블록체인기반 여행 디앱에 관한 연구

우창수*, 이재훈*, 장준호*, 권순조**, 정기현*
*경일대학교 사이버보안학과
**㈜크리에이티브마인드
ckd1105a@naver.com, ljhpop5@naver.com, pivvv88@naver.com, prena@prena.co.kr, kingjung@kiu.kr

A Study on Blockchain for Travel dApp

Chang-Soo Woo, Jae-Hoon Lee, Jun-Ho Jang, Sun-Joe Gwon, Ki-Hyun Jung

요 약

기존 여행 앱에서는 여행객들이 얻을 수 있는 기능으로 대부분 여행지에 대한 정보를 확인하고 후기를 제공받는 것이었다. 이러한 경우에 자신들이 다녀온 여행지에 관해서는 정보가 삭제될 경우 잊혀질 가능성이 높았다. 본 논문에서는 여행 앱에 데이터의 수정 및 삭제가 불가능한 블록체인 기술을 접목하여 자신들이 다녀온 여행지와 여행에 관한 정보를 소중하게 간직할 수 있도록 제공하고자 한다. 또한 여행객들에게 관리자 추천에 의한 여행 코스를 다녀올 경우 코인을 보상으로 제공하여 성취감을 이루도록 설계하고자 한다.

I. 서론

2008년에 사토시 나카모토가 비트코인 시스템을 발표하며 출발하였다. 블록체인 기술은 암호화폐뿐만 아니라, 4차 산업혁명의 한 분야로 자리잡고 있으며, 금융, 제조, 의료 등 다양한 산업 분야에서 블록체인 기술을 도입하기 위한 노력을 기울이고 있다 [1].

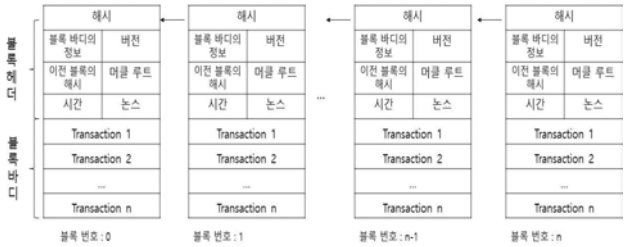
최근 블록체인 연구에서는 자격증 위조 방지를 위한 QR코드 및 디지털 워터마킹을 이용한 인증서 위조 방지 시스템에서 QR코드의 제작, 배포 과정에서 보안의 위험성을 파악하고 하이퍼레저 패브릭(Hyperledger Fabric)을 이용하여 자격증 관리 시스템을 구현하였다 [2]. 다른 연구에서는 분실물에 대한 정보를 QR코드를 통해 접근 가능하게 하며 이 QR코드를 블록체인상에 기록하여 QR코드에 대한 수정 및 삭제를 막고 이를 이용하여 분실물을 주인에게 찾아주고 분실물에 대한 정보를 토대로 소유자의 이더리움 주소를 확인하고 분실물을 되찾았을 때의 보상 금액 정보를 블록체인에 기록하여 분실물을 찾아주었을 때 보상을 지급하는 시스템 또한 연구가 이루어지고 있다 [3].

그러나, 블록체인 기술을 여행 앱에 추가한 사례는 찾아보기 힘들다. 본 논문에서는 블록체인은 데이터의 수정 및 삭제가 불가능하다는 특성을 가지고 있으며 블록체인의 코인 발행을 통하여 여행객들에게 추가 보상을 통해 특정 관광 루트를 다녀올 경우 코인 발행을 하여 루트 클리어라는 성취감도 또한 제공할 수 있을 것이다. 단순 여행을 통해 머리에서만 남는 추억을 제공하는 것이 아닌 영구적으로 기록을 남겨 데이터가 삭제나 수정되는 것을 막고 사람들에게 성취감을 제공하는 시스템을 제안하고자 한다.

II. 관련 연구

1. 블록체인

블록체인에서 블록은 크게 헤더(Header)와 바디(Body)로 구성된다. 블록 바디에는 트랜잭션이 저장되어 있고 블록 헤더에는 블록 바디에 대한 정보, 버전, 이전 블록의 해시값, 머클(Merkle) 루트, 시간, 논스(Nonce) 등이 저장되어 있다. 헤더는 이전 헤드와 해시값으로 연결되어 있으며 이러한 블록들이 연결되어 있는 구조를 블록체인이라고 일컫는다 [4].



