ISSN 2508-6820

Innovating Data into Strategy and Business

BIO ECONOMY REPORT

April 2018. Issue 11

블록체인 기술과 헬스케어 데이터 혁신

KoreaBio 한국바이오협회

한국바이오경제연구센터
KOREA BIO-ECONOMY RESEARCH CENTER

BIO ECONOMY REPORT
April 2018. Issue 11

블록체인 기술과 헬스케어 데이터 혁신

문세영 부센터장

들어가는 말

블록체인 기반의 디지털 자산에 자금이 몰리면서 블록체인 기술은 우리에게 익숙한 이름이 됐다. 최근에는 블록체인 기술의 헬스케어 분야에 대한 적용이 활발히 논의되고 있기도 하다. 지난 리포트[1]에서 블록체인 기술이 바이오헬스산업에 접목될 수 있는 가능성을 개략적으로 살펴봤다. 이번 호에서는 블록체인 기술이 헬스케어 생태계를 혁신하기 위한 문제의식과 기술적인 과제들을 살펴보고 헬스케어 산업에서 블록체인 기술의 가능성과 한계를 가늠해보고자 한다.

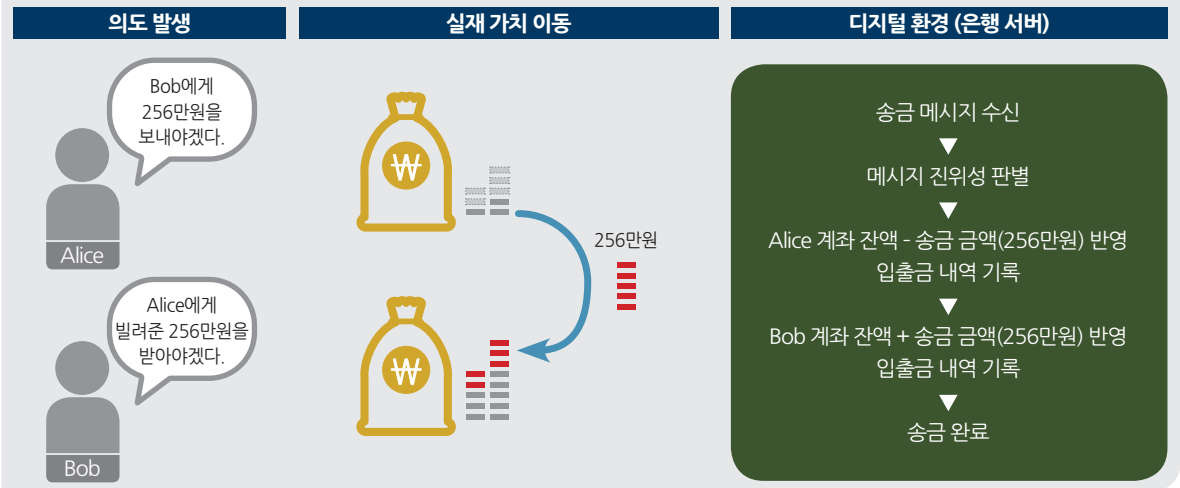
"인간을 전적으로 신뢰할 수 없기 때문에 신뢰 가능한 체제는 항상 비용을 동반한다."

1) 안지영, "블록체인 기술과 바이오헬스 산업," Bio Economy Report 2018 09호

블록체인의 등장으로 신뢰에 대해 다시 생각하다

신뢰는 현대 사회를 유지하는 근간이 되는 개념이다. 신용카드 없이 보내는 하루를 상상하기 힘들 정도로 우리의 경제 활동의 대부분은 디지털 기술과 신뢰를 바탕으로 구축되어 있다. 그러나 인간이 신뢰할 만한 존재인가에 대한 답은 저마다 다르기 때문에 신뢰를 토대로 구축한 체제는 비용을 동반한다. 불완전한 신뢰로 인한 불확실성을 통제하기 위해 "믿을 수 있는" 제

[그림 1] 은행을 통한 금전 거래 상황

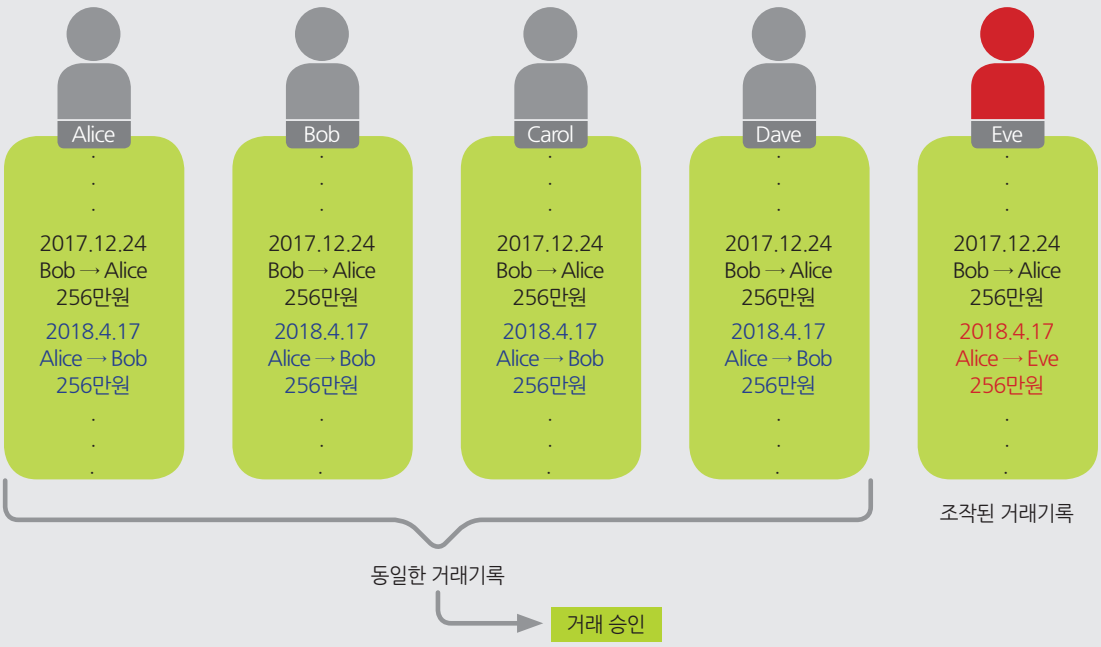


삼자를 동원하는 것이 가장 손쉬운 해결책이고 대부분의 상황에서 인류가 지금까지 선택해 온 방식이다. 우리는 은행을 신뢰하고, 은행이 스마트폰 뱅킹 어플리케이션에 보여주는 계좌 잔고 숫자를 신뢰한다. 화폐를 사용하지 않고 앨리스가 밥에게 256만원을 주고 싶다면 앨리스는 은행에게 밥의 계좌로 256만원을 송금하라는 메시지를 보내고, 은행은 앨리스의 계좌 잔고를 확인한 후 256만원을 차감하고 밥의 계좌 잔고에 256만원을 더해준다.[2] 앨리스와 밥이 은행을 신뢰하는 한 이들의 거래는 전자적으로 무결하고, 그 무결성을 은행이 담보한다.

