

스마트 컨트랙트를 활용한 공유숙박 서비스

유지성*, 김제인*, 서승현*
*한양대학교 에리카 전자공학부

wtjd1014@hanyang.ac.kr, rean5123@hanyang.ac.kr, seosh77@hanyang.ac.kr

Home Sharing Service Using Smart Contract

Ji-Sung Yoo*, Jane Kim*, Seung-Hyun Seo*

*Dept. of Electronic Engineering, Hanyang University ERICA

요 약

에어비엔비와 같은 공유숙박시스템은 하루 400 만명 이상 이용하고 있는 거대한 시장이다. 일반적으로 지출해야 할 숙박비용보다 더 저렴한 가격이나 좋은 조건으로 머물 곳을 찾을 수 있다는 점에서 많은 사람들이 이용하고 있다. 그러나 호스트와 게스트에게 부담되는 과도한 수수료 문제가 존재한다. 또한 기존의 공유숙박 시스템은 호스트가 게스트에게 직접 비밀번호나 열쇠를 전달하기 때문에 보안 상의 이슈가 발생한다. 본 연구는 공유숙박시스템에 스마트 컨트랙트 기술을 도입하여 해당 이슈들을 개선, 해결하여 더 안전하고 합리적인 공유숙박시스템을 제안한다.

1. 서론

공유 숙박이란 중개시스템을 통해 주택의 빈방을 숙박용으로 제공하는 서비스이다. 호스트, 게스트 그리고 중개사이트로 구성되는 이 시스템은 호스트와 게스트가 중개사이트에 중개수수료를 지불하게 되어 있다. 현재 에어비엔비에서 호스트와 게스트가 지불하는 중개수수료는 전체 숙박비의 8%~15% 차지한다 [1]. 또한 기존의 공유숙박 플랫폼들은 호스트가 게스트에게 직접 숙소의 비밀번호나 열쇠를 전달하는 과정을 거친다. 게스트가 숙소 사용이 허락된 시간외에 숙소를 이용할 수 있다는 부분은 보안상의 문제가 발생 할 수 있다. 최근 이러한 문제들을 해결하기 위해 또다른 공유숙박 플랫폼인 wehome 은 스마트 컨트랙트 시스템을 도입하여 중개 수수료를 절감했다. 또한 보안사고를 막기 위하여 숙소 체크인 방법을 개선하고자 하는 움직임이 있다.

위의 문제를 개선하기 위하여 본 연구에서도 이더리움(Ethereum) 블록체인 플랫폼에서 스마트 컨트랙트를 사용하여 기존 플랫폼보다 적은 중개수수료로 이용할 수 있는 서비스를 제작한다. 뿐만 아니라 게스트에게 비밀번호나 열쇠 대신 체크인 할 수 있는 일회용 QR 코드를 발급하여 보다 안전한 공유숙박시스템을 제안한다. 숙박하는 기간에만 사용할 수 있는 QR 코드는 기존의 보안상의 문제를 해결 할 수 있다. 이 시스템을 통해 더 안전하고, 중개수수료가 감면된 혁신적인 공유숙박 시스템을 이용할 수 있을 것이라 기대한다.

2. 관련 연구

2.1 스마트 컨트랙트

이더리움은 최초의 블록체인 기반의 스마트 컨트랙트 플랫폼이다[2]. 스마트 컨트랙트는 코드화 시킨 조건이 만족하면 계약이 자동으로 성사되어 '이더(ETH)' 라는 암호 화폐가 사용되는 시스템이다. 이런 자동화 시스템으로 제 3의 보증기관의 도움 없이 개인 간 거래가 원활하게 이루어질 수 있다. 'Solidity'라는 프로그래밍 언어로 작성된 스마트 컨트랙트 코드는 바이트 코드로 컴파일 되고, 블록체인 네트워크에 배포된다. 블록체인 네트워크에 기록된 바이트 코드는 이더리움 가상머신(EVM) 환경에서 작동한다. 계약을 진행중인 참여자가 발생시키는 모든 트랜잭션의 데이터는 전체 노드들에 의해서 실행되고 저장되는데, 이 노드들은 전부 이더리움 가상머신 환경 속에서 존재한다. 스마트 컨트랙트는 다수의 노드에 의해 데이터들이 공유되기 때문에 특정 공격자가 계약 결과를 조작하는 것은 불가능하고, 결과적으로 무결성을 보장한다.

