블록체인 노드 신뢰성 향상을 위한 사용자 검증 시스템

User verification system for improving blockchain node reliability

저자
(Authors)

안규황, 서화정
Kyuhwang An, Hwajeong Seo

출처
(Source)

한국정보통신학회논문지 22(9), 2018.9, 1264-1270 (7 pages)
Journal of the Korea Institute of Information and Communication Engineering 22(9), 2018.9, 1264-1270 (7 pages)

발행처
(Publisher)

한국정보통신학회
The Korea Institute of Information and Communication Engineering

URL

http://www.dbpia.co.kr/Article/NODE07538588

APA Style

안규황, 서화정 (2018). 블록체인 노드 신뢰성 향상을 위한 사용자 검증 시스템. 한국정보통신학회논문지, 22(9), 1264-1270.

JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 22, No. 9: 1264~1270, Sep. 2018

블록체인 노드 신뢰성 향상을 위한 사용자 검증 시스템

안규황[1] · 서화정[1*]

User verification system for improving blockchain node reliability

Kyuhwang An[1] · Hwajeong Seo[1*]

[1*]Department of IT Engineering, Hansung University, Seoul 02876, Korea

요 약

블록체인(Blockchain)이란 중앙 서버를 둔 기존의 시스템에서 중앙 서버를 제외 하고 각 노드를 P2P(Peer to Peer) 방식으로 직접 연결하는 기술이다. 블록체인의 종류 중 하나인 public 블록체인 같은 경우 체인에 연결되기 위한 노드로 구성 되는데 별다른 규제 조건 없이 아무나 참여할 수 있으며, 체인에 연결하기 위한 nonce만 발견한다면 모든 노드에 데이터를 전파(broadcast)할 수 있다. 이때 nonce를 발견한 노드가 악의적 의도로 블록에 악성코드를 숨겨 전파한다면, 블록체인의 탈중앙화 시스템의 특징으로 인해 체인에 참여한 모든 노드가 악성코드에 감염 돼 큰 문제가 발생 할 수 있다. 본 논문에서는 해커들이 악용할 수 있는 public 블록체인의 특징인 아무나 노드로 참여할 수 있다는 점을 해결하기 위해, AI 기술이 접목 된 방화벽을 통하여 악의 의도를 가진 사용자는 노드로 참여할 수 없게 제한하여 각 노드에서 전파하는 데이터에 대하여 기존의 데이터보다 신뢰성을 높이고자 한다.

ABSTRACT

Blockchain is a technology that directly connects each node to P2P method, except for the central server. A public blockchain is one of the blockchain types, anyone can participate without any restriction. If some node find nonce, which node can broadcasted data to all nodes. At this time, if a node that finds a nonce hides malicious code in the block, all nodes participating in the chain may be infected with malicious code due to the characteristics of the decentralization system of the blockchain. In this paper, to solve the problem that hackers can participate as an any node, we propose that a user with malicious intent can not participate as a node through a firewall with AI technology. This will improve the reliability of the propagated data over existing data.

키워드 : 블록체인, 악성코드, 암호 화폐, 원장, 인공지능

Key word : AI, Blockchain, Crypto-currency, Ledger, Malicious code

Received 18 May 2018, **Revised** 29 May 2018, **Accepted** 21 June 2018

*** Corresponding Author** Hwa-jeong Seo(E-mail:hwajeong@hansung.ac.kr, Tel:+82-2-760-8033)
Department of IT Engineering, Hansung University, Seoul 02876, Korea

Open Access http://doi.org/10.6109/jkiice.2018.22.9.1264 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

최초의 암호 화폐[1]는 2008년 10월 31일에 사토시 나카모토(Satoshi Nakamoto)에 의해 제안되었다. 처음에 나왔을 때는 현재와 같이 엄청난 이슈를 이끌어 내진 못하였다. 그러나 2017년 8월 경 랜섬웨어(ransomeware)[2]가 전 세계적으로 강타를 하였고 이때 랜섬웨어에 감염 된 pc를 복호화 하고 싶을 경우 일정 비트코인(bitcoin)을 요구하면서 비트코인에 대한 사람들의 관심을 이끌어 냈고, 본격적으로 붐이 일어나기 시작했다. 전문가들은 실물도 없는 암호 화폐를 어떻게 신뢰하는가에 대한 문제를 제기함과 동시에 과연 그 암호 화폐가 해커들에게 공격당하지 않고 지켜낼 수 있는지 많은 전문가들이 의문을 제시했다. 그럼에도 불구하고 이렇게 비트코인이 유명세를 떨칠 수 있는 이유는 바로 비트코인에 적용된 블록체인 기술 덕분이다.