(그림 1) 블록체인 구조.

교신저자: 정기현 (Tel. 053-600-5626)

블록에 있는 트랜잭션 값이 위/변조되면 헤더의 해시값이 바뀌게 되며 이후의 블록들이 가지고 있는 해시값을 전부 바뀌어 주어야 되므로 누군가가 임의로 데이터를 위변조할 수가 없는 것이다.

블록체인에서는 전자서명과 해시함수가 사용되는데, 이 기술들은 데이터의 위/변조를 방지하기 위한 기술이다. 블록체인은 블록에 데이터가 저장된 후에는 위/변조가 불가능한 기술이지만 저장되기 전의 데이터 위/변조는 막을 수가 없다. 블록체인은 크게 퍼블릭(Public), 프라이빗(Private)과 컨소시엄(Consortium) 블록체인으로 구분할 수 있다. 퍼블릭 블록체인은 암호화폐처럼 누구나 네트워크에 참여할 수 있고, 거래가 익명으로 이루어지며 거래 속도가 느리고 네트워크의 확장이 어렵다. 프라이빗 블록체인은 승인된 사용자만 네트워크에 참여가 가능하다. 퍼블릭 블록체인은 누구나 참여가 가능하기에 운용 규칙을 변경하기 어려운 반면에 프라이빗 블록체인은 상대적으로 쉽게 가능하며, 네트워크 참여자 통제가 가능하기 때문에 보안성에서 더 높은 성능을 보인다. 컨소시엄 블록체인은 퍼블릭과 프라이빗의 혼합형이라 볼 수 있다. 네트워크의 참여는 자유롭고 권한은 특정 참여자에게 제한한다. 권한을 부여받은 참여자의 동의에 의해서만 거래가 기록되고 보관된다.

2. 이더리움

이더리움은 기본적으로 메인넷, 테스트넷을 제공하고 있으며, 게스(Geth)와 패리티(Parity) 등을 사용하여 로컬 네트워크를 구축할 수 있다. 구축된 네트워크에서 솔리디티(Solidity) 프로그램을 활용하여 이더리움 스마트 컨트랙트(Smart Contract)를 개발하고 배포할 수 있다. 이더리움 로컬 네트워크를 구축할 경우에는 제네시스 블록을 가장 먼저 만들어야 하는데 제네시스 블록이란 블록 번호가 0이 되는 블록을 뜻하며 특정 지갑 주소에 이더리움 할당을 위해서는 제네시스 블록이 필요하다.

블럭해시	state_root
이전 블럭해시	parent hash
거래 관련 루트 해시	TRIEHASH(transaction_list) TRIEHASH(uncle_list) TRIEHASH(stact_trace)
난이도	difficulty
타임스탬프	timestamp
난스	nonce
그외 데이터	extra_data (block) number coinbase address,(채굴 주소)

(그림 2) 이더리움 블록 구조.

기본적으로 제네시스 블록 정보에는 chainId, homesteadBlock, eip155Block, eip158Block, difficulty, gasLimit, alloc, nonce, mixhash, parentHash, timestamp, coinbase, extradata 등이 있다 [5].

이더리움에서 계정(Account)을 이용할 때 개인키와 공개키를 사용하는데 트랜잭션을 발생할 때 개인키로 서명을 하게 되고, 개인키는 256비트가 무작위로 섞여 있는 값이며, 공개키는 만들어진 개인키와 타원 곡선 함수를 이용하여 만들어진다. 계정은 공개키를 SHA256과 RIPEMD160 해시함수를 차례로 이용하여 나온 결과에서 160비트만 사용한다. 스마트 컨트랙트는 1996년 컴퓨터 과학자인 닉 재보(Nick Szabo)에 의해서 처음 기술되었는데 후에 블록체인과 처음 접목하게 된 것이 이더리움이다. 스마트 컨트랙트는 조건과 상황에 따라 자동으로 계약을 수행하며 프로그램에 의하여 진행되므로 계약의 변경이나 실행의 중지를 수행할 수 없다.

