디지털산업정보학회 논문지 제15권 제1호-2019년 3월
https://doi.org/10.17662/ksdim.2019.15.1.077

블록체인 안전성 확보를 위한 거래 검토*

최 희 식**·조 양 현***

Examination of Transaction Secure Safety of Block Chain

Choi Heesik · Cho Yanghyun

〈Abstract〉

Comparative analysis to secure safety of Blockchain Many investors have invested in virtual currency such as bit coins as a new investment due to increased popularity of virtual currency around the world. Also, virtual currency such as bit coin has a security technology and it has been relatively proved. popularity of virtual currency is rising as a new investment alternative because of this reason. This paper focused on the block chain's transparency and security of distributed ledger technology, which is relatively safe without third party's intervention. Many governments and companies around the world are developing and working on block chain technological development to introduce due to these reasons However, there are some suggestion that block chain has minor risks to its security. In this paper, it will examine security vulnerabilities from importance of security of Blockchain which relates to transactions of Bitcoin which stored by governments and companies around the world. This paper will propose measure which will improve safety and efficiency of Blockchain technology such as the existing Blockchain method, Blockchain proposal, traceability and awareness about hacking.

Key Words : Virtual Currency, Block Chain, Crypto Currency, Block Chain Secure, Security Treatment

Ⅰ. 서론

최근 블록체인은 4차 산업혁명의 핵심 기술로 떠오르고 있다. 블록체인을 사용하는 가장 대표적인 암호화폐인 비트코인은 이미 많은 관심을 받았고 그중 블록체인에 대한 안정성과 투명성으로 이슈화 되었으므로 블록체인의 관심은 더욱 커지게 되었다[1].

현재 전 세계의 많은 국가의 은행을 포함한 금융업계는 블록체인을 도입하고자 연구하고 있다. 또한, 많은 정부와 기업들 또한 블록체인을 금융 거래 목적 외에도 블록체인의 보안성에 금융 거래에 중요한 요소로 작용하므로 차세대 보안 기술로 도입 예정을 고려하고 있다. 하지만 일부에서는 블록체인의 보안성이 문제가 있고 완벽하지 않다는 의견이 불분명하여 블록체인 기술 도입에 대한 우려의 목소리도 높다.

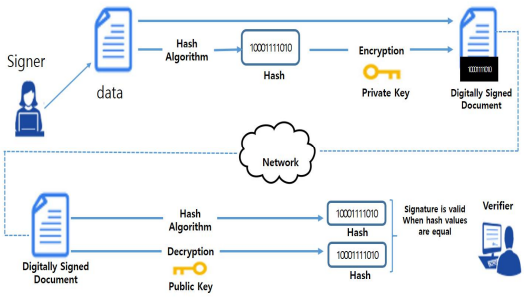
* 본 연구는 2019년도 한국 연구재단 이공학 개인기초연구지원비(No. 2017R1D1A1B03030759)로 수행됨.
** 경민대학교 IT경영과 외래교수
*** 삼육대학교 컴퓨터 · 메카트로닉스공학부 교수(교신저자)

본 논문에서는 암호화폐 블록체인 기술이 과연 보안성에 따른 안정성에 문제가 있는지에 대한 검토를 통해 분석하고자하며 다음과 같이 논문 구성을 하였다. 2장 본문에서는 암호화폐 기술의 하나인 블록체인의 정의 및 블록체인 도입 사례에 대해서 살펴보고 3장에서는 가상화폐 거래에 따른 안정성을 저해하는 블록체인 보안 위협에 대한 취약점이 무엇인지에 대해서 살펴보고 4장에서는 블록체인 안전성에 대한 문제점이 무엇인지를 검토하여 보다 안전한 블록체인에 대한 방안을 제시한 후, 5장에서 결론으로 마무리하고자 한다.

II. 본문

2.1 블록체인 정의

블록체인은 암호화폐(cryptocurrency)의 모든 거래 정보를 담고 있는 거대한 장부로 공개된 디지털 장부로 일컫는다[2]. 블록체인에서 서로 다른 사용자들의 거래 및 데이터를 블록이라고 하며 블록은 순차적, 공개적으로 체인에 추가되어 진다. 블록체인은 거래가 진행될 경우 새로운 정보를 지속해서 추가할 수 있지만 이미 블록에 저장된 블록체인은 거래 장부 변경이 불가능하다. 블록체인은 기존의 중앙 화된 기술과 다르게 데이터가 중앙 서버가 아닌 네트워크에 참여한 다수의 컴퓨터에 <그림1>과 같이 안전하게 저장되게 된다[3]. 거래 데이터가 네트워크에 추가될 때마다 네트워크에 참여한 모든 컴퓨터가 참가한 사용자들의 동의를 기반으로 거래가 이루어지므로 그림에서 살펴본 바와 같이 매우 안전하며, 또한, 검증된 거래 데이터만이 통과되어 추가될 경우 각각 컴퓨터에 저장된 체인을 실시간으로 동기화하게 된다[4]. 블록체인(Blockchain)은 크게 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain), 컨소시엄 블록체인(Consortium Blockchain)으로 구분되며 각 블록체인의 특징적인 요소 및 응용에 대해서는 <표 1>에서 살펴보도록 한다[5].



