http://dx.doi.org/10.15813/kmr.2018.19.4.007

개인 의료정보 보호를 위한 블록체인 적용 방안: 프라이빗 블록 스킴을 중심으로[1]

A Blockchain Application for Personal health information: Focusing on Private Block Scheme

권 혁 준 (HyukJun Kwon) 순천향대학교 IT금융경영학과[2]
김 협 (Hyeob Kim) 연세대학교 정보대학원[3]
최 재 원 (Jaewon Choi) 순천향대학교 경영학과[4]

ABSTRACT

In this paper, I research the issue of information security for medical information system of each parties. The outflow of the Personal medical information can lead to problems of medical systems and disadvantage to an individual. In this paper, we research the information security based on a blockchain. In addition, I have analyzed blockchain. I suggest a medical information system framework that can help to keep the privacy of patients by using a blockchain network. Also, In this paper try to explain using private blockchain for medical system. Blockchain can keep the integrity and transparency of the medical records.

This research, shows how can build the private blockchain for medical records and how to get the integrity of Data from Private Blockchain and Distuributed Ledger Technology.

***Keywords**: Blockchain, Private blockchain, Private block scheme, Medical system*

1. 서론

최근 보건의료 분야는 병원중심에서 환자 기반 환경으로 급격하게 이동하고 있다. 이러한 변화의 기반에는 ICT의 비약적인 발전과 최신 의료기술(의료정보의 전산화, 네트워크화)이 접목되어 그 원동력을 이루고 있다(Griggs et al. 2018). 이에 따라 보건의료 관련 기관에서 생산 되는 모든 기록을 관리, 전달, 이용하는 방식에도 빠른 변화를 이루고 있다. 지금까지 활용되는 대표적 의료정보 시스템은 병원정보시스템(Hospital

1) 본 연구는 순천향대학교 학술연구비 지원으로 수행하였음.
이 논문 또는 저서는 2017년 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF2017S1A3A2065831).
논문접수일: 2018년 10월 7일; 1차 수정: 2018년 11월 21일; 게재 확정일: 2018년 11월 21일
2) 제1저자 (gloryever@sch.ac.kr)
3) 제2저자 (hyubiii@yonsei.ac.kr)
4) 교신저자(jaewonchoi@sch.ac.kr)

Information System)과 가장 널리 쓰이고 있는 전자의무기록(EMR, Electronic Medical Record, 이하 EMR)이 대표적으로 쓰이는 시스템이다. 이중 EMR은 환자의 질병과 관련이 있는 전체 사항과 병원에서 환자에게 제공한 검사, 치료 및 그 결과에 대한 사항을 의료인이 전자적인 형태로 작성한 것이다. 이러한 EMR은 보건의료 제공자들 사이의 진료 협력을 강화하는 의사소통 창구뿐만 아니라 여러 기간 동안 축적된 자료로서 정보를 만들어내고 이를 지식화해 환자에 맞는 최적의 진료 의사결정을 위한 방법으로 활용된다. 따라서 이를 체계적으로 보관하고 관리하며 신속하며 정확한 의무기록 및 여러 정보의의 작성 및 의무기록에 대해 의료정보 관계자들 에게 무결한 근거 자료를 제공해 주는 역할을 한다. 한편 의료정보의 정보화로 다량의 개인정보가 수집 및 보관되어 관련 기관들이 공유할 수 있어, 환자의 사생활을 보호하는 점이 중요한 관심사로 대두되고 있다. 또한 의료정보 유출에 따른 부작용은 사생활의 보호 차원을 넘어서 개인의 직업선택, 보험혜택, 금융기관 대출관련 등 개인의 경제활동에 직접적인 불이익을 초래할 수 있는 상황이며, 환자와 의료제공자간의 신뢰관계가 훼손될 가능성이 증대되고 있는 상황이다(박민정·채상미 2017).

정보발생의 원천인 보건의료기관에 의하여 의료정보가 대외적으로 비인가 자에게 이용되는 경우 특히 보안 문제가 발생될 수 있다. 이러한 개인의료정보를 취급하고 있는 의료분야는 개인정보보호 수준의 제고를 위해 정부차원에서 종합적, 체계적인 노력이 요구된다고 할 수 있다. 특히 환자 각 환자를 식별할 수 있는 개인의 의료정보는 환자의 상태, 질병 및 치료와 관련된 여러 정보를 의료기관에서 대부분 생산·보관·관리되고 있으며, 의료정보의 특성상 가장 민감하게 보호될 필요가 있는 부문이라 할 수 있다. 따라서 강력한 보호가 필요하며, 외부로 유출되거나 틀린 환자정보가 생산될 경우 개인의 사생활 및 개인정보가 침해될 수 있다. 따라서 본 연구에서는 환자와 의료기관 사이 또는 의료정보 소비자 간 환자의 프라이버시가 존중되고, 비인가 자에게 의료정보가 노출되지 않는 안전하게 의료정보를 공유하는 방안에 대해 연구하고자 한다. 이를 위해 네트워크 내의 모든 참여자가 거래 정보를 공동으로 소유 및 검증, 보관함으로써 거래 기록의 무결성, 신뢰성을 획득 및 확인 할 수 있는 블록체인을 적용한 방안을 제시하고자 한다.

