2020 제주 블록체인 해커톤 서비스 설명 및 사업계획서

[Chain:A - 체인코로나]

사용플랫폼 ■으로 표시 *중복선택 가능]
■ Ground X KAS [트랙잭션해시값(Klaytn): 0xa36cb6b28924c4496d5809473ef4fbed5a1661879474d48838bee88fa0d1f138/ 어카운트 아이디(KAS): dorothy0602@gmail.com]

□ 삼성 블록체인 키스토어 SDK

□ 삼성 블록체인 플랫폼 SDK

■ 기타(직접작성: 클라이언트: Android Studio, Caver-java sdk / 서버: Node.js, SQL Lite)

가. 서비스 모델 구현 및 결과

1) 서비스 모델 개발 범위, 개발 내용 등 결과 위주 설명

(1) 클라이언트 – Android Studio / Caver / Web3.js

- ❖ 업주용: 업주가 가게 상호명과 도로명 주소를 입력하면 유저가 Transaction을 보낼 수 있는 QR코드를 생성
- ❖ 유저용: Foreground에서 1시간 단위로 위치 수집 / 위치는 로컬 DB인 Room에 저장 / 장소 방문시 QR코드를 인식, QR코드의 담긴 정보와 현재까지의 위치를 Json String으로 변환 / Caver, Web3.js로 Unsigned Transaction 생성 후 sign / signTransaction으로 배포한 Smart Contract의 InsertInformation function execute

(2) 서버 - Nodejs / Express / SQLite / KAS / AWS EC2

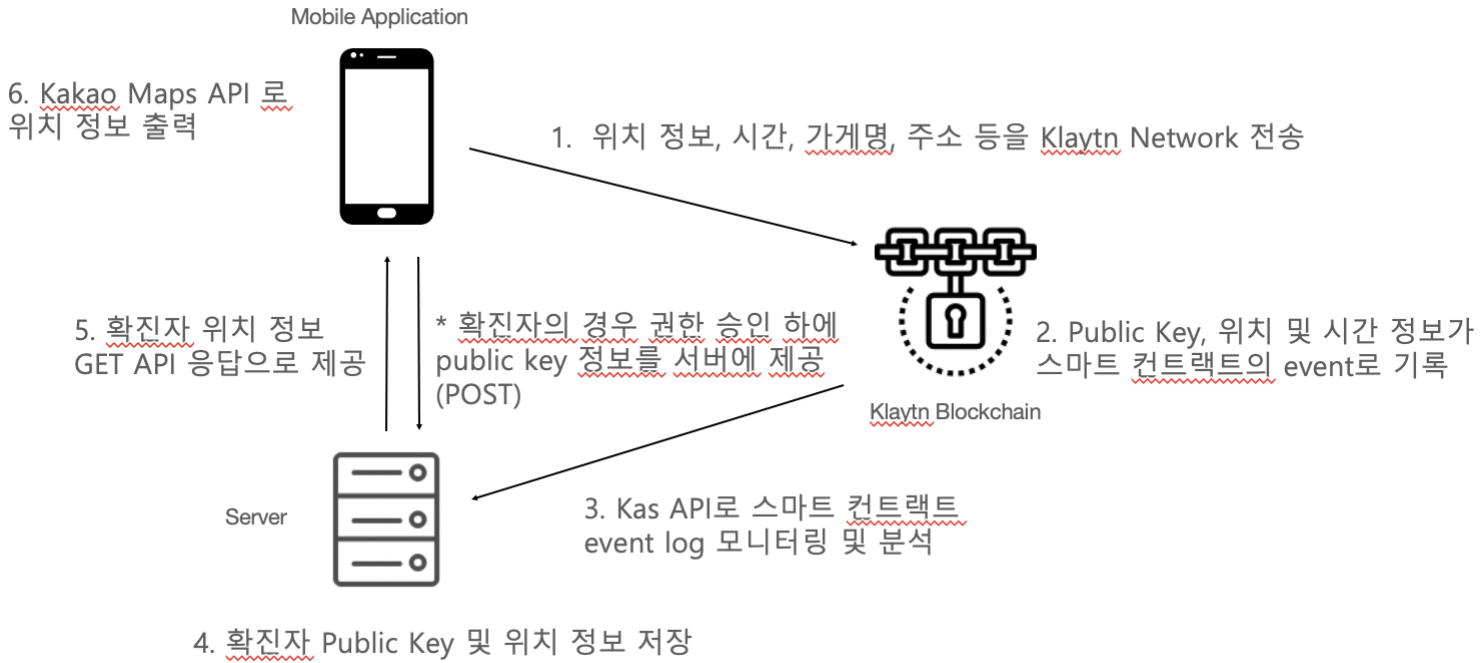
- ❖ KAS API 중 getPastEvents을 이용해서 event log(개인의 위치 및 시간 정보)를 분석/ RESTful API 구현- POST로 확진자 public key 추가 가능/ GET으로 확진자 위치 정보 쿼리 가능/ DB에 확진자 public key 및 위치 정보 저장