블록체인이란 원장에 기록되는 데이터들을 블록으로 형성하여 모든 블록을 체인으로 구성하는 기술이다. 비트코인에 적용된 블록은 그림 1과 같이 구성되어 있다. Header안에는 이전 prev_hash 값이 들어있어, 만약 block02를 악의적인 목적으로 해킹하려고 한다면 현재 해시 값(hash values)을 수정하게 되는데, 그렇게 되었을 경우 앞에 있는 block01의 prev_hash와 뒤에 있는 block03의 prev_hash또한 수정이 이루어져야하고, 수십만 개로 이루어진 체인의 경우 연쇄적인 작용으로 인해 모든 노드의 prev_hash값을 수정 해줘야하기 때문에 해킹할 수 없는 안전한 구조라고 말하고 있다. 그러나 이것은 연결된 블록이 신뢰할 수 있는 안전한 블록이라는 가정 하에 안전한 구조라고 말할 수 있다.

블록체인은 탈중앙화 시스템으로 모든 노드가 자신의 데이터 기록만 갖고 있는 구조가 아닌 모든 노드의 데이터 기록을 갖고 있는 구조이다. 따라서 새로운 노드가 추가 될 경우, 새로운 노드가 기존의 노드들이 가지고 있는 데이터 기록을 저장하게 되는데 이때 기존의 데이터에 악성 코드가 담긴 블록이 존재한다면 새로 들어온 노드 역시 감염되게 된다. 이는 블록체인의 탈 중앙화라는 특징으로 인해 어떠한 노드가 블록을 체인으로 구성하는데 있어 nonce를 발견하여 별다른 규제 없이 등록한다면 걷잡을 수 없는 혼란을 일으킨다. 따라서 본 논문에서는 이에 대한 해결 방안을 제시하고자 한다.

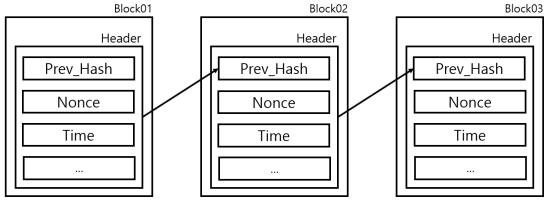

Fig. 1 A blockchain structure that shows how connected

Ⅱ. 관련 연구 동향

본장에서는 블록체인 취약점을 분석하기 위한 사전 지식으로 어떤 블록체인 알고리즘이 취약점에 노출 되었는지 알아보기 위해 블록체인 알고리즘 종류에 대해 알아보며, 블록체인을 활용한 anti-malware를 제안한 기술 그리고 탈 중앙화 방화벽을 이용하여 malware로부터 시스템을 보호하는 블록체인 기술에 대하여 알아보겠다.

2.1. Blockchain algorithm type

블록체인의 알고리즘은 크게 2가지로 분류할 수 있다. 첫 번째로 public 블록체인 알고리즘과 두 번째로 private 블록체인 알고리즘이다. Public 블록체인 종류는 대중에 가장 많이 알려진 비트코인[1]과 이더리움(etherum)[3]에서 사용하는 알고리즘으로 채굴(mining)을 하는데 아무런 규제 조건 없이 모든 사람이 참여할 수 있는 알고리즘 방식이다. 반면 private 블록체인은 리플(ripple)[4]에서 채택한 알고리즘 종류로 최초의 노드가 참여하는 노드를 선택하여 채굴에 참여시킬 수 있는 구조이다.