2. 기존문헌 연구

2.1 개인의 의료정보

의료법 제21조(기록 열람 등)에서 의료정보를 '환자에 관한 기록' 이라 정의 하고 있다. 일반적으로 의료제공의 필요성을 판단하기 위한 것, 의료행위를 통해 수집된 자료 및 그 자료들을 바탕으로 한 연구 및 분석 정보 모두를 포함 것으로 진단과 치료행위, 치료 후의 환자 관찰 등이 전부 포함된다. 또한 의료행위 전체 프로세스 에서 수집된 그리고 결과들, 환자의 건강상태 등에 관한 정보를 의미한다. 환자 진료과정을 통해 산출되는 다양한 문자정보, 초음파 또는 방사선 등 화상정보들이 서로 병합되어 생성되는 정보로서, 개인신상 정보와 결합하여 해당 개인을 식별할 수 있게 되어 이에 따라 보호법익을 가지게 된다. 이러한 의료정보, 개인의료정보는 환자 진료 및 치료, 처방, 관련연구, 소

송에 따른 증거자료인 법률적 자료 제출, 의료비 청구 등 의료기관 내·외부적으로 다양한 분야에서 사용되고 있으며, 손실 혹은 파손이 발생하면 환자 안전에 위험이 발생하고, 비인기자의 접근이나 정보유출은 윤리적인 문제뿐만 아니라 해당 의료기관에 대한 평판저하와 대중적 신뢰도 하락 등의 위험이 발생한다(백윤철 2005).

건강과 관련된 개인의 의료정보는 다른 정보와 경중을 비교하여도 민감도가 매우 높은 개인정보이므로 의료정보는 인격권의 하나로서 충분한 보호를 받아야 한다(문성재·이경환 2005). 의료정보의 법율적 성격에 대하여 인격권적 부분에서 보호되어야 하는 자기정보 통제권에서 근거하는 것으로 일종의 기본권에 속한다라고 보고 있으며 또한 일반적으로 정보주체는 수진자이고, 정보 보유자는 의료기관이라고 보고 있다(이백휴 2010).

미국은 진료기록부의 소유권 및 저작권은 해당 의료기관에게 있고, 진료기록부에 포함되어 있는 의료정보의 소유권은 해당 환자에게 종속되어 있다라고 보고 있다. 또한 환자의 진료기록 접근 권을 인정하고 있다. 환자의 의료정보는 환자의 개인정보를 바탕으로 의료인의 객관적인 전문지식 및 가치판단이 첨가되어 작성·보관되고 법률상 그 작성의무와 보존의무가 의료인에게 부여되어 있다(전영주 2007).

보건의료기본법 제3조 '보건의료정보'와 '보건의료'의 개념을 규정해 설명하고 있다. 이를 살펴보면 보건의료정보는 국민의 건강을 보호하고 증진하기 위하여 국가·지방자치단체·보건의료기관 또는 보건의료인 등이 행하는 활동과 관련하여 의료 현장에서 작성되는 모든 종류의 보건의료 자료라고 말 할 수 있다.

의료정보의 여러 종류를 살펴보면 의료법 시행규칙 제14조의 의무기록 기재사항에서 보여 주고 있는 진료기록부, 조산기록부,·간호기록부와 제15조의 의무기록 보존연한에서 말 하고 있는 처방전·수술기록·검사 소견기록·방사선사진 및 그 소견서·환자명부·진단서 등의 부본의 의료정보에 해당 할 수 있다. 그 외에도 병원행정 및 경영에서 생성되는 의료정보가 있다.

2.2 블록체인(Block chain)

블록체인(Block chain)은 P2P(Peer-to-Peer) 방식을 기반으로 관리하고자 하는 데이터를 블록(Block)이라는 분산 데이터베이스에 저장하고, 이를 각 블록 간에 체인이 형성되어 있어 임의로 수정할 수 없고, 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기반의 데이터 위조 및 변조 방지 기술이다(Pirtle and Ehrenfeld 2018; Nakamoto 2008). 블록체인 트랜잭션은 네트워크 당사자들이 참여할 수 있는 분산원장에 저장된다. 블록체인 기술은 신뢰할 수 없는 트랜잭션을 생성할 때 신뢰하는 제 3자 없이 분산 시스템을 구현한다. 이때, 해당 트랜잭션의 소유권 및 무결성은 신뢰기관과 제3자가 아닌 암호학 기술로 입증이 된다. 그러므로, 블록체인의 특징은 분권화, 불변성, 그리고 비 신뢰환경에서의 합의과정이라 할 수 있다(박정호 2018).

또한 블록체인 기술은 분산원장기술(DLT, Distributed Ledger Technology)로도 일컬어지고 있으며, 거래정보를 기록한 원장을 어떤 정해진 기관의 중앙집중식 서버들이 아닌 P2P (Peer-to-Peer) 참여 네트워크에 분산 되어져 있는 참가자가 공동으로 기록을 가지며 관리하여 데이터의 무결성을 획득하는 방식을 의미한다. 분산처리와 암호화를 동시에 적용할

수 있어 높은 보안성을 확보할 수 있으며, 거래과정의 신속성과 투명성을 특징으로 가지고 있다. 확보된 보안성의 강화로 의료정보의 위협과 데이터의 왜곡 그리고 현재 중앙집중 서버 방식(Central Server)에서 가장 큰 위협 포인트인 디도스 공격을 원천적으로 방어 할 수 있다. 그리고 중간자인 제3자의 거래에 의존하던 다양한 절차들을 블록체인 플랫폼을 통해 줄이거나 생략할 수 있으며, 수반되는 비용을 획기적으로 감소시킬 수 있다(권혁준 2017). 보안 성이 높고 위·변조가 어렵다는 특성 때문에 데이터 원본의 무결 성 증명이 요구되는 다양한 공공민간 영역에 적용되고 있으며, 새로운 신뢰 사회 구현의 기반 기술로 주목을 받고 있다.