(3)블록체인 - Klaytn / Solidity

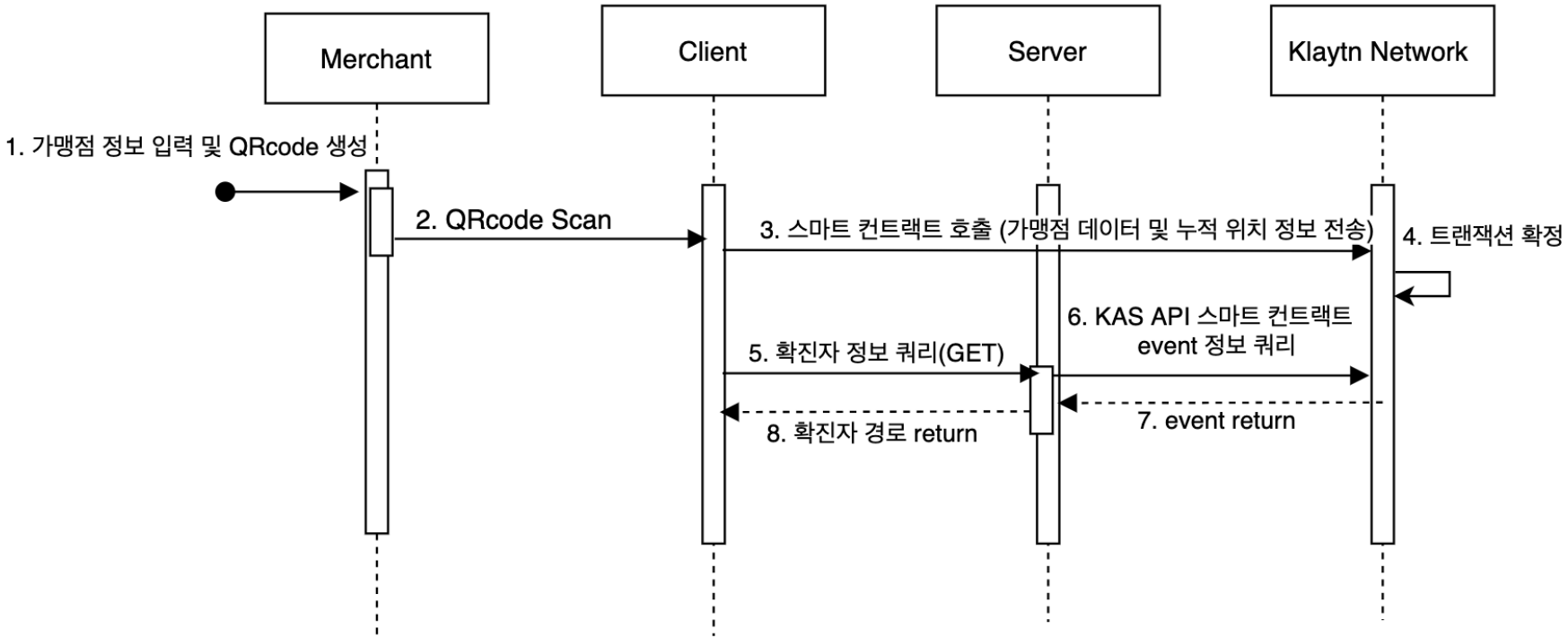
- ❖ 위치 및 시간 정보를 String으로 저장하고 있는 smart contract 을 Klaytn testnet에 배포/ 컨트랙트 내에 insert event을 emit하는 InsertInformation 메소드를 구현