구체적으로 public 블록체인과 private 블록체인의 대표적인 알고리즘을 비교해 보면, 표 1과 같다. Public 블록체인에서 가장 대표적인 알고리즘은 PoW(Proof of Work)[1]이며, private 블록체인의 가장 대표적인 알고리즘은 PBFT(Practical Byzantine Fault Tolerance)[5]이다. PoW의 경우 데이터가 들어오면 데이터가 들어오면 해당 데이터가 신뢰할 수 있는 데이터인지 체인에 연결된 모든 노드가 신뢰성 검증에 참여하고 신뢰성을 검증한 노드가 일정 코인(coin)을 지급 받는다. 1개의 데이터를 모든 노드가 참여해 신뢰성을 검증하기 때문에 1대라도 작동 중이라면 시스템이 돌아가는데 문제없다. 이때 데이터를 검증하는데 있어 CPU가 사용 되는데, CPU

의 성능이 좋은 컴퓨터는 계속 데이터 신뢰성 검증에 성공해 독점하게 될 가능성이 있으며, 전기세가 낮은 지역에서 많은 컴퓨터를 돌려 독점할 가능성 또한 존재한다. PBFT의 경우 private 블록체인 알고리즘이기 때문에 제일 처음에 존재하는 노드가 부여한 신뢰할 수 있는 노드만 참가할 수 있으며, 참가 된 노드는 모두 평등하다. 따라서 데이터가 들어왔을 때 신뢰성을 검증하는데 다수결의 원칙을 사용한다. 1/3이상의 컴퓨터가 문제가 없다면, 시스템이 동작하는데 문제가 발생하지 않는다.

Table. 1 Blockchain typical algorithm which are Proof of Work and Practical Byzantine Fault Tolerance[6] compare which part is better

	PoW	PBFT
Fault tolerance	Over 1 computer	Under 1/3 computers
Decision	CPU calculation amount	Majority
Authority	Low electricity bill has more power	Every server equal
Participation condition	Everyone can take part in	Only trusted servers participate
Authentication key	The public encryption key	The private encryption key

2.2. BitAV: Fast Anti-Malware by Distributed Blockchain Consensus and Feedforward Scanning

Charles Noyes는 2016년 1월에 blockchain기법을 이용하여 기존에 나와 있는 방법보다 빠르게 Anti-Malware[7]를 전파하는 방법을 제안하였다. 본 논문에 의하면 블록체인의 특징인 탈 중앙 화 시스템을 이용하여 사용자들에게 보다 빠르게 Anti-Malware를 전파할 수 있다고 한다. 제안 기법은 다음과 같다. 본 논문에서 제안하는 BitAV는 블록을 전송(transaction)할 때 tx field를 보면 2가지 정보로 나눠서 정의하고 이는 identifier field와 invalidation field로 구분한다. Identifier field에는 여태 chain에 정의되지 않았던 새로운 malware identifiers를 정의할 수 있다. 각 field에서는 확실하게 검증되고 참여한 노드가 합의점을 이루어야한다. 합의점을 이루는 방법은 다음과 같다.

$$\sum Trust\,of\,Submitter - \sum Trust\,of\,Invalidators$$

(1) 믿을 만한 전송자의 합이 식별되지 않은 사람이 보낸 합보다 크면 믿을 수 있다고 판단되어 합의점을 이루게 된다. 만약 저 합보다 작다면 전송 자는 뺄셈 결과와 동일한 수준으로 신뢰를 잃게 된다. 찬성한 노드 역시 신뢰를 잃게 된다. 이때 유권자에 대한 처벌을 내리는 것이 '공정한'것처럼 보이지 않을 수 있지만, 많은 신뢰를 얻은 악의적 노드가 반대자의 제출을 무효화하여 네트워크를 장악하지 못 하게 하는 것이 필요하다. 그 결과 체인에 구성 되어 있는 모든 노드를 scanning하는데 기존의 업체에서 제공하는 Anti-Malware software보다 1400% 향상 된 속도를 제공한다.

