정 보 보 호 학 회 지
제 31 권 제3호, 2021. 6

블록체인 네트워크 보안 위협 탐지 기술 동향 분석

이 은 영*, 문 정 현**, 한 채 림***, 이 일 구****

요 약

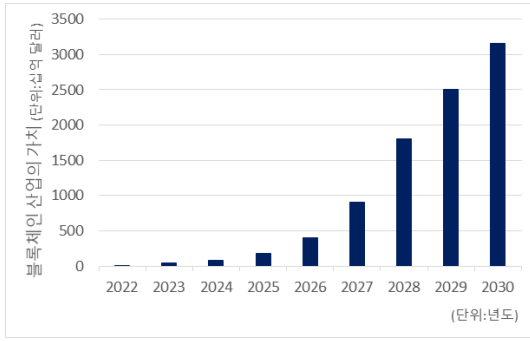
최근 블록체인 기술의 적용 범위가 전 산업으로 확대되고 있으며, 고부가가치 정보와 디지털 자산이 블록체인 분산 데이터베이스에 저장되고 관리되면서 블록체인을 대상으로 하는 보안 위협이 급격히 증가하고 있다. 특히 가용성 저하 공격, 분산 서비스 거부 공격, 비정상 거래, 악의적 거래, 51% 공격과 같이 블록체인을 대상으로 한 공격 기법이 고도화되고 피해 규모가 커지고 있다. 블록체인은 금융, 물류, 의료, 인증 등 전 산업 분야에 활용될 가능성이 높아지고 있어서 블록체인 네트워크 보안 위협을 신속하고 정확하게 탐지하는 기술에 대한 연구가 요구된다. 본 논문에서는 블록체인 네트워크 보안 위협에 대해 분석하고, 주요 위협 탐지 기술과 최신 동향을 분석한다.

Ⅰ. 서 론

블록체인은 데이터의 투명성과 무결성이 보장되는 분산 원장 기술로, 기존의 중앙집중형 시스템의 한계를 극복하는 탈중앙화 시스템의 장점이 알려지면서 다양한 산업에서 블록체인을 적용하려는 시도가 증가하고 있다.

블록체인 기술 도입이 가장 빠른 분야는 중 하나는 암호화폐 시장이다. 2008년 10월 31일 발표된 사토시 나카모토(Satoshi Nakamoto)의 논문 Bitcoin: A Peer-to-Peer Electronic Cash System[1]이 등장한 이후, 비트코인과 같은 암호화폐의 가치가 꾸준하게 성장하며 주목받고 있다. 최근 페이팔(Paypal), 팔란티어(PLTR.N)와 같은 글로벌 기업이 암호화폐의 결제를 허용해 가상 자산 산업의 발전을 장려할 뿐만 아니라 금융사들의 투자 참여가 이어져 시장에서의 기술에 대한 관심을 알 수 있다.

이처럼 금융, 물류, 의료 등 다양한 분야에서 사업을 추진할 뿐만 아니라, 정부의 적극적인 지원에 따라 주목받는 신기술로 자리 잡아 행정안정부에서 발표한 '전자정부 10대 유망기술'에 2017년부터 2019년까지 3년 연속 선정되었다. 이는 국내뿐만 아니라 세계 각국



〔그림 1〕블록체인 산업의 가치

에서도 동일한 흐름을 보인다. 그림 1은 2030년까지 블록체인 산업의 가치를 나타낸 그래프이다[2]. 미국의 시장조사기관인 가트너(Gartner)는 2030년까지 블록체인 기술이 전 세계적으로 약 3조 1천억 달러의 가치를 창출할 것으로 전망했다.

중요 정보와 디지털 자산이 블록체인 분산 데이터베이스에 저장되고 관리되어 블록체인의 가치가 상승함에 따라 블록체인 또한 해커의 주요 공격 대상이 되고 있다. 블록체인 기술의 처리 속도 한계와 거래 정보 관리에 대한 부담을 악용한 가용성 저하 공격, 거래 유효성 검사 시간을 지연시키는 분산 서비스 거부 공격

이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(No. 2020R1F1A1061107)과 2021년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원(P0008703, 2021년 산업혁신인재성장지원사업)을 받아수행된 연구임
* 성신여자대학교 미래융합기술공학과 (대학원생, o.lee.eunyoung@gmail.com)
** 성신여자대학교 융합보안공학과 (학부생, moon_aver@naver.com)
*** 성신여자대학교 융합보안공학과 (학부생, cherry7524@naver.com)
**** 성신여자대학교 융합보안공학과/미래융합기술공학과 (조교수, 교신저자, iglee@sungshin.ac.kr)

(Distributed Denial of Service, DDoS), 블록체인 익명성을 악용한 비정상 거래 등 다양한 보안 위협이 증가함에 따라, 블록체인 보안 사고에 의한 경제적 손실이 매년 증가하고 있어[3] 기술 발전 및 도입을 저해하고 있다.

기술 발전을 위해서 블록체인의 안정성을 보장할 수 있는 연구가 필요하다. 보안 위협을 판단할 수 있는 데이터를 수집하고, 분석하여 사전에 위협을 탐지하고, 보안 사고 발생 시 사후 대응의 솔루션으로 활용하고자 하는 연구가 활발히 이뤄지고 있다.

논문의 나머지 부분에서는 2장에서 블록체인을 소개하고, 3장에서는 블록체인에 존재하는 보안 위협을 소개한다. 4장에서 3장의 보안 위협을 탐지하기 위해 수집할 수 있는 데이터와 블록체인 보안 위협 탐지 연구를 소개하고 5장에서 결론을 내린다.

Ⅱ. 블록체인 개요

블록체인은 네트워크 구성원들이 해시 기반으로 암호화한 거래 정보를 공동으로 확인하고 기록, 보관함으로써 신뢰할 수 있는 제3자 없이도 신뢰성 및 무결성을 제공하는 P2P(Peer to Peer) 기반의 분산원장 기술이다. 분산원장 기술은 분산되어 동기화되고, 저장되는 분권화된 합의 알고리즘을 사용해 네트워크 노드들이 안전하게 데이터 상태를 변경하고, 검증할 수 있게 하는 프로세스 관련 기술을 의미한다.