2.2 메타마스크

이더리움을 송금하거나 안전하게 관리할 수 있는 이더리움 암호화폐 지갑이다[3]. 메타마스크는 크롬

웹 브라우저 환경에서 작동하는 구글 확장프로그램 중 하나이다. 이더리움 디앱(Dapp)은 이더리움 노드들 위에서 동작하므로 일반적인 웹 브라우저 환경에서는 동작하지 않는다. 메타마스크를 이용하면 이더리움 노드들이 실행되고 있지 않은 웹 브라우저 환경에서도 디앱을 동작시킬 수 있다. 또한, 블록체인 네트워크 참여자들이 만드는 트랜잭션에 대한 서명을 받을 수 있는 기능을 제공한다. 본 연구에서는 메타마스크를 이용해 웹 브라우저 환경에서 블록체인 네트워크 참여자들은 계약금을 주고받는 서명을 통해 숙박 공유 스마트 컨트랙트 디앱을 동작시킨다.

2.3 가나슈

블록체인 개발 테스트에 사용되는 프라이빗 간이 블록체인이다[4]. 가나슈는 간이 블록체인이기 때문에 별도의 네트워크 연결이 필요하지 않고 로컬에서 동작하므로 스마트 컨트랙트를 쉽게 배포할 수 있다. 블록체인 개발을 위해 geth와 같은 클라이언트를 이용하면 트랜잭션이 작동하기까지 채굴하는 시간이 소요되기 때문에 개발 속도가 느리다. 가나슈는 트랜잭션이 발생할 시 자동으로 채굴하도록 만들 수 있으며, 블록이 생성되는 시점도 초 단위로 설정할 수 있다. 가나슈는 개발 테스트를 위해 테스트 전용 계정을 만들 수 있고, 해당 계정에 스마트 컨트랙트를 위한 가상의 이더를 넣을 수 있다. 계정 잔액, 블록과 트랜잭션의 로그 정보를 가나슈 사용자 인터페이스에서 확인 가능하다. 가나슈의 테스트용 계정은 메타마스크와 연동이 되어 웹 브라우저 환경에서 실제로 스마트 컨트랙트를 테스트해볼 수 있다. 본 연구에서는 가나슈를 이용하여 10개의 테스트 계좌를 만들고 각 계정에 100ETH를 세팅한다. 테스트용 계정을 이용해 숙박 공유 스마트 컨트랙트를 동작시키고, 가나슈 인터페이스를 통해서 해당 결과를 분석한다.

3. 제안하는 SQome 서비스



그림 1. 시스템 진행단계

SQome은 Smart QRcode home의 의미로 본 연구에서 제안하는 시스템 이름이다. SQome은 다음과 같이 총 3단계로 진행되고 모든 숙박 시설에는 QR코드를 통해 문을 열 수 있는 스마트 잠금 장치가 있다고 가정한다.

- 1 단계: 호스트의 숙박 등록 단계
- 2 단계: 게스트의 숙박 예약 단계

3 단계: QR 코드 확인 단계

3.1 호스트의 숙박 등록 단계

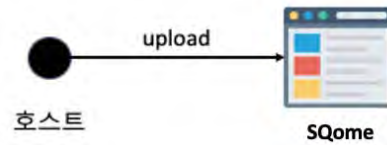


그림 2. 호스트의 숙박등록

호스트는 SQome에 숙박 정보를 게시한다. 숙박을 등록하는 트랜잭션이 발생하면 그 트랜잭션은 호스트의 비밀키로 서명한다. 트랜잭션들이 모여 블록을 생성하고, 각 노드는 해당 스마트 컨트랙트의 바이트코드를 가진다. 이후에 트랜잭션의 내용에 따라 스마트 컨트랙트를 실행하고, 다른 모든 노드가 해당 내용을 저장한다.

3.2 게스트의 숙박 예약 단계

게스트는 SQome에서 호스트가 등록한 숙박을 조회한다. SQome에서는 블록체인 네트워크에서 숙박의 상태, 즉 예약 여부를 조회하여 SQome에 표시한다. 게스트는 예약을 할 때 이름, 전화번호를 입력 후 메타마스크를 통해 계약금을 지불한다. 트랜잭션은 스마트 컨트랙트의 상태를 변경할 수 있다. 게스트가 이더를 지불함과 동시에 스마트 컨트랙트가 체결된다. 호스트는 계약이 체결됨과 동시에 이더를 제공받고 게스트는 숙박기간동안 사용할 수 있는 QR코드를 제공받는다. 예약이 완료되면 스마트 컨트랙트의 내용을 변경시키는 트랜잭션을 발생시키고 호스트가 숙박을 등록될 때와 마찬가지로 모든 노드가 바뀐 내용을 얻게 된다.



그림 3. 스마트 컨트랙트 체결

3.3 QR 코드 확인 단계

스마트 컨트랙트 체결과 동시에 SQome에서 해당 숙박은 예약완료되며 이 결과는 SQome에 표시된다. 그 후 조회를 통하여 게스트는 자신이 예약한 숙소의 상세정보와 QR코드를 확인할 수 있다. 해당 QR코드를 이용하여 숙박기간동안 체크인이 가능하다.

