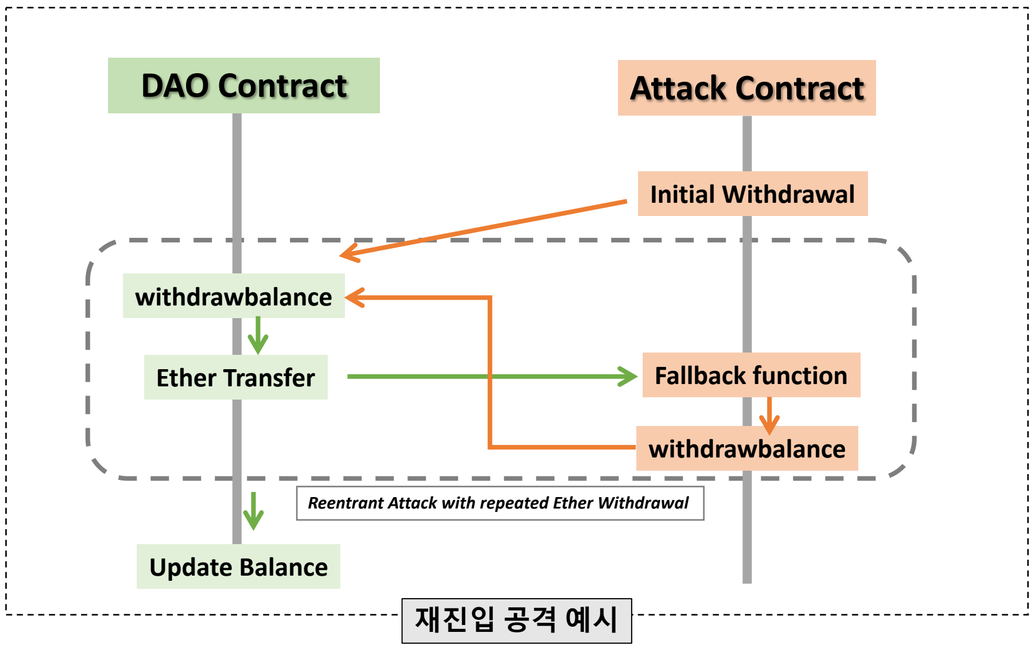
51 Smart Contract 취약점 탐지 툴

소속 정보컴퓨터공학부 분과 D 팀명 컴쪽이 참여학생 김윤하, 최지원, 윤지원 지도교수 최윤호

작품 소개



재진입 공격 예시

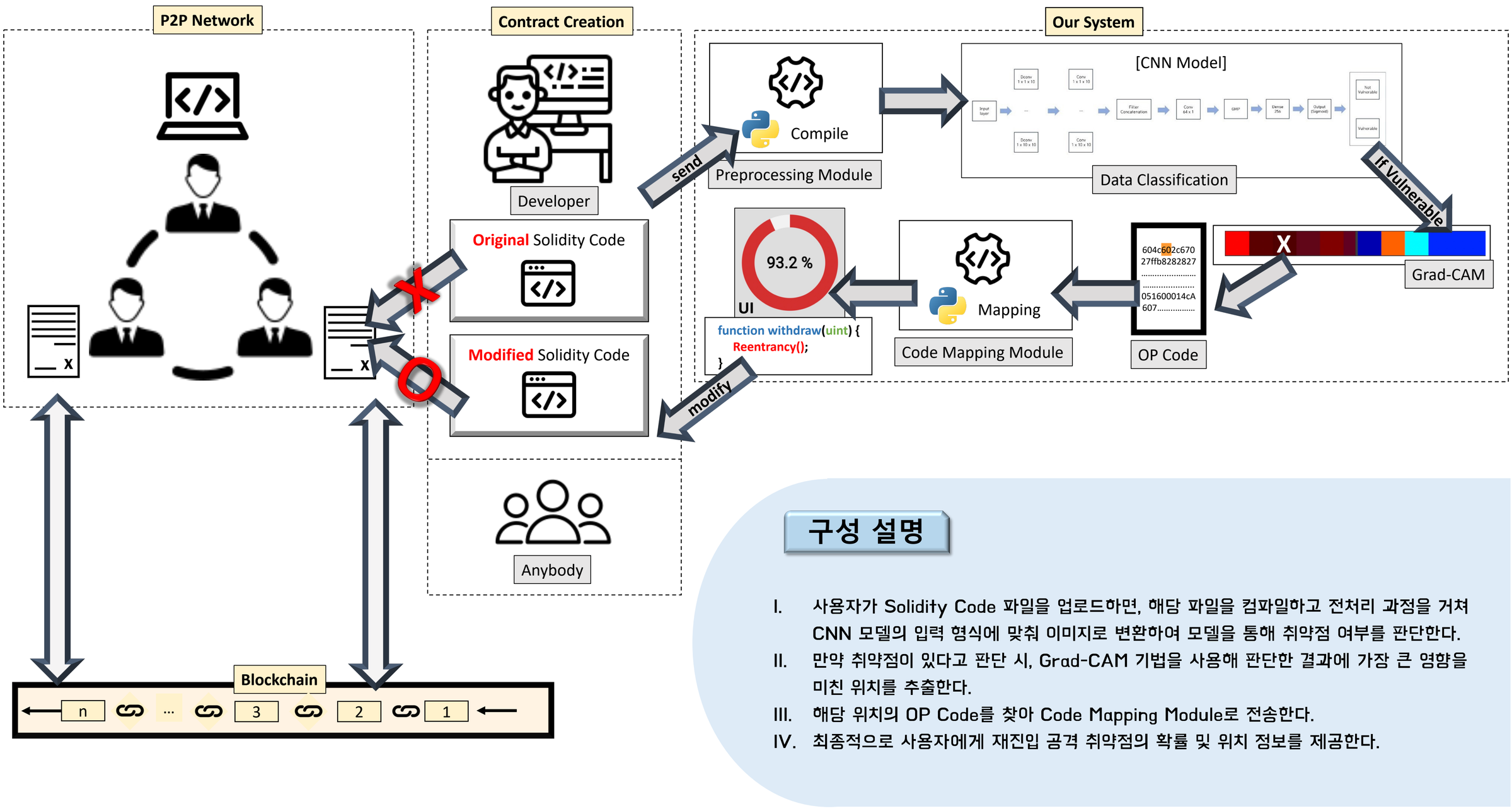
과제 배경

스마트 컨트랙트는 블록체인의 핵심 구성 요소로, 자동으로 실행되는 코드로서 복잡한 계약 조건을 처리한다. 하지만, 코드가 복잡해질수록 취약점이 발생할 가능성이 증가하며, 한 번 배포되면 변경이 불가능하기 때문에 해커에 의해 악용될 위험이 크다.

과제 목표

스마트 컨트랙트의 보안 취약점을 자동으로 탐지하여, 체계적으로 분석하고 평가하는 도구를 개발한다. 또한, 사용자에게 취약점의 위치를 시각적으로 보여주는 UI를 제공하며, 취약점이 포함된 코드 부분도 함께 제시한다.

시스템 구성



구성 설명

I. 사용자가 Solidity Code 파일을 업로드하면, 해당 파일을 컴파일하고 전처리 과정을 거쳐 CNN 모델의 입력 형식에 맞춰 이미지로 변환하여 모델을 통해 취약점 여부를 판단한다.

II. 만약 취약점이 있다고 판단 시, Grad-CAM 기법을 사용해 판단한 결과에 가장 큰 영향을 미친 위치를 추출한다.

III. 해당 위치의 OP Code를 찾아 Code Mapping Module로 전송한다.

IV. 최종적으로 사용자에게 재진입 공격 취약점의 확률 및 위치 정보를 제공한다.

기대효과

I. 취약점을 사전에 탐지하고 수정할 수 있기 때문에 해킹, 보안 사고의 가능성을 줄이며, 위험에 효과적으로 대응할 수 있다.

II. 자동화된 도구를 통한 체계적인 취약점 탐지가 가능하게 되므로, 수동 보안 검사와 비교했을 때 시간과 비용이 절약된다.

III. 스마트 컨트랙트의 안정성이 검증되면 사용자, 개발자 모두에게 더 높은 신뢰성을 제공하기 때문에 전체적인 블록체인 생태계 안전성 강화에 기여할 것으로 기대한다.