<그림 1> 블록체인 거래 방식 [6]

2.2 퍼블릭 블록체인 (Public Blockchain)

퍼블릭 블록체인은 공개형 블록체인으로 많이 알려져 있으며 합의(Consensus) 방식을 기반으로 네트워크상의 모든 사람들에게 공유가 자유로운 것이 특징이다. 퍼블릭 블록체인은 통제하는 중앙 관리자 없이 네트워크 환경에서 사용자가 직. 간접적인 암호화폐를 통한 안전한 거래를 제공[7]하며, 누구나 자유롭게 네트워크에 참여할 수 있고 읽기, 쓰기, 검증 권한도 가지게 된다. 이런 특징으로 퍼블릭 블록체인은 익명성으로 자유롭게 이용되므로 거래에 따른 추적이나 규제가 쉽지 않아서 해커로 부터 표적이 되어 네트워크 공격이나 해킹을 당할 수 있는 위험요소가 존재할 수 있다. 또한, 퍼블릭 블록체인은 중앙 관리자가 없기 때문에 누구나가 운영의 주체가 될 수 있으므로 체인에 추가될 거래 데이터를 검증하기 위한 분산 알고리즘을 사용하게 된다. 분산 알고리즘은 신뢰를 위해 작업증명(POW, Proof of Work), 지분증명(POS, Proof of Stake) 등 내부 화폐를 필요로 하는데 이것이 투명성을 보장하는 역할이 된다. 대표적인 퍼블릭 블록체인으로는 잘 알려진 비트코인(Bitcoin)과

이더리움(Ethereum) 등이 있다[8].

- 장점: 탈 중앙 관리자로부터 모든 사용자가 거래 내용을 볼 수 있는 투명성
- 단점: 확실한 데이터를 보장해야 하는 금융권에서는 사실상 적용이 어려움

2.3 프라이빗 블록체인 (Private Blockchain)

프라이빗 블록체인은 읽기, 쓰기, 검증 권한을 중앙 관리자가 독자적으로 관리하므로 네트워크상에 들어가는 이용자들은 다소 제한이 따른다. 즉, 프라이빗 블록체인에 참여하기 위해서 중앙 관리자의 승인이 반드시 필요하며 중앙 관리자는 참여자를 필요에 따라 추가, 삭제할 수 있는 권한도 가진다. 프라이빗 블록체인 내의 허가된 그룹이나 사용자들끼리 거래 데이터를 내부에서 검증할 수 있게 되어있다.

프라이빗 블록체인은 퍼블릭 블록체인보다 처리해야 하는 데이터의 양이 적음으로 처리 비용도 적고 데이터를 처리하는 속도도 빠른 장점이 있다.

또한, 네트워크 이용이 자체적으로 제한되어 관리되므로 외부의 해커나 악의적인 참여자가 프라이빗 블록체인(Private Blockchain) 네트워크에 들어가는 것은 사실상 불가능하다. 그런 이유로 프라이빗 블록체인은 해킹 피해에 대해서는 비교적 안전하다고 볼 수 있다. 보안성이 확실하다는 보장 이유로 프라이빗 블록체인 기술은 많은 글로벌 기업들이 자사의 거래 시스템에 블록체인의 보안 기술과 효율성, 신뢰성, 안정성을 높이기 위해 블록체인 도입에 관심이 높다. 프라이빗 블록체인으로는 MONAX, Multichain, Linux 펀딩, R3CEV등이 있다[8].

- 장점: 바른 거래 처리 속도와 향상된 보안성
- 단점: 중앙 관리자의 권력과 힘이 작용하여 탈중앙화 네트워크 거래와는 다소 차이가 있음

2.3 컨소시엄 블록체인 (Consortium Blockchain)

컨소시엄 블록체인은 퍼블릭 블록체인이나 프라이빗 블록체인과는 달리 여러 기관들이 그룹을 이뤄 네트워크에 참여하는 블록체인 기술로 중앙 관리자는 존재하지만 하나의 중앙 관리자가 아닌 다수의 관리자가 존재하는 개념이다. 즉, 컨소시엄 블록체인은 다수의 기관 또는 기업이 하나의 그룹을 이루어 블록체인 네트워크 구성을 만들어 네트워크에 참여할 수 있다는 것이 특징이다.