P2P 모델, 클라이언트나 서버 즉 중앙관리자가 필요 없는 참가자들이 클라이언트와 서버의 역할을 동시에 수행하고 각각의 정보를 서로 공유하는 방식으로 이루어진다. 블록체인은 온라인상 참여자들이 분산되어 있고, 참가한 참여자들이 정보를 공유하면서 신뢰성을 얻기 때문에 제 3자의 개입이 필요 없게 되어 불필요한 비용을 절감할 수 있다. 블록체인의 주요 특징으로는 보안성, 신속성, 안전성, 투명성, 효율성 등이 있으며 아래 <표 1>은 대표적인 특징들을 정리한 것이다(박정홍 2018; Innoventures and Wyman 2017).

현재까지 블록체인의 종류는 두 가지로 나눌 수 있다. 먼저 비트코인과 같이 누구나 네트워크에 참여할 수 있는 블록체인인 퍼블릭 블록체인(Public Blockchain)과 허가된 노드(node)만 참여하여 독자적인 네크워크인 프라이빗 블록체인(Private Blockchain)이다. 퍼블릭 블록체인(Public blockchain)은 개방형 블록체인으로 누구나 트랜잭션을 생성할 수 있어 앞에서 설명한 공공거래장부에 해당하며, 통상적으로 블록체인이라 하면 퍼블릭 블록체인을 지칭한다. 퍼블릭 블록체인은 누구나 노드로 참여할 수 있고 참여자의 상호 검증 (Proof of work)을 거쳐 신뢰도 와 무결성이 높다. 거래내역이 모두에게 공개되어 블록체인 네트워크 에 참여한 모든 노드가 이 사실을 검증하고 거래를 승인한다. 하지만 모든 참여자의 거래 기록을 저장하고 이를 공유하기 때문에 기록 및 처리 속도가 느릴수 있다는 문제점이 있다.

프라이빗 블록체인(Private blockchain)은 폐쇄형 블록체인으로 퍼블릭 블록체인의 상대적 개념이

<표 1> 블록체인의 주요 특징

구분	특징
보안성 (Secure)	데이터를 다수가 공동으로 소유, 기록 하여 해킹이 되지않음
신속성 (Instantaneous)	거래의 승인 및 기록은 다수의 노드가 참여 하여 자동기록
탈중개성 (P2P-Based)	어떤 특정한 제3자의 증명 없이 개인과 개인간의 거래가 가능
투명성 (Transparent)	거래기록에 누구나 접근 가능 단 KYC 인증을 준수하지 않음
확장성 (Scalable)	오픈 소스에 의해 쉽게 구축, 연결, 확장 가능

다. 프라이빗 블록체인은 서비스 제공자(기업 또는 기관)의 승인을 받아야만 참여할 수 있으며, 주로 기업에서 활용하여 엔터프라이즈 블록체인(Enterprise blockchain)이라고도 한다. 기업들(또는 기관들)이 함께 참여하여 프라이빗 네트워크를 구성하는 컨소시엄 블록체인(Consortium blockchain)도 프라이빗 블록체인의 한 종류로 프라이빗 블록체인범주에 속한다. 프라이빗 블록체인은 법적 책임을 지는 기관만이 트랜잭션을 생성할 수 있다. 또한 프라이빗 블록체인은 승인과 검증된 기관만이 거래내역 및 데이터를 검증하고 거래를 승인한다. 프라이빗 블록체인은 허가를 받은 노드만 참여하고, 허가 받지 않은 다른 노드의 승인과 검증을 요구할 필요가 없으므로 블록의 생성 주기나 검증이 빠르게 이루어진다. 하지만 프라이빗 블록체인의 사용자는 서비스 제공자에게 전적으로 의존하여야 하기 때문에 퍼블릭 블록체인에 비하여 신뢰성에 한계가 있다. 하지만 프라이빗 블록체인에서 발생하는 시간상의 트랜젝션을 해쉬 함수를 만들어 퍼브릭 블록체인에 저장하는 방식, 앵커링(Anchoring)으로 신뢰성을 극복하며, 이러한 기술적 발달이 프라이빗 블록체인의 여러 문제를 해결하고 있으며 이용하고 있다. 프라이빗 블록체인의 설치는 네트워크 참여 컴퓨터(node)의 개수의 조정으로 설치비용의 감소를 기존 서버 중심의 비용을 줄일 수 있다. 블록체인 플랫폼은 기존의 서비스 단위의 개별 서비스마다 만들어내는 서비스 단위의 단일 프로그램이 아니라 여러 가지 응용 프로그램을 한 플랫폼에서 서비스 할 수 있다.

아래 <표 2>는 주요 블록체인의 종류인 퍼블릭 블록체인과 프라이빗 블록체인의 특징을 비교하여 설명한 것이다.

