이더리움 컨트랙트 모니터링 및 분석시스템

고경찬 O, 이채현, 홍원기

포항공과대학교 컴퓨터공학과

{kkc90, chlee0211, jwkhong}@postech.ac.kr

Design of Monitoring and Analysis system on Contract in Ethereum

Kyungchan Ko O, ChaeHyeon Lee, James Won-Ki Hong

Department of Computer Science and Engineering, POSTECH

요 약

블록체인은 네트워크 참여자 모두에게 저장되는 정보에 대한 투명성을 공개하는데, 이것을 기반으로 하는 신뢰할 수 있는 공개된 분산 원장기술이다. 비트코인뿐만 아니라 스마트 컨트랙트 기능이 추가된 2 세대 블록체인 플랫폼 이더리움도 상당한 인기를 누리고있다. 이더리움도 블록체인에 저장되는 정보들을 모두 공개하며, 이로서 악의적인 사용자가 데이터를 의도적으로 수정하려는 시도를 네트워크 참여자 모두가 주시할 수 있다. 하지만 스마트 컨트랙트 정보도 함께 공유가되기 때문에 공개된 취약한 코드를 악용하여 해킹하려는 시도가 증가하고 있다. 이러한 해킹을 방지하기 위해서는 블록체인에 전파되어 저장되는 컨트랙트 관련정보들을 수집하여 컨트랙트의 취약성을 분석해야 한다. 본 논문에서는 컨트랙트 모니터링 및 취약한 컨트랙트를 탐지하는 방법에 대해서 소개하고 향후 연구 방향에 관해 기술하고자 한다.

I. 서 론

비트코인 [1]의 출현으로 비트코인의 기반 기술인 블록체인이 사람들 사이에 많이 언급되고 있다. 비트코인은 이전에 존재하는 여러 기술들을 집약하여 구현했지만, 이를 통해 블록체인기술을 세상에 알려고 사람들은 비트코인 이후로 블록체인을 언급했다. 그래서 비트코인은 1 세대 블록체인 기술이라고 알려져 있다. 비트코인 이후에 블록체인으로 구현한 많은 암호화폐들이 개발되기 시작했다. 그 중에서 스마트 컨트랙트[2]의 개념을 최초로 도입한 이더리움 [3]이라는 블록체인 플랫폼이 있다. 스마트 컨트랙트는 1994 년에 닉 사제보(Nick Szabo)가 최초로 제안한, 신뢰할 수 없는 컴퓨터 인터넷 환경에서 고도로 발달된 계약을 준수하도록 하는 프로토콜이다. 이더리움은 스마트 컨트랙트의 개념을 도입해서 블록체인 컴퓨팅 플랫폼으로서 구현되으며, 최초로 플랫폼의 역할을 할 수 있는 암호화폐 플랫폼의 출현이다. 이후로 많은 암호화폐 플랫폼들이 스마트 컨트랙트의 개념을 도입하려는 시도를 하고 있고, 그래서 이더리움을 2 세대 블록체인 기술이라고 알려져 있다.

최근에 블록체인 업계로 많은 자본이 투입되고 있는데, 이를 뒷받침 해주는 것이 이더리움의 스마트 컨트랙트이다. 이더리움에서는 스마트 컨트랙트를 이용해서 누구나 토큰(Token)을 발행할 수 있다. 이를 통해서 사람들은 ICO(Initial Coin Offering)을 진행하여 투자를 받는데, 이러한 부분에서 많은 투자금액이 유입되었다. 하지만 이러한 장점 뒤에는 스마트 컨트랙트의 취약점을 악용하여 해킹할 수 있다는 단점이 있다. 대표적인 해킹사례로 SMT(SmartMech) 토큰 무한 생성 해킹, 패리티 멀티시그 지갑 해킹(Parity Mulisig Wallet Hacked), DAO(Decentralized autonomous organization) 해킹 등이 있다. 이러한 해킹들은 이더리움 전체 네트워크에 악영향을 미치고 있다. 이러한 해킹사례들을 방지하기 위해서는 취약한 컨트랙트들을 탐지할 수 있는 모니터링 및 분석기법이 먼저 연구되어야 한다. 그리하여 본 여구에서는 컨트랙트 모니터링 방법과 이를 통해 수집된 정보를 이용해서 취약한 컨트랙트를 탐지하는 방법을 소개한다.

II. 관련 연구

1. Oyente

Oyente [4]는 싱가폴 국립대학에서 주관하는 연구 프로젝트의 일부로서, Symbolic execution 을 사용하여 이더리움 스마트 컨트랙트를 분석하는 도구이다. Oyente 는 오픈소스로 공개되었고 bytecode 레벨에서 분석 가능하기 때문에 Solidity, LLL, Serpernt, Viper 를 포함하는 모든 High-level EVM 언어들에서도 작동하기 때문에 범용적으로 사용될 수 있다.

2. Mythril

Mytril [5] 은 오픈소스로 공개되었고 이더리움 스마트 컨트랙트를 위한 보안 분석 도구이다. 이

도구는 스마트 컨트랙트의 다양한 보안 취약점들을 탐지하기 위해서 concolic analysis, taint analysis , control flow checking 등의 분석기법을 사용한다. 또한, Mytril 은 스마트 컨트랙트를 분석할 때 분석 대상으로 Solidity code, Solidity bytecode, Contract address 를 선택할 수 있다.

