블록체인 네트워크 모니터링 및 분석시스템

고경찬*°, 정태열*, 유재형† , 홍원기*

*포항공과대학교 컴퓨터공학과

† 포항공과대학교 정보통신대학원

{kkc90, dreamerty, styoo, jwkhong}@postech.ac.kr

Design of Monitoring and Analysis system on Blockchain network

Kyungchan Ko*°, Taeyeol Jeong*, Jae Hyoung Yoo† , James Won-Ki Hong*

*Department of Computer Science and Engineering, POSTECH

† Graduate school of Information Technology, POSTECH

요 약

블록체인은 공개된 분산 원장(Distributed Ledger) 기술이라고 할 수 있다. 분산 원장은 거래 장부로 명명되는 거래 데이터를 하나의 중앙시스템에 저장시키는 것이 아니라 공개적으로 여러 곳에 분산시켜 저장하는 개념을 의미한다. 이를 이용하면 거래 장부를 누군가 임의로 수정 또는 삭제할 수 없기 때문에, 인터넷상에서 행해지는 거래의 무결성을 보장할 수 있다. 최근에는 이러한 블록체인(Blockchain)을 활용한 암호화폐인 비트코인이 많은 관심을 받고 있으나, 한편으로는 비트코인의 익명성을 악용한 불법거래의 수가 증가하고 있는 문제가 존재한다. 이러한 불법거래들을 추적하고 대응하기 위해서는 블록체인 네트워크에서 발생하는 정보들을 수집하고 분석하는 기술이 요구된다. 따라서 본 논문에서는 블록체인 네트워크 모니터링 및 불법거래를 탐지하는 방법을 소개하고 향후 연구 방향에 관해 기술하고자 한다.

Ⅰ. 서 론

최근 비트코인의 거래량 증가와 시세 급등으로 인해 많은 사람들이 비트코인에 관심을 갖고 있으며, 이와 함께 비트코인의 기반 기술인 블록체인 또한 주목을 받고 있다. 블록체인은 처음에는 비트코인에 비해 큰 관심을 받지 못했지만, 점차 블록체인의 기술적 요소로 인해 주목을 끌기 시작해 지금은 미래를 바꿀 잠재적인 기술 중 하나로 평가되고 있다. 이미 블록체인 기술을 이용해 여러 분야에 접목시키려는 연구가 진행되고 있으며, 수년 이내에 블록체인이 금융, 은행, 보안, 물류, 네트워크, IoT, 보험, 운송, 스토리지, 기부, 투표, 행정, 의료, 온라인 콘텐츠, 소매업, 크라우드 펀딩 등의 산업에 영향을 미치며 큰 변화를 일으킬 것으로 예견되고 있다. 뿐만 아니라 블록체인은 데이터를 다루거나 중간자가 개입 되어있는 모든 산업에 적용되어 혁신을 일으킬 수 있는 기술이다.

블록체인 기술은 사토시 나카모토라는 익명의 개발자가 2008 년 10 월 31 일 암호화 기술 커뮤니티 메인에 올린 “Bitcoin: A Peer-to-Peer Electronic Cash System” [1] 이라는 논문을 통해 처음 공개되었다. 논문을 통해 소개된 비트코인의 기본 개념은 제 3 자인 금융기관을 거치지 않고 거래 당사자들 간에 직접 전달되는 전자화폐이다. 또한, P2P 네트워크를 이용해서 이중지불 문제를 해결하는 솔루션도 제안되어 비트코인을 실제 거래에 사용할 수 있다.

블록체인은 무결성을 보장 받아야 하는 중요한 데이터들을 숨겨야 한다는 기존의 보안 패러다임을 뒤엎는 기술이다. 예를 들어, 기존의 시스템을 이용하는 은행의 경우 거래기록(장부)을 안전하게 유지하기 위해서 물리적으로 각종 보안 장비를 도입하고 유출되지 않도록 보안 시스템을 구축하지만, 블록체인을 적용하면 거래기록 정보를 네트워크에 참여하는 모든 노드와 공유함으로써 거래정보 조작을 방지한다. 즉, 블록체인은 무결성이 보장되어야 할 데이터를 한 곳에 숨기는 것이 아니라 모두에게 공개하고 관리하게 함으로써 해당 데이터의 신뢰성을 보장하는 것이다. 또한, 블록체인은 P2P 네트워크의 문제점 중의 하나로 지적된 사용자끼리 서로를 신뢰할 수 없다는 문제를 작업증명(Proof of Work)을 도입해서 해결한다. 이를 통해, 블록체인에 의해 공개되고 관리되는 데이터는 무결성이 보장되는 데이터를 제공할 수 있다.

