공학석사 학위논문

의료 데이터 공유를 위한 블록체인 기반의 무결성 보장 및 프라이버시 보호와 사용사례 구현

2019년 2월

부 경 대 학 교 대 학 원

정보보호학 협동과정

김 현 우

공학석사 학위논문

의료 데이터 공유를 위한 블록체인 기반의 무결성 보장 및 프라이버시 보호와 사용사례 구현

지도교수 이 경 현

이 논문을 공학석사 학위논문으로 제출함.

2019년 2월

부 경 대 학 교 대 학 원

정보보호학협동과정

김 현 우

김현우의 공학석사 학위논문을 인준함.

2019년 2월

주심　　이학박사 신 상 욱　　(인)

위원　　공학박사 김 창 수　　(인)

위원　　이학박사 이 경 현　　(인)

차 례

그림 차례

표 차례

Blockchain based Integrity and Privacy Protection

for Healthcare Data Sharing and Implementation of a Use Case

Hyunwoo Kim

Interdisciplinary Program of Information Security, The Graduate School,
Pukyong National University

Abstract

In general, the center of the medical institution operates the medical information system. In most current systems, the medical data are stored in the provider database, so that the patients do not have full access rights to manage the data. Moreover, the problem is augmented if the medical data is fragmented into several medical institutions. Whenever a dispute occurs between the medical institution and patient, the institution cannot use patient's medical data as evidence to judge the appropriateness of medical treatment because the patient has no way to prove it.

As a solution, we can use the blockchain to determine the integrity of medical data. However, the nature of blockchain gives the privacy problems for the patients due to blockchain stores the data publicly in the network. In this sense, every party in the network allows viewing the transaction as well as the patient record. Public data is contrary to the nature of medical data which is sensitive to each party. To address the problem, we use the stealth address protocol to disguise the identity of the parties. In this thesis, we implement the smart contract as an escrow to enable fairness sales of medical data. A payee enables to sell medical data to the payer safely with a guarantee that the payer will pay compensation and the payee will send the corresponding medical data. To do so, the payer needs to deposit the coins (cryptocurrency) to the smart

contract. If all procedures are met, the smart contract shows the IPFS address which is the links to access the data. By leveraging this model, we solve the privacy issue of the patient's identity. Based on our evaluation, the smart contract produces a reasonable gas cost for every transaction. Therefore, this smart contract is usable in a practical environment.

I. 서 론

1. 연구배경

고령화 사회가 도래하고 현대인의 건강에 대한 높은 관심, 만성질환 환자가 증가함에 따라 최근 전 세계적으로 보건의료 분야는 치료 중심의 의료패러다임에서 예방·관리 중심의 의료패러다임으로 변화하고 있다. 이러한 패러다임의 변화는 최근 기하급수적으로 증가하고 있는 축적된 의료데이터와 4차 산업혁명으로 대두되는 인공지능(AI)이 의료분야에 접목되면서 가속화되고 있다. 즉, 그 기반에는 방대한 의료데이터와 AI의 의료분야 접목으로, 그 예로는 전자건강기록(EHR, Electroinc Health Record)과 개인의 웨어러블 디바이스에서 생성된 데이터를 수집·분석·저장·활용함으로써 맞춤의학과 같은 개인에게 특화된 의료 서비스 제공 하거나 AI 기술을 이용해 질병의 새로운 예방법이나 치료법 개발하는 것이다. 실제로 가천대학교 길병원의 경우 국내 최초로 2016년 IBM 왓슨을 집단진료 체계에 도입하여 환자의 데이터가 입력될시 수 많은 임상사례와 300여개 가량의 의학저널 등 방대한 빅데이터를 학습하여 최적의 치료방법을 제시함으로써 의료인들의 의사결정을 보조하는 역할을 수행하고 있다. 하지만, 아무리 훌륭한 알고리즘을 기반으로 방대한 의료데이터를 분석하여 결과물을 산출했다 하더라도 잘못된 데이터로 학습하게 되면 성능을 바르게 발휘할 수 없다. 컨설팅 기관인 Accenture이 최근 발표한 자료[1]에 의하면 의료기관 최고경영진 89%는 AI를 도입 시 의

료데이터의 무결성이 매우 중요한 이슈가 될 것으로 예상하고 있는 것으로 나타났다. 의료데이터에서 무결성은 신뢰성 있는 무결한 데이터 인가 의 개념으로 결국 의사에게서 생성된 데이터가 맞는지에 대한 신뢰성과 의료데이터가 의사에게 생성된 이후 변경되지 않았는지 무결성 여부이다.

2. 연구 내용 및 구성

환자가 단일 의료기관 내에서만 진료를 받고 헬스케어 서비스(맞춤 의학 서비스, AI에 기반한 서비스 등)을 받을시 의료 데이터의 무결성은 단일기관 내에서 검증할 수 있지만 보통 환자의 의료 데이터는 여러 의료기관내에 산재되어 있으며 단일 의료기관에서 생성된 소량의 데이터를 기반으로 헬스케어 서비스를 받을 시 분석결과의 정확성이 떨어질 우려가 있다. 결국 새로운 보건의료 패러다임에서 환자에게 의료서비스를 제공하기 위해서는 제공받은 의료 데이터에 대한 무결성 검증과 산재 되어있는 의료데이터를 어떻게 통합 할 것 인가 이다. 이 문제를 해결하기 위해서 본 논문에서는 환자가 본인의 의료 데이터를 직접 의료기관에게 공유하며 블록체인을 통해 의료 데이터의 무결성을 검증할 수 있게 한다. 이로써 헬스케어 서비스 제공자는 양질의 의료 데이터를 갖고 진료를 하고 환자는 양질의 의료 데이터를 갖고 진료를 받을 수 있다.

본 논문의 연구 범위는 의료 데이터 공유를 위한 무결성 보장 시스템은 제안하지만 공유하는 기법이나 방법에 대해서는 제안하지 않는다.

본 논문의 구성은 2장에서는 관련 연구에 대해 살펴보고 3장에서는 제안하는 의료 데이터 공유를 위한 무결성을 보장하는 블록체인 시스템을 살펴 본다. 4장에서는 무결성이 보장되는 시스템(3장)을 활용하는 스마트 컨트랙트 기반의 의료 데이터 판매 시스템을 구현한다. 끝으로 5장에서는 결론을 맺는다.

II. 관련 연구

본 장에서는 무결성을 보장하는 기법 및 연구와 블록체인 기반의 의료 데이터 공유 연구에 대해서 간략히 살펴보고 문제점을 도출한다.

1. 기존 모델과의 비교

저장된 데이터에 대한 무결성 보장함과 동시에 데이터의 투명성을 보장하는 것은 의료정보 시스템의 중요한 이슈이다. 기존의 의료정보 시스템은 의료기관 중심으로 운영되어지고 있다. 환자의 의료데이터를 한 기관이 독점적으로 관리 할 경우 환자는 자신의 의료 데이터가 임의로 변경되었는지의 여부를 파악하기 어렵다. 또한 의료기관간 의료정보를 공유할 때 공유 받은 의료정보가 변경 없이 관리되었음을 확인하는 것은 어렵다. 그리하여 미래의 의료정보 공유 시스템은 신뢰할 수 있는 단일 기관이 의료 데이터를 관리하는 것이 아닌 시스템 내 참가하는 개체들이 의료데이터의 무결성과 투명성을 제공하는 시스템을 구축해야한다. 이를 위해 본 논문에서는 블록체인의 거래불변성과 투명성의 성질을 이용하여 단일 기관이 의료 데이터를 생성할 때 발생하는 문제를 해결하고자 한다.

의료정보 시스템 경우별 한계점 : 데이터 베이스를 사용한 의료 데이터 관리시 환자는 자신의 의료 데이터에 대한 접근 권한이 없어 각 의료기관의 진료기록 조작 문제에 대해서는 의료인들의 양심에 맡길 뿐 데이터의 무결성이 훼손되어도 이를 확인할 방법이 없어 의료사고

발생 시 의료 행위가 종료된 시점 이후에 수정되거나 추가 기재하여 의료행위의 적절성을 판단하는 자료로 사용될 경우 환자나 보호자 측이 이를 확인할 방법이 없다. 즉, 관리자는 데이터 생성(Create), 읽기(Read), 갱신(Update), 삭제(Delete)의 기능을 수행하는 반면 블록체인은 추가만 가능한 Append-Only의 성질을 갖기 때문에 사용자는 읽기와 쓰기의 기능만 수행할 수 있음. 접근 권한을 부여 했다고 하여도 여러 의료 기관에 산재되어 있는 본인의 의료데이터에 대한 무결성을 지속적으로 확인하기 힘들다[2].

또한 현재 의료기관간 데이터 공유는 보통 환자에 의해 이뤄지고 있으며 진료 기록은 환자의 요청에 따라 진료 기록 요청 시 비용을 지불하고 CD 형태로 제공 받으나 훼손이나 분실로 인한 보관의 어려움과 본인에게 유리하게 데이터 조작이나 편집의 문제가 발생할 수 있어 원본 증명이 어려워 데이터의 신뢰성을 인정받지 못해 결국 중복검사를 하게 되는 문제가 있다. 건강보험심사평가원의 보도 자료에 따르면 2010년부터 2012년 까지 MRI · CT · PET 중복 검사로 인한 급여 청구액이 23.3% 증가한 것으로 나타났다[3].

보건복지부의 마이차트[4]는 환자정보, 진료기록, 검사기록과 같은 의료기록을 의료기관간 공유할 수 있는 프로그램을 지원하지만 2015년 국가통계포털 KOSIS의 통계자료에 따르면[5] 전국에 총 63,471개의 병원이 있고 이중 마이차트에 참여한 병원은 1307개에 불구하며 마이차트는 의료기관간 의료 데이터 공유에 국한되어 있으며 연구기관에 제공하는 것은 허용하지 않고 있어 환자의 의료데이터를 활용하는데 어려움이 있다.

