블록체인 핵심 기술과 국내외 동향

서강대학교 ▌이동영·박지우·이준하·이상록·박수용

1. 서 론

블록체인 기술은, 2008년 익명의 '사토시 나카모토'란 인물이 'Bitcoin: A Peer-to-Peer Electronic Cash System[1]'라는 연구를 공개함으로서 대중들에게 알려졌다. 해당 연구는 중개 기관에 의존적인 기존의 거래 방식에서 벗어나 중개 기관 없이 거래 당사자들 간의 직접적인 거래를 가능케 하고, 동등한 계층의 제3자들 간 거래의 신뢰성을 보장한다. 이는 중개 기관을 통하여 이루어지던 기존 거래 시스템에서 발생하는 비용 및 시간 낭비의 문제를 완화시킬 수 있는 가능성을 선보였다. 예를 들어, 현행 시스템의 국제 송금 서비스는 거래의 신뢰성 보장을 위해 실거래 은행뿐만 아니라 중개, 환거래 은행 등을 거치는 추가적인 송금이 필요로 한다. 따라서 이러한 구조 하에서는 수수료가 이중으로 발생하는 문제점을 지니게 된다. 이중 수수료를 없애기 위해서 중개 은행을 배제하고 직접적인 거래를 하더라도, 거래 당사자 간의 신뢰가 보장될 수 없다. 하지만 블록체인 기술은 모든 정보를 참여자들에게 동등하게 제공함으로써 거래에 대한 신뢰성을 부여할 수 있게 된다. 따라서 블록체인 기반의 송금 서비스는 거래 당사자 간의 신뢰를 보장하는 직접적인 거래를 가능케 한다.

블록체인 기술의 시작점인 비트코인 블록체인은 이러한 신뢰의 문제를 해결하기 위하여 Proof of Work(PoW)라는 합의 알고리즘과 분산 장부(Distributed Ledger)라는 개념을 고안하였다. 전체적인 비트코인 블록체인의 신뢰 문제 해결 방안은 다음과 같다. 먼저, 모든 사용자는 비트코인 블록체인 네트워크상에서 발생하는 모든 거래를 동일하게 저장한다. 다음 각각의 사용자는 새로운 거래들을 기반으로 하나의 블록을 수학적인 연산(Proof of Work)을 통하여 생성한다. 가장 먼저, 작업 증명을 끝낸 블록은 기존 분산장부의 마지막 위치에 추가되며 이는 모든 블록체인 사용자의 분산장부에 동일하게 수행된다. 이를 통해 모든 사용자가 합의된 거래들로만 이루어진 네트워크 구성을 이루어낼 수 있다. 또한, 악의적인 사용자가 거래를 조작하는 공격(Replay Attack)을 하는 경우 정의로운 사용자들은 기존 거래 내역을 통하여 공격을 감지 할 수 있고 공격이 포함된 거래는 블록이 생성되지 않도록 하여 분산장부에는 정상적인 거래들만 추가 되게 된다.

본 논문은 블록체인 시스템을 구현하기 위한 기반 기술들에 대해 소개하고 블록체인 기술의 세계적 동향을 소개한다.

따라서 본 논문의 2장에서는 블록체인의 핵심 기술 4가지인 P2P 네트워크, 암호화 알고리즘, 합의 알고리즘, 분산장부의 개념 및 기술, 스마트 컨트랙트에 대해 소개하고 3장에서는 블록체인 관련 산업계와 정책 현황을 소개한다. 마지막으로 4장에서는 블록체인 기술의 미래 전망 및 한계점에 대해 논한다.

2. 블록체인의 핵심 기술 소개

블록체인은 P2P(Peer-to-Peer) 네트워크, 암호화, 분산 장부, 분산 합의와 같이 크게 4가지의 기반 기술로 구성되어 있다. 각각의 기술들은 블록체인의 가치라 할 수 있는 탈중앙화, 데이터의 무결성 유지 등을 위해 상호 보완적인 관계를 취하고 있으며 블록체인 동작 메커니즘의 근간을 이루고 있다. 한편, 블록체인 환경에서의 응용 기술인 스마트 컨트랙트는 프로그램의 실행 코드 및 그 결과에 대한 무결성, 신뢰성을 제공해주는 기술로서 자동화된 거래, 제어 등의 분야에서 주목받고 있다. 본 장에서는 이러한 핵심적인 기술들에 대해 간략히 소개하고 블록체인에서 어떻게 적용되고 있는지를 소개한다.