가. 서비스 모델 구현 및 결과

2) 서비스 모델 시스템 구성 및 사용 시나리오 표현



Sequence Diagram



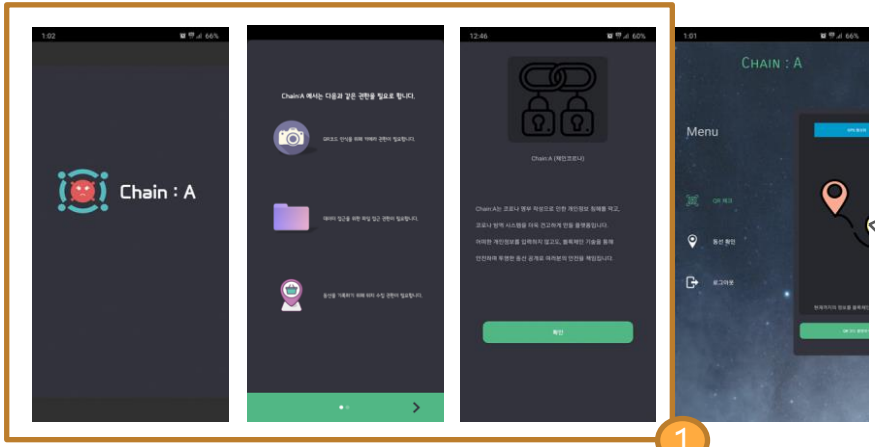
업주용 앱 시나리오 및 UI

1. 가게명을 입력한다

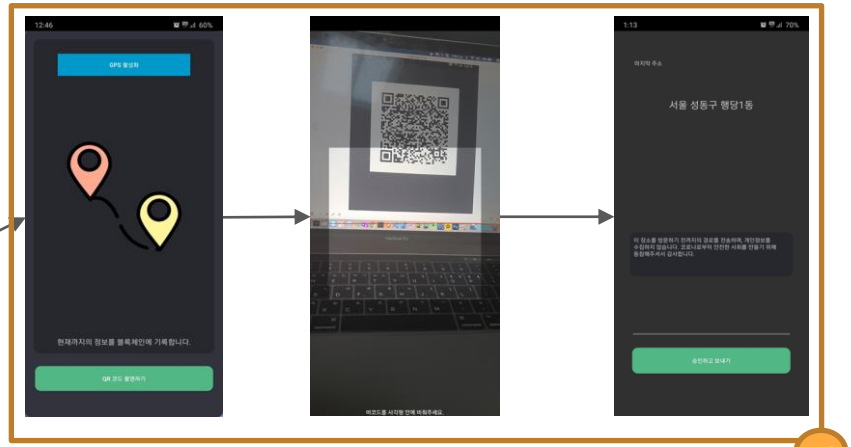
2. 도로명 주소를 검색한다.

3. QR코드 생성 버튼을 클릭 후 QR 이미지 저장이 가능하다.
가게명, 도로명, 위도, 경도에 대한 정보가 들어가있다.

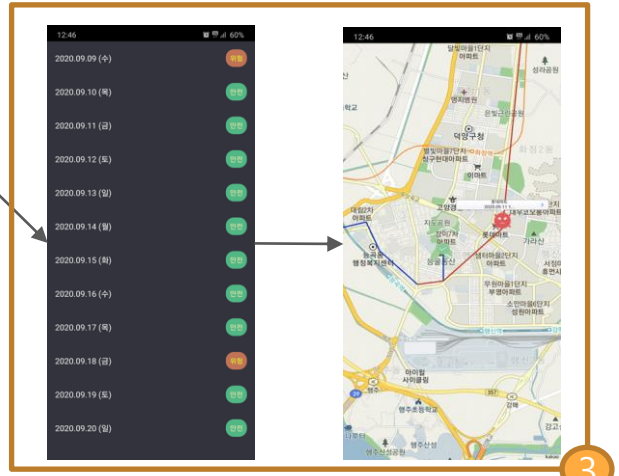
사용자 앱 시나리오 및 UI



1



2



3

1. 처음에 필요한 권한 허용을 한다 (위치, 카메라, 파일 접근)

2. 어디로 방문했는지 기록하기 위한 QR 코드 리더기 및 GPS 기록기 화면이다. 평소 내 동선을 로컬에 기록하다가 QR 코드 스캔 시 동의 하에 이동 경로에 대한 정보를 KAS 블록체인 네트워크로 보낸다. 물론 보내지는 위치 정보는 전부 익명성을 보장한다.

3. 확진자의 동선과 방문했던 곳과 비교해 겹치면 위험, 없으면 안전으로 리스트로 매일을 표시해서 보여준다. 익명성이 보장되기에 해당 확진자가 누구인지 특정할 수는 없다.