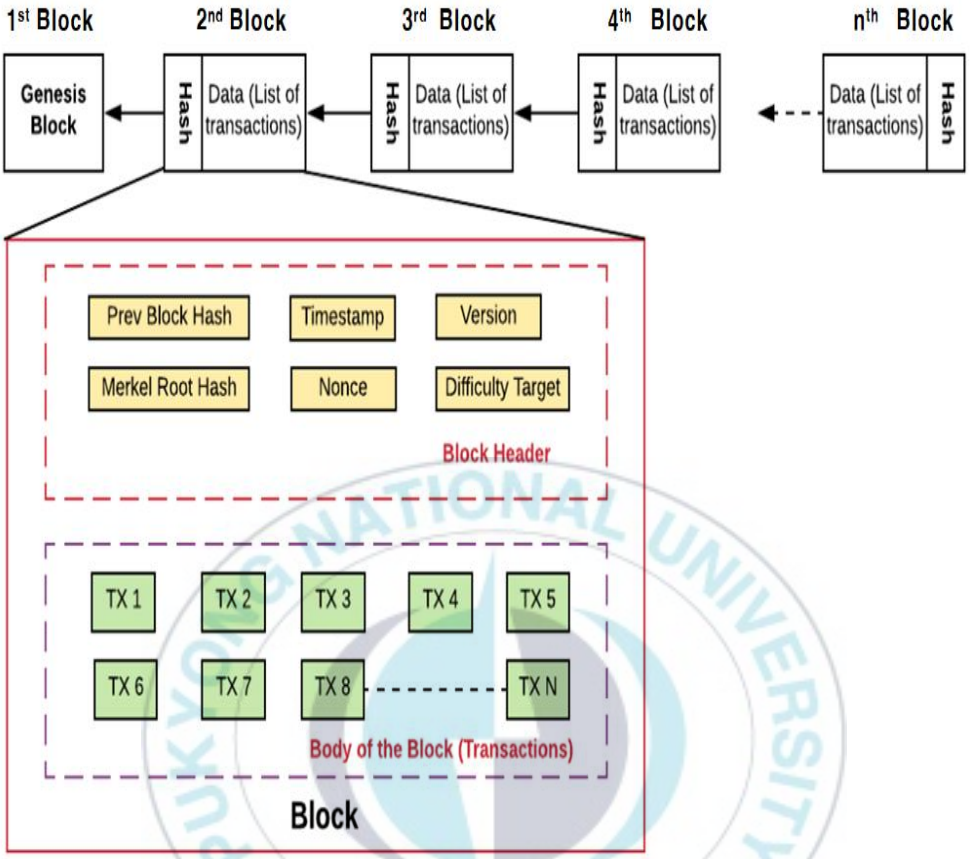
2. 프리미티브

가. 블록체인

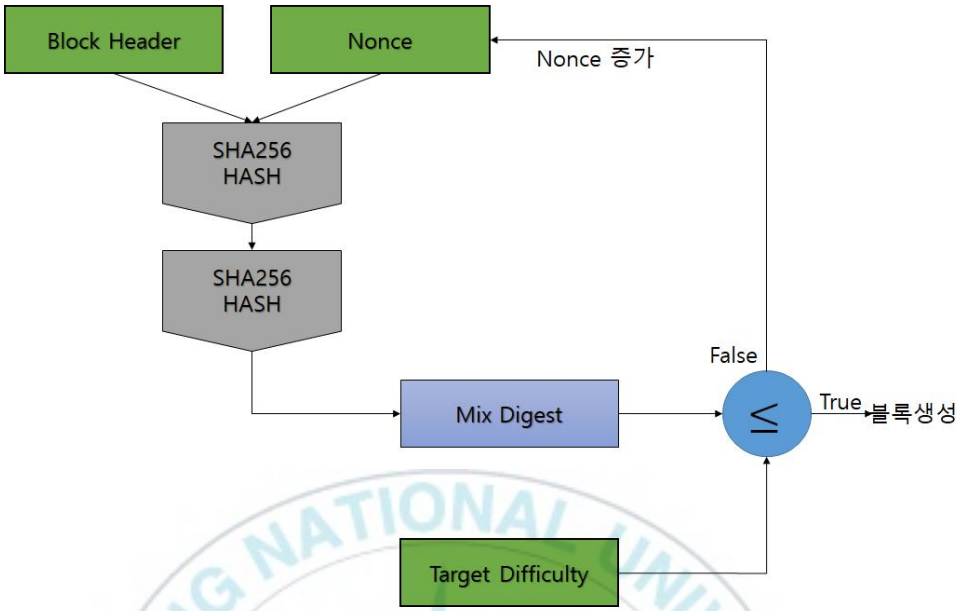
최근 가상화폐에 대한 관심과 더불어 학계와 다양한 산업에서 블록체인을 활용하기 위한 연구와 투자가 늘어나며 그에 대한 결과로 다양한 활용사례가 등장하고 있다. 특히, 블록체인 기술은 금융, 헬스케어, IoT, 전자투표, 전자정부 등의 분야에서 적용되어 활용되고 있다.

블록체인의 대표적인 구현사례로는 Satoshi Nakamoto의 비트코인[11]으로 주된 작업은 참여자 간 서로 신뢰할 수 없는 P2P(Peer to Peer) 네트워크에서 제 3자의 기관없이 P2P 노드간 암호화폐를 주고 받기위해 모든 참여자들이 공유하는 단일화된 데이터베이스를 만드는 것으로 이 때 합의과정이라고 하는 분산 및 결함을 허용하는 프로세스를 통해 악의적인 개체들로 부터의 결함을 허용할 수 있도록 설계하였다.

그림 1과 같이 블록체인 환경에서 발생된 거래는 마이너에 의해 블록으로 생성되며 마이너는 거래들을 수집하고 체크리스트를 통해 정당한 거래임을 검증한다. 검증된 거래들은 메모리 풀(Memory Pool) 또는 트랜잭션 풀 (Transaction Pool)에 저장되며 트랜잭션 풀에 있는 거래 내역을 하나의 블록으로 생성하기 위해 비트코인의 경우 작업증명 과정을 수행하게 된다. 유효한 블록을 생성하기 위해



[그림 1] 비트코인 블록체인 구조



[그림 2] 작업증명 알고리즘 흐름도

그림2의 흐름도의 과정을 거쳐 블록을 생성한다. 이를 위해 난이도 목표값(Target Difficulty) 안에 있는 nonce값을 찾는 과정을 반복하며 가장먼저 유효한 nonce값을 찾는 채굴자가 블록을 생성 할 권한을 갖게 된다. 난이도의 최대값은 $2^{256}-1$이며, 난이도 목표값은 네트워크의 참여자 수의변화나 네트워크 전체의 해시파워에 따라 10분의 블록 생성 주기를 갖고 2주간 2016번째 블록을 생성하도록 아래의 계산식을 통해 재조정 된다.

$$Difficulty = Old\,Difficulty * (Actual\,Time\,of\,2016\,Blocks / 20160\,minutes)$$

높은 컴퓨팅 파워를 가질수록 빠른 속도로 해시 연산을 수행함으로 블록을 생성할 확률이 높아진다. 위의 과정을 통해 생성된 블록은 다른 참여자들에게 전파되며 전파 받은 참여자는 블록의 유효성을 검증

하고 유효할시 다른 참여자들에게 전파하게 된다. 이와 같은 합의과정을 통해 신뢰하지 않는 블록체인 참여자간 신뢰성 있게 블록을 생성하고 검증할 수 있게 된다.

작업 알고리즘을 사용하는 블록체인의 거래내역을 변경하기 위해서는 해당 거래내역이 포함된 블록부터 다음 생성될 블록까지 모두 변경해야하기 때문에 사실상 변경 불가능하다는 거래 불변성의 장점이 있다. 이는 블록체인의 가장 유명한 취약점인 51%공격을 방지 할 수 있는 구조로 악의적인 공격자가 51%의 공격을 하기 위해서는 51% 이상의 해시 파워를 확보해야하기 때문에 이는 현실적으로 공격을 통해 얻는 이득보다 투자비용이 큰 구조이다.

비트코인은 공개형 블록체인 환경으로, 블록체인의 거래는 누구나 참여가능하기 때문에 참여자들은 비밀키 공개키를 통해 주소값을 생성하기 때문에 참여자의 가명성을 제공한다. 하지만, 체인널리시스 리액터[15]의 경우 비트코인 지갑 주소를 이용하여 트랜잭션을 추적하여 다크넷에서 악용되는 지갑 주소를 검색해 수사에 활용할 수 있게 하고 모든 트랜잭션들에 대해서 연관성을 그래프를 통해 분석하여 시각화된 데이터로 트랜잭션 경로를 파악한다 이러한 기술을 악용할 경우 공격자는 참여자의 가명정보를 실제 신원과 연관 지을 수 있다. 또한 블록체인은 모든 참여자들이 거래기록들을 가지고 있고 모든 거래기록은 연결되어 있기 때문에(이더리움의 경우 최신 상태 업데이트) 모든 기래기록에 공개적으로 접근 가능하여 확인 · 검증한 투명성의 특징이 있다.