다음은 암호화, 전자서명, 해시 등의 보안 기술과 분산형 네트워크를 기반으로 응용 서비스를 구현하는 블록체인의 동작원리[4]를 나타낸 것이다.

① A가 B에게 송금
② 해당 거래 정보 온라인상에서 블록에 저장
③ 해당 블록 정보 구성원에게 전파
④ 구성원은 거래의 유효성 승인
⑤ 승인된 거래는 새 블록으로 기존 블록체인에 연결
⑥ A에서 B로 자금 이동

블록체인의 주요 기술은 다양하게 분류가 가능하나, 핵심 기술, 플랫폼 기술, 서비스 기술 및 관리 기술로 분류할 수 있다. 핵심 요소 기술은 네트워크, 분산원장, 암호, 합의 알고리즘, ID 관리 접근 제어, P2P로 구성되며, 플랫폼 기술은 스마트 컨트랙트(Smart Contract), 자산 등록 기술, 클라우드 연동 기술, 서비스 기술은 디지털 화폐, 부동산 관리, 전자 투표 등이 포함되며, 관리 기술은 보안, 안전, 컴플라이언스 기술을 포함한다.

〔표 1〕 블록체인의 장·단점

분류	장점	단점
보안성	- 장부 공동 소유 (무결성) - 보안 비용 절감	- 개인키 해킹, 분실 시 해결 방법 없음 - 기밀성 미제공
시스템 안정성	일부 참여 시스템 오류 및 성능 저하 시 네트워크에 미치는 영향 적음	- 대형 마이닝 풀에 채굴 집중 - 실시간, 대용량 처리 어려움
익명성	- 개인정보 미요구 - 은행 계좌나 신용카드 등 기존 금융 분야에 비해 높은 익명성	- 불법 거래, 비자금 조성, 탈세 가능
투명성	- 거래 기록 공개 접근 - 거래 비용 절감 - 규제 비용 절감	- 거래 내역이 공개되어 모든 거래의 추적 가능성 - 익명성 미보장 - 재식별 가능성 (조합)
확장성	- 오픈 소스에 의해 쉽게 구축 - IT 구축비용 절감	결제 처리가 가능한 거래가 실제 경제 규모 대비 미미
P2P	- 제3자 없이 거래 가능 - 수수료 절감	문제 발생 시 책임 소재 모호

블록체인은 기존 거래 구조의 패러다임을 크게 변화할 수 있다는 점에서 효과적이며 그 활용도가 높으나, 동시에 관련 우려도 큰 실정이다. 표 1에서 그 장단점을 설명한다.

블록체인을 크게 6가지 분야(보안성, 시스템 안정성, 익명성, 투명성, 확장성, P2P)로 나누어볼 수 있다. 보안성의 경우, 장부를 공동으로 소유하면서 무결성을 보장받을 수 있지만 기밀성을 제공하지 못하는 단점이 존재한다. 또한 시스템 안정성 측면에서는 대형 마이닝 풀에 채굴이 집중될 수 있다는 가능성이 있으며, 익명성 측면에서는 높은 보안성을 가지나, 불법 거래에 악용될 수 있는 소지가 있다. 네트워크에 참여하는 모든 노드가 공동으로 데이터를 관리하는 투명성 덕분에 규제 비용이 절감되지만, 느린 처리 속도로 인한 제한된 확장성으로 인해 실시간 응용 서비스에 활용되기 어려운 상황이다. 마지막으로, P2P를 통해 제3자 없이도 거래가 가능하여 수수료가 절감되지만 한편으로는 문제가

발생했을 때 책임의 소재가 모호하다는 점 등이 있다.

실제 블록체인 기술은 1세대에 거쳐 2세대, 3세대를 향해 범위를 확장하는 중이다. 여기서, 1세대란 비트코인 등장한 2009년 이후 블록체인 기술 기반 암호화폐가 1,600개 이상 등장할 때까지의 기간을 의미하며, 2세대는 이더리움, 하이퍼레저 등 스마트 컨트랙트가 추가된 블록체인과 프라이빗(Private) 블록체인이 등장한 기간을 의미한다. 이러한 블록체인은 거래를 지원하는 중간관리자나 인증을 담당하는 중앙 인증 서버가 필요 없고, 자산에 대한 가치 평가 과정을 변화시켰다. 뿐만 아니라 스마트 컨트랙트로 인간의 개입 없이 기업 간 계약 이행이 가능해지면서 더욱 그 확장성이 커지고 있다. 이는 디지털 디스럽션(Digital Disruption, DD)과 연관이 있다. 이때, DD란 신기술의 등장에 따라 과거 기술이 파괴되는 것을 의미한다. 현 블록체인은 DD2(두 번째 단계) 단계이며, 아직 기술 개발에 활용되고 있는 상황이다. 그러나 2년 후인 2023년에는 DD3 단계에 진입해, 본격적인 상용화와 함께 사회에 파급력을 가져올 것이며, 그 시장이 기하급수적으로 확산될 것으로 전망한다[5]. 이 단계 이후에 블록체인 기술은 기존의 중앙 집중 방식을 넘어 성능 개선 및 신뢰성 구축에 큰 획을 그을 것으로 전망되고 있다.

현재까지 블록체인은 주로 금융 분야에 집중되어 왔으나, 기술의 적용 범위가 확대되며 최근에는 금융 분야 외에 사물인터넷, 클라우드 등 플랫폼 서비스에 적용되면서 비금융 분야에서도 파급력이 확산되고 있다. 의료 분야는 환자의 의료 데이터 수집, 검증 및 공유 관련 연구가 활발하게 진행되고 있으며, 공급망 분야는 제품 및 콘텐츠의 분산 데이터베이스에서 수요가 높다. 음악 및 영상 분야는 저작권 보호 서비스에 블록체인이 적용되고 있으며, 미디어 분야는 SNS(Social Networking Service) 내에서 암호 키를 활용해 메시지, 사진, 영상 등을 안전하게 송·수신하는 서비스에 블록체인을 적용하는 것을 활발하게 검토 중이다.

