# 블록체인 기반 탈중앙화된 개인간 차량 대여 시스템

김명현, 박기성*, 박요한**, 박영호

경북대학교, *한국전자통신연구원, **계명대학교

kimmyeong123@knu.ac.kr, *ks.park@etri.re.kr, **yhpark@kmu.ac.kr, parkyh@knu.ac.kr

# A Decentralized Peer-to-Peer Mobile Vehicle Rental System based on Blockchain

Kim Myeong Hyun, Park Ki Sung*, Park Yo Han**, Park Young Ho

Kyungpook National Univ., *Electronics and Telecommunications Research Institute, **Keimyung Univ.

요 약

도시 차량의 수가 증가하면서 발생하는 교통 혼잡, 환경 오염 문제를 해결하기 위해 차량 대여 서비스가 확대되고 있다. 그러나 기존의 차량 대여 시스템은 중앙화된 시스템 구조로 인해 단일 장애점에 대한 보안 위험성이 존재하며 이러한 보안 위협을 해결하기 위해 탈중앙화된 차량 대여 시스템 설계가 필요하다. 본 논문에서는 탈중앙성과 무결성을 제공하는 블록체인을 이용하여 블록체인 기반 탈중앙화된 개인간 차량 대여 시스템을 제안한다.

## Ⅰ. 서 론

차량 대여 시스템은 공유 경제 개념이 접목된 스마트 모빌리티 시스템으로 주차된 시간이 많은 유휴 차량을 효율적으로 이용하여 도시의 환경 문제와 복잡한 교통 문제를 해결할 수 있다. 최근 차량 대여 시스템에서 대여 서비스 업체는 대여 차량에 대한 유지관리 비용 부담을 줄이면서 차량을 소유한 개인은 대여 차량을 제공함으로써 수익을 얻는 개인간 차량 대여 시스템이 성장하고 있다 [1].

그러나 기존의 개인간 차량 대여 시스템은 중앙 서버에서 차량의 정보 및 서비스 사용자의 정보를 관리하고 차량 대여 서비스를 운영하고 있으며 이러한 중앙화된 시스템 구조는 트래픽 집중화 공격 등과 같은 단일 장애점에 대한 위험성이 존재한다 [2, 3]. 만약 개인간 차량 대여 시스템의 중앙 서버가 DDoS 등의 공격을 받는다면 정상적인 서비스 제공이 힘들어진다. 또한 악의적인 공격자에 의해 관리하는 데이터가 변경 및 삭제되면 서비스 문제뿐만 아니라 경제적인 피해가 발생할 수 있다 [4, 5]. 특히 차량을 이용한 사용자는 과거 기록을 통해 이용한 차량에서 분실한 물품을 찾을 수 없고 차량 제공자는 차량이 손상 및 도난될 경우 차량을 이용한 사용자의 정보를 찾기 힘든 문제 등이 발생할 수 있다. 본 논문에서는 중앙화된 개인간 차량 대여 시스템에서 발생할 수 있는 보안 취약점을 해결하기 위해 탈중앙성과 무결성을 제공하는 블록체인 기술을 이용하여 안전한 차량 대여 서비스를 제공할 수 있는 블록체인 기반 탈중앙화된 개인간 차량 대여 시스템을 제안한다.

## Ⅱ. 블록체인

블록체인은 탈중앙성, 무결성을 제공하는 분산 원장 기술이다. 블록체인에서 가장 기본적인 정보 단위인 트랜잭션들이 블록에 저장되며, 블록들은 이전 블록의 해시값을 가진 체인 구조로 이어진다 [6]. 이러한 블록체인은 참여자들이 합의를 통해 같은 블록체인을 공유한다. 만약 블록체인에 저장된 트랜잭션을 변경 및 수정하려면 해당 블록뿐만 아니라 모든 블록의 해시값도 수정해야 한다. 또한 일부 참여자의 블록체인이 수정되거나 변경되어도, 다수의 참여자들은 올바른 블록체인을 가지고 있으므로 수정된 블록체인이 유효한 블록체인으로 인정받을 수 없다. 따라서 블록체인에 저장된 정보는 위변조하기 어렵고 단일 장애점이 존재하지 않으므로 블록체인은 탈중앙성과 무결성을 보장한다.

