디지털산업정보학회 논문지 제14권 제4호-2018년 12월
http://dx.doi.org/10.17662/ksdim.2018.14.4.047

블록체인 기술 및 보안 위협 분석

전 은 아* · 이 철 희**

Analysis of Technology and Security Threats on Blockchain

Jun Euna · Lee Cheulhee

〈Abstract〉

We analyzed security threats and suggested countermeasures about the block chain technologies which has emerged as a core technology of the fourth industrial revolution. We know that increasing the security leads to slow down program processing rate in the block chain systems. The block chain system which is currently an early stage of technological development, to become an economic and social infrastructure, development of technology and active policy implementation will be necessary.

We studied on the security threats and countermeasures of the Bit Coin based on block chain. Further research should be undertaken on the possibility that future studies could have a real adverse effect on the integrity of the data.

Key Words : Block Chain, BitCoin, Security, Security Countermeasure

Ⅰ. 서론

미래를 위한 핵심 기술로 블록체인에 대한 관심은 인공지능을 뛰어 넘는 위대한 기술로 평가가 되고 있으며, 블록체인의 신뢰를 기반으로 현재 암호 화폐, 가상통화 그리고 가상화폐 등 금융권에서 활발한 기술 발전을 보이고 있으며, 세계경제포럼(WEF, World Economic Forum)은 2016년 8월 보고서를 통해 블록체인이 세계 금융 시스템 의 중심이 될 것이라는 전망을 내놓았다. 또한 블록체인은 탈중개성(P2P-based), 보안성(Secure), 신속성(Instantaneous), 확장성(Scalable), 투명성(Transparent) 등의 장점으로 큰 관심을 받고 있으며, 혁신적인 서비스에서의 블록체인 기술이 많이 고려되고 있다.

블록체인은 네트워크 내의 모든 참여자가 공동으로 거래 정보를 검증, 기록, 보관함으로써 중앙 집중형 서버 없이도 즉, 공인된 제 3자가 없이도 정보의 무결성 및 신뢰성을 확보할 수 있는 기술이다. 개인 간(P2P, Peer to Peer) 네트워크를 가능하게 함으로써 기존 중앙 집중 시스템을 혁신할 수 있는 잠재력을 갖춘 기술로 부상하고 있다.

블록체인의 장점을 기반으로 산업계의 관심이 증가되고 있으며 혁신적인 서비스에 블록체인 기술을 다양하게 고려하여 기술 발전은 극대화 되고 있다. 그러나 현재 블록체인 도입의 대표적인 비트코인 해킹으로 블록체인에 대한 안전성에 대한 논란이 확대

* 한국폴리텍대학교 모바일정보통신과 외래교수
** 한국폴리텍대학교 모바일정보통신과 교수

되고 있으며, 블록체인 기술이 애플리케이션 소프트웨어 및 암호화 기술에 의존하고 있기 때문에 블록체인 기술을 개발하고 제공하는 스타트업에서 사용하는 검증되지 않은 알고리즘에 대한 위험이 존재하고 있다.

따라서 본 논문의 2장에서는 블록체인의 기본 개념을 소개하고, 3장에서는 블록체인 주요 기술에 대해 소개한다. 4장에서는 블록체인과 관련된 보안 위협 및 대응방안에 대해 알아보고, 5장에서 결론을 맺는다.

Ⅱ. 블록체인 개요

2.1 블록체인 정의와 종류

2.1.1 블록체인 정의

블록체인(Block chain, Blockchain)은 관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장환경에 저장되어 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 데이터 위변조 방지 기술이다. 이라고 정의하고 있다. 이는 근본적으로 분산 데이터 저장기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안되었다. 블록체인 기술은 비트코인을 비롯한 대부분의 암호 화폐 거래에 사용된다. 암호화폐의 거래 과정을 기록하는 탈중앙화된 전자장부에 쓰이는 것인데, 이로써 블록체인 소프트웨어를 실행하는 많은 사용자들의 각 컴퓨터에서 서버가 운영되어 중앙은행 없이 개인 간의 자유로운 거래는 불가능 할 수 있다.

2.1.2 블록체인 종류

블록체인 기술을 분류하는 방법은 여러 가지가 있지만, 대표적으로 참여자의 자격을 제한하는 정도에 따라 주로 공개형(public)과 비공개형(private) 으로 분류를 하게 된다. 결과적으로, 참여자가 얼마나 광범위하게 블록체인 네트워크에 참여할 수 있는지에 대한 공개 범위에는 네트워크 접근 및 합의 참여 권한에 따라 공개형, 비공개형, 반공개형(Consortium) 3가지로 구분하며, 사용용도에 맞게 그 응용이 가능하다.

