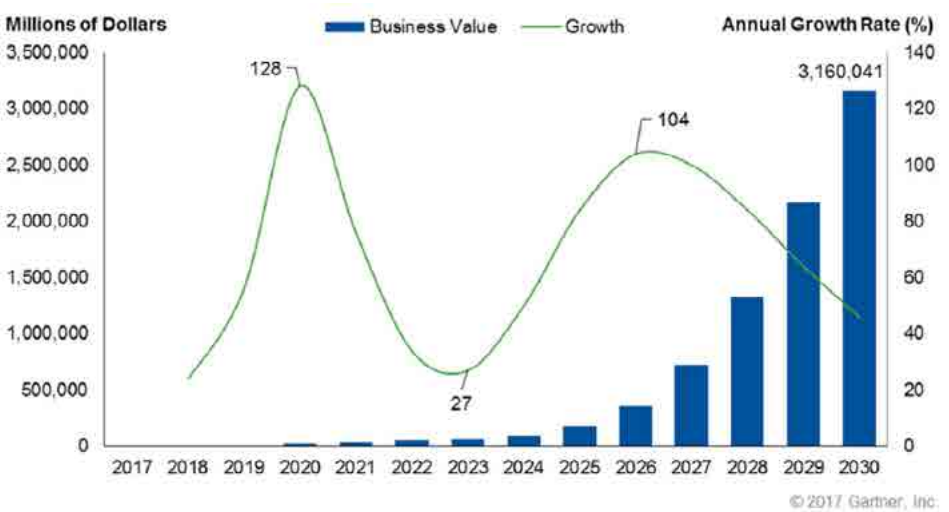
Ⅰ-1. 블록체인 기술과 보건의료분야 활용

최영진 교수
을지대학교 의료경영학과

1. 들어가는 글

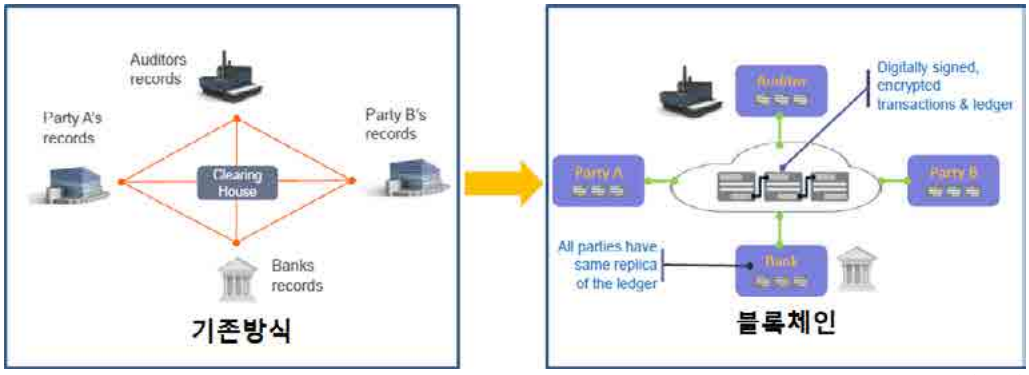
- 지능화, 디지털, 연결로 대표되는 4차 산업혁명 시대의 핵심기술로 블록체인 기술이 부각되고 있음
  - 시장 조사기관인 가트너(Gartner)는 2017년에 미래 기술 트렌드 중 하나로 블록체인을 선정하였으며, 2020년에 128%의 성장률을 기록하는 등 초고속으로 성장하여 2030년에는 비즈니스 가치가 3조 달러를 초과할 것으로 예측함
  - 세계경제포럼(World Economic Forum)은 가상화폐 중심의 블록체인기술이 향후 제조, 서비스, 문화, 공공분야 전반에 활용되면서 2027년에는 전세계 GDP의 10%가 블록체인 기술을 활용할 것으로 예측함