2.3 기존 의료정보 시스템

<표 2> 블록체인 종류별 비교

구분	퍼블릭 블록체인	프라이빗 블록체인
관리자	모든 거래 참여자	하나의 중앙 기관이 모든 권한 보유
거버넌스	정해진 법칙을 변경하기가 매우 어려움	중앙의 의사 결정에 따라 법칙을 수정 할 수 있음
열람 권한	누구나 열람 가능	인가된 기관만 열람 가능
거래 검증 및 승인	누구나 네트워크에 참여하면 거래 검증 및 승인을 수행	인가된 기관과 감독기관
트랜잭션 생성 주체	누구나 트랜잭션을 생성	법적 책임을 지는 기관만 참여 가능
합의 알고리즘	PoW(Proof of Work), PoS(Proof of Stake) 알고리즘	BFT(Byzantine fault tolerance) 알고리즘
속도(TPS)	7~20 TPS(Transaction per Second)	1000 TPS(Transaction per Second) 이상
식별성	익명성	식별 가능
데이터 접근	누구나 접근 가능	인가된 사용자만 접근 가능
사용 예시	비트코인, 이더리움 등	IBM 패브릭, R3 코다 등

개인의료정보를 대부분 생산·보관·관리하고 있는 의료기관의 정보화는 1977년 의료보험제도 시작 시 진료비 청구수단으로 활용된 이후 점차 병원정보시스템(HIS), 전자의무기록(EMR), 처방전달시스템(OCS, Order Communication System), 의료영상저장전송시스템(PACS, Picture Archiving and Communication System) 등 각종 정보시스템이 도입됨에 따라 의료정보 시스템에 의존하는 비중이 높아지게 되었다(김상만·이연주 2010).

기존의 대표적인 의료정보 시스템으로는 병원정보시스템(HIS)과 전자의무기록(EMR)을 들 수 있다. 첫째, 병원정보시스템(HIS)은 병원의 전반적인 업무를 자동화한 시스템으로 진료행정시스템과 진료정보제공시스템으로 나누어 살펴 볼 수 있다. 옛날 청구 중심에서 현재 진료를 지원하는 시스템으로 변해가는 가운데 처방전달시스템(OCS)은 요구사항 및 여러 사항을 포함한 것으로 의학정보 및 환자들의 진찰자료를 보관한 데이터를 의사가 환자를 진단한 후 처방전을 시큐어한 정보망을 통해 각 담당 진료부서 및 진료과로 정보를 송부해주는 시스템이다. 둘째, 전자의무기록(EMR, Electronic Medical Record)은 종이차트에 기록했던 기존의 인적 사항, 병력, 건강상태, 진찰, 입원 및 퇴원 기록 등 환자의 정보를 데이터 화하여 저장, 입력, 관리의 형태를 뜻한다. EMR은 종이에 기록하는 방식이 아니라 디스크나 다른 저장 매체 에 저장하여 정보 보관하는 방법에서 발전하여, 현재 의료기기 안에 있는 컴퓨터가 주된 시스템들과 연계되어 원격진료에 이용된다. EMR로 신속한 업무처리와 인력 및 비용 절감의 효과가 있고, 과거의 기록을 찾는 시간까지 절감할 수 있어 병원에서 대기하는 환자들의 시간 단축 등 환자들이나 병원 측에서 제공되는 서비스의 향상 효과가 있다.

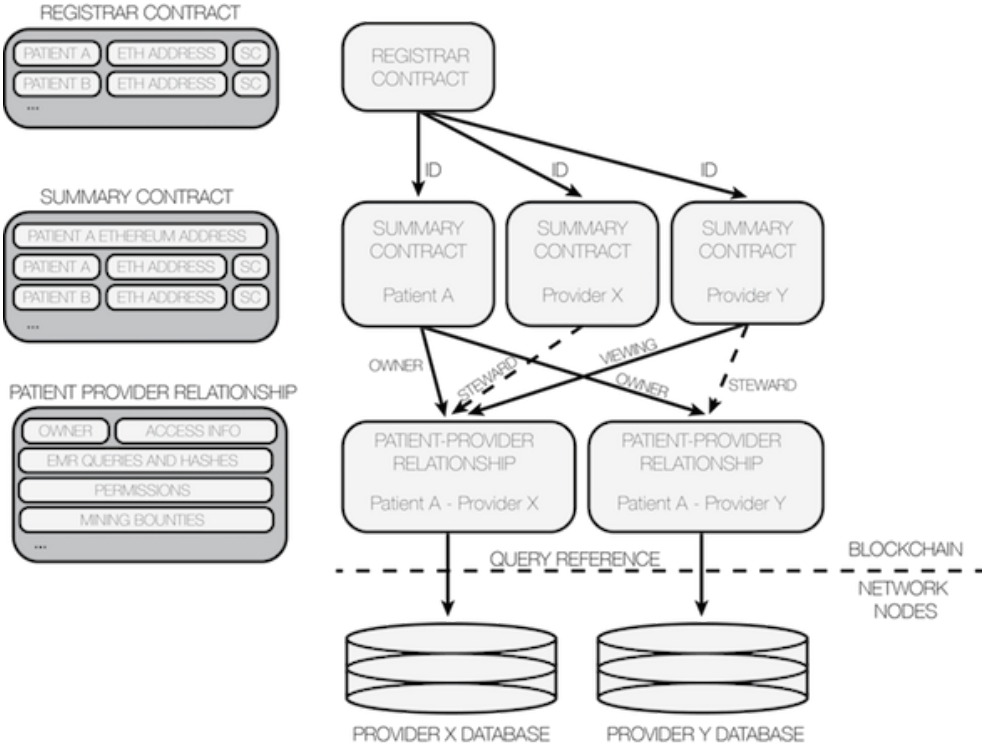
HIS나 EMR의 데이터는 의료기관들이 보유하는 데이터이고, 의료비 청구 데이터보다 실제 진료를 받은 데이터 항목수가 더 많아 정보는 다량이지만 병원마다 데이터 항목이나 데이터의 형식들이 상이할 수 있다. 이에 따라 다른 병원의 데이터들을 수집해 연구할 때에는 데이터 형식의 표준화가 되어있지 않아 많은 어려움을 겪는다. 이들 데이터는 의료기관 단위의 데이터이므로 해당 데이터의 이용이 적절한 역학 연구의 종류와 범위에 제한이 있다.

