KICSP 한국 융합신호처리학회

한국융합신호처리학회논문지 Vol. 20, No. 4 : 218~225 December. 2019

블록체인 기술 동향에 관한 연구

박찬홍[1], 이영실[2*]

[1]상지대학교 정보통신공학과, [2]동서대학교 컴퓨터공학부

An Overview of Blockchain Technology: Concepts, Consensus, Standardization, and Security Threats

Roy C. Park[1], Young Sil Lee[2*]

[1]Department of Information Communication Engineering, Sangji University

[2]Division of Computer Engineering, Dongseo University

요 약 2008년 비트코인에 대해 나카모도 사토시 백서가 발표된 이후 블록체인은 단순 암호화폐의 수단을 넘어서 다양한 산업에 사용될 수 있는 4차 산업혁명의 핵심 기술 중 하나로 각광받고 있다. 이에 블록체인 기술을 활용하기 위한 전 세계적으로 다양한 연구와 개발이 이루어지고 있으며, 글로벌 블록체인 컨소시엄을 결성하고 금융 분야뿐만 아니라 물류, 유통, 의료 등 다양한 산업분야로의 적용을 위한 시도가 계속되고 있다. 그러나 여전히 블록체인의 기술 발전이 이러한 관심과 기대를 충족시키는 수준까지 도달하지 못하고 있다. 이러한 블록체인 기반 서비스의 개발은 아직 시작 단계인 만큼 블록체인 플랫폼의 생태계 구축을 위해 필요한 요소들에 대한 논의가 중요하다. 본 논문에서는 블록체인 기술의 전반적인 개요를 살펴보고자 한다. 이를 위해 먼저 블록체인 기술의 개요에 대하여 설명하고 , 생성된 블록을 기존의 체인에 연결하기 위한 합의 알고리즘, 국제표준 기구를 중심으로 한 블록체인 표준화 동향 및 블록체인의 한계점과 발생 가능한 보안 위협에 대하여 기술한다.

• 주제어 : 블록체인, 합의 알고리즘, 블록체인 표준화, 블록체인 보안위협, 블록체인 플랫폼

Abstract Since the publication of Satoshi Nakamoto's white paper on Bitcoin in 2008, blockchain is in the spotlight as one of the core technologies of the Fouth Industrial Revolution, which can be used in various industries beyond simple cryptocurrency. various researches and developments are being conducted worldwide to utilize blockchain technology, and a global blockchain consortium is formed. In addition, attempts are being made to apply to various industries such as logistics, distribution, and medical care as well as the financial sector. However, blockchain tecnology developments still do not reach the level that meets these concerns and expectations. In this paper, we presents a comprehensive overview of blockchain technology by giving its brief concepts, consensus algorithms, standardization, and security threats.

• Key Words : Blockchain, Consensus Mechanism, Blockchain Standardization, Blockchain Security Threats, Blockchain platform

Received 09 December 2019, **Revised** 27 December 2019, **Accepted** 30 December 2019

*** Corresponding Author** Young Sil Lee, Division of Computer Engineering, Dongseo University, 47, Jurye-ro, Sasang-gu, Busan, Korea.
E-mail: youngsil.lee0113@gmail.com

Ⅰ. 서론

2009년 비트코인으로부터 시작된 블록체인은 2016년 초 세계경제포럼(World Economic Forum, WEF)에서 제 4차 산업혁명 시대를 이끌 핵심 기술 중 하나로 선정되는 등 미래 신기술로 각광받으며 금융권을 중심으로 기존의 비즈니스 프로세스를 바꿀 새로운 패러다임으로 등장하였다[1]. 또한 글로벌 시장조사기관인 가트너(Gartner)와 딜로이트(Deloitte)에서도 각각 2017년 기술 트랜드 중 하나로 블록체인을 선정하면서, 블록체인과 관련된 산업들이 빠른 속도로 진화하고 있다[2].

블록체인은 네트워크에 참여하는 모든 거래 참여자가 인터넷으로 상호 연결되어 모든 거래내역 등을 암호화하여 네트워크 구성원에게 데이터를 분산 저장하는 디지털 원장(ledger)를 의미하며, 체인으로 형성된 모든 블록을 변경하거나 네트워크를 통합하지 않으면 변경할 수 없다는 점에서 신뢰성과 안전성, 효율성, 보안성을 제공하는 분산 컴퓨팅 기술로 이제는 금융권에서의 단순한 암호통화의 수단을 넘어서 의료서비스, 에너지 산업, 공공, 물류, 유통 등 다양한 산업분야에서 중요한 혁신 수단으로 여겨지고 있다.