4. SQome 구현

본 연구에서 제안한 SQome은 크게 이더리움 블록체인 네트워크의 스마트 컨트랙트 부분과 웹 페이지 부분으로 구성되어있다. SQome의 스마트 컨트랙트 부분은 솔리디티(Solidity) 언어를 통해서 구현했다. 솔리디티는 블록체인 플랫폼에서 스마트 컨트랙트 작

성과 구현에 사용되는 계약 지향 프로그래밍 언어이다. 작성된 스마트 컨트랙트는 dApp 관리 프레임워크인 트러플을 통해 컴파일과 배포가 가능하다. 시뮬레이션을 위해 간이용 블록체인인 가나슈를 통해 테스트 계좌 10 개를 생성하고, 각 계좌에 100 이더를 설정하였다. 작성한 스마트 컨트랙트를 트러플을 통해 컴파일 후에 가나슈 네트워크에 배포하였다.

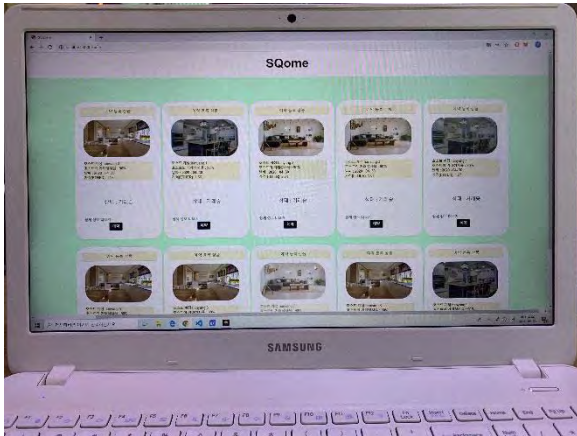


그림 4. SQome 메인 페이지

그림 4 는 실제 로컬 호스트에서 구현된 SQome 의 메인 페이지 모습이다. Node.js 의 Express 프레임워크를 이용하여 SQome 의 웹 페이지를 제작했다. 게스트는 메인 화면에서 호스트들이 등록해 놓은 거래 물품을 확인할 수 있으며, 예약 버튼을 통해 거래를 진행할 수 있다.

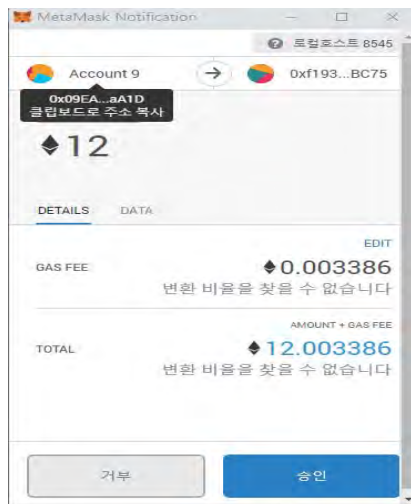


그림 5. 메타마스크를 통한 거래 과정

그림 5 는 게스트가 예약을 신청할 때 볼 수 있는 인터페이스 화면이다. 게스트는 메타마스크를 통해 거래 금액, 가스화 같은 상세 내용을 확인하고 해당 거래에 대한 서명을 할 수 있다. 게스트가 거래에 대한 승인을 마치고 호스트에게 이더를 전송하면 스마트 컨트랙트가 정상적으로 작동한다.

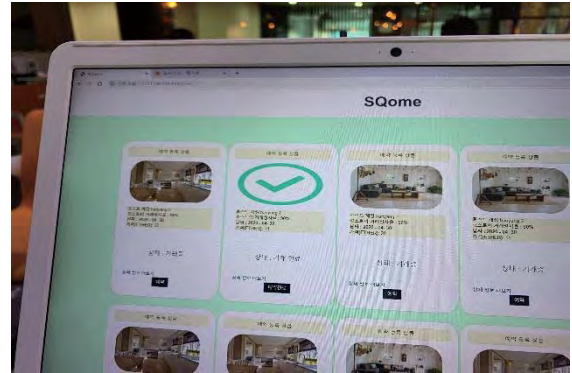


그림 6. 예약 완료된 페이지

그림 6 은 예약완료 후 결과를 확인 할 수 있는 페이지이다. 이 페이지에서 '예약 확인하기' 버튼을 통해 게스트는 예약 내역을 확인할 수 있는 페이지로 넘어갈 수 있다.