2.1 P2P 네트워크

블록체인의 참여자들 간 연결 및 통신은 P2P 네트워크를 기반으로 하여 이루어진다. P2P 네트워크는

† 본 연구는 미래창조과학부 SW중심대학사업의 지원으로 수행되었습니다.

기존 클라이언트-서버 방식에서 탈피한 동등한 계층의 참여자들로 이루어지는 네트워크로서 크게 structured P2P(구조적 P2P)와 unstructured P2P(비구조적 P2P)로 분류된다. 특히 unstructured P2P는 서버를 중심으로 참여자들 간의 망이 이루어지는 중앙 집중형 방식과 데이터의 flooding 알고리즘을 기반으로 하는 분산형 P2P 네트워크로 다시 구분 할 수 있다. 블록체인은 기술의 특징이자 이념인 탈중앙화 분산 네트워크를 위해 flooding 기반의 unstructured P2P 네트워크를 사용한다. 또한 P2P 네트워크의 통신은 UDP를 통하여 이루어지는 것이 일반적이지만, 블록체인에서는 TCP/IP를 사용하고 있다. 따라서 블록체인의 참여자들은 자신과 물리적으로 가장 인접한 참여자들의 IP를 유지하고 있으며(비트코인의 경우, 3개의 IP를 유지한다.) 이를 사용하여 메시지 및 데이터를 주고받는다.

2.2 암호화 기술

블록체인에서 사용되는 암호화 기술은 1)데이터의 무결성 검증을 위한 머클 트리(Merkle Tree), 2) 거래의 부인방지를 위한 공개키 기반 디지털 서명 기법이 사용되고 있다.

Merkle tree는 해시 트리의 일종으로 모든 비 리프 노드의 이름이 자식 노드들의 해시로 구성된 트리[4]를 일컫는다. 즉, 리프 노드들은 파일이나 특정 값 등의 데이터를 가리키며 상위 노드는 이 리프 노드의 해시로 구성된다. 이러한 방식으로 구성된 Merkle tree의 루트 노드는 트리를 구성하는 모든 리프 노드들의 데이터의 해시값으로 이루어져있으며 사용자는 루트 노드의 해시를 검증하는 것만으로 데이터들의 위·변조를 검증할 수 있다. 따라서 블록체인에서는 리프 노드에 참여자들 간의 거래, 정보 들을 삽입함으로써 merkle tree의 기초를 구성하며 상위 노드를 만들 때 사용될 수 있는 해시 함수는 여러 가지가 있으나 블록체인에서는 SHA-256 함수를 사용하여 merkle tree를 활용하고 있다.

공개키 기반의 디지털 서명 방식은 사전에 비밀 키를 나누어 가지지 않은 참여자간의 안전한 통신을 이루어지게 하는 암호화 기술로 본인 인증 등의 분야에서 널리 사용되고 있다. 공개 키 기반 구조에서는 공개 키와 비밀 키 두 개의 키 쌍이 존재하며, 공개 키는 모든 참여자들이 알 수 있지만 이에 대응되는 비밀 키는 해당 소유자만이 알 수 있도록 유지되어야 한다. 이러한 공개 키 기반 디지털 서명 방식을 블록체인에서는 거래의 유효성을 검증하는데 사용하고 있다. 거래를 발생시키려는 사용자가 자신의 비밀 키를

