

표준화 동향

블록체인

표준화 동향 2017-02



표준화 동향

블록체인



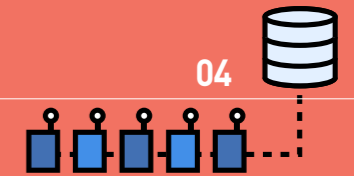
본 저작물은 공공누리 제4유형: 출처표시+상업적이용금지+변경금지 조건에 따라 이용할 수 있습니다.

Contents

블록체인

1. 배경 및 필요성

- 블록체인의 이해
블록체인의 기술적 이해
블록체인 기술 활용
클라우드 기반의 블록체인 서비스
블록체인 장단점



2. 블록체인 표준화 동향

- 블록체인을 표준화 동향
ISO/TC 307 표준화 동향
ITU-T 표준화 동향
WC3 표준화 동향
국내 표준화 동향
전망 및 대응방안



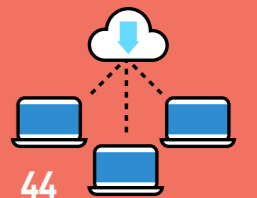
3. 블록체인의 진화: Ethereum, Hyperledger 32

- 블록체인을 활용한 새로운 시도
이더리움(Ethereum)
• 스마트 계약을 이용한 클라우드 펀딩
Hyperledger



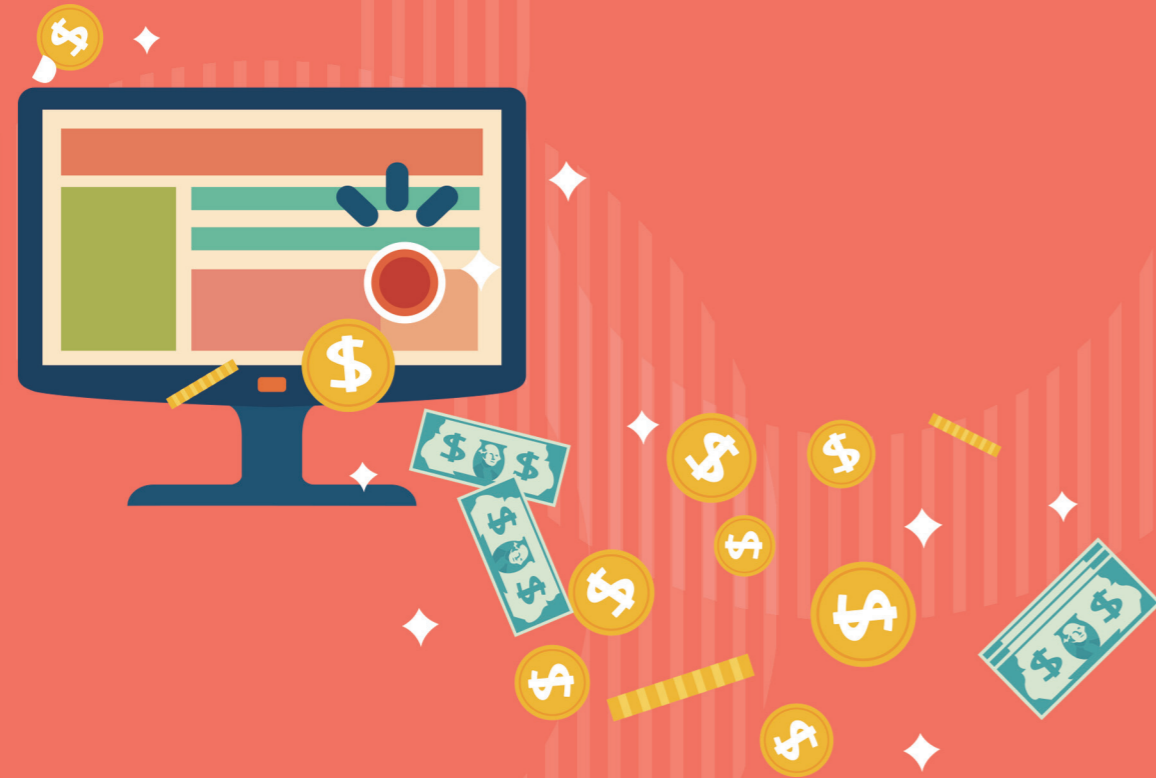
4. 결론 및 시사점

- 블록체인의 미래
블록체인 표준화의 중요성



1. 배경 및 필요성

"인터넷이 지난 30년을 지배했다.
 앞으로는 블록체인(blockchain)이 우리 미래를 30년 이상 지배할 것이다."
 미국 돈 탭스콧 경영 컨설턴트가 블록체인에 던진 찬사다.
 블록체인은 분산 시스템을 기반으로 한 새로운 형태의 보안 기술로,
 지금까지의 기술 중 최고의 보안기술로 손꼽힌다.
 비트코인이라는 암호화폐가 유명해지면서
 그 토대가 된 블록체인이 덩달아 주목을 받았지만
 암호화폐는 단지, 시작일 뿐이다.



블록체인의 이해

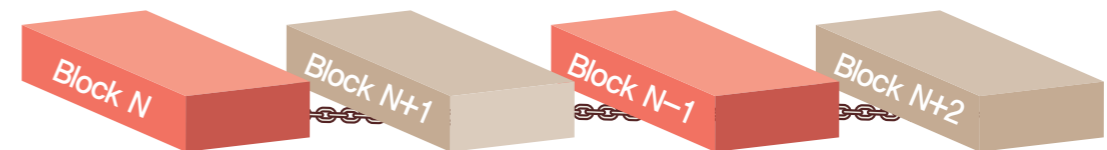
블록체인의 가장 큰 특징은 기존 중앙 통제 방식에서 벗어난 분산된 구조로 이루어지고, 분산구조임에도 중앙 통제 방식 이상의 효과를 거두는데 있다. 블록체인 기술은 기본적으로 중앙통제 방식보다 보안성 및 투명성이 더욱 높고, 금융뿐만 아니라, 공공, 사회, 문화 등 모든 면에서 포괄적으로 활용이 가능함이 증명되고 있다. 이에 실제 산업 전반적인 부분에서 적용을 위한 활발한 기술 개발과 표준화 작업이 진행 중에 있다. 본 장에서는 블록체인의 기본적인 기술적 이해부터 표준화 현황 및 금융권에서 활발히 논의 되고 있는 블록체인 2.0에 대한 고찰을 하고자 한다.

블록체인의 기술적 이해

블록체인이란?

블록체인은 P2P네트워크기반으로 거래 내역이 담긴 장부(帳簿)를 거래에 참여한 모든 구성원에게 분산하여 저장하는 기술을 말한다. 다른 말로 '분산 원장 기술' (Distributed Ledger Technology)이라고도 부른다. 거래 내역을 한 곳에 모아 저장하는 중앙 집중적인 시스템이 아니고 정보를 분산하는 형태이기 때문에 보안성이 좋고, 데이터 보호에 드는 비용을 줄이는 효과가 있다.

실행 측면에서 살펴보면 여러 건의 거래내역이 일정 시간마다 하나의 블록(Block)으로 묶여, 기존 생성된 블록에 체인(Chain)처럼 연결하여 기록을 연속적으로 보관하는 것이다. 새로 생성된 블록들은 이전 거래 내역의 검증 데이터를 연계하여 블록을 생성하기 때문에, 블록이 쌓일수록 보안이 강화되는 구조를 갖는다[아래 그림 참조]. 다시 말해, 각 블록들은 그 이전에 생성된 블록들의 모든 내역에 대한 검증 기록을 가지고 있게 되며, 한번 등록되면 변경이 불가능한 구조이다.



블록체인 개념도

분산 원장 기술 (Distributed ledger technology)이란?

분산 원장은 거래(트랜잭션)가 발생했을 때 거래 내역을 중앙의 장부에 기록을 보관하는 기존의 방식과 달리, 거래 구성원(참가자) 모두에게 내용을 공개하는 분산형 디지털 장부다.

지금까지의 은행거래를 떠올려보면 분산원장과의 차이점을 쉽게 파악할 수 있다. 은행에 돈을 맡기게 되면 은행은 내부에 소비자가 돈을 맡긴 기록을 꼼꼼하게 기록하고 관리한다. 제3의 기관에서 원장을 관리하는 것으로, 중앙 집중형 원장관리라고 한다. 즉 은행과 같이 신뢰할 수 있는 검증된 제3의 기관을 통하여 거래 내역을 관리하는 구조이다. 당연히 일반인은 이 내역을 열람하거나 함부로 조작할 수 없다. 은행을 포함한 금융사들은 지금까지처럼 중앙 집중형으로 관리하기 위해 보안과 관리에 엄청난 투자를 해왔다.

그러나 분산원장은 반대로, 거래 구성원 모두에게 내용을 공개한다. 모든 이용자들이 거래 내용을 자동으로 기록하고 열람하고, 기록된 내역을 바탕으로 새로운 내역을 생성하기 때문에 사실상 내용을 위조하거나 변조할 수 있는 가능성이 없다. 따라서 시스템 구축이나 보안에 드는 비용은 낮아지게 되는 것이다.

구분	중앙 집중형 원장 관리	분산 원장 관리
구조		
유형	중앙 집중형 관리	분산형 관리
공증 및 관리주체	<ul style="list-style-type: none"> · 중앙의 제3자가 모든 거래내역을 공증 · 중앙의 제3자가 모든 거래 내역을 보관/관리함 	<ul style="list-style-type: none"> · 모든 거래 참여자가 거래 내역을 확인하고 공증 및 관리함 · 거래내역이 모든 네트워크 참여자에게 공유되고 보관됨
비용	<ul style="list-style-type: none"> · 유지(관리) 비용 높음 	<ul style="list-style-type: none"> · 적은 시스템 구축 비용 · 낮은 유지보수 비용
특징	<ul style="list-style-type: none"> · 장점: (1)빠른 거래 속도, (2)제어의 용이성 · 단점: 보안에 취약함 (DDos공격 및 해킹에 취약함) 	<ul style="list-style-type: none"> · 장점: ① 거래 정보 투명성 유지 ② DDos공격 불가능 ③ 거래내역 위조가 불가능 · 단점: ① 상대적으로 느린 거래 속도 ② 제어의 복잡성

중앙 집중형 원장 관리 기술과 분산 원장 관리 구조 비교

블록체인의 동작 원리

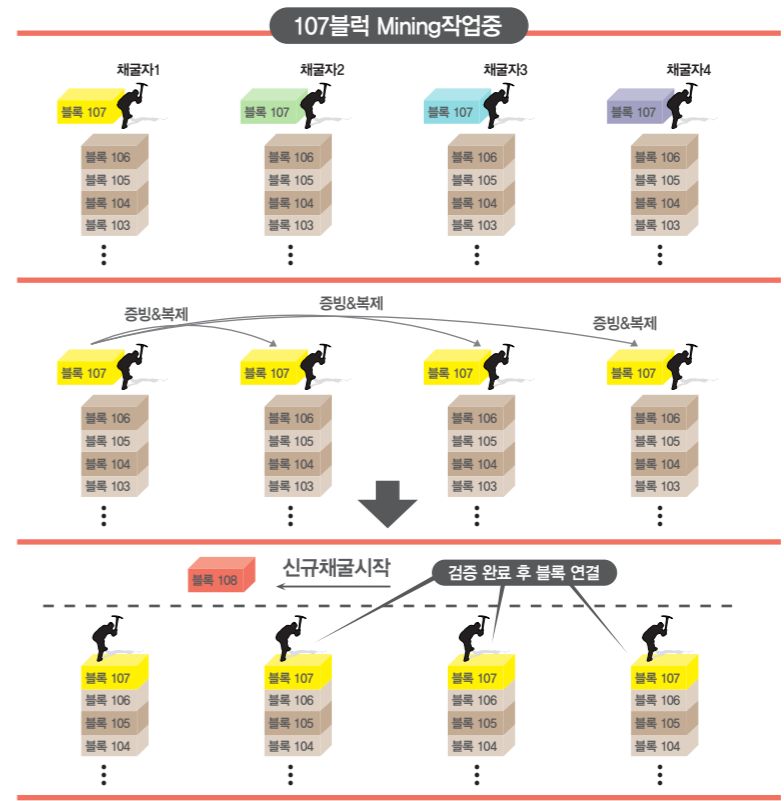
- ① 블록체인은 앞서 언급한 바와 같이 모든 구성원들과의 합의 (Consensus) 체제로 동작한다. 다시 말해 거래(트랜잭션)을 중재하기 위해 금융 기관과 같은 제3의 기관을 이용하는 대신 블록체인의 네트워크의 구성원은 합의(Consensus) 프로토콜을 사용하여 원장 내용의 동의 과정 (작업 증명: Proof of Work)을 거치게 된다.
- ② 작업 증명 과정을 거친 블록은 이전 블록에 새롭게 연결되고, 모든 구성원에 동일하게 저장된다. 이러한 합의 알고리즘의 가장 강력한 특성 중 하나는 조작위험성이 낮다는 것이다. 분산된 원장을 변형하기 위해서는 정확히 동일한 시간에 여러 노드(구성원)에 공유된 원장에 대해서 전체적으로 이루어져야 하기 때문이다.
- ③ 작업 증명(Proof of Work)에는 특정 해시 알고리즘을 사용하는데, 이는 상당한 많은 자원과 시간이 소요되며, 이로 인하여 위조 및 변조 자체가 매우 어려운 특성을 가진다.

