdropHunter	1437	0.9020	0.7077	0.7931

污点排查过程



Certora形式化验证

Prove your code works with mathematical certainty

Certora Prover is a powerful tool that compares your smart contract bytecode against a rule detailing how you expect your code to behave. This process, known as *formal verification*, will check every possible contract state and contract path to identify critical vulnerabilities that hackers can exploit.

Solidity

/contracts/ERC20.sol

```
contract ERC20 is IERC20, IERC20Metadata {
...
    function transferFrom(address from, address to, uint256 value) public vir
        _spendAllowance(from, msg.sender, value);
        _transfer(from, to, value);
        return true;
    }
...
```

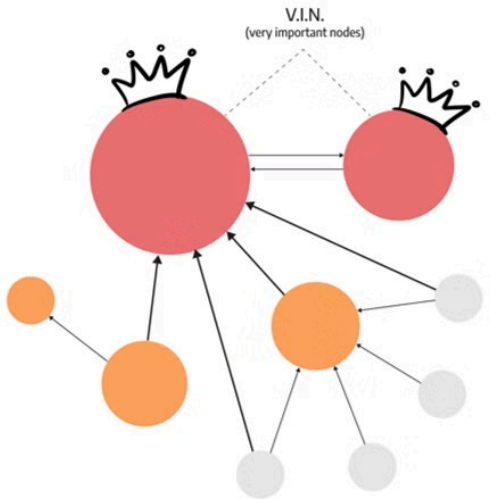
Rule

/specs/ERC20.spec

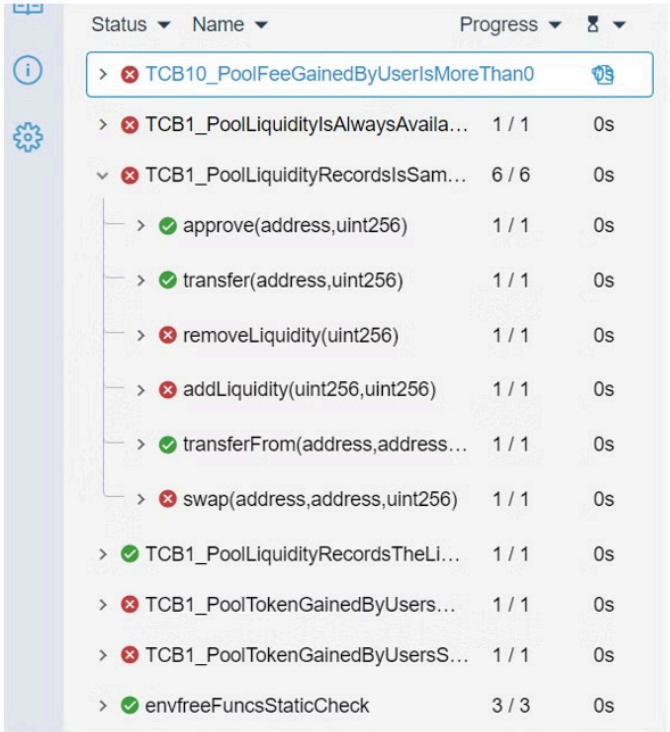
```
// Checks that transferFrom() decreases allowance of `e.msg.sender`

rule checkTransferFrom(address sender, address recipient, uint256 amount) {
    env e; // represents global variables like msg.sender
    require sender != recipient && amount > 0;

    uint256 allowanceBefore = allowance(sender, e.msg.sender);
    transferFrom(e, sender, recipient, amount);
    uint256 allowanceAfter = allowance(sender, e.msg.sender);

    assert (allowanceBefore > allowanceAfter),
        "allowance must decrease..."; // error message
}
```

报告生成&用户教育

风险判定



合约一致性检测



操作指导

Demo演示 - *长夜将至，我们从今开始守望*

YouTube

Night's Watch Demo Bethink Hack

香港科大（广州）
区块链协会

团队 & Thanks

Jupiter

香港科技大学（广州）区块链协会
会长

复旦大学区块链协会 核心成员

数据科学与分析 MPhil

Vertin

香港科技大学（广州）区块链协会
副会长

中山大学 Inplus Lab 核心成员

金融科技（区块链）PhD

扫一扫上面的二维码图案，加我为朋友。

联系我们

社区合作

活动场地

学术交流

开发者培训

....