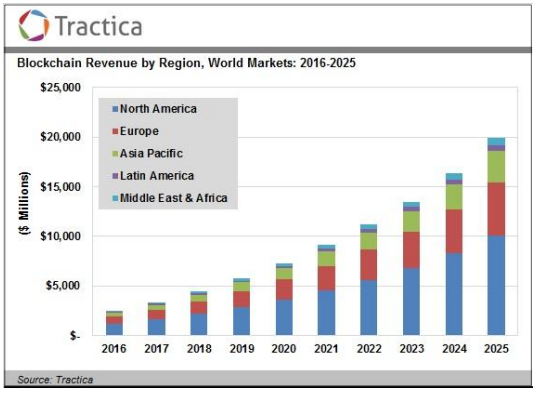
컨소시엄 블록체인 역시 퍼블릭 블록체인보다 처리해야 하는 데이터가 적어 처리하는 속도는 빠르지만 비용 규모는 낮아서 효율성이 높다는 게 장점이다. 컨소시엄 블록체인으로는 R3. EWF등이 있다[9].

<표 1> 블록체인 유형별 특징 [10]

	퍼블릭 블록체인	프라이빗/컨소시엄 블록체인
접근 권한	읽기/쓰기 누구나 가능	읽기/쓰기 허가가 필요
속도	느림(7~20 TPS)	빠름(1,000 TPS+)
검증 및 보안	작업증명(Proof of Work) 지분증명(Proof of Stake) 다른 합의 방식 (Consensus Mechanisms)	사전 승인된 참가자
비용 발생	비용이 많이 듦	비용이 적게 듦
탈 중앙관리자	제약 없음	제약 있음
신원	익명	실명

2.4 블록체인 활용 분야

현재 블록체인은 다양한 분야에서 활용되고 있거나 활용되기 위해 개발 중에 있다. 트랙티카(Tractica)의 조사된 보고 자료에 의하면 2016년에 블록체인으로 인한 발생 수익이 25억 달러 정도로 밝혔으며 2025년에는 200억 달러 정도의 예상수익이 발생하리라고 기대하고 있다. <그림 2>는 트랙티카가 예측한 블록체인에서 나오는 연도별 수익 성장 분포이다.



<그림 2> 블록체인 수익 성장 분포 [11]

다음은 블록체인이 활용되고 있는 다양한 주요 분야들에 대해서 살펴본다.

가. 금융 분야

금융 분야는 가장 널리 블록체인 기술을 활용하고 있는 대표적인 사례로 볼 수 있다. 최근에는 많은 은행들이 블록체인 기술을 이미 도입하였거나 또는 도입 추진을 준비하고 있다. 영국에 본사를 둔 글로벌 은행 기업인 바클리스 은행의 활용 사례이다.

바클리스 은행은 작년에 블록체인의 보안성 및 투명성 기술 측면을 자사의 거래 방식에 구현하였다. 바클리스 은행은 오르누아(Ornua)와 세이셸 트레이딩 컴퍼니(Seychelles Trading Company)간에 블록체인 방식의 신용 거래를 최초로 발표하였으며 이 거래 문서는 최초로 블록체인 네트워크에서 암호화되고 관리된 거래문서가 되었다. 바클리스 은행에서는 도입된 블록체인 기술을 이용하여 분산된 거래 원장을 사용하여 외부적으로 문서를 저장하여 보냈을 때 은행의 입장에서는 거래 과정에서 안정성 확보로 상당한 시간과 경비를 절감할 수 있게 되었다. 바클리스 은행은 이 거래를 통하여 상당한 이익과 경쟁력을 확보할 수 있었으며 다른 금융 기업들도 블록체인 기술 도입에 더욱 관심을 가질 수 있는 역할을 제공하였다.

금융 업계의 관심이 커지면서 회계 및 컨설팅 기업인 딜로이트(Deloitte)는 글로벌 차원의 블록체인 기술 구현에 대한 주요 자문 원칙 설명과 정부 및 법률 기관에서의 매크로 구현 및 사이버 보안 통제에 대한 정보가 포함된 보고서를 최근에 발간하였다.

컨설팅 기업인 액센츄어(Accenture) 역시 금융 산업이 데이터를 저장하고 처리하기 위해 블록체인 기술을 도입할 경우 100억 달러 정도를 절감할 수 있다고 예측하였다[12].