출처: Gartner, 2017

[그림 1] 블록체인 산업 전망

- 블록체인 기술은 거래당사자 간의 직접적인 거래를 가능하게 하는 분산원장 기술임
  - 블록체인 기술이란 거래정보를 저장한 블록을 모든 거래당사자가 네트워크를 통해 분산 저장하고 주기적으로 암호화한 후, 체인 형태로 연결하여 저장하는 분산원장 기술임
  - 거래당사자가 중앙집중시스템에 의존하지 않고 peer-to-peer 방식으로 각자의 원장을 분산 · 보유하여 거래 중개자를 거치지 않음
  - 또한 원장은 네트워크 참여자 모두에게 공개되며(복사본 보유), 거래자간의 합의가 없이는 변경이 불가능하기 때문에 신뢰성이 있음
  - 중개자(기존의 중앙기관이나 은행 등)의 개입없이도 자산이나 정보의 교환이 가능해지면서 전통적인 사회의 신뢰구조가 블록체인 기반의 신뢰구조로 변화함



출처: IBM (2018)

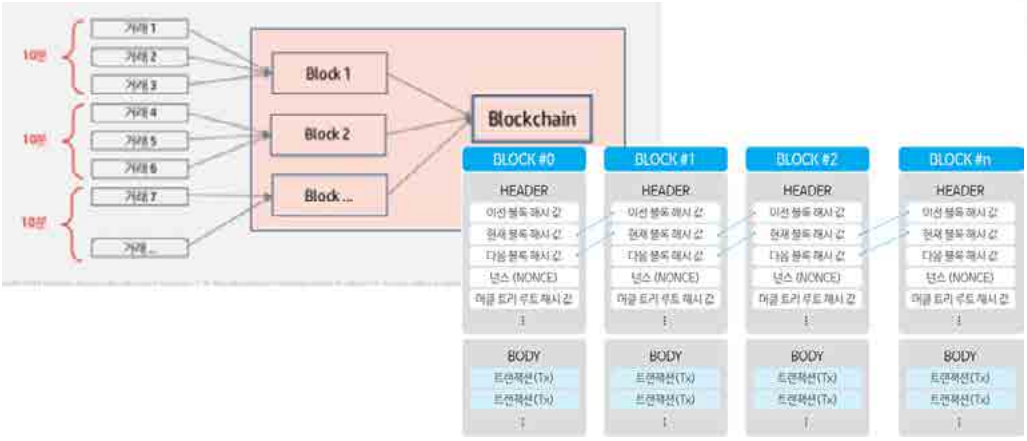
[그림 2] 거래 방식의 변화

2. 블록체인 기술 구조

- 블록체인은 암호화된 블록을 기반으로 한 분산원장, 암호화, 합의, 스마트계약 등의 구성요소를 포함하는 집합체임

[그림 3] 블록체인 구성 요소

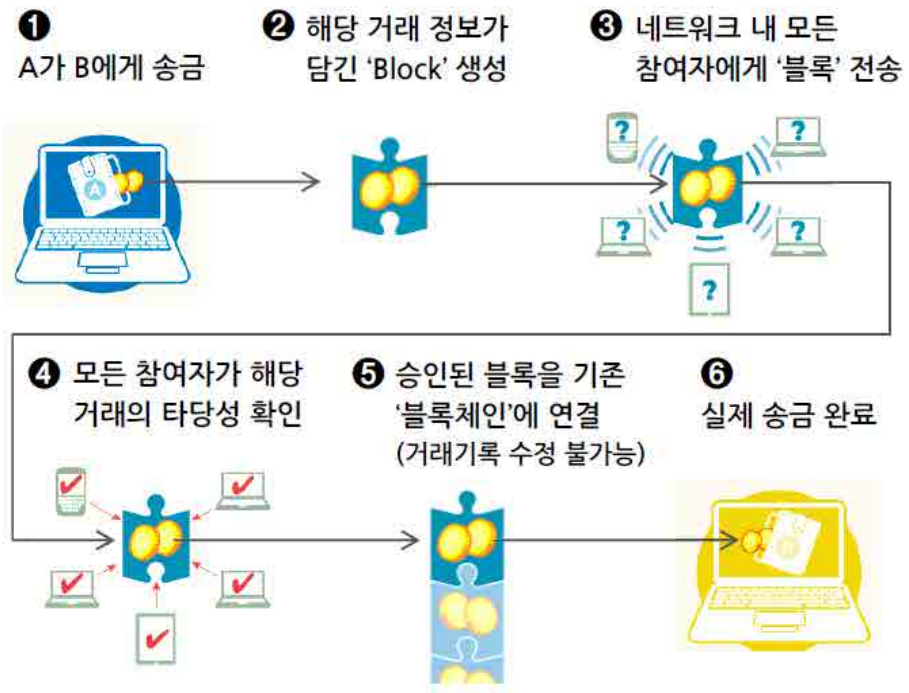
- 블록체인은 해쉬함수 기반의 암호화로 안전한 거래를 보장하며, 블록은 블록해쉬 이외에도 유효한 정보의 묶음으로 블록 헤더와 거래 정보를 포함하는 블록 바디로 구성
  - 블록체인은 거래의 시간 순으로 기록된 장부로 네트워크의 모두가 접근할 수 있는 공개된 분산원장임
  - 블록 헤더는 소프트웨어/프로토콜 버전, 이전 블록의 블록 해쉬, 머클 해쉬, 블록이 생성된 시간, 작업 증명시 이용되는 nonce값으로 구성됨
  - 머클트리(Merkle Tree)는 거래정보에 대한 해쉬로 구성되며, 블록의 바디에 해당함. 개별 거래 정보에 대한 해쉬값을 합친 후 다시 해쉬하는 과정을 거치면서 거래정보가 조작되면, 복사된 체인과 비교하여 조작된 위치를 정확하게 알 수 있도록 구성됨