한편, 암호화폐와 블록체인이 주목받음에 따라 익명성이 보장되는 블록체인의 특성을 악용하여 암호화폐를 범죄에 이용하는 사례도 발생하고 있다. 예를 들어, 비트코인을 이용해서 마약 거래, 불법무기거래 등의 불법적인 거래가 발생하고 있으며, 돈세탁, 사기 등 범죄를 위한 행위로 비트코인이 활용되고 있다. 이와 같은 범죄에 이용되는 불법 거래를 방지하기 위해서는 우선적으로 불법 거래 내역을 추적하는 기술이 요구된다. 이를 위해 블록체인 네트워크 모니터링 기법이 필요하며, 퍼블릭 블록체인뿐만 아니라 프라이빗 블록체인에서도 가용성을 향상시키기 위한 모니터링 기술 개발이 선행적으로 이루어져야 한다. 따라서 본 논문에서는 블록체인 네트워크 모니터링을 위한 에이전트를 설계하고, 이를 통해 수집된 데이터의 분석을 통해 불법 거래를 탐지하는 방법을 소개한다

Ⅱ. 관련 연구

1. Explorers

최근에는 Blockexplorer [2], Etherscan [3]와 같이 블록체인과 관련된 업데이트 및 통계정보를 웹 서비스로 제공하는 사례가 있다. 이들은 블록체인 네트워크에서 생성된 블록, 거래내역 등의 정보를 제공한다. 본 논문에서는 하나의 블록체인에만 국한되는 것이 아니라 모든 블록체인을 모니터링할 수 있는 모니터링 시스템을 제안한다.

2. 블록체인 모니터링 관련 연구

BitIodine [4]는 모니터링 데이터를 이용해서 같은 사용자 혹은 같은 그룹에 속할 가능성이 있는 주소를 클러스터링(Clustering) 하는 시스템이다. 이를 위해 BitLodine 는 주소와 사용자 간의 경로 및 역 경로를 정적분석하는 기능을 가진다. 본 논문에서는 비트코인에 없는 Smart Contract 을 모니터링하는 기능을 포함한 모니터링 시스템을 제안한다.

Ⅲ. 블록체인 네트워크 모니터링 및 분석

블록체인 네트워크 모니터링 시스템의 구조는 전반적으로 그림 1 과 같다. 실제 블록체인 네트워크의 풀 노드에 모니터링 에이전트를 구동해 실시간으로 Block, Transaction, Node 등의 정보들을 수집한다. 수집된 데이터들은 에이전트-서버 통신을 통해서 모니터링 서버의 노드 인터페이스로 전송된다. 노드 인터페이스에서는 서버 안에 구현된 데이터베이스로 각각 다른 블록체인 네트워크에서 유입된 정보들을 분류하여 저장한다. 모니터링 서버에 구현된 웹서버에는 데이터베이스 안에 저장된 정보들을 웹 브라우저와 애플리케이션에 보여주는 시각화 기능을 제공한다. 또한, 불법 거래 탐지를 위한 모델을 만들기 위한 분석 엔진도 모니터링 서버 안에 구현된다. 본 논문에서는 전체 구조에서 블록체인 모니터링 에이전트 설계와 불법거래 탐지 방법 연구에 대해 제안한다.