나. 투표와 선거

블록체인 기술을 선거 투표에 구현하게 되면 각 시민의 투표는 암호화 처리되어 추적할 수도 있도록 되어 있다. 이때 개인키 생성하기 위해, 난수 발생기 256개 랜덤 값의 쌍을 만든 후, 키 하나당 256비트의 길이를 갖게 된다. 또한, 해시함수를 통해 생성된 512개의 해시 값들이 사용자의 공개키가 되며, 전달받은 사용자의 인증을 승인받게 된다[13]. 블록체인 기술이 구현된 투표 시스템은 분산 원장 방식으로 인해 관리되기에 중앙 관리자에 의해 결과가 처리되지 않아 투표의 조작 위험 요소를 최소화할 수 있어 투명성이 보장된다[12].

다. 스마트 계약 (Smart Contract)

스마트 계약은 프로그램 코드로 작성되고 특정 블록체인 거래에 포함된 계약을 일컫는다. 이 프로그램 코드에는 조건이 충족될 경우 자동으로 실행하게 될 모든 규칙, 조건, 만료일과 같은 계약이행에 필요한 정보들이 포함되어 있다. 스마트 계약은 주관적일 수 있고 사법 해석 차이가 있을 수 있는 기존 정통방식의 계약들과는 다르게 프로그래밍 언어로 만들어져

있기에 더 객관적 일 수 있다[14].

기존 소셜 플랫폼 상의 계약은 네트워크 특성상 위·변조가 일어날 수 있지만 스마트 계약은 암호화된 원장에 저장[16]되며, 블록체인의 탈중앙화로 인해 중앙 관리자 임의로 데이터를 수정하거나 위조할 수 없으며 스마트 계약과 스마트 계약의 히스토리가 네트워크에 영구적으로 기록되기에 외부의 조작을 방지할 수 있다. 스마트 계약 역시 조건이 충족될 때 자동으로 실행되기에 중개인을 거치지 않고도 계약 및 거래를 할 수 있으며 투명성이 보장된다. 또한, 중개인을 거치지 않는다는 이점은 계약하는 과정의 시간이 단축될 뿐만 아니라 편의성과 신뢰성을 증가시킬 수 있다.

라. 의료 분야

블록체인 기술은 의료 분야에서도 활용할 수 있는데 각 환자의 의료 기록에 대한 정보들을 쉽고 신속하게 관리할 수 있다. 또한, 블록체인의 암호화를 통하여 환자의 사적이거나 민감한 개인 정보의 보안성을 높일 수 있다. 또한, 블록체인 기술을 이용하여 의약품의 분배, 규정 준수, 관리 및 감독하는 데에도 충분히 활용될 수 있다[12].

Ⅲ. 블록체인 보안 위협 검토

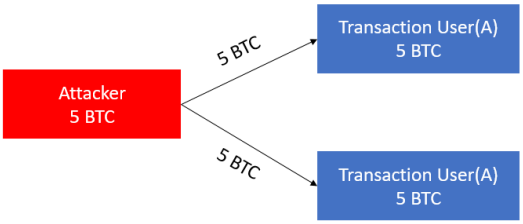
블록체인 기술은 근본적으로 안전한 거래 기술이다. 일반 사용자들에게는 안전하다고만 여겨지고 있지만 보안상의 문제점이 유추되고 있으므로 3장에서는 기존 블록체인이 안고 있는 성능 및 저장과 관련된 확장성 및 보안을 위협하는 쟁점에 대해서 검토해 보도록 한다.

3.1 확장성 문제

블록체인 기반 기술의 인기가 높아짐에 따라 저장장치에 대한 문제, 분산 원장 크기에 대한 문제, 처리량에 대한 문제가 더욱더 심각해지고 있으면서 거래 원장에 대한 동기화하는데 있어서도 심한 병목현상도 두드러질 수 있다. 이를 해결하기 위해 채굴 난이도를 낮추고 블록 생성 속도를 증가시키게 되면 보안에 대한 레벨이 낮아지므로 보안의 문제점이 초래될 수 있다. 반면에 처리 속도를 높이기 위해 블록 크기를 커지게 하면 속도가 저하되는 것과 동시에 원장의 크기가 증가하므로 비용 문제가 발생할 수 있다[15].

3.2 51%어택과 더블 스펜딩(Double Spending) 거래

51%어택은 블록체인 네트워크의 과반수가 넘는 지분을 소유하거나 지지를 받는 사용자가 블록체인과 블록체인의 데이터를 지배하는 행위를 일컫는다. 특히, 더블 스펜딩(Double Spending)은 <그림 3>처럼 동일한 암호 화폐가 두 번 이상 지출되는 것을 의미하는데, 블록체인에서 두 개 이상의 거래가 충돌할 경우 다수의 참여자가 선택한 거래를 받아들이고 그 외의 거래들을 취소시키게 된다. 51%어택과 더블 스펜딩을 조합할 경우 이와 같은 블록체인의 특성을 악용하는 것이 가능해지는 문제점이 속출할 수 있다[17].