그러나 "믿을 수 있는" 제삼자가 과연 무한한 시간 동안 무한한 신뢰를 담보할 수 있을지를 생각해보면 의문이 생기는 게 당연하다. 은행의 전산 시스템이 해킹을 당할 수도 있고, 범죄에 연루되었다는 의혹으로 계좌가 동결될 수도 있다. "믿을 수 있는" 제삼자를 배제한 거래 플랫폼의 힌트는 인류가 지금으로부터 약 7,000년 전부터 사용해온 장부에서 찾을 수 있다.[3] 앞선 사례에서처럼 은행이 단일한 장부를 관리하는 방식[4]이 아니라 거래에 참여할 수 있는 모든 사람들이 장부를 가지고 자신의 거래 내역을 순차적으로 기입하는 방식을 생각해보면 그리 나쁜 방법은 아니다. 다만 직접 자신의 디지털화된 거래 장부를 관리할 때 실제 지출보다 작게 기입하고 싶은 욕망을 이기지 못한다면 심각한 인플레이션과 공황이 발생하는 것은 시간 문제다. 블록체인 기술을 대중에게 알린 Bitcoin은 은행과 같은 중앙화된 "믿을 수 있는" 제삼자의 개입 없이 완전히 분산화된 통화체제를 추구한 결과물이다.

2) 암호학이나 전산 보안에서 프로토콜 설명시에 사용하는 이름으로 알파벳 순서로 A는 Alice, B는 Bob, C는 Carol 등이다.
3) 인류의 가장 오래된 회계기록물은 메소포타미아의 점토판에서 나타난다.
4) 실제 은행에서는 전자금융감독규정에 따라 전산상 동일한 데이터를 미러링하여 관리한다.

[그림 2] 분산원장을 이용한 거래



30년 암호 통화 역사의 이정표, Bitcoin

"비트코인은 암호기술을 적용하여 위변조가 어렵게 한 순차적 거래 정보를 단위로 하는 전자 통화체제다."

신뢰를 바탕으로 권한이 집중된 기관에 의존하지 않는 암호통화(cryptocurrency)[5]가 실질적으로 제안된 것은 1983년이다. UC버클리 암호학자 David Chaum은 RSA 암호[6]를 이용해 화폐의 암호화 공식을 개발했고 DigiCash라는 회사를 설립했다. 그로부터 25년이 지난 2008년, 사토시 나카모토(Satoshi Nakamoto)라는 필명을 내세운 개발자(혹은 개발자 그룹)가 암호화 기술 메일링 리스트에 공개한 논문에서 비트코인이라는 해시 암호를 사용하는 암호통화를 구현했고 여기에 블록체인 기술을 적용했다. 블록체인 기술은 위변조가 불가능한 시간 기록(time stamp) 도구로 1991년 처음 제안된 바 있다.[7] 결국 비트코인은 현실적으로 와해하기 어려운 암호기술을 적용해서 만든 위변조가 어려운 순차적 거래 기록을 정보의 단위로 하는 전자 통화체제다.

현존하는 수많은 블록체인 기술에 대한 이해를 돕기 위해 비트코인이 구현되는 방식을 살펴보도록 하자. 앞서 기술했듯이 비트코인은 "믿을 수 있는" 제삼자의 개입이 필요 없는 전자통화 체제다. 제삼자를 제외하기 위해 통화 체제에 속한 모두가 전자거래원장을 소유하고, 자신의 거래 내역을 시간 순으로 업데이트 하는 방식이다.[8] 이런 전자통화 체제는 다음의 조건들을 충족해야 한다. 첫째, 모두가 모든 거래 정보를 소유하되 그 모든 정보는 동일하게 유지한다. 거래 정보를 제삼자에게 맡기지 않는 대신 참여자 모두가 공유한다. 동일한 정보를 분산함으로써 백업과 대조의 기능을 기대할 수 있다. 둘째, 거래정보는 계좌의 소유자가 전자서명을 포함하여 생성하고 네트워크 상에 공유한다. 누구나 자발적으로 참여할 수 있는 체제에서 계좌 소유자가 직접 정보를 생산하도록 하기 때문에 정보 생산자와 계좌 소유자의 일치를 확인할 수 있는 강력한 전자서명이 필요하다. 셋째, 새로운 거래정보는 현재 계좌잔고의 한도를 넘지 않는 범위에서 유효하다. 비트코인은 거래 정보를 기본 단위로 다루기 때문에 거래의 시점에서 잔고를 확인해야 하고, 이전 거래들을 순차적으로 추적하는 방식으로 유효 잔고를 확인할 수 있다.

전자통화를 실제로 적용하려면 사용자 진위판별, DDoS[9] 와 같은 시스템 과부하 공격에 대한 방어, 고의에 의한 부당이득과 같은 발생 가능한 문제를 사전에 차단해야 한다. 비트코인은 암호화 기술을 적용하여 사용자 진위판별 문제를 해결했고[10] 반복구문을 포기하면서 DDoS 공격을 사전에 차단했다. 남는 것은 고의에 의한 부당이득의 발생이고, 누군가는 시스템을 속이려고 할 것이기 때문에 이 문제의 해결은 선량한 다수를 위한 시스템 구현에 필수다. 이 상황은 디지털 공간상 다자간 의사소통에서 거짓 메시지를 배척하는 문제로 Leslie Lamport 등이 작성한 비잔틴 장군의 문제라는 제목의 논문[11]으로 잘 알려져 있다. 문제 상황은 이렇다. 적의 성을 포위하고 최후의 일전을 앞둔 연합군의 장군들은 동시에 적을 공격해야 승리할 수

5) Cryptocurrency를 일반적으로 암호화폐로 칭하기도 한다. 정부·공공기관은 가상 통화라는 용어를 사용한다. 이 글에서는 암호화 기술의 중요성과 디지털 통화체제의 의미를 결합하여 암호 통화로 지칭하고자 한다.

6) RSA: 1997년 Ron Rivest, Adi Shamir, Leonard Adleman이 소수(prime number)를 이용한 암호화 복호화 기법을 개발했고, 이들의 이름 첫 글자를 따서 명명됐다.

7) Haber, Stuart, Stornetta, W. S, "How to time-stamp a digital document," J. Cryptology (1991)

8) 분산원장의 개념이다.

9) Distributed Denial of Service, 분산 서비스 거부 공격. 수많은 컴퓨터가 동시에 대량의 정보를 전송하여 과부하를 유도하는 공격

10) 시스템 내에서 메시지 전송자의 진위 판별은 가능하지만 해킹에 의한 개인 암호 유출에 대한 위험은 여전히 존재한다.