2.4 블록체인을 활용한 국외의 의료정보시스템

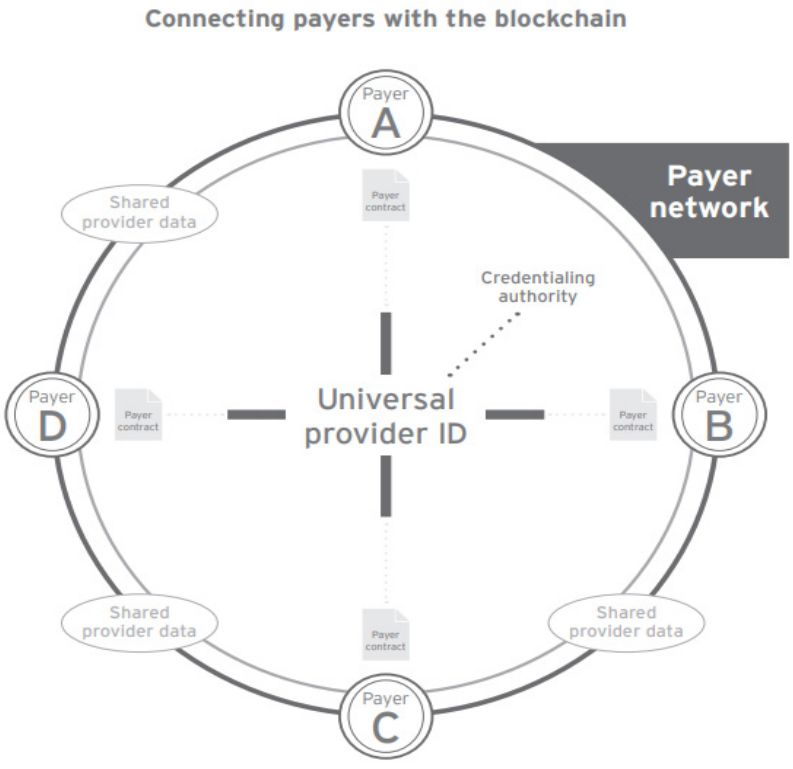
블록체인을 활용한 의료정보시스템으로는 MIT Media Lab의 MedRec과 Ernst & Young의 EY Contract를 대표적인 사례로 들 수 있다.

첫째, MedRec은 MIT Media Lab에서 개발한 블록체인 기술 도입 프로토타입이다. 등록기관의 계약서를 통해 Google 등의 신뢰할 수 있는 기관의 인증을 통해 로그인(아이디, 패스워드)을 하고 의료정보의 접근권한을 환자와 의사 모두 자유롭게 열람이 가능하도록 하였다. 의료연구원은 익명으로 처리된 메타데이터에 대한 접근 대가로 “인증 수수료” 형태의 블록체인 인증 로그를 안전하게 유지하는데 필요한 수수료를 지불하게 된다. MedRec의 목적은 의료연구원들에게 많은 의료 데이터를 제공하면서 환자가 메타데이터의 공개여부를 선택할 수 있게 하는데 있다(Griggs et al. 2018). 다음 <그림 1>은 MedRec의 프로토타입을 나타낸 것이다.

둘째, EY Contract는 의료 제공자들의 편의를 위한



<그림 1> MedRec의 프로토타입(MedRec, 2018)



<그림 2> EY Contract의 플랫폼(Dan Gietl et al., 2016)

플랫폼이다. 의료 제공자들은 등록된 의료면허를 사용하여 통합 제공자 ID에 로그인 되어 지게 된다. 통합 제공자 ID에서의 허가된 의료 제공자들의 증명이 분류된 사용자간의 ERM데이터의 공유가 이루어진다. 다른 의료시스템과는 다르게 제공자가 정해진 환자만 데이터의 취급과 접근 이 가능하게 되어 있어, 미지정된 환자의 의료정보에 접근을 차단할 수 있다. EY Contract는 의료 제공자들 간 하나의 통합 ID 사용으로 의료정보에 대한 접근성이 편리하다(Dan Gietl et al. 2016). 다음 <그림 2>는 EY Contract의 플랫폼을 도식화 한 것이다.

3. 개인 의료정보의 위협

미국의 ITRC(Identity Theft Resource Center)의 보고서에서는 개인 정보 유출사례를 매년 발표해오고 있는데, 2017년 전체 데이터 유출 사고의 비중에서 의료 분야가 23%로 나타나며 그 심각성을 드러내고 있다(ITRC 2017; 2018). 이는 의료기관의 정보시스템 사용률이 높아지고, 대규모 디지털화가 되고 있으며 U-Health, Smart-Health 등과 같은 정보통신 기술의 발전에 따라 개인의료정보에 대한 접근성이 용이해지면서 개인의료정보의 침해 노출 위험은 점점 더 증가하고 있는 것이다.