<그림 3> 더블 스펜딩 어택 공격

3.3 검증되지 않은 인증 코드

블록체인 기술에 대한 보안 인증 기술은 현재에도 꾸준히 개발되고 있지만 아직까지는 실험적인 단계이므로 다소 검증되지 않은 코드에 대한 문제가 유발될 수 있다. 즉, 블록체인 기술이 너무 새로운 기술이다 보니 구현하는데 있어서 검증되지 않는 오류가 발생하게 되면 보안에 쉽게 노출되어 취약점이 악용될 수 있다는 것이다. 이런 가운데 보안 적으로 확실히 검증되지 않은 코드가 블록체인 기술 개발에 사용될 경우 큰 보안 위협으로 공격을 받게 된다. 보안과 관련된 이더리움 피해의 한 사례를 살펴보자. 이더리움의 개발자들은 The DAO(탈중앙화 자율 조직, Decentralized Autonomous Organization)라는 시스템을 개발하였다. 개발자들은 크라우드 펀딩을 통하여 1억 5000만 달러를 모았다. 크라우드 펀딩을 모으던 중 이더리움 커뮤니티의 많은 사용자들이 The DAO의 코드에 보안 취약점이 있다고 의견을 제시하였다. The DAO 개발자는 DAO 펀드에는 블록체인 기술은 검증되어 안전하므로 네트워킹 보안 위협에 크게 되지 않을 거라고 주장하였다. 하지만 결국 The DAO는 해커들에 의해 5500만 달러 정도의 손실을 입는 해킹 피해를 입게 되었다[18].

3.4 표준과 규제의 부족

경제 잡지인 포브스는 블록체인의 보안 문제점으로서 표준과 규제의 부족을 꼽았다. 표준 규약이 부족하다는 것은 블록체인 개발자가 다른 사람들의 실수로부터 혜택을 쉽게 받을 수 없다는 것을 의미한다. 각 회사, 각 컨소시움이 각자 다른 표준 및 규제를 하고 있으면 비표준 기술로 인한 보안 위험이 발생할 수도 있다. 예를 들어, 필요 상황이 발생하여 체인들을 통합해야 할 경우 블록체인 기술에 대한 비표준 및 규제가 미 확보된 상태에서는 다양한 새로운 문제점과 블록체인에 대한 보안 위험성이 초래될 상황이 발생할 수도 있다[18].

3.5 블록체인 사용자 공격

블록체인 기술을 구축하는 데 필요한 툴들과 주변 기술을 노리는 예도 있다. 블록체인과 연동되는 소프트웨어나 웹 애플리케이션들이 주요 표적이다. 블록체인을 직접 기술적으로 노리는 것보다 성공률이 높다. 이는 사용자들이 블록체인 기술과 그 위험성에 대해 제대로 이해하고 있지 못하기 때문에 생기는 약점을 노리는 공격이라고 분류할 수 있다. 사용하는 해킹기술로 멀웨어, 익스플로잇 등이 다양하게 사용되고 있으며, 기업과 개인, 기관 등 표적을 가리지 않고 무차별하게 공격을 가하고 있다. 공격자는 공격을 통해 웹 페이지를 가로채거나 해킹한 수신자로 가장해 많은 사람의 거래를 가로채어 금전적 이득을 취하게 된다[19].

Ⅳ 보안 위협 검토 방안

블록체인 거래는 원래 익명성을 가지고 있으므로 자금 세탁과 관련지어 충분히 비정상 거래를 통해 사기성 거래가 시도될 수 있다. 이러한 거래에 대해서는 탐지가 쉽지 않으며, 업무 특성상 수행된 거래에 대해서는 취소도 되지 않으므로 복구 또한 쉽지 않다. 4장에서는 3장에서 검토된 블록체인에 대한 안정성을 위협하고 거래의 투명성을 조장할 수 있는 블록체인 보안 위협에 대한 안전한 제시 방안을 마련한다.