비트코인 채굴 과정

* 채굴의 목적
새로운 블록을 만들어주는 역할, 거래 검증 및 승인

* 채굴의 의미
새로운 비트코인 통화 공급 역할을 하는 매우 중요한 과정임

* 분산화된 합의 (작업 증명 후)
각각의 노드마다 독립된 검증 실시. 검증된 거래들을 새로운 블록에 독립적으로 추가함. 모든 노드들이 새 블록을 독립적으로 검증한 후 기존 블록 체인 연결



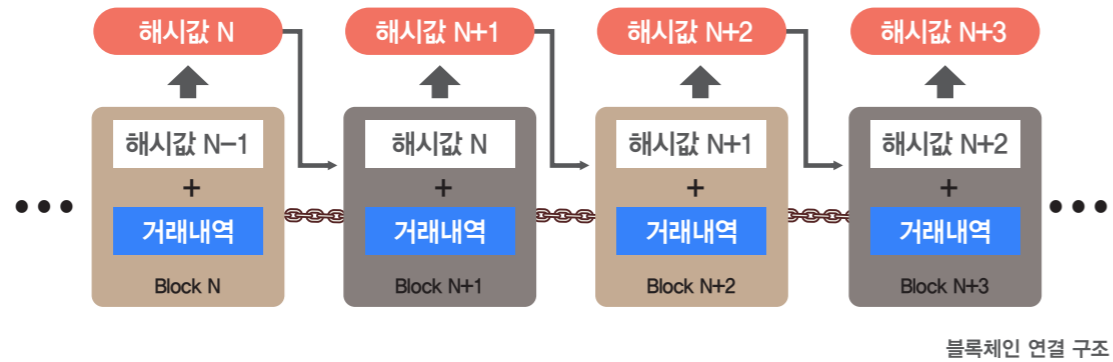
블록체인의 동작 원리(채굴 과정)

블록체인의 구조와 해시

블록체인은 일정시간 동안 진행된 거래 내역을 블록화해서 연결하는데, 이때 블록화의 방법에는 해시(Hash) 알고리즘¹⁾이 이용된다. 구체적으로 일정 시간 동안 모인 거래 내역과 직전 블록에서 전달된 해시값이 포함된 데이터를 대상으로 난스(Nonce)값을 추가하여 새로운 해시값을 구한다.

해시 과정은 미리 합의된 특정 조건을 만족하는 해시값이 도출되도록 난스 값을 계속 조정하면서 계산해보는 것이다. 만일 조건에 맞는 해시값이 도출되었다면 증명과정이 성공한 것이며, 그때의 해시값과 난스(Nonce)값 및 해당 거래내역 등을 묶어서 새로운 블록을 생성하고 직전 블록과 연결하면 되는 것이다.

이때 새로 생성된 블록에는 직전 블록의 해시값도 포함된다[아래 그림 참조]. 이러한 방식으로 계속해서 직전 블록의 해시값이 포함됨으로써 블록 간의 긴밀한 연결이 이루어지며, 조작이 발생했을 때 해시값의 검사를 통해 쉽게 파악되는 구조이다.



1) 해시값은 해시 함수를 이용해서 임의의 데이터로부터 고정된 길이의 난수를 만들어 내는 방법으로 입력값에서 출력으로 계산은 단순하지만, 역으로 출력 값에서 입력 값을 계산하는 것은 거의 불가능하거나 극히 어려운 작업임. 즉 한정된 시간 내에 모든 블록의 해시값을 다시 구해서 특정 블록을 새로 만들고, 구성원의 정보를 조작하는 것은 불가능함. 또한 특정 블록의 내역을 조작하여 새로운 블록을 만드는 데 성공하더라도, 그 블록 이후로 만들어진 모든 블록들을 새로 만들어 구성원의 합의를 받아야 함.

블록체인의 종류

블록체인에는 참여 주체의 네트워크의 성격, 범위 등에 따라 '퍼블릭(공공) 블록체인', '컨소시엄(또는 컨소시엄) 블록체인' 및 '프라이빗 블록체인'으로 분류된다. 현재 널리 알려진 전자화폐인 비트코인은 누구나 참여가 가능한 공공 블록체인에 해당되며, 하이브리드 또는 컨소시엄 블록체인은 여러 기관들이 컨소시엄을 이루어서 블록체인을 운영하는 것으로, 금융 분야에서 은행을 중심으로 컨소시엄 형태로 추진하는 형태를 떠올리면 된다. R3 CEV²⁾가 대표적인 컨소시엄 블록체인이다. 프라이빗 블록체인은 1개의 주체가 모든 권한을 가지고 블록체인을 독자적으로 관장하는 것이다. 허가 받은 대상들만 참여가 가능하다. 아래의 표는 각각의 블록체인 종류별 특성을 간략히 정리한 내용이다.

구분	개념 및 특징	주요 니즈/선결 요건	예시
퍼블릭 블록체인	· 인터넷을 통해 모두에게 공개 운용 가능한 거래장부 · 컴퓨팅 파워를 네트워크에 제공함으로써 누구든 공중에 참여 · 네트워크 확장이 어렵고 거래 속도가 느림	· 네트워크 효과 · 안정적인 Ecosystem · 51% 공격이아 이중송금 위험(Risk) 관리	비트코인
컨소시엄 블록체인 (하이브리드 블록체인)	· 반중앙형 블록체인 · 미리 선정된 N개의 주체들만 참여가능 · N개의 주체들 간의 합의된 Rule을 통해 공중 참여 · 네트워크 확장이 용이하고 거래 속도가 빠름	· 참여 주체들 간의 비즈니스 적인 동의/합의 · 시스템 안정성확보	R3 CEV
프라이빗 블록체인	· 개인형 블록체인 · 1개의 주체가 내부 전산망을 블록체인으로 관리 · Private Blockchain 개발을 위한 플랫폼 서비스도 등장	· 시스템 변경 감수 /안정성 확보 · 1개의 주체 내 글로벌 Branch	나스닥의 비상장 주식거래소 플랫폼인 링크(Linq)

블록체인 유형별 특징 및 예시
[출처: 금융보안원, 국내외 블록체인 활용동향, <http://www.fsec.or.kr>]

2) R3 CEV: 세계 최대의 블록체인 컨소시엄. 20개 대형은행들인뱅크오브아메리카, 씨티그룹, 골드만삭스 등 미국 핀테크 기업 R3와의 제휴를 통해 블록체인 표준 플랫폼 공동 개발

블록체인 기술 활용

블록체인 기술은 비트코인으로 대변되는 암호화폐(Cryptocurrency)가 이슈화 되면서 알려졌지만, 이 외에도 네트워크 및 암호분야에서의 응용과 제공하는 서비스의 기능에 따라 활용범위가 산업 전반으로 확대되고 있다. 초기에는 비트코인과 전자화폐 시스템으로 제안되어 사용되어왔지만, 이더리움과 하이퍼레저 등의 기술 개발로 인해 현재는 '금융' 뿐만 아니라 '공공 및 보안', '전자 결제', '산업응용' 분야 등 다양한 분야에서 활용이 가능하다.

구분	내용
금융	· 금융거래, 해외지불결제, 자본시장, 무역거래, 규제 및 감리, 돈세탁 방지, 고객인증, 보험, P2P거래
암호화폐	· 암호화폐(비트코인, 라이트코인, 리플코인)
공공 및 보안	· 기록물관리, 전자시민증, 전자투표, 세금, 부동산관리, 금융감독, 법률관리, 규제감시, 디지털 계약, 중고 거래, 경매서비스, 논문물 유통 예) 온두라스의 국가 토지 대장
전자결제	· 핀테크, 소액거래, 지불 검증 등에 사용
산업 응용	· 사물 인터넷, 소셜 네트워크, 전자상거래, 헬스케어/의료, 콘텐츠저작권 보호 등으로 활용됨
사회, 문화	· 음원 및 디지털 콘텐츠관리/유통, 티켓 서비스, 미술품 거래

분야별 주요 활용 분야

금융 분야

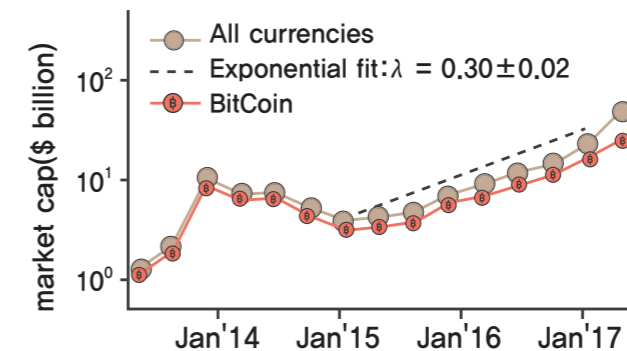
블록체인 기술은 금융 분야에 큰 변혁을 가져오고 있다. 현재의 은행가 사용되는 중앙집중식 처리를 살펴보면, 은행이 고객의 입출금 내역을 승인/기록하고, 중앙은행에서 은행별 잔고를 원장에 기록하고 은행 간 자금이체를 처리하는 방식이다. 이때 제 3의 신뢰할 수 있는 기관을 통하여 신뢰성을 보증한다. 그러나 이러한 방식에서는 해킹 매우 취약하며, 이를 방지하기 위해서는 높은 유지 및 관리 비용이 필요하다. 그에 반해 블록체인 기술을 활용하면 신뢰성이 높은 분산원장 기술을 통하여 적은 비용으로 신속하게 금융 처리 문제를 해결할 수 있다.

3) 비트코인은 가상화폐라는 이름으로 더 많이 알려졌지만, 가상화폐는 사이버머니나페이팔 같은 결제시스템을 포함한 넓은 의미의 단어다. 비트코인은 여타의 가상화폐와 달리 생산주체가 암호화 되어서 일종의 중앙시스템에 종속된 화폐가 아니므로, 엄밀하게는 가상화폐 중 암호화폐에 해당된다.

금융권에서도 이에 대한 중요성을 일찍이 파악하여, 이미 많은 기술 개발과 활용방안이 논의되고 있다. 대표적으로 최근 골드만 삭스 (Goldman Sachs), JP Morgan 등 글로벌 금융기관 22개사가 비트코인전문 기업인 R3 CEV와 제휴하여 공동 블록체인 시스템 개발 및 국제 표준 추진 중에 있으며, 블록체인을 일반 금융거래에 활용하기 위한 기술로 채택하였다. 또한 2016년 1월 JP모건, 웰스파고, 스테이트스트리트, 영국 런던거래소등 금융 대기업이 참가하는 '오픈레저(Open Ledger)' 프로젝트를 세워 기업의 최적화된 블록체인 기술 개발 지원하기로 하였다.