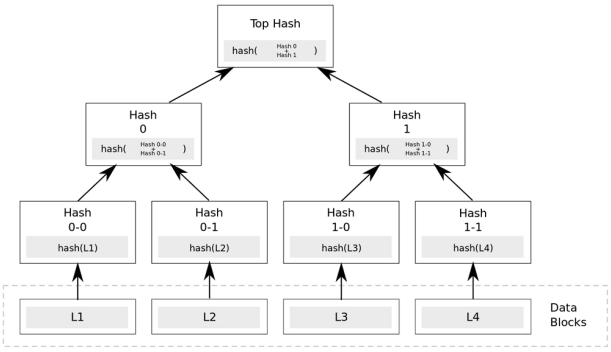

그림 1 Merkle tree의 구조

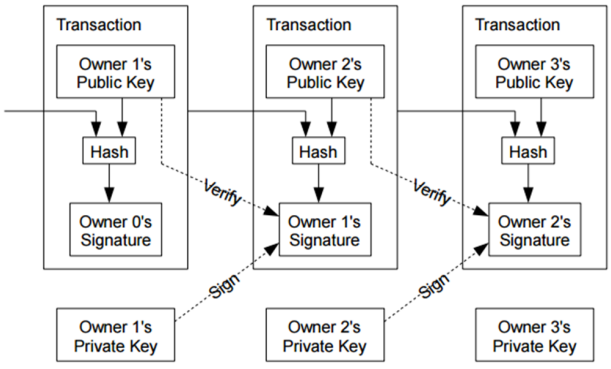

그림 2 블록체인에서의 공개키 기반 서명 방식의 사용 예시

사용하여 해당 거래에 대해 서명을 하고 이에 대응되는 자신의 공개 키와 함께 블록체인 네트워크에 거래 정보를 전송한다. 이 거래 정보를 받은 다른 모든 참여자들은 거래에 담긴 송신자의 공개 키를 이용하여 해당 거래의 유효성을 검증하고 이를 통해 그 거래는 블록체인의 참여자가 보냈음을 확인한다.

2.3 분산 장부

분산 장부는 참여자들 간의 합의에 의해 복제되고 공유, 동기화된 정보의 기록 저장소[3]이다. 특히 분산 장부가 P2P 네트워크상에서 적용되기 위해서는 분산 장부의 기록에 대한 참여자들의 합의가 필요하다는 특징을 가지며 이는 블록체인에서도 그 특징을 유지하고 있다. 블록체인에서 분산 장부는 발생하는 모든 거래, 정보들을 참여자들의 검증과정을 거쳐 기록하며, 모든 참여자가 동일한 정보를 유지한다. 거래나 정보를 검증 할 시에는 먼저 참여자 개개인이 유지하고 있는 분산 장부에 이미 기록되어 있는 정보와의 연결성을 확인하고 참여자들 간의 합의를 거쳐 적법한 거래나 정보만이 블록체인의 분산 장부에 저장된다. 거래나 정보를 저장 시에는 이들을 일정 시간동안 누적하여 블록이라는 단위로 저장하고 이 블록 간의 연결성을 부여한 상태에서 분산 장부에 저장한다.

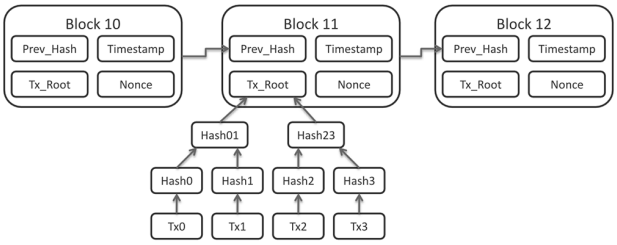

그림 3 분산 장부에 저장되는 블록의 개략적인 구조도

이러한 분산 장부는 블록체인이 제공하는 데이터 무결성 보장의 바탕이 된다. 블록체인에 참여하고 있는 모든 사용자들은 동일한 분산 장부의 데이터를 유지하고 있기 때문에 외부에서 공격자가 특정 데이터를 위・변조하거나 이중거래 등을 시도하기 위해서는 참여자들이 유지하고 있는 분산 장부들 중 절반 이상의 장부들에 대해 공격을 시도해야하기 때문에 높은 비용과 컴퓨팅 리소스가 필요로 한다.

그러나 블록체인의 핵심 기술 중 하나인 분산 장부는 사용자에게 높은 저장 용량을 요구하고 발생하는 모든 정보들을 기록하는 특성 상 요구되는 용량은 지속적으로 증가할 수밖에 없는 구조를 가지고 있어 블록체인의 확장성과 사용성을 제한하는 한계를 지니고 있다.

2.4 분산 합의

분산 합의는 분산 컴퓨팅과 멀티 에이전트 시스템 등의 분야에서 결함이 있는 프로세스가 있는 경우, 전반적인 시스템의 신뢰성을 달성하기 위하여 프로세스나 에이전트 간의 특정 데이터 값에 대한 동의를 이끌어내는 프로토콜이다. 이를 위한 분산 합의 프로토콜은 다음과 같은 성질을 지니고 있다.[4]

유효성(Validity): 모든 올바른 프로세스들이 동일한 데이터를 제안 했다면, 모든 프로세스들은 제안된 데이터에 결정(유효, 무효)을 내린다.

무결성(Integrity): 모든 올바른 프로세스들이 하나의 데이터를 채택하였다면 그 데이터는 다른 프로세스에 의해 제안된 데이터이다.

동의(Agreement): 모든 올바른 프로세스들은 반드시 어떤 데이터에 대해 동의하여야 한다.

종료(Termination): 모든 올바른 프로세스들은 어떤 데이터들에 대해 결정을 내려야 한다.