또한, 블록체인의 활용을 위한 국제적 협업 사례도 증가하고 있다. 2015년 세계 최대 글로벌 블록체인 컨소시엄인 R3CEV이 구성되어 금융 산업 내 블록체인 기술 표준화를 추진하고 있으며, 같은 해 리눅스 재단(Linux Foundation)과 IBM의 주도로 오픈소스 프로젝트인 하이퍼레저(Hyperledger)가 시작되어 여러 산업에서 범용적으로 도입 가능한 블록체인 기술 표준을 제시하며 현재 Intel 등 대표적인 글로벌 IT기업부터 금융, 통신, 에너지, 산업을 아우르는 글로벌 컨소시움과 국내의 한국거래소, 예탁결제원 삼성 SDS, LG CNS, 카카오뱅크 등이 General 멤버로 참여하면서 전 세계에서 가장 대표적인 블록체인 플랫폼으로 상용 블록체인 기술의 혁신을 이끌고 있다.

그리고 미국의 경우 미 헬스 IT 조정국(ONC)에서 의료정보 기록 및 보안을 위해 블록체인 기술을 도입할 예정[3]이며, 스웨덴에서는 자국 스타트업 기업인 크로마웨이(ChromaWay)와 협력하여 현재 블록체인 기반 국가 토지 등기시스템을 테스트하고 있다[4]. 싱가포르에서도 무역 금융사기 대비책의 일환으로 정부가 글로벌 은행들과 협력하여 블록체인 기술에 기반한 중복 자금청구 알람 시스템을 개발[5]하고 있는 등 전 세계적으로 블록체인을 이용한 국가 차원의 시스템 개발이 활발히 이루어지고 있다. 국내에서도 2016년 '금융권 공동 블록체인 컨소시엄'이 구성되어 블록체인 기술을 상용화를 추진하고 있으며, 미래창조과학부에서 블록체인을 4차 산업혁명의 중심기술 중 하나로 이를 정보보호 분야에 적용한 시범사업(Pilot Project)을 추진 중에 있다[6].

그러나 여전히 블록체인의 기술 발전이 이러한 관심과 기대를 충족시키는 수준까지 도달하지 못하고 있다. 퍼블릭 블록체인의 낮은 거래 처리 속도, 거래량의 증가로 인한 참여자의 정보 저장 용량의 증가와 과도한 연산 작업, 무엇보다 블록체인의 보안 위협에 대한 분석 및 대응방안에 대한 문제가 제기되고 있다[7-8].

본 논문에서는 블록체인의 기본적인 개념 및 합의 알고리즘에 대하여 상세히 살펴보고, 국제 표준화기구인 ISO, ITU-T를 중심으로 블록체인 표준화 활동 현황에 대하여 살펴보았다. 또한, 현재 블록체인의 한계점과 이를 위협하는 다양한 형태의 보안 위협에 대하여 분석하였다.

본 논문의 구성은 다음과 같다. 2장에서 블록체인 기술 개요 및 합의 알고리즘, 플랫폼에 대하여 설명하고 3장에서 표준화 동향에 대하여 살펴본다. 4장에서는 현재 블록체인의 한계점이라고 제기되고 있는 문제와 다양한 보안위협에 대하여 설명한다. 마지막으로 5장에서 본 논문의 결론을 짓는다.

Ⅱ. 블록체인 기술 동향

2.1 블록체인

블록체인은 참여자들의 순차적인 거래내역을 블록으로 형성한 체인형태의 공공거래 장부라고도 불리며, P2P(peer-to-peer) 네트워크 방식에 기반을 두어 거래 시 중개자의 필요성을 없앰으로써 거래의 투명성과 효율성을 제공할 수 있다[9].

블록체인에서의 블록(Block)이란 거래 참여자 사이에서 이루어진 거래 정보를 저장한 단위로서, 거래 원장의 복사본이 각 네트워크 구성원에게 분산되어 새로운 거래가 발생할 때마다 구성원들의 동의를 통해 해당 거래를 인증한다. 이 때문에 하나의 거래 정보를 임의로 변경하기 위해서는 수많은 거래 참여자의 정보를 모두 변경해야 하기 때문에 거래의 신뢰성을 높여주고 정보의 추적이 용이하다는 장점을 가지고 있다.