암호화폐 활용 사례

블록체인 기반의 암호화폐의 실제 활용 사례를 널리 알린 비트코인을 시작으로, 현재는 수많은 종류의 암호화폐가 개발 보급되어 있다. 대표적인 것이 비트코인을 비롯하여 이더리움, 리플코인, 라이트코인 등 총 680여종의 암호화폐가 유통되고 있으며, 2017년 기준으로 총액이 600억불을 넘어섰다. 이들 암호화폐는 화폐로서의 기능 뿐만 아니라 각종 금융거래, 주식, 보험, 투자들에 활용되고 있으며, 실제 물건 거래에도 활용되고 있다. 다음 그림은 2017년 6월에 유통되고 있는 전체 암호화폐의 시가총액 추이를 나타낸 것이다. 2016년에 비교하여 1000% 가까이 증가한 것을 볼 수 있다.



전체 암호화폐 시가총액 변화 추이 및 상위 10종의 시가 총액
[출처: 코인마켓캡닷컴, <https://coinmarketcap.com/>]

공공 및 보안

블록체인을 통한 공공분야에서는 더욱 다양한 분야에서 적용이 가능하다. 공공 기록물을 비롯하여, 전자 시민증, 부동산 거래, 토지 대장 및 유통 관리 등에 활용 될 수 있으며 실제로 많은 곳에서 적용되고 있다. 대표적인 사례는 온두라스에서 국토의 토지 대장 관리에 블록체인 기술을 도입한 것이다. 온두라스는 작은 섬나라로 부정·부패가 많아 정부 관료들이 토지대장을 조작하는 일이 발생하는 등 안전한 토지대장에 관리가 어려웠다. 이에 토지계약 시스템을 블록체인에 적용하는 방안으로 해결책을 찾았다.



온두라스

에스토니아는 2016년 3월 e-government system 프로젝트의 일환으로 국가 차원의 블록체인 망을 구성하여 주민 관리, 건강 기록, 금융 기록, 전자 선거 서비스를 제공하고 이를 토대로 나토 사이버 방어 사령부, 유럽 연합 IT 서비스 본부 등을 유치한다고 발표하였다. 이외에 농산물 유통 관련하여 미국 팜웨어(FarmStare)는 ConsenSys기업과 함께 지역 사회의 농산물 유통을 지원하는 이더리움 기반의 블록체인 플랫폼을 구축하여 운용중이다.

블록체인은 안전하고 투명한 전자 투표에서 활용이 가능하다. 실제 미국에서 2016년도 대통령 선거 과정 중 유타주에서 공화당 대통령 후보지명에 블록체인 기반의 투표를 실시한 바 있다.

전자 결제

신한은행은 핀테크 전문 기업인 '스트리미', 영국의 핀네트 업체 및 연구 기관과 전략적인 업무를 제휴/협업하여 외환송금 시스템을 공동개발 중이다. 또한 비대면 인증정보가 가능한 디지털 키오스크를 실행하여 보다 안전한 자료보관을 할 수 있는 서비스를 시행하고 있다.

KB국민카드는 블록체인(Block Chain) 기술을 활용한 개인인증 시스템 즉 '간편인증 서비스'를 도입하였다. 개인인증 시스템 도입은 앞으로 결제 등의 금융서비스를 사용할 때 별도의 공인인증서가 필요 없어진다는 것을 의미한다. 금융고객들이 공인인증서를 발급 받고 매년 만기 때마다 이를 재발급 받는 불편함이 사라지게 된다. KB금융에서는 또한 블록체인기반 해 외송금서비스 기술검증에 성공하여 안전하고 빠른 해외송금 서비스를 제공할 수 있는 기반을 마련하였다. 또한 국내 최초로 블록체인 기반 증빙자료 보관서비스를 실시하여 비대면 실명확인 시스템을 구축하였다.

이외에서 NH농협은행, 하나금융그룹, IBK기업은행, 전북은행 및 KB저축은행 등에서도 블록체인에 기반한 핀테크 개발이 활발히 이루어지고 있다.

산업 응용

사물 인터넷 분야에서도 블록체인 기술은 활발히 논의되고 있다. 대표적으로 IBM에서 삼성전자와 함께 사물인터넷에 적용 가능한 어덱트(Adept)를 개발하였다. 어덱트는 블록체인 구조와 텔레해시 프로그램 및 비트토렌트 기술을 활용한 IoT플랫폼이다. 블록체인 같은 장부 시스템에 각각의 디바이스를 등록하고 기기들 사이의 통신 역시 비트토렌트(P2P 파일 공유 프로토콜), 텔레해시(P2P 암호화 프로토콜) 같은 P2P 방식으로 구현하겠다는 것이다. 이처럼 IBM이 P2P방식을 활용하는 이유는, 사물인터넷 기기 수가 대폭 증가하면서 지금과 같은 중앙집중화된 네트워크로는 수십 억개에 달

하는 사물들의 원활한 사용성을 장담할 수 없기 때문이다. 따라서 보다 분산적이고 효율적인 구조가 가능한 기술이 필요했고, 블록체인의 P2P 분산 네트워크를 그 해답으로 찾은 것이다.

또 다른 예로 2017년 NIA는 'IoT 활성화 기반조성 시범사업'을 통해 IoT 수요확산, 이용자 활성화를 위한 융합서비스 모델 발굴을 위해 블록체인 기술을 활용한 신규 플랫폼·서비스 개발을 통한 'IoT 융합 서비스 실증사업'을 추진하고 있다.

사회, 문화

사회나 문화 측면에서는 폭 넓은 블록체인 기술의 활용이 가능하다. 한 예로 저작물 기록에의 활용을 들 수 있다. 블록체인 방식으로 기록을 저장하면, 블록체인은 특성상 가장 먼저 기록하고 저장된 것에 대한 기록이 남기 때문에 설령 다른 사람이 그 뒤에 저작권을 주장하더라도 처음 저작권에 대한 보호를 받을 수 있다.

**클라우드 기반의
블록체인 서비스**

클라우드 기반의 블록체인^{BaaS: Blockchain as a service}
필요성 및 장점

블록체인 기술은 근본적으로 신뢰성을 담보하는 중앙 집중적인 기관이 필요 없으며, 전자금융 거래 분야에서 높은 보안성을 제공한다. 또한 운영비용 측면에서 획기적인 절감을 가져올 것으로 보인다. 따라서 최근 금융권에서 높은 관심을 보이고 있으며, 더불어 글로벌 IT 업체(MS, 아마존, IBM 등)들도 이에 대한 중요성을 인식하여 관련 서비스를 준비하고 있다. 특히 클라우드 서비스를 제공하는 기업에서 이에 대해 활발히 준비를 하고 있는 것으로 파악된다. 그렇다면 클라우드 서비스를 기반으로 하는 블록체인은 어떤 장점이 있는지 알아보자. 기업에서 클라우드 환경을 제공하기 위해선 기본적으로 서버가 필요하다. 그러나 블록체인 기술을 이용한다면 사용자들이 조금씩 저장 공간을 내놓고 이를 P2P형태로 관리할 수 있다. 이 경우 해커들이 공격할 수 있는 중앙 서버가 없기 때문에 보안 측면에서도 보다 안전하다. 실제로 메이드 세이프라는 스타트업은 분산된 클라우드 저장소 서비스를 만들었고, 데이터를 올린 본인만 암호를 해독해 데이터를 활용할 수 있도록 하였다. 클라우드 인프라의 이점 위에 블록체인의 서비스 개발 시간 단축, 개발 용이성 등의 이점을 더한 것이다. 아래의 표는 이러한 관점에서 클라우드 기반의 블록체인에 대한 장점을 보인 표이다.

구분	내용
원활한 블록체인 프로비저닝	PaaS 환경의 일부로써 블록체인을 생성할 수 있는 매우 간단한 모델 제공 가능
탄력적인 확장성	블록체인 네트워크에 노드를 추가하고 제거하는 작업이 단순하여 탄력적인 확장성 확보
글로벌 가용성	클라우드 환경에서는 세계 어떤 지역에서도 블록체인 프로비저닝(Provisioning: 사용자의 요구사항에 맞게 시스템 자원을 실시간으로 할당, 제공하는 서비스)이 가능
단순한 프로그래밍 모델	기본적인 블록체인 인프라를 추상화하여 블록체인 응용프로그램을 만드는 단순한 프로그래밍 모델을 제공

클라우드 기반 블록체인 서비스의 장점

클라우드 기반의 블록체인 기술의 산업계 현황

클라우드 서비스를 제공하는 글로벌 IT 업체에서는 각자의 클라우드 서비스 환경에서 블록체인 기술을 활용한 다양한 서비스를 개발하여 제공하기 시작했다. 아래는 각각의 업체별로 현황을 정리한 것이다.

▶ Microsoft

2015년 블록체인 기술을 이용한 클라우드 서비스로서 자사의 클라우드 플랫폼인 애저(Azure)위에 '이더리움(Ethereum) 클라우드 서비스를 구현해 블록체인 플랫폼 개발 업체인 '컨센시스(ConsenSys)'와 손잡고 '이더리움(Ethereum)'을 자사 클라우드 서비스인 '애저' 위에서 '이더리움 클라우드 서비스(Blockchain as a Service now on Azure, ETH BaaS)'로 구현함.

▶ AWS

글로벌 전자상거래와 클라우드 서비스 시장을 주도하고 있는 아마존은 자사의 클라우드 서비스 '아마존 웹 서비스(AWS)' 고객들이 블록체인을 활용할 수 있도록 한다는 계획 하에, 디지털 화폐 그룹(DCG)과 파트너십을 맺고, DCG의 투자를 받고 있는 스타트업과 협업을 진행하고 있음

▶ IBM

2017년 3월 리눅스 재단의 프로젝트 오픈소스 하이퍼레저 패브릭(Hyperledger Fabric)에 기반하여 오픈소스 클라우드 호스트형 블록체인 플랫폼을 개발, 제공하고 있음. 이를 통해 블록체인 도입을 쉽게 해주는 일련의 작업이 가능하며 관리자가 블록체인 네트워크를 설정하는 정책 도구, 역할 할당 도구, 가시성 레벨 도구, 멤버십 관리 도구, 컴플라이언스 준수 도구 등을 용이하게 활용토록 함. 전체적으로 IBM은 안전하고 클라우드 기반으로 동작하는 블록체인 도입 인프라스트럭처 제공을 목적으로 하고 있음

블록체인 장단점

블록체인은 그 특성에 기인하여 앞서 언급된 다양한 분야에서 적용 가능하며, 무수히 많은 장점들이 존재한다. 특히 높아진 보안 능력 및 적은 관리 비용 등에서 많은 가능성을 제시한다. 그러나 블록체인에도 몇 가지 단점이 존재한다. 이 장에서는 이 부분에 대해서 간략히 정리하고자 한다. 아래의 표는 주요한 몇몇 분야별로 현재의 블록체인이 가지는 장단점을 기술한 것이다.

분류	장점	단점
익명성	개인정보를 요구하지 않음. 은행계좌, 신용카드 등 기존 지급수단에 비해 높은 익명성을 제공	불법 거래대금 결제, 비자금 조성, 탈세를 가능함
거래 방식 (P2P)	공인된 제3자(은행 등) 없이 P2P방식으로 거래가 가능함. 불필요한 수수료를 절감할 수 있음	문제 발생 시 책임 소재가 모호함
확장성	공개된 소스에 의해 쉽게 구축.연결.확장이 가능함. IT 구축비용 절감 효과가 있음	결제 및 처리 가능한 거래건수가 실제 거래규모에 비해 낮음
투명성	거래 내역이 공개되어 있어 원칙적으로 모든 거래에 접근가능함. 거래 양성화 및 규제 미용 절감 효과 있음	완벽한 익명성 보장이 어려울 수 있음 (조합에 의한 재식별이 가능함)
보안성	장부를 공동으로 소유(무결성)하기 때문에 보안 관련 비용이 절감됨	개인키의 해킹, 분실 등의 경우 일반적인 해결방법이 없음
안정성	일부 참가자 시스템에 성능 저하에 따른 전체영향력이 미미함	실시간, 대용량 처리가 어려움

클라우드 기반 블록체인 서비스의 장점
[출처 핀테크지원센터, <https://goo.gl/BQ6bMy>]

2. 블록체인 표준화 동향

블록체인 간 데이터를 공유하고

효율적인 생태계를 구축하기 위해 표준화는 필수다.