11) Lamport, Leslie et al., "The Byzantine generals problem," ACM TOPLAS

[그림 3] 분산형 디지털 통화체제의 필요 조건

있고, 공격 방식(시간)에 대한 합의를 도출해야 하지만 모여서 회의를 할 수는 없다. 오로지 전령을 통해서 메시지를 주고받을 수 있다. 장군들 중에는 배신자가 있고 그게 누구인지는 모르는 상황이다. "믿을 수 있는" 장군들은 최상의 공격 방식을 메시지로 전하여 동시에 공격해서 승리하고 싶지만 배신자는 메시지에 혼선을 주고 연합군의 승리를 방해할 것이다. 비유적으로 설명했지만 현실 세계에서 다수의 정보생산 단위가 모여 있는 컴퓨팅 시스템 혹은 통신 네트워크가 늘 안고 있는 문제이고 디지털 기술을 토대로 네트워크 효과가 극대화 될 것으로 예견하는 4차 산업혁명 시대에 반드시 해결해야 할 문제이기도 하다.

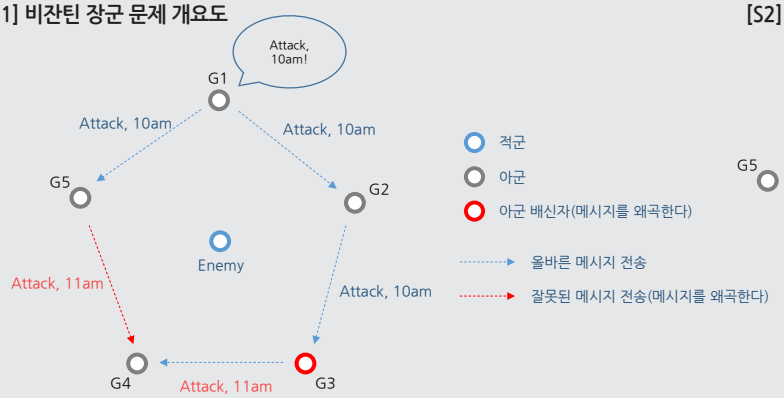
"비잔틴 장군 문제에 기술적으로 구현 가능한 대안을 제시함으로써 블록체인은 4차 산업혁명의 핵심기술이 됐다."

비잔틴 장군의 문제에 대해 비트코인은 작업 증명 방식이라는 합의 알고리즘을 제시했다. 메시지의 전송 단위인 블록을 생성하기 위해 해시 암호를 만족하는 계산을 하는 노력[12]을 강제하고 블록을 생성하는 주체들이 경쟁적으로 블록을 생성하게 한다면 소수의 "배신자"가 부정한 방법으로 시스템을 압도하는 일은 확률적으로 일어나기 매우 어렵다. 노력을 통해 메시지의 진의를 증빙하는 합의 방식을 작업 증명(proof of work, PoW)이라 부른다. 분산화된 디지털 통화를 구축하는데 "배신자"로 인한 문제를 해결하기 위해 작업의 난이도를 높게 설정하면 개인이 통화를 사용하는 편익보다 발생하는 비용이 커져서 아무도 사용하지 않을 것이

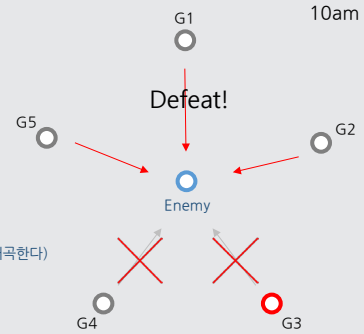
12) 무작위 수치 대입과 해시값의 검증 작업을 요구한다. 상당한 계산능력이 필요하기 때문에 자원(computing resource) 소모를 동반한다.

[Box 1] 비잔틴 장군 문제와 작업 증명(PoW) 방식의 해법

[S1] 비잔틴 장군 문제 개요도



[S2] 배신자로 인해 공격이 실패하는 상황



비잔틴 제국은 적국의 도시를 점령하려고 연합군을 모았다. 병사들은 각 장군의 지휘를 받으며, 장군들은 모여서 작전을 논의할 수 없고 오로지 전령을 통해 메시지를 교환하는 방식으로 합의된 작전을 수행해야 한다. 적군의 저항이 거세기 때문에 전군이 동시에 공격하지 않으면 각개격파를 당할 것이다.

상황이 더 어려운 것은 병사를 이끄는 장군이나 메시지를 전달하는 전령 중에 배신자가 포함돼 있고, 배신자는 메시지를 왜곡하여 협동작전을 방해하고 제국은 전쟁에서 패하고 말 것이다. 어떻게 하면 배신자의 방해에도 불구하고 합의된 작전 수행으로 전쟁에서 승리할 수 있을까?

위의 이야기는 역사에서 사라진 비잔틴 제국의 전쟁 이야기로 빗대어 설명한 다자간 메시지 송수신 상황에서 오류(fault)에 내성이 있는 통신 프로토콜의 수립에 대한 문제다. 분산 컴퓨팅의 아버지로 불리는 Leslie Lamport가 Robert Shostak, Marshall Pease와 공저한 논문에서 악의적인 참여자(배신자)로부터 시스템을 지킬 수 있는 방법을 찾기 위해 공론화 했다.

그림 S1에서와 같이 G3이 배신자이고, G5가 G4에게 전하는 메시지를 메신저가 실수로 왜곡하는 경우, G3(배신자)와 G4(잘못된 메시지 수신)는 정해진 시각(10시)에 공격에 가담하지 않고, 연합군은 패배하게 된다(그림 S2). 신뢰를 담보할 수 없는 조건에서는 메시지의 생산 과정을 통제하는 것이 유일한 해법이다. 메신저(전령)의 실수로 인한 메시지 왜곡을 예방하기 위해서는 메시지에 장군의 친필 서명(수신자가 확인 가능)을 동원해서 메시지의 위변조를 방지할 수 있다. 실제 블록체인 상에서는 공개키 기반구조(Public Key Infrastructure)를 이용한 전자서명을 사용한다.

이제 남은 것은 의도적으로 메시지를 왜곡하는 배신자의 문제다. 수신한 메시지를 송신할 메시지에 연결하고, 메시지 작성에 일정 시간이 반드시 소요되도록 한다면 이 메시지를 수신하는 참여자가 메시지의 진위를 간접적으로 판별할 수 있게 된다. 예를 들어 G1, G2, G3, G4로 이어지는 순차적인 메시지 전송과 G1, G5, G4로 이어지는 순차적인 메시지 전송을 생각해보자. 하나의 메시지를 작성하는 데 10분이 소요되고, G3가 배신자라면 G4에게 보낼 메시지를 작성할 때 G1, G2가 순차적으로 보낸 메시지 모두를 위조해야 한다. 자신의 메시지까지 총 30분 이상이 소요된다. 반면 같은 메시지가 G5를 통한 루트로 전달된다면 G4는 20분만에 메시지를 전달받게 된다. G4는 메시지의 분량과 도착까지 걸린 시간으로 위변조를 가늠할 수 있다.

[S3] 작업 증명(PoW) 방식을 적용한 메시지 전송

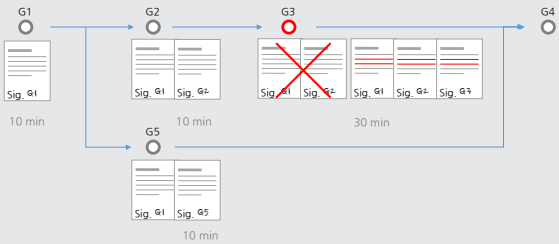


그림 S3는 이 같은 작업 증명 방식을 적용한 메시지 전송을 나타낸다. 그림에서 두 경로로 다른 메시지를 받은 G4는 G3를 통해 받은 메시지에 소요된 시간(10분 + 10분 + 30분 = 50분)과 B5를 통해 받은 메시지에 소요된 시간(10분 + 10분 = 20분)을 가지고 메시지의 진위를 파악할 수 있다.