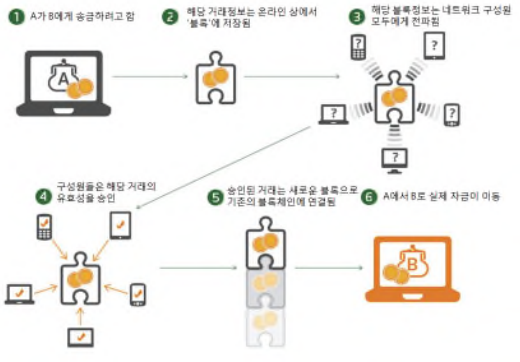

Fig. 1. Blockchain based transaction process [10]

Fig 1은 블록체인기반 거래 방법에 대하여 설명하고 있다[3]. 네트워크에 참여하고 있는 참여자가 새로운 거래를 시작하려고 할 경우, 해당 거래 정보는 온라인 상에서 새로운 블록으로 저장된다. 이후 생성된 블록을 네트워크상의 모든 거래 참여자에게 전달하고 합의(Consensus)와 블록의 유효성이 검증된 이후 거래를 승인하게 된다. 거래가 승인될 경우 기존의 블록체인에 새 블록이 연결되고 해당 거래를 처리하는 방식을 취한다. 이렇게 블록들이 순차적으로 연결되어 체인을 형성하게 되고, 모든 참여자들은 동일한 정보가 기록된 원장을 저장 및 관리하게 된다.

여기에서 블록들이 연결된다는 의미는 일정시간의 거래내역뿐만 아니라 새로운 블록에 해당 블록의 해쉬값과 이전 블록의 정보에 대한 해쉬값이 포함되어 기록되는 것을 말한다. 메시지 다이제스트 함수(Message digest function)라고도 부르는 해쉬함수는 임의의 길이를 갖는 메시지를 입력하여 고정된 길이의 해쉬값을 출력하며, 출력값으로부터 입력값을 유추할 수 없는 단방향성을 특징으로 가지고 있어, 생성되는 해쉬값을 포함하여 연결되는 블록의 무결성을 제공해준다.

2.2 블록체인 합의 알고리즘

블록체인 시스템에서 거래 참여자들 간에 무결성과 신뢰성을 제공하는 블록을 생성하고 연결하기 위해서는 참여자간의 블록을 합의하는 과정이 필요하다. 이는 블록체인 역시 분산 원장의 형태를 가지고 탈중앙화된 구조이기 때문에 분산처리시스템에서 흔히 발생할 수 있는 오류와 관련된 개념인 비잔티움 장군 문제[11]를 해결하기 위함이며, 이 과정에서 주어진 조건을 만족하는 경우 블록을 생성하고 기존의 체인에 생성된 블록을 연결하게 된다.

대표적으로 사용되는 합의 알고리즘으로는 작업증명(Proof of Works, PoW), 지분증명(Proof of Stake, PoS), 위임지분증명(Delegated PoS, DPoS), PBFT(Practical Byzantine Fault Tolerance) 등이 있다.

먼저, 작업증명[12]은 1993년 스팸메일에 대항하기 위해 Cynthia Dwork와 Moni Naor에 의해 처음 소개되었으며 2008년 사토시 나카모토 (Satoshi Nakamoto)의 비트코엔에 적용된 합의 알고리즘으로 합의에 참여하기 위해 리소스를 투입했다는 것을 증명하는 방식이다. 비트코인에서는 신규 블록을 추가하기 위해 채굴(Mining)이라는 과정을 통해 참여자들이 암호화된 퍼즐(해쉬함수 기반의 수학적 문제)을 풀게 하여 운영되고, 처음 퍼즐을 푼 채굴자가 그에 합당한 보상을 코인 형태로 얻게 된다. 결국 고성능의 많은 장비를 보유한 사람들에게 더 많은 보상이 돌아가기 때문에 사람들로 하여금 일명 채굴 농장(Mining Farm)을 세우게 하여 과도한 전력낭비를 야기하며 이러한 채굴 농장들이 모여 마이닝 풀(Mining Pool)을 조직하게 되어 탈중앙화를 목표로 하는 블록체인의 개념과는 반대로 중앙화를 야기하기도 한다. 또한 만약 악의적인 참여자가 임의로 잘못된 블록을 추가하기 위해서는 정상적인 참여자 전체와 경쟁하여 전체 참여자의 과반 이상인 51%를 차지해야 하는데, 이러한 큰 마이닝 풀이 모인다면 51% 공격을 가능케 하여 블록체인 전체를 컨트롤할 수 있는 최악의 상황이 초래될 수도 있다.