주요국들은 이미 블록체인 표준화에 팔을 걷어붙이고

왕성한 활동을 벌이는 중이다.

물론 현재는 매우 초기 단로, 기본적인 공통적인 표준 개발을 시작하고 있으나, 향후 다양한 적용 분야로 확대될 것으로 전망된다

우리에게도 주도권 확보를 위한 빠른 전략과 대응이 중요한 시점이다.



블록체인을 표준화 동향

블록체인 기술과 관련된 표준화는 2017년부터 본격화됐다. 국제표준화기구 ISO에는 새로운 TC가 설립되었고, ITU-T에도 분산 디지털 원장에 관련된 포커스그룹이 신설되었다. 또한, 사실 표준화기구인 W3C에서는 커뮤니티 그룹을 통하여 유즈케이스를 개발하고 있다. 국내에서는 블록체인 표준화 포럼을 설립하여 민간 중심의 표준 이슈 발굴을 통한 표준화 추진을 위하여 산업계 의견을 기반으로 표준 분과 활동을 추진하고 있다.

본 장에서는 블록체인 관련한 표준 기구별 주요 개발 현황과 이슈에 대해서 살펴본다.

ISO/TC 307 표준화 동향

표준화 그룹 구성

2016년 9월 ISO의 기술관리이사회는 호주에서 제안한 블록체인과 전자분산원장기술 그룹을 승인했다. 그 결과 TC 307을 신설하고, 작업범위를 사용자, 애플리케이션, 그리고 시스템간 상호운용성 및 데이터 교환을 지원하는 블록체인 및 분산 원장 기술 표준화로 결정하였다. 2017년 4월 1차 TC 307 회의에서는 1개의 신규 표준안 및 관련 작업그룹(WG), 그리고 5개의 연구 그룹(SG)을 신설하였다.

그룹 구성 및 표준화 개발 내용	그룹형태
용어(Terminology) - ISO/IEC 22739 (Blockchain and Distributed Ledger Technologies — Terminology and Concepts) 개발	작업그룹 (WG)
참조 구조, 택사노미, 온톨로지 (Reference Architecture, Taxonomy, and Ontology) : - ISO/IEC 17789 (클라우드컴퓨팅 참조구조)를 포함한 관련 분야의 참조구조 검토 - 참조 구조, 택사노미, 그리고 온톨로지에 대한 표준화 방법 권고 제시 - ISO/IEC 22739 등 관련 그룹 작업 참조	연구그룹 (SG 1)
유즈케이스 (Use Cases) - 블록체인의 일반적인 사용 형태에 따른 유즈케이스 분석 - 기존 유즈케이스 및 응용의 잠재적인 영향을 고려	연구그룹 (SG 2)

그룹 구성 및 표준화 개발 내용	그룹형태
보안 및 개인정보 (Security and Privacy) - 관련 표준 검토 및 블록체인과의 관계 분석 - 블록체인 및 분산원장 기술 관련 보안 및 개인정보 보호를 위한 요구사항 분석	연구그룹 (SG 3)
식별 (Identity) - 식별 관련 표준, 특히 JTC 1/SC 27 WG5에서 개발한, 분석 - 기존의 비즈니스 유즈케이스 및 기능 유즈케이스 분석 - 블록체인 내의 데이터 및 기능에 필요한 식별 타입 도출 - 데이터 무결성 및 접근 제어와 같이 블록체인 외부에서 필요한 식별 관리 요구사항 도출 - 블록체인과 관련하여 식별의 생성, 사용, 그리고 관리에 영향을 미칠 수 있는 규제 검토 - JTC 1/SC 27 WG5 공동 작업 연구 및 협력 작업 그룹(Joint Working Group) 생성의 가능성 타진 - 필요한 경우, 하나 또는 이상의 NWP 및 임시 작업 초안 개발	연구그룹 (SG 4)
스마트 컨트랙트 (Smart Contract) - 기술적 및 법적 관점에서 스마트 계약에 대한 현재 상태 분석 - 스마트 계약의 검증, 집행, 라이프사이클을 포함하는 법적인 상호운용성 고려 - 자동제어, M2M 정보 전달, 라이선스 관리 및 실제 정보의 통합과 같은 다른 도메인에서의 트랜잭션을 포함하는 스마트 계약의 개념 정립 - 프로그램 개발자가 아는 사람들도 조건을 표현할 수 있도록 프로그래밍 방법론, 도메인 특정 언어 적용 고려 - 필요한 경우, NWP 개발	연구그룹 (SG 5)

개발 표준

블록체인 및 분산원장기술과 관련하여 용어에 대한 표준을 개발하고 있는 작업그룹(WG)에서는 ISO/IEC NP 22739를 통해 세 가지의 대표적인 용어 및 개념을 다음과 같이 정의하고 있다.

▶ **원장 (Ledger)**

비즈니스 트랜잭션 기록을 보관하는 정보 저장소

▶ **분산원장기술 (Distributed Ledger Technology; DLT)**

네트워크 상의 일련의 노드에 분산 혹은 분포된 형태로 원장을 저장하는 기술

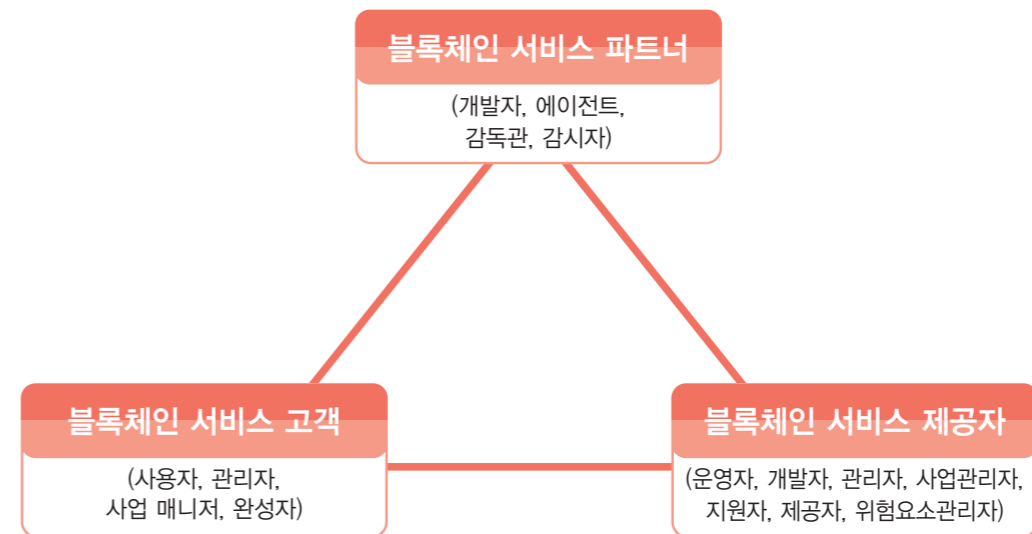
▶ **블록체인 (Blockchain)**

상호 연결된 블록 내에 일련으로 저장된 트랜잭션 데이터베이스로서, ISO/TC 307에서는 블록체인을 분산원장기술(DLT) 중 하나의 개념으로 구분하여 정의하고 있다. 또한, Corda 와 IOTA와 같은 비 블록체인 기반 분산원장기술(Non-Blockchain DLT) 역시 분류체계에 포함하고 있다.

ISO/TC 307 산하 5개의 연구그룹 중 참조구조 및 기술 분류 등을 담당하는 SG1에서는 블록체인 시스템 참조모델, 에코시스템, 그리고 기술 분류 등에 대해 논의하고 있다.

ISO/TC 307에서 바라보는 블록체인 에코시스템에서는 트랜잭션, 공유된 원장, 인증 및 인가, 스마트계약 등의 기술요소 간의 컨센서스 프로토콜을 통해 형성되는 분산원장의 신뢰성을 기반으로 데이터 저장, 생산, 사물인터넷, 금융, 공공 서비스 등의 다양한 응용성을 시사하고 있다.

그 뿐만 아니라, SG1에서는 블록체인 시스템의 참조모델을 다음 그림과 같이 기술하고 있는데, 서비스 파트너, 서비스 제공자 및 서비스 고객의 세 가지 요소로 구분하여 각 요소별 세부 역할을 자세하게 정의하고 있다.



ISO/TC 307에서 제시한 블록체인 기술분류에 따르면, 블록체인 플랫폼 형태는 크게 3가지로 분류되는데 퍼블릭 블록체인, 콘솔시움 블록체인, 프라이빗 블록체인이 있으며, 승인 절차, 보안, 저장, 통신 등의 세부 기술을 바탕으로 전자원장을 관리한다. 블록체인 세부 기술들은 오픈소스 커뮤니티 형태로 개발 및 관리되며, 사용자 개인뿐만 아니라 산업 연합체들이 참여하여 핀테크, 공급체인, 인공지능적 생산공정, 의학 등 다양한 분야에서 활용이 가능한 것으로 정의한다.

ITU-T 표준화 동향

ITU-T에서는 2017년 새로운 회기를 맞이하면서, 분산원장기술 관련 포커스 그룹 신설을 시작으로 SG13, SG16, SG17, SG20 등 여러 산하 표준화 그룹에서 표준개발을 위한 논의를 시작하였다.

ITU-T SG17 및 FG-DLT

ITU-T TSAG (Telecommunication Standardization Advisory Group; 표준화 자문그룹)은 2017년 5월 회의를 통하여 "분산 원장 기술(DLT: Distributed Ledger Technology)"에 대한 포커스 그룹(FG-DLT)을 구성하여 블록체인 이슈에 대한 표준화 작업을 착수하기로 결정하였다. FG-DLT의 블록체인 기술 기반 주요 표준화 항목은 다음과 같다.

- 블록체인 용어정의 **Block chain terminology**
- 디지털 금융서비스 및 비 금융 서비스를 위한 블록체인 유즈케이스 **Blockchain use cases for digital financial services/non-financial services**
- 블록체인 유즈케이스에 기반한 보안 및 프라이버시 위협 **Security and privacy threats and requirements based on blockchain use cases**
- 블록체인 보안 참조 모델 **Security reference architecture for blockchain**
- 블록체인 기반 신원 관리 **Identity management based on blockchain**
- 블록체인 기반 키 입증 **Key attestation based on blockchain**
- 블록체인 응용 및 서비스를 위한 보안 및 프라이버시 가이드 **Security and privacy guidance for blockchain applications and services**

블록체인 기술에 대한 표준화 이슈는 현재 블록체인 기술 관련 표준화 개발을 시작하는 산하 표준화 그룹들 즉, SG17 (보안), SG20 (IoT 연계), SG16 (서비스 프레임워크), SG13 (클라우드 기반 블록체인) 등에서 중요한 이슈다. 따라서 향후 본 포커스 그룹에서 개발되는 표준화 결과의 영향력이 상당할 것으로 예상된다.

특히 보안과 관련된 표준화 이슈를 중점적으로 다루는 표준화 그룹 ITU-T SG17은 3월 첫 총회의 시작과 함께 블록체인에 대한 표준화 현안을 다루기 위한 특별 세션으로 세미나를 개최했다.

제 1세션에서는 블록체인에 대한 기술적 개요로써 분산 원장 기술 및 응용 그리고 블록체인과 보안의 상호 작용에 대한 발표가 있었다.