Ⅲ. 블록체인 보안 위협

본 장에서는 블록체인 시스템에서 발생하는 보안 위협의 종류 및 실제 공격 사례와 대책에 대해 알아본다.

3.1. 가용성 저하

가용성 저하는 참여자가 급증하고, 거래량이 증가함에 따라 거래 처리 속도와 거래 정보 관리 부담이 증가하여 발생한다. 일반적으로 블록체인은 거래에 대한 유효성 확인을 모든 거래자가 수행하기 때문에 거래 참여자의 수가 증가할수록 속도가 저하되어 서비스 개발에 한계가 있다. 전체 거래 정보의 증가와 처리 속도 저하로 인한 가용성 저하 문제를 개선하기 위한 보안 대책은 다음과 같다.

첫째, 참여자 검증을 통한 거래 합의를 통해 보안을 유지한다. 네트워크에 참여하는 노드의 MAC(Medium Access Control) 주소나 IP(Internet Protocol) 주소와 같은 기기 정보를 이용한 접근제어 및 다중 인증을 방법으로 권한 없는 부적절한 사용자 접근을 방지할 수 있다. 다만, 일부 검증 노드만으로 거래의 유효성을 검증하므로 잘못된 검증으로 인해 유효하지 않은 거래가 정상 처리될 수 있다는 가능성이 존재한다. 둘째, 거래 수수료를 활용해 가용성을 보존할 수 있다. 블록체인은 거래를 발행할 때마다 거래 수수료를 지급해야 하기 때문에 대량의 거래를 발행하여 공격을 수행하는 DDoS 공격은 공격자에게 높은 비용을 발생시킨다. 셋째, DDoS 공격에 대응하는 코드를 실행할 때, 정보가 저장되어 있는 디스크인 볼륨에 비례해 제한을 둠으로써 가용성을 보존할 수 있다.

3.2. 분산 서비스 거부 공격

분산 서비스 거부 공격은 스팸 거래를 발행해 거래 유효 검사 시간을 지연시켜 전체 블록체인의 성능을 저하시킨다. 실제로 2016년 3월 비트코인은 대량의 스팸으로 인해 서비스가 거의 중단되었다. 채굴자는 고액의 수수료를 받기 위해 높은 수수료 거래를 우선적으로 실행하고, 평균적인 수수료를 갖는 거래는 블록에서 배제된다. 이로써 정상 거래에 서비스 거부 현상이 발생한다. 이를 막기 위해 채굴자는 비정상적으로 높은 수수료를 제안하는 거래 등 블록을 생성할 때 불안전한 거래의 우선순위를 낮춰 공격에 대응했다. DDoS 공격은 악성코드에 감염된 분산 노드에 의해 공격이 수행되기 때문에 전체 사용자에 대한 악성코드 감염 확인 등 그 대응이 어렵다.

최근 비트코인, 이더리움 등 주요 블록체인에서 DDoS 공격 발생 가능성이 발견되었다. 2018년, 블록체인 분야에서 DDoS 공격을 예방하기 위한 대책을 마련했으나, 여전히 다수의 암호화폐에서 취약점이 발견

되어 주의가 요구되고 있다. 그리고 확장성을 증대시키기 위해 최근 많이 사용되고 있는 세컨드 레이어 솔루션을 대상으로 DDoS 공격 발생 가능성이 발견되어 대응 방안이 필요하다.

블록체인 노드에 DDoS 공격이 일어나는 원리를 이해하기 전에 암호화폐 노드 작동 방식에 대한 이해가 선행되어야 할 것이다. 암호화폐 노드는 트랜잭션 내용을 해시 값으로 정리한 인벤토리 메시지(Inventory Message)를 상대의 노드와 비교해 전체 네트워크의 거래 내용을 실시간으로 동기화하며 작동한다. 이때, 암호화폐는 탈중앙성을 최우선 가치로 두기에, 노드에 도달한 메시지가 악의적 메시지인지에 대한 여부를 판단하는 것은 해당 노드의 판단에 의존한다. 다만, 비정상적 메시지와 정상적 메시지의 판별 모호하기 때문에 노드가 비정상적 메시지를 실제로 발견하기 매우 어렵다. 해커는 이와 같은 블록체인의 구조적 결함을 공격해 목적을 달성한다.

3.3. 비정상 거래

블록체인 기술을 통해 효과적인 서비스를 제공하거나 기존의 문제점을 개선하고자 하는 시도가 활발하게 진행됨에 따라 다양한 취약점을 이용한 비정상 거래 시도 또한 증가하고 있다. 블록체인은 비정상 거래가 발생하더라도 한번 승인된 거래의 경우 거래 취소와 같은 대응이 어려워 사전에 탐지 및 차단하는 것이 중요하다. 비정상 거래 보안 위협 중 1) 이중 지불, 2) 유출된 키 서명, 3) 정책 미준수 거래, 4) 거래 허용 참여자 관리에 대해 살펴본다.

3.3.1. 이중 지불

이중 지불 공격은 거래가 확정되어 블록이 생성되기 전에 대가를 제공받아 거래를 취소하거나 재사용하는 공격이다. 가장 흔하게 알려진 비정상 공격인 이중 지불 공격 2가지에 대해 소개한다.

- 레이스 공격(Race Attack)은 지불한 코인을 본인의 지갑에 다시 전송하는 거래를 발생시켜 정상 거래내역보다 먼저 채굴 및 전파하는 것으로, 하나의 전송내역만 승인되어 블록에 기록된다는 점을 악용한 공격이다.
- 피니 공격(Finney Attack)은 공격자가 직접 채굴에 참여하여 타임스탬프 상의 짧은 하드 포크를 이용하는 공격이다. 이 공격은 공격자가 정상적인 블록을 늦게 전파하는 방법을 이용하기 때문에 제3자가 블록을 채굴할 위험을 갖고 있을 뿐만 아니라 현재는 해시 파워와 블록 생성의 난이도의 상승으로 인해 이뤄지기 어려운 공격으로 인식되고 있다.