출처 : 한국보건산업진흥원(2017) 재구성

[그림 4] 블록 및 블록체인 구조

- 분산원장은 중앙통제 및 전체 시스템 중단 위험을 해결함
  - ▸ 분산원장기술(Distributed Ledger Technology)은 중앙서버나 중앙관리자의 제어없이 분산화된 네트워크의 참여자가 정보를 공유하고 동기화하는 기술임
  - ▸ 기존의 전통적인 시스템에서는 은행과 같은 제3의 관리기관에 비용을 지불하고 제3자가 권한을 위임받아 서비스와 데이터를 관리하였음
  - ▸ 분산원장은 분산되어 있는 네트워크 참여자 각자에게 데이터가 복제 · 공유되어, 네트워크 참여자 모두가 원장을 관리하고 동기화함에 의해 거래의 유효성, 단일성을 확보함
  - ▸ 분산원장 기술 기반으로 송금이 이루어지는 경우, 거래 정보가 포함된 블록이 생성되고, 이를 네트워크 참여자에게 전송하여 거래의 타당성 확인 후 블록체인에 연결하여 송금이 완료됨



출처 : KB금융지주경영연구소(2015)

[그림 5] 블록체인 기반 거래 개념도

- 분산시스템의 신뢰 확보를 위해 합의가 필요함
  - 합의 문제는 분산 시스템의 신뢰도를 보장하기 위해 나온 개념으로 모든 분산 시스템에 참여하고 있는 모든 프로세스가 합의에 의해 동일한 데이터로 결정됨
  - 네트워크 참여자간의 합의는 복잡한 문제로 합의 알고리즘은 모든 참여자가 같은 값을 결정하고 결정된 데이터는 특정 참여자에 의해 제안된 것이어야 하며, 언제나 1 또는 0을 판단할 수 있어야 함
  - 복잡한 합의에 사용되는 알고리즘은 전통적인 Proof of Work 이외에도 Proof of Stake, Unique Node List, PBFT 등의 방법이 사용됨

[표 1] 합의 알고리즘

Proof of Work	Proof of Stake	Unique Node List	PBFT
– 비트코인에서 사용 – 모든 노드는 블록헤더에 들어갈 해시값을 맞추는 연산 수행 – 채굴에 성공한 노드는 블록을 형성하며 그에 따른 이득을 취함 – 막대한 연산 과정 필요	– PoW의 연산 부담을 줄이기 위해 등장 – 블록 생성 확률이 각 노드가 가진 지분에 따라 결정 – 생성에 성공한 노드는 생성에 따른 이득을 동일하게 받음	– Ripple에서 사용하는 알고리즘 – UNL은 합의의 주최가 되는 선택받은 노드 – 리플에서 추천하는 신뢰 노드 리스트 사용 – 합의구조 참가에 대한 내부적인 보상이 없어 참여노드의 신뢰성이 보장되어야 함	– 참여자들이 한정된 프라이빗 블록체인에서 사용 – 정해진 정도(1/3)를 넘지 않는 한도내에서 fail이 일어나도 정확한 값을 전달 – 검증을 담당하는 validating Peer와 블록 생성 리더로 구분 – 리더가 트랜잭션 정렬 및 블록 생성 후 VP에게 전달 – 3f+1의 피어 중 2f+1이 동의하면 블록체인에 추가

