

# 블록체인 네트워크를 이용한 코로나19 역학조사

## Epidemiological investigation of COVID-19 using blockchain network

### 요 약

2019년 발발한 코로나 바이러스가 세계적으로 유행하며 코로나의 확산을 사전에 방지하는 것이 국가의 최우선 과제가 되었다. 우리나라의 같은 경우, 확진자에 대한 역학조사를 통해 2차 감염을 통한 코로나의 추가 확산을 억제하고 있다. 그러나 현재 실행하고 있는 역학조사에는 두 가지 큰 문제점이 존재한다. 첫 번째로는 역학조사가 완료되는 기간이 코로나 19의 확산세를 억제하기에는 다소 길다는 점, 두 번째로는 무분별하게 수집되는 확진자와 밀접 접촉자의 개인정보를 효과적으로 관리하지 못하는 경우가 발생한다는 점이다. 본 논문에서는 Proximity tracing 기법을 사용하여 모든 접촉자들의 데이터를 블록체인의 형태로 저장하여 확진자의 개인정보를 보호하는 동시에 빠르고 정확하게 밀접 접촉자들을 가려낼 수 있는 방법을 제안한다.

### 1. 서 론

2019년 발발한 코로나 바이러스가 세계적으로 유행하며 코로나의 확산을 사전에 방지하는 것이 국가의 최우선 과제가 되었다. 우리나라는 확진자에 대한 역학조사를 통해 2차 감염을 통한 코로나의 추가 확산을 억제하고 있다.

이러한 역학조사엔 두 가지 큰 문제점이 존재한다. 첫 번째로는 역학조사의 기간이 코로나 19의 확산세를 억제하기에는 다소 길다는 점이다. 밀접 접촉자를 가려내기 위해서는 기존의 방역 시스템을 통한 정보 수집과 더불어 확진자에게서 추가적인 정보를 제공받아 확진자의 동선, 같은 장소와 시간대에 있던 사람들을 가려내야 한다. 하지만 대화만을 통해 이를 정확히 파악하는 것은 한계가 있으며 현장의 CCTV를 활용하거나 신용카드 정보를 대조, 휴대폰 기지국의 협조를 받아 정보를 확인하는 시간은 밀접 접촉자에게 접촉 사실을 고지하는데 걸리는 시간을 늦추는 결정적인 역할을 한다.

두 번째 문제점은 수집되는 확진자와 밀접 접촉자의 개인정보를 효과적으로 관리하지 못하는 경우가 발생할 수 있다는 점이다. 역학조사 과정에서 확진자의 신용카드 사용내역과 같은 거래 기록, 위치정보와 이동 경로를 토대로 개인의 취향과 사회적 관계 등 민감한 개인 정보들이 수집된다. 확진자의 개인 정보들은 조사관이 확진자와 인터뷰를 하면서 추가적인 정보가 필요하다고 판단되면 수집이 가능하다. 감염 경로 및 접촉자 파악이라는 목적에 부합한다면 문제가 되지 않지만, 이러한 개인정보의 수집은 조사관의 자의적인 판단에 맡겨져 있을 뿐, 이를 통제할 수 있는 아무런 법적 장치가 마련되어 있지 않다 [1].

본 논문에서는 기존의 역학조사는 밀접 접촉자를 가려내는 시간이 재생산수(Reproductive number)를 억제하기에는 시간이

길다는 점, 확진자의 개인정보가 무분별하게 수집되어 유출되거나 악용될 수 있다는 점을 해결하기 위해 Proximity tracing 기법을 사용하여 모든 접촉자들의 데이터들을 블록체인의 형식으로 저장하여 확진자의 개인정보를 보호하는 동시에 빠르고 정확하게 밀접 접촉자들을 가려낼 수 있는 방법을 제안한다.

본 연구는 스마트폰의 앱을 이용하여 Proximity tracing을 활용한 밀접 접촉자들의 데이터들을 수집했다. 밀접 접촉자들의 데이터들을 Bluetooth Low Energy Beacon을 통해 수집할 것이며, 스마트폰의 외부 저장소에 엑셀 파일의 형식으로 저장될 것이다. 엑셀파일에 저장된 데이터들은 블록체인 네트워크에 저장된다. 저장되는 데이터는 기기의 Device ID로 제한하였으며, 이는 Device ID가 앱의 이용자들을 식별하는 가장 쉬운 방법이기 때문이다[2].

관련된 연구로는 스마트폰을 사용하여 Proximity tracing 기법으로만 확진자를 추적하는 방법[3]과 블록체인을 주식거래 서비스, 실물 자산거래 서비스 등 금융 관련 분야와 게임 또는 콘텐츠 및 공유 분야에 적용한 연구[4], 시스템의 안전성 보장에 대한 연구가 있다 [5].

### 2. 시스템 제안

#### 2.1 시스템 요구사항

본 논문에서 제안하려는 시스템은 기존 역학조사의 문제점을 보완하고 보다 투명하고 정확한 역학조사를 수행할 수 있도록 돕는다는 목표를 가지고 있다. 보다 더 나은 역학조사와 관련한 시스템의 요구사항은 다음과 같다.