블록체인에서는 위와 같은 분산 합의 프로토콜 설계하고 이를 통해 발생하는 거래나 정보에 대해 참여자 간의 합의를 이끌어낸다. 합의를 거쳐 적합한 거래나 정보만이 블록체인에서 유지되기 때문에 핵심이 되는 부분 중 하나이다. 또한 어떠한 방식의 분산 합의 프로토콜을 사용하고 있는가에 따라 블록체인의 특징이 구별되어지고 시스템의 신뢰성 또한 영향을 받는다.

대표적인 블록체인 서비스라고 할 수 있는 비트코인의 경우 작업 증명(Proof-of-work)[1]이라는 분산 합의 프로토콜을 사용하고 있다. 이 작업 증명 프로토콜은 참여자들이 블록으로 저장되기 위한 거래 및 데이터들과 SHA-256 해시 함수를 사용하여 시행착오 방식으로 특정 해시 값을 찾아내는 '작업'을 함으로써 참여자간의 블록 정보에 대한 합의를 이끌어내는 프로토콜이다.

그러나 작업 증명 방식의 분산 합의 프로토콜은 평균 약 10분이라는 시간이 소요됨과 동시에 많은 양의 전력과 컴퓨팅 리소스의 낭비 문제가 있어 그 확장성이 떨어지며 실제로도 비트코인 이후에 출시되고 있는 블록체인에서는 사용되지 않는 추세이다. 최근 출시되고 있는 블록체인은 대부분 지분증명(Proof-of-stake)[6]이라는 투표 기반 합의 알고리즘을 사용하며 보안성은 작업 증명 합의보다 낮아졌지만 합의 속도, 전력낭비 문제를 해결하였다. 이러한 지분증명(Proof-of-stake)을 기초로 하여 (DPoS) 위임지분증명(Delegated Proof-of-Stake)[7], PBFT(Practical Byzantine Fault Tolerance)기반의 Tendermint[8] 등의 합의알고리즘이 개발되어 활용되고 있다.

2.5 스마트 컨트랙트

스마트 컨트랙트는 Nick Szabo에 의해 처음 제시된 전자 상거래를 위한 컴퓨터 프로토콜이다. Szabo는 계약 조건을 실행하는 컴퓨터 트랜잭션 프로토콜[5]로 정의하고 있으며 거래의 신뢰를 위한 중개인을 최소화하는 한편 계약 조건을 충족시키고 악의적인 예외를 최소화하는데 그 목적이 있다.

블록체인에서는 이와 같은 스마트 컨트랙트를 지원함으로써 중개 혹은 중앙 기관 없이 거래 당사자 간의 자동화된 직접 거래를 가능케 하며, 그 조건과 결과를 모두 분산 장부에 유지함으로써 거래 정보의 신뢰성과 무결성을 보장한다. 즉, 사용자는 자신이 원하는 조건을 담은 프로토콜 스마트 컨트랙트를 프로그래밍하여 블록체인에 저장하고, 특정 조건이 만족되면 해당 스마트 컨트랙트는 다른 블록체인 참여자들에 의해 검증 및 실행이 된다. 실행 결과는 다시금 블록체인에 저장되어 거래 결과에 대한 정보의 무결성과 신뢰성 또한 보장한다. 이와 같은 개념은 이더리움 블록체인에서 처음 상용화되었으며 금융 거래뿐만이 아닌 새로운 컴퓨팅의 개념으로 받아들여지고 있다. 특히, 컴퓨팅 파워를 가진 기기 간의 자동, 자율적 협업 및 제어가 블록체인의 스마트 컨트랙트로 가능 할 것으로 전망된다.

3. 국내외 블록체인 동향

현재 많은 산업계와 학계에서는 블록체인의 기반 기술의 한계점을 해결하고 타 산업과의 융합을 추진해 나가고 있다. 가장 먼저 기존 비트코인 블록체인의 대표적인 문제점인 느린 검증 속도, 블록체인의 저장을 위한 100GB의 데이터 낭비 등은 대부분 해결되고 있다. 우리 사회에서 실제로 어떻게 블록체인이 이용되고 있는지 확인하기 위해 본 장에서는 블록체인 국제 현황을 분석하며 이에 기반 한 기술 및 응용 서비스, 동향에 대해 소개한다.

3.1 블록체인 기반 산업 시나리오

블록체인은 4가지 기반 기술을 토대로 하여 금융 산업을 시작으로 다양한 산업으로의 진출을 앞두고 있다. 이는 블록체인의 장점인 투명성, 신뢰성, 보안성에 대해 산업계의 관심이 커지고 있기 때문이다.