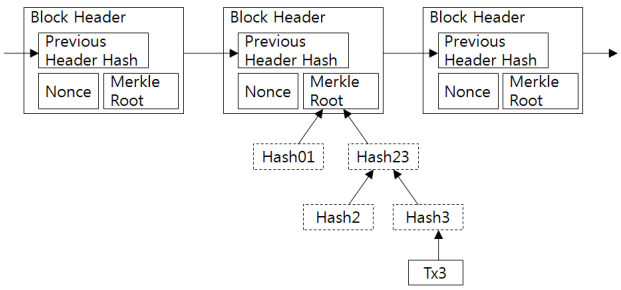


그림 1. 블록체인 구조.

## Ⅲ. 제안하는 시스템 모델

### 3.1 시스템 구성

제안하는 개인간 차량 대여 시스템 모델은 참여자들의 신원 보증을 지원하는 신뢰 기관, 대여 차량을 제공하는 차량 소유자, 차량 대여 서비스를 이용하는 서비스 사용자, 블록체인 네트워크를 구성하고 담당 구역에서 발생하는 차량 대여 서비스를 지원하는 대여 스테이션으로 구성된다. 그림 2는 블록체인 기반 탈중앙화된 개인간 차량 대여 시스템을 나타낸다. 구체적인 각 개체의 설명은 다음과 같다.

- 신뢰 기관은 시스템의 공개 파라미터를 생성하고 스테이션이 사용할

키, 차량 소유자와 서비스 사용자가 차량 대여 시스템에서 사용할 가명과 운전면허증을 확인하여 시스템에 참여할 수 있는 자격 및 신원을 보증할 수 있는 증명서를 발행한다. 또한 개인 차량 대여 서비스에서 분쟁이 발생하면 블록체인에 기록된 정보를 기반하여 악의적인 사용자의 실제 신원 정보를 추적하여 제공한다.

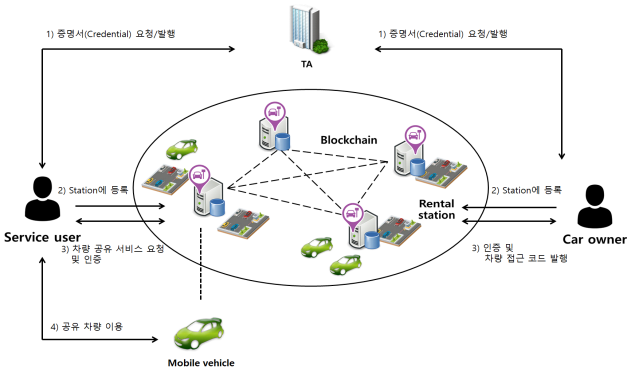


그림 2. 블록체인 기반 탈중앙화된 개인간 차량 대여 시스템 모델.

• 스테이션은 일정 구역마다 배치되어 있으며 각 스테이션은 지정된 구역 내 대여 서비스를 관리한다. 또한 스테이션들은 블록체인 네트워크를 유지하며 발생한 대여 서비스 정보들을 블록체인에 기록한다. 스테이션은 차량 소유자와 서비스 사용자 사이에서 차량 대여 서비스를 제공하는 중계자 역할을 수행한다. 스테이션은 대여 차량을 이용하려는 사용자로부터 서비스 요청을 받으면 차량 소유자에게 알림을 보내어 대여 허가 여부를 확인한다. 허가 스테이션은 차량 소유자로부터 차량을 이용할 수 있는 접속 코드를 서비스 사용자와 차량에 전송한다.

• 서비스 사용자는 자신의 모바일 단말기를 사용하여 차량 대여 서비스를 이용할 수 있다. 사용자는 스테이션에 서비스 요청 메시지를 보내면 블록체인에 기록된 정보를 기반으로 인증을 수행한다. 올바른 사용자로 인증이 되면 사용자는 스테이션으로부터 차량 소유자가 발행한 접속 코드를 받고 모바일 단말기를 이용해 대여 차량을 이용할 수 있다.

• 차량 소유자는 유휴 개인 차량을 대여함으로써 이익을 얻기 위해 차량 대여 시스템에 차량 정보를 등록한다. 스테이션으로부터 사용자의 차량 이용 요청을 받으면, 차량을 이용할 수 있는 접속 코드를 발행하여 스테이션을 통해 사용자와 차량에 전송한다.