이제 다자간에 실시간으로 통신이 이루어지는 상황에서 상충하는 메시지를 수신한 경우 G5를 통해 전달된 메시지를 채택하는 것으로 모든 참여자가 동의한다면 배신자는 동기를 상실하게 된다. 메시지 전송의 프로토콜을 수립하는 것만으로 인위적인 위변조 가능성으로부터 안전한 시스템을 갖게 됐다.

다. 비트코인 체제는 블록 생성에 소요되는 노력 중 시스템의 합의로 채택된 유일한 블록에 대해 비트코인이라는 인센티브를 제공한다. 결국 비트코인의 합의 방식은 비잔틴 장군의 문제에 기술적으로 구현 가능하며 현실적으로 수용 가능한 해법을 제시했다고 볼 수 있다.[13] 블록체인 기술이 4차 산업혁명의 핵심 기술로 거론되는 이유이기도 하다.

암호와 블록, 그리고 합의 방식으로 산업 생태계 혁신에 도전장

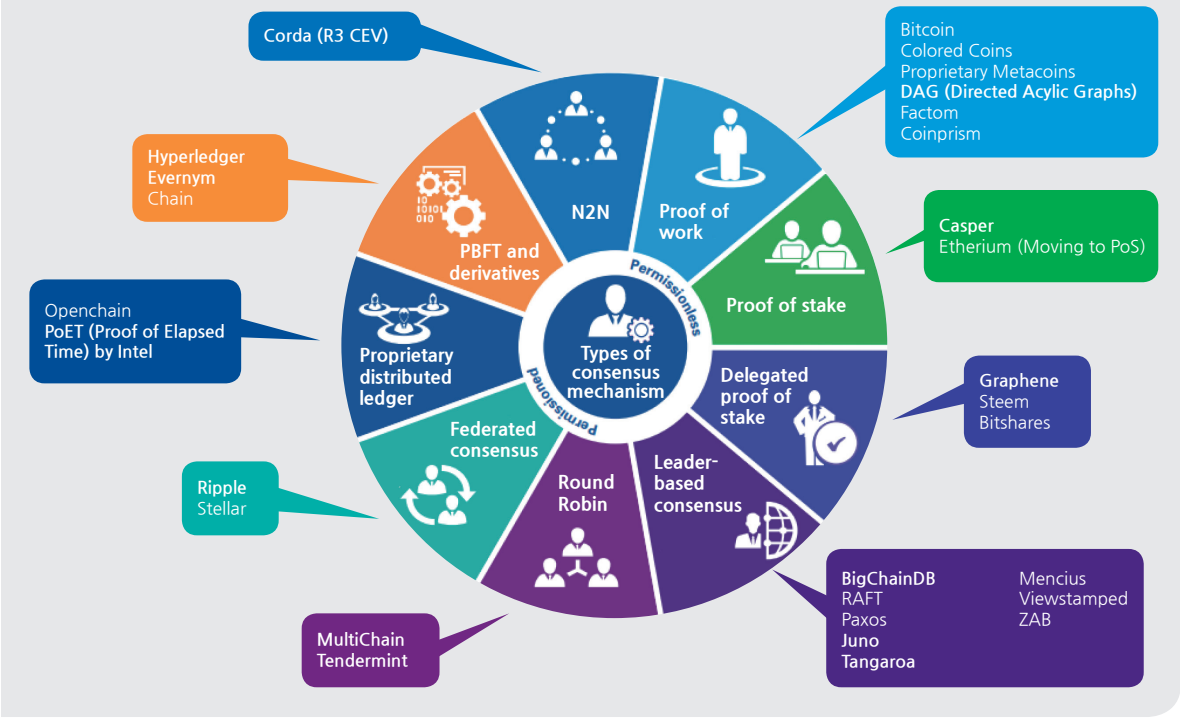
"블록체인 기술은 강력한 암호화, 다양한 합의 방식으로 산업계의 문제에 특화된 해결책을 제안한다."

비트코인의 사례로 살펴봤지만 메시지의 요체와 합의 방식에 따라 다양한 형태의 블록체인 플랫폼들이 있다. 비트코인으로 대표되는 1세대 블록체인은 암호통화를 실제 구현 가능하도록 했다는 데 의의가 있다. 디지털 분산원장은 제삼자의 개입을 배제한 거래승인을 가능하게 했고, 해시암호를 이용한 블록체인 기술과 PoW 합의방식은 위변조 가능성을 매우 희박하게 만들었다. 2세대 블록체인으로 불리는 이더리움은 스마트 계약(smart contract)을 구현한 소프트웨어 플랫폼이다. 누구나 이더리움을 기반으로 다양한 계약 조건에 따라 결과물을 산출하는 방식의 어플리케이션을 만들어낼 수 있기 때문에 보다 확장성을 갖게 됐다고 평가 받는다.

블록체인 플랫폼은 분산된 주체들이 합의된 동일한 결과물을 공유하는 것을 원칙으로 한다. 이 때 사용하는 합의 방식은 블록체인의 고유한 기술적 특징이기도 하면서 활용성에도 영향을 미치는 요인이다. 비트코인의 사례에서 소개한 작업 증명은 이제 너무 유명한 합의 방식이다. 작업 증명은 합의가 필요한 메시지의 생산에 에너지를 소비하게 하고, 나쁜 의도로 체제를 속이려는 참여자의 보상을 박탈하는 원리로 작동한다. 체제의 유지를 위해 막대한 양의 에너지가 소모되며, 유일한 기여자에게 보상을 집중하는 방식으로 에너지 활용의 비효율성이 문제로 제기되기도 한다. 다른 합의 방식으로 지분 증명(proof of stake, PoS)이 있다. 메시지에 대한 신뢰 여부를 체제 상에 존재하는 자원의 총량 중 메시지 생산자가 가진 지분에 따라 결정하는 방식으로 에너지 소모를 줄여 체제 유지에 필요한 비용을 감소하고 참여자의 진입 장벽을 낮추는 효과가 있다.[14] 여기서 파생된 방식으로 자원의 집중에 따른 체제의 중앙화 효과를 상쇄하기 위한 위임 지분 증명(delegated proof of stake) 방식도 있다. 그 밖에도 체제 전체의 합의 도출을 위해 필요한 정족수를 분할하는 연방 합의 방식(federated consensus), 필요한 경우를 제외하고 양자간의 합의를 체제 전체가 존중하는 분산 합의 방식(distributed consensus, or node-to-node consensus), 임의의 대표를 선출하여 합의 결정을 위임하는 리더기반 합의 방식(leader-based consensus) 등 다양한 합의 방식이 존재한다. 합의 방식은 블록체인 기술이나 분산 원장만을 위해 고안된 것이 아니라 그 전에도 존재해오던 방법들로 상황과 활용도에 맞게 블록체인 기술에 접목되고 있다.

13) 비잔틴 장군 문제에 대한 실질적인 대안은 1999년 Practical Byzantine Fault Tolerance에서 제시된 바 있다.
14) BitFury Group은 2015년 이러한 내용을 골자로 하는 백서를 공개했다.

[그림 4] 분산된 합의 방식의 종류



출처: KPMG, 저자 재구성

정리하면 블록체인 기술의 핵심적인 요소는 메시지에 해시 암호를 적용한 연결된 블록 구조의 데이터와 임의의 다자간에 합의를 도출하는 방식이다. 따라서 특정 정보를 시간적 선후 관계에 따라 정렬하고, 투명하게 공개하며, 다수가 참여함으로써 혜택이 되는 분야라면 블록체인 기술이 도움이 될 여지는 있다. 산업 분야들 중 금융, 통신, 물류, 헬스케어 등이 대표적으로 거론되는 블록체인 응용 분야이지만 최근 보고자료에 따르면 무려 36가지 산업에서 블록체인이 혁신을 가져다줄 가능성이 높은 것으로 예견됐다.[15] CBInsights의 자료에 나타난 36가지 분야를 분류해보면 금융 일반, 인터넷 서비스, 사회안전 및 공공, 보건의료, 인증, 경영, 산업 혁신, 공유경제, 문화/스포츠 분야에 이르기까지 우리 사회 전반을 망라한다. 한국과학기술기획평가원의 연구보고서에서는 금융, 의료, 물류/유통, 에너지, 공공서비스 분야로 구분하기도 했다.[16]

15) 36 industries blockchain can transform, CBInsights
16) 유거송, 김경훈, "블록체인," KISTEP 기술동향브리프, 2018-01호

분류	상세 분야
금융 일반	은행, 헷지펀드, 크라우드 펀딩, 선물 투자, 주식 거래, 부동산, 보험, 암호통화 거래 중개, 신용기록 관리
인터넷 서비스	인터넷 신원과 도메인명, 클라우드 저장, 클라우드 컴퓨팅
사회안전 및 공공	사회안전망 보안, 투표, 정부와 공공기록, 총기 추적, 법 집행(증거 관리)
보건의료	의료/헬스케어 데이터 관리
인증	유언과 유산, 교육/학력 증빙
경영	인적자원 관리, 비즈니스와 회사 지배, 기프트카드와 고객관리, 인터넷 광고, 공급망 관리
산업 혁신	산업 IoT, 에너지 관리
공유경제	차량 공유, 3D 프린팅 인프라 공유, p2p 거래, 차량 대여와 판매, 기부
문화/스포츠	스포츠 배팅, 문화 컨텐츠 저작권, 스포츠 매니지먼트

출처: CBInsights, 저자 재가공

헬스케어의 오랜 숙제: 데이터, 유통

"블록체인 기술이 지향하는 신뢰 프로세스를 적용하여 헬스케어의 고질적인 데이터와 유통망 관리 문제를 해결할 수 있을까?"

헬스케어에 대한 정의는 관점에 따라 다르다. 메리엄웹스터는 헬스케어를 훈련받고 면허를 가진 전문가에 의한 육체, 정신 또는 감정상의 건강을 유지하거나 복원하려는 노력으로 정의하고 있다.[17] 넓은 의미에서 헬스케어는 치료를 중심으로 하는 보건의료 서비스와 질병 예방 및 관리 개념을 포괄하는 전반적인 건강관리로 정의되며, 좁은 의미에서는 원격 검진, 건강 컨설팅 등의 전통적인 의료 외 영역을 뜻하는 것으로 정의하기도 한다.[18] 어떤 정의를 사용하든 헬스케어는 인간의 건강과 직결되는 각종 서비스를 포괄한다. 수명이 증가하고, 생활환경이 변화하고, 인구와 물류의 이동이 잦아지면서 건강을 위협하는 요인이 다양해지는 현대 사회에서 헬스케어에 대한 개인, 사회, 국가와 국제사회의 관심이 고조되고 있다.

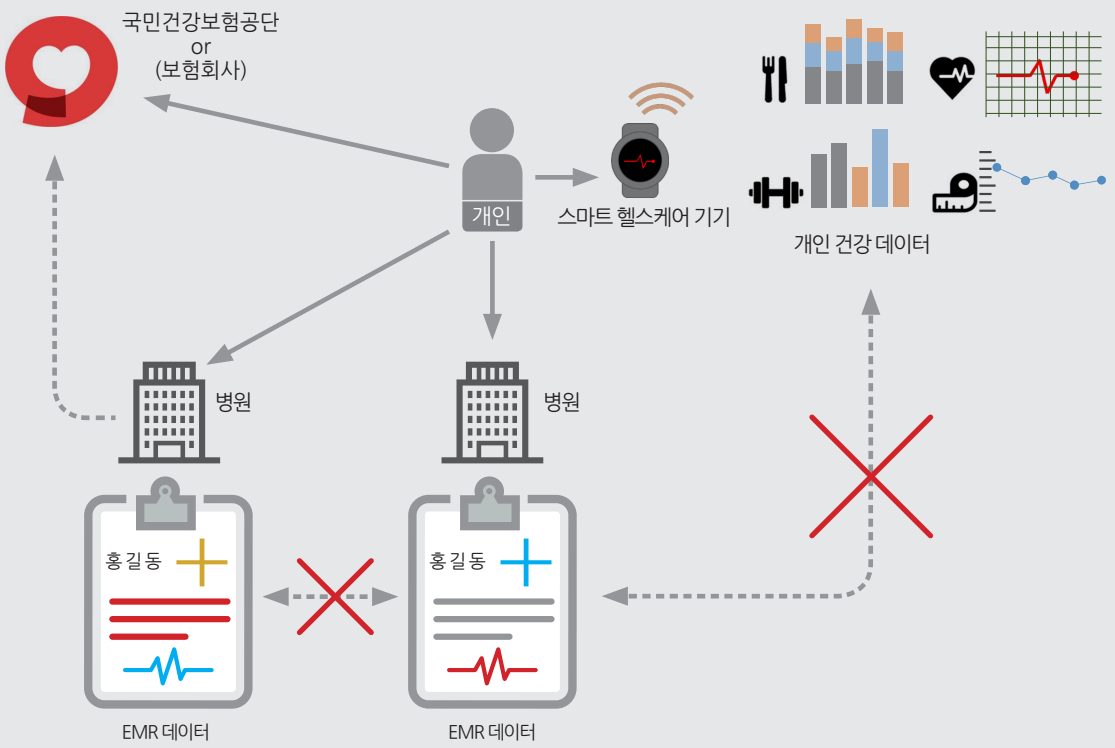
블록체인은 디지털 도메인 상에서 위변조할 수 없는 연쇄된 정보구조를 도구로 무신뢰의 영역에 적용 가능한 신뢰 프로세스를 제안한다. 전문가들은 블록체인 기술이 의약품의 제조, 유통이나 헬스케어 관련 연구개발의 수행 과정에서 생성되는 제품 정보와 임상 데이터의 무결성을 담보할 해법을 제시할 수 있을 것으로 기대한다. 블록체인이 헬스케어의 혁신을 가져올 수 있는 세부 분야로 의료정보 관리, 의약품 개발과 공급망 무결성, 보험 청구 관리, 의료 연구(임상연구정보 관리), 의료정보 보안 정도가 거론된다.[19]