출처: http://www.itworld.co.kr/print/94202

- 스마트 계약
  - ▸ 거래당사자간 합의된 규칙을 코드로 생성, 스마트 계약으로 구현하여 자동화된 거래의 처리를 지원함
  - ▸ 스마트 계약은 블록체인에 스크립트 형태로 구현되며, 스마트 계약은 체인 내의 고유한 주소로 접근하여 트랜잭션을 직접 보냄으로써 해당 계약을 처리함

- 리눅스 재단의 하이퍼레저(Hyperledger)
  - ▸ 하이퍼레저는 리눅스 재단에서 주관하는 블록체인 오픈소스 프로젝트로 금융뿐만 아니라 IoT, 물류, 제조, 기술 산업 등 여러 산업에 걸쳐 응용 가능한 블록체인 기술을 추구함
  - ▸ 이는 모듈화, 플러그 앤 플레이, 상호 운용성을 지향하며, 스마트 계약을 지원하기 위한 기술로 멤버쉽, 합의, 비즈니스로직 등 세부항목으로 구성되어 있음

구 분	설 명
멤버쉽 서비스	– 네트워크의 거래 인증에 접근하기 위해서는 모든 개체들이 멤버쉽 서비스에 등록
합의 서비스	– P2P 프로토콜은 HTTP/2 표준을 따른(양방향 스트리밍, 다중 요청 등을 제공하는) Google RPC를 이용하며, 이 프로토콜은 방화벽, 프록시, 보안을 포함한 인터넷 인프라에 포함 – 분산장부는 블록체인을 효율적으로 관리하고 암호화 캐쉬를 계산 – 합의 매니저는 합의 알고리즘과 다른 Hyperledger 구성요소 사이에서 인터페이스 역할
비즈니스 로직 서비스	– 확인된 노드들이 실행되는 분산 거래 프로그램으로 체인코드 서비스는 특정 가상 머신이나 컴퓨터 언어에 의존하지 않고 체인노드를 관리하기 위해 Docker를 이용

출처: http://blockchain-finance.com/

[그림 6] 하이퍼레저 구성요소

3. 블록체인 활용 사례

- 블록체인은 전자화폐 기반의 금융서비스뿐만 아니라 디지털 정보의 안전한 보관과 거래, 그리고 계약 자동화 기능 등을 이용하여 상품 유통 및 공공 서비스에 활용할 수 있음

[표 2] 블록체인 활용 분야 및 사례

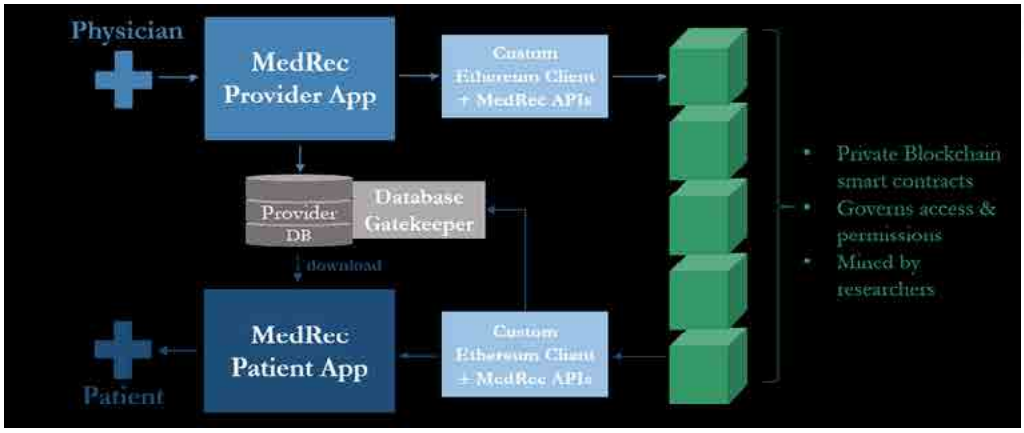
구 분	내 용	사례
금융	증권 거래, 청산결제, 송금 등의 금융 서비스에 블록체인을 활용	. Kraken(증권거래) . Aviva(보험) . Clearmatics(송금) . Funderbeam(투자관리) . Skuchain(무역금융)
일반 산업	상품의 수송 및 유통과정에서 안전성 확보에 활용	. La'Zooz(수송) . pey(유통) . Chronicled(보안) . MaidSafe(스토리지) . RWE(전력거래)
공공 서비스	안전하고 편리한 정보보관 기능을 이용하여 공공서비스에 활용	. Block Notary(공증) . Chainalysis(신원관리) . 덴마크(전자투표) . 에스토니아(전자시민권)

