인공신경망 기반 스마트계약 취약점 탐지 기법 연구 동향

김원웅

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

서론

관련 연구

본론

결론

서론

- 데이터의 위변조를 방지할 수 있는 블록체인 기술이 각광받고 있음

- 그 중 이더리움의 스마트 계약의 특성이 주요하게 작용
  -> but, 다양한 보안 취약점 존재
  -> 따라서, 취약점을 탐지하는 기법들이 연구되었으며,
  그 중 딥러닝 기반 탐지 기법이 활발이 연구되고 있음

관련 연구

- 이더리움
  - 블록체인 플랫폼
  - EVM (Ethereum Virtual Machine)

- 스마트 계약
  - 거래 시 사용
  - 신뢰성 제공

관련 연구

- 스마트 계약 취약점
  - SWC (Smart contract Weakness Classification)
  - 산술 취약성, 재진입성, 알려지지 않은 주소가 포함된 거래

- 스마트 계약 취약점 탐지
  - 기호 실행
  - 형식 검증
  - 퍼지 테스트
  - ML기반 방법

- 인공신경망

본론 [1]

< A new scheme of vulnerability analysis in smart contract with machine learning. >

- 취약점: has_short_address, has_flows, is greedy
- 취약점 특징 추출 방법: slicing matrix
- 취약점 특징 추출 -> 취약점 탐지 모델 (CNN)
- f1-score: has_short_address: 0.91% / has_flows: 0.76% / is_greedy: 0.83%

본론 [2]

< Smart Contract Vulnerability Detection Model Based on Multi-Task Learning. >

- 다중 작업 학습 기반 취약점 탐지
- 하단 공유 계층 / 작업 특화 계층
- 작업 분류 모델 : CNN (Convolution Neural Network)
- F1-score: 산술 취약성 - 24.91% / 재진입 탐지 - 20.73% 향상

본론 [3]

< Smart Contract Vulnerability Detection using Graph Neural Network. >

- 탐지 모델 : GNN (Graph Neural Network)
- 노드 - 함수 호출, 변수 간선 : 임시 실행 추적
- DR-GCN (Degree-free Graph Convolution Neural Network)
- TMP (Temporal Message Propagation)

본론 [4]

< Transaction-based classification and detection approach for Ethereum smart contract. >

- 탐지 모델 : LSTM (Long Short Term Memory)
- Slicing Algorithm (4단계)
- F1-score: 0.691 ~ 0.825

결론

- 스마트 계약에 다양한 취약점 존재
- 기존의 방법은 시간적 비용이 많이 소모됨
- 인공신경망 기반 취약점 탐지 기법들이 효율적으로 사용됨
- 취약점을 탐지하는 것만이 아닌 탐지 유형을 식별하는 기술 또한 연구되어야 한다.

Q & A