가장 직관적으로 생각할 수 있는 의료정보의 관리 문제는 헬스케어 커뮤니티에서 상당 기간 고민해오던 이슈다. 전통적인 헬스케어 서비스 체제에서는 의료기관(헬스케어 전문인)과 개인의 관계가 서비스 공급의 통로다. 서비스 공급을 둘러싼 전체 구조에는 서비스와 관계된 정보를 토대로 개인, 의료기관, 공보험 당국, 민간 보험사들이 연결되고, 헬스케어 서비스로부

17) "efforts made to maintain or restore physical, mental, or emotional well-being especially by trained and licensed professionals —usually hyphenated when used attributively"- Merriam-Webster
18) 한경 경제용어 사전
19) Forbes, "This is why blockchains will transform healthcare" 2017.11.29

터 파생되는 연구개발 영역까지 포함하면 제약사, 의료기기 제조사, 규제당국이 연결된다. 방대한 데이터 유통망이 구축되고, 이 네트워크에서 유통되는 데이터는 개인의 의료정보와 파생정보들이다.

[그림 5] 헬스케어 데이터 생산과 분절



인간이 가지고 있는 생물학적 다양성과 가변적인 환경의 영향으로 인해 헬스케어에서 유의미한 데이터는 기하급수로 증가하고 있으며, 헬스케어 서비스 기관(병원, 제약회사)은 다양한 인구집단에서 발생하는 정보를 취합하고자 하는 유인이 있다. 결국 기관 단위로 생산, 관리하는 개인의 헬스케어 데이터의 기관들 간 상호운용성 확보는 어찌 보면 헬스케어 커뮤니티의 숙원인 셈이다. 최근 주목받고 있는 공통데이터모델(common data model, CDM) 기반의 분산형 데이터 상호운용 체제도 이 문제의 해법으로 제안된 방안이다.

블록체인은 금전뿐 아니라 디지털화 가능한 모든 종류의 정보의 교환을 관리할 수 있는 메타정보 관리 방안을 제안한다. 앞선 사례에서는 개인의 계좌 잔고를 추적할 수 있는 거래정보의 원장을 분산관리하는 방안을 묘사했다. 거래정보의 내용이 어딘가에 존재하는 개인의 헬스

케어 데이터로 바뀐다면 헬스케어 데이터에 대한 소유 증명과 정보 거래에서 파생되는 효과(경제적 이익 배분)를 개인 수준에서 정의할 수 있다는 것이 이 분야에 도전장을 내민 블록체인 기술의 비전이다. 이들의 계획이 실현된다면 개인의 헬스케어 데이터의 소유권과 관계된 권리행사를 정당화하고, 데이터의 교환을 활성화하면서도 파생되는 경제적 이익 배분을 공정하게 할 수도 있을 것으로 기대된다.

블록체인이 해결책을 제시할 수 있을 것으로 기대하는 의약품의 공급망 무결성 이슈는 헬스케어 제품의 유통 관점에서 해결이 필요한 문제다. 2015년 식품의약품안전처가 발간한 국내외 위조의약품 유통 및 관리 현황 연구 보고서에 따르면 전세계적으로 유효성분 부재(32.1%), 표준품과 상이한 유효성분 함량(20.2%), 효과가 다른 유효성분 함유(21.4%), 포장 문제(15.6%), 불법 복제품(1%), 불순물이나 유독성분 함유(8.5%)와 같은 위조의약품 문제가 발견된다. 이러한 문제들은 신뢰와 관리의 이슈로 보고서에서는 규제당국의 적극적인 관리체계 구축을 해법으로 제안하고 있다.

헬스케어 혁신을 꿈꾸는 기업들

"이미 블록체인 기술을 의료정보, 유전체 정보의 관리에 활용하기 위한 개념검증(proof of concept)이 이루어 지고 있다."

이미 국내외에서 블록체인 기술을 활용하여 헬스케어를 혁신하려는 노력이 다양한 모습으로 나타나고 있다. 의료정보의 유통을 개인이 직접 관리할 수 있게 하는가 하면 앞으로 생산될 개인의 유전체 정보 거래를 블록체인 기술로 구현하려 하기도 한다. 블록체인이 헬스케어 분야에 성공적으로 적용될 수 있을지 가늠하기 위해 대표적인 기업들이 해결하고자 하는 문제의식과 기술적 과제들을 살펴보자.

1. 써트온

CERTON

써트온은 2016년 5월 설립 후 블록체인과 보안인증 분야의 전문성을 인정받아 2017년 6월 포스링크의 자회사로 편입되었다. 2017년 9월에는 의료정보시스템 업체인 포씨게이트, LG 유플러스와 와 컨소시엄을 구성하고 의료제증명 서비스의 개념검증에 돌입했다. 블록체인 기술을 문서 이력관리에 적용하고 기존의 인증서비스에 연동하는 방식으로 서비스를 구현할 것으로 예상된다. 써트온은 의료기관이 부담해온 의료제증명 문서의 발급뿐 아니라 사용 이력까지도 관리할 수 있는 원스톱 솔루션을 지향한다. 컨소시엄은 서비스 구축으로 의료제증명 문서 발급을 용이하게 하면서도 보안 수준을 유지하겠다는 목표를 가지고 있다. 그러나 보건소 등의 제증명 문서는 상당수 온라인 발급이 가능하고, 대학병원 등 의료기관들도 온라인 의료제증명 발급 서비스를 제공하고 있다. 현재 의료제증명 문서는 해당 기관을 통해서 발급을 받아야 하기 때문에 여러 의료기관을 이용하는 소비자들에게 동일한 플랫폼 상에서 모든 의료기관의 의료제증명 발급은 편리한 서비스가 될 것이다. 그러나 아직 개념증명 단계로

증명서 보존 비용과 발급비용 등 수익모델이 뚜렷하지 않다. 서비스의 추가적인 기능으로 제시하는 의료제증명 문서의 이력관리가 사용자에게 얼마나 매력적인 솔루션이 될지가 서비스 도입 여부를 결정하게 될 공산이 크다.