- (1) 완전성 - 각 데이터베이스에 저장된 정보들은 사실과 정확하고 완전하게 이루어져야 한다.
- (2) 무결성 - 각 디바이스가 가진 데이터베이스의 값은 모두 일치하며 그렇지 않은 데이터가 입력될 경우 값이

저장되지 않아야 한다.

- (3) 검증성 - 관리자는 참여자들이 접촉한 디바이스들을 확인할 수 있으며 어느 누구도 데이터를 조작할 수 없어야 한다.
- (4) 편리성 - 데이터베이스에 대한 쿼리를 통하여 확진자와 밀접 접촉자를 빠르고 정확하게 분류할 수 있어야 한다.

## 2.2 시스템 구현

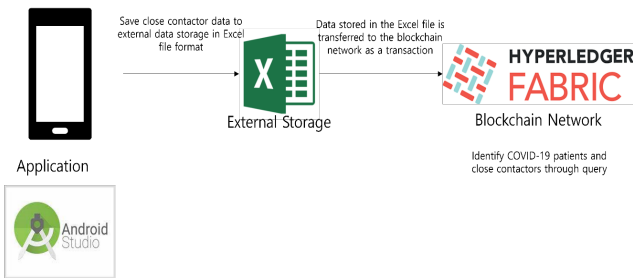


그림 1 System structure

먼저, 사용자와 접촉한 디바이스에 대한 정보들을 수집하기 위하여 블루투스 리시버, 레코더를 안드로이드 스튜디오를 사용하여 개발하였다. 디바이스는 블루투스 비콘을 만들어 전파하고, 동시에 주변 기기의 블루투스 비콘을 받아 기기 내 외부 저장소에 엑셀파일의 형식으로 저장하도록 하였다.

블록체인 네트워크는 허가형 블록체인을 사용하는 하이퍼레저 패브릭을 이용하여 구성하였다. 관리자에게 허가(인증)를 받은 사용자들만 네트워크가 구성될 수 있도록 하였으며 트랜잭션은 외부 저장소에 기록된 밀접 접촉자들의 데이터를 저장하는 것으로 설정하였다.

## 2.3 시스템 흐름도

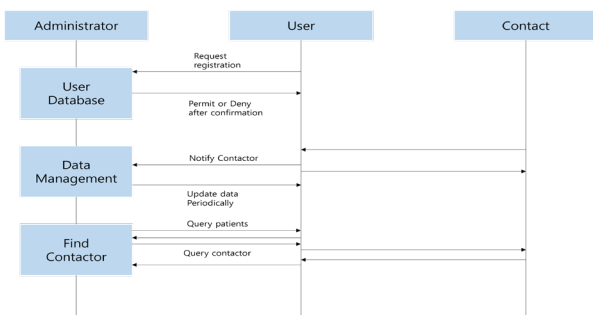


그림 2 System relationship

허가형 블록체인에서는 거래를 인증하기 위한 참여자와 거래에 참여할 참여자를 등록하고 관리하는 관리자가 필요하다. 다음은 참여자, 관리자와 시스템 간의 관계도다.

- (1) 관리자
  - 시스템을 사용할 참여자를 등록한다.
  - 일정 주기로 데이터를 업데이트하여 데이터의 무결성을 보장한다.
  - 확진자로 분류된 참여자의 밀접 접촉자를 찾아낸다.
- (2) 참여자
  - 시스템을 사용할 수 있도록 일련의 과정을 거쳐 참여자가 된다.

- 자신을 인증하고 밀접 접촉한 사람의 데이터를 블록체인 네트워크에 저장한다.

## 3. 시스템 구현

### 3.1 Bluetooth beacon

사용자가 앱을 실행하면 디바이스는 비콘을 만들어 주위로 송신하는 동시에 주위의 비콘들을 수신해 엑셀파일의 형식으로 디바이스 내에 있는 외부 저장소인 /storage/emulated/0/Android/data/com.yoo.taek.bleescann\_recorder/files에 동일한 형식으로 저장된다.

### 3.2 사용자 등록 허가

관리자는 블록체인 네트워크를 사용할 사용자를 등록한다. 사용자의 데이터는 Device ID, Device Address, 그리고 감염여부인 infected로 구성된다. 다음으로 자산인 Contactor를 등록한다. Contactor의 데이터는 앞서 등록한 사용자와 동일한 Device ID, Device Address를 가지며 자신과 접촉한 Device의 ID를 담은 ContactedUser란 문자열의 배열로 이루어져 있다.