지분증명[13]은 2011년 비트코인 포럼에서 참가자가 작업증명방식의 단점을 보완하기 위해 제안한 방법으로 연산능력이 아닌 무작위의 투표 방식을 적용하여 어떤 참여자가 다음 블록을 생산할 것인지를 결정한다. 투표 후보군에 들어가기 위해서 각 참여자는 이 네트워크에 코인을 입금하여 지분을 보유해야 하고, 이 지분의 보유량에 따라 다음 블록을 생산하고 보상을 받을 검증자(Validator)로 선출될 확률을 높인다. 이때 검증자는 자신이 생산한 블록 안에 있는 거래들의 수수료를 받게 되며, 만약 검증자가 사기성의 거래를 승인하고 그 행위가 발각된다면 자신의 지분 중 일부를 잃고 다음번 검증자가 될 확률이 매우 낮아진다. 이 방식은 모든 사람이 채굴을 할 수 없기 때문에 전력낭비가 매우 낮으며, 마이닝 풀의 조직이 불가능하기 때문에 작업증명보다 더 탈중앙화되다는 장점을 가지고 현재 이더리움(Ethereum)등의 플랫폼에서 적용을 시도

중이다. 그러나 단점으로 지분이 많은 참여자들이 검증자로 선출될 확률이 높기 때문에 독점이나 과점 현상이 발생할 수 있다.

위임지분증명[14]은 지분증명과 유사한 방식의 합의 알고리즘이지만, 한명의 검증자를 선출하는 것이 아니라 지분을 가지고 있는 참여자에게 시스템 내 지분의 일부를 대표할 목격자(witnesses)를 선택할 수 있는 기회를 제공한다는 차이점을 가지고 있다. 선출된 목격자들은 자신을 지지하는 참여자들의 지분을 락업하고 검증 과정에 참여할 수 있으며, 목격자와 자신의 지분을 제공한 참여자는 추가된 블록으로부터 수수료를 보상으로 받을 수 있다. 또한 적절하지 않은 행동을 하는 목격자를 퇴출시킬 수 있는 방법이 포함되어 있다. 이오스(EOS), 스팀(Steam), 비트셰어(Bitshare) 등의 플랫폼에서 이 방식을 채택하고 있으나, 2018년 9월 이오스 블록 생성을 담당하는 대표 목격자 중 일부가 본인의 자격을 유지하기 위해 서로에게 투표했다는 의혹이 제기되면서 치명적인 결함이 있다는 사실이 알려졌다. 이처럼 참여자들의 낮은 투표 참여율에 따라 제한된 수의 목격자에게 권한을 부여함으로써 마찬가지로 중앙화를 야기할 수 있다는 단점을 가진다.

PBFT방식[15]은 빠른 속도를 위해 고안된 방식으로 참여자들의 자발적인 참여와 검증을 기반으로 합의를 수행하며, 비잔티움 장군 문제를 해결하는 동시에 비동기 네트워크 환경에서 참여자들간에 두 번의 브로드캐스트 과정을 거쳐 합의에 도달하게 된다. 이러한 특징으로 이 방식은 기업 내부 시스템에 적용할 수 있는 프라이빗 블록체인에서 주로 사용되고 있다. 이 방식은 전체 참여자의 2/3를 초과한 참여자가 합의하면 검증이 이루어지기 때문에 속도가 향상되지만, 작업증명 방식에 비하여 보안성이 떨어진다. 블록체인 전체에 참여자의 수를 n이라 가정하였을 때, (n-1)/3 이하의 참여자가 악의적인 행동을 보인다 하더라도 합의를 정상적으로 이끌어 낼 수 있다. 이는 반대로 34%의 공격이 이루어졌을 때 전체 블록체인 생태계가 무너지게 된다. 이를 막기 위해서는 전체 참여자의 수를 늘려야 하지만, 이 경우 모든 참여자들 간의 통신이 이루어져야 하는 구조이므로, 속도가 저하되게 된다.

2.3 블록체인 플랫폼

2009년 비트코인을 시작으로 현재까지 다양한 형태의 블록체인 플랫폼이 개발되고 있으며, 이들 플랫폼을 분류하는 방법 역시 다양하다. 이중 가장 대표적으로 사용하는 방법은 새로운 블록을 추가할 수 있는 주체에 따른 분류 방법이다. 이에 따라 누구나 블록체인에 참여할 수 있는 공개된 형태의 플랫폼인 퍼블릭(Public 또는 permissionless) 블록체인과 미리 선정된 참여자들에 의해 블록체인을 구성하고 제어되는 형태의 플랫폼인 프라이빗(Private 또는 permissioned) 블록체인으로 분류할 수 있다.