나. 핵심기술 및 주요 특징

1) 블록체인 기술이 접목되어야 하는 타당성

블록체인 기술이 접목되어야 하는 분야는 기술의 특징을 잘 녹여낼 수 있는 분야여야 하며, 그 특징으로는 데이터 투명성, 익명성, 탈중앙성이 있다. 방역 시스템에 블록체인 기술이 접목되어야 하는 이유는 현재 코로나 방역 체계의 개인정보 침해에 대한 문제의식에서 비롯되었다. 현재의 체계는 확진자 동선 공개 및 방문지 명부 작성 등을 이용해 감염 경로를 추적한다. 반면, 이름, 전화번호, 주소 등에 대한 민감한 개인정보들이 불특정 다수에게 수집되고 있고, 그 과정에서 개인정보 유출 문제가 심각하다. 그렇기 때문에, 블록체인 기술로 방역 시스템을 구축한다면, 블록체인의 신원 익명성(pseudo anonymous) 덕분에 블록체인 위에 민감한 동선 정보를 올리면서도 개인 정보를 보호할 수 있다. 동시에 블록체인의 데이터 투명성 때문에, 확진자가 자신의 Public key를 공개할 시 이 동선을 추적하여 훨씬 더 강력한 방역 시스템을 구축할 수 있다. 뿐만 아니라, 개인의 동선을 허위로 진술하는 문제를 백그라운드로 수집한 정보를 블록에 올림으로써 훨씬 정확한 동선을 수집하는 방법으로 해결 가능하며, 조작이 불가능 하기 때문에 방역 시스템에 접목된다면 그 효과가 뛰어날 것으로 예상된다. 마지막으로 탈중앙성 덕분에, 개인정보를 자신의 Device에 저장 및 블록체인에 올림으로써, 중앙 DB에 저장하지 않기 때문에, 자신외에 누구도 그 데이터가 나의 데이터임을 알 수 없어 데이터 주권을 지킬 수 있다.

나. 핵심기술 및 주요 특징

2) 서비스 모델 구현시 블록체인 기술의 장점은 극대화/단점은 최소화 모델 제시

본 모델에서는 블록체인의 익명성, 투명성, 탈중앙성(데이터 주권 개인으로 이전)과 같은 장점을 극대화 하기 위해서 다음과 같은 방법을 사용했다. 익명성의 장점을 충분히 활용하기 위해서 개인정보를 수집하지 않고 Public key로 동선을 추적하며, 확진이 된 경우에 자신의 Public key를 검증 및 공개하여 확진자의 동선을 파악한다. 투명성을 활용하기 위해 트랜잭션에 담는 데이터를 백그라운드에서 지속적으로 위치 데이터를 쌓아 QR코드를 인식했을 때 트랜잭션을 보내게 하여 동선에 대한 투명성을 보장한다. 또한 이러한 데이터는 Device내에 저장되며, 자신이 Private key로 검증해 트랜잭션을 보내야 하기 때문에 탈중앙성을 구현했다고 할 수 있다.

반면 블록체인의 단점은 낮은 tps이며, 빠르게 정보를 클라이언트에 제공해야 하기 때문에 이를 최소화 하기위해 웹서버를 구축하였다. 웹서버에서는 Klaytn API를 사용해 Klaytn Network 에 배포된 Smart Contract의 이벤트 로그를 분석하여 위치 정보를 DB에 저장 및 분석하고, 확진자의 public key가 알려졌을 때, 해당 확진자의 경로를 제공하는 REST API을 구축하였다.

나. 핵심기술 및 주요 특징

3) 기존 서비스 또는 기능 대비 블록체인 기술 적용의 차별성과 우수성 제시

기존 방역 시스템에 블록체인 기술을 적용한다면, 개인정보를 보호함과 동시에 확진자의 경로 및 접촉자 공개가 가능하다. 개인정보를 보호할 수 있는 이유는 블록체인 상의 신원정보는 pseudo-anonymous 한 성질을 가지고 있기 때문이다. 언제든 여러 개의 공개 키를 생성할 수 있고, 자신이 드러내지 않는 한 신원 정보를 감출 수 있다. 추적 가능성에 대한 우려가 있지만, 개인이 공개 키를 계속 바꾸거나, mixer등의 기술로 추적을 피할 수 있다.