이외에도, 피니 공격과 공격 방식은 유사하지만 공격이 실패하더라도 공격자는 채굴 보상을 지급받을 수 있는 위험 헤지 전략인 Vector76 공격, 트랜잭션 ID를 변경하는 Transaction Malleability Attack[6] 등이 있다.

3.3.2. 유출된 키 서명

유출된 키 서명은 키를 도난당하거나 취약한 키 생성으로 인해 발생하는 키 관리 보안 위협이다. 공격자가 정상 참여자의 키를 취득할 경우, 공격자는 정상 참여자로 위장해 참여자의 자산 손실 또는 기밀 거래 메시지 유출 공격을 할 수 있다.

- 키 도난 : 암호화되지 않은 원문이 저장되어 있거나, 거래에 사용하는 모든 키(서명, 암호화 등)로 동일한 키를 사용할 경우 공격 성공 가능성이 커진다.
- 취약한 키 생성 : 블록체인 거래에 사용하는 암호키의 생성 방식이 안전하지 않을 경우에 공격자는 이러한 취약점을 이용해 키를 재생성할 수 있다. 따라서 키 생성 시 안전한 난수발생기와 암호 알고리즘을 이용하여 키를 생성해야 한다.

블록체인 시스템에서는 개인을 구분하기 위해 전자지갑을 사용한다. 전자 지갑 속에는 디지털 서명, 디지털 키, 주소 등이 포함되어 있어 이를 분실하게 되면 정상적인 사용자의 참여가 어려운 상황이 발생한다. 따라서 안전한 시스템을 구축하는 것도 중요하지만, 키를 분실하거나 접근 권한을 상실하지 않도록 개인 사용자의 주의가 요구된다.

3.3.3. 정책 미준수 거래

누구나 참여가 가능한 퍼블릭 블록체인과 달리 운영 및 참여 주체가 존재하는 프라이빗 블록체인에 참여하기 위해서는 허가를 받아야 한다. 하지만 허가받지 않는 참여자가 서비스에 대해 거래를 요청하는 경우에는 기존 수립 정책인 ‘허가된 사람만 참여할 수 있다’는

기준에 위배된다. 이는 서비스 정책에 어긋난 거래를 의미하는 취약점으로, 다음의 요소들이 사전 검토되어야 한다.

- 인증 : 폐쇄형 네트워크인 프라이빗 블록체인에 접근하기 위해서는 참여 노드 및 클라이언트의 인증 절차가 필수적으로 요구된다. 인증에 사용되는 보안키는 안전한 환경에 저장하여 허가받은 사용자만이 접근 가능하도록 관리되어야 한다.
- 네트워크 : 시스템 및 노드 간의 데이터 전송 시 기존에 존재하는 위협인 스니핑, 스푸핑 등을 통해 정보를 탈취하여 접근하는 등의 문제가 발생할 수 있으므로 데이터 암호화가 필수적이다.
- 접근제어 : 분산원장에 데이터가 저장되는 경우 참여자는 데이터에 손쉽게 접근할 수 있게 되므로, 개인정보 및 공유 불가 데이터인지에 대한 분류와 저장 및 처리 방식을 사전에 검토해야 한다.
- 인프라 : 참여 노드, 저장되는 데이터의 형태, 자체 시스템 구성 여부에 따라 인프라 환경이 구성되어야 한다.

3.3.4. 거래 허용 참여자 관리

블록체인은 거래내역이 모두 공개되어 장부를 누구나 쉽게 확인할 수 있지만, 신분증명 없이 문자열로 이뤄진 주소를 통해 거래가 이뤄져 익명성이 보장된다. 거래 허용 참여자 관리는 정부, 금융기관과 같이 신뢰 가능한 기관에서 제공하는 허용 참여자 목록을 활용하는 것을 의미한다. 화이트리스트 방식을 활용하는 것으로, 비인가자에 의한 자금 세탁 거래 등의 의심 거래를 차단하기 위해 연구가 이뤄지고 있다.

3.4. 불법 거래

블록체인은 탈중앙화, 무결성, 투명성, 익명성을 특징으로 하는 기술로, 블록체인에서의 모든 거래는 익명화된 주소를 통해 거래되기 때문에 개인정보를 알 수 없다. 하지만 이러한 익명성은 양날의 검이 되어 악의적인 행위에 활용된다. 마약거래와 같은 불법 거래나 자금 세탁, 탈세에 사용되는 경우가 존재한다. 이외에도 악의적인 목적으로 거래를 발생시켜 블록체인의 익명성을 이용해 불법 행위를 저질러 타인에게 손해를 입히는 경우가 존재한다.

블록체인 기술을 활용한 거래의 경우, 익명성을 이용하여 거래자의 신원을 알 수 없어야 하지만, 비트코인 사용자 신원 추적에 관한 연구에 따르면 비트코인 사용자의 40%는 추적이 가능하다[7]. 한편, 공격자들은 추적을 방해하는 방법을 개발하여 악성 행위를 이어나가고 있다. 그중 대표적인 추적 방지 대책 두 가지에 대해 소개한다.

- Mixer : 거래내역을 뒤섞어 거래 추적이 어렵도록 함으로써, 정보 연결점에 혼란을 야기해 사용자 프라이버시를 제공하는 서비스이다. 하지만 수사기관이 해당 서비스를 제공하는 업체를 압수수색할 경우, 추적이 가능하여 본래 목적을 완전히 달성한다고 보기는 어렵다.
- Dark Coin : 믹서 사이트의 도움 없이 자체적으로 추적 기능을 차단하기 위해 개발된 코인이다. 대표적으로 N번방 사건에서 사용된 모네로(Monero)가 존재하는데, 모네로는 추적 방지를 위해 안전장치를 사용하였다. 거래의 송금자와 수신자 식별을 어렵게 하는 링서명과 스텔스 주소, 금액 정보를 숨기는 RingCT(Ring Confidential Transactions), I2P(Invisible Internet Project) 라우터인 코브리를 이용해 안전하게 거래를 보장하고 거래 흐름 파악을 어렵게 하였다. 하지만 이를 추적하고자 하는 연구 또한 이뤄지고 있어 해당 코인도 절대적으로 추적이 불가능한 것은 아니다.