출처: 금융보안원(2017) 재구성

- 보건의료 분야에서도 의료서비스의 혁신과 비용 효율성을 추구하기 위해 적극적으로 블록체인 기술 활용(Deloitte, 2016; 한국보건산업진흥원, 2017)
  - ▶ 미국의 국가의료정보표준(Office of the National Coordinator for Health Information Technology)의 건강정보교환에서는 네트워크의 모든 참가자의 신원증명 및 인증, 건강정보에 대한 접근 권한을 해결하기 위한 방법으로 블록체인 기술에 대한 관심
  - ▶ 또한 정밀, 맞춤형 의료에 대한 관심이 높아지면서 개인의 생체 및 진료정보의 안전한 유통과 디지털 건강기기의 도입 및 이용이 증가할 것으로 예상되면서 이에 대한 확인과 정보유통 수단으로 블록체인 필요성 증가

- 보건의료 분야에서 블록체인 기술은 임상시험을 위한 안전한 데이터 공유, 개인주도형 건강관리, 보험청구 심사, 의료기기 · 의약품 유통 등에서 활발하게 적용(한국보건산업진흥원, 2017)
  - Gem Health : 의약품 유통, 자동차 보험, 사회기반 서비스 등 다양한 분야에서 활용 가능한 공유 ID 체계 구축을 목표로 블록체인을 구성
  - Medibloc : 환자 개인이 직접 여러 의료기관에 분산된 자신의 의료정보를 통합, 관리 및 유통을 할 수 있게 하는 블록체인 기술
  - Shovom : 환자의 게놈 데이터를 안전하게 저장 및 유통하기 위한 블록체인 플랫폼
  - Mygenomebox : 개인에게 유전체 분석 결과에 대한 서비스 제공과 확보된 데이터를 제약사 및 연구기관에 제공
  - Mediledger : 의약품 운반과 공급관리를 위해 개발된 플랫폼으로 모든 처방 의약품과 공급된 의약품을 식별 및 추적관찰
  - HealthCoin : 만성 질환 합병증 예방을 위해 환자의 행동을 웨어러블 기술로 추적 관찰, 보험사 및 의료기관을 연결해 정보를 제공하고 환자에게 금전적 보상

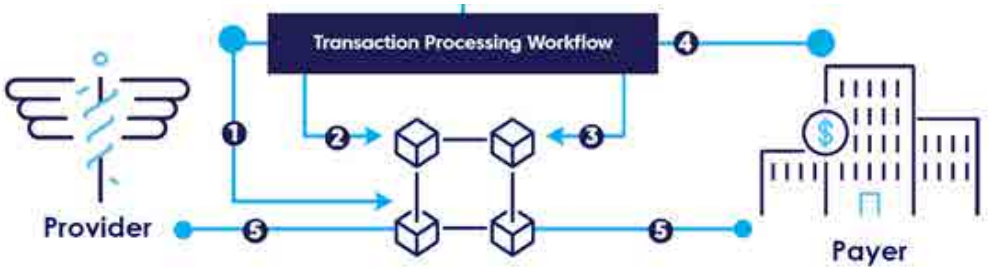
- MedRec
  - 2016년 미국 MIT Media Lab과 이스라엘의 Beth Israel Deaconess Medical Center가 이더리움의 이더 플랫폼 기반 블록체인 원장(MedRec)으로 환자의 약물치료 정보 공유 시험
  - 시험에서는 의료기록이 발생될 경우, 임의 조작이 불가능한 의료기록 로그와 EHR에 대한 접근정보를 환자에게 제공하고 별도의 의료정보 중개기관 없이 환자가 선택한 제3의 의료기관에서 자신의 의무기록에 대한 조회 권한을 제공
  - 의무기록 생성/변경 통지단계에서는 의무기록이 생성되거나 변경되면 블록체인에 Hash값 저장하고 환자의 공개키로 EHR DB 주소 전송
  - 의무기록 내용 확인 단계에서는 환자의 개인키로 생성이나 변경된 의무기록을 확인하고, 환자 스스로 개인의무기록(PHR)에 저장할 것인지 결정
  - 의무기록 공유단계에서는 병원과 환자 간 스마트계약 사용하여 제3자에게 의무기록 생성기관의 EHR 주소를 제공하는 구조