또한 확진자가 선별진료소에서 확진 시 관리자에게 자신의 Public key임을 Private key로 인증, 검증하면 확진자의 Public key를 서버에서 분류하여 클라이언트에게 전달해 확진자의 동선정보를 UI상으로 알기 쉽게 제시한다. 또한 동선이 투명하기 때문에 (백그라운드에서 수집된 위치정보를 저장) 기존 시스템에 비해 투명성이 높다고 할 수 있다. 네이버 및 카카오 QRcode을 이용해서 방문자 신원 인증을 하고 방문자 명부를 수기로 작성해 감염 경로를 추적 및 관리하는 기존 시스템과 비교했을 때 블록체인을 이용하면 이전에는 불가능했던 개인 정보 보호와 방역 시스템 모두를 얻을 수 있으므로 차별점을 두고 있다.

다. 서비스 활용 방안

1) 고객 관점에서의 서비스 활용성에 대한 구체적 설명

사용자는 자신의 위치 정보를 계속해서 수집한다는 것에 대해 거부감을 느낄 수 있다. 하지만 UI를 통해 블록체인 기술을 통해 구현된 방역시스템은 수집된 위치정보에 대한 주권은 이용자에게 있으며, 이 정보를 전송한다고 하더라도 누구도 이 정보가 누구의 정보인지 알 수 없다는 점을 UI상에서 설명한다. 또한 블록체인 기술이 어렵다는 인식이 많기 때문에 어플리케이션을 이용하면서 블록체인 기술을 사용하고 있는지 인지하지 못하도록 Abstraction 과정을 거쳐 편리하게 사용할 수 있도록 UI를 구성하였다.

또한 요일별로 자신의 Device에 내장된 경로정보를 카카오 맵 API를 통해 띄워줌과 동시에 서버에서 REST API로 확진자의 동선을 보내주어 클라이언트에서 자신의 동선이 확진자의 동선과 겹쳤는지 쉽게 확인할 수 있다. 기존 코로나 맵 서비스와 다르게 자신의 동선을 저장해 이를 확진자의 동선과 비교할 수 있기 때문에 개개인이 더 조심하고 방역에 도움이 될 수 있도록 서비스를 제공한다.

다. 서비스 활용 방안

2) 향후 서비스 개발과 사업 수행 계획

서비스의 지속을 위해선 더 많은 기능을 개발함과 동시에 빠른 데이터 처리를 통해 시스템을 유지해야 한다. 데이터 처리 개선에 대해서 말하자면 Klaytn Network에 올라간 동선정보를 서버에서 데이터를 Parsing하고 분석하는 Logic을 더 개선해야 할 것이다. 기능적인 측면에서는 백그라운드로 위치정보를 계속 수집하고 있기 때문에, 확진자의 동선으로 만든 좌표들을 통해 자신의 위치가 확진자의 동선에 들어왔다는 알림을 표시하는 기능을 구현할 계획이며 이를 통해 방역 시스템에 기여할 수 있다. 또한 개인키 관리를 좀 더 쉽게 할 수 있도록 이후 Wallet 혹은 Keystore를 Integration 할 계획이다. 또한, 사용자가 수수료를 부담하는 것이 아니라, smart contract 배포자인 정부가 수수료를 지불할 수 있도록 fee delegate transaction 을 이용할 예정이다.

이 시스템이 방역 시스템에 적용된다면 세계 각국에서 한국이 방역 우수 국가로서 한번 더 인증받아 국제적 위상이 높아질 것이다. 이를 통해 많은 이용자를 가지고 있는 플랫폼에 현재 적용된 동선 기록 방식 (카카오, 네이버 QR)을 대체한다면 B2G모델로서 한국 뿐 아니라 방역 관리에 어려움을 겪고있는 국가와 비즈니스를 하는 것이 가능할 것이다.

다. 서비스 활용 방안

3) 팀 구성원 소개

팀장 서건식

담당
안드로이드 유저용,
트랜잭션 생성 및 처리

경력
* 20.02 FOUNDERS X
삼성전자 블록체인 해커톤
우수상

팀원 오시환

담당
안드로이드 업주용, 지도 개발 담당

경력
* 2017.09 ~ 2018.03
(주)Optimize TripBuddy 서버 개발
* 2019
국방부 스타트업 챌린지 육군참모총장
상 수상

팀원 고서영

담당
블록체인 스마트 컨트랙트 및 서버 개발 담당

경력
*2019.07 ~ IoTeX 블록체인 코어 프로토콜 개발자
*2020.08 IEEE BCCA 2020 paper accpeted
(EMS: An Extensible and Modular Staking
Architecture for Proof-of-Stake Systems)