공개형 블록체인의 경우 별도의 권한이 필요 없으며, 누구나 참여 할 수 있는 블록체인으로 가장 일반적으로 이용된다. 네트워크 참여자들은 컴퓨팅 자원을 이용하여 거래의 정당성을 입증할 수 있고 누구든 허가 없이 블록체인의 데이터를 읽고 쓰고 검증할 수 있다. 이러한 이유 때문에 고도화된 암호화 검증이 필요하고, 한 번 정해진 규칙을 변경하기 쉽지 않다는 점과 네트워크의 확장과 거래 속도가 느린 특징이 있다. 또한 완벽한 분산형 구조를 이루고 있어 네트워크 참여자의 익명성이 제공된다. 이에 대한 가장 대표적인 예로는 비트코인이 있으며, 비트코인은 익명성을 기반으로 블록체인을 다운로드하여 어떠한 기록이 담겨있는지 조회하거나 전자서명을 이용해 기록에 참여할 수 있는 것이다.

비공개형 블록체인은 익명성을 제공하는 공개형 블록체인과 달리 주체의 식별이 가능한 것이 특징이다. 개인화된 블록체인으로써 한 중앙기관이 모든 권한을 가지며 네트워크에 참여하기 위해서는 네트워크 접근 및 증명 작업에 권한이 필요하다. 한 기관에 권한이 부여되어 있어 기존의 인프라와 유사하기 때문에 인프라 구축을 위한 비용 절감과 효율성 향상 등의 특징이 있다. 비공개형 블록체인은 허가형 원장(Permissioned Ledger)으로도 정의하며, 이는 읽기, 쓰기, 합의 과정에 참여할 수 있는 참여자가 미리 지정되어 있는 것으로 기본적으로 허가형 원장이 필요

하지만 필요에 따라 특정 주체가 새로 추가되거나 제거될 수 있으며, 설계 목적에 따라 여러 가지 버전으로 비공개형 블록체인을 설계할 수 있는 등 사용자가 원하는 대로 커스터마이징이 가능하다. 중앙 기관이 모든 권한을 보유하고 있어 의사결정에 따라 용이하게 규율을 변경할 수 있고 네트워크 확장이 용이하고 거래 속도가 빠르다는 장점이 있다. 최근에는 비공개형 블록체인을 다양한 형태로 변형한 사례들이 등장하고 있다.

반공개형 블록체인은 공개형 블록체인과 비공개형 블록체인이 결합된 형태로써, 네트워크 접근은 자유로우나 증명 작업에는 권한이 필요하다. 분산형 구조를 유지하면서 제한된 참여를 통해 보안을 강화할 수 있고 공개형 블록체인에서 제기된 느린 거래 속도와 네트워크 확장성의 문제도 해결할 수 있다. 일반 이용자들에게는 기록을 열람할 수 있도록 권한을 부여할 수 있지만, API를 통해 특정 대상에게만 공개할 수도 있다. 일부 기업이나 기관 등의 협업을 위해 연합체를 구성하는 모델이 이에 해당될 수 있다. 연합체에 소속된 참여자가 합의에 따라 상대적으로 용이하게 규율을 변경할 수 있다.

2.2. 블록체인 기능 특징

블록체인의 특징은 크게 무결성, 높은 가용성, 오류 저항성, 그리고 비용 절감이 있다. 이러한 특징으로 블록체인 기술이 금융서비스(통화, 지불 및 결제, 주식 및 채권 발행, 유통, 신탁 등) 및 기타 산업의 이전 원장, 문서관리, 공증, 추적관리, IoT 등에 적용될 것으로 기대된다. <표 1>은 블록체인 기능의 특징을 설명한다.

<표 1> 블록체인 기능 특징

구분	내용
무결성	합의가 성립되면 노드 간 데이터는 변경되지 않는다.
높은 가용성	모든 노드가 거래 장부를 가지고 있기 때문에 비록 노드의 일부가 동작하지 않더라도 다른 노드가 살아있는 한 네트워크는 계속 동작한다.
오류 저항성	노드 사이의 네트워크가 망가졌다고 해도 시스템 오류가 발생하지 않는다.
비용절감	시스템 비용, 계약 관리 비용, 지불 및 결제 작업, 유지보수 비용 등은 분산 처리에 의해 감소된다.

Ⅲ. 블록체인 주요 기술 분석

3.1 블록체인 기술 정의

3.1.1 P2P 분산 데이터베이스

고가용성을 위해서는 운영체제 배포가 필수적이다. 하드웨어/지역/지정학적 위험이 분산된 국경 간 운영체제는 안정화된 운영체제가 되도록 한다.

3.1.2 합의 알고리즘

정확한 거래의 유효성을 확인을 위한검증을 위해서는 “Proof of Work” 혹은 이더리움의 지분 증명 “Proof of Stake, PoS”이 대표적인 방법이며, 이를 포함한 합의 절차가 필요하다. 일부 참가자가 잘못된 정보를 보내는 경우에도 참가자간에 올바른 합의를 달성해야 한다.