제 2세션에서는 블록체인의 응용 및 유즈케이스를 주제로 Swisscom 관점에서 보는 다양한 로열티 플랫폼 유즈케이스, 블록체인 솔루션, G-Cloud 상에서의 블록체인 플랫폼 및 암호화폐 유즈케이스, 그리고 블록체인 보안 사고 및 취약점 등을 소개했다.

제3세션에서는 블록체인에 대한 정책 및 규제에 대해서 다루었는데, 그 중에서도 EC-DG-CONNECT의 블록체인과 금융에 관한 유럽 정책, 튀니지의 e-Dinar 및 MobiPoste 등 블록체인의 상업적 활용에 대한 경험과 돈세탁 등 블록체인의 문제점 등을 소개했다. 또한 강력한 법적규제들로 인해 블록체인과 같은 신기술의 활용 가능성이 저해될 수 있는 현실과 이를 극복하기 위한 방안에 대해서 소개했다.

제4세션에서는 블록체인에 대한 온라인 상에서의 보안 및 신뢰성 이슈를 다루었다. 특히, 블록체인 연합 네트워크에서의 인증과 인가, 키 관리와 플랫폼 등 보안적 측면에서의 연구 필요성 등이 제시되었다.

마지막으로 제5세션에서는 현재 블록체인에 대한 표준의 필요성을 강조하면서 FIDA에서의 인증관련 블록체인 연구 동향과 블록체인에 대한 향후 표준화 방향 등의 발표와 함께 패널 토의가 이루어졌다.

이와 같은 세미나 활동 이후, 2017년 8월에 개최된 SG17 총회(의장: 영흥열 교수, 순천향대)에서는 블록체인 기술 표준화 이슈를 다루기 위해 신규 Q14/17 신설을 확정하고 한국대표단 오경희 위원을 라포처로 선임하였다. 그러나, SG17 산하 전체 표준화 워킹그룹(Question) 재구성할 필요성이 제기되어, 이에 대한 논의를 차기 SG17 총회(2018년 3월)까지 마무리하기로 하였다.

이번 총회에서는 전자분산원장 및 블록체인 이슈와 관련된 신규 표준권고안 10건이 제안되었다. 그 중 ISO/IEC TC 307 및 FG-DLT에서 개발 진행 중 혹은 예정인 표준화 항목과의 충돌이 예상되는 2건을 제외하고, 나머지 건들은 총 7개의 신규 표준화 아이템으로 재구성하여 제안을 승인하였다. 승인된 표준권고안들은 신설된 Q14/17에 할당되었으며, 세부내용은 다음 표와 같다.

표준 코드	표준 제목	에디터	승인목표
X.sradlt	Security architecture for Distributed Ledger Technology	KepengLi, Petr Kalambet, Qiwi Kirill Ivkushkin, Bilyk Tatiana, Min Shu (중국, 러시아)	2019년 상반기
X.strdlt	The security threats and requirements for digital payment services based on distributed ledger technology	Kyeong Hee Oh, Chang Oh Kim (한국)	2019년 상반기
X.sct-dlt	Security capabilities and threats of Distributed Ledger Technology	Min Zuo, Ke Wang, Junjie Xia, Zhaoji Lin, Kai Wei (중국)	2019년 상반기

표준 코드	표준 제목	에디터	승인목표
X.ss-dlt	Security Services based on Distributed Ledger Technology	Min Zuo, Ke Wang, Junjie Xia, Zhaoji Lin, Kai Wei (중국)	2019년 상반기
X.dltsec	Privacy and security considerations for using DLT data in Identity Management	Abbie Barbir (캐나다)	2019년 상반기
X.sadlt	Security assurance for Distributed Ledger Technology	Mee Yeon Kim, Heung Youl Youm (한국)	2019년 상반기
X.stov	Security threats to online voting using distributed ledger technology	Keundug Park, ChangOh Kim, Heung Youl Youm (한국)	2019년 상반기

ITU-T Q14/17 표준화 항목 및 세부사항

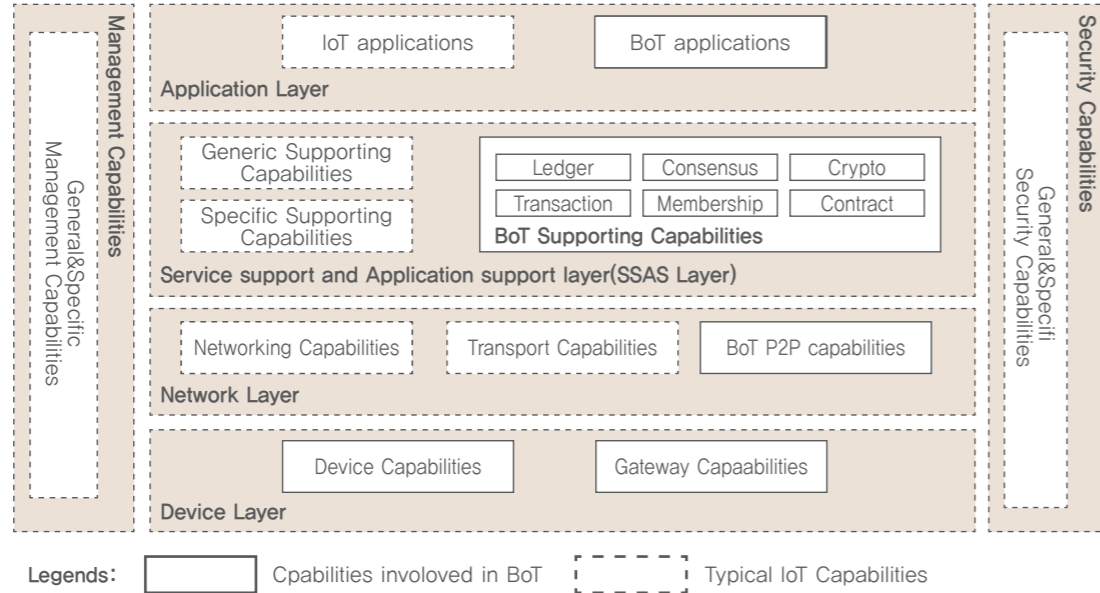
ITU-T Q14/17에서는 상기 할당된 표준권고안 개발을 적극적으로 추진하기 위해 차기 SG17 총회 이전에 두 차례(2017. 10 및 2018. 1)의 라포처 그룹 회의(Rapporteur Group Meeting; RGM)를 개최하기로 결정했다.

ITU-T SG20 및 FG-DPM

사물인터넷 및 스마트시티 응용 관련 표준화 이슈를 다루고 있는 SG20에서는 최근 사물인터넷 기반의 블록체인 기술에 대한 표준화 개발(Y.IoT-BoT-fw)이 중국의 주도로 시작되었다. Y.IoT-BoT-fw⁵⁾(Framework of blockchain of things as decentralized service platform)은 사물 블록체인 (Blockchain of Things) 개념 소개, IoT를 위한 분산화 된 서비스 플랫폼으로서 사물인터넷 블록체인을 위한 공통 기능 및 요구사항 개발, IoT 및 SC&C 애플리케이션 및 서비스의 개선을 위한 블록체인 이점에 대한 비교 분석 등을 표준범위로 확정하고 표준개발을 논의하기 시작했다

아래 그림은 사물인터넷 기반 블록체인 프레임워크의 참조구조를 보여준다. 사물인터넷 참조구조 상에서 블록체인을 위한 기술적 요소들이 추가된 형태로 개발이 시작되었으나, 아직 개발 초기단계이기 때문에 표준개발 방향에 대해서는 좀 더 지켜볼 필요가 있다.

5) https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14099



사물인터넷 기반 블록체인 프레임워크 참조구조

SG20은 2017년 3월 사물인터넷 및 스마트시티를 위한 데이터 처리 및 관리 이슈에 대한 표준화 개발을 논의하기 위해 포커스 그룹 (FG-DPM; Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities)을 신설했다. 2017년 7월 1차 회의를 통해 표준화 그룹 구성 및 작업 범위 등을 논의했고 기술문서(deliverable) 개발 계획 역시 수립했다. FG-DPM은 총 4개의 작업그룹(WG)으로 구성되었으며, 그 중 WG3에서 블록체인을 포함한 오픈데이터 및 상호연동에 대한 표준화 이슈를 다루기로 확정했다.

FG-DLT가 분산원장기술의 세부기술 요소를 다루는 반면, FG-DPM WG3에서는 블록체인 기반의 응용에 대한 이슈를 다루고 있다. 관련 기술문서 주요내용은 다음과 같다.

- 블록체인 및 사물인터넷 개요 Overview of IoT and Blockchain
- 블록체인 기반 데이터 교환 및 공유기술 Blockchain based Data Exchange and Sharing Technology
- 데이터 관리 향상을 위한 블록체인 기술 활용 Using blockchain to improve data management

이 중에서 1st phase 기간 동안 블록체인 및 사물인터넷 개요 (Overview of IoT and Blockchain)에 대한 기술문서를 우선 개발하기로 논의하였다

ITU-T SG13 및 SG16

그 밖의 ITU-T 산하 표준화 그룹들 중 SG16에서 분산원장 서비스에 대한 요구사항⁶⁾, Requirements for distributed ledger services)을 정의하기 위해 표준 개발을 착수하였으며, SG13 역시 클라우드 기반 블록체인 (Blockchain as a Service)에 대한 표준화 개발을 추진하기 위해 표준화 아이템에 대한 논의를 시작한 바 있다.

ITU-T에서는 블록체인 기술 관련 모든 표준들이 모두 2017년 개발을 시작한 단계로 현재 진행 중인 포커스 그룹의 결과에 따라 보다 다양한 표준화 아이템 발굴 및 개발 방향이 설정될 것으로 예상된다. 또한, ISO/TC 307과 관련이 있는 부분이 많은 관계로 ITU-T와 ISO/TC 307 상호 간의 전략적 협력 역시 중요하기 때문에 한국은 ISO/TC 307 뿐만 아니라 ITU-T의 활동에 전략적인 표준 개발이 필요한 상황이다.

WC3 표준화 동향

W3C는 2016년 3월 블록체인 CG(Community Group)[10]를 설립하여 현재 전 세계의 금융서비스 회사, IT 회사 등 다양한 기업에서 117명의 멤버가 참여하고 있다. 그룹의 목표는 국제표준화기구(ISO)가 발표한 실시간 지급결제 표준인 ISO20022 기반으로 블록체인 메시지 포맷 표준 개발, 스토리지, 공용 블록체인, 사설 블록체인 등 블록체인 관련 기술 표준 지침 개발 및 웹 기반 블록체인 생태계를 위한 유즈케이스 문서 개발 등이다. 지금까지는 주로 유즈케이스 문서 개발에 집중하고 있다.

블록체인 유즈케이스 문서는 용어, 생태계 구성요소 및 역할, 주요 적용도메인 및 도메인별 유즈케이스 정리 그리고 요구사항으로 구성되어 있다. 신원 및 식별자 관리, 교육, 난민, 소매, 생산 및 공급 관리, 부동산, 금융서비스, 정부기록물, 헬스케어 등 포괄적인 내용을 다루고 있으며, 주요 내용은 다음 표에서 볼 수 있다.