출처 : MIT(2018)

[그림 7] MedRec 시스템 구조

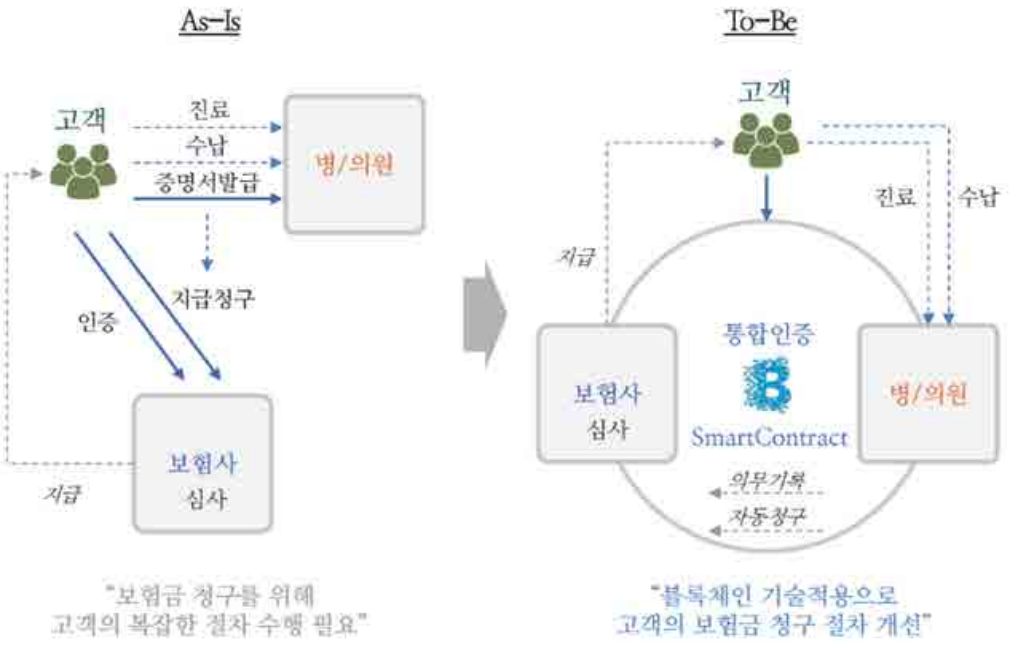
- 보험 청구 및 지급 사례 : change healthcare
  - 오픈 소스 블록체인 프레임워크인 Hyperledger Fabric 1.0을 사용하여 의료서비스 제공자와 보험지급자간에 청구 및 지불절차를 효율적으로 처리하는 분산 원장
  - 의료 공급자에 의한 보험 청구 이벤트가 발생하면, 워크플로우가 블록체인에 요청 기록하고, 스마트 계약이 구현된 블록체인 이벤트가 워크플로우를 활성화하여 심사한 후 보험금 지급



출처 : Change Healthcare

[그림 8] Change Healthcare 사례

- 교보생명의 보험 청구
  - 교보생명과 디레몬이 2017년 과학기술정보통신부의 지원을 받아 블록체인 기술을 활용해 보험계약자에게 실손보험금 등의 자동 지급시스템 개발
  - 기존에 보험가입자가 진료 후 병원비를 수납하고 증빙서류를 발급받아 보험사에 제출하여야 하는 불편한 절차를 보험가입자가 보험금을 따로 청구하지 않아도 병원비 수납 내역과 보험사의 계약정보를 기반으로 보험금 지급하는 서비스
  - 블록체인 기술을 활용하여 보험유지고객이 별도의 보험금 신청없이 보험금을 지급하는 분산원장에 기재된 보험계약을 활용하는 방법으로 보험금 지급조건 충족시 의무기록 사본과 보험금 청구서가 자동 생성되어 청구되는 서비스



출처 : 교보생명(2017)