2.3. Decentralized firewall for malware detection

해당 논문[8]에서 제안하는 기법은 블록체인 기술을 활용하여 malware를 탐색하는 기법으로 체인으로 등록된 노드들을 사용하여 들어오는 모든 파일을 탐색하는 작업이다. 노드가 네트워크에 추가 될 때 마다 중앙 서버는 해당 노드에게 malware가 탐지 가능한 소프트웨어를 제공하고, 노드는 해당 소프트웨어를 이용하여 탐지한 결과를 특정 숫자로 나타낸다. 특정 숫자는 악의적일 가능성을 말하며, 각 노드마다 신뢰할 수 있는 가중치가 부여되어 해당 가중치와 합하여 탐지 결과를 반환한다. 해서, 네트워크에서 발생하는 모든 event(외부 파일 download, update 등) 작업이 전송을 통해 블록체인에 저장된다. 각 노드에서 발생하는 모든 event를 체인에 묶여있는 모든 노드가 자동으로 malware인지 아닌지 탐색해 줌으로써 알려지지 않은 악의적인 공격도 막을 수 있다. 따라서 본 논문과 같이 블록체인 기술을 활용한다면 다양한 규모의 네트워크에 대한 완벽한 보안을 제공할 수 있다.

Ⅲ. 제안 기법

이전 장에서 확인해 보았듯이 private 블록체인은 채굴에 신뢰 된 노드만 참여할 수 있는 반면 public 블록체인의 경우 채굴에 참여하는데 아무런 규제, 규약 없이 누구든 다 참여할 수 있다. 그러나 누군가 악의적 의도로 채굴에 참여한 후 nonce를 발견해 그림 2와 같이 악성코드를 배포한다면, 체인으로 구성 된 이후에는 각 노드들에 대해 별 다른 보안 적 점검이 없이 노드에서 전

파한 데이터를 최신화하기 때문에 사용자들의 컴퓨터에 악성 코드가 설치되게 되고 해커의 악의적 의도에 의해 체인에 연결된 노드들은 큰 타격을 입을 것이다.

이를 위한 해결 방안은 다음과 같다. 최초의 블록체인이 체인을 형성할 때는 체인에서 요구하고 전달하고자 하는 데이터가 있을 것이다. 이를 α, β, ɣ라고 정의하자. 이때 체인의 최초 설립자가 지정한 데이터 값 α, β, ɣ 이외에 δ를 포함하여 다른 노드로 전송을 하고자 할 때 해당 데이터에 연결된 모든 노드의 1/3이상의 동의 결과를 받아야 database column에 추가되고, 다음부터는 default 데이터가 α, β, ɣ, δ가 되는 것이다. 이렇게 되면 체인에 포함 된 사용자 들이 새로 추가 된 전송 목록을 확인 할 수 있으며 만약 악의적인 목적이 있다고 판단했을 경우 거부할 수 있는 권리가 생겨, 아무런 제제 없이 모든 데이터를 받아야하는 기존의 방식보다는 보다 보안 적이라고 할 수 있다.

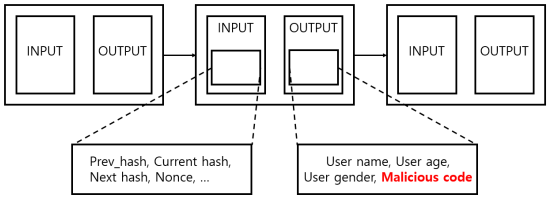

Fig. 2 A transaction that shows malicious purpose with malicious code in transaction

또한 기존의 public 블록체인에서는 아무런 규제 없이 체인에 참여가 가능하다. 체인에 참여한 사용자가 새로운 데이터를 얻어 원장을 최신화 하려고 할 때, nonce만 발견(데이터의 신뢰성 검증)하면 바로 전파할 수 있는 구조이다. 이렇게 되면 악의적 의도를 갖고 있는 해커 또한 너무도 쉽게 악성 데이터를 전파할 수 있다. 이를 방지하고자 AI를 도입하여 보안 단계를 한 단계 업그레이드(upgrade)하고자 한다. 여기서 말하는 AI의 역할은 그림 3과 같다. 익명의 사용자가 사전에 구성 된 체인에 참여하기 위해 참여 의사를 밝힌다면, AI가 사용자의 정보를 자체적으로 확인한다. 우선적으로 확인해야 하는 사용자의 정보는 해당 사람의 MAC 주소를 확인하고 해당 주소가 과거에 악의적인 행동을 한 흔적이 없는지, 한 흔적이 있다면 해당 사용자는 영구적으로 체인에 참여할 수 없도록 블록처리하고 해당 MAC 주소를 데이터베이스(database)에 등록시켜 블랙리스트(blacklist)를 만들어 다음에는 blacklist에 등록 된 사용자 인지 먼저 검색하여 똑같은 사용자가 접속 했을 때 MAC 주소를 검색하는 수고를 줄일 수 있다.