3.5. 51% 공격

블록체인은 P2P 분산 네트워크에 의해 거래가 이뤄지는 기술로, 분산화된 시스템의 보안과 무결성을 달성하기 위한 다양한 합의 알고리즘이 존재한다. 트랜잭션의 유효성을 보장하기 위한 대표적인 합의 알고리즘은 사토시 나카모토에 의해 설계된 작업증명(Proof of Work, PoW)으로, 해시 파워를 이용해 논스 값을 변경하며 블록을 생성하기 위한 정답을 찾는 방법이다. 이때, 논스 값은 연산 시마다 값이 변경되며 난이도가 높아질수록 더욱 많은 해시 파워를 요구한다. 다음의 과정을 통해 연산 경쟁에서 승리 시 채굴자는 채굴에 성공하게 되어 블록을 생성하고, 최초로 생성된 블록은 전체 네트워크에 전파되어 무결성을 유지하게 된다. 하지만 합의 알고리즘에도 보안 취약점이 존재하는데, 그중 대표적인 취약점은 51% 공격이다.

시빌 공격(Sybil Attack), 밸런스 공격(Balance Attack) 등을 통해 블록체인 네트워크에서 51%의 해시 파워를 장악할 경우, 블록체인을 통제할 수 있게 되어 거래 내역을 조작할 수 있다. 블록체인은 거래 내역의 무결성을 보장하지만, 블록 생성 시 거의 동시에 채굴 작업이 성공할 경우, 블록체인은 일시적으로 포크 현상이 발생하여 블록이 두 갈래로 나누어질 수 있다. 나누어진 블록은 일정 시간이 초과한 후 더 많은 선택을 받은 블록을 선택하여 하나의 메인체인만 남게 된다. 공격자는 이러한 점을 악용하여 거래내역을 교체함으로써, 이중 지불 공격 등의 부정한 이득을 취할 수 있다. 51% 공격의 절차는 다음과 같다[8].

① 공격자는 51%의 점유율을 획득 후, 비공개 채굴 수행
② 이중 지불 공격을 위해 메인체인에 거래소로 송금하는 거래와 비공개 체인에 공격자의 다른 지갑으로 송금하는 거래 각 체인에 블록 추가
③ 블록의 안정성이 충분히 검증되는 시간 이후, 메인체인에 송금한 거래가 확인되면 해당 화폐 매도 후 다른 화폐를 구매하여 공격자의 지갑으로 송금
④ 비공개 체인을 공개하고, 51%의 점유율을 통해 메인체인 교체

이러한 과정을 통해 공격자는 거래소로 보낸 화폐 거래를 무효화시켜 이중 지불 공격에 성공하게 된다. 채굴 난이도가 높아짐에 따라 연산에 필요한 장비의 사양이 높아져 과거에는 이론적으로만 위협이 제시되었지만, 클라우드 컴퓨팅 기반 채굴 회사 등의 등장으로 인해 공격에 드는 예상 비용이 매우 저렴해져 규모가 작은 알트코인에게 51% 공격은 위협이 되고 있다[9]. 실제로 Bitcoin Gold, Ethereum Classic, MonaCoin, ZenCash, Litecoin Cash는 51% 공격의 피해자로 널리 알려져 있는 암호화폐로, 공격 대응 방안으로 거래 완결성 기준을 상향 조정하거나, 거래소 입금 정지, 해시 파워 분배 조절 등의 대처를 수행했다. 이러한 후속 대처 방법 이외에도 기존의 작업증명 방식이 아닌 새로운 합의 알고리즘을 통해 위협을 회피하고자 하는 연구가 수행되고 있다. 다음은 블록체인의 대표적인 합의 알고리즘이다.

- 지분증명(Proof-of-Stake, PoS) : 지분에 따른 증명 방식으로, 51% 공격을 위해서는 컴퓨팅 파워뿐만 아니라 전체 지분의 51% 이상을 확보해야 하기 때문에 공격에 필요한 비용을 높여 보안성을 강화했다. 따라서 공격자의 부담이 클 뿐 아니라, 채굴에 필요한 해시 파워가 많이 필요하지 않다 보니 컴퓨팅 자원 낭비를 줄일 수 있어 경제적이다. 하지만 지분에 따라 이자를 지급하기 때문에 코인 유통량이 감소할 수 있을 뿐만 아니라 지분을 보유한 사람이 권력을 독점할 수 있다는 문제점이 존재한다.
- 권한증명(Proof-of-Authority, PoA) : 프라이빗 블록체인에서 사용되는 합의 알고리즘으로, 검증자의 신원을 미리 검증함으로써 허가받은 노드는 신원에 기반한 합의 방식을 통해 블록을 생성할 수 있다. 따라서 권한증명 프로토콜에서 51% 공격을 수행하기 위해서는 권한을 인증 받은 검증자의 절반 이상의 공모 또는 배신이 이뤄져야 하므로 공격 가능성이 낮다.
- 지연작업증명(delayed Proof of Work, dPoW) : 초기 합의 알고리즘(PoW)을 보완한 방식으로, 스냅샷을 통해 체인의 주소 및 자산을 기록하고 블록체인 원장에 체인의 스냅샷을 저장하는 합의 알고리즘이다. 이렇게 만들어진 블록은 공증 블록이라 불리며, 공격에 성공하기 위해서는 해킹하려는 블록체인 네트워크와 공증 블록이 저장되어 있는 네트워크의 51% 지분을 모두 얻어 변경해야 한다.

Ⅳ. 블록체인 네트워크 보안 위협 탐지 방법

본 장에서는 진행 중인 블록체인 네트워크 보안 위협 탐지 연구들을 검토한다. 보안 위협 탐지 프로세스에 따라 판단의 근거가 되는 데이터를 수집하고, 다른 노드에게 배포하는 단계, 수집한 데이터를 토대로 위협 상황을 탐지하는 단계, 관리자가 해석하기 쉽게 데이터를 시각화하는 단계로 나누어 살펴본다.

4.1. 수집·배포

수집·배포 단계는 블록체인 시스템의 위협을 탐지하기 위한 정보를 수집하고, 다른 노드와 공유하는 작업을 진행한다. 수집된 정보를 토대로 보안 위협을 판단하기 때문에 위협 상황 판단의 근거가 될 수 있는 지표들을 수집하는 것이 중요하다. 또한 분산형 네트워크의

특성상, 각 노드가 소유한 정보가 다를 수 있기 때문에 개개인이 수집한 데이터들을 다른 노드와 공유하고, 동기화하는 작업이 중요하다. 이때 노드 간 빠르게 정보를 동기화하는 것이 요구된다.

4.1.1. 수집 데이터

표 2는 위협 상황 탐지를 위해 수집할 수 있는 데이터와 종류를 나타낸다. 데이터는 수집 위치에 따라 노드, 트랜잭션, 블록, 네트워크로 분류할 수 있다.

〔표 2〕 수집 위치에 따른 수집 데이터

분류	수집 데이터
노드	초당 트랜잭션 수
	평균 응답 지연
	CPU(Central Processing Unit)당 트랜잭션 수
	메모리당 트랜잭션 수
	디스크 I/O당 트랜잭션 수
	네트워크 데이터당 트랜잭션 수
트랜잭션	트랜잭션 해시
	수신자
	발신자
	전송 암호화폐 양
	가스비
	가스 한도
	논스
	비트
	서명 관련 정보
블록	블록 높이
	블록 숫자
	타임
	블록 해시
	이전 블록 해시
	언클 해시
	코인베이스
	사이즈
	가스 사용량
	가스 한도
	거래 정보 해시
네트워크	피어 검색 속도
	RPC(Remote Procedure Call) 응답 속도
	트랜잭션 전파 속도
	계약 실행 시간
	상태 업데이트 시간
	합의 비용 시간
	포크가 시작된 시간
	포크가 탐지된 시간
	포크에서 식별된 악성 거래의 수
	포크에서 식별된 악성 거래의 유형
	누적 블록 크기
	누적 거래 수
	채굴된 암호화폐 수
	1일 생성 블록 수
	1일 생성 블록 크기
	1일 생성 트랜잭션 수
	악성 블록
	악성 계정

4.1.2. 공개 데이터

블록체인의 거래 내역은 누구나 접근할 수 있도록 공개되어 있다. 블록체인 탐색기를 통해 발행된 트랜잭션을 간편하게 확인할 수 있다. 블록체인 탐색기는 가장 처음 블록인 제네시스 블록부터 가장 최근의 블록에 걸쳐 담긴 정보들을 검색할 수 있다. 대표적인 블록체인 탐색기로 블록체인 익스플로러(Blockchain Explorer)와 이더스캔(Etherscan)이 있다. 블록체인 탐색기에서 제공하는 API(Application Programming Interface)를 사용해 보안 위협 탐지를 위한 대량의 데이터를 수집할 수 있다. 수집 가능한 정보로 주소, 트랜잭션, 블록 정보 등이 있다.

사전에 수집된 악성 데이터 셋을 활용할 수도 있다. EtherScamDB는 이더리움 사기 사건들을 기록한 오픈소스 데이터 셋이다. CryptoScamDB[10]는 EtherScanDB의 확장 버전으로 이더리움뿐만 아니라 비트코인, 이오스 등 여러 암호화폐 플랫폼의 사기 사건을 저장한다. 사기, 가장, 피싱, 폰지 등 암호화폐 편취 사건에 사용된 URL(Uniform Resource Locator)과 주소 그리고 해당 사기 사건의 상세 정보 등을 확인할 수 있다.

Nitesh[11] 등은 CryptoScamDB로부터 4,375개의 이더리움 악성 계정, Etherscan API를 사용해 5,000개의 이더리움 정상 계정을 수집한다. 수집한 계정에서 발행

된 트랜잭션의 특징 44개를 추출하여 이더리움 불법 계정 탐지 모델 학습에 사용한다.

4.1.3. JSON-RPC

JSON(JavaScript Object Notation) - RPC는 블록체인 네트워크에서 사용하는 통신 방법이다. 블록체인 노드는 JSON-RPC를 사용하여 다른 노드와 통신, 정보 공유, 거래 발행 등 다양한 작업을 수행한다. 데이터를 수집하기 위해 노드는 다른 노드에게 직접 공유를 요청하여 데이터를 획득한다. JSON-RPC 통신으로 노드 정보, 트랜잭션 정보, 블록 정보를 수집할 수 있다[12]. JSON 형식으로 데이터를 받아오기 때문에 데이터 전처리 및 저장이 용이하다.

4.1.4. 로그

로그 기반 수집 방법은 JSON-RPC 기반 데이터 수집 방법의 단점을 보완한 방법이다. 데이터 수집, 동기화만을 목적으로 하는 노드를 두어 각 노드에 로그 분석기를 설치하고, 로그를 파싱하여 배포하는 방식으로 운영된다. RPC 기반 수집 방법보다 오버헤드가 95% 낮게 측정되었다. 또한 로그 저장 형식이 지정되어 있어 새로운 피어를 쉽게 추가할 수 있고, 다양한 블록체인 시스템의 데이터를 함께 수집·저장할 수 있기 때문에 확장성이 있다[13].

4.2. 탐지·대응

보안 위협 탐지 단계는 수집한 정보를 바탕으로 위협 상황을 판단하는 작업을 수행한다. 위협에 따라 필요한 정보가 다르기 때문에 먼저 사용자가 탐지하고자 하는 위협을 파악하는 것이 중요하다.