금융권에서는 먼저, 가상화폐를 이용한 금융 서비스를 시작으로 개인 인증, 금융 문서 관리, 보험등에 관심을 보이고 있다. 현재 일본에서는 정부와 대기업에서 비트코인을 활용한 산업을 준비 중이며, 또한 가상화폐를 이용한 세계여행, 투자등 사람들의 참여가 가장 활발하게 이루어지고 있다. 최근 은행권에서 사용성이 떨어지는 공인인증서를 대체할 방안으로 블록체인을 활용하려 한다.

금융권에서의 블록체인 응용 서비스가 세계적으로 출범하자, 비금융권에서도 블록체인 기술에 관심을 가지기 시작하고 있다. 먼저 금융권에서 사용되고 있는 블록체인 인증 기술을 토대로 IoT, 특허, 예술품 등 인증 기술 및 인증서가 적용되는 산업에 적용되고 있다. 또한 분산화 된 환경이라는 동일한 특징을 가지고 있는 공유경제에서도 같은 흐름을 보이고 있다. 공유 경제의 대표 주자인 Airbnb(에어비앤비)에 적용할 수 있는 이더리움 스마트 컨트랙트를 이용한 자산 공유 서비스인 Slock.it이 2015년 개발되었다. WEF(세계경제포럼)에 따르면 2025년 글로벌 GDP의 10%가 블록체인에 저장 될 것이라고 보고[9]되고 있는 것처럼 블록체인에 대한 산업계의 전망은 높다고 본다.

3.2 국내 블록체인 기업 현황

현재 국내 블록체인 전문 기업은 10개이며, 대표적인 기업으로는 코인플러그, 블로코, 코빗, 코인원 등이 있다. 국내 기업들은 비트코인 등 가상화폐 거래를 지원하는 거래소와 블록체인 기반 응용 서비스를 제공하는 SI 기업으로 구분한다.

최근 국내의 대표적인 블록체인 전문 거래소인 코인원은 세계 3위 규모의 이더리움 거래소로 성장하는 등 가상화폐 투자 및 거래소는 활발하지만 국내 블록체인 응용 서비스 기업들의 활약은 아직까지 미비하다. 하지만 각 기업들은 블록체인 기술 분석 및 개발을 통해 신규 응용 서비스를 준비하고 있으며, IBM이 주도하는 'HyperLedger' 컨소시움에 참여하는 등 국제적인 경쟁력 확보를 위하여도 노력하고 있다.

이 외에도 국내 블록체인 전문 기업들은 비트코인을 이용한 외환 거래 서비스, 블록체인 기반 문서 무결성 보증 서비스 등 개인 인증 서비스외에도 많은 금융 세부 분야에 블록체인을 접목하기 위해 준비 중이다.

국내 대기업 또한 자체적으로 블록체인을 활용한 서비스를 개발하였다. 'HyperLedger'에 참여중인 삼성SDS는 자체 기업용 사설(Private) 블록체인인 'NexLedger'을 토대로 제휴사 회원인증 서비스와 제휴사간 포인트 통합 거래 서비스를 준비 중이며, 자사 생체인증 솔루션인 'Nexsign'과의 연동 또한 지원한다. LG CNS는 국내 대기업 중 가장 먼저 블록체인 기술에

표 1. 국외 대기업들의 블록체인 활용 현황

기업	기업 소개	블록체인 프로젝트
월마트	세계 최대 유통 기업 – 미국	돼지 유통망에 신뢰도 보장을 위하여 블록체인 기술 적용을 통한 유통망 관리 시스템 개발 예정
MAERSK	세계 최대의 컨테이너선 운용 회사 – 덴마크	HyperLedger의 Fabric 블록체인을 사용하여 공급망 관리 과정을 스마트 계약 시스템 테스트 완료
bhpbilliton	세계 최대 광산 업체 – 호주	인증 및 유통 비용 축소를 위해 채굴 암석에 대한 자체 공급망 시스템에 블록체인 기술 적용 예정
알리바바	세계 최대 전자상거래 업체 – 중국	호주 정부와 함께 중국 내 전반적으로 문제가 되고 있는 가짜 음식에 대한 해결책으로 블록체인을 이용한 식품 검증 시스템 개발 예정
NYIAX	세계 첫 광고 거래소 – 미국	광고주와 출판사들이 자유롭게 광고를 거래할 수 있는 광고 계약 거래소인 NYIAX(New York Interactive Advertising Exchange)가 블록체인 기반으로 운용 예정

대한 연구를 시작하며 블록체인을 기반으로 한 비상장주식 거래 플랫폼 파일럿 시스템 개발에 성공하였다. SK C&C의 경우 IBM과 협업하며 블록체인 기반 모바일 디지털 ID 인증 서비스를 통해 제휴사 인증 서비스를 제공하고 있다.