Table 1. public blockchain vs. private blockchain

	public blockchain	private blockchain
열람권한	누구나(anyone)	허가된 참여자 (member)
거래검증	누구나(anyone)	허가된 감독기관 (policy-based)
블록생성	누구나(anyone)	허가된 기관 (policy-based)
권한변경	어려움	보통
거래속도	느림(5~40TPS)	빠름(1000TPS 이상)
합의과정	PoW, PoS 등	PBFT
적용분야	암호화폐, 투표시스템	금융거래, 공급망
플랫폼	비트코인, 이더리움, 아더	하이퍼레저 페브릭, R3, Corda, Tendermint

Fig. 1은 퍼블릭 블록체인과 프라이빗 블록체인을 비교한 결과를 나타내고 있다. 퍼블릭 블록체인의 가장 큰 장점은 누구나 쉽게 참여가 가능하고 모든 거래가 투명하며, 이를 통해 블록체인에서 추구하는 탈중앙화를 구현할 수 있다는 점이다. 주로 사용되는 합의 알고리즘은 작업증명과 지분증명 방식이며, 현재 다양한 암호화폐와 게임 등의 영역에서 활발히 사용되고 있으나, 거래 처리 속도가 느리고 참여자들의 신원 확인이 어렵기 때문에 금융관련 법과 규제사항을 준수해야 하는 환경에서 사용이 어렵다.

반면 소수의 허가된 참여자만이 참여하는 프라이빗 블록체인의 경우 허가된 기관만이 데이터를 열람하고 거래를 검증하며 생성한다. 따라서 거래 처리 속도가 빠르며 성능도 높은 편이다. 그러나 폐쇄적이고 중앙화된 시스템이라 볼 수 있어 투명성이 떨어진다는 단점이 있다.

Ⅲ. 블록체인 표준화 동향

2016년 9월 설립된 ISO/TC307(Blockchain and Distributed Ledger Technologies)을 시작으로 2017년 8월 ITU-T에서도 여러 연구 그룹(Study Groups, SG) 및 포커스 그룹(Focus Gropus, FG)에서 블록체인 및 분산원장 기술 표준화를 시작하는 등 다양한 블록체인 표준화 활동이 급속도로 증가하고 있다.

국제표준화기구 ISO 기술위원회에서는 현재 블록체인 이슈를 각 분야별로 집중적으로 다루기 위해 5개의 작업그룹(Working Group, WG)과 1개의 연구그룹(SG)이 결성되어 있다. 또한 자문그룹 및 공동그룹까지 합하여 총 10개의 작업그룹이 구성되어 운영되고 있으며 현재 1개의 ISO표준안을 게시하였으며 10개의 표준을 개발하고 있다. ISO/TC 307의 구조는 Table 2와 같다[16].

Table 2. Structure of ISO/TC 307 working group [16]

Reference	Title
ISO/TC 307/AG1	SBP 검토자문그룹(SBP Review Advisory group)
ISO/TC 307/AHG	연락 검토 특별 그룹(Liaison Review Ad Hoc Group)
ISO/TC 307/CAG1	의장조정그룹(Convenors coordination group)
ISO/TC 307/JWG4	ISO/TC 307과 ISO/IEC JTC 1/SC 27 공동 작업그룹: 블록체인 및 분산원장 기술 및 IT 보안기술(Blockchain and distributed ledger technologies and IT Security techniques)
ISO/TC 307/SG7	블록체인과 분산원장기술시스템의 상호운용성(Interoperability of blockchain and distributed ledger technology systems)
ISO/TC 307/WG1	블록체인 기반(Foundations)
ISO/TC 307/WG2	블록체인 보안, 프라이버시 및 아이덴티티(Security, privacy and identity)
ISO/TC 307/WG3	블록체인 스마트 컨트랙트 및 그 응용(smart contracts and their application)
ISO/TC 307/WG5	블록체인 거버넌스(Governance)
ISO/TC 307/WG6	블록체인 사용 사례(Use cases)

2019년 10월 게시된 표준 ISO/TR 23455:2019는 블록체인과 분산원장기술시스템에서의 스마트 컨트랙트에 대한 개요 및 상호작용에 관한 내용이 포함되어 있다. 또한 개발 중인 블록체인 및 분산원장기술 표준은 아래의 Table 3과 같다.

Table 3. Standard and/or Project under The Direct Responsibility of ISO/TC 307 Secretariat [16]

Reference	Title
ISO/CD TR 3242	블록체인 및 분산원장기술-사용사례(Blockchain and distributed ledger technologies - Use cases)
ISO/DIS 22739	블록체인 및 분산원장기술-용어(Blockchain and distributed ledger technologies－Terminology)
ISO/CD TR 23244	블록체인 및 분산원장기술-개인정보 및 개인식별정보 보호 고려사항(Blockchain and distributed ledger technologies－Privacy and personally identifiable information protection considerations)
ISO/CD TR 23245	블록체인 및 분산원장기술-보안 위험, 위협 및 취약점(Blockchain and distributed ledger technologies－Security risks, threats and vulnerabilities)
ISO/NP TR 23246	블록체인 및 분산원장기술-블록체인 및 분산원장기술을 이용한 신원관리 개요(Blockchain and distributed ledger technologies－Overview of identity management using blockchain and distributed ledger technologies)
ISO/CD 23257.2	블록체인 및 분산원장기술-참조구조(Blockchain and distributed ledger technologies－Reference architecture)
ISO/WD TS 23258	블록체인 및 분산원장기술-분류 및 온톨로지(Blockchain and distributed ledger technologies－Taxonomy and Ontology)
ISO/AWI TS 23259	블록체인 및 분산원장기술-법적구속력을 갖는 스마트 컨트랙트(Blockchain and distributed ledger technologies－Legally binding smart contracts)
ISO/CD TR 23576	블록체인 및 분산원장기술-디지털자산 관리자의 보안관리(Blockchain and distributed ledger technologies－Security management of digital asset custodians)
ISO/NP TS 23635	블록체인 및 분산원장기술-관리지침(Blockchain and distributed ledger technologies－Guidelines for governance)