3.1.3 분산 원장기술

분산 원장은 블록체인이 탈중앙화가 가능하게 하는 특징으로, 참여자들 간의 합의에 의해 복제 및 공유되며, 블록이라 부르는 저장소에 동기화된 정보를 기록한다. 블록체인에서 분산 장부는 발생하는 모든 거래와 정보들을 참여자들의 검증 과장을 거쳐 기록하며, 모든 참여자들이 동일한 정보를 소유하게 된다.

3.1.4 암호화 기술

블록체인을 기반으로 동작하는 화폐를 지칭할 때 흔히 암호 화폐(Cryptocurrency)라는 용어를 사용하는데, 이는 암호화 기술이 블록체인의 핵심 요소 이다. 암호화 기술 중에 대표적인 기술로 PKI(Public Key Infrastructure) 기반의 디지털 서명과 암호화 해시(Cryptographic hash)가 있으며, PKI는 흔히 사용되고 있는 공인인증 시스템이라 볼 수 있다. 블록체인 상에서 발생하는 거래의 부인 방지를 위해 사용하며 암호화 해시는 어떤 입력값에 대해 출력 값은 알기 쉽지만 역으로 주어진 출력값에 대응하는 입력값을 알아내는 것은 불가능하므로, 이를 통하여 블록체인 데이터의 무결성을 유지하며, 또한 분산원장 간의 연결성을 부여하는 중요한 요소 기술이다.

3.1.5 스마트 컨트랙트 (Smart Contract)

스마트 컨트랙트는 Nick Szabo가 작성한 “Smart Contract: Building Blocks for Digital Market”라는 글에 처음 등장한 개념으로, Szabo는 스마트 컨트랙트란 “디지털 형식으로 표현된 약속의 집합으로 약속을 이행하는 주체가 이를 수행하는 프로토콜을 포함한다.”고 정의하였으며, 거래의 신뢰를 위한 중개인을 최소화하고 특정 계약 조건을 실행하기 위한 전자상거래를 위한 프로토콜이다. 2세대 블록체인이라 불리는 이더리움 이후의 블록체인들은 스마트 컨트랙트를 지원하여, 중개 혹은 중앙 기관 없이 거래 당사자 사이에 직접 거래가 가능케 하는 한편, 거래된 조건과 결과는 분산 원장에 기록하여 거래 정보의 신뢰성과 무결성을 보장한다.

3.2 블록체인 요소 기술 분석

3.2.1 검증을 위한 동의와 합의 기술

본 논문 3.1장에서 기 서술한 바와 같이 블록체인 기술은 인터넷상에서 사용자 간 직접 데이터를 주고받는 구조인 P2P 네트워크를 기반으로 하고 있어 사용자간의 신뢰가 중요하며, 이는 중앙 관리 주체 없이 모든 참여자가 동시에 운영 가능한 분산 구조이기 때문에 누구나 임의로 데이터를 입력, 변경, 또는 삭제할 수 있어 거래 승인에 참가자들의 합의가 필요하다. 블록체인은 특정인들에게 합의 참여 권한을 주고 합의 알고리즘을 통해 원장에 기록될 데이터를 선별 및 검증하여 데이터의 완전성을 유지한다. 즉, 참여자들이 서로 데이터가 무결한지 동의한 후에 거래를 진행한다. 블록체인 기술에 사용되는 4개의 주요 합의 알고리즘은 PoW(Proof of Work), PoS(Proof of Stake), PoI(Proof of Importance), PBFT(Practical Byzantine Fault Tolerance)로 나눌 수 있다.

(1) 작업 증명 (PoW, Proof of Work)

블록체인의 가장 기본적인 합의 알고리즘으로 블록체인 기술의 근원인 비트코인에 사용된다. 네트워크 참가자가 비트코인 P2P 네트워크에서 거래의 정확성을 확인하고 검증하여 관리자 중개 없이 가치 이전을 가능하게 하는 구조이다. 거래를 확인하는 참가자를 채굴자(Mining Node)라고 하며, 이들에 의해 검증된 거래는 블록이라고 불리는 단위로 기록된다. 여러 채굴자가 동시에 블록을 연결할 때 블록체인 분기가 발생하고, 분기 이후에 연결된 일부 블록들의 체인은 되돌릴 수 없다. 일반적으로 비트코인에서는 승인절차(블록추가)는 10분 간격으로 수행되며, 6회가 수행되었을 때(약 1시간 경과 후) 명확한 것으로 간주된다. 그러나 거래 승인 과정에서 고비용의 컴퓨팅 자원을 요구하는 작업 또는 문제를 해결하게 하였을

때, 이를 해결하여 형성된 블록체인 중 가장 긴 블록체인, 즉, 비용이 많이 소비된 체인을 진짜로 인식하여 다른 기록들은 폐기하는 알고리즘이다. 블록을 생성하는 것은 간단하지만 많은 컴퓨터 자원이 요구되는 채굴작업이 필요하기 때문에 악의적인 채굴자가 가짜 블록체인을 확장하고 유효성을 검증하기 위해서는 거대한 컴퓨터 자원을 요구하므로 블록체인을 수정하는 것은 사실상 불가능 하며, 블록체인을 조작하기 위해서는 전체 참여자의 과반수보다 많은 컴퓨팅 자원을 보유해야 한다. 또한 PoW 알고리즘 채굴자는 고비용을 지불해야 하므로 특정 채굴자 그룹에 집중되어 있다.