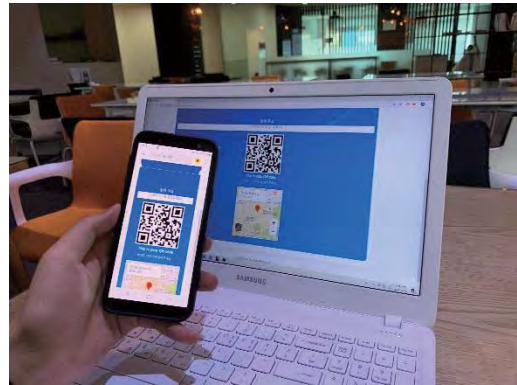


그림 7. QR 코드 확인 페이지

그림 7 은 게스트의 상세 예약 정보를 확인 할 수 있는 페이지이다. 이 페이지에서 게스트는 숙박 기간에 사용할 수 있는 일회용 QR 코드와 숙박하게 될 상세한 주소를 확인할 수 있다. 해당 페이지는 모바일 환경에서도 접속이 가능하며 게스트는 QR 코드를 통해 호스트의 숙소에 체크인 할 수 있다.

ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS
ACCOUNT 1	0	0	0	0	0
ACCOUNT 2	0	0	0	0	0
ACCOUNT 3	0	0	0	0	0
ACCOUNT 4	0	0	0	0	0
ACCOUNT 5	0	0	0	0	0
ACCOUNT 6	0	0	0	0	0
ACCOUNT 7	0	0	0	0	0
ACCOUNT 8	0	0	0	0	0
ACCOUNT 9	0	0	0	0	0
ACCOUNT 10	0	0	0	0	0

그림 8. 가나슈 계정 정보

그림 8 은 가나슈 툴을 이용하여 미리 생성한 10 개

의 계좌 주소와 잔액 등을 보여준다. 초기 100 이더로 세팅한 다른 계좌와 달리 구매를 진행한 9 번째 계정은 거래금액만큼 줄어든 계좌잔액을 확인할 수 있다.

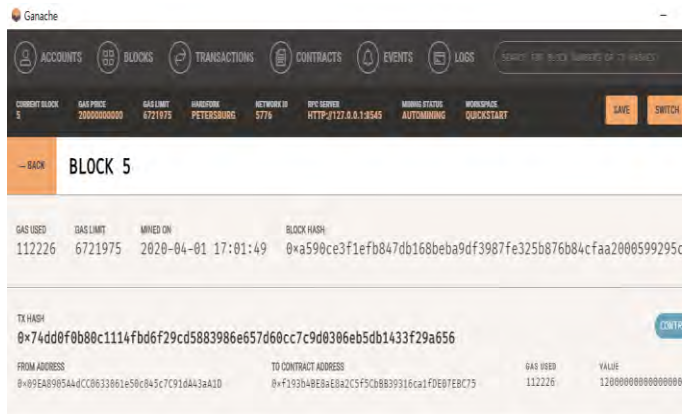


그림 9. 블록에 저장된 거래 정보

스마트 컨트랙트가 실행되면 이더리움 블록체인 네트워크에 새로운 블록을 추가하고, 해당 거래 정보를 블록에 저장한다. 그림 9 는 가나슈를 통해 앞서 진행한 스마트 컨트랙트가 체결되면서 생성된 블록 정보를 보여준다. 블록에는 거래 일시, 이더를 주고받은 계좌 주소, 거래 금액 등이 포함되어 있다.

5. 결론 및 향후 연구

기존의 공유숙박서비스는 제 3 의 보증 기관이 별도로 필요하며 추가적인 수수료가 부과되고 있다. 본 논문에서는 스마트 컨트랙트를 공유숙박 서비스에 접목함으로써 중개 기관이 필요치 않은 블록체인 활용 플랫폼을 제안하였다. 이는 블록체인 네트워크에 존재하는 전체 노드들이 네트워크 참여자들이 만드는 모든 트랜잭션을 검증하고 기록하기 때문에 가능하다. 또한 기존 공유숙박 서비스는 호스트의 개인 열쇠나 비밀번호를 게스트에게 알려주어야 하는 불필요한 과정이 필요하다. 본 논문에서 제안한 서비스는 스마트 컨트랙트의 결과로 일회용 QR 코드를 제공함으로써 이 문제를 해결하였다.

향후 연구에서는 QR 코드 뿐만 아니라 다양한 인증 수단을 스마트 컨트랙트와 연동을 시켜 접근성이 확장된 서비스 구축을 목표로 할 것이다.

참고문헌

- [1] <https://www.airbnb.co.kr>
- [2] 정효연, 임미숙, 강희조, 김윤희 "블록체인 기반 스마트 컨트랙트 기술동향", 한국정보기술학회, 2018.6, 60~62
- [3] 메타마스크, <https://metamask.io>
- [4] 가나슈, <https://github.com/trufflesuite/ganache>