3.3 국외 블록체인 산업 현황

국내에서는 아직까지 비트코인 등 블록체인 1.0에 기반한 응용 서비스를 준비 중에 있지만 국외에서는 이미 스마트 컨트랙트, 신규 합의 알고리즘등 블록체인 1.0의 문제점을 해결하고 보다 발전된 기술을 적용한 블록체인 서비스와 응용 서비스를 준비 중에 있다.

위와 같이 글로벌 기업들이 블록체인에 관심을 가지는 가장 큰 이유는 바로 비용 문제이다. 알려진 바에 따르면 블록체인을 이용할 경우 기존 SW 시스템 비용의 30%가량을 축소시킬 수 있다고 알려져 있다[10]. 또한 블록체인 기술을 통해 자사 품목에 대한 신뢰성 향상을 통한 고객 유치가 높아질 수 있으며, 또한 기존에 문제가 되고 있던 물품 손상, 배송 추적 등이 보다 쉽게 이루어 질 수 있기 때문에 활용도가 높아지고 있다.

이와 같은 블록체인과 스마트 컨트랙트 기술이 적용 가능한 이유는 기존 문서로만 이루어지던 계약 산업이 전자화 되면서 이에 대한 보안성이 중요해졌기 때문이다. 또한 블록체인 기반 기술 아래에서 모든 사물이 동작하게 되면서 네트워크상에서 이루어지는 데이터 또한 신뢰성을 가지게 된다.

대표적으로 운송 시나리오에서 블록체인을 이용한 신뢰 보장을 확인할 수 있다.

1) 운송 이해관계자들은 스마트 컨트랙트를 통하여 계약서를 작성한다.

2) 상품이 운송되며 센서를 통해 전달되는 기록들이 스마트 컨트랙트를 통하여 블록체인 상에 기록되며 이해관계자들은 블록체인을 통하여 언제든지 기록을 확인 할 수 있다.

3) 스마트 컨트랙트는 운송상에서 전달된 거래 중 계약된 내용에 벗어난 내용이 있을 경우 계약에 따른 패널티나 알림 행위를 실시한다.

4) 운송이 완료 된 후, 가상 화폐를 이용하여 계약에 따른 비용을 지불한다.

3.4 블록체인 전문 컨소시움

현재 블록체인 네트워크는 약 800개 이상 존재한다. 이 외에도 각 기업들이 추진 중인 자체 블록체인 기술까지 포함된다면 약 3000여개 이상의 블록체인 네트워크가 존재한다. 이렇게까지 많은 블록체인 네트워크가 존재하는 이유는 바로 각 기업이 원하는 블록체인의 요구사항이 다르며 이에 맞는 기반 기술을 적용하여 차이점이 존재하기 때문이다. 블록체인의 다양성은 블록체인 기술 공유의 부재로 생긴 문제점이다. 기업들은 이러한 문제점을 인식하여 산업 도메인에 따른 컨소시움을 구성하여 이에 적합한 기술 공유를 시도하고 있다. 대표적으로 금융 컨소시움인 'R3CEV', 'ChinaLedger'과 산업 플랫폼인 'HyperLedger' 등이 있다. 그리고 최근 IoT 분야에 블록체인 기술을 적용하기 위해 Bosch, Cisco, Foxconn 등 글로벌 테크 기업들이 컨소시움을 구성하였다. 가장 잘 알려진 컨소시움인 'R3CEV'의 경우 글로벌 금융 기업의 대부분이 참가하며, 국내에서는 하나은행과 신한은행이 약 3억원의 금액을 지불하고 가입을 하였다. 'HyperLedger' 의 경우 실제 응용서비스에 블록체인을 이용하기 위한 컨소시움으로 Linux 재단, Microsoft, IBM, LG, 삼성SDS 등 세계 유수의 IT와 HW 기업들이 참여 하고 있다. 이들은 각각의 기업 도메인 특성에 따른 블록체인 기반 기술을 통해 플랫폼을 구축 중 이며, 현재 IBM의 'Fabric', Intel의 'Sawtooth Lake', 삼성SDS의 'Nexledger' 등의 플랫폼이 시현되었다. IBM의 'Fabric' 경우 모듈형태로 구성하여 사용자가 서비스에 따른 모델 재구성이 가능하게 하였다.