4.1 확장성 방안

블록체인은 금융, 물류, 유통, 의료, 사물인터넷 분야 등 다양한 분야에서 블록체인 기술을 사용하고 있지만 최근에는 거래 처리량에 따른 확장성 문제점으

로 인한 블록체인 기술 효율성에 기대가 못 미친다는 문제점이 제기되고 있다. 블록체인 확장성에 대한 문제는 거래 건수가 늘어남에 따라 데이터 처리량, 저장 능력, 처리 속도에 대한 성능 저하가 요인이므로 무엇보다 연산 능력에 따른 처리 속도가 빠른 새로운 블록체인 연산 기술이 절대적으로 필요하다. 블록체인에 대한 처리 능력을 향상시키고 대규모 거래 처리 서비스를 원활히 제공하기 위해 블록 구조에 대한 알고리즘을 블록 단위로 수정해서 블록 크기를 늘려서 속도를 늘리는 방법을 제안한다. 또한, 거래 처리량에 따라 처리되는 트랙잭션 알고리즘을 가변적으로 유동성 있게 처리하여 속도 및 안정성에 따른 원활한 거래 처리 반영되도록 적극 권장한다.

4.2 블록체인 거래 방식

블록체인 거래에 따른 보안 요소는 비교적 블록 식별자 역할을 하는 SHA-256 해시 함수를 2번 적용하여 해시 값을 생성하게 되므로 암호 부분에 대해서는 비교적 안정적이다 볼 수 있다. 뿐만 아니라 암호화폐 거래에 따른 거래 정보의 무결성을 보장하기 위해 블록체인 거래 정보의 해시 값을 공개키 기반 암호화를 통해 거래 내역을 입증하여 증명하고 있다. 하지만 위에서 살펴본 대로 비트코인 거래 시 동일한 암호 화폐가 전산 조작을 통해 동시에 이중 지출되는 것은 문제적 요인이 발생하게 된다. 흔히, 우리가 P2P와 같은 자료 공유에 대한 불신적인 개념과 불법적인 자료 유통으로 많이 알려져 있지만 블록체인은 양방향 동시간대에 이루어지므로 간혹 이중 지출과 같은 거래 요인이 발생할 수도 있게 되는 것이다. 이러한 불법적인 편법 거래를 막기 위해 노드와 노드가 양방향으로 전송되는 Duplex 전송 방식을 반이중방식으로 전송되는 Half Duplex 방식으로 변경되어 불법으로 진행되는 블록체인에서 두 개 이상의 거래가 충돌할 경우 거래 내역을 포함한 블록 정보가 변경되지 않았다는 투명한 거래를 증명하는 방안을 제시한다.

4.3 인증 과정에서 인적 요소 제거

인증 시 사용되는 보통 거래 인증 방식과는 다르게 블록체인 인증은 시스템 인증과정에서 블록체인 기술을 도입하게 되면 기업들은 암호를 요구하지 않고도 장치와 사용자를 인증할 수 있게 된다. 이렇게 된다면 인증 과정에서 사람의 개입이 없어지기에 잠재적인 공격 요소가 현저히 줄어들 수 있다. 현 인증 방식은 중앙 집중형 설계와 간단한 로그인 시스템으로 진행되었기에 기존 보안체계에서는 큰 약점으로 지정되었다. 기업에서는 현 시스템의 보안을 강화하기 많은 돈을 투자하여 보안 시스템을 도입하더라도 직원이나 고객이 공격당하기 쉬운 암호를 사용하게 된다면 보안 시스템은 무용지물이 되기 십상이다. 그런 이유로 장치 및 사용자 인증 보안 시스템을 강화하기 위해 새로운 거래 보안 기술인 블록체인의 분산 공개 시스템을 도입하는 방안을 제시한다. 보안 시스템의 역할은 각 장치에 암호 대신 특정 SSL 인증서를 제공하며 이 인증서 데이터의 관리는 블록체인이 수행하도록 되어 있으며 인증서 데이터 관리를 블록체인이 수행할 경우 공격자가 데이터를 임의로 수정하거나 위조할 수 없게 되어있어 인증 보안 시스템의 보다 안정성이 확보될 수 있을 것으로 예측된다.

4.4 탈중앙화 보관소

블록체인의 사용자는 네트워크에 있는 데이터를 관리할 수 있으며 체인이 붕괴하는 것을 방지할 수 있어야 한다. 즉, 데이터의 소유자가 아닌 공격자가 임의로 블록 변경을 시도하게 되면 전체 시스템이 모든 블록의 변경 유무를 검사하여 변경된 블록의 이상 유무가 발견된다면 블록이 위조된 것으로 인식되어 체인에서 제외되도록 블록체인에 대한 위협적 신호

와 함께 저장 장치에 대한 거래 중지가 작동되어야 한다. 블록체인 거래 기술은 저장 위치 및 중앙 권한이 없는 방식으로 설계되었기에 네트워크에 속한 모든 사용자들은 데이터가 함부로 수정, 삭제 및 위조되는 것을 방지하도록 되어야 하며 다른 사람이 데이터에 대한 조회가 이루어지지 않도록 시스템에 대한 권한도 재검토되어야 한다.