2. 메디블록

메디블록은 의료정보가 의료기관에 분산되어 있는 상황을 개선하고자 하는 기업이다. 환자의 진료로부터 발생하는 모든 정보는 해당 의료기관이 관리한다. 일부 정보는 환자의 동의 하에 연구 목적으로 활용되기도 하고, 글로벌 제약사들은 의료기관과의 공동연구 형태로 정보에 접근하기도 한다. 그러나 의료기관에서 생산하고 관리하는 의료정보의 소유권은 환자 개인에게 있다. 메디블록은 바로 이 정보의 소유 주체를 매개로 분산된 의료정보를 통합할 수 있는 플랫폼을 만들려고 한다. 의료기관이 관리해온 개인의 의료정보를 소유자가 직접 관리하도록 하여 정보의 유통을 통제하며 원할 경우 대가를 받고 개인의 정보를 연구자(의료기관, 제약사)에게 제공할 수 있는 체제를 지향하고 있다. 이렇게 된다면 의료서비스의 이용으로부터 발생하는 의료정보의 보관과 관리의 비용도 개인이 지불해야 하는 필요성이 있다. 또한 블록체인 상에 다양한 비정형 의료정보를 포함하는 것은 불가능하기 때문에 블록체인과는 별도로 의료정보 저장소가 필요할 수도 있다. 무엇보다 의료정보의 생산 또는 관리에 인센티브를 부여하면서 개인에게 민감한 정보(병원, 진료과, 내역)를 공개하지 않는 합의방식을 찾는 것이 중요하며, 이는 현재 메디블록 개발팀의 최우선 과제이기도 하다. 스마트한 솔루션을 찾아낸다면 창업자들의 바람처럼 국내에서 최초로 블록체인을 헬스케어 분야에 적용한 사례가 될 것이다.

3. MedRec

MIT Media Lab에서 탄생한 MedRec의 문제의식은 메디블록과 유사하다. MedRec은 개인이 여러 의료기관을 거치며 평생 생산하는 의료정보의 원활한 통합과 전자의료기록(Electronic Medical Record, EMR)의 무결성을 추구한다. 개별적인 EMR 정보의 생성보다는 특정 요건에 맞는 정보를 질의하고 질의에 응하는 의료기관에 인센티브를 부여하는 방식으로 디자인하고 있다. MedRec이 추구하는 플랫폼에서 개인정보의 노출 없이 개인을 매개로 EMR 정보를 연계하는 것이 관건이며 어떤 정보보안 솔루션을 제시할지 많은 사람들이 관심을 갖고 지켜보고 있다.

4. Gem

의료정보의 통합관리 문제를 고민하는 Gem은 미국의 질병통제예방센터(Center for Disease Control and Prevention, CDC), 북유럽 공공섹터에 소프트웨어 솔루션을 제공하는 Tieto와 협력하여 분산 환경에서도 필요에 따라 관련된 정보들을 통합할 수 있는 유연한

정보관리 체계를 구축하려고 한다. Gem의 전략은 개인에게 글로벌한 식별자를 부여하고, 이 식별자에 개인의 의료정보의 위치를 연계하여 블록체인에 기록하는 것이다. Gem은 환자 중심의 헬스케어 생태계를 구축하려는 Philips의 Blockchain Lab과 파트너십을 체결하기도 했다. 분산된 헬스케어 정보 체제에서 유연한 정보의 흐름을 만들어내기 위해서는 정보를 보유한 기관과의 협업이 중요하다. CDC, Tieto와 팀을 이룬 Gem은 이 점에서 경쟁자들보다 앞서가는 듯한 인상을 준다. 자체개발한 블록체인 플랫폼인 GemOS를 기반으로 한 정보보안이 파트너십 구축에서 이점으로 작용한 것으로 보인다.

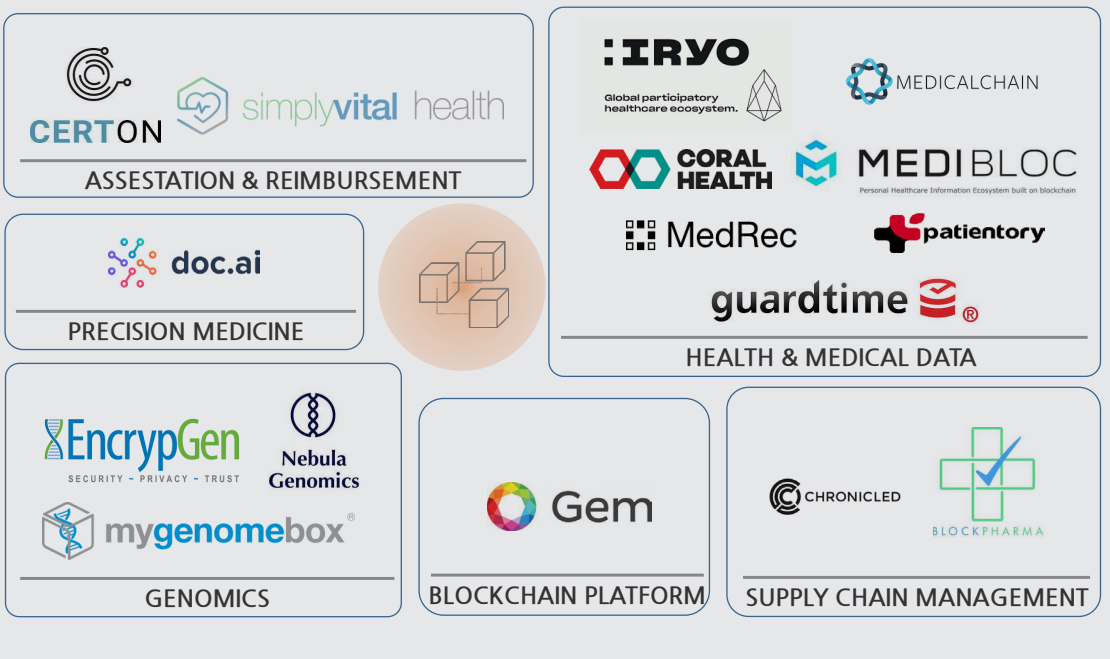
5. 마이지놈박스

마이지놈박스는 개인의 유전체 분석 결과를 토대로 다양한 어플리케이션을 적용하는 DNA 앱스토어를 구현하고 유전체 기반 오픈 플랫폼 비즈니스를 수행하는 기업이다. 차세대염기서열해독[20] 장비 기업 일루미나의 자회사인 Helix의 비즈니스 모델과 유사하다. 마이지놈박스는 최근 암호화폐공개[21] 계획을 발표했다. 유전체 분석기업이나 의료기관이 개인의 유전체 분석 결과를 제약사나 과련 연구기관에 제공하는 대가로 금전적인 보상을 받지만 유전체 정보의 최초 제공자인 소비자에게 이익이 배분되지 않는 점을 개선하려는 문제의식이다. 마이지놈박스의 비즈니스 모델은 암호 통화만 제외하면 유전체 분석 스타트업 Genos가 업계

20) Next Generation Sequencing, NGS, DNA 조각의 서열을 병렬로 읽어낸 후 조합하는 방식의 염기서열 해독 방식

21) Initial Coin Offering, ICO, 최초로 암호화폐를 발행하여 자금을 조달하는 일련의 과정

[그림 6] 헬스케어 분야 블록체인 적용 스타트업



에 제안한 모델과 동일하다. 소비자는 Genos의 키트를 구매하여 자신의 유전체 분석 결과를 받고, 제약사 등 수요처에 자신의 유전체 정보를 제공하고 대가를 지불받는다. 마이지놈박스의 경우는 DNA 앱스토어 플랫폼을 보유하고 있기 때문에 소비자를 플랫폼 내에 가두는 효과를 기대할 수는 있지만, 소비자들에게 암호통화 활용의 이점을 추가로 설득해야 하는 과제를 안고 있다.