도메인	유즈 케이스
신원 및 식별자 관리	사용자 관련한 신원확인이 외부 기관에 의한 제어가 아니라 웹 기반으로 자신이 제어하기를 원함. 사용자가 소유를 증명할 수 있는 익명의 식별자를 등록할 수 있고 이는 웹사이트의 Single Sign on 기능 뿐 아니라 운전면허증과 같은 디지털 자격증이 식별자에 발급하여 사용이 가능해야함
교육	교육기관이 교사 자격증을 발급한 후에도 교사는 자격증을 유지하기 위해서는 지속적으로 교육기관의 시험 요구사항을 만족시켜야함. 만일 교사가 이를 충족시키지 못했을 경우 교육기관은 자격증을 폐지할 수 있음. 블록체인 기반의 폐지 원장을 사용할 경우 교사 자격증에 문제가 없는지 검사 시 폐지 원장을 검사를 통하여 가능함
난민	HumanNGO는 난민에 대한 정보를 수집하고 블록체인 기반의 디지털 ID를 난민에게 발급함. 난민이 다른 NGO나 국가로 이주 시 이들 증빙할 수 있는 정보를 제공할 수 있음
소매	한번만 사용가능한 디지털 쿠폰을 발급하고 관리할 경우 쿠폰 블록체인에 각 쿠폰의 시리얼 코드를 입력하여 사용한 쿠폰을 확인 할 수 있음
연쇄적인 생산 및 공급관리	식품제조 회사가 생산하는 제품의 구성 원료에 대한 원산지 정보와 생산과정을 변경이 불가능한 블록체인 기반으로 저장하고 공유하여 소비자의 신뢰확보 가능
부동산	Freddy는 특정 사이트에 올라온 부동산 렌트 정보를 Real Estate 사이트에 복사해서 올렸고, Joe는 부동산 렌트를 위해서 Freddy에게 여러 가지 문의를 함. Freddy는 Joe에게 계약전 선금을 요구했지만 Joe는 부동산 블록체인에서 렌트할 집의 소유주가 Freddy가 아니라는 것을 확인하고 렌트 사기를 피할 수 있었음

블록체인 유즈케이스

6) https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14071

국내 표준화 동향

2017년 하반기까지 블록체인 유즈케이스 문서 정리 후 2차 블록체인 워크숍을 진행하여 표준화 작업 대상을 선정하고 2018년부터 본격적인 블록체인 표준 개발 추진할 예정이다.

블록체인 표준화 포럼은 국내 블록체인 생태계 활성화를 위해 주요 이슈 발굴, 관련 대중소기업 및 전문가 간 교류확대 등을 담당할 목적으로 2017년 설립되었으며, 다음의 표준화를 추진할 예정이다.

- 블록체인 표준용어 및 온톨로지 정립 Blockchain Terminology and Ontology
- 스마트계약 분쟁 조정 및 중재 Smart Contract Mediation and Arbitration in Response to Conflicts
- 블록체인 기반 전자투표 Blockchain-based Online Voting
- 블록체인 기반 사물인터넷 보안 및 프라이버시 보호 Blockchain-based IoT Security and Privacy Protection
- 이종 블록체인 간 상호링크 및 원장연결 프레임워크 Framework for inter-Blockchain links, interledger

또한, 한국전파연구원은 ISO/TC 307을 대응하기 위하여 전문위원회를 설립하고 TC 307 대표단 구성, 총회 대응, 투표 문서 의견 개발, 표준 개발 등을 논의 중이다. 한국정보통신기술협회는 2017년부터 블록체인 전략맵 개발을 통하여 블록체인의 표준화 항목 설정 및 관련한 국제 표준화에 대한 전략을 수립 중에 있다.

그러나 국내에서 아직까지 블록체인을 위한 구체적인 표준 개발은 이루어지지 않고 있으며 2017년 하반기에 관련하여 표준 개발이 시작될 것으로 보여 진다.

전망 및 대응방안

블록체인은 신뢰성과 안정성, 효율성, 보안성을 제공하는 분산 컴퓨팅 기술로, 4차 산업혁명의 기반기술로 자리 매김하고 있다. 블록체인은 금융 부문 뿐 아니라, 제조업과 정부의 기능에도 근본적인 변화를 불러일으킬 것으로 예상된다. 가트너는 2016년부터 블록체인 기술이 플랫폼 혁명의 중심에 있으며, 향후 5~10년 내에 큰 기술 성장을 이룰 것으로 예측하고 있다.

이러한 시장 전망과 기술 변화에 따라 블록체인 표준화는 주요 표준화 기구에서 블록체인 및 분산 디지털 원장의 활성화와 연계하여 활발하게 진행되고 있다. 현재는 매우 초기 단계이고 기본적인 공통적인 표준 개발을 시작하고 있으나, 향후 다양한 적용 분야로 확대될 것으로 전망된다.

블록체인은 다양한 산업의 기반기술이기 때문에 생태계 활성화를 위해서는 이종 플랫폼과의 융합을 쉽게 지원할 수 있는 기반표준 개발 반드시 필요하다. 이에 따라, 블록체인 분야의 IPR 및 표준화 선점 노력이 절실히 요구되는 시점이며, 특히 우리가 강점을 지닌 분야를 중심으로 한 특화된 블록체인 기술 개발 및 표준화 추진에 대한 고민도 새롭게 시작해야 하는 시점이라고 할 수 있다.



3. 블록체인의 진화 : Ethereum, Hypherledger

블록체인 기술은 거래기록(블록)이 생성되는 순간 모든 참여자가 블록체인에 저장된 내용을 나눠서 보관하는 구조다. 그렇다면 굳이 저장 대상이 금융거래내역일 필요가 있을까? 이와 같은 질문에서 시작된 것이 이더리움(Ethereum)과 하이퍼레저(Hypherledger)다. 거래내역 대신 프로그램 코드를 올려 블록체인의 새로운 가능성을 연 것이다. 이제 블록체인은 금융시장을 넘어서, 인공지능·사물인터넷·빅데이터·공공행정 등 다양한 분야의 파괴적 혁신을 예고하고 있다.



블록체인을 활용한 새로운 시도

앞서 소개한 블록체인 기술은 전자화폐거래에서 거래의 무결성을 보증하는 주체 없이 P2P 형태로 거래될 시 거래 내역의 무결성을 보증하기 위해 개발된 기록유지기술이라고 할 수 있다. 즉 화폐거래의 내역을 저장하되 저장된 내용이 임의로 수정될 수 없도록 해주는 메커니즘을 포함하고 있는 기술이다.

블록체인 기술 자체는 사실 체인형태로 구현되는 블록 데이터베이스 상에 무엇이 저장되든 관계가 없는 요소기술이다. 즉 비트코인으로 대표되는 전자화폐는 화폐거래의 내역이 담긴 원장 (ledger) 을 저장하는 블록체인을 구현하였을 뿐 사실 블록체인 데이터베이스의 저장 대상에는 제약이 없다고 할 수 있다.

그렇다면 어떠한 성격의 데이터들이 블록체인에 저장되기에 적합할까? 블록체인에 적용되는 P2P 기술이나 블록체인이 제공하는 변조 방지 메커니즘의 성격에 비추어 생각해보면 “제3자가 볼 수는 있으나 변경되어서는 안되는(irreversible) 성격의 데이터” 가 적합한 대상이 될 것이다. 앞서 언급한 거래원장이 가장 일반적인 사례라고 할 수 있다.

지금까지는 블록체인에 저장되는 “데이터” 라고 언급을 해왔지만, 데이터라는 것은 사람의 입장에서 인지할 수 있는 개념일 뿐, 컴퓨터의 입장에서 보면 저장되는 그것이 데이터든 데이터가 아니든 0과 1로 표현되는 비트의 나열일 뿐이다. 이러한 개념에 착안해서 거래원장과 같은 데이터뿐만 아니라 프로그램 코드 자체를 블록체인에 올리려는 시도가 나타나게 되었다.

이더리움 (Ethereum)

이더리움(Ethereum)⁷⁾

이더리움 (Ethereum)은 비탈릭 부테린 (Vitalik Buterin)이 2013년에 제안하고 2015년에 공개한 암호화폐이자 플랫폼이다.⁸⁾

이더리움은 블록체인에 단순한 데이터뿐만 아니라 프로그램 바이너리 코드와 같은 보다 광의의 데이터가 올라가 동작할 수 있음을 보여주었다. 비탈릭 부테린은 이더리움의 개발의 혁신성을 인정받아 포브스와 타임 등이 주관하는 ‘월드테크놀로지 어워드’ 에서 마크 저커버그 페이스북 CEO를 제치고 수상자로 선정되기도 했다.

7) 이더리움 (Ethereum, <https://www.ethereum.org/>)

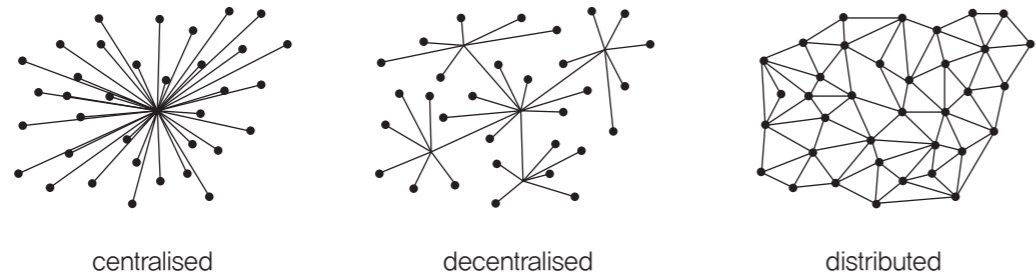
8) <http://webzine.etri.re.kr/20170811/sub04.html>

이더리움의 특징⁹⁾¹⁰⁾

이더리움은 블록체인을 기반으로 금융거래정보를 여러 네트워크에 실시간으로 나눠 저장하기 때문에 비트코인과 같은 암호화폐와 비슷해 보인다. 하지만 기존의 블록체인 기반의 암호화폐와 다른 큰 차이점은 블록체인 상에서 구동 가능한 컴퓨팅 기능을 제공한다는 점이다. 이더리움은 다음과 같은 특징을 갖는다.

기존 비트코인이 제공하는 속성/특징을 모두 만족함

비트코인은 거래내역이 분산 P2P 구조를 가지는 네트워크에 저장이 되는 암호화폐로 익명성(Anonymity), 무국경성(Borderlessness), 탈중앙성(Decentralization), 분산 네트워크(Distributed network), 투명성(Transparency) 등의 특징을 가지며 이러한 특징들은 이더리움도 모두 만족한다.



분산 네트워크 구조

9) http://www.seunghwanhan.com/2015/06/ethereum-introduction_3.html
10) <http://www.ethdocs.org>

튜링 완전성 (Turing-Completeness)을 만족하는 프로그래밍 언어의 지원

1930년대 수학자 앨런 튜링은 기계가 처리하고자 하는 내용을 체계화하고, 그 체계화된 작업을 작은 단위들로 나누고, 반복적인 작업과 연속적인 연산으로 수행하게 한다면 인간처럼 움직일 수 있을 것이라며, 이를 실현하는 가상의 기계로 튜링 머신을 고안했다. 이는 훗날 현대 컴퓨터의 원형이 되었다.

튜링완전성이란 튜링머신이 할 수 있는 일을 실제 내부 동작은 다르더라도 동일하게 수행할 수 있는 머신/언어에 대해 튜링완전성을 만족한다고 정의한다. 어떤 프로그래밍 언어가 튜링완전하려면 조건문과 반복문을 지원할 수 있어야 한다. 쉽게 생각하면 최근의 범용 PC나 프로그래밍 언어는 튜링완전성을 만족한다고 보면 된다. 하지만 원조격 암호화폐인 비트코인의 경우 자체 스크립트 언어를 지원하지만 조건문만을 지원하기 때문에 튜링완전하지 않다고 할 수 있다.

그렇다면 왜 튜링완전성을 만족하는 프로그래밍 언어가 중요할까? 어떤 언어가 튜링만족성을 지원한다는 의미는 우리가 실생활에서 모델링할 수 있는 거의 모든 상황을 프로그래밍 할 수 있다는 의미이기 때문이다. 이것은 이더리움의 또 다른 중요한 특징인 스마트 컨트랙트(Smart Contract)가 성립할 수 있는 중요한 조건이기도 하다. 이더리움은 스마트 컨트랙트를 위해서 이러한 튜링완전성을 만족하는 solidity라는 프로그래밍 언어를 지원한다. 스마트 컨트랙트는 아래에서 자세히 다루도록 한다.

이더리움 가상머신

이더리움은 프로그래밍 가능한 블록체인이다. 이 말은 곧 기존의 비트코인 처럼 사전에 정해져있는 트랜잭션만을 처리할 수 있는 것이 아닌, 이더리움 상에서 사용자가 원하는 응용을 프로그램 할 수 있다는 의미이다. 이러한 응용은 암호화폐처리 응용뿐 아니라 블록체인의 특성을 활용한 다양한 분산 응용까지 활용이 가능하다.