최근 연구에 의하면, 스마트 컨트랙트가 발생하게 되면 블록체인 안에는 개인정보가 기록되는데 블록체인의 특성상 데이터의 위/변조가 불가능하기에 개인정보법에 관한 문제가 발생하게 되는데 이를 보완할 기능이 필요하다 [6]. 다른 연구에서는 스마트 컨트랙트를 이용하여 공유숙박 서비스의 과도한 수수료 문제와 보안상의 문제로 인해 계약 조건이 성립되어 거래가 이루어지면 일회용 QR코드를 발급하는 연구도 있다 [7]. 이러한 이더리움의 스마트 컨트랙트를 이용하여 코인 발급 기준의 신뢰성을 제공하며, 코인이 발행 되었을 때 해킹할 수 없다는 안전성, 스마트 컨트랙트를 활용하여 발급받은 코인들을 사용하고 난 이후의 문서들을 처리하며 효율성을 제공할 수 있을 것이다.

3. 여행 앱

지금부터는 현재 많이 사용하고 있는 트리플, 볼로, 대한민국구석구석 등의 여행 앱에 대해서 살펴보고 개선점을 알아보고자 한다.

트리플은 일부 지역을 선택할 수 있는데, 한 지역을 설정하게 되면 다양한 관광지들을 볼 수 있으며 입장료, 그 관광지의 정보 등을 제공한다. 자신이 일정을 선택할 수도 있는데 날짜를 입력하게 되면 사용자의 여행 스타일을 입력받고, 어플에서 추천 관광지를 보여준다. 몇 가지 관광지를 선택하게 되면 지도에서 관광지별 위치와 거리를 계산하여 사용자

에게 보여준다. 그리고 각 위치별로 길찾기 기능을 통해 간단하게 내비게이션과 연동도 가능하다.

볼로는 회원가입 후 첫 화면에서 여행지를 추천해 준다. 한국을 포함한 다양한 나라의 추천 여행지를 제공하는 특징이 있다. 볼로를 이용하여 순위가 높은 여행지를 정리하여 보여주기도 하며, 자신의 여행 후기를 볼로 책이란 것으로 작성하며 타인과 공유하는 차별화를 제공한다.

대한민국구석구석은 추천 여행지, 코스 여행지, 축제 등을 볼 수 있다. 한국 전체 지역이 표기되어 있으며, 지역별 유명한 음식이나, 음식들의 할인 정보 등 다양한 정보를 제공한다. 특정 여행 별로 안전수칙도 제공하는 특징을 가진다.

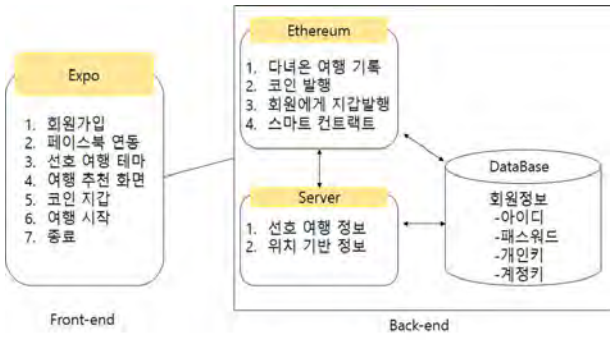
위와 같은 여행 앱은 원하는 지역을 선택한 후 여행을 가려고 하는 날짜를 지정하며 그 지역에서의 여행 테마를 정하고 그에 관련된 정보들을 사진과 함께 가격, 후기 등을 보여준다. 이를 자신의 일정에 등록하여 관광지들의 이용 가격을 총 합산하여 보여주는 식으로 구성되어 있다. 이러한 앱을 분석해 본 결과 아래와 같은 개선할 내용을 가지고 있다.

1) 여행을 다녀온 후 방문한 여행에 대한 정보는 며칠이 지난 후에 사라지게 되어 있다.
2) 특정 여행 어플을 통하여 여행을 다녀왔음에도 추가 보상은 이루어지지 않는다.

이러한 개선 내용에 대하여 블록체인의 특성을 활용하면 충분히 사용자를 만족시킬 수 있는 기능을 제공할 수 있는 디앱 개발이 가능할 것이다.

