

Hackathon Tesouro Nacional

por Ewerton Lopes
05/12/2023

Grupo: GUIZO

Solução: Tese: Testes de Interoperabilidade com IA



Solução

A solução proposta neste projeto envolve a aplicação de modelos de machine learning, inspirados na abordagem do Lightning Cat, para realizar testes de segurança em smart contracts do Tesouro Direto do Brasil.

Solução

Identificação de vulnerabilidades específicas:

- Realização de uma análise minuciosa dos protocolos de comunicação entre smart contracts e soluções da Web2.
- Avaliação abrangente de possíveis vulnerabilidades, incluindo exposição de dados sensíveis, manipulação não autorizada, falhas na autenticação e autorização, e garantia da integridade dos dados durante a interoperabilidade.

Solução

Desenvolvimento de modelos personalizados:

- Criação de modelos de machine learning adaptados às nuances dos contratos inteligentes do Tesouro Direto.
- Treinamento dos modelos com dados específicos do Tesouro Direto, levando em conta as regras de negócios, a estrutura do código-fonte e os requisitos de interoperabilidade.
- Validação iterativa para garantir a precisão na detecção de vulnerabilidades específicas.

Solução

Análise estática de código:

- Criação de modelos de machine learning adaptados às nuances dos contratos inteligentes do Tesouro Direto.
- Treinamento dos modelos com dados específicos do Tesouro Direto, levando em conta as regras de negócios, a estrutura do código-fonte e os requisitos de interoperabilidade.
- Validação iterativa para garantir a precisão na detecção de vulnerabilidades específicas.

Solução

Análise dinâmica de execução:

- Simulação de transações para avaliar dinamicamente o comportamento do código em diferentes cenários.
- Detecção de comportamentos anormais durante a execução dos smart contracts.

Solução

Simulações realistas para treinamento:

- Geração de dados sintéticos que representem fielmente os cenários operacionais do Tesouro Direto.
- Utilização de técnicas avançadas, como Redes Generativas Adversárias (GANs), para criar dados sintéticos semelhantes aos dados reais.
- Validação iterativa para garantir a precisão e a relevância dos dados sintéticos.

Solução

IA para detecção de padrões de fraude:

- Desenvolvimento de características específicas para detecção de fraude, considerando padrões temporais, comportamentais e transacionais associados a atividades fraudulentas.
- Aplicação de aprendizado supervisionado e não supervisionado para identificar transações fraudulentas e comportamentos suspeitos.
- Integração com sistemas de prevenção de fraudes para uma resposta proativa a atividades suspeitas.

Público-alvo

O público-alvo desta solução inclui instituições financeiras, desenvolvedores de smart contracts no âmbito do Tesouro Direto do Brasil, reguladores do mercado financeiro e demais entidades envolvidas na gestão e segurança de ativos financeiros.

Além disso, a solução visa beneficiar investidores e usuários finais, garantindo a integridade e segurança de suas transações no contexto do Tesouro Direto.

Problema

O problema central abordado é a segurança dos smart contracts no Tesouro Direto do Brasil, especialmente no que diz respeito à interoperabilidade com soluções da Web2.

A crescente adoção dessas tecnologias traz consigo desafios complexos, como a exposição de dados sensíveis, manipulação não autorizada, falhas na autenticação e autorização, além da necessidade de garantir a integridade dos dados durante a interoperabilidade.

Modelo de negócio

Plataforma de segurança para Smart Contracts:

- Desenvolvimento de uma plataforma que oferece serviços automatizados de testes de segurança para smart contracts, utilizando modelos de machine learning.
- Modelo de subscrição ou pagamento por uso para instituições financeiras e desenvolvedores.

Treinamento e conscientização em segurança:

- Desenvolvimento de programas de treinamento e conscientização em segurança para equipes de desenvolvimento e gestão de ativos financeiros.
- Cursos e workshops

Diferencial competitivo

O diferencial competitivo desta solução reside na abordagem abrangente, integrando modelos de machine learning em diferentes fases do ciclo de vida dos smart contracts.

A combinação de análise estática e dinâmica de código, simulações realistas para treinamento, detecção de padrões de fraude e aplicação contínua de IA oferece uma cobertura ampla e adaptável aos desafios específicos do Tesouro Direto.

Obrigado!
Ewerton Lopes