작업그룹(WG)에서 표준을 개발하고 이를 위한 사전 연구는 연구그룹(SG)에서 진행하는 ISO와는 달리 ITU-T에서는 연구그룹(SG)에서 표준을 개발하고 포커스그룹(FG)에서 사전 연구를 진행한다. 이에 따라

ITU-T에서는 4개의 연구그룹(SG)과 2개의 포커스그룹(FG)에서 블록체인 및 분산원장기술 표준화 활동을 진행하고 있다 (Table 4 참고) [17].

Table 4. DLT related work in ITU-T Focus Group (pre-standardization) and Study Groups (formal standardization) [17]

Reference	Title
FG DLT	분산원장기술적용에 관한 포커스그룹(Focus Group on Application of Distributed Ledger Technology)
FG DPM	IoT, 스마트도시 및 커뮤니티 지원을 위한 데이터 처리와 관리에 관한 포커스 그룹(Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities)
FG DFC	디지털법정화폐를 포함하는 디지털 화폐에 관한 포커스 그룹(Focus Group on Digital Fiat Currency)
SG13	BaaS 클라우드 컴퓨팅 요구사항(cloud computing requirements for blockchain as a Service(BaaS))
SG16	분산원장기술 및 전자서비스(DLT and e-services)
SG17	분산원장기술의 보안 측면에서 다양한 연구수행(various work items on security aspects for DLT)
SG20	사물의 블록체인(blockchain of things)

Table 3에서 연구그룹 17을 제외한 다른 연구그룹은 각 연구그룹의 핵심기술 분야에 블록체인을 융합한 기술과 관련한 권고안을 개발하고 있다.

이 외 W3C, IEEE 등에서도 블록체인 관련 다양한 표준화를 진행 중에 있다. 먼저, W3C의 블록체인 커뮤니티 그룹(W3C Blockchain Comminity group), 블록체인 디지털 자산 커뮤니티 그룹, 체크포인트 커뮤니티 그룹, 원장 간 지불 커뮤니티 그룹, 크리덴셜 커뮤니티 그룹 등에서 블록체인 관련 다양한 연구를 수행하였으며 보고서를 발간하고 있다[18-20]. IEEE에서도 2017년 블록체인 작업그룹을 수립하고 2019년 12월 현재 총 10개의 표준 시리즈가 개발되고 있다 (Table 5 참고) [21].

Table 5. IEEE Active Standards Projects related blockchain and DLT [14]

Reference	Title
P2418.1	사물인터넷에서의 블록체인사용을 위한 표준 프레임워크(Standard for the Framework of Blockchain Use in Internet of Things (IoT))
P2418.2	블록체인시스템의 표준 데이터 형식(Standard Data Format for Blockchain Systems)
P2418.3	농업에서 분산원장기술 사용을 위한 표준 프레임워크(Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture)
P2418.4	CAVs에서의 분산원장기술 사용을 위한 표준 프레임워크(Standard for the Framework of Distributed Ledger Technology (DLT) Use in Connected and Autonomous Vehicles (CAVs))
P2418.5	에너지분야의 블록체인 표준(Standard for Blockchain in Energy)
P2418.6	의료, 생활 및 사회과학에서 분산원장기술 사용을 위한 표준 프레임워크(Standard for the Framework of Distributed Ledger Technology (DLT) Use in Healthcare and the Life and Social Sciences)
P2418.7	금융 공급망에서의 블록체인 사용 표준(Standard for the Use of Blockchain in Supply Chain Finance)
P2418.8	정부의 블록체인 어플리케이션 표준(Standard for Blockchain Applications in Governments)
P2418.9	암호화폐 기반 보안토큰의 표준(Standard for Cryptocurrency Based Security Tokens)
P2418.10	블록체인 기반 디지털 자산관리 표준(Standard for Blockchain-based Digital Asset Management)