이를 위해서 각 이더리움 노드는 EVM(Ethereum Virtual Machine)을 구동하게 된다. EVM은 자바스크립트나 파이썬 같은 언어를 사용한 응용도 구동시킬 수 있지만, 스마트 컨트랙트의 작성을 위해서는 solidity를 이용해야 한다. solidity로 기술된 스마트 컨트랙트는 EVM 컴파일러를 통해서 바이트 코드로 컴파일되고 이것은 이더리움 클라이언트를 통해서 블록체인 상으로 업로드 되게 된다.

어카운트

이더리움에서도 비트코인의 지갑과 동일한 개념인 어카운트(account)가 존재한다. 대신 이더리움에서는 두 가지 종류의 어카운트가 존재하는데, Externally Owned Account(EOA)와 Contract Account가 그것들이다. EOA 는 비트코인에서의 지갑과 거의 동일한 역할을 하며 이더리움에서의 암호화폐인 이더(Ether)를 거래하는데 쓰인다. Contract account는 뒤의 스마트 컨트랙트 파트에서 추가로 설명한다.

이더(Ether) & 개스(Gas)¹¹⁾¹²⁾

이더는 이더리움에서 통용되는 암호화폐의 이름이다. 이더는 이더리움의 EVM 환경에서 제공하는 연산기능의 사용료를 지불하는 데 쓰인다. 하지만 이더리움에서는 코드실행환경을 제공하는 특징으로 인하여 DOS 공격의 위험이 상존하기 때문에, 사용자가 이더리움에서 제공하는 연산기능의 구매를 바로 이더로 지불할 수 있게 하지 않고 개스라는 새로운 지불 단위를 만들었다. 이 개스는 결국 이더로 지불되는 것이긴 하지만 응용코드의 각 연산기능 별로 개스 가격을 차등적으로 매겨놓도록 하였다. 따라서 손쉽게 DOS 공격이 이루어질 수 있는 코드를 실행하려면 천문학적인 개스가 필요하도록 만들어 이더리움에 대한 DOS 공격을 원천 차단하도록 하였다.

11) ETRI 전자통신동향분석 제 32권 제 1호 2017년 2월 “비트코인 후 블록체인”
 12) <http://www.ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html#example-transaction-cost>

Operation Name	Gas Cost	Remark
step	1	default amount per execution cycle
stop	0	free
suicide	0	free
sha3	20	
sload	20	get from permanent storage
sstore	100	put into permanent storage
balance	20	
create	100	contract creation
call	20	initiating a read-only call
memory	1	every additional word when expanding memory
txdata	5	every byte of data or code for a transaction
transaction	500	base fee transaction
contract creation	53000	changed in homestead from 21000

이더리움 개스

스마트 컨트랙트(Smart Contract)

이더리움은 블록체인을 기반으로 하여 단순한 암호화폐에서 한걸음 더 나아가 임의의 응용코드를 동작시킬 수 있는 플랫폼으로 만들었다. 이렇게 만든 이유가 무엇인지 한번 고찰해보자. 블록체인 상에서 코드를 구동시켜서 얻는 장점은 과연 무엇일까?

화폐를 기반으로 임의의 동작을 허용하는 환경이라면, 그 임의의 동작은 바로 경제활동을 의미할 것이다. 기본적으로 경제주체 간의 경제활동은 거래를 하는 양자(혹은 다자간의) 계약(컨트랙트)을 기반으로 하게 된다. 실물 경제환경에서 경제주체 간의 계약활동은 항상 그 계약이 지켜지지 못하고 파기될 위험을 수반하게 된다. 이러한 이유 때문에 보험이 존재하고 법적 분쟁이 발생되는 것이다.

하지만 이러한 경제활동의 환경을 이더리움으로 옮겨보면 어떨까? 이더리움에서 컨트랙트는 다름 아닌 코드 및 데이터의 묶음으로 구현이 되며, 이더리움 환경에서 EVM 바이트코드로 컴파일되어 블록체인의 임의의 주소에 존재하게 된다. 앞에서 튜링완전성 및 튜링완전성을 지원하는 언어에 대해서 언급을 했는데, 실제 다자간의 거래에서 컨트랙트는 임의의 내용으로 성립이 될 수 있다. 이것은 곧 튜링완전성을 만족하는 언어만이 임의의 컨트랙트를 온전히 기술할 수 있다는 의미가 된다.

그렇다면 이더리움 상에서 코드로 구현이 된 컨트랙트는 어떠한 효과를 가질까? 앞서 이더리움을 블록체인 상에 구현이 되는 플랫폼이며, 이더리움의 블록체인에는 응용 프로그램의 코드도 올라갈 수 있다고 소개했다. 따라서 코드로 구현된 컨트랙트도 블록체인 상에 저장이 될 것이고, 블록체인의 특성상 한번 저장된 컨트랙트는 수정하기가 거의 불가능 할 것이다. 또한 이더리움을 사용하기 위해서 사용자는 앞서 언급한 어카운트를 발급 받아야 하는데, 이를 종합해 보면 거래 당사자들의 어카운트 및 이 어카운트를 기반으로 코드로 기술된 컨트랙트가 모두 이더리움 블록체인 상에 올라가게 된다. 이것은 곧 이더리움 상에서 일단 한번 맺어진 계약관계는 반드시 지켜지게 된다는 것을 의미하게 된다. 따라서 금전적인 관계에서 채무 불이행 같은 것들은 절대로 일어날 수 없게 되고, 보험이나 법적 강제력이 없어도 안심하고 거래를 할 수 있게 된다.

이더리움에서는 이렇게 이더리움 상에서 코드로 구현된 거래자간의 계약을 스마트 컨트랙트라고 정의하고 있다. 이러한 스마트 컨트랙트의 대표적인 사용 예로 다음 페이지와 같은 클라우드 펀딩을 들 수 있다.

스마트 컨트랙트를 이용한 클라우드 펀딩

최근 많이 활성화되어 있는 클라우드 펀딩 같은 경우, 투자자는 대부분 결과물을 보지 못한 채 개발사의 설명만 보고 투자여부를 판단해야 한다. 설명 시간이 지난 후 결과물을 제대로 받아보지 못하더라도 많은 경우 투자비가 중/소액 규모이기 때문에 손해를 변제받기 어려워 투자금을 날릴 위험이 상존하고 있는 편이다. 하지만 이러한 클라우드 펀딩을 스마트 컨트랙트를 이용해서 받는다면 이러한 우려는 사라지게 된다. 개발사가 투자를 받기 위해서 펀딩 조건이 만족하지 않는다면 투자금을 다시 회수하는 내용으로 스마트 컨트랙트를 기술하고 투자를 받게 된다면, 투자자는 결과물이 원안대로 나오지 않을 경우 자동으로 투자금을 회수받게 되므로 손실에 대한 걱정을 하지 않아도 되는 것이다. 이것은 더불어 개발사로 하여금 개발에 대한 독려의 효과도 가져오게 되므로 양자 모두에게 이득이다.



Solidity

Solidity는 이더리움 상에서 스마트 계약을 기술하기 위해 만들어진 언어이다. 이더리움 상에서 스마트 계약을 기술하는 데 사용할 수 있는 언어는 Solidity 외에도 Serpent나 LLL (Lisp Like Language) 등이 있는데, 현재는 solidity가 주로 사용되고 있다. 문법은 javascript와 유사하다. 아래 예는 이 코드가 실행될 때마다 블록체인 상에 "Hello, World!" 라는 로그를 남기는 코드의 예이다.

```
contract HelloWorld {
  event Print(string out);
  function() { Print( "Hello, World!" ); }
}
```

자세한 사항은 <https://solidity.readthedocs.io/en/latest/> 을 참조하면 된다.

Hyperledger

Hyperledger 프로젝트 개요¹³⁾



HYPERLEDGER

하이퍼레저 프로젝트는 리눅스 재단에서 운영하고 있는 블록체인 프로젝트의 이름이며, 하이퍼레저의 목적은 기업에서 적용이 가능한 블록체인 기술들을 구현하는 것이다(하이퍼레저는 어느 하나의 기술을 의미하는 것이 아니며 하이퍼레저라는 프로젝트명 하에 다양한 기술들이 개발되고 있다, Fabric은 그중 하나이다).

하이퍼레저는 여러 하위 프로젝트를 운영하고 있는데, 패브릭(Fabric), 이로하(Iroha), 쏘우투스레이크(Sawtooth Lake) 등의 프로젝트가 있다. 그중 Fabric 프로젝트는 하이퍼레저에서의 블록체인 런타임을 구현하고 있으며

13) <https://www.hyperledger.org>

블록체인의 엔진을 만드는 핵심 프로젝트다. 보통 기술을 지칭하는 용도로 하이퍼레저를 사용했을 때는 하이퍼레저 Fabric을 의미하는 경우가 많다. 이 하이퍼레저 Fabric은 IBM에서 구현하여 오픈소스 프로젝트에 공헌한 코드이다.

해당 프로젝트를 주로 이끌고 있는 기업으로는 Accenture, Airbus, CME Group, Deutsche Bourse Group, Digital Asset, DTCC, Fujitsu, Hitachi, IBM, Intel, JP Morgan, R3, Wanda Group 등이 있다.

Hyperledger vs. Ethereum

하이퍼레저 프로젝트는 이더리움처럼 블록체인 기반의 기술이지만 다음과 같은 유사점/차이점이 있다.

- ▷ 이더리움은 퍼블릭기반 블록체인인데 반해 하이퍼레저는 인가된 사용자들만 접근할 수 있는 프라이빗블록체인을 지향함
- ▷ 하이퍼레저의 기술들은 기본적으로 암호화폐를 지원하지 않음(다만 이것이 암호화폐를 구현할 수 없다는 의미는 아니며, 필요하면 구현해서 사용할 수는 있음)
- ▷ 하이퍼레저의 어떤 기술들은 EVM (Ethereum Virtual Machine)을 이용해서 구현되었음
- ▷ 이더리움은 기본적으로 퍼블릭블록체인을 지향하고 있지만, EEA(Enterprise Ethereum Alliance)¹⁴⁾ 프로젝트는 하이퍼레저처럼 기존의 이더리움을 기반으로 기업레벨의 요구사항을 만족시킬 수 있는 프라이빗한 이더리움 플랫폼을 만드는 것을 목표로 하고 있음

14) <https://entethalliance.org/>

Hyperledger 프로젝트

하이퍼레저 프로젝트는 다음과 같은 기술을 개발하고 있다.

▶ Fabric (<https://www.hyperledger.org/projects/fabric>)

Fabric은 IBM이 주로 개발된 코드를 제공하고 있으며, 블록체인 런타임을 개발한다. 모듈방식의 구조를 채용하여, 합의 알고리즘이나 사용자 인증서비스 등 필요한 서비스를 필요한 시점에 추가할 수 있도록 되어 있으며, "chaincode" 라는 스마트 컨트랙트 기술을 제공한다.

▶ Burrow (<https://www.hyperledger.org/projects/hyperledger-burrow>)

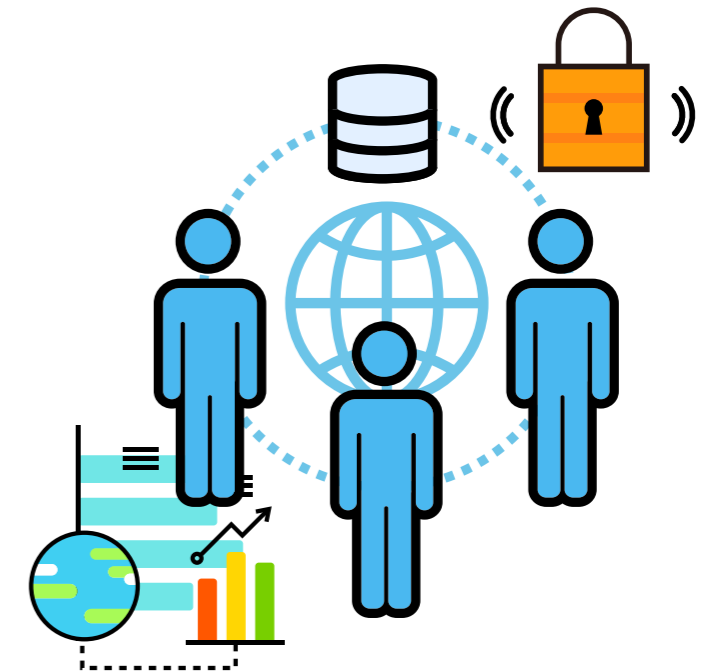
Burrow는 스마트 컨트랙트 인터프리터를 가지고 있는 EVM에 기반한 블록체인 클라이언트이다. Monax에 의해서 코드가 개발되어지고 있다.