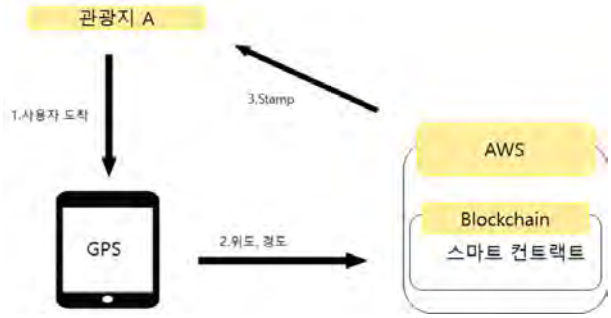
III. 블록체인 dApp 설계

이더리움 블록체인으로 로컬 네트워크를 구축하고 엑스포(Expo) 개발 툴을 사용하여 Mysql 데이터베이스관리시스템과 연동한다. 최종적으로는 그림 3과 같이 AWS 클라우드 환경을 이용하여 서비스하도록 설계하고 구축하고자 한다.



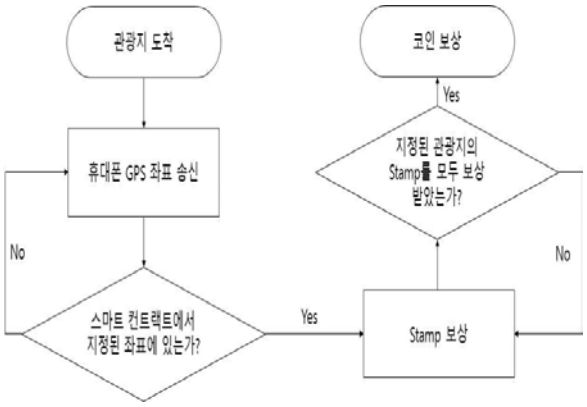
(그림 3) 시스템 구성도.

블록체인 네트워크와 스마트 컨트랙트는 그림 4와 같이 클라우드 환경에서 서비스되도록 하고 사용자의 GPS 정보를 주고받아서 위치 정보를 파악한다.



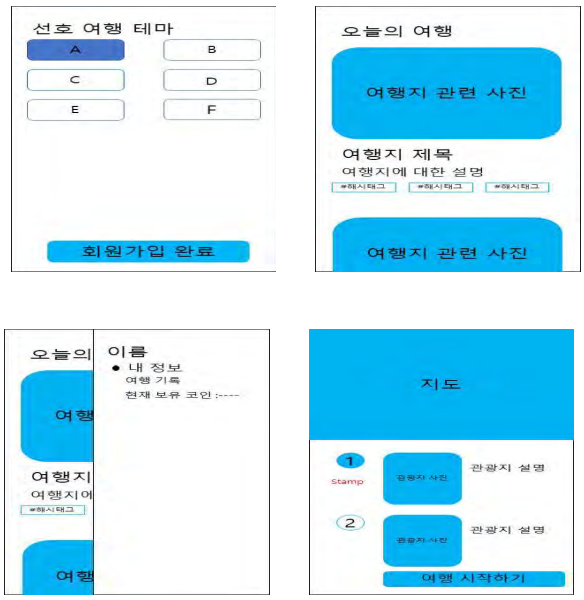
(그림 4) 블록체인에서 코인 발행 프로세스.

스마트 컨트랙트를 이용하여 코인 보상을 받기 위한 조건에는 사용자가 A라는 관광지에 도착한 후 자신의 휴대폰 GPS를 켜고 자신의 현재 위도와 경도를 서버에 전송하고, 위도와 경도가 설정해둔 값 오차 범위 안에 들어올 경우에 사용자에게 클리어 스탬프를 그림 5와 같이 발행한다. 그리고 선택한 관광지 경로를 모두 방문하여 전체 스탬프를 받았을 경우에는 사용자에게 일정 코인을 보상으로 제공한다.



(그림 5) dApp에서 코인 보상 과정.

위와 같은 사항을 고려하여 그림 6과 같이 dApp 화면을 설계하였다. 사용자가 선호하는 여행 테마를 입력받는 화면과 이를 기반으로 여행지를 추천하고, 사용자가 자신이 얼마의 코인을 가지고 있는지 확인할 수 있는 지갑을 보여주는 화면과 사용자가 여행지를 선택하고 선택된 여행지를 지도를 이용하여 화면에 위치를 알려주고 스마트 컨트랙트에서 설정된 오차 범위 내에 사용자가 있는 경우 스탬프를 보상해주는 프로세스로 진행될 수 있을 것이다.