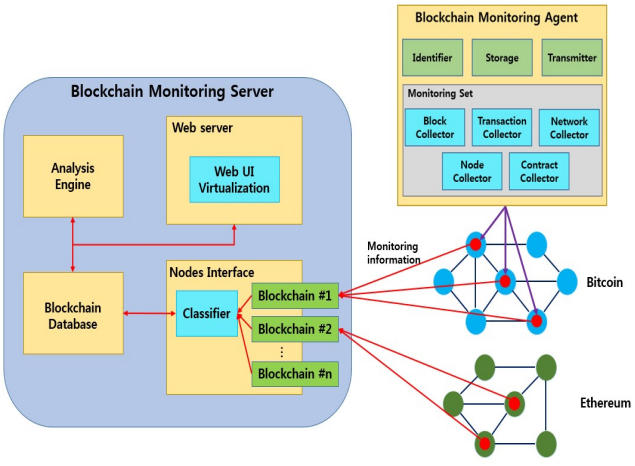

그림 1. 블록체인 네트워크 모니터링 시스템

1. 블록체인 모니터링 에이전트

모니터링 에이전트 설계를 위해서 우선 에이전트가 수집해야 할 데이터인 Block, Transaction, Contract, Node 등을 수집할 수 있도록 모니터링 범위를 설정한다. 이러한 데이터를 효율적으로 수집하기 위해서 데이터의 종류마다 검출하는 주기를 다르게 설정한다. 예를 들어 비트코인 네트워크에서 Block 은 생성 주기에 맞춰서 10 분, 기록 가능한 Transaction 은 초당 수 회이기 때문에 Transaction 은 1 초로 모니터링 주기로 설정할 수 있다. 또한, 여러 개의 블록체인 플랫폼 특성을 각각 고려하여 데이터 검출 방법을 특성화시켜야 한다. 각 블록체인 플랫폼마다 블록의 구성과 네트워크에 존재하는 데이터가 다르기 때문인데, 예를 들어, 이더리움에는 Smart Contract 기능이 있지만 비트코인에는 존재하지 않는다. 또한, 수집된 데이터의 블록체인 종류를 파악하기 위해 식별자를 저장해야 한다.

2. 불법거래 탐지

제안하는 모니터링 시스템은 수집한 데이터를 분석하여 불법거래를 탐지하는 기능을 제공한다. 우선 특정 주소에 대한 거래 내역 분석 기능으로 특정 주소에 연관된 Transaction 개수, 주소가 보유하는 잔액, 보낸 총 금액, 받은 총 금액, 처음 거래일, 마지막 거래일 등의 정보를 추출하여 거래 날짜 별로 '잔액', '송금', '수금'의 시간 별 그래프를 생성한다. 이때 날짜 범위, 금액 범위를 입력하면 그 범위들에 해당하는 Transaction 들 검색이 가능하다. 그리고 주소들 사이의 상관관계를 분석하는 기능으로 특정한 주소가 전송하거나 수신한 Transaction 을 모두 검색하여 input/output 을 시각화하고, 주소들 사이의 관계를 찾아서 클러스터링한다. 이때 한 주소에서 다른 주소로 전송되는 관계를 분석해서 이들 사이의 경로를 추출할 수 있다. 앞에서 언급한 기능들을 이용해서 불법거래, 랜섬웨어 거래, DDoS 공격 등과 연관된 Transaction 을 분석할 수 있다. 또한, Transaction 의 특징을 추출해서, 알려진 의심스러운 행동은 지도학습(Supervised Learning)을 이용해서 패턴을 식별하고, 알려지지 않은 미래의 의심스러운 행동은 비지도 학습(Unsupervised Learning)을 이용해서 예측할 수 있다.

Ⅳ. 결론 및 향후 연구

블록체인 네트워크 모니터링은 블록체인의 악용을 막는 핵심기술이다. 본 연구에서는 이를 위한 모니터링 시스템의 전체 구조에서 모니터링 에이전트를 설계하고 모니터링 방법에 대해서 정의하며, 불법거래 탐지를 위한 분석 메커니즘에 대해 논의하였다. 향후 연구로는 모니터링 시스템을 실제로 구현하고 불법거래 탐지 기술 연구를 진행할 예정이다.

ACKNOWLEDGMENT

이 논문은 2017 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. 2017-0-00195, 멀티 서비스를 지원하는 프로그래머블 스위치 제어 기술 개발)

참 고 문 헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[2] Davies R. W." The Data Encryption standard in perspective,"Computer Security and the Data Encryption Standard, pp. 129-132.

[3] Miles E. Smid, "From DES to AES," 2000, (http//www.nist.gov/aes).

[4] Shamir, A. "On the security of DES," Advances in Cryptology, Proc.Crypto '85, pp. 280-285, Aug. 1985.