Algorithm 1 Shows AI parts

```
Input: User MAC address
Output:
  IF malicious history = MAC address THEN
  Make blacklist
  ELSE
    IF user has malicious software THEN
      recognized to remove malicious software
      upgrade newest version of OS defender
    ELSE
      IF user does not have security program THEN
        suggest for download security program
      ELSE
        can access
      ENDIF
    ENDIF
  ENDIF
```

Fig. 3 Pseudo code that shows AI parts

다음으로 해당 사용자가 과거에 악의적인 행동을 한 흔적이 없다면, 사용자의 컴퓨터는 안전한 상태인지 점검한다. 블록체인 기술은 중앙 서버가 없는 대신, 기록해야 하는 데이터를 체인에 참여한 모든 사용자의 컴퓨터에 저장하는 방식이다. 체인에 참여한 사용자는 다른 사용자의 정보도 내 컴퓨터에 저장되기 때문에 내 정보뿐만 아니라 모두의 정보를 볼 수 있다. 따라서 사용자의 컴퓨터가 악성코드에 감염 된 흔적이라든지 보안 적으로 취약하면 쉽게 목표물(target)이 될 것이다. 이를 방지하고자 두 가지 방법을 제안한다. 첫 번째는 그림 4와 같다. 본 논문에서 제시하는 AI는 사용자의 컴퓨터에 악성 프로그램이 있는지 검사하고, 악성 프로그램이 있다면 사용자에게 알려 해당 프로그램을 삭제 해야만 체인에 들어올 수 있다고 알린다. 이와 동시에 해당 유형의 악성 프로그램을 데이터베이스에 저장하여 다른 사용자가 체인에 들어오려고 똑같은 절차를 밟을 때 처음보다 단시간에 검색할 수 있도록 한다. 컴퓨터에 악성 프로그램이 있는지 확인하고 이를 지우는 행위는 아주 중요한 행위이다. 블록체인은 개개인의 컴퓨터에 블록체인에 참여한 모든 노드의 정보를 저장하는 기술이다. 그렇기 때문에 내 컴퓨터만 안전하다고 하여 나의 정보가

안전하다고 생각하는 것은 오산이다. 만약 악성 프로그램에 감염 된 컴퓨터가 있을 경우 내 정보뿐만 아니라 다른 사람들의 정보도 해커들에게 유출되는 일이 발생할 수 있다.

두 번째로 체인에 구성되기 위하여 의사를 밝은 사용자의 컴퓨터에 보안 프로그램이 없다면 1차적으로 OS 방화벽 업그레이드를 제안하고 2차적으로 시중에 개발된 보안 프로그램을 제안한다.

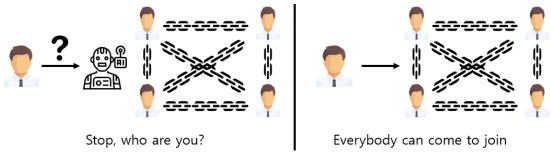

Fig. 4 (Left) Structure of blockchain using AI, (Right) Structure of blockchain

4차 산업혁명 시대가 열리면서 각 기기(device)에서 창출 되는 데이터는 단지 데이터 값만 갖고 있는 수준이 아닌 창출 되는 데이터로부터 사용자의 행동 패턴을 분석해 사용자 정보도 뽑아 낼 수 있다. 따라서 데이터를 단지 정보의 값으로 볼 것이 아니라 누구나 접근해서 활용할 수 없도록 하는 보안적 장치가 필요하다. 사물과 사람이 연결 되어 매일매일 쏟아져 나오는 사물인터넷 기술에 연쇄적으로 발생하는 데이터를 체인형식으로 연결하는 블록체인 기술을 많은 사람들이 언급하고 있다. 하지만 현재의 블록체인 기술은 다른 시스템에 적용하기엔 취약점이 존재하여 해당 취약점을 해결하기 위해 AI를 활용하는 방법을 제안한다.

Ⅳ. 성능 평가

본장에서는 2장에서 다룬 관련 연구 동향에서 사용한 기법인 BitAV[7], Decentralized firewall for malware detection[8]과 3장에서 다뤘던 제안 기법인 AI를 활용한 블록체인 그리고 public 블록체인을 비교 분석 해보겠다. 기존의 블록체인은 블록체인에 참여하는 노드로 구성되기 위해서는 아무 규제 조건 없이 누구나 참여할 수 있는 반면, AI를 활용한 블록체인은 블록체인에 참여하기 위해서는 노드의 신뢰성에 대하여 먼저 검증이 이루어진 이후 신뢰할 수 있다면 블록체인 노드로 참여할 수 있다. 이는 체인에 참여하기 전부터 사용자의 고유 컴퓨터 MAC 주소 값을 본 논문에서 제안하는 AI 기술을 활용해 과거에 악의적인 행동을 한 이력은 없는지 조회하고 신뢰할 수 있음을 검증 받은 후에 체인으로 구성될 수 있어, 참여한 노드들에 대해 신뢰할 수 있다. 반면 기존의 public 블록체인, BitAV, Decentralized firewall for malware detection에서는 체인에 참여하려는 사용자가 누구든 아무런 조건 및 검증 없이 체인에 참여할 수 있기 때문에 집으로 따지면 대문이 없는 것과 마찬가지이므로 1차적인 보안 장치가 없는 것이 된다. 따라서 참여한 노드들에 대해 신뢰성을 가질 수 없다. 신뢰할 수 있는 사용자가 만든 데이터와 신뢰할 수 없는 사용자가 만든 데이터에 대한 신뢰성 역시 마찬가지일 것이다. 물론 신뢰할 수 있는 사용자가 만든 데이터라고 해도 100% 신뢰할 수 있는 것은 아니다. 따라서 전파하기 전에 AI가 해당 데이터에 악성 코드는 없는지, 기존의 데이터베이스 column에서 갖고 있지 않은 데이터가 추가되는지 2차적으로 검증하고 진행하기 때문에 신뢰성을 더욱 상승시킨다. 그러므로 AI를 활용한 블록체인의 노드에서 나온 데이터는 높은 확률로 신뢰할 수 있으며, public 블록체인에서는 익명의 노드로부터 나온 데이터이기 때문에 낮은 신뢰성을 보인다.

표 2와 같이 CPU 사용량을 보면 AI를 활용한 블록체인이 기존의 public 블록체인에 비해 상대적으로 높을 것이다. 그 이유는 기존의 public 블록체인보다 전파 하는데 까지 거쳐야할 단계가 많기 때문이다. 그러나 블록체인에서 나온 데이터로부터 시스템이 돌아가는 상황이라면, 신뢰할 수 없는 곳으로부터 나온 데이터보단 상대적으로 느리고 CPU를 많이 사용하지만 신뢰할 수 있는 곳으로부터 나온 데이터를 사용하는 것이 사용자를 위해서 더 나은 결정이다.

Table. 2 Compare chart of AI blockchain and public blockchain

	AI block chain	Public block chain	BitAV [7]	Decentralized firewall for malware detection[8]
Participation condition	Only trusted nodes that do not have malicious software	Everybody can join	Everybody can join	Everybody can join

	AI block chain	Public block chain	BitAV [7]	Decentralized firewall for malware detection[8]
Node reliability	HIGH	LOW	LOW	LOW
Data reliability	HIGH	LOW	HIGH	HIGH
CPU usage	HIGH	LOW	HIGH	HIGH
Transaction time	Slow	Fast	Slow	Slow

ACKNOWLEDGEMENT

This work was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1C1B5075742) and the MSIT(Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (2014-1-00743) supervised by the IITP (Institute for Information & communications Technology Promotion)

Ⅴ. 결 론

4차 산업혁명 시대가 오면서 한 개의 기기로부터 나온 데이터 하나하나의 가치도 중요하지만 모든 데이터가 모여야 진정한 가치를 창출한다. 블록체인은 한 개의 기기로부터 나온 데이터들을 해시 키(hash key)로 관리하여 체인으로 묶는 미래 산업에 없어서는 안 될 기술[9]로 평가 받고 있다. 그러나 아직까지는 상용화하여 사용하는데 기술적 문제가 존재한다.

본 논문은 앞서 언급한 기술적 문제를 보안하기 위하여 신뢰할 수 없는 사용자를 같은 블록체인 네트워크에 형성하는 것이 아닌 AI를 활용하여 신뢰할 수 있는 사용자만 같은 블록체인 네트워크를 형성하게 만들고자 한다. 악성 프로그램을 검출하는 AI에서 사용자들의 신뢰성을 확보하기 위해 여태까지 검출한 악성 프로그램을 data set을 open source화하여 공개할 예정이며, AI가 하는 일에 대한 코드 역시 open source화 하여 공개할 예정이다.

본 논문에서 제안하는 기술을 사용한다면 안전한 블록체인 네트워크를 형성하고 진보 된 기술을 맞이할 것이라 예상한다. 현재도 블록체인을 이용한 다양한 분야의 플랫폼 개발을 위해 많은 연구([10], [11])가 진행되고 있으며, 아직 블록체인을 적용하지 않은 분야 중에서도 선행 된 연구[12]를 기반으로 블록체인을 적용이 가능할지도 생각해 볼 필요가 있다.

마지막으로 현재보다 발전 된 미래를 만들기 위하여 본 논문에서 살펴보았듯이 많은 연구가 선행 될 필요가 있다고 본다.

References

[1] Bitcoin. Bitcoin: A Peer-to-Peer Electronic Cash System [Internet]. Available: https://bitcoin.org/bitcoin.pdf.

[2] F. Mercaldo, V. Nardone, A. Santone, C. A. Visaggio, “Ransomware steals your phone. formal methods rescue it,” In: *International Conference on Formal Techniques for Distributed Objects, Components, and Systems*. Springer, Cham, pp. 212-221, 2016.

[3] Ethereum. A Next-Generation Smart Contract and Decentralized Application Platform [Internet]. Available: https://github.com/ethereum/wiki/wiki/White-Paper.

[4] Whitepaper Database. RIPPLE (XRP) - WHITEPAPER [Internet]. Available: http://whitepaperdatabase.com/ripple-xrp-whitepaper/.

[5] M. Castro, B. Liskov, “Practical Byzantine fault tolerance,” In: *OSDI*, pp. 173-186, 1999.

[6] A. Yosihalu, A. Manabu, “Consensus Algorithm,” in *Blockchain Structure and Theory*, Wikibook., ch. 8, pp. 109, 2017.

[7] arXiv. Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning [Internet]. Available: https://arxiv.org/pdf/1601.01405.pdf.

[8] arXiv. Decentralised firewall for malware detection [Internet]. Available: https://arxiv.org/pdf/1711.01353.pdf.

[9] K. Christidis, M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” *IEEE Access*, 4, pp. 2292-2303, 2016.

[10] Kyuhwang An, Hwajeong Seo, “Building bicycle management system using Blockchain,” *Journal of the Korea Institute of Information and Communication Engineering*, Korea, vol. 22, no. 8, pp. 1139-1145, Aug. 2018.

[11] Kyuhwang An, Hwajeong Seo, “Donate system development using Blockchain technology,” *Journal of the Korea Institute of Information and Communication Engineering*, Korea, vol. 22, no. 5, pp. 812-817, May 2018.
[12] Jae Yoon Lee, Lahari Kolasani, "Security Based Network for Health Care System," *Asia-pacific Journal of Convergent Research Interchange*, HSST, ISSN : 2508-9080, Vol. 1, No. 1, Mar. 2015.

안규황(Kyu-hwang An)

2018년 2월: 한성대학교 IT응용시스템공학과 공학 학사
2018년 3월~현재: 한성대학교 정보시스템공학과 석사과정
※관심분야 : 블록체인, 블록암호, IoT 보안, Hash 함수

서화정(Hwa-jeong Seo)

2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
※관심분야 : 정보보호, 암호화 구현, IoT