결과적으로 PoW는 데이터의 무결성은 보장해 주지만 채굴풀의 집중화와 독점화 문제, 과도한 에너지 소비와 같은 문제점이 있다.

(2) 지분 증명 (PoS, Proof of Stake)

PoW의 단점을 보완하고자 개발되었으며, 채굴대신 참여자들의 코인 보유량 및 코인 보유 기간에 따라 채굴의 어려움을 감소시켜 컴퓨터 자원 낭비를 줄인다. 참여자들의 코인 지갑이 블록을 만들고 이에 대한 보상으로 코인을 받는 형식으로 코인을 보유하고 있으면 이자개념의 코인을 받을 수 있어 채굴하지 않아도 된다. 따라서 참여자의 소유 지분이 블록 생성권 지분율이 되며 블록의 생성 주기가 매우 짧아질 수 있고 독점화 현상을 막을 수 있다는 장점이 있다. 하지만 전체 네트워크의 사용자 상태를 알아야한다는 점과 지분율이 높은 사용자가 블록을 생산할 가능성이 높기 때문에 빈익빈 부익부 현상이 나타날 수 있다는 단점이 있다.

(3) 중요성 증명 (PoI, Proof of Importance)

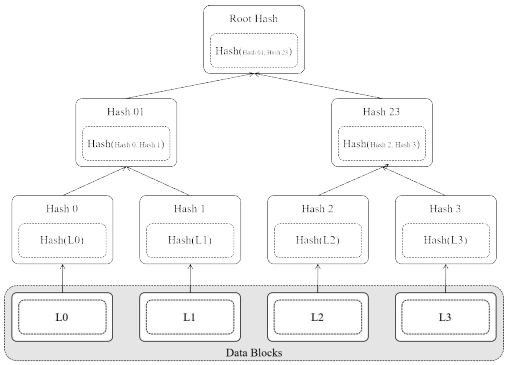
디지털 통화인 NEM(New Economy Movement)에서 처음 제안되었으며 네트워크 참여도로 평가등급이 결정된다. PoI는 구글의 검색 알고리즘이었던 Page Rank 알고리즘을 응용하였으며, PoS와 유사하지만 계정의 잔액 규모에만 의존하지 않는 점이 다르다. PoS에서 제기된 빈익빈 부익부 현상을 방지하고자 계정의 잔액 규모가 아니라 많은 양의 코인을 빈번하게 거래할수록 더 많은 보상을 갖게 된다.

(4) 실용적 비잔티움 장애 허용 (PBFT, Practical Byzantine Fault Tolerance)

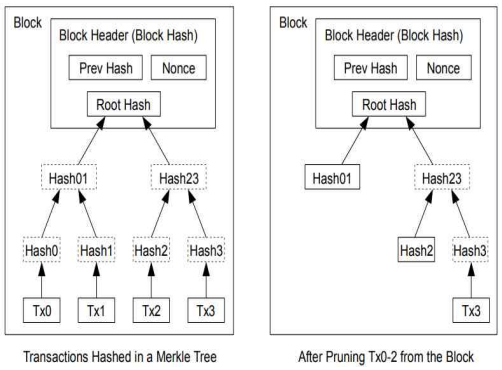
블록을 생성하는 권한이 특정 사용자(코어 노드)에 의해 지배되고 거래의 유효성이 특정 사용자의 회의에 의해 검사되는 구조이다. 특정 사용자는 신뢰할 수 있는 조직에서 운영해야 하며, 이 구조에서는 PoW, PoS 및 PoI와 같은 "특정 관리자의 중재 없이 만들 수 있는 합의"와 같은 기능은 없지만 민첩하고 신뢰할 수 있는 가치 이전을 가능하게 한다. 그러나 일반적으로 네트워크에서 PBFT를 채택하면 특정 사용자의 장애로 인해 전체 네트워크가 중단될 수 있다는 우려가 있어 가용성에 주의를 기울여야 한다.