• 차량은 외부와 통신할 수 있는 통신 모듈과 안전하게 정보를 저장할 수 있는 변조 방지(Tamper-proof) 모듈이 탑재되어 있다. 통신 모듈을 통해 가까운 스테이션으로부터 접속 코드를 수신받고 해당 코드를 사용하여 차량을 이용하려는 사용자의 접속 가능 여부를 확인한다. 차량은 수신받은 접속 코드를 차량의 변조 방지 모듈에 저장한다.

### 3.2 시스템 동작

제안한 블록체인 기반 탈중앙화된 개인간 차량 대여 시스템 모델의 동작은 다음과 같다.

1) 개인의 유휴 차량을 대여함으로써 수익을 얻기 위한 차량 소유자와 차량 대여 서비스를 이용하려는 사용자는 차량 대여 시스템에 참여하기 위해 먼저 개인 신분증 및 운전면허증을 TA에 전달하고 시스템에 참여할 자격이 있음을 증명하는 증명서를 발급받는다.

2) 차량 소유자와 대여 서비스 사용자는 스테이션에 증명서를 제출한다. 스테이션은 해당 증명서를 통해 차량 소유자와 대여 서비스 사용자의 자격을 확인하고 블록체인에 관련 정보를 저장함으로써 개인간 차량 대여 시스템 등록을 완료한다.

3) 서비스 사용자는 대여 서비스 요청 메시지를 스테이션에 전송한다. 스테이션은 서비스 사용자를 인증한 후 대여 차량의 소유자에게 알린다. 차량 소유자는 차량을 이용할 수 있는 접속 코드를 발행하여 스테이션을 통해 서비스 사용자와 차량에 전송한다.

4) 서비스 사용자는 접속 코드가 저장된 모바일 단말기를 이용하여 대여 차량을 사용한다. 이후 사용자는 대여 차량의 사용을 마칠 경우, 가까운 스테이션에 차량을 주차하고 대여 서비스 종료 메시지를 스테이션에 전송한다.

차량 대여 시스템에서 대여 서비스를 요청 과정은 무선 통신 채널을 통해 정보를 송수신하기 때문에 안전한 통신 채널을 보장하기 위한 인증 및 키 합의가 필요하다 [7]. 따라서 제안한 차량 대여 시스템의 동작 3), 4)에서 구성원들은 인증 및 키 합의를 수행하여 안전한 통신을 유지한다.

## Ⅳ. 결론

본 논문에서는 기존의 중앙화된 차량 대여 시스템에서 발생할 수 있는 보안 위협을 해결하기 위해 블록체인 기술을 접목한 탈중앙화된 개인간 차량 대여 시스템 모델을 제안하고 있다. 향후 제안한 차량 대여 시스템에서 시스템 구성원 간의 안전한 통신을 위한 인증 및 키 합의 기술을 접목시켜 안전한 블록체인 기반 탈중앙화된 개인간 차량 대여 시스템을 제안할 계획이다.

## 참 고 문 헌

[1] Guyader H. and Piscicelli L. “Business model diversification in the sharing economy: The case of GoMore,” Journal of Cleaner Production, vol. 215, pp. 1059-1069, 2019.

[2] Kim M., Yu S., Lee J., Park Y., and Park Y. “Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain,” Sensors, vol. 20, no. 10, pp. 1-21, 2020.

[3] Kim M., Park K., Yu S., Lee J., Park Y., Lee S., and Chung B. “A Secure Charging System for Electric Vehicles Based on Blockchain,” Sensors, vol. 19, no. 13, pp. 1-22, 2019.

[4] Upstream Security, “Upstream Security‘s Global Automotive Cybersecurity Report 2019,” 2019, (https://upstream.auto).

[5] Upstream Security, “Upstream Security‘s Global Automotive Cybersecurity Report 2020,” 2020, (https://upstream.auto).

[6] Son S., Lee J., Kim M., Yu S., Das A. K., and Park Y. “Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System using Bblockchain,” IEEE Access, vol. 8, pp. 192177-192191, 2020.

[7] Park Y. and Park Y. “Three-Factor User Authentication and Key Agreement Using Elliptic Curve Cryptosystem in Wireless Sensor Networks,” Sensors, vol. 16, no. 12, pp 1-17, 2016.