4.2.1. 성능 측정

블록체인 시스템의 성능을 측정하여 시스템이 정상적으로 동작하는지 판단한다. 비정상적인 성능 측정 결과가 나온다는 것은 네트워크 과부하가 걸리거나, 위협 상황에 노출되었다는 의미이다. 블록체인 시스템의 성능을 측정하는데 가장 중요한 것은 블록체인 시스템의 성능 측정 지표를 선정하는 것이다. 블록체인 시스템은 아직 정형화된 성능 측정 지표가 없으며, 현재 활발하게 연구가 진행 중이다[14][15].

Peilin[13] 등은 블록체인 시스템의 성능을 정량적으로 측정할 수 있는 지표 12가지를 제안한다. 전체 시스템을 평가할 수 있는 지표로 초당 트랜잭션 수, 평균 응답 지연, CPU당 트랜잭션 수, 메모리당 트랜잭션 수, 디스크 입력/출력당 트랜잭션 수, 네트워크 데이터당 트랜잭션 수를 제안한다. 거래 프로세스에 따른 평가 지표로 피어 검색 속도, RPC 응답 속도, 트랜잭션 전파 속도, 계약 실행 시간, 상태 업데이트 시간, 합의 비용 시간을 제안한다. 이를 토대로 피어 수에 따른 이더리움의 성능을 측정하고 비교한다.

블록체인 시스템의 성능을 측정하는데 중점을 두는 연구가 많기 때문에 이를 기반으로 이상치의 기준을 설정하고 블록체인 시스템의 보안 위협을 탐지하는 연구가 필요하다.

4.2.2. 필터링

필터링 방식은 악성 노드, 악성 트랜잭션 정보를 다른 노드와 공유하여 차단한다. 악의적인 활동을 수집, 저장하고 다른 노드들과 함께 공유하여 이미 발생한 공격이 다시 공격에 성공하는 것을 막는다.

블록체인에 악성 행위를 기록하여 위협 행위를 탐지·차단할 수 있다[16]. 피해 노드는 위협 행위를 네트워크의 모든 노드가 확인할 수 있도록 블록체인에 기록한다. 위협 행위가 악성 블록일 경우, 일정 단위로 분할하여 저장한다. 만약 다른 노드들에게 블록체인에 기록된 악성 행위가 발생한다면, 공격을 방어하여 피해를 방지할 수 있다. 이 방식은 정직한 노드의 수를 줄이는 이클립스 공격과, 여러 노드에게 같은 행위를 반복하는 공격을 방어하는데 효과적이다. 추가적으로 공격자가 위조하여 악의적인 활동을 확산시키는데 사용될 가능성이 있는 포크 정보를 기록하여 방어 효과를 높일 수 있다[17].

각 노드에 모니터링 테이블을 구성하여 악성 노드를 필터링할 수 있다[18]. 블록 헤더와 네트워크 패킷에서 수집한 정보를 모니터링 테이블에 저장한다. 노드는 다른 노드의 동작을 모니터링하여 특정 노드의 블록만 전달하는 노드를 확인한다. 임계치가 초과한 노드는 블랙리스트에 추가하고, 해당 노드의 블록은 수신하지 않는다.

4.2.3. 인공지능

인공지능 기술을 사용하여 블록체인 시스템에서 이루어지는 악성 행위의 패턴을 파악한다. 블록체인 시스템에서 수집한 데이터를 학습하고 위협 행위를 판단한다.

Farrugia[19] 등은 머신러닝 기반으로 이더리움 악성 계정을 탐지하는 연구를 수행하였다. 공개 데이터를 활용하여 학습 데이터를 구축하였다. EtherScamDB에 저장된 이더리움 악성 계정 2,179개를 수집하였고, Sokolowska[20]의 도구를 사용하여 이더리움 정상 계정 2,502개를 수집하였다. 또한 Etherscan API를 사용하여 정상 계정과 악성 계정의 최근 트랜잭션 내역 10,000개를 수집하였다. 학습 데이터의 특성으로 사용하기 위하여 트랜잭션에서 42개의 특성을 추출하였다. XGBoost(eXtreme Gradient Boosting) 모델로 정상 계정과 사기 계정을 학습하여 이더리움의 불법 계정을 탐지하였다.

Patel[21] 등은 OCGNN(One Class Graph Neural Network) 기반 악성 노드 및 악성 트랜잭션 탐지에 관한 연구를 수행하였다. 트랜잭션의 연속성을 반영하기 위하여 속성 그래프로 데이터를 구성한다. 노드로 사용자를 표현하고 엣지로 트랜잭션을 표현하다. 수신자, 발신자, 트랜잭션 해시 등 26개의 특성을 추출하여 학습 데이터로 사용하였다.

4.3. 시각화

시각화 단계는 사용자에게 수집한 데이터를 그래프, 표 등의 표현 방식으로 제공하는 작업을 진행한다. 수집한 정보를 이해하기 쉽게 시각화하여 사용자가 위협 상황을 빠르게 인식할 수 있도록 돕는다. 그리고 공격을 사전에 효과적으로 막기 위해서는 보안 전문가가 시스템을 모니터링할 수 있는 도구가 필요하다.

블록체인 시스템을 관제하는 보안 전문가를 위해 트랜잭션 정보, 네트워크 활동, 취약점 점검 결과를 시각화할 수 있다[22]. 또한 다양한 블록체인 플랫폼을 관제하기 위하여 트랜잭션, 블록, 네트워크 정보를 수집하고 사전 처리를 수행한 뒤 시각화 작업을 수행할 수 있다[23]. 효과적인 관제를 위한 탐색 기능을 제공하여 블록 해시, 트랜잭션 아이디 등을 사용해 수집한 데이터를 검색할 수 있다[24].