3.2.2 거래내역의 무결성 검증 기술

블록 내에 있는 거래내역, 즉, 송금지시의 삽입·삭제 방지와 블록체인 내 블록 삽입·삭제 방지를 위해 체이닝(chaining) 기술을 적용한다. 체이닝 기술은 하나의 블록을 생성하였을 때 이전에 생성된 블록들과 연결시키는 기술이다. 연결되는 블록에는 앞선 부모 블록의 해쉬 값을 기록하기 때문에 <그림 1>에서 보는 바와 같이 연결리스트 구조 및 해쉬트리(또는 머클트리) 구조로 블록들이 연결되어 있다. 블록 생성 시 해쉬트리의 루트 값이 정해져 블록에 기록되기 때문에 임의로 연결되어 있다. 임의로 특정 거래내역을 변조할 경우 해쉬트리의 루트 값과 불일치하게 되어 탐지가 가능하다. 이 때, 루트해쉬는 트리구조에서 송금지시를 최하위 노드로 하여 계산된 값으로, 루트 해쉬를 통해 송금지시의 무결성을 검증한다.



<그림 1> 해쉬트리 [30]



<그림 2> 해쉬트리 변형 [30]

또한 중간에 있는 블록의 변조를 위해서는 마지막 연결 블록에서부터 변조하고자 하는 블록까지를 빠른 시간 안에 순차적으로 조작해야 하는데, 이 과정은 검증시간보다 오래 걸리기 때문에 데이터 위·변조가 어렵다.

따라서 체이닝 기술에서는 생성된 블록을 블록체인에 연결시키고자 할 때 보다 많은 블록이 연결되어 있는 블록체인이 악의적인 조작 가능성이 낮은 것으로 간주하여 이에 연결시킨다.

이 때, 모든 거래가 누적된 블록의 사본을 저장해야 하므로, 전체적으로 상당한 디스크 공간이 소모된다. 이 문제를 해결하기 위해, 대부분의 사용자들은 블록 헤더만을 저장하며, 전체 블록은 일부 사용자만 저장함으로써 문제를 해결할 수 있다. 다만, 블록 헤더가 무결성 확인에 기여할 수 있도록, 해당 블록에 포함되어야 할 거래들을 leaf로 한 해쉬트리를 구성하고 이 트리의 루트를 블록 헤더에 포함하는 과정을 <그림 2>에서 보여주고 있다.

Ⅳ. 블록체인 보안 위협 및 대응방안

블록체인 기술 적용의 경우 보안 고려사항에 대해서는 현재 2017년 금융보안원에서 금융권 블록체인 도입 시 보안 위협을 키 관리, 거래 검증 및 합의, 참여자 권한 관리, 블록체인 S/W 보안, 서비스 보안의 5가지로 분류하여 그 위협에 대한 대책을 마련해야함을 경고하고 있다. 본 장에서도 블록체인 도입의 경우 현재 발생 가능한 위협과 대응방안에 대해 키 관리, 개인정보유출, 통화소 위협, 분산구조에 대한 위협, 이중지불 위협에 대해 분류 및 분석하였으며 블록체인 위협 기술에 대해 비트코인의 경우를 통해 이에 대한 대응방안도 함께 제시한다.

4.1 사용자의 개인키 분실, 유출

블록체인은 거래의 내역을 생성하는 블록에 대한 무결성 등을 보장하기 위해 사용되는 암호학적 방식인 개인키와 공개키를 사용한다. 키의 분실과 유출의 시 접근 권한 상실로 인해 블록체인에서 제공되는 기능 보장을 할 수 없게 된다. 공개키는 비트코인의 주소가 되고 개인키는 비트코인 지갑을 이용하여 생성 및 관리할 수 있다. 비트코인을 안전하게 보호하기 위해서 비트코인 주소와 쌍이 되는 개인키를 안전하게 보호해야 할 것이다. 개인키와 공개키가 분실되거나 유출되는 경우는 대표적으로 사용 디바이스에 악성코드에 감염되어 저장된 개인키에 접근하거나 개인키가 암호화 함수에 호출될 때 악성코드에 의해 유

출되는 경우와 디바이스를 분실하거나 파기된 경우로 분실의 경우는 획득한 사람이 비트코인 자원을 사용할 수 있게 되며, 파기된 디바이스를 복구하여 비트코인 지갑을 획득할 수 있는 경우도 동일한 손실을 가져오게 된다. 이에 대한 대응방안으로는 지갑의 암호 설정을 통해 안전성이 검증된 암호길이 및 알고리즘을 사용하여야 하며, 비트코인 지갑의 데이터를 백업하여 사고에 대비해야 한다. 그러나 이러한 경우도 기술·관리적으로 보호 되지 않다면 위협이 될 수 있다.

4.2 개인정보 유출 피해

블록체인이라고 불리는 이유는 '노드'라고 불리는 참여자 모두가 특정 정보를 공유함으로써 정보의 체인이 형성되어 블록 형태로 묶이기 때문이다. 블록체인의 해킹에 대한 문제는 "블록체인은 DDoS 공격에 아주 취약한데, 특정 노드단을 공격하면 그 노드단에 물려있는 노드들이 막혀버리면서 상당한 어려움에 빠지게 되며 블록체인에 올라가는 개인정보를 어떻게 보호할 것인가에 대한 주제가 부각되고 있다"는 문제가 대두되고 있다.

현재 블록체인 기술이 적용된 분야 중 인터넷을 통한 채굴 및 거래 과정에서 자동으로 기록되는 IP주소, 거래시간 등 개인정보 성격의 정보를 내재하고 있어 개인정보에 대한 유출 우려도 제기되고 있으며, 개인정보를 보호하기 위해 암호화를 적용하는 경우에도 암호키 관리에 대한 문제로 다시 귀결된다. 이에 대한 대응방안으로 유출로 인한 2차 피해사고가 발생하지 않도록 개인정보에 대해 암호학적인 방식을 적용하여 보호해야하며, 개인정보가 보호되지 않는다면 거래 과정에서 개인정보에 대한 요구사항을 제한적으로 사용해야한다. 블록의 내용에 따라 달라질 수 있으나 특정인에 대한 정보가 너무 많으면 개인의 보안이 침해되는 문제가 발생할 수 있기 때문이다.

4.3 디지털통화 거래소의 기술 및 관리 미흡

거래소의 기술적·관리적 조치 미비와 사고 발생 보안의식 부족 및 과실로 인한 데이터 유·노출 사고가 발생할 수 있다. 이는 암호화폐 거래소들의 연이은 해킹으로 거래소를 규제해야 한다는 논의가 지속적으로 진행되고 있으며, 2018년 6월에 발생한 빗썸 해킹 사건으로 암호화폐 거래소가 보안 이슈를 비롯해서 안전성 및 투명성과 관련된 여러 문제들이 대두되고 있다. 거래소에서는 전자적인 방식으로 환전이 이루어지기 때문에 거래소는 지속적인 공격 대상이 되어 금전적 손실이 발생할 수 있다. 이러한 문제는 거래소에 대한 보안성 향상에 대한 요구는 필수적이다.

이에 대한 대응방안으로 플랫폼 개발사에서는 이용자의 주요 신용 정보, 거래 정보 등을 보호해기 위한 기술을 영역별로 정확하게 설계되어 있어야 한다. 그러나 보안에 대한 기반기술의 이해 등이 부족할 경우 암호화에 대해 간과하거나 암호통신 구조 설계의 오류로 인해 다양한 공격에 취약하게 된다. 이를 위해서는 모든 암호화폐 거래소를 대상으로 국내의 경우에는 ISMS-P 인증 등을 취득하도록 제도적으로 강화하고 거래소의 미흡한 보안 부분에 대해서도 민간영역에서 자율규제와 보안수준 향상을 위한 투자가 이루어져야만 한다.

4.4 분산네트워크 구조 공격

블록체인은 네트워크로 연결된 모든 참여자가 공동으로 거래 정보를 검증하고 기록·보관하게 해주는 기술로 P2P 분산네트워크 공격 등 신종 보안위협이 등장하고 있다. 지난 2014년 일본의 마운트 콕스 비트코인 거래소는 수십억 달러에 해당하는 해킹 피해로 파산 신청을 하였고, 미국의 Input.io사는 1백 2십만 달러 상당의 비트코인을 해킹 당한 바가 있다.

국내에서는 2014년 말 비트코어(bitcore) 거래소에서 해킹으로 의심되는 사건이 발생하였다. 개인 간 거래 중개 플랫폼(P2P)을 통해 지속적으로 거래를 기록하고 있어 미들웨어, 데이터베이스, 보안, 분석, 금융 등에서도 부담을 줄 수 있는 문제점이 있다. 이러한 경우 프라이빗 블록체인의 경우 의심 거래를 발생시키는 참여자를 네트워크에서 차단하는 등의 조치가 가능하지만 공격자가 많은 수의 노드를 장악할 경우 여전히 DDoS 공격이 가능은 존재하게 되는 위협을 가지고 있다. 그러나 블록체인 해킹에 대응하기 위한 방안으로 분산 네트워크에서 수집된 수많은 위협 정보에 대한 상관관계를 분석해 공격을 찾고, 대응 방법을 각 분산 노드에 배포하고 보안 정책을 업데이트하는 과정에 대한 자동화를 통해 문제 해결이 가능하다.

4.5 이중지불 공격 위협

2015년 금융보안원에서는 이중 지불 공격을 소개했다. 해당 보고서는 이중 지불 공격자가 지불된 비트코인을 회수 또는 재지불하여 성공적으로 거래 승인을 완료하고 최종적으로는 지불받지 못한 자의 손실이 발생되는 현상을 설명하고 있다. 이와 같은 공격이 가능한 이유는 블록체인 과정 중 검증 합의 과정의 특성으로 발생될 수 있는 현상이며, 블록체인을 기반으로 한 전자화폐시스템은 분기된 체인들 중 가장 긴 체인을 선택하는 방식을 취하기 때문에 낮은 확률이지만 여전히 이중지불이 발생하는 가능성이 존재하는 공격 위협이다.