4.5 국제적 표준안 개발 노력

블록체인 관련 국제적 표준안과 규제 법령안에 대한 대책마련 미비로 인해 국내의 경우 무역 거래 시 해당 국가에서 거래 중지로 인한 손해를 입게 되었다. 이에 손해 배상을 소송하는 법적 분쟁에 대한 국제 형사법이 특별히 법제도화 되어있지 않았으므로 분쟁으로 인한 시간낭비와 손해를 감수할 수밖에 없다. 또한, 블록체인 거래 업무에 필요한 암호 보안 적용 오류와 거래 지연으로 인한 피해 감소를 최소화하는 표준안 방안도 반드시 필요하다. 블록체인 기술은 금융, 교통, ICT, 건설, 교육, 병원 등 전 분야에 걸쳐 사용하기 때문에 가급적 리스크를 줄이고 거래 분산원장이 지정된 표준 시간에 결과가 처리될 수 있도록 하는 표준안 명시도 중요하다. 아울러 늘어나는 거래량으로 발생하는 손해 등에 대한 언급과 투기 조장을 막는 익명성 거래량 등에 대한 일일 사용 거래 건수도 조정이 필요할 때라고 본다.

4.6 거래 투명성 제공

퍼블릭 블록체인 및 프라이빗 블록체인에 추가되는 모든 거래는 거래별로 타임스탬프가 찍히고 디지털로 서명되도록 되어있다. 즉, 네트워크에 속한 사용자 및 기업은 모든 거래에 대해 특정 기간에 대한 거래를 추적할 수 있으며 해당 공개 정보를 통해 블록체인에서 해당 당사자를 찾는 것도 당연히 가능하다. 블록체인에 새로운 거래가 추가될 때마다 블록체인의 현재 상태가 색깔별로 또는 버튼을 표시하여 추가되는 거래마다 기존 상태와 차별되어 기록되도록 구분하여 보존하는 것이 투명성을 강화될 것으로 본다. 또한, 거래 조장에 관한 해킹과 관련된 불안정한 거래에 대해서 제시한 방안을 이용하여 적용할 경우, 불공정 거래에 대한 추적이 가능하며 이는 블록체인의 거래 보안성과 투명성을 동시에 확보할 수 있으므로 사용자와 기관의 입장에서 안전한 거래 데이터 확보로 처리된 데이터가 변조되지 않았음을 인정할 수 있는 보증도 확보될 수 있는 증거 자료를 만드는 역할을 하게 된다.

<표 2> 블록체인 적용 검토

구분	기존 블록체인 거래방식	제안 블록체인 거래방식
확장성	속도, 처리, 성능 저하	블록 구조의 크기를 수정하여 가변적 거래 처리로 성능 개선
해킹 위협	무조건 안전하다고 인식한 무방비 상태 거래	암호 알고리즘 적용된 블록체인 인지 및 경각심 확인
표준안	법제도화 표준 미비	국내/국제적 표준화 기술 개발 및 방안 법제도화로 안정적인 거래 확산
투명성	투명성 조장	투명성 강화에 따른 기존 거래와 추가된 거래를 현실성 있게 색깔 등으로 구분하여 추적 경로를 확보

4.7 사용자 공격 회피

사용자 공격은 대부분의 기관 및 일반 사용자들이 블록체인 기술에 대한 안정성만 믿고 그 위험성을 제대로 인지하지 못하기 때문에 공격자들이 이에 대한 약점을 노리는 공격으로 볼 수 있다. 가상화폐에 대한 투자 지식만 챙길 것이 아니라 무엇보다 소중한 내 재산을 보호하기 위해 블록체인에 대한 위험성과 안정성을 저해하는 문제성이 있는지에 대해 사전에

인지할 필요성이 있다. 보다 안전하게 블록체인 공격으로부터 보호하기 위해서는 우선적으로 암호 알고리즘 구현이 안정성으로 검증된 확실한 프로그램 접근으로 거래 이용을 권고한다. 이러한 사전 노력 없이는 가상화폐와 블록체인의 해킹 피해를 입을 수 있는 위협이 있으므로 블록체인 기술에 대한 무결성 기록에 대한 조작이 없었음을 충분히 확인한 후 이용하는 것이 바람직하다.