실제로 미국에서는 2015년 Premera Blue Cross 사의 웹 사이트 해킹을 통해서 가입자 1,100여만명의 개인정보가 유출된 사건이 있었으며, 생명 및 건강 보험사 Anthem 에서 8천만의 고객과 직원의 개인정보가 유출된 적이 있다. 보험정보 유출뿐만 아니라, 의료기기 보안 위협에 대한 사례도 상당히 증가하고 있다. 전기로 강제로 심장박동을 뛰게 만드는 전자심장 박동기의 동작을 해킹으로 멈추게 만들 수 있다는 경고가 미국 식품의약국(FDA)에 의해 발표 되었다.

근래에는 의료정보 불법 유출 및 악용 그리고 램섬웨어의 여러 방향의 범죄가 증가하고 있는 추세이다. 2016년 할리우드에 위치한 장로병원(Hollywood Presbyterian Medical Center)이 에 1만달라에 해당되는 가상화폐를 지불한 적이 있고, 그 외 에도 메드스타(Medstar), 독일의 루카스 병원(Lukas Hospital) 등이 랜섬웨어의 피해를 입었다. 국내 의료기관 및 관련 기관에서도 환자정보에 대한 불법적인 수집, 환자의 동의 없이 제 3자에게 제공, 의료기관의 관리 소홀로 인한 환자정보 유출, 내부 관리자에 의한 고의적인 환자정보 유출 사건이 지속적으로 발생되고 있다.

이처럼 개인 의료정보에 대한 해킹과 자료유출은 꾸준히 늘어나는 형태를 가지고 있다 그 위협의 근원 외부 해커들로만이 아닌 내부자에 의한 정보유출 그리고 관계자 공모 에의한 정보의 불법적인 반출과 획득, 행정기관 및 감독기관 등에 의한 정보유출 사례도 있는 만큼 환자의 프라이버시를 지키면서 안전하게 의료레코드를 저장 관리가 필요한 시점이다.

4. 개인 의료정보 보호를 위한 블록체인 적용 방안

4.1 블록체인 적용의 타당성

블록체인 기반인 분산원장 기술 (Distributed Ledger Technology)의 일반적인 장점은 보안성의 강

화, 데이터의 무결성 확보, 처리과정의 신뢰성 증진과 감시가능성의 확대, 비용 절감 등 이다. 그러나 현재까지 소개되고 있는 블록체인 기술의 활용 사례들의 일반적인 장점들을 모두 수용하기 보다는 의료정보 보호 분야에 맞춰 블록체인을 적용해야 할 필요성이 있다.

개인 의료정보에 블록체인을 적용할 때 큰 장점은 무결성, 데이터 접근권한의 특징이다. 파일의 무결성은 해시를 통해 보호받으며, 해시는 레코드 식별자로 숫자, 문자 형태로 사용된다. 암호화된 알고리즘을 통해 파일의 내용을 일정한 숫자, 문자로 나타내게 되기 때문이다. 블록체인은 실제 데이터들이 저장되는 것이 아니라 해시 값을 통해 유효성을 검증하는 최소한의 정보를 기록하게 된다. 이 기록에 대한 변경이 있을 경우 새로운 해시가 생성되어 사용자는 누군가 나의 자료에 접근했는지 알 수 있고, 또한 수정된 자료는 블록체인에 저장되지 않는다. 데이터에 접근권한을 부여하여 인가된 사용자만 레코드에 접근할 수 있고, 블록체인에 사용자 권한과 관련된 추가 정보를 포함 시킬 수 있다(Angraal et al. 2017).

블록체인은 과반수 이상을 점유해야 해킹이 가능하다. 하지만 현재 의료기관에서 사용하고 있는 ERM은 해커들이 데이터가 저장된 서버를 공격하면 쉽게 정보를 얻을 수 있으며, 이때 저장되어있던 데이터의 위·변조가 가능하다. 블록체인 기술을 적용한다면 분산되어 있는 데이터베이스가 타격을 입는 경우에도 분산된 데이터 구조로 몇 개의 시스템 장애가 발생하여도 전제의 네트워크 타격이 미비하며 이 또한 쉽게 복구가 가능하다. 이에 따라 블록체인을 적용할 때에는 기존 방식보다 네트워크 관리, 해킹에 대한 위험 등 많은 부분이 감소된다.