우선 블록체인에서 거래내역은 블록에 포함되어야 하며 해당 블록이 정상 체인에 연결되기 위해서는 블록이 채굴자에게 도달해야 한다. 하지만 공격자가 생성한 거래내역이 포함된 블록이 먼저 채굴자에게 도달하게 한다면 정상적인 거래내역보다 공격자에 의해 생성된 거래내역이 먼저 채굴에 성공하게 된다. 이점을 이용하여 이중거래 등의 위협이 발생가능하다.

또한 블록체인의 또 다른 구조적 특징은 블록체인에 상충된 블록체인 등장하게 되면 모든 노드들은 길이가 긴 블록체인을 받아드리게 되는데, 그 이유는 블록체인이 길다는 건 그만큼 채굴 비용이 많이 투자되었고 정상적인 검증이 많이 이루어졌다고 판단하기 때문이다.

이러한 특징은 공격자의 채굴 환경이 고비용으로 구축되고 상충된 긴 길이의 블록체인을 형성할 수 있다면 공격에 성공할 수 있다는 것을 의미하며, 공격자의 성공확률은 채굴성능에 기반하며 채굴성능이 높을수록 상충된 블록체인의 길이를 길게 만들 수 있고 이를 통해 비정상 거래내역이 포함된 블록체인이 신뢰받는데 성공할 수 있게 된다.

만일 전체 채굴성능이 50%이상의 성능을 공격자가 구비하고 있다면 길이가 긴 상충된 블록체인을 생성하는데 높은 성공 확률을 보유하고 있다고 할 수 있으며, 또한 블록체인을 생성하는 네트워크를 일부 단절시켜 단절된 네트워크를 제외한 채굴 성능의 50%를 유지하여 공격에 성공할 수 있다. 이에 대해서는 2018년 7월 캐나다 중앙은행이 대형 블록체인 네트워크에 대한 이중지불 공격이 현실적으로 불가능하다는 연구 결과를 토대로 대응방안을 제시하고자 한다. 방안으로 게임이론을 응용해 이중지불 공격으로부터 작업증명 합의 프로토콜의 보안과 공공원장 기록의 불가역성을 보장할 수 있는지를 이중지불 가상공격을 실시하여 거래 확인 지연을 증가시켜 이중지불 공격의 위험을 낮출 수 있다고 하였으며, 거래 관련 서비스나 상품을 제공하기에 앞서 확인해야 할 블록 수를 증가시키는 방식으로, 이중지불이 발견될 때 권장되는 최초 대응방안을 제시하였다. 이중지불 공격에 대한 또 하나의 대응방안으로 새로운 작업증명 합의 알고리즘 개발이다. 현재 블록체인에 적용 가능한 완벽한 합의방식은 아직 존재하지 않기 때문에 합

의 알고리즘 개발이 이중지불에 대한 공격에 대한 대응방안으로 모색될 수 있다.

Ⅴ. 결론

본 논문에서는 세계적으로 4차 산업혁명의 핵심기술로 부각되고 있는 블록체인의 주요 기술에 대해 보안 위협을 분석하고 이에 대한 대응 방안을 제안하였다. 블록체인 기술에 대해 많은 기술 분석이 이루어지고 있지만, 보안성을 향상 시키는 경우 발생하는 속도 저하 등의 문제 등에 대해 해결하지 못한 문제점이 존재하고 있으며, 현재 기술 발달의 초기 단계인 블록체인 기술이 경제·사회의 인프라로 자리 잡기 위해서는 기술의 연구를 통한 발전과 더불어 적극적인 관련 정책 추진이 필요할 것이다.

특히 본 논문에서 블록체인의 보안 위협 및 대응방안에 대해 블록체인 중 가장 오래, 널리 연구된 비트코인에 대해서 노드들 간의 미세한 확인(validation) 시간차를 활용하거나 특정 노드 주변의 네트워크를 무력화시킴으로써 가능해지는 이중 지불 공격, 일부 비트코인 응용 구현의 프로그램 버그를 활용하는 공격 또는 해킹에 의한 개인키 탈취 공격, 채굴풀을 이용한 불공정 채굴 경쟁 등 5가지로 분류하여 분석하였다. 향후 연구로 새로운 작업 증명 합의 알고리즘 개발과 데이터의 무결성에 실질적 악영향을 미칠 수 있는 공격 위협 및 대응방안에 대한 더 많은 연구가 수행되어야 한다.

참고문헌

[1] 고경찬 외, “블록체인 네트워크 모니터링 및 분석 시스템,” KNOM Conf. 2018.