[그림 9] 교보생명의 보험청구

4. 블록체인 기술 적용

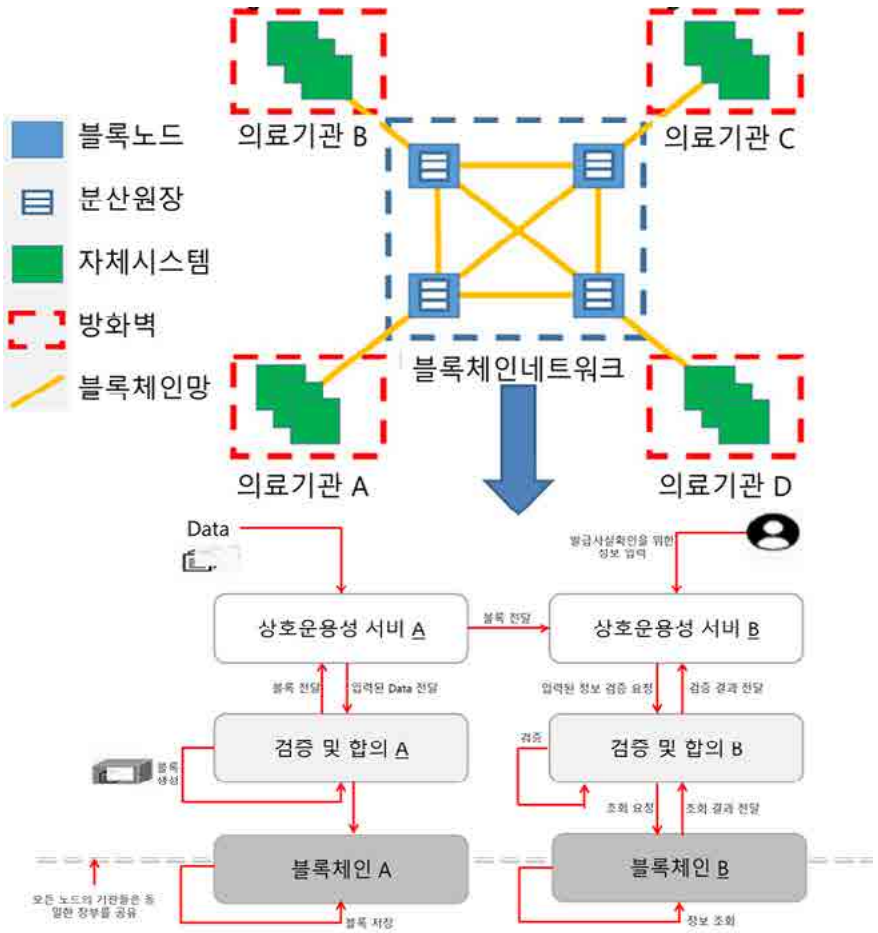
- 현재 우리나라에서 실시되고 있는 공공 보건의료 서비스 중에서 블록체인 기술 활용이 가능한 분야를 선정하면 의료기관간 진료정보 교류, 의약품 유통 등이 가능함
  - ▸ 공공 보건의료 서비스는 기존 제도에서 허가된 기관만 참여가 가능하므로 개방형이 아닌 승인된 기관만 네트워크에 참여하는 폐쇄형 블록체인 적용

[표 3] 공공 보건의료 서비스 적용 분야

구분	진료정보 교류	의약품 유통
개요	- 환자의 과거 진료기록(약물 처방기록, 검사기록 등)을 확인하지 못해 발생하는 약물사고 등 오진을 예방하고, 병원을 옮길 때마다 환자가 일일이 종이나 CD로 진료기록을 발급받아 제출했던 불편함 등을 해소하기 위한 사업	- 의약품의 생산과 수입부터 공급을 거쳐 최종 소비되는 과정의 의약품 유통현황 정보를 수집·조사·가공·이용 및 제공
이해 당사자	송신기관, 수신기관, 환자	제약사, 요양기관, 도매업체, 의약품관리종합정보센터