HyperLedger와 같은 컨소시움 구성을 통하여 블록체인에 대한 기업들간의 기술 공유가 쉽게 이루어지며, 프라이빗 블록체인 상에서 문제가 되고 있는 노드 확보 문제를 해결할 수 있게 되었다. 또한 하나의 기본 프레임을 통하여 기업만의 요구사항에 맞는 블록체인 구성이 가능해진 것도 장점이다.

3.5 블록체인 지원을 위한 정부 정책의 방향

블록체인에 대한 산업계의 관심이 커지면서 이를 지원하기 위한 정부 차원의 정책 논의가 각 국가에서 시작되고 있다. 현재 블록체인을 활용한 직접적인 사업을 준비 중인 국가와 블록체인 산업을 지원하기 위한 정책 준비를 하는 국가로 나뉘어져 있다. 전자의 경우, 현재 에스토니아에서는 블록체인 투표 시스템을 개발하고 있으며 온두라스에서는 국가 토지대장 관리를 위해 블록체인 기술 도입을 추진하고 있다[11]. 후자의 대표적인 국가는 미국으로 블록체인 산업의 선두주자이지만 국가 차원의 활용보다는 산업을 지원하기 위한 정책 연구를 하고 있으며, 주정부감독당국협의체가 디지털통화 테스크 포스팀을 구성하여 가상화폐에 대한 표준규제체계 마련과 블록체인 지원을 위한 규제 완화를 준비 중 이다.

표 2. 국내 정부기관의 블록체인 지원 현황

기관명	내용
금융위원회	– 금융 위원회의 3조원 투자 규모의 '2단계 핀테크 발전 로드맵' 기본 방향에 블록체인 연구 포함 – 블록체인 협의회 출범 및 금융권 공동 블록체인 컨소시움 운영 – 개인 인증 적용 방안을 위해 '범금융권 공동인증 TF' 결성
미래과학부	– 블록체인 확산을 지원하기 위한 규제 개선 정책 연구 추진 – 블록체인 활용 가능성을 검증하기 위한 시범 사업 예정 – 블록체인 기초 연구를 위한 R&D 사업에 약 300억 규모 투자
KISA (한국인터넷진흥원)	– 블록체인 TF팀, 암호화기술팀 구성 – 블록체인 지원센터 개설 예정 – 블록체인 오픈 포럼 출범 지원 – 블록체인 테크비즈 컨퍼런스, 핀테크 블록체인 해커톤 개최 – 핀테크x블록체인 아카데미 운영
경기도	– 주민공동체를 대상으로 한 주민제안공모심사에 블록체인 기반 투표 시스템 이용 – 경기도의료원 산하 병원에 대한 병원비 지원 관리에 블록체인 기술 도입 – 경기도 내 농산물 인증인 G마크에 블록체인 활용 방안 검토 중

우리나라의 경우 블록체인 시장에 대한 진입이 늦어지며 이에 대한 정부 정책 지원 또한 늦어지고 있다. 하지만 최근 위의 표 2 같은 움직임을 보이며 블록체인 지원을 위한 관심을 보이고 있다.

4. 결 론

블록체인에 대한 산업계와 정부의 관심은 더욱 커지고 있다. 또한 각 국가들이 4차 산업혁명 시대에 핵심 기술을 선점하기 위해 블록체인에 참여하는 기업과 정부가 증가하고 있다. 그리고 많은 학계에서 블록체인 연구센터 및 학회를 설립하여 연구 중이며, 기업체 블록체인 전문 연구센터 설립을 통해 신규 블록체인 적용 방안을 연구 중이다.

한 보고서에 따르면 블록체인 시장은 2024년까지 770억 달러까지 증가하며, 매년 평균적으로 37%씩 성장할 것이라고 예상[12]한다.

많은 연구와 함께 블록체인 적용 산업 범위가 커지며 최근 각 산업 별 블록체인 연동에 대한 논문들이 많이 게재되고 있다. 또한 사회적으로 문제가 되고 있는 식품 안전, 사기 범죄, 고수수료 등의 신뢰 보장의 문제를 해결할 수 있는 산업에 대한 실제 기업들의 응용 서비스들이 개발 되고 있다. 앞으로 4차 산업혁명의 핵심 분야 인 IoT 산업에서 기기간의 통신 환경에 보안성을 확보하기 위해 블록체인이 활용될 가능성이 높으며, 중국에서는 스마트 시티 구축에 블록체인을 기반 인프라로서 개발 할 예정이다. 이러한 상황에서 미래의 블록체인 산업은 다양한 분야에서 우리 인류의 생활에 신뢰 기반 인프라로서 자리 매김 할 것이라 예상된다.