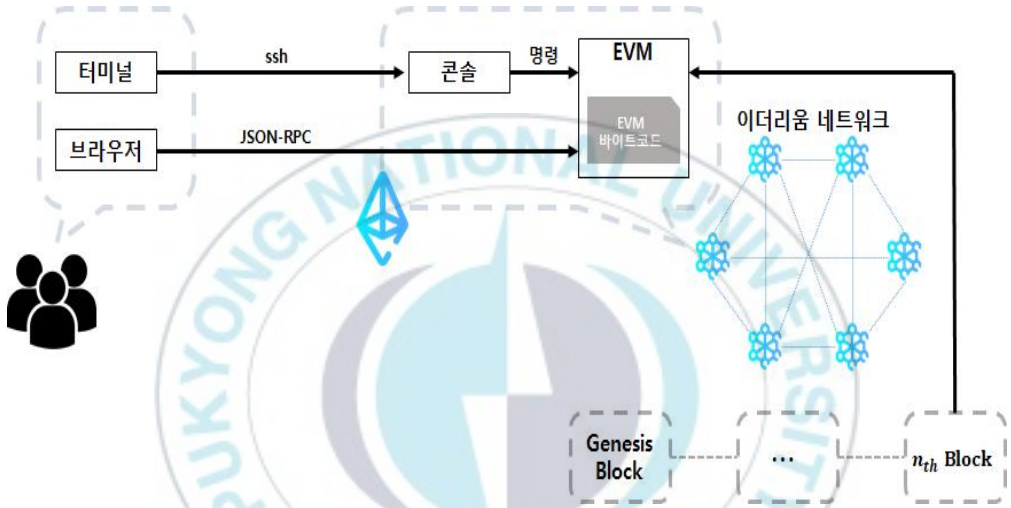
<표 1> 블록체인 기술의 특징

	장점	단점
가명성	• 유저의 개인정보를 요구하지 않음	• 불법 거래대금 결제, 탈세, 블랙마켓에서 사용 등 악용될 우려가 있음
P2P	• 불필요한 수수료 없이 유저간 서비스 유지 • 공인된 제3자 없이 거래 가능	• 문제가 발생하면 책임소재가 모호해 질 우려가 있음
투명성	• 모든 거래기록에 누구나 접근가능	• 거래 내역이 공개되어 있어 원칙적으로 모든 거래내역 추적가능 • 체인널리스와 같이 유저를 식별할 수 있음
보안성	• 장부를 공동으로 소유하고 분산된 합의를 통해 무결성 보장 • 이로인해 경우에 따라 보안유지 비용 감소 효과를 가짐	• 개인키의 분실시 복구할 방법이 없음 • 기밀성을 제공하지 않음

(2) 이더리움 스마트 컨트랙트

이더리움[12,13]은 2013년 Vitalik Buterin에 의해서 제안되었다. 블록체인 1.0으로 대면되는 비트코인의 경우 신뢰 기관 없이 암호 화폐 거래를 지원했다면 블록체인 2.0으로 대변되는 이더리움은 암호 화폐 기능과 더불어 블록체인에 튜링 완전한 컴퓨팅 기능과 그 기능을 이용할 수 있는 환경을 제공하였다. 우선 스마트 컨트랙트를 생성하고자 하는 유저는 Solidity와 같이 튜링 완전한 언어로 스마트 컨트랙트를 소스 코드를 생성한다. 그 후 생성한 소스 코드를 컴파일

하여 EVM(Ethereum Virtual Machine)이 인식가능한 바이트 코드를 생성한다. 유저는 생성된 EVM 바이트 코드로 ABI를 얻고 ABI로부터 컨트랙트 객체를 생성하여 트랜잭션을 생성하여 블록체인에 포함시킨다. 이를 배포과정이라고 하며 이러한 과정을 통해 P2P환경에서 중개자 없이 편리하고 쉽게 계약을 체결할 수 있다.



[그림 3] 이더리움 스마트 컨트랙트

이더리움 EVM에서 스마트 컨트랙트상에 정의된 함수들을 실행하면 이더리움 네트워크의 모든 노드들은 이를 검증한다. 이때 만약 스마트 컨트랙트 상에 while(1) {…}와 같은 무한루프가 존재하면 모든 노드가 무한루프를 계속 실행하게 된다. 이러한 무한루프를 방지하기 위해서 이더리움에서는 가스(Gas)의 개념을 도입하여 특정 함수를 실행하기 위해서는 특정 Gas가 지불되도록 설계하였다[12].
예) 이더 송금(21,000Gas) 즉, 이더리움에서 수수료와 같은 개념으로 Gas가 사용되며 총 수수료는 $Gas\,Price$에 가스 $Gas\,Limit$을 곱한

것으로 계산된다.

$$Total\,Fee = Gas\,\mathrm{P}rice \times Gas\,Limit$$

$Gas\,\mathrm{P}rice$(가스 가격)는 1Gas당 가격을 책정하는 것으로 Gas 가격을 높게 책정할수록 해당 트랜잭션이 블록에 포함될 확률은 상대적으로 높아진다. $Gas\,Limit$은 이더리움 엘로우 페이퍼[13]에 정의된 함수당 Gas 가격으로 사용한 함수에 따라 측정된다. 이더리움의 현재(2018년 11월)경우 노드들의 과도한 연산을 막기 위해 하나의 블록당 8,000.000만큼의 가스 총량을 갖는다[18].

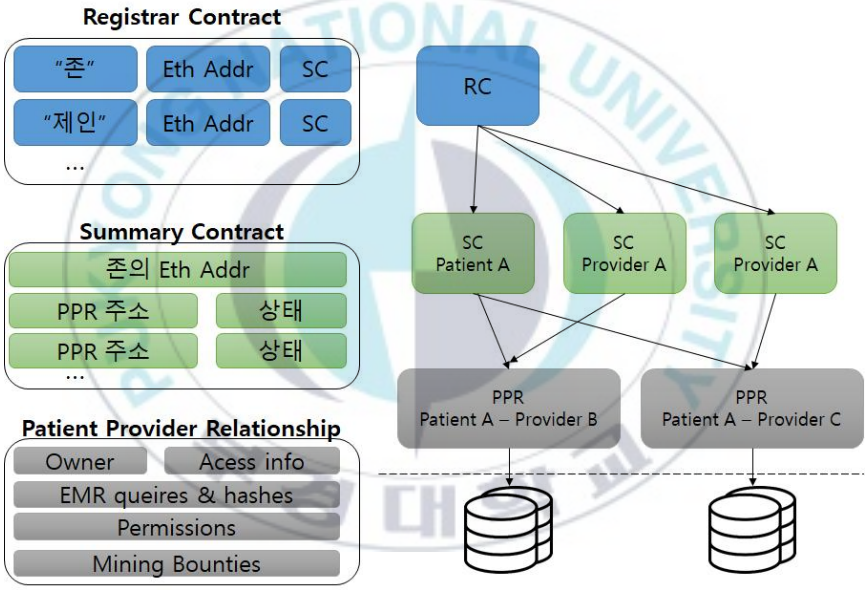
3. 블록체인 기반의 의료데이터 공유

이 절에서는 대표적인 블록체인 기반 의료 데이터 공유 시스템을 소개하고 그 문제점을 도출한다. Azaria등의 연구[7]은 Medrec이라고 하는 이더리움을 기반으로 자체 구현한 의료 데이터 공유 시스템을 제안하였다. Medrec의 의료 데이터 생성 개체인 의사는 의료 데이터를 생성하고 의료기관 데이터베이스에 저장하고 의료 데이터에 대한 해시값을 블록체인에 저장한다. 추후 의료데이터에 접근하는 환자는 의료데이터에 대한 무결성을 블록체인에 저장된 해시값과 통해 검증할 수 있다. 또한 연구기관과 의료관련기관들의 블록체인 마이닝 과정에 참여를 유도하기 위해 Bounty라고 하는 의료 데이터를 인센티브로 제공한다. 이 과정들은 유저의 신원과 이더리움 주소를 매핑하여 환자의 고정 ID를 생성하는 스마트 컨트랙트인 Register Contract(RC)와, 환자와 의사가 의료기관내 데이터베이스에 접근 할 수 있는 정보에 대한 스마트 컨트랙트인 Patient-Provider Contract(PPR), 환자의 의료데이터들의 요약정보인 Summary Contract(SC)로 구성되어 있다. 하지만 RC는 환자의 고정 ID를 생성하기 때문에 환자의 익명성을 보장할수 없다. 왜냐하면 비트코인과 이더리움은 익명성을 보장하지 않고 가명성을 보장하기 때문에 환자의 프라이버시는 보장되지 않는다. 그 이유는 블록체인내 트랜잭션 분석과 다른 기술을 통해 환자의 신원이 쉽게 확인되기 때문이다[14]. 이러한 서비스를 지원하는 업체로는 체인널리시스가 있다[15].

하이퍼레저 기반의 MedicalChain[16]에서 환자는 프라이빗 블록

체인에 참여하기 전 신원인증을 하고 블록체인 ID인 UUID를 생성한다. MedicalChain 역시 Medrec과 같은 이유로 환자의 익명성이 보장되지 않고 드러나는 문제가 발생한다.

기존의 블록체인 기반 의료 데이터 공유 시스템에서는 체인널리시스와에서 사용하는 기법처럼 블록체인 내 트랜잭션 분석과 다른 기술을 통해 환자의 신원이 쉽게 확인되기 때문에 본 논문에서는 블록체인 사용할 때 발생하는 문제를 해결하기 위해 스텔스 주소를 사용하여 블록체인 트랜잭션의 수신자(환자)를 숨긴다.



[그림 4] Medrec 환자 ID 스마트 컨트랙트 RC

Patient

Variable Type	Variable	Description
String	ID	A unique String

[그림 5] MedicalChain 환자 ID 구조

III. 블록체인 환경에서 프라이버시를 보호하는 의료 데이터 공유 시스템

본 장에서는 제안하는 의료 데이터 공유 모델에서 사용되는 시나리오 및 가정사항과 참여개체를 정의하고 의료 데이터 공유를 위한 블록체인 기반의 무결성 보장 및 프라이버시를 보호하는 시스템을 제안한다.

1. 시스템 모델

가. 시스템 모델 시나리오 및 가정사항

(1) 가정사항

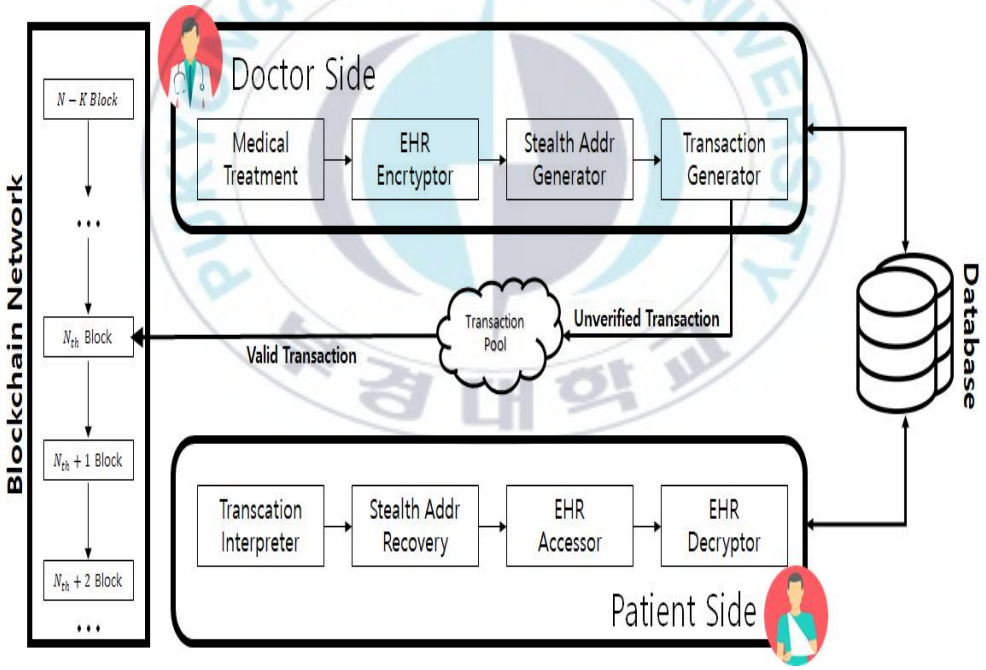
본 논문에서는 의사가 생성한 의료데이터를 의료기관 데이터베이스에 저장할 때 대칭키 기반 암호 기법을 사용하여 암호화 한다고 가정하며 의료 데이터 공유시 의사는 의사(송신자)와 환자(수신자)만 복호화 가능한 암호 기법을 사용하여 암·복호화 한다고 가정한다. 또한 의사는 DICOM 포맷을 사용한다고 가정한다. 그 이유로는 데이터를 생성하여 변조하지 않고 열람만으로도 확장자에 따라서는 데이터의 해시값은 달라질 수 있다. 예를 들어 MS 2007 이전버전 CFBF(Compound File Banary Format) 경우 데이터의 열람만으로 해시값이 변경되었으나 MS 2007 이후버전에서 MCDF(MS Compound Document File)로 전환됨에 따라 데이터의 열람만으로

해시값이 변경되지 않는다. 이와 같이 열람만으로 데이터의 해시값이 변경되지 않기 위하여 본 논문에서는 국내 · 국외 의료 디지털 영상 · 이미지 표준인 DICOM(.dcm)포맷을 사용하여 의료 데이터를 저장한다고 가정한다.

(2) 시스템 모델

본 논문에서 사용되는 블록체인은 퍼블릭 블록체인으로, 퍼블릭에 참여하고자 하는 개체는 이더리움 파라미터에 맞춰 공개키와 이더리움 주소를 생성하고 감독기관에 자신의 신원을 증명하는 서류를 제출하여 공개키와 이더리움 주소를 등록한다. 이 과정 후 환자가 진료를 요청했을 때 의사는 진료 후 의료 데이터를 생성하며 본인의 서명을 포함한 EHR을 생성한다. 의사는 임의의 랜덤한 값을 뽑아 대칭키 암호기법을 생성하고 이를 사용하여 EHR을 암호화하며 암호화된 EHR을 생성한다. 이 암호화 키는 추후 의사(송신자)와 환자(수신자)만 복호화 할 수 있다. 의사는 암호화된 EHR과 이 데이터의 해시값을 의료기관 데이터 베이스에 저장한다. 이를 받은 의료기관 데이터 베이스는 URL값을 반환한다. 의사는 본인의 서명을 입력으로하고 환자의 이더리움 주소를 출력으로하는 의료 데이터의 무결성에 필요한 모든 메타데이터 값을 모아 트랜잭션을 생성하고 P2P 네트워크상에 전파한다. 이더리움 블록체인은 후보 트랜잭션들을 모아 트랜잭션 풀에 저장하고 순서대로 블록에 포함시기 위해 PoW 합의과정을 거쳐 블록에 포함된다. 본인만 구할 수 있는 스텔스주소를 통해 블록체인내의 본인 트랜잭션을 검색하고 환자와 의사만 블록체인에 적시된 URL주소를 통해 암호화된 EHR을 다운로드하여 대칭키 암혹법으로 복호화 한다. 복호화 후 환자는 의사의 서명이 포함된 EHR을 획득할

수 있고 이로써 신뢰성 있는 양질의 의료 데이터로 활용 할 수 있다. 환자는 신뢰성 있는 양질의 데이터를 두 형태로 활용할 수 있는데 다음과 같다. 1)사회 공헌을 위한 자발적 데이터 기부 2)판매를 통한 이윤 창출. 블록체인을 통한 직접적인 거래시 중개기관이 없기 때문에 환자가 의료데이터를 제공하고 헬스케어 소비자에게 돈을 받지 못하거나 그 반대의 경우가 발생하기 때문에 1)의 목적으로만 블록체인을 사용하고 2)의 경우는 4장에서 스마트 컨트랙트 기반으로 개인간 의료데이터 판매를 구현한다.



[그림 6] 시스템 모델

나. 참여개체

제안 시스템은 의사(Doctor), 환자(Patient), 감독기관, 사회공헌 기관으로 구성된다.

(1) 의사

의료 데이터를 생성하는 개체로 환자에게 의료 서비스를 제공하고 의료 데이터를 생성한다. 본인의 서명을 입력값으로 하고 환자의 이더리움 계좌 주소를 출력 값으로 하는 트랜잭션을 생성하며 이때 이더리움 입력데이터의 Optinal Data필드에 의료 데이터와 관련된 메타데이터를 입력한다. 형태와 크기가 다양한 의료데이터를 직접 블록체인에 포함시킬시 비 허가된 개체가 접근할 수 있고 블록체인의 크기가 커지는 결과를 초래함으로 의사는 환자의 의료데이터와 관련된 메타데이터만을 포함한다.

(2) 환자

환자는 본인의 의료데이터를 적극적으로 활용(판매, 기부, 헬스케어 서비스 제공)하고자 하는 개체로 적극적인 활용을 위해 의료데이터의 무결성과 신뢰성을 얻고자한다.

(3) 사회 공헌 기관 (SCA)

의료 데이터를 기부 받는 기관으로 돈을 주고 받지 않기 때문에 스마트 컨트랙트를 사용하지 않고 의료데이터 기부자는 의료 데이터 기부자와 사회 공헌 기관만 복호화 할 수 있는 암호기법을 사용하여 의

료 데이터를 기부한다.

(4) 감독기관

감독기관은 환자의 신원을 인증하고 환자가 생성한 이더리움 공개키, 주소를 저장하고 있으며 한 개체가 다른 개체의 신원을 요청하면 응답한다. 예를 들어 데이터를 공유 받은 개체가 의료 데이터가 의사에게서 생성된 데이터가 맞는지 확인하기 위해 EHR에 있는 $Addr_{Doctor}$가 의사가 맞는지 신원 요청시 이를 감독기관의 데이터 베이스를 통해 검증 할 수 있게 한다.

즉, 하나의 의료데이터에 대해 TXID, 공개키, 서명값, Data Type을 저장하고 있고 누구나 TXID 번호를 통해 이를 검증 비교 할 수 있다.

다. 보안 요구사항

제안하는 모델에서는 아래와 같은 보안 요구사항을 만족해야한다.

1. 의료 데이터의 위·변조 방지 : 의료 데이터 생성자인 의사는 생성된 의료데이터를 임의로 수정하거나 변조할 수 없어야 하며 참여 개체 누구나 이를 확인할 수 있어야한다.

2. 환자의 익명성 보장 및 환자의 정보 연계불가 : 인가된 의료인과 의료기관을 제외하고 해당 의료데이터가 어떤 환자의 것인지 알 수 없어야 하며 의료 데이터간의 연계를 통해 특정 환자의 데이터임을 알 수 없어야한다.

3. 데이터 소유권 주장 및 책임 추궁성 제공 : 의료분쟁발생시 특정 의료데이터를 특정 의사가 생성했음을 부인할 수 없어야 하며 중요한 증거로서 활용 가능해야 한다.

<표 2> 표기법

표 기	의 미
PU_{entity}, PR_{entity}	Entity들의 공개키, 비밀키쌍
$Enc(Key, Data)$	key를 이용하여 $Data$를 암호화
$Dec(Key, Data)$	Key를 이용하여 $Data$를 복호화
$H(\cdot)$	암호학적 해시함수 (Keccak-256)
h	데이터의 해시값($H(data)$)
MD_{entity}	의사가 생성한 Entity의 의료 데이터
$Sig_{key}(Data)$	key를 이용하여 $Data$를 서명
EHR_A	환자 A에 대한 의료 데이터에 의사의 서명이 포함된 데이터
B	환자가 스텔스 주소 생성을 받기 위해 생성하는 두 번째 공개키 개인키 쌍
CT_{EHR}	EHR을 암호화 한 의료 데이터
T	ECDSA 공개 파라미터 셋
P	Modulo 소수
a	타원곡선 방정식에서 사용되는 계수1
b	타원곡선 방정식에서 사용되는 계수2
G	생성점 (Generator Point)
n	포인터 G의 위수(The order of Point G)
h	여인수(Cofactor)

2. 제안 시스템 모델의 프로토콜

앞 절에서 설명한 시스템 모델 시나리오 및 개체 정의를 통해 의료 데이터 공유 및 활용 시 프라이버시를 보장하는 의료 데이터 공유 모델을 설계한다. 제안 모델은 시스템 모델 환경 설정, 사용자 등록, 환자 의료 데이터 생성, 스텔스 주소 및 접근제어 구조 생성, 접근제어 키 암호화 및 데이터 베이스 저장, 트랜잭션 검증 및 블록생성, 데이터 검색 및 의료 데이터 복호화, 환자의 데이터 활용 단계로 구성되어있다.

가. 이더리움 개인키, 공개키 및 이더리움 주소 생성 및 사용자 등록

감독기관을 제외한 모든 참여자들은 의료 데이터 블록체인 시스템을 참여하기 위해 사전에 공개되어있는 공개 파라미터(T)를 통해 이더리움 개인키, 공개키 및 주소를 생성하는 단계이다. 이더리움의 경우 ECDSA 파라미터로(T) secp256k1 Curve를 사용한다. 공개 파라미터 $T = P, a, b, G, n, h$, secp256k1는 다음과 같다.

P : FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFC2F

a : 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

b : 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

G : 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

n : FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

h : 01

(가) 개인키(PR) 생성 :

① 모든 참여 개체는 암호학적 난수생성기를 사용하여 256비트의 각자의 개인키(PR_{Entity})를 생성한다.

(나) 공개키(PU) 생성 :

① 모든 참여 개체는 각자의 (pu_{Entity})공개키를 생성한다.

$PU = PR \times G$

단, 환자는 스텔스 주소 생성을 위해 공개키 쌍을 2개 생성한다.

(다) 이더리움 주소($Addr$) 생성 :

① 모든 참여 개체는 각자의 이더리움 주소($Addr_{entity}$)는 공개키를 Keccack-256 해시 함수를 통해 해시한 결과의 마지막 20바이트로 구성된다.

② 생성된 20바이트 주소 앞에 0x를 붙여 이더리움 주소임을 표시한다.

(라) 이더리움 주소($Addr$) 생성 :

① 공개키와 이더리움 주소를 생성한 감독기관에 자신의 신원을 증명하는 서류를 제출하여 공개키와 이더리움 주소를 등록한다.

나. 환자 의료 데이터 생성

의사가 환자를 진료하고 의료 데이터를 생성하는 단계이다. 사용자 등록과정을 끝낸 환자는 의료기관으로 가서 의사에게 진료를 요청한다. 의사는 대면한 환자 진료를 시작한다. 진료를 마친 후 의사는 환자 의료데이터 MD_A를 생성하고 본인의 서명이 포함된 EHR_A를 생성한다.

$$EHR_A = Addr_A||Addr_B||tistamp||MD_A||Sig_{PR_B}(Addr_A||Addr_B||tistamp||MD_A)$$

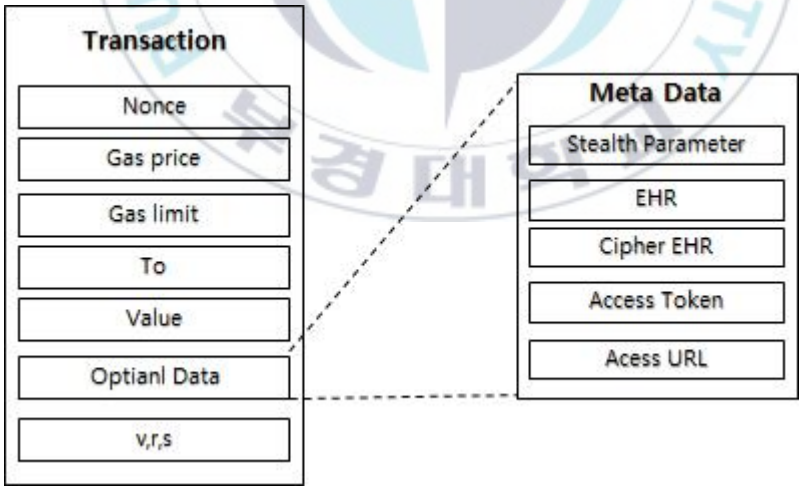
다. 스텔스 주소 생성

의사는 환자의 의무기록을 공유하고 환자와 의사간 연계성을 없애기 위해 즉, 수신자(환자) 프라이버시를 보장하기 위해 스텔스 주소를 생성한다. 의사는 의료 데이터 공유를 위해 랜덤한 $r \in [1, P-1]$를 선택하고 $R = r \cdot G$를 계산한다. 환자는 세션 접근키 $B = b \cdot G$를 생성하고 의사에게 전달한다. 이 과정을 마친 후 환자를 위한 스텔스 주소 SA_A를 생성한다.

$$SA_A = (H(r \cdot PU_A)) \cdot G + B$$

라. 암호화 및 데이터 베이스 저장

의사는 의사와 환자만 복호화 할 수 있게 암호화하는 기법을 적용한다고 가정한다. 암호화된 의무기록 CT_{EHR}의 무결성 보장을 위하여 $H(CT_{EHR})$를 통해 해시 값을 생성한다. 그런 다음 의사는 의료기관 데이터 베이스에 CT_{EHR}과 $H(CT_{EHR})$을 저장한다. 의료기관 데이터베이스는 이를 저장하고 이에 접근할 수 있는 URL을 반환한다. 의료기관 데이터 베이스에 의료 데이터 입력을 마친 의사는 트랜잭션을 생성하여 P2P 네트워크 상으로 브로드 케스트 하여 의료 데이터 검증자에게 전달한다. 트랜잭션 구조와 입력되는 메타데이터 값은 그림 7과 같다.



[그림 7] 이더리움 트랜잭션 및 제안 시스템 메타데이터

● To : 해당 트랜잭션을 받는 송신자를 의미하며. 송신자와 수신자

의 연계성을 제거하기 위해 Stealth Address를 사용한다.

- Stealth Parameter : 스텔스 주소를 생성한 송신자가 사용한 파라미터 값을 의미한다.

- EHR : 실제 환자 의료데이터를 해시함수로 해시한 결과로 고정된 길이의 비트열을 가진다. 복호화된 의료 데이터에 접근 가능한 개체는 해당 의료 데이터가 변경되지 않았음을 확인할 수 있다.

- Cipher EHR : 암호화된 의료 데이터를 해시함수로 해시간 결과로 고정된 길이의 비트열을 가진다. 암호화된 의료 데이터에 접근 가능한 개체는 해당 의료 데이터가 변경되지 않았음을 확인할 수 있다.

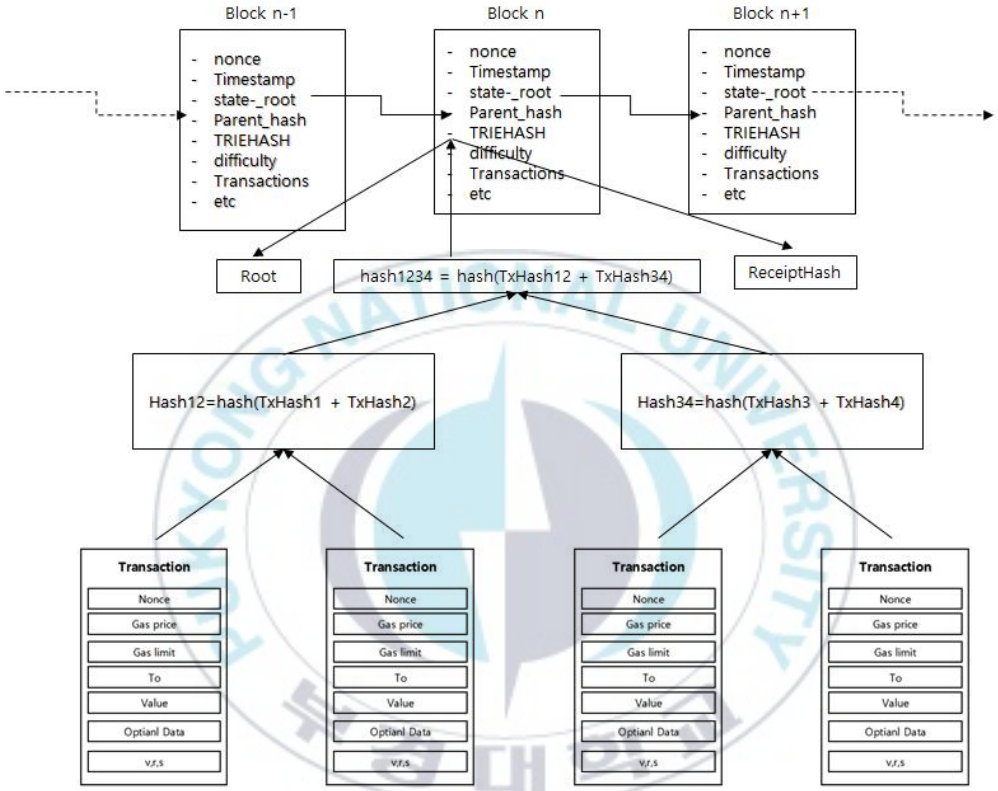
- Access Token : 의료 데이터(EHR_A)를 암호화할 때 쓰인 대칭키 값을 암호화한 값으로 오직 해당하는 개체나 속성값을 가진 개체만이 암호화된 CT_{EHR}을 Key_{EHR}로 복호화하여 의무기록을 열람할 수 있다.

- Access URL : 암호화된 EHR기록이 저장되어 있는 데이터 베이스 주소이며 블록체인을 통해 누구나 접근하여 다운로드 할 수 있지만 Access Token(대칭키)을 가진 개체만이 복호화할 수 있다.

마. 트랜잭션 검증 및 블록생성

본 논문에서 트랜잭션 검증 및 블록생성과정 (마이닝)은 이더리움

에 기반하여 PoW를 사용하며 이더리움 블록의 구조는 그림 7와 같다.



[그림 8] 이더리움 블록 구조 및 트랜잭션 구조

바. 데이터 검색 및 의료 데이터 복호화

해당 단계에서는 블록체인에서 자신과 관련된 블록을 찾고 의료 데이터베이스로부터 의료 데이터를 얻고 복호화 하는 과정을 나타낸다.

환자는 블록체인 내의 자신이 소유권을 가지고 있는 스텔스 주소를 찾기 위해 다음과 같은 연산을 진행한다.

$$SA_A{}' = (H(PR_A \cdot \quad R) \bmod P) \cdot \quad G + B$$

환자는 SA와 연관성 있는 주소를 찾기 위해 SA'를 계산하고 블록체인에서 본인의 데이터를 찾은 후 블록체인에 기록된 URL 주소를 통해 의료 데이터가 있는 데이터 베이스에 접속하고 의료 데이터를 요청한다. 의료 데이터 베이스는 환자에게 저장되어 있던 CT_{EHR}를 반환하고 환자는 환자와 의사만이 복호화할 수 있는 암호키로 복호화를 수행한다.

사. 환자의 데이터 활용

앞서 가-바의 과정을 통해 블록체인에 저장된 무결성이 보장되는 데이터를 환자는 활용하며 활용 방법은 크게 두 가지로 분류 될 수 있다.

① 사회 공헌을 위한 자발적 데이터 기부
② 판매를 통한 이윤 창출

3장에서는 블록체인 네트워크 참여자간 신뢰관계가 없기 때문에 환자가 본인의 의료데이터를 먼저 넘겨주고 헬스케어 소비자에게 돈을 받지 못하거나 그 반대의 경우로 헬스케어 소비자가 환자에게 돈을 주고 의료 데이터를 받지 못하는 상황이 발생할 수 있다. 이러한 문제는 4장에서 스마트 컨트랙트를 기반으로 하여 서로간 신뢰가 없는 네트워크에서 의료 데이터 판매를 구현(2번의 경우)하고 분석하며 3장에서는 사회 공헌을 위한 자발적 데이터 기부(1번의 경우)로 환자는 사회에 공헌하는 기관에 자신의 의료 데이터를 무료로 제공한다.

자. 보안 요구사항 분석

1. 의료 데이터의 위·변조 방지 : 블록체인의 모든 블록은 연결되어 있기 때문에 현재 $n+100$ 높이만큼의 블록이 생성되었을 때, n번째 블록의 거래정보를 바꾸기 위해서는 $n+101$ 만큼의 블록을 생성해야하기 때문에 데이터의 변조는 사실상 불가능하다. 이더리움은 PoW(작업증명) 알고리즘을 기반으로 합의를 진행하기 때문에 2018년 12월 이더리움 네트워크의 전체 해시파워는 184194.67 GH/s로 사실상 하나의 블록을 생성하도 힘들다. 공격자가 의사가 Input Data 필드를 사용하여 생성한 의료 데이터의 메타데이터 값을 삭제하거나 위·변조 하는 것은 거의 불가능하며 위·변조 시 얻는 이득이 위·변조 시도 시 드는 비용보다 작다.

2. 환자의 익명성 보장 및 환자의 정보 연계불가 : 의사는 의료데이터를 생설 할 때 환자에게 일회용 주소인 스텔스 주소를 생성 ($SA_A = (H(r \cdot \ PU_A)) \cdot \ G + B$) 하여 환자만 알 수 있게끔 한다. 이

때 환자는 같은 B값을 사용하더라도 랜덤한 r로부터 R이 계산되어 져 같은 환자에게도 서로 다른 일회용 주소를 생성하여 특정 환자임을 특정할 수 없다.

3. 소유권 주장 및 책임 추궁성 제공 : 스텔스 주소를 구할 때 사용되는 B를 생성하는 b값은 환자만 알기 때문에 본인의 의료 데이터임을 주장하여 보험 청부 등에 사용될 수 있으며. 또한, 블록에 트랜잭션을 추가할 때 의사의 서명값이 필요하기 때문에 의료분쟁 발생시 특정 의료데이터를 특정 의사가 생성했음을 부인할 수 없어 중요한 증거로서 활용 가능하다.

IV. 사용 사례 : 스마트 컨트랙트 기반의 의료 데이터 판매 구현

1. 구현 목표 및 실험환경 구성

본 장에서는 3장의 프로토콜을 기반으로 의료데이터의 무결성을 안전하게 보장했을 때 이를 활용하는 사용 사례를 구현하고자 한다. 3장에서의 의료데이터 판매자가 의료데이터를 공유하고 상응하는 보상을 못 받을 수 있는 문제와 반대로 구매자가 보상을 지불하고 상응하는 의료 데이터를 못 받을 수 있는 문제점을 해결하는 스마트 컨트랙트 기반의 P2P 의료 데이터 판매를 구현 한다.

스마트 컨트랙트와 웹 페이지는 Ubuntu Server 18.04 LTS 상에서 구동하며 Nginx를 통해 웹 페이지를 설계하여 스마트 컨트랙트의 UI를 제공하여 유저가 쉽게 스마트 컨트랙트를 생성 할 수 있게 개발하였다. 의료 데이터 검증을 위한 DB는 Ubuntu Server 16.04 LTS 상에서 구동하며 Apache2를 통해 php언어 기반으로 MySQL에 쿼리를 날려 DB의 값을 읽어온다. 스마트 컨트랙트는 Browser Solidity에서 0.4.24 버전 프라그마을 통해 작성하였으며, 이더리움의 테스트넷인 Ropsten 테스트넷을 사용하였다. 이더리움 지갑으로는 Chrome 확장 프로그램인 Metamask와 이더스캔 홈페이지를 통해 블록체인을 다운로드 받지 않고 데이터를 확인하고 검증하였다.

<표3>과 <표4>의 환경에서 스마트 컨트랙트를 구현하였으며 그

결과를 실험하였다. 구현 과정과 시나리오는 2절에서 서술하고 실험 결과는 3절에서 살펴본다.

<표 3> 웹 테스트 환경

구분	내용
OS	AWS (Ubuntu Server 16.04 LTS, Ubuntu Server 18.04 LTS)
Web Server	NGINX 1.10.3, Apache2.4.18
DB	IPFS, MySQL
Language	JavaScript, PHP

<표 4> 스마트 컨트랙트 테스트 환경

구분	내용
Platform	Ethereum
Blockchain	Ropsten Testnet
Solidity	0.4.24
Wallet	Metamask
Ethereum browser	Remix (Online)

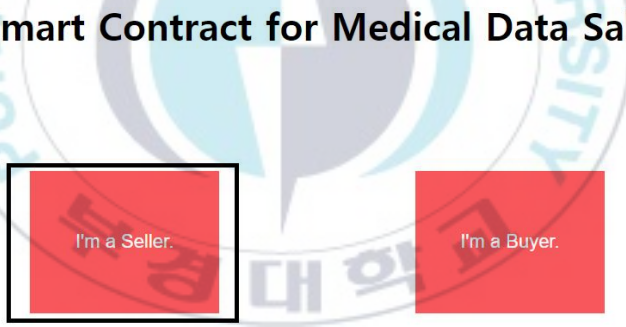
2. 구현 세부사항

가. 적용 시나리오

스마트 컨트랙트 기반의 의료데이터 판매 시나리오는 다음과 같다.

<의료 데이터 판매 등록 스마트 컨트랙트 작성>

① 홈페이지 접속 : 판매자는 의료데이터 판매 사이트에 접속하여 “I’ m a Seller” 버튼을 클릭한다.



[그림 9] 의료데이터 판매 웹 페이지 초기 화면 - 판매자

② 의료데이터 판매 스마트 컨트랙트 생성 : 판매자는 의료데이터 판매 스마트 컨트랙트 생성을 위해 판매하고자 하는 의료 데이터의 금액을 정하여 금액의 2배를 예치하며. 의료 데이터의 타입에 대한 설명을 적고 해당 의료데이터가 포함되어 있는 트랜잭션 번호(TXID)를 입력한다. 마지막으로 판매할 데이터를 업로드한다. 업로드한 데이터는 IPFS API를 통해 IPFS에 저장된다.

<표 5> 의료정보 판매를 위한 스마트 컨트랙트 매개변수 및 설명

구분	특징
Value in Gwei you want (Value)	• 판매자가 희망하는 의료데이터의 금액의 2배만큼 Value값으로 예치함 • 세밀한 거래 금액 설정을 위해 Gwei단위로 거래
Describe medical data (Data Type)	• 판매할 의료 데이터의 유형입력 (사전정의) • 감독기관 데이터 베이스는 하나의 의료데이터에 대해 TXID, 의료 데이터를 생성한 의사의 공개키, 의사의 서명값, 데이터 유형을 저장함
TXID	• 향후 구매자는 TXID를 검색을 통해 감독기관 데이터 베이스에서 해당 의료데이터를 검증 할 수 있게함

판매자 컨트랙트의 예시는 그림10과 같이 진행된다.

Value : 1,000,000,000 (Gwei) 약 5만 1천원

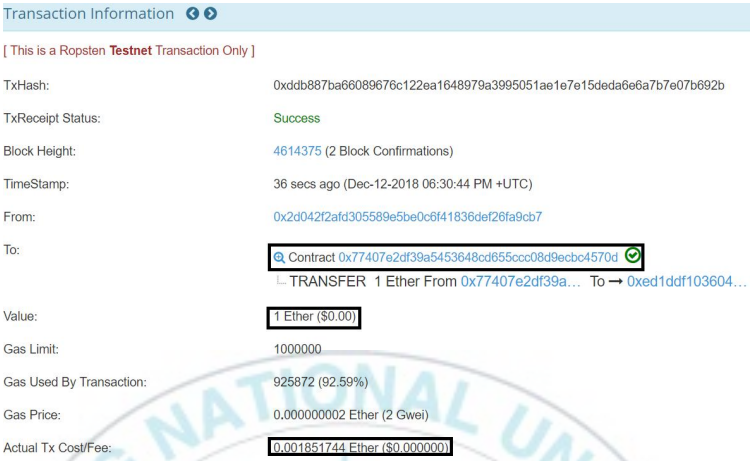
Data Type : Blood sample of gestational diabetes (임신성 당뇨병의 혈액샘플)

TXID :

0xc56d506c51959f5b76abddf7cb93959eea9cfb34bbf21f9a799a884b456908c0 (사전에 의사에게서 생성된 의료데이터)

판매자는 판매하고자 의료데이터에 대한 정보를 입력하면 웹 페이지는 판매자가 입력한 정보에 알맞는 스마트 컨트랙트를 생성한다. 이때 스마트 컨트랙트는 판매자가 판매하고자 하는 금액의 2배를 예치하도록 하여 유효하지 않은 의료 데이터를 입력할 시 예치한 금액

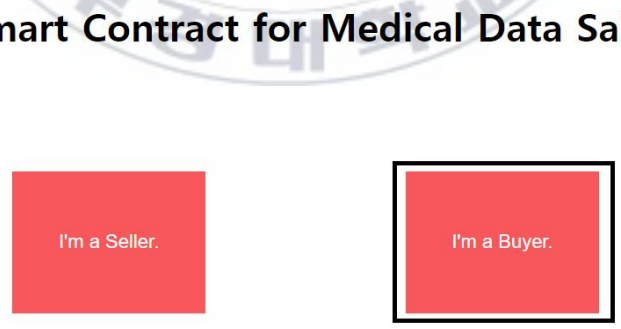
을 사용하지 못하도록 하여 정당한 거래를 등록 하게 유도한다.



[그림 10] 의료데이터 판매 등록 컨트랙트 상세정보

<의료 데이터 구매>

① 홈페이지 접속 : 구매자는 의료데이터 판매 사이트에 접속하여 “I’ m a Buyer” 버튼을 클릭한다.



[그림 11] 의료데이터 판매 웹 페이지 초기 화면 - 구매자

② 희망하는 의료데이터 검색 : 구매자는 웹 페이지에 업로드된 판매

스마트 컨트랙트를 보고 희망하는 가격의 의료 데이터 판매자를 찾는다. 그림 12의 우측의 정보들은 스마트 컨트랙트 주소를 이더스캔에 검색을 통해 확인할 수 있기 때문에 웹 페이지 관리자가 무단으로 변경하여도 이를 검증 할 수 있다. 의료 데이터 판매 스마트컨트랙트는 Created 상태와 Inactive 상태로 나뉘며 Created는 아직 판매되지 않은 의료데이터를 의미하며 Inactive는 판매 완료된 의료데이터를 의미한다.

[그림 12] 웹 페이지를 통한 의료 데이터 판매 컨트랙트 상세정보

③ 희망하는 의료 데이터 검증 : 구매자는 구매할 의료 데이터가 의사에게서 생성되었는지 여부와 Data Type이 맞는지 감독기관의 데이터 베이스에서 확인할 수 있다. 그림 13과 같이 해당 의료데이터의 TXID를 통해 검색하고 해당 트랜잭션의 메타데이터 필드에 입력된 의료데이터의 해시값과 데이터 베이스의 의사의 공개키 값과 서명값을 통해 의사에게서 생성된 데이터가 맞는지 검증 할 수 있으며 데이터 유형이 스마트 컨트랙트상에 등록된 것과 같은

유형인지 검증할 수 있다.

Medical Institution DB

txid	public_key
0xc27e5ba730bd7c6e79e5657d06221504a0f6e7c500955a964c9e6691ad84de06	04e231184465a0cc22bf4f067e56f2092f4b4a9207e926e9815786855596bb96410bc86a10b83b6b156267dcc8c156def8775a0be8560468fbf7db70b92e2366bc
0xc3842567827c693d2ba4ad131e14ea8730e8cc4e79728f11603e0d41f4749242	040fdccc869d5239a4f1c997d903801a950fea6f29129cc9bd70b87e2597fd221d5bfcf63c513e3d01209632be452780816e9c22d12208545cea4806081243966c
0xfe8f3c3c24123aae68b69e164451bd41469f1f5c838943b897a45c75ff7048c9	04efac6c46ff55805c58fa7a49ae66bd09013cb3a8721d2e8efa17a49107bbf2d18dfd2a0480c45046af8ea69759da6ec861d6ae971d264d820effe67fa7b573d4

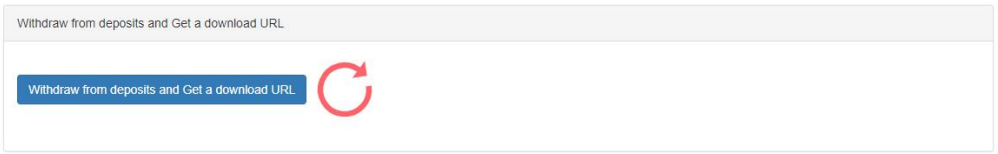
[그림 13] 의료데이터 검증을 위한 데이터 베이스 구현

④ 의료데이터 구매 결정 : 구매자는 그림 14와 같이 의료데이터 구매를 위해 의료데이터 금액의 2배만큼의 금액을 예치한다. 이때, 구매자가 예치금을 예치하고 의료데이터를 받게 될 시 본인의 예치 금액을 손해 보면서 의료데이터 금액을 판매자에게 전송하지 않는 문제가 발생할 수 있기 때문에 예치만으로 의료데이터를 바로 주지 않는다.

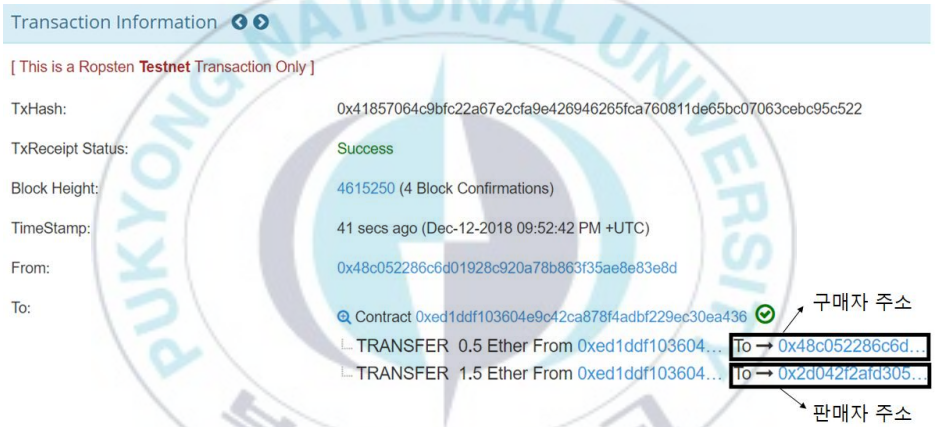
[그림 14] 의료데이터 구매를 위한 예치를 통한 상태변화

⑤ 의료데이터 구매 확정 : 그림 15의 구매 확정 버튼을 통해 구매자가 거래를 확정하면 판매자에 의료데이터 판매 컨트랙트의 전체 예치금의 3/4만큼, 구매자에게 전체 예치금의 1/4만큼 이더리움을 전송하는 트랜잭션이 발생된다. 그림 16을 통해 정상적으로

거래가 처리되었음을 알 수 있다. 끝으로, 그림 17과 같이 트랜잭션 발생 후 구매자는 해당 의료데이터를 다운로드 할 수 있는 IPFS 주소를 얻게 된다.



[그림 15] 의료데이터 구매 확정 구현



[그림 16] 의료데이터 판매 스마트 컨트랙트 구매확정후 예치금 변화상태

[그림 17] 구매 종료 후 의료데이터 IPFS 접근 구현

3. 구현결과 분석

국내의 에스크로 서비스 프로바이더들은 신용카드를 통한 에스크로 서비스 이용시 국내 결제의 경우 프로바이더들에 따라 3.3~3.7%의 수수료를 지불해야하며 국외의 경우 4.5%가량의 수수료를 지불해야 하며 사용유형에 따라 별도로 연 관리비를 납부해야한다. 하지만, 스마트 컨트랙트 기반의 의료 데이터 판매의 경우 소모되는 비용(Gas)는 표7과 같다. 의료데이터 판매 스마트 컨트랙트 배포 비용의 경우 한화로 환산할 경우 약 13원이며 예치금 반환 스마트 컨트랙트 배포 비용의 경우 한화로 환산할 경우 약 9원이며 의료 데이터의 메타데이터 등록 트랜잭션의 경우 약 26원으로 하나의 의료 데이터를 생성하고 판매하기 까지 48원이 소모된다. 스마트 컨트랙트 기반은 거래 금액에따라 별도의 수수료가 붙지 않기 때문에 기존의 에스크로를 통한 판매보다 비용적인 측면에서 수수료를 낮출 수 있다.

<표 6> 트랜잭션과 스마트 컨트랙트 배포 비용

구분	비용(Gas)
스마트 컨트랙트 배포	• Gas Used : 44284 • Gas Price : 2 Gwei
예치금 반환 스마트 컨트랙트	• Gas Used : 63494 • Gas Price : 2 Gwei
의료 데이터의 메타데이터 등록 트랜잭션	• Gas Used : 37048 • Gas Price : 7Gwei

V. 결 론

향후에도 의료 데이터의 양은 가파르게 증가할 것이고 AI 기술도 꾸준히 발전할 것으로 전망된다. 따라서 발전된 AI 기술과 방대한 의료데이터를 효율적으로 사용하기 위해서 의료 데이터의 무결성을 보장하는 것과 현대 의료 패러다임에 맞춰 의료 데이터를 활용하는 방법에 대한 중요도는 더욱 커질 것으로 예상된다.

현재 의료정보 시스템은 의료기관 중심으로 운영되어 환자는 자신의 의료 데이터에 대한 접근 권한이 없다. 그래서 여러 의료 기관에 파편화된 본인의 의료 데이터의 진료조작 문제에 대해서는 해당 의료기관 의료인의 양심에 맡길 뿐 데이터의 무결성이 훼손되어도 이를 확인할수 있는 방법이 없으며 의료 행위가 종료된 시점 이후에 수정되거나 추가 기재하여 이를 부정적인 방법으로 사용하여 의료 행위의 적절성을 판단하는 자료로 사용할 경우 환자는 이를 증명할 방법이 없다. 또한 본인의 의료 데이터를 활용하는데 있어 여러 가지 어려움이 존재한다.

본 논문에서는 의료 데이터를 활용하고자 할 때 발생했던 기존의 여러 문제점을 해결하기 위해서 블록체인의 투명성과 보안성등의 특징들을 사용하였고, 블록체인 사용시 발생하는 환자의 프라이버시 문제를 스텔스 주소를 통해 해결하고자 하였다. 또한, 의료 데이터의 무결성이 보장될 때 환자가 이를 활용하는 사례로 스마트 컨트랙트 기반의 의료 데이터 판매를 구현하여 판매자가 의료 데이터를 구매자에게 전송하고 상응하는 보상을 못 받을 수 있는 문제와 반대로 구매자가 보상을 지불하고 상응하는 의료 데이터를 못 받을 수 있는 문제

점을 해결하기 위해 판매자와 구매자가 의료 데이터 가치 이상의 금액을 예치함으로써 구매자가 판매자에게 이더리움을 전송하는 트랜잭션을 발생했을 때 의료 데이터를 전송 받을 수 있는 스마트 컨트랙트를 구현하였다. 끝으로, 의료 데이터 판매 외에도 스마트 컨트랙트를 통해 자동 보험료 청구나 특정 병력을 지닌 사람을 위한 보험 판매 시 투명한 본인의 병력공개를 통한 특화된 보험가입을 할 수 있는 등 환자는 블록체인에서 보장받은 의료 데이터를 기반으로 본인의 의료 데이터를 다양한 방법으로 활용할 수 있을 것으로 기대된다.

참고 문헌

[1] Accenture, “Digital Health Tech Vision 2018,” [Online], Available : https://www.accenture.com/t20180625T060849Z__w__/us-en/_acnmedia/PDF-78/Accenture-digital-health-tech-vision-2018.pdf., 2018.

[2] Nambiar, R., Bhardwaj, R., Sethi, A., & Vargheese, R, “A look at challenges and opportunities of big data analytics in healthcare,” In Big Data, 2013 IEEE International Conference on pp. 17-22 IEEE, 10. 2013.

[3] 건강보험심사평가원, “ 30일 이내 동일상병으로 타 의료기관에서 특수의료장비 CT, MRI, PET 재촬영한 현황,” 보도자료, 2014

[4] 마이차트. [Online], Availabe: https://mychart.kr/portal/about/intro.do

[5] KOSIS 통계자료. [Onlie]. Available: http://kosis.kr/statHtml/statHtml.do?orgId=110&tblId=DT_11001N_2013_A042

[6] R.J Krawiec., et al., "Blockchain: Opportunities for health care." Proc. NIST Workshop Blockchain Healthcare. 2016.

[7]]. A. Azaria, et al., “Medrec: Using Blockchain for medical data access and permission management,” Open and Big Data(OBD), International Conference on, IEEE, 2016.

[8]]. C. ESNosito, et al., “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,” IEEE

Cloud Computing 5.1, pp. 31-37, 2018.

[9] S. Wilkinson, "Storj: A Peer-to Peer Cloud Storage Network," , 2014.

[10] S. Wilkinson, et al.,. "Metadisk a blockchain-based decentralized file sotrage application, " Technical Report. 2014.

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system. [Online], Available:https://bitcoin.org/bitcoin.pdf, 2008.

[12] G. Wood, "Ethereum: A secure decentralised generalisedtransaction ledger," Ethereum Project Yellow Paper, 2014.

[13] Vitalik Buterin, "Ethereum: A Next-Generation SmartContract and Decentralized Application Platform," 2013 [Onlie]. Available: http://ethereum.org/ethereum.html.

[14] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security andprivacy issues of bitcoin," IEEE Communications Surveys & Tutorials,2018.

[15] 체인널리스. [Online], Available: https://www.chainalysis.com/

[16] MedicalChain Whitepaper [Online], Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

[17] The Cointelegraph, "A Brief History of Ethereum FromVitalik Buterin's Idea to Release," 2015, [Onlie]/ Available: https://cointelegraph.com/ethereum-for-beginners/a-briefhi

story-of-ethereum-from-vitalik-buterins-idea-torelease

[18] 이더리움 *GasLimit*. [Online]. Available: https://ethstats.net/

감사의 글

석사생활을 하며 수많은 사람들의 도움을 받았습니다. 그분들의 도움이 없었다면 졸업논문이 나올 수 없었을 것이기에 이 자리를 빌려 감사의 인사를 드리고자 합니다.

먼저 언제나 밤낮없이 연구실에서 그 어떤 학생보다도 더 열심히 솔선수범 연구하시던 제 지도 교수님이신 이경현 교수님께 깊은 감사의 뜻을 전합니다. 연구에 대해서 아무것도 모르던 저를 교수님께서는 연구방법뿐만 아니라 인생에 필요한 지혜와 같이 살아감에 있어 필요한 부분들까지 가르쳐주셨습니다. 잦은 실수에도 넓은 마음으로 받아주시고 연구자로서의 길을 가르쳐주신 덕분에 2년을 무탈하게 보낼 수 있었습니다. 교수님께서 제 지도교수님이 아니셨다면 졸업 논문을 작성할 수 없었고 석사 졸업을 할 수 없었을 것입니다. 정말 감사드립니다.

또한, 바쁜 시간을 내주시며 논문 심사위원을 맡아주신 신상욱 교수님과 김창수 교수님께도 감사의 말을 전하고 싶습니다.

이 외에도 연구실 사람들에게서도 많은 도움을 받았습니다. 특히 연구실의 정신적 지주이신 박영호 선배님과 서철 선배님 부족한 제 논문을 항상 피드백해주시고 세미나 시간에 많은 가르침을 주셔서 졸업논문을 쓸 때 많은 도움이 되었습니다. 그리고 연구실장인 시완 선배, 연구를 진행함에 막히는 부분을 같이 토론하며 해결하는 데 많은 조언을 받았습니다. 그로 인해 다양한 사고와 깊은 사고를 할 수 있었습니다. 하나뿐인 한국인 석사 후배인 경모야 너의 도움이 없었다면 석사생활을 견딜 수 없었을 거다 고맙다. 제 인생의 처음 사귄 외국인 친구들이자 연구실 동료인 Bayu, Akash, Sandi, Chocho 그리고 같이 졸업을 하게 되는 Bruno까지 작은 부분부터 큰 부분까지 많은 도움이 되었습니다. 감사합니다. 더하여 함께 즐거운 연구실 생활을 하게 해준 재효, 지형, 민호,

김민음 선배, 짧은 시간이나마 함께한 범창, 희수, 소연 그리고 김동이 선배와 2017학번 대학원 동기들 모두에게도 감사의 말을 전합니다.
항상 옆에서 힘이 되어주며 오랜 시간을 함께한 형들과 친구들과 동생들 여러분들이 만들어주는 긍정 에너지로 인해 한 발짝 한 발짝 끊임없이 더 나아갈 수 있었습니다.
마지막으로 언제나 변함없이 저를 믿고 지원해주시는 아버지, 어머니, 형께 감사의 인사를 드립니다. 저를 믿고 아낌없는 성원을 보내주신 그 분들이 있었기에 저는 힘든 상황에 굴하지 않고 이겨낼 수 있었습니다. 정말 고맙습니다.
이외에도 여기에 미처 적지 못한 많은 분께 감사드립니다.
이렇게 많은 분의 도움으로 저는 석사 졸업을 할 수 있었습니다. 이러한 도움이 더욱 빛나도록 앞으로도 최선을 다하겠습니다. 감사합니다.

2019년 1월 9일