- 진료정보 교류사업은 4종에 대하여 시범서비스를 통해 과거 환자가 직접 방문하여 의료기록을 종이나 CD로 수령하여 전달하는 불편 해소 가능한 서비스로 블록체인 기술 적용시 파급효과가 예상되므로 블록체인 기반의 진료정보 교류 방법을 설명하면 다음과 같음
  - ▸ 의료기관간 진료정보를 교류하기 위해서는 블록체인을 기반으로 네트워크에 참여하는 의료기관이 연결되어야 하는데 의료기관의 자체시스템과 직접 연결이 어려우므로 별도의 중계서버를 설치
  - ▸ 의료기관간 정보의 공유와 상호운용성을 위한 중계 서버를 별도로 두고 이를 매개로 하는 방법이며, 블록체인 기반으로 진료정보 교류를 위해서는 블록관리 부분과 조회 부분으로 구분 필요
  - ▸ 블록 관리에서는 A라는 의료기관에서 발급된 인증서가 시스템에 입력되면 해당 데이터를 검증 레이어에 전달하고, 검증이후 공유블록을 생성한 후, 블록체인에 공유블록을 저장 요청하고 상대 의료기관에 전달

▸ 공유블록이 B의료기관에 전달되면 해당 공유 블록을 검증과 합의를 진행한 후 블록체인에 저장



[그림 10] 진료정보교류 시스템 구조

5. 블록체인 한계 및 미래

- 블록체인 기술은 금융분야 뿐만 아니라 모든 종류의 자산이나 정보의 등록, 보관, 거래에 적용될 것임(과학기술정책연구원, 2017)
  - 초기에는 인증 등 보안 분야를 시작하여 비용절감 효과가 큰 자산에 대한 거래 후 과정, 지불결제 및 송금, 스마트계약 분야로 확산될 것으로 전망됨
  - 4차 산업혁명의 핵심 산업인 보건의료 분야도 블록체인을 이용하여 기존의 거버넌스나 신뢰구조를 빠르게 대체 할 것으로 예상

- 블록체인은 초연결 사회를 해결해 줄 수 있는 비용 효율적인 대안이지만 아직 기술적으로 해결할 과제들이 존재함
  - 블록체인은 거래처리 시간의 단축, 중개자의 오버헤드 비용 감소로 인한 비용절감, 조작 및 사이버 범죄 위험 감소, 분산원장 및 프로세스 공유로 위변조가 어려워짐에 따른 신뢰성 증가 등의 장점을 가지고 있음
  - 반면 거래 내역이 공개됨에 따라 원칙적으로는 모든 거래가 추적 가능하여 완벽한 익명성 보장이 어려울 수 있으며, 채굴이 대형 마이닝 풀에 집중됨에 따라 실시간, 대용량 처리의 어려움이 존재
  - 블록체인 기술의 장점을 최대한 활용하려면 개방과 공유가 중요하므로 실행과정에 필요한 일련의 규칙에 합의해야하는 사회공동체의 공감대 형성이 필요

- 보건의료 분야에서는 블록체인 기술이 개인 건강정보 관리, 의료기기 및 약물의 추적, 임상시험 및 연구 데이터의 공유와 활용, 개인 의료정보 보호, 책임추적성 등 전반에 걸쳐 활용될 것으로 기대됨
  - 특히 정보의 기밀성과 가용성은 상호 배타적인 근본적인 문제를 지니고 있었으나 블록체인은 정보 기밀성과 가용성 모두를 충족이 가능하므로 보건의료 분야의 변혁을 주도할 것으로 예상됨

참고 자료

[1] 과학기술정책연구원, 블록체인 기술동향과 시사점, 2017

[2] 금융보안원, 블록체인 응용기술 개발 현황 및 산업별 도입 사례, 2017

[3] 한국보건산업진흥원, 헬스케어 산업에서의 블록체인 기술의 활용, 2017

[4] Deloitte, Blockchain:Opportunities for Health Care, 2016

[5] Gartner, Top 10 Strategic Technology Trends for 2018, 2017.10

[6] Gartner, Forecast: Blockchain Business Value, Worldwide, 2017-2030, 2017.10

[7] IBM, Making blockchain real for business explained, 2018.

[8] MIT, MedRec: Medical Data Management on the Blockchain, https://viral.media.mit.edu/pub/medrec

[9] World Economic Forum, The future of financial infrastructure, 2016.8

[10] https://hitconsultant.net/2017/09/25/change-healthcare-enterprise-blockchain-healthcare/

[11] http://blockchain-finance.com/

[12] http://www.itworld.co.kr/print/94202