그러나 기존 데이터베이스 시스템의 성능을 따라가지 못하는 한계점이 존재하며, 보안성을 높이면 발생하는 속도 저하, 사용 용량의 문제등을 완벽하게 해결하지 못한 문제점이 존재한다. 또한 현재 블록체인이 가지고 있는 탈중앙화의 가치를 훼손하는 문제점도 대두되고 있다. 따라서 보다 신뢰성 있는 세상을 만들기 위해서는 블록체인이 필수적인 기술이나 많은 연구가 지금보다 더 수행되어야 한다.

참고문헌

[1] NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption Function". Advances in Cryptology — CRYPTO '87. Lecture Notes in Computer Science. 293. p. 369. doi:10.1007/3-540-48184-2_32. ISBN 978-3-540-18796-7.

[3] Distributed Ledger Technology: beyond block chain (Report). UK Government, Office for Science. January 2016

[4] Coulouris, George; Jean Dollimore; Tim Kindberg (2001), Distributed Systems: Concepts and Design (3rd Edition), Addison-Wesley, p. 452, ISBN 0201-61918-0

[5] NICK SZABO.(1997) "Smart Contracts: Formalizing and Securing Relationships on Public Networks", First Monday, Volume 2, Number 9 - 1 September 1997, doi: http://dx.doi.org/10.5210/fm.v2i9.548

[6] VASIN, Pavel. Blackcoin's proof-of-stake protocol v2. 2014.

[7] LARIMER, Daniel. Delegated Proof-of-Stake (DPOS).

Bitshare whitepaper, 2014.
[8] KWON, Jae. Tendermint: Consensus without mining. URL http://tendermint. com/docs/tendermint {_} v04. pdf, 2014.
[9] Deep Shift: Technology Tipping Points and Societal Impact(Report). Global Agenda Council on the Future of Software & Society, World Economic Forum. September 2015
[10] LG Business insight: 블록체인 비트코인을 넘어 세상을 넘본다(Report). LG경제연구원. August 2016
[11] Issue Monitor: 블록체인이 가져올 경영 패러다임의 변화, 금융을 넘어 전 산업으로(Report). 삼정KPMG 경제연구원. September 2016
[12] Next Generation Technologies: Blockchain Technology Market Analysis By Type, By Application, By Region, &Segment Forecasts, 2015-2024(Report). Grand View Research. December 2016

약 력

이 동 영

2016 서강대학교 컴퓨터공학과 졸업(학사)
2017~현재 서강대학교 컴퓨터공학과 석사과정
관심분야: 소프트웨어 공학, 블록체인, 분산 파일 시스템
Email: freesam02@naver.com

박 지 우

2016 서강대학교 컴퓨터공학과 졸업(학사)
2017~현재 서강대학교 컴퓨터공학과 석사과정
관심분야: 소프트웨어 공학, 블록체인, 알고리즘
Email: desjin2002@naver.com

이 준 하

2007 단국대학교 컴퓨터공학과 졸업(학사)
2010 서강대학교 컴퓨터공학과 졸업(석사)
2014 서강대학교 컴퓨터공학과 졸업(박사)
2014~2015 Kettering University General Motors Institute 박사후 과정
2015~현재 Magna International in North America, Systems Engineer
관심분야: 자동차, CAN 통신, 블록체인
Email: zuna.lee@gmail.com

이 상 록

2011~현재 서강대학교 철학과 학부과정
관심분야: 소프트웨어 공학, 블록체인, 핀테크
Email: vhdys251@gmail.com

박 수 용

1986 서강대학교 전자계산학과 졸업(학사)
1988 미국 플로리다 주립대학교 컴퓨터학과 졸업(석사)
1995 미국 조지메이슨 대학교 정보기술학과 졸업 (박사)
1996~1998 TRW ISC 선임 소프트웨어 개발자
1998~2002 서강대학교 컴퓨터공학과 조교수
2002~2007 서강대학교 컴퓨터공학과 부교수
2003~2004 한국정보통신대학교 객원교수
2003~2006 미국 카네기멜론대학교 컴퓨터공학 객원 교수
2009~현재 서강대학교 공학부 컴퓨터공학 교수
관심분야: 소프트웨어 공학, 핀테크, 블록체인, 요구 및 검증 공학 기술
Email: sypark@sogang.ac.kr