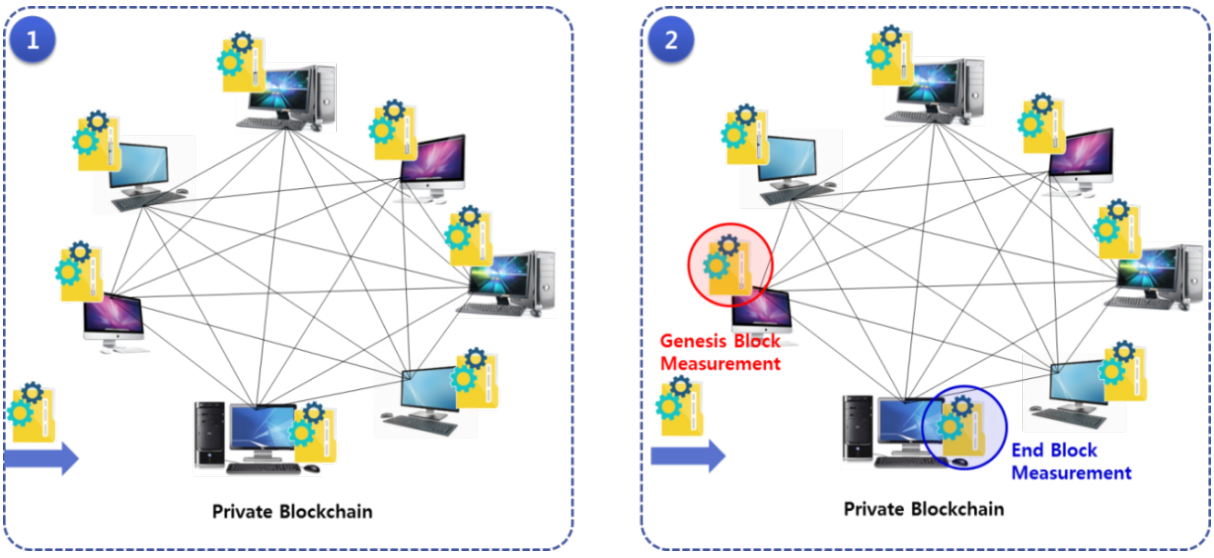
4.2 블록체인 적용에 따른 편의성

기존 국내 개인의료시스템은 서버, 클라이언트 구조로 되어있으며, 해킹이 발생할 경우 하위 기관까지 엄청난 피해를 입게 된다. 진료를 받는 환자나 진료를 하는 의료인들간의 자료 공유가 쉽지 않아 의료데이터를 얻는 과정은 상당히 어렵다. 하지만 블록체인을 개인의료시스템에 적용하면 인가된 사용자들만 블록체인에 접근권한이 부여됨으로 의료 연구진, 의사, 환자들이 언제든지 안전하게 열람이 가능하다.

기존 의료시스템은 유지 및 보수에 엄청난 시간과 경제적 요인이 수반되지만 블록체인을 의료시스템에 적용하게 되면 기존 시스템에 들어간 경제적 요인과 시간이 절감될 것이고, 해킹에 의한 개인정보 유출 우려도 저감될 것이다.

또한 의사는 환자들이 상급병원에서 진단을 받아온 의료정보 데이터가 그 환자의 의료 데이터가 맞는지 진위여부를 블록체인을 통해 확인이 가능할 것이고, 의원 급에 있는 의사가 A환자를 상급병원, 종합병원에 진료를 의뢰할 때 필요한 진단서, 초진차트 등 많은 의료 데이터에 블록체인을 적용하게 되면 A환자에 대한 의료 데이터, 즉 의료정보를 입력해 블록에 저장을 하면 기존에 사용했던 초진차트, 진료의뢰서 등이 필요 없게 된다. 시간과 비용측면에서 상당한 수준으로 절감될 것이고, 환자 입장에서도 개인정보유출에 대한 불안감을 줄어들게 되어 개인의료시스템에 대한 신뢰도가 상승하게 된다(홍병선 등 2016).

더불어 블록체인을 통해 표준화된 의료보안 플랫폼을 구축해 의료정보를 의료기관(병원) 내부 또는 외부



<그림 3> 프라이빗 블록 스킴

로 안전하게 전송관리 할 수 있다. 이를 통해 대형 의료기관과 중소형 의료기관에 적합한 의료보안 관리체계를 만들어 국내 의료정보시스템의 표준화를 이룰 수 있다.

환자 중심의 의료서비스가 확대되어 1차~3차 병원간의 의료서비스의 질과 보안의 격차를 줄일 수 있고 의료정보가 유출될 경우, 의료정보 자체가 상대적으로 가치가 높은 만큼 이로 인한 사회적 비용도 다른 산업에 비해 발생되는 부분을 크게 줄일 수 있다. 블록체인을 도입함으로써 보안환경과 의료보안 수준이 향상되어 보다 안전한 의료정보를 관리할 수 있다.

다음 <그림 3>는 프라이빗 블록 스킴에 관해 도식화한 것이다.

본 연구에서 기술한 프라이빗 블록체인은 다른 용어로 허가된 컴퓨터 즉 노드(node)만 블록체인에 참여하는 블록체인으로 블록체인의 산업적용으로 현재 사용되고 있는 상태이다. 의료시스템의 블록체인 또한 허가된 또는 관여하는 단체 또는 기관이 노드(node)로 참여하게 되어 일차적인 보안성과 신뢰성을 주게 되며, 설치 또한 용이하다. 과거 서버중심의 의료정보 데이터가 아닌 분산원장기술 (Distributed Ledger Technology)의 적용으로 서버의 침해 정보의 누출을 막을 수 있는 장점과 블록의 사이즈 TPS(Tractions per second) 를 <그림 3>에서의 마스터 노드가 정책을 수립, 권한 정책도 수립 할 수 있다. 블록에 저장할 수 있는 정보 또한 해시 함수를 비롯한 여러 데이터를 손쉽게 넣을 수 있다.

5. 결론 및 시사점

개인의료정보는 개인정보보호가 가장 중요시하게 보호를 받아야 할 곳이라고 생각한다. 현재 국내에서 사용되고 있는 의료시스템은 병·의원들이 유지, 보수, 관리하기가 어렵고 그에 따른 인원과 비용이 많이 투입된다. 블록체인을 도입하게 되면 기존 발생했던 비용

보다 훨씬 더 절감이 될 것이라 판단된다.

미국에서는 이미 의료시장에 블록체인을 도입해 안전한 의료정보시스템을 유지하고 있다. 전술했던 바와 같이 미국의 의료정보시스템인 서터 피지션 이용 환자 의료정보 유출사건이 또다시 발생하지 않도록 하기 위해 블록체인을 통한 의료정보시스템을 개발, 사용 중에 있다. MedRec의 경우 제 3자를 통해 신뢰기반을 만들어 환자와 의사가 데이터를 공유하고, 다른 의료연구원들이 많은 데이터를 확보 및 제공받을 수 있어 관련 연구를 진행하는데 간편하게 의료데이터를 이용할 수 있다.