(그림 6) dApp 화면 설계도.

위와 같이 본 논문에서는 블록체인을 활용한 여행 디앱을 설계함으로써 블록체인이 가지고 있는 데이터 조작을 불가능하게 만들고 사용자에게 코인을 보상할 지갑과 스마트 컨트랙트를 통해 코인을 보상하는 기능을 제안하였다. 블록체인을 이용한 디앱 개발을 통하여 블록체인의 특징인 투명성, 분산성, 확장성, 보안성, 안정성 등을 제공할 수 있을 것이다.

IV. 결 론

요즘은 개개인마다 자신의 여가 생활을 중요시하는 시대로 바뀌었다. 게임, 운동, 레저, 스포츠 등 많은 생활을 하며 타지에 여행을 가는 것 또한 중요한 여가 생활 중에 하나로 꼽힌다. 대부분의 여행 앱은 여행을 다녀온 후의 정보들을 잃어버릴 가능성들이 있으며, 특정 어플을 이용하게 되었을 때 수수료와 같은 것들은 전부 특정 어플들이 가져가도록 구성되어 있는 것이 일반적이다. 이와 같은 문제점을 극복하기 위해서 본 논문에서는 블록체인을 통하여 다녀온 여행지에 대한 정보를 위/변조없이 저장하며 수수료의 일부분을 디앱 사용자에게 코인으로 제공함으로써 디앱 사용자에게 보상으로 줄 수 있고, 여행을 떠나는 사람에게 특정 관광지를 다녀왔다는 의미로 스탬프를 발행함으로써 목표 달성과 보상을 동시에 제공할 수 있을 것이다. 또한 본 논문에서 설계한 여행 앱을 활성화함으로써 최종적으로는 지역 관광 발전에도 도움이 될 것으로 보인다.

감사의 글

이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업 (NRF-2018R1D1A1A09081842)과 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 해외우수신진연구자지원사업 (KRF, Korea Research Fellowship)의 연구임 (No. 2019H1D3A1A01101687).

참고문헌

[1] 유광현, “국제운송에서의 블록체인 기술 활용을 위한 개선방안”, 통상정보연구, 22(1), pp. 49-72, 2020.

[2] 배승훈, 이석훈, 정동원, “자격증 위조 방지와 빠른 진위 확인을 위한 블록체인 기반 자격증 관리 시스템 설계 및 구현”, 한국정보기술학회논문지, 18(3), pp. 67-77, 2020.

[3] 홍성호, 이상윤, 박지우, 김희열, “블록체인 기반의 분실물 보상 및 회수 모델”, 한국정보기술학회논문지, 18(4), pp. 89-99, 2020.

[4] 조성현, 이광성, 박혜리, “파이썬으로 배우는 블록체인 구조와 이론”, 위키북스, 2019 19면

[5] 김철진, “블록체인 기반의 스마트 컨트랙트 정적/동적 설계 기법”, 한국산학기술학회논문지 19(6), pp. 110119, 2018.

[6] 김용훈, “개인정보보호를 위한 스마트컨트랙트 연구”, 디지털융복합연구 17(3), pp. 215-220, 2019.

[7] 유지성, 김제인, 서승현, “스마트 컨트랙트를 활용한 공유숙박 서비스”, 정보처리학회 춘계학술발표대회 27(1), pp. 9-12, 2020.

[8] 황원용, 김효관, “Hyperledger Fabric을 활용한 블록체인 투표시스템 구현에 관한 연구”, 한국정보전자통신기술학회논문지 13(4), pp. 298-305, 2020.

[9] 박환, 김미선, 서재현, “블록체인 기반의 토큰을 이용한 IoT 다단계 인증 시스템”, 정보처리학회논문지 8(6), pp. 139-150, 2019.

[10] 이수진, 김애영, 서승환, “자동차보험용 스마트 컨트랙트를 위한 사고정보 기반 신뢰도 산정 모델”, 정보처리학회논문지 9(4), pp. 89-100, 2020.