▶ Iroha (<https://www.hyperledger.org/projects/iroha>)

Fabric에 기반한 블록체인 플랫폼이며 주로 모바일환경 (스마트폰)에 초점을 맞추고 있다. 주 코드 개발은 Soramitsu 가 맡고 있다.

▶ Sawtooth (<https://www.hyperledger.org/projects/sawtooth>)

sawtooth는 기업레벨에서의 사용을 목표로 하고 있는 스마트 컨트랙트를 지원하는 블록체인 프로젝트이다. 주 코드개발은 인텔이 맡고 있다.



4. 결론 및 시사점

블록체인은 무궁무진한 활용을 예고하고 있고, 시장은 그에 맞춰 들쭉이는 중이다.
 4차 산업혁명과 함께 전부 파악할 수 없을 만큼 많은
 블록체인을 기반의 플랫폼과 기술들이 등장할 것이다.
 난립하는 블록체인의 상호연결성을 확보하는 방법이 바로 표준화다.
 아직은 초기단계지만 앞으로의 국가적 이익을 위해
 블록체인의 표준화는 반드시 선도해나가야 할 대상이다.



블록체인의 미래

블록체인은 비트코인이라는 암호화폐가 화제가 되면서 관심을 받기 시작했지만 암호화폐는 단지 시작일 뿐, 앞으로 금융시장을 넘어 다양한 분야에 적용되며 미래 혁신을 이끌 것으로 예상된다.

블록체인은 기존의 중앙 통제방식에서 벗어나 P2P네트워크기반으로 거래 구성원(참가자) 모두에게 내용을 공개하는 분산형 거래장부다. 모든 이용자들이 거래 내용을 자동으로 기록하고, 열람하고, 기록된 내역을 바탕으로 새로운 내역을 생성하기 때문에 사실상 내용을 위조하거나 변조할 수 있는 가능성이 없다. 기존의 중앙 집중형 관리 시스템은 보안을 위해, 시스템 구축에 막대한 비용을 투자해야만 했지만 블록체인은 이러한 비용을 현저하게 낮출 수 있다.

블록체인에 올린 데이터는 누구나 열람할 수 있지만 위변조가 불가능하다. 이러한 특성이 가장 잘 활용될 수 있는 분야가 바로 금융 거래다. 블록체인 기술로 비트코인과 같은 암호화폐가 은행이나 증권사 등의 기관의 보증이 없이도 신뢰성을 확보하며 화폐로서 활발히 거래되기 시작했다.

블록체인은 앞으로 다양한 활용가능성을 예고하고 있다. 블록체인의 데이터베이스 위에 금융거래 원장 내역을 저장한 것이 암호화폐일 뿐, 데이터베이스 위에 올릴 수 있는 저장대상은 무궁무진하기 때문이다. 프로그래밍 언어를 그 저장할 수도 있어서, '제3자에게 공개될 수 있지만 위변조가 절대 불가능한' 특성을 이용한 여러 분야에 활용이 가능하다.

실제로 온두라스에서는 부정부패가 만연한 토지대장 관리에 블록체인을 사용해 관리하겠다는 방안을 밝혔으며, 에스토니아나 스페인의 신생정당들은 이미 블록체인 기반의 전자투표를 실시하고 있다. 조작이 불가능하기 때문에 통제를 할 중앙선거관리위원회가 필요 없다.

최근 각광받고 있는 이더리움은 블록체인을 이용한 암호화폐이기도 하지만, 암호화폐에서 한걸음 더 나아가 스마트 컨트랙트라는 전자계약 기능을 추가했다. 이것은 이더리움 상에서는 코드로 구현된 계약이 가능하다는 것을 의미한다. 코드로 약속을 정해 블록체인에 저장했으니 한번 맺어진 계

약관계는 수정할 수 없고 반드시 지켜진다. 금전적인 관계에서 채무 불이행 같은 일들도 일어날 수 없게 된다. 사람이 개입하지 않아도 보험이나 법적 강제력이 따로 필요없게 되는 것이다. 이것을 스마트 컨트랙트라고 말한다. 스마트 컨트랙트를 이용하면 크라우드 펀딩같은 시스템, 보험이나 채권, 은행업무 등에서 두루 쓰일 수 있게 된다. 이와 같은 혁신성 덕분에 이 더러움은 기존 가상화폐의 한계를 극복했다는 평가를 받는다.

이렇게 무궁무진한 활용 가능성에, 블록체인을 보는 시각은 낙관적이다. 미국의 돈 탭스콧은 “인터넷이 지난 30년을 지배했듯, 앞으로는 블록체인이 우리 미래를 30년간 지배할 것이다”라는 평을 내놓았다. 가트너는 블록체인 시장이 2022년이면 100억달러(약 11조 2700억원)까지 클 것으로 전망했다. 다보스포럼은 2027년 전 세계 국내총생산(GDP)의 10%가 블록체인 기술로 저장될 것으로 전망했다. 각 나라는 지금 필요에 따른 블록체인을 연구, 개발하여 생활에 적용하고 있는 중이다. 블록체인을 단순히 가상화폐의 결제수단 정도로 보아선 안 되는 이유다.

블록체인 표준화의 중요성

블록체인의 다양한 활용가능성이 각광받으면서 다수 기술의 난립이 예상되고 있다. 새로운 암호화폐도 끊임없이 생성되는 중이다. 이에 따라 벌어지는 혼란을 최소화하고 데이터 간 상호연결성을 확보하는 방법이 바로 표준화다. 국제표준화기구에서는 블록체인 표준화에 박차를 가하기 시작했다. 초기단계임에도 각국 전문가들이 적극적으로 참여하고 있는 중이다.

ISO는 2016년 블록체인과 전자분산원장기술 그룹을 승인하여 TC 307을 신설했다. 2017년 4월 열린 1차 회의에서는 용어에 대한 표준을 개발하는 작업그룹(WG)과 참조구조, 유즈케이스, 보안 및 개인정보, 식별, 스마트 컨트랙트 등을 연구하는 다섯 개의 연구그룹(SG)을 신설했다.

ITU-T는 2017년 5월 블록체인에 대한 포커스그룹(FG-DLT)을 구성하여 블록체인 이슈에 대한 표준화 작업을 착수하기로 결정했다. 특히 보안과 관련된 표준화 이슈를 중점적으로 다루는 표준화 그룹 SG17(의장: 염흥열

교수, 순천향대)의 2017년 8월 개최된 총회에서 우리나라는 블록체인 기술 표준화 이슈를 다루는 신규 Q14의 신설을 확정하고 한국대표단 오경희위원을 라포처로 선임하는 등, 보안 표준화의 주도권을 확보했다.

웹의 표준을 만드는 단체인 W3C에서는 2016년 3월 한국 주도로 신설한 블록체인 커뮤니티 그룹(CG)에 전 세계 117명의 멤버가 참여하고 있다. 그룹의 목표는 국제표준화기구(ISO)가 발표한 실시간 지급결제 표준인 ISO20022 기반으로 블록체인 메시지 포맷 표준 개발, 스토리지, 공용 블록체인, 사설 블록체인 등 블록체인 관련 기술 표준 지침 개발 및 웹 기반 블록체인 생태계를 위한 유즈케이스 문서 개발 등이다.

블록체인 표준화 분야는 이제 막 발걸음을 뚫다. 용어의 정립부터 시작한 매우 초기 단계로 기본적인 공통적인 표준개발을 시작하고 있다. 그러나 블록체인은 다양한 산업의 기반 기술로 각광받고 있는 만큼 생태계의 활성화를 위해 플랫폼 간의 융합과 상호연결성을 쉽게 지원할 수 있는 기반 표준 개발이 필수적이다. 이에 블록체인 분야의 IPR 및 표준화 선점하고 국가적 이익을 추구하는 일은 매우 중요한 일이라고 할 수 있다.

참고문헌

- 금융보안원, 국내외 금융분야 블록체인(Blockchain) 활용 동향
- 동아비즈니스리뷰, '모든 거래 기록된 장부 '블록체인' 진정한 P2P시대 여는 인터넷의 미래', 김진화
- 디지털데일리, "IBM, 클라우드 기반 블록체인 서비스 출시"
- 모든거래 기록된 장부, 블록체인 진정한 P2P시대 여는 인터넷의 미래
- 블록체인 기술의 현재와 미래, 류진호, 임재곤
- 블록체인 클라우드 서비스 'ETH BaaS' 선보여, <http://www.bloter.net/archives/243623>
- 비트코인 원천기술, "블록체인, 너 대체 뭐니?" <http://dongascience.donga.com/news/view/19301>
- 성신여대, 블록체인기술 금융분야 도입방안을 위한 연구. 2016
- 암호화폐암호화폐시장의 폭발적인 성장과 그 미래, <http://polarizedlentium.tistory.com/125>
- 핀테크지원센터, <https://goo.gl/BQ6bMy>
- Back, Adam et al. "Enabling Blockchain Innovations with Pegged Sidechains." (white paper, Genius.com, 2010), URL: <https://genius.com/Adam-back-enabling-blockchain-innovations-with-pegged-sidechains-annotated>
- Blockchain as a Service: The New Weapon in the Cloud Wars?, <https://dzone.com/articles/blockchain-as-a-service-the-new-weapon-in-the-clou>
- Blockchain Hub, <https://blockchainhub.net/glossary/>
- Blockchain Technology Glossary: Industry Definitions and Explanations (Technology Trends, [2016]). URL: <http://www.blockchaintechnologies.com/blockchain-glossary>
- ETRI Insight, 블록체인 기술의 활용과 전망
- InterPARES Trust, 2017. "Blockchain and Distributed Ledger Terminology Database, <http://arstweb.clayton.edu/interlex/en/term.php?term=blockchain>
- ISO/TC 307(블록체인 및 분산원장기술) 제1차 국제표준화 회의, 제171호, pp 78 ~ 81, 2017년 5월, http://www.tta.or.kr/data/reportDown.jsp?news_num=4851
- ISO/TC 307, <https://www.iso.org/committee/6266604.html>
- ITU-T Focus Group Digital Financial Services, Digital Financial Services (DFS) Glossary, 2017
- ITU-T Focus Group Digital Financial Services, Distributed Ledger Technologies and Financial Inclusion, 2017
- ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), <http://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx>
- ITU-T SG20, Framework of blockchain of things as decentralized service platform (Y.IoT-BoT-fw) http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14099
- KISA, '클라우드 서비스 형태의 블록체인(Blockchain as a Service) 출시'
- The Blockchain as a Service is Coming to a Cloud Near You, <https://medium.com/@jrodthoughts/the-blockchain-as-a-service-is-coming-to-a-cloud-near-you-1d5ccb214b91>
- W3C Blockchain CG, <https://www.w3.org/community/blockchain/>

편집위원장 ETRI 표준연구본부

김 형 준 본 부 장

편집위원 ETRI 표준연구본부

이 강 찬 실 장

ETRI 표준연구본부

인 민 교 책임연구원

ETRI 표준연구본부

이 주 철 책임연구원

ETRI 표준연구본부

최 영 환 선임연구원

ETRI 표준연구본부

이 병 남 전문위원

ETRI 표준연구본부

현 성 은 기술원