III. 컨트랙트 모니터링 및 분석시스템

컨트랙트 모니터링 및 분석시스템의 아키텍처는 전반적으로 그림 1 과 같은 구조를 갖는다. 추가적으로, 해당 아키텍처는 스마트 컨트랙트를 이용하는 대표적인 블록체인 플랫폼인 이더리움을 기반으로 설계되었다. 컨트랙트와 관련된 정보들로는 컨트랙트를 생성하는 트랜잭션, 컨트랙트 어카운트, 컨트랙트의 함수를 실행시키기 위한 트랜잭션 등이 있다. 따라서 정보들은 트랜잭션과 어카운트 정보를 모니터링 함으로써 얻을 수 있다. 이더리움 클라이언트 geth 를 구동시켜, Monitor 가 RPC 를 통해서 트랜잭션, 어카운트 정보를 모니터링 한다. Monitor 가 수집한 정보는 Preprocessor 에게 전달되어 전처리를 거친 후에 Database 에 컨트랙트 관련정보들이 저장된다. 두 개의 분석기(코드 기반, 통계 기반)는 이 정보들을 이용해서 트랜잭션의 취약성 정도를 판단하여 취약한 컨트랙트 주소를 추출한다. 추출된 정보는 Database 에 저장되고, 웹 서비스를 통해서 취약한 컨트랙트 주소 List 를 공개한다.

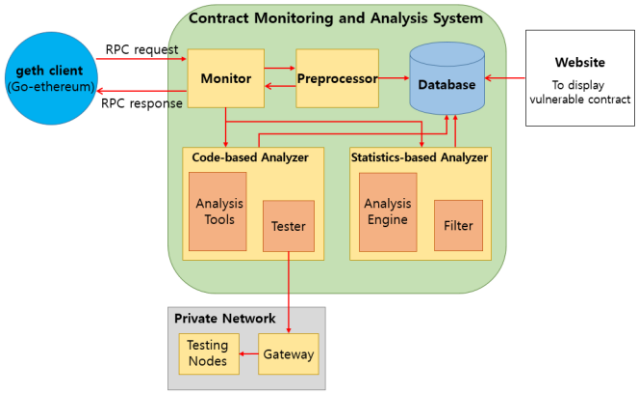

그림 1. 컨트랙트 모니터링 및 분석시스템

1. 코드 기반 분석기

코드 기반 분석기는 모니터링되는 트랜잭션들 중에서 'to' 필드가 nil(없음)인 트랜잭션들에 포함된 'data' 필드 내용을 이용해서 bytecode 레벨에서 컨트랙트를 검증한다. Analysis Tools 정적분석을 수행하며 Oyente, Mythril 등 bytecode 레벨에서 스마트 컨트랙트를 분석할 수 있는 도구들을 포함한다. 이것은 추후에 성능이나 정확도가 높은 분석도구가 개발되면 추가할 수 있도록 확장 가능한 구조로 설계된다. 정적분석뿐만이 아니라 Tester 는 추출된 bytecode 를 Private Network 의 Gateway 로 전달하여 해당 Gateway 에서 동일한 바이트 코드를 이용해서 컨트랙트를 생성하고, Private Network 상에서 여러 노드들이 일련의 패턴을 이용하여 동적분석을 실행한다. 정적 및 동적분석을 통과하지 못한 컨트랙트는 취약한 컨트랙트로 판단되기 때문에, Database 에 해당 컨트랙트 어카운트 주소를 전달한다.

2. 통계 기반 분석기

통계 기반 분석기는 지금까지 수집된 Historical 트랜잭션 및 컨트랙트 정보를 기반으로 분석한다. Analysis Engine 에서는 Historical 정보들을 수많은 DApp 및 스마트 컨트랙트 해킹사례들을 통해서 트랜잭션의 Outliner 를 추출한다. 예를 들어, 어느 하나의 외부 소유 계정에서 취약한 컨트랙트로 일정 패턴이나 한번에 많은 컨트랙트 함수 호출을 위한 트랜잭션을 보냈다면, 이를 이용하여 일정 주기마다 혹은 단시간에 일정 개수의 트랜잭션을 하나의 오부 소유 계정에서 생성하여 전파했다는 취약한 컨트랙트를 악용하려는 시도로 탐지할 수 있다. Filter 에서는 이러한 패턴이나 통계정보를 기반으로한 Outlier 에 걸리는 트랜잭션들을 추출하여 해당하는 외부 소유 어카운트와 취약한 컨트랙트 어카운트의 주소를 Database 로 전달한다.

IV. 결론 및 향후 연구

컨트랙트 모니터링 및 분석시스템은 취약점을 가지고 있는 스마트 컨트랙트가 해커들에게 해킹되어 악용되거나 일반적인 사용자가 잘못 사용되는 것을 막기 위한 핵심기술이다. 본 연구는 스마트 컨트랙트와 관련된 정보를 블록체인 네트워크에서 어떻게 수집할 수 있고, 수집한 데이터를 이용하여 취약점을 분석할 방법들에 대해 논의하였다. 또한, 이더리움 블록체인 플랫폼의 스마트 컨트랙트를 모니터링하고 분석하는 것에 초점을 맞추었다. 향후 본 연구에서 제안한 전반적인 구조를 실제로 구현하고 취약한 스마트 컨트랙트를 탐지하기 위한 다양한 연구를 진행할 수 있도록 할 예정이다.

ACKNOWLEDGMENT

이 논문은 2018 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00539)

참 고 문 헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
[2] Buterin, Vitalik. "A next-generation smart contract and decentralized application platform." white paper (2014).
[3] Szabo, Nick. "The idea of smart contracts." Nick Szabo's Papers and Concise Tutorials 6 (1997).
[4] Oyente github: https://github.com/melonproject/oyente
[5] Mythril github: https://github.com/ConsenSys/mythril-classic