Ⅴ. 결 론

본 논문에서는 블록체인에서 수집할 수 있는 데이터를 수집 위치 별로 정리하고, 블록체인 네트워크 보안 위협을 탐지하는 선행 연구를 검토하였다. 블록체인 보안 위협을 탐지할 수 있는 데이터를 선정하고, 탐지하고자 하는 위협에 맞추어 적절한 탐지 대응 기술을 적용해야 한다. 기술이 발전하고 적용 범위가 넓어지며 블록체인 시스템을 대상으로 하는 보안 위협이 증가하고 있다. 따라서 블록체인 산업의 도입과 활성화를 위해 시스템의 위협을 조속히 탐지하여 블록체인의 안정성을 확보하기 위한 보안 위협 탐지 연구가 활발히 수행될 필요가 있다.

참 고 문 헌

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system," *Manubot*, 2019.

[2] Lovelock, J. D., et al. "Forecast: Blockchain business value, worldwide, 2017-2030," *Gartner*, 2017.

[3] 블록체인 전문위원회, “블록체인 기술 동향 보고서”, *한국정보보호산업협회*, 2020.

[4] Manuel, Scott, and Sarah Andrews. "Blockchain technology: Is 2016 the year of the blockchain," *Thomson Reuters: Toronto*, 2016.

[5] Kandaswamy, R., D. Furlonger, and A. Stevens. "Digital Disruption Profile: Blockchain’s Radical Promise Spans Business and Society," *Gartner*, 2018.

[6] Decker, Christian, and Roger Wattenhofer. "Bitcoin transaction malleability and MtGox," *European Symposium on Research in Computer Security*. Springer, Cham, 2014.

[7] Androulaki, Elli, et al. "Evaluating user privacy in bitcoin," *International Conference on Financial Cryptography and Data Security.* Springer, Berlin, Heidelberg, 2013.

[8] Kim, In-Yeung, Ji-Soo Park, and Chang-Hoon Lee. "New consensus algorithm against 51% attack," *Proceedings of the Korea Information Processing Society Conference,* Korea

Information Processing Society, 2018.

[9] Shrivas, Mahendra Kumar, Thomas Yeboah Dean, and S. Selva Brunda. "The Disruptive Blockchain Security Threats and Threat Categorization," *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T),* IEEE, 2020.

[10] CryptoScamDB, last modified Jun 29,2018, accessed May 20,2021, https://cryptoscamdb.org/

[11] Kumar, Nitesh, et al. "Detecting Malicious Accounts on the Ethereum Blockchain with Supervised Learning," *International Symposium on Cyber Security Cryptography and Machine Learning*. Springer, Cham, 2020.

[12] Ko, Kyungchan, et al. "Design of RPC-based Blockchain Monitoring Agent," *2018 International Conference on Information and Communication Technology Convergence (ICTC),* IEEE, 2018.

[13] Zheng, Peilin, et al. "A detailed and real-time performance monitoring framework for blockchain systems," *2018 IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Practice Track (ICSE-SEIP),* IEEE, 2018.

[14] Dinh, Tien Tuan Anh, et al. "Blockbench: A framework for analyzing private blockchains," *Proceedings of the 2017 ACM International Conference on Management of Data*. 2017.

[15] Weber, Ingo, et al. "On availability for blockchain-based systems," *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS),* IEEE, 2017.

[16] Signorini, Matteo, et al. "Bad: blockchain anomaly detection," *arXiv preprint arXiv:1807.03833*, 2018.

[17] Signorini, Matteo, et al. "ADVISE: Anomaly Detection tool for blockchain Systems," 2018 IEEE World Congress on Services (SERVICES), IEEE, 2018.

[18] Swathi, P., Chirag Modi, and Dhiren Patel. "Preventing sybil attack in blockchain using distributed behavior monitoring of miners," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT),* IEEE, 2019.

[19] Farrugia, Steven, Joshua Ellul, and George Azzopardi. "Detection of illicit accounts over the Ethereum blockchain," *Expert Systems with Applications,* 2020

[20] “How to interact with the Ethereum blockchain and create a database with python and sql,” Medium, last modified Jun 29,2018, accessed May 20,2021, https://medium.com/validitylabs/how-to-interact-with-the-ethereum-blockchain-and-create-a-database-with-python-and-sql-3dcbd579b3c0

[21] Patel, Vatsal, Lei Pan, and Sutharshan Rajasegarar. "Graph Deep Learning Based Anomaly Detection in Ethereum Blockchain Network," *International Conference on Network and System Security*. Springer, Cham, 2020.

[22] Putz, Benedikt, Fabian Böhm, and Günther Pernul. "HyperSec: Visual Analytics for blockchain security monitoring," arXiv preprint arXiv:2103.14414, 2021.

[23] Bang, Jiwon, and Mi-Jung Choi. "Design and Implementation of Storage System for Real-time Blockchain Network Monitoring System," 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), IEEE, 2019.

[24] Lee, Chaehyeon, et al. "Blockchain Explorer based on RPC-based Monitoring System," *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC),* IEEE, 2019.

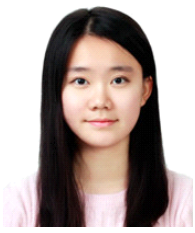
〈저 자 소 개〉

이 은 영 (Eunyoung Lee)

2021년 2월 : 성신여자대학교 융합보안공학과 졸업
2021년 3월~현재 : 성신여자대학교 미래융합기술공학과 석사
<관심분야> 블록체인, 네트워크보안, 융합보안

한 채 림 (Chaerim Han)

2020년 3월~현재 : 성신여자대학교 융합보안공학과 학사
<관심분야> 블록체인, 융합보안, 정보보호



문 정 현 (Junghyun Moon)

2019년 3월~현재 : 성신여자대학교 융합보안공학과 학사
<관심분야> 융합보안, 블록체인, 네트워크보안

이 일 구 (Il-Gu Lee)

2003년 2월 : 서강대학교 전자공학과 졸업
2005년 2월 : KAIST 정보통신대학원 석사
2016년 2월 : KAIST 전산학부 박사
2005년 2월~2017년 2월 : 한국전자통신연구원 5G기가통신시스템연구본부 선임연구원
2017년 3월~현재 : 성신여자대학교 미래융합기술공학과/융합보안공학과 조교수
<관심분야> 융합보안, 미래융합기술