Ⅳ. 블록체인 기술의 보안 위협

블록체인은 현재의 기술로 해결하기 어려운 몇 가지 한계점을 가지고 있다. 블록체인의 성능은 초당 처리할 수 있는 트랜잭션의 수(Transaction Per Second, TPS)로써 표현 가능하며 현재 작업증명, 지분증명 방식의 경우 5~40TPS, PBFT의 경우 1000~1500TPS의 성능을 제공(시스템의 규모에 따라 차이가 있음)하고 있어 여전히 충분한 수준에 도달하지 못하고 있다. 또한

블록체인은 분산된 거래 원장을 관리하기 때문에 모든 참여자는 동일한 원장을 각자 저장해야 하며, 시간이 지날수록 규모가 커지므로 이를 저장하기 위한 비용 문제가 발생한다.

이뿐만 아니라 대부분 블록체인은 보안이 강화된 시스템이라고 인식되고 있으나, 블록체인은 여러 가지 보안 요소 중 원장 정보에 대한 무결성과 비가역성을 제공하는 데 집중되어 있으며, 다른 보안요소는 부족한 경우가 있다[7].

블록체인의 합의 과정에서 발생할 수 있는 가장 대표적인 보안 위협은 이중지불(Double Spending)과 Mining/Pool이다. 이중지불은 참여자가 거래에 동일한 암호화폐를 여러 번 사용하는 방법으로 Race attack, Finney attack, Vector76 attack (one-confirmation attack), alternative history attack, 51% attack 등 다양한 공격을 통해 이중지불을 가능토록 할 수 있다. 그리고 Mining/Pool 위협은 작업증명 방식의 단점으로 꼽히는 것 중 하나로 사람들이 모여 일종의 마이닝 풀을 형성함으로써 발생 가능한 보안 위협이다. Selfish Mining/Block-discard attack, Block-withholding attack (BWH), fork-after-withhold attack (FAW), Bribery attack, Pool Hopping attack 등이 여기에 속한다.

블록체인에서 참여자 간의 네트워크 연결은 P2P로 연결되는데, 이 과정에서 발생 가능한 공격으로, 참여자의 연결을 공격자에게만 연결되도록 하여 임의로 다른 노드들로부터 고립시키는 Eclipse attack, 악의적인 ISP가 주변 라우터들로 잘못된 라우팅 정보를 브로드캐스트하여 비정상적으로 처리되도록 하는 BGP Jijacking과 이를 통해 partition Routing attack 및 Delay Routing attack을 시도하는 것 외에도 DDoS attack, Transaction Malleability attack, Timejacking attack, Sybil attack, Refund attack, Balance attack, Punitive and Feather forking attack 등의 다양한 공격이 가능하다[22-24].

Ⅴ. 결론

본 논문에서는 4차 산업혁명시대를 이끌어갈 핵심 기술 중 하나로 각광받고 있는 블록체인의 기본적인 개념 및 대표적으로 사용되는 합의 알고리즘인 작업증명(Proof of Works, PoW), 지분증명(Proof of Stake, PoS), 위임지분증명(Delegated PoS, DPoS), PBFT(Practical Byzantine Fault Tolerance)에 대하여 상세히 살펴보았다. 또한 국제 표준화기구인 ISO, ITU-T를 중심으로 블록체인 표준화 활동 현황 및 현재 블록체인의 한계점과 이를 위협하는 다양한 형태의 보안 위협에 대하여 살펴보았다.

블록체인 및 분산원장 기술은 시작 단계에 속해있으며, 금융 분야뿐만 아니라 물류/유통, 의료, 사물인터넷의 IoT기기 인증 및 스마트 컨트랙트 기반 자동 제어 등 현재 다양한 영역으로의 적용을 확장하기 위해 많은 연구가 진행되고 있으나 여전히 블록체인의 기술 발전이 이러한 관심과 기대를 충족시키는 수준까지 도달하지 못하고 있다. 신기술이 신뢰감 있고 안정적으로 전 세계의 다양한 산업군에 확산 및 응용되기 위해서는 더욱 많은 노력이 필요하다. 추후 연구로는, 본 논문에서 언급한 블록체인에서 발생 가능한 각 보안 위협에 대하여 분석하고 이를 막기 위한 대응 방안에 대하여 연구할 계획이다.

ACKNOWLEDGMENTS

This work was supported by Dongseo University, “Dongseo Cluster Project“ Research Fund of 2019 (DSU-20190012).

REFERENCES

[1] World Economic Forum, The future of financial infrastructure, 2016.8.12.

[2] Young-young Lee(2017), Blockchain Technology Trends and Implications. Trends and Issues(34), 1-21.

[3] Cointelegraph (2017.4.16.). US Government Invests in Blockchain to Protect Healthcare Companies from hackers.