Ⅴ. 결론

블록체인은 가상화폐인 비트코인 거래에서 데이터 거래에 따른 보안성 확보와 안전한 운영, 비용 절감에 따른 장점으로 다양한 분야에서 활용되어지고 있다. 본 논문에서 살펴본 대로 블록체인이 다양한 비즈적인 측면에서 보안적인 부분, 안정적인 거래 처리 부분에서 자리를 잡기위해서는 우선적으로 가상화폐 투자자를 위한 블록체인 국제 표준화 개발이 시급하다. 블록체인에 대한 표준화 작업이 개발된다면 데이터의 거래 내용과 관련된 추적성과 투명성, 보안적인 측면, 안정적인 측면을 고려하여 블록체인에 대한 활용도에 따른 경쟁력도 확보될 수 있을 것이다. 하지만 블록체인이 뛰어난 잠재력과 투명한 분산 거래 기술을 가졌다 하더라도 블록체인 도입 시 발생할 수 있는 리스크 문제, 익명성 거래, 고성능 컴퓨터를 이용한 거래 조작 문제, 데이터 처리량에 따른 속도 문제 등으로 블록체인 거래가 안전성을 해결하지 못한다면 여전히 블록체인의 약점을 악용한 우회 거래 및 블록체인 기술을 신뢰하지 못하는 넘어야 할 새로운 사회적 문제가 남을 수 있다. 끝으로, 블록체인이 부정거래를 방지하고 안전하고 투명성 있는 거래로 활용되기 위해서는 앞으로 블록체인에 대한 새로운 비즈니스측면의 보안 서비스 기술 개발과 거래에 따른 안정성 연구가 꾸준히 개발되어야할 것이다.

참고문헌

[1] 이세열, "블록체인을 적용한 시설 클라우드 기반 침입시도탐지," 디지털산업정보학회, 제14권, 제2호, 2018년, pp.17~26.

[2] Y. H. Kang, "A Research on Blockchain-based Copyright Protection for Computational Creativity," Journal of the Korea Convergence Socity, 9(11), 2018, p.76.

[3] https://www.investopedia.com/terms/b/block-chain.asp

[4] https://mastanbtc.github.io/blockchainnotes/block-chaintypes/

[5] 전은아, 이철희, "블록체인 기술 및 보안 위협 분석," 디지털산업정보학회, 제14권, 제4호, 2018년, pp. 47~56.

[6] https://www.code-brew.com/blog/2017/12/30/-blockchain/

[7] Y. J. Lee & S. H. Lee, "Efficient RBAC based on Block Chain for Entities in Smart Factory, Korea Convergence Socity," 9(7), p.71.

[8] https://coinsutra.com/different-types-blockchains/

[9] https://blockchainhub.net/blockchains-and-distribut-ed-ledger-technologies-in-general/

[10] S. T. Kim, Analysius on Consensus Algorithms of Blockchain and Attacks, Korea Convergence Socity, 9(9), p.84.

[11] https://www.tractica.com/newsroom/press-releases/blockchain-for-enterprise-applications-market-to-reach-19-9-billion-by-2025/

[12] https://lisk.io/academy/blockchain-basics/use－cases

[13] S. H. Hong & S. H. Park, The Research on Blockchain-based Secure IoT Authentication, Korea Convergence Socity, 8(11), p.61

[14] https://www.forbes.com/sites/forbescommunicationscouncil/2018/03/27/five-non-financial-blockchain-use-cases-marketers-need-to-understand/2/#3e22d82e756a
[15] https://medium.com/
[16] S. W. Han & S. I. Kim, A User Experience Study in Blockchain Based Social Platform, Korea Convergence Socity, 9(8), p.136.
[17] https://www.zdnet.com/article/9-reasons-to-be-cautious-with-blockchain/
[18] https://igniteoutsourcing.com/publications/block-chain-security-vulnerabilities-risks/
[19] https://www.boannews.com/media/view.asp?idx=70338

논문접수일 : 2019년 2월 28일
수 정 일 : 2019년 3월 21일
게재확정일 : 2019년 3월 22일

■ 저자소개 ■

최 희 식
(Choi Heesik)

2008년 9월 ~ 현재 경민대학교 IT경영과 외래교수
2002년 2월 숭실대학교 컴퓨터학과(공학박사)
2006년 2월 숭실대학교 컴퓨터공학과(공학석사)

관심분야 : 정보보안, 클라우딩컴퓨터, IoT, 핀테크 금융보안
E-mail : dali3054@ssu.ac.kr

조 양 현
(Cho Yanghyun)

1997년 9월 ~ 현재 삼육대학교 컴퓨터·메카트로닉스공학부 교수
2011년 2월 광운대학교 전자통신학과 (공학박사)
1985년 2월 광운대학교 전자통신학과 (공학석사)
1982년 2월 광운대학교 전자통신학과(공학사)

관심분야 : 컴퓨터네트워크, 통신망(BcN), GMPLS
E-mail : yhcho@syu.ac.kr