헬스케어 분야에서 블록체인 기술의 가능성과 한계

"블록체인 기술이 정보와 유통망 관리의 투명성을 제공하며 헬스케어 데이터 혁신에 기여할 여지는 충분하다. 그러나 헬스케어의 현실은 블록체인과 같은 디지털 기술만 덧씌워서 해 결하기 어려운 문제를 안고 있기 도 하다."

살펴본 것처럼 헬스케어는 보다 나은 제품과 서비스의 발굴을 위한 정보의 유통과 신뢰 가능한 유통망 관리 체제 구축을 위해 블록체인 기술을 활용할 유인이 충분하다. 그러나 헬스케어의 현실은 블록체인이 제안하는 디지털 기술만으로 해결하기 어려운 문제를 안고 있기도 하다. 헬스케어 데이터 유통 과정을 투명하게 하는 일에 반대할 명분은 없지만 이같은 혁신 방안은 늘 기존 생태계의 저항에 부딪히게 마련이다. 헬스케어 서비스기관과 산업 주체들이 방대한 헬스케어 데이터를 활용하며 이 분야의 경제 규모에 기여하면서 스스로 부여한 인센티브까지 공개되는 상황을 받아들일지는 차치하더라도 데이터를 기반으로 경쟁우위를 점유하는 비즈니스 전략을 쉽게 포기하기는 어려울 것이다. 개인들도 민감한 개인 헬스케어 데이터를 공개된 블록체인 체제로 관리할 때 충분한 개인정보 보호를 요구할 것이다. 정보의 보호는 모든 참여자가 확인 가능한 정보를 토대로 인센티브를 제공하는 일반적인 블록체인 플랫폼의 작동 방식에 정면으로 배치되는 이슈이기도 하다. 관련된 프로젝트들이 이 문제를 어떻게 해결하는지 눈 여겨 볼 필요가 있다.

제품의 유통을 블록체인으로 관리하는 이슈에 있어서는 제품의 실물과 디지털 도메인의 비트들의 일치에 대한 담보가 필요하다. 의약품을 예로 들면 블록체인 상에 기록된 의약품의 신원을 실물 제품상에서 실수 혹은 고의로 위변조하는 상황은 블록체인 기술이 해결할 수 없는 문제다. 이런 상황에 적용 가능한 기술로 물리적 복제방지 기능(physically unclonable function, PUF)을 가진 반도체 칩의 적용을 고려해볼 수 있지만 이 경우 의약품 포장을 전면 수정해야 하는 수준으로 문제가 확대된다.[22)]

블록체인을 헬스케어에 적용하려는 기업들은 대부분 효율적인 의료정보의 유통에 초점을 맞추고 있다. 개인을 매개로 하여 각 의료기관에 분산된 정보를 통합하는 일은 무척 매력적인 일이다. 대규모 인구 기반의 가상 임상시험을 해볼 수도 있고, 보험사에 암호화된 인증 처리만 보내주면 보험료 청구가 자동으로 처리되는 편리한 서비스도 기대할 수 있다. 물론 의료기관들이 충분한 보안을 가지고 저장된 정보를 외부 블록체인 네트워크에 연계해주어야 하고, 정보의 생산, 관리, 유통에 발생하는 비용과 이익이 합리적으로 배분되어야 하고, 민감한 개

22) 최근 경희대학교 한호현 교수 팀은 PUF 칩을 기반으로 동작하는 퓨어체인을 개발, 공개했다.

인정보를 공개된 블록체인 플랫폼에 연결하는 것에 개인이 동의해야 하며, 이 모든 사안들을 충분히 감안한 사회적 합의를 도출하는 숙제만 해결된다면 가능한 일이다.

"코인에 대한 열기 속에서도 기술의 핵심과 우리가 해결해야 할 문제를 직시할 수 있어야 한다."

블록체인은 4차 산업혁명과 함께 대중의 관심을 받았고, 향후 많은 혁신사례를 창출할 수 있는 기술임에는 틀림 없다. 블록체인은 신뢰 프로세스 자체에 대해 다시 생각하게 한다는 점에서 기술 영역을 벗어난 정치 영역에 존재하기도 한다. 중요한 점은 기술로 해결하고자 하는 문제를 명확히 하고, 해결 방안에 대한 사회적 합의로 나아가는 과정이다. 블록체인 기술을 이용해 보다 나은 헬스케어 체제를 만들어가는 여러 팀들의 노력을 응원하며, 이들이 제안하는 문제와 해결방안에 우리 사회가 관심을 기울였으면 한다.

〈참고문헌〉

1. https://bitcoinmagazine.com/articles/gem-partners-nordic-tech-giant-tieto-and-cdc-put-healthcare-blockchain/
2. https://chainpoint.org/
3. https://enterprise.gem.co/health/
4. https://medium.com/tierion/liasion-partners-with-tierion-to-secure-enterprise-data-using-blockchain-proof-technology-d7001e6ad506
5. https://www.ibtimes.co.uk/gem-shows-off-first-blockchain-application-health-claims-1622574
6. 조선비즈, 암호화폐·가상화폐·가상통화… 정부·업계 관점따라 다양한 호칭, 2018.1.22
7. 안지영, "블록체인 기술과 바이오헬스 산업," Bio Economy Brief 2018년 09호
8. 유거송, 김경훈, "블록체인," KISTEP 기술동향브리프, 2018-01호
9. BitFury Group, "Proof of steak versus proof of work-white paper," 2015
10. Castro, M., Liskov, B. (2002) "Practical Byzantine fault tolerance and proactive recovery," ACM Transactions on Computer Systems 20 (4) 398-461
11. CBInsights, "Banking Is Only The Beginning: 36 Big Industries Blockchain Could Transform," Research Briefs, 2018.2.1
12. CBInsights, "How blockchain is disrupting insurance," Research Briefs, 2018.3.21
13. Frost & Sullivan, "Top 5 reasons why every healthcare company should invest in blockchsin," Frost Perspectives, Healthcare, 2017.9.5
14. Haber, S. & Stornetta, W.S. (1991) "How to time-stamp a digital document," J. Cryptology 3(2) 99-111
15. Lamport, Leslie et al., (1982) "The Byzantine generals problem," ACM Transaction on Programming Languages and Systems (TOPLAS) 4(3) 382-401
16. Nakamoto, Satoshi. (2009). Bitcoin: A peer-to-peer electronic cash system

April 2018. Issue 11

저자소개

문 세 영

한국바이오협회 한국바이오경제연구센터 부센터장
전화 : 031-628-0021
e-mail : smoon@koreabio.org

BIO ECONOMY REPORT

발 행 | **2018년 4월**
발행인 | **유 승 준**
발행처 | **한국바이오협회 한국바이오경제연구센터**
13488 경기도 성남시 분당구 대왕판교로 700
(삼평동, 코리아바이오파크) C동 1층
www.koreabio.or.kr

한국바이오경제연구센터
KOREA BIO-ECONOMY RESEARCH CENTER

Innovating Data Into Strategy & Business

ISSN 2508-6820