[2] 과학기술정보통신부, “신뢰할 수 있는 4차 산업혁명을 구현하는 블록체인 기술 발전전략,” 2018.

[3] 금융보안원, “ 블록체인 개발 플랫폼 현황 및 활용 사례,” 2016.

[4] 금융보안원, “국내외 블록체인 활용 동향 및 보안 기술 보고서,” 2015.

[5] 금융보안원, “금융권 블록체인 활용 방안에 대한 정책 연구,” 2016.

[6] 금융보안원, “블록체인 기술과 보안 고려사항,” 2017.

[7] 금융보안원, “블록체인 및 비트코인 보안 기술,” 2015.

[8] 금융보안원, “블록체인 응용기술 개발 현황 및 산업별 도입 사례,” 2017.

[9] 금융보안원, “전자금융과 금융보안,” 2016.

[10] 금융보안원, “해외 금융권 블록체인 컨소시엄 동향,” 2016.

[11] 김광훈, “블록체인 기술의 이해 및 적용 현황,” ie 매거진, 25권, 1호, 2018, pp. 13-19.

[12] 김상근, “M2M 환경의 혼잡 네트워크 개선을 위한 블록체인 경량화에 대한 연구,” 디지털산업정보학회 논문지, 14권, 3호, 2018, pp. 69-75.

[13] 김정숙, “블록체인 기술의 이해 및 적용 현황 및 문제점 분석,” 융복합지식학회논문지, 6권, 1호, 2018, pp. 135-140.

[14] 김희열, “블록체인 플랫폼의 보안 위협과 대응 방안 분석,” 한국정보기술학회논문지, 16권, 5호, 2018, pp. 103-112.

[15] 박준한 외, “블록체인 구현측면 정보보안 동향 및 시사점,” 정보기술진흥센터 주간기술동향, 2018.08.

[16] 오경희, “분산원장기술(블록체인) 국제 표준화 현황,” 정보보호학회지, 제28권, 4호, 2018, pp. 41-47.

[17] 이동영 외, “블록체인 핵심 기술과 국내외 동향,” 정보과학회지, 제35권, 6호, 2018, pp. 22-28.

[18] 이세열, “블록체인을 적용한 사설 클라우드 기반

침입시도탐지," 디지털산업정보학회 논문지, 제14권, 2호, 2018, pp. 11-17.
[19] 이제영, "블록체인(Blockchain) 기술동향과 시사점," 동향과 이슈, 34호, 2017, pp. 1-21.
[20] 정성교, "블록체인 기술 및 연구 동향 분석," KERC, 2018.
[21] 정용식 외, "블록체인 기반 가상화폐 거래의 보안 위험 및 대응방안," 한국정보전자통신기술학회 논문지, 2018, 제11권, 1호, pp. 100-106.
[22] 조주현, "블록체인(Block chain)의 등장과 기업 금융에 미치는 영향," POSRI 보고서, 2016.12.
[23] 최대선 외, "블록체인과 인증," 한국통신학회지(정보와 통신), 제35권, 7호, 2018, pp. 11-17.
[24] 홍상원 외, "이더리움 블록체인 성능 향상을 위한 기술 동향," 한국정보과학회, 2018, pp. 1943-1944.
[25] ETRI 미래전략연구소 표준연구본부, "블록체인," 표준화 동향, 2017.
[26] F. Tschorsch and B. Scheuermann, Bitcoin and beyond: a technical survey on decentralized digital currencies, IEEE Communication surveys & tutorials, Volume: 18, Issue: 3, 2016, pp. 2084–2123.
[27] http://www.ddaily.co.kr/news/article.html?no=168281
[28] https://bitcoin.org/en/how-it-works~
[29] https://ko.wikipedia.org/wiki/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8#cite_note-6
[30] https://www.wired.co.uk/article/bitcoin-myspace-cryptocurrency-blockchain
[31] MultiChain Private Blockchain — White Paper, http://www.multichain.com/download/MultiChain-White-Paper.pdf
[32] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009, [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

■ 저자소개 ■

전 은 아
(Jun Euna)

2017년 3월~현재
한국폴리텍대학 정수캠퍼스
모바일 정보통신과 외래교수
2011년 8월
고려대학교 정보보호대학원
정보보호학과 (공학박사)
관심분야 : 정보보안, 디지털포렌식, 사용자인증
E-mail : eajun@korea.ac.kr

이 철 희
(Lee Cheulhee)

1997년 3월~현재
한국폴리텍대학 정수캠퍼스
모바일정보통신과 교수
2000년 8월
조선대학교 대학원 전자공학과
(공학박사)

관심분야 : IoT, 네트워크보안, 시스템보안,
E-mail : lch@kopo.ac.kr

논문접수일 : 2018년 11월 22일
수 정 일 : 2018년 12월 3일
게재확정일 : 2018년 12월 17일