[4] Reuters (2016.6.16.), Sweden tests blockchain technology for land registry.

[5] Govlnsider (2016.6.7.), singapore Government builds blockchain system to protect banks.

[6] Ministry of Public Administration and Press release (January 2, 2017). E-Government Gets Smarter with High Tech Convergence. Avaliable: http://www.korea.kr/news/pressReleaseView.do?newsId=156178437

[7] Young-young Lee, Cheong-won Woo, (2018). Prospects, Limitations, and Implications of Blockchain Technology.

Future Horizon(38), 12-15.

[8] Heeyoul Kim. (2018). Analysis of Security Threats and Countermeasures on Blockchain Platforms, Journal of KIIT. vol. 16, no. 5, pp. 103-112.

[9] Shamistha Dash, Anirban Majumdar, Presanna Gunikkar, “Blockchain: A Healthcare Industry View,” Gapgemini. 2017(7).

[10] Thomson Reuters (2016.1.16.). Blockchain technology: Is 2016 the year of the blockchain?. Avaliable: https://blogs.thomsonreuters.com/answerson/blockchain-technology/

[11] Leslie Lamport, Robert Shostak, Marshall Pease. (1982). “The Byzantine Generals Problem,” Journal of ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4. issue 3, pp. 382-401.

[12] Wikipedia, Proof of Work, Avaliable: https://en.wikipedia.org/wiki/Proof_of_work

[13] V. Buterin and V. Griffith. (2017). "Casper the Friendly Gadget", Avaliable: https://ethresear.ch/uploads/default/original/1X/fdbebd67c8a9671efabf4e53d6267789cd91d96c.pdf.

[14] M. Castro and B. Liskov. (2002). "Practical Byzantine Fault Tolerance and Proactive Recovery", ACM Transactions on Computer Systems, vol. 20, no. 4, pp. 398-461.

[15] J. Kwon. (2014). "Tendermint: Consensus without Mining", Avaliable: https://tendermint.com/static/docs/tendermint.pdf.

[16] ISO/TC 307. Avaliable: https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0

[17] ITU-T. Avaliable: https://www.itu.int/en/Pages/default.aspx

[18] W3C Blockchain Community Group. Avaliable: https://www.w3.org/community/blockchain/

[19] W3C Web Payments Working Group, Avaliable: https://www.w3.org/Payments/WG/

[20] W3C Interledger Payments Community Group, Avaliable: https://www.w3.org/community/interledger/

[21] IEEE Blockchain. Avaliable: https://blockchain.ieee.org/standards

[22] Jamal Hayat Mosakheil. (2018). “Security Threats Classification in Blockchains,” Culminating Projects in Information Assurance. 48. Avaliable: https://repository.stcloudstate.edu/msia_etds/48

[23] Xiaoqi Li, Peng Liang, Ting Chen, Xiapu Luo, Qiaoyan Wen. (2017). “A survey on the security of blockchain system,” Future Generation Computer system. Avaliable: http://dx.doi.org/10.1016/j.future.2017.08.020.

[24] Xiaochun Yun, Weiping Wen, Bo Lang, Hanbing Yan, Li Ding, Jia Li, Yu Zhou. (2018). Cyber Security, Communications in Computer and Information Science. Avaliable: https://doi.org/10.1007/978-981-13-6621-5

[25] Atzei, N., Bartoletti, M., & Cimoli, T. (2016). A survey of attacks on Ethereum smart contracts (No. 1007). Retrieved from http://eprint.iacr.org/2016/1007.

[26] Tapscott D, Tapscott A. (2016), “The Impact of the Blockchain Goes Beyond Financial Services,” Harvard Business Review.

저자 소개

이 영 실 (Young Sil Lee)

2006년 2월 : 동서대학교 정보네트워크학과 (공학사)
2010년 8월 : 동서대학교 디자인&IT전문대학원 유비쿼터스IT학과 (공학석사)
2015년 8월 : 동서대학교 일반대학원 유비쿼터스IT학과 (공학박사)
2017년 4월 ~ 현재 : 동서대학교 컴퓨터공학부 조교수
관심분야 : 암호학, 정보보안, 헬스케어

박 찬 홍 (Roy C. Park)

2008년 8월 : 상지대학교 산업공학과 (공학사)
2010년 8월 : 상지대학교 컴퓨터정보공학과 (공학석사)
2015년 2월 : 상지대학교 컴퓨터정보공학과 (공학박사)
2015년 3월 ~ 2019년 2월 : 동서대학교 컴퓨터공학부 교수
2019년 3월 ~ 현재 : 상지대학교 정보통신공학과 교수
관심분야 : 클라우드, 빅데이터, 헬스케어, 인공지능, HCI, 정보검색, 추천 시스템