우리나라의 의료정보 해킹사례는 급진적으로 증가하고 있다. 이는 많은 의료시스템이 의료 현장에서 활용되고 있지만, 의료분야에 근무하는 연구진들이 의료기관에서 제공해준 데이터를 분석하여 연구하고자 할 때 의료시스템마다 다른 데이터의 정보를 합의되어 도출된 일원화된 형식으로 정리할 필요가 있다.

참고문헌

[국내 문헌]

1. 권혁준 2017. “Blockchain (분산원장) 기술의 현황 및 주요 이슈,” *한국 IT 서비스학회 학술대회 논문집*, pp. 25-32.
2. 김상만, 이연주 2010. “의료서비스산업에서의 고객지식 획득과 활용방안: 기대 불일치 이론을 중심으로,” *지식경영연구(11:3)*. pp. 59-76.
3. 문성재, 이경환 2005. “환자의 진료정보와 통제권에 관한 소고,” *민사법학* (29), pp. 363-390.
4. 박민정, 채상미 2017. “빅데이터 환경 형성에 따른 데이터 감시 위협과 온라인 프라이버시 보호 활동의 관계에 대한 연구,” *지식경영연구(18:3)*. pp. 63-80.
5. 박정호 2018. “블록체인 산업 현황 및 동향,” NIPA 이슈리포트 2018-제17호.
6. 박정홍 2018. “의료산업 블록체인 도입을 위한 연구,” *한국콘텐츠학회논문지*(18:6). pp. 155-168.
7. 백윤철 2005. “헌법상 환자의 의료정보에 대한 권리에 관한 연구-미국의 HIPAA 프라이버시규칙을 중심으로,” *헌법학연구 (11)*, pp. 337-373.
8. 이백휴 2010. “환자의 의무기록 관련 의료인의 법적 지위,” *의료법학(10:2)*, pp. 309-335.
9. 홍병선, 고준, 정기주 2016. “고객센터 지식관리시스템 재구축 성공과 활용에 영향을 미치는 요인에 관한 탐색적 연구: K 보험사 사례를 중심으로,” *지식경영연구(17:3).* pp. 93-115.

[국외 문헌]

1. Angraal, S., Krumholz, H. M., and Schulz, W. L. 2017. "Blockchain technology: applications in health care," Circulation: *Cardiovascular Quality and Outcomes* (10:9), e003800.
2. Griggs et al. 2018. "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," *Journal of medical systems* (42:7), 130.
3. Innoventures, S., and Wyman, O. 2017. "The fintech 2.0 paper: rebooting financial services"
4. Nakamoto, S. 2008. "Bitcoin: A peer-to-peer electronic cash system"
5. Pirtle, C., and Ehrenfeld, J. 2018. "Blockchain for Healthcare: The Next Generation of Medical Records?," *Journal of Medical Systems* (42:172).

[URL]

1. MedRec, 2018, https://medrec.media.mit.edu/technical/
2. Dan Gietl et al., "Blockchain in health," Ernst & Young, 2016. https://www.hyperledger.org/wp-content/uploads/2016/10/ey-blockchain-in-health.pdf
3. Identity Theft Resource Center, "2017 annual data breach year-end review" 2017, https://www.idtheftcenter.org/2017-data-breaches/
4. Identity Theft Resource Center, "March 2018 data breach stats" 2018, https://www.idtheftcenter.org/data-breaches/

저 자 소 개

권 혁 준 (HyukJun Kwon)

현재 순천향대학교 IT금융경영학과 조교수로 재직하고 있으며, Virginia Commonwealth University 경영학학사, 연세대학교 경영학과 석사, 연세대학교 정보시스템 박사를 취득하였다. Computers in Human Behavior, Multimedia Tools and Applications 등의 국제학술지 및, 융합보안논문지, 한국전자거래학회지 등의 국내학술지에 다수의 논문을 게재하였다. 주요 관심분야는 Blockchain, Crypto economy, Fintech, 디지털 화폐, VR 가상현실, E-Business 등이다.

김 협 (Hyeob Kim)

현재 대진대학교 경영학과 Adjunct Instructor로 재직 중이다. 연세대학교 정보대학원에서 정보시스템학 박사를 취득하였으며, 연세대학교 정보대학원에서 ITRC(Information Technology Research Center) 연구원으로 근무하였다. Computers in Human Behavior, Multimedia Tools and Applications 등의 국제학술지 및 IT서비스학회지, 융합보안논문지, 한국융합학회논문지 등의 국내학술지에 다수의 논문을 게재하였다. 주요 관심분야는 Blockchain, Information Security, Medical system, Big data & Social Network Analysis 등이다.

최재원 (Jaewon Choi)

2018년 현재 순천향대학교 경영학과 조교수로 재직하고 있으며 가톨릭대학교에서 경영학 박사를 취득하였으며, 연세대학교 정보대학원에서 연구교수 및 KAIST경영대학에서 연수연구원으로 근무하였다. International Journal of Electronic Commerce, Technological Forecasting and Social Change, Journal of Global Information Systems, Cyberpsychology Behavior and Social Networking 등의 국제학술지 및 지식경영연구, 전자거래학회지, IT서비스학회지 등의 국내학술지에 다수의 논문을 게재하였다. 주요 관심분야는 Web Personalization, Block Chain, Digital Marketing, Big data & Social Network Analysis 등이다.