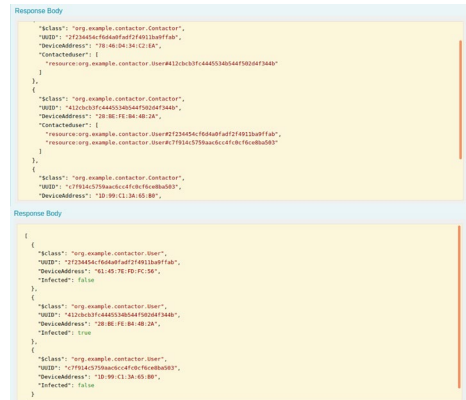


그림 3 User & Contactor

### 3.3 트랜잭션

트랜잭션은 디바이스 내 엑셀파일에 저장된 접촉자의 Device ID를 자신의 Device ID와 동일한 Device ID를 가지고 있는 자산, Contactor의 배열에 저장하도록 하였다.

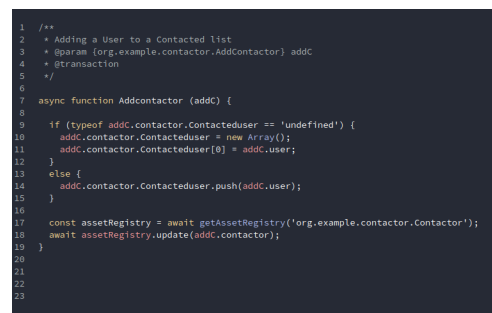


그림 4 Chaincode of transaction

### 3.4 쿼리를 통한 밀접 접촉자 추적

관리자인 역학조사관은 확진자의 Device ID를 알아낸 후, 쿼리를 통해 확진자와 접촉한 Device를 찾아낸다.

마지막으로 관리자는 블록체인에 등록된 접촉자의 데이터를 보고 코로나 19에 감염될 수 있는 밀접 접촉자에 해당하는지 판단한다. 이를 위해 관리자는 확진자의 Device ID와 접촉자의 Device ID와 관련된 transaction을 쿼리를 통해

조회한다. 조회한 transaction 중 timestamp에 적힌 시간이 확진자의 증상 발현 2일 이내라면 밀접 접촉자로 분류하고 Device ID를 서버에 있는 Device ID와 비교하여 실제 기기에 알린다.

```

1  /**
2   * New query file
3   */
4
5  query getContactor {
6    description: "find Contacted people based on UUID"
7    statement:
8      SELECT org.example.contactor.Contactor
9         WHERE (ContactedUser CONTAINS _$ContactedUser)
10  }
11
12 query getInfectedUser {
13   description: "find infected user"
14   statement:
15     SELECT org.example.contactor.User
16        WHERE (Infected == true)
17  }

```

그림 5 Chaincode of query



그림 6 Query close contactor



그림 7 Timestamp of transaction

#### 4. 결론

본 논문에서는 Proximity tracing을 통해 수집한 데이터들을 블록체인 네트워크에 저장함으로써 역학조사의 효율성을 높이고, 개인정보 유출에 대한 위험성을 줄이는 시스템을 제안하고 구현하였다.

허가형 블록체인을 사용하여 모든 데이터들은 관리자만 열람할 수 있도록 하였고, 데이터들이 각 사용자들의 디바이스에 분산 저장되어 있는 블록체인의 분산 원장을 활용하여 시스템을 구성하였기 때문에 기존 역학조사에서 보였던 개인 정보 유출의 위험성과 실용성을 보완할 수 있으리라 생각한다.

본 논문에서 활용된 데이터들은 가상의 적은 데이터들을 토대로 진행한 연구이며, 스마트폰 뿐만 아니라 모든 블루투스를 이용하는 디바이스들을 데이터로 저장하였기 때문에 실제 대규모 사용자를 등록하고 데이터베이스에 저장되는 데이터들을 적절히 필터링 할 수 있는 기술과

알고리즘을 적용하고 운용하는 것이 필요하다.

#### 참고 문헌

[1] 오병일, 코로나 19와 정보인권, <https://www.humanrights.go.kr/site/inc/file/fileDownload?fileid=10701&filename=b77ebe30cfc919257c7c0324a2f74734.pdf>

[2] 기기 ID | 정의, <https://www.adjust.com/ko/glossary/device-id/>

[3] EPFL, ETHZ, KU Leuven, TU Delft, University College London, CISPA, University of Oxford, University of Torino / ISI Foundation, Aix Marseille Univ, Universite de Toulon, CNRS, CPT, IMDEA Software Institute, INSEC TEC, Decentralized Privacy-Preserving Proximity Tracing, PEPP-PT, April 4, 2020

[4] D. Shrier, J. Larossi, D. Sharma and A. Pentland. Blockchain & Transactions, Markets and Marketplaces [Internet]. Available: [https://cdn.www.getsmarter.com/career-advice/wpcontent/uploads/2016/12/mit\\_blockchain\\_transactions\\_report.pdf](https://cdn.www.getsmarter.com/career-advice/wpcontent/uploads/2016/12/mit_blockchain_transactions_report.pdf).

[5] L. Luu, V. Narayanan, and C. Zheng, “A Secure Sharding Protocol For Open Blockchains,” In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications