KIPS Trans. Comp. and Comm. Sys.
Vol.12, No.7 pp.217~226
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2023.12.7.217

Blockchain-Based Shared Electric Kickboard User Management Model

Soojin Lee† · Min-Jeong Park†† · Na-Hee Kim†† · Seung-Hyun Seo†††

ABSTRACT

As the use of shared electric kickboards is rapidly increasing, there are many cases of illegal parking of shared mobility. In order to solve this problem, local governments are taking measures such as towing illegally parked shared electric kickboards, but user management is not considered and the methods are inefficient. Accordingly, in this paper, we propose a blockchain-based shared electric kickboard user management model. The shared electric kickboard is equipped with a camera sensor and GPS that can check the parking status, and when the user ends the use of the shared electric kickboard, information on the parking status is collected through the installed sensors and the shared electric kickboard company You can check if the user has parked correctly. In addition, trust points are given according to the user's parking history and incentives are provided according to the trust points, inducing users to return the shared evangelism kickboard correctly. The information is shared through the consortium blockchain in which shared electric kickboard companies participate, enabling integrated user management of shared electric kickboard companies.

Keywords : Blockchain, Shared Electric Kickboard, Smart Contract, User Management

블록체인 기반 공유 전동킥보드 이용자 관리 모델

이 수 진† · 박 민 정†† · 김 나 희†† · 서 승 현†††

요 약

공유 전동킥보드의 사용이 급증하면서 공유 모빌리티의 불법 주차 사례가 많이 발생하고 있다. 이 문제를 해결하기 위해 지자체에서는 불법 주차된 공유 전동킥보드 견인 등의 조치를 취하고 있지만 악의적인 이용자에 대한 관리는 이루어지지 않고 있으며 비효율적인 방안이다. 이에 따라 본 논문에서는 블록체인 기반의 공유 전동킥보드 이용자 관리 모델을 제안한다. 공유 전동킥보드에는 주차 상태를 확인할 수 있는 카메라 센서, GPS 등이 탑재되어 있으며 이용자가 공유 전동킥보드 이용을 종료를 하게 되면 반납 시 주차 상태에 대한 정보를 탑재된 센서들을 통해 수집하여 공유 전동킥보드 회사가 이용자가 올바르게 주차했는지 확인할 수 있다. 또한 이용자의 주차 내역에 따라 신뢰점수를 부여하고 신뢰점수에 따라 인센티브를 지급하여 이용자가 스스로 공유 전동킥보드를 올바르게 반납할 수 있도록 유도한다. 해당 정보들은 공유 전동킥보드 회사들이 참여하는 컨소시엄 블록체인을 통해 공유되어 공유 전동킥보드 회사들의 통합적인 이용자 관리가 가능하다.

키워드 : 블록체인, 공유 전동킥보드, 스마트 컨트랙트, 이용자 관리

1. 서 론

공유 퍼스널모빌리티는 다른 개인 또는 회사에서 대여하거나 공유하여 이용하는 1인용 이동수단을 의미하며 대표적인 예로는 공유 전동킥보드, 공유 스쿠터, 공유 전기 자전거 등이 있다. 공유 퍼스널모빌리티 서비스는 버스, 전철과 같은 교통수단을 이용할 수 없는 구간을 시간에 상관없이 편리하게 이용할 수 있는 점과, 저렴한 가격을 장점으로 하여 큰 성장세를 보이고 있다. Grand View Research에 따르면 글로벌 퍼스널 모빌리티 시장의 경우 2028년까지 연평균 약 5.8% 성장할 것으로 예측된다[1]. 그 중 특히 공유 전동킥보드의 경우, 2020년 10월 기준으로 115만 명의 이용자가 공유 전동킥보드 서비스를 이용하고 있으며 1년 새 31.4%로 급성장하였다[2].

그런데 공유 전동킥보드의 사용자가 늘어나는 만큼 공유 킥보드 무단방치로 인한 문제점도 발생하고 있다. 공유 킥보드를 반납 시 차도, 지하철역 출입구, 버스 정류소 등 도로에

※ 이 논문은 2022년도 정보재원(과학기술정보통신부 여대학원생 공학연구팀제 지원사업)으로 과학기술정보통신부와 한국여성과학기술인육성재단의 지원을 받아 연구되었음.
※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2023-2018-0-01417).
※ 이 논문은 2022년 한국정보처리학회 ACK 2022의 우수논문으로 "블록체인 기반의 시민 참여형 공유 전동킥보드 관리 서비스 모델 연구"의 제목으로 발표된 논문을 확장한 것임.
† 준 회 원 : 한양대학교 전자공학과 박사과정
†† 준 회 원 : 한양대학교 ERICA 캠퍼스 전자공학부 학사과정
††† 종신회원 : 한양대학교 ERICA 캠퍼스 전자공학부 정교수
Manuscript Received : December 21, 2022
First Revision : February 6, 2023
Accepted : March 23, 2023
* Corresponding Author : Seung-Hyun Seo(seosh77@hanyang.ac.kr)

무단 방치하여 차량과 시민의 통행에 불편함을 줄 수 있다. 특히 일반인들보다 교통약자들 사이에서 그 피해가 더 크다. 시각장애인의 경우, 공유 킥보드의 부피가 작아 지팡이에 걸리지 않기 때문에 부상을 당할 위험이 크다. 또한 휠체어를 이용하는 사람의 경우, 무단 주차되어 있는 킥보드가 있을 시 부피가 큰 휠체어가 지나다닐 수 없어 이동에 어려움이 있다.

이러한 문제를 해결하기 위해 지자체에서는 공유 킥보드에 대한 규제를 강화하고 있다. 서울시의 경우, 서비스사업자에게 킥보드 반납 제한 구역을 두어 지하철 출입구와 같은 특정한 장소에 전동킥보드를 주차 반납할 경우, 견인업체를 불러 전동킥보드를 수거하도록 한다[3]. 그러나 지자체에서 도시 전 범위에 위치한 공유 전동킥보드를 모니터링하는 것은 비용과 시간적인 측면에서 비효율적이다. 또한 전동킥보드의 견인 금액은 공유 모빌리티 회사에서 부담하기 때문에 공유 모빌리티 회사에서는 직접 공유 전동킥보드 상태를 확인하고 타 견인 업체가 수거하기 전에 직접 관리하기를 원한다. 상습적으로 공유 전동킥보드를 방치 및 불법 주차하는 이용자는 그의 악의적인 행위로 특정 공유 전동킥보드 회사에서 서비스가 제한되어도 그 정보가 다른 공유 전동킥보드 회사와 공유되지 않는다. 그렇기 때문에 여전히 악의적인 이용자는 다른 공유 전동킥보드 서비스를 이용할 수 있다. Carrese[4]는 공유 전동킥보드의 주차 문제를 해결하기 위해 드론을 이용하여 공유 전동킥보드의 주차 상태를 확인하는 모델을 제안하였다. 그러나 [4] 역시 공유 전동킥보드 회사들 간의 이용자 정보가 공유되지 않는다는 문제가 있다. 그러므로 효과적인 공유 전동킥보드 및 이용자 관리를 위해서는 공유 전동킥보드 회사들이 이용자 정보를 공유할 수 있는 방안이 필요하다. 또한 본질적인 불법 주차 문제를 해결하기 위해서는 이용자가 스스로 사용한 전동킥보드를 올바르게 주차와 반납을 하도록 유도하는 서비스 모델이 요구된다.

효과적인 공유 전동킥보드 관리를 위해 본 논문에서는 블록체인 기반 공유 전동킥보드 이용자 관리 모델을 제안한다. 블록체인은 다수의 참여자들이 제3의 신뢰되는 기관 없이 공동의 원장을 유지하고 공유하는 기술로 투명성, 데이터 무결성의 특징을 갖는다. 제안 모델에서는 공유 전동킥보드 회사들은 컨소시엄 블록체인을 이루어 전동킥보드 이용자의 신뢰점수를 공유한다. 이때 공유되는 정보들은 블록체인의 특성에 따라 위변조가 불가능하다. 이용자가 전동킥보드를 반납할 때, 전동킥보드에 탑재된 IoT 센서들이 주차 상태 정보를 측정하고 회사는 이를 토대로 올바른 주차 여부를 확인할 수 있다. 또한 스마트 컨트랙트 기반의 인센티브 지급을 통해 이용자가 공유 전동킥보드를 안전하고 올바르게 주차하도록 동기 부여할 수 있다. 이용자의 공유 전동킥보드 반납 내역은 이용자 관리용 스마트 컨트랙트에 기록되며 특정 임계값 이하의 신뢰점수를 갖는 이용자는 공유 전동킥보드 서비스 이용을 더 이상 하지 못하도록 한다.

본 논문은 [5]를 기반하여 구체적인 공유 전동킥보드 서비스 모델 프로세스와 스마트 컨트랙트 설계 및 성능 분석에 대해 서술한다. 본 논문의 전체 구성은 다음과 같다. 2장에서는 관련 연구로 컨소시엄 블록체인과 블록체인 기반 공유 모빌리티 모델에 대해 설명한다. 3장은 제안하는 전체 모델의 구성요소와 프로세스에 대해 서술한다. 4장은 제안 모델에서 사용하는 이용자 관리용 스마트 컨트랙트 설계에 대해 설명하며 5장은 제안한 스마트 컨트랙트 및 제안 모델에 대해 성능 분석을 한다. 6장은 향후 연구 계획에 대해 서술하며 결론을 짓는다.

2. 관련 연구

2.1 컨소시엄 블록체인

블록체인 기술은 전자서명, 해시 함수와 같은 암호 알고리즘 적용을 통해 다수의 참여자들이 중간에 신뢰되는 제3의 노드가 없음에도 안전한 데이터 공유가 가능하다. 그 중, 컨소시엄 블록체인은 공동의 목적을 가지고 있는 기관, 단체들이 블록체인에 노드로 참여하는 허가 형 블록체인이다. 기존 비트코인과 같은 공개형 블록체인은 블록을 채굴하는 데 시간이 걸려 트랜잭션 처리 속도가 느리지만 컨소시엄 블록체인은 참여 노드가 한정적이기 때문에 트랜잭션 처리 속도가 빠른 PBFT(Practical byzantine fault tolerance)[6]를 합의 알고리즘으로 적용할 수 있어서 빠른 블록생성이 가능하다. 또한 허가된 기관만 노드로 참여하기 때문에 관련이 없는 다른 노드와는 블록체인의 원장 정보를 공개하지 않고 관리할 수 있다. 이러한 컨소시엄 블록체인의 특성을 활용하여 최근 은행, 스마트 그리드, 스마트 시티 등의 분야에서 컨소시엄 블록체인 기반 모델을 제안하였다[7].

본 논문에서는 공유 전동킥보드 회사들이 참여하는 컨소시엄 블록체인을 제안하여 공유 전동킥보드 회사들이 이용자의 신뢰점수, 악의적인 이용자의 정보를 공유할 수 있도록 한다. 이를 통해 통합적인 고객 관리와 악의적인 이용자의 행위 제한이 가능하다.

2.2 블록체인 기반 공유 모빌리티 시스템

최근 공유 모빌리티 서비스에 블록체인을 적용한 연구들이 있다[7-9]. Wang[8]은 컨소시엄 블록체인을 적용한 차량 운전자와 탑승객 간 차량 공유 매칭 서비스를 제안하였다. 프록시 재암호화(proxy re-encryption) 기법을 적용하여 RSU (Roadside-unit)가 중간에서 운전자와 탑승객을 연결하며 운전자와 탑승객이 서로를 평가하여 안전한 차량 공유가 가능하도록 했다. Baza[9]는 프라이버시를 고려한 블록체인 기반이 차량 공유 및 결제 시스템을 제안하였다. Zero-

knowledge set membership proof(ZKSM)을 적용하여 블록체인 상에서 사용자의 픽업 위치가 드러나지 않도록 하였다. Pirker[10]는 대체 불가한 토큰인 ERC-721 토큰을 공유 모빌리티 플랫폼에 적용하여 차량에 대한 ERC-721 토큰을 발급하고 이를 통해 차량의 소유권을 변경함으로써 차량을 공유하는 방안을 제안하였다. [8,9]들은 주로 개인과 개인 간의 모빌리티 공유 서비스를 중점으로 모델을 설계하였다. [10]은 상업적 차량에 대한 공유도 고려하였으나 공유 차량을 어떻게 관리할지에 대한 방안은 제안하지 않았으며 공유 전동킥보드 서비스가 특수하게 가지는 불법 주차 문제에 대한 연구는 수행되지 않았다. Carrese[4]는 공유 전동킥보드 서비스에서 불법 주차 문제를 해결하기 위해 각 공유 전동킥보드 회사들이 주차 상태를 확인하기 위해 드론을 이용하는 방안을 제시하였다. [4]는 불법 주차된 공유 전동킥보드 상태를 효과적으로 확인할 수 있으나 각 회사들이 드론을 소유하고 컨트롤해야 한다는 한계가 있으며 드론은 보안상 취약하기 때문에 제안 모델은 실효성이 없다. 추가적으로 특정 회사의 서비스를 이용하던 악의적인 이용자가 잘못된 주차를 할 했을 때, 그 정보가 다른 공유 전동킥보드 회사와 공유되지 않기 때문에 악의적인 이용자가 다른 서비스를 이용하면서 지속적으로 불법 주차를 할 수 있다는 문제가 있다. 이를 보안하기 위해 제안 논문에서는 전동킥보드가 주차할 때마다 전동킥보드에 탑재된 센서를 통해 주변 정보를 수집하여 공유 전동킥보드 회사들이 주차 상태를 확인할 수 있도록 한다. 또한 컨소시엄 블록체인을 통해 전체적인 이용자의 전동 킥보드 반납 행위에 대한 평가를 다른 공유 전동킥보드 회사들이 공유할 수 있도록 하여 효과적인 이용자 관리가 가능하다.

3. 제안 시스템

3.1 전체 모델

제안하는 블록체인 기반 공유 전동킥보드 이용자 관리 모델에는 공유 전동킥보드 회사, 공유 전동킥보드 이용자, 그리고 이용자 등록기관(Registration authority: RA)이 참여한다. 전체 모델의 그림은 Fig. 1에서 보인다. 공유 전동킥보드 회사들은 자신이 소유하고 있는 전동킥보드의 대여 서비스를 제공하는 주체이다. 회사들은 컨소시엄 블록체인의 노드가 되어, 전체 블록체인 원장을 유지하고 기록한다. 전동킥보드 회사들은 블록체인을 통해 사용자의 공유 전동킥보드 서비스 이용 내역과 신뢰점수를 공유한다.

제안 모델에서는 이름, 주소 등의 이용자 개인정보가 공유 전동킥보드 회사들 사이에서 무분별하게 공유되는 것을 방지하기 위해 분산ID 신원 모델[12]을 적용한다. 이용자 등록기관은 공유 전동킥보드를 사용하고자 하는 이용자의 계정을 분산ID(분산 식별자)로 발급해주는 역할을 한다. 공유 전동킥

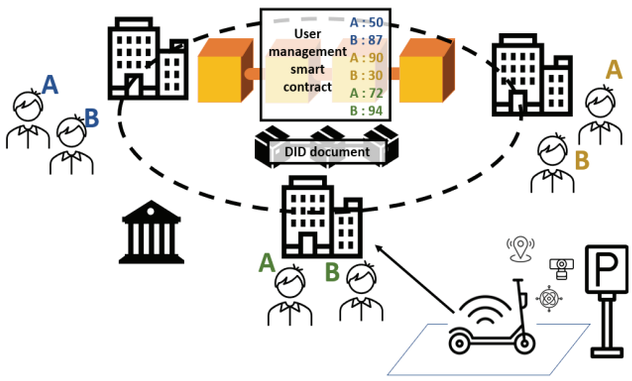

Fig. 1. Overall Model

보드 이용자는 공유 전동킥보드 회사의 서비스를 이용하기 위해 이용자 등록기관을 통해 분산ID를 발급해야 한다. 사용자 신원은 사용자의 분산ID로 식별되며 분산ID 소유권 검증을 위한 DID document를 관리하기 위해 공유 전동킥보드 회사들은 별도의 이용자 신원관리 블록체인을 추가로 운영한다고 가정한다. 공유 전동킥보드에는 기울기 센서, 카메라 센서, GPS(Global positioning system 센서와 같은 IoT 센서들이 탐재되어 있다. 이용자가 사용한 공유 전동킥보드를 반납할 때, 전동킥보드에 부착된 센서들을 현제 전동킥보드의 주차 상태 정보를 수집하여 공유 전동킥보드 회사에 전송한다. 회사는 이를 기반하여 공유 전동킥보드의 주차 상태를 파악하고 결과에 따라 사용자의 신뢰점수를 업데이트한다. 본 논문에서 전동킥보드는 공유 전동킥보드 회사와 통신이 가능하고, 회사를 통해 블록체인 정보를 읽거나 트랜잭션을 생성하여 회사 서버에 전달할 수 있다고 가정한다. 제안 모델은 공유 전동킥보드 회사들이 참여하는 컨소시엄 블록체인을 적용하지만 이용자들도 요청 시, 블록체인 원장 정보를 읽을 수 있다.

블록체인에는 이용자 관리용 스마트 컨트랙트가 사전에 배포되어 있다. 이용자 관리용 스마트 컨트랙트에는 공유 전동킥보드 이용자의 신뢰점수와 인센티브 잔액이 기록된다. 이용자 관리용 스마트 컨트랙트를 통해 공유 전동킥보드 회사들은 이용자의 신뢰점수 및 인센티브를 통합적으로 관리할 수 있다. 신뢰점수가 임계값 이하인 이용자는 악의적인 고객으로 분류되어 서비스를 이용을 제한받게 된다. 반대로 높은 신뢰점수를 갖는 사용자는 인센티브를 받게 되며 해당 인센티브는 요금 할인, 추가 시간 제공 등의 해택을 받는데 사용될 수 있다.

3.2 공유 전동킥보드 이용자 신뢰점수 산정

공유 전동킥보드 이용자의 신뢰점수는 이용자가 전동킥보드를 이용한 후 반납할 때 올바르게 주차했는지 여부에 따라 결정된다. Table 1은 공유 전동킥보드 주차 상태를 평가하기

Table 1. Parking Condition Factors

No.	Factor	Related Sensors
1	No parking zone parking	GPS, Camera
2	Inclination of a electric kick board	Tilt sensor
3	Gait disturbance	Camera
4	Damage of a electric kick board	Camera(User)

위한 요소와 그 요소 값을 결정하기 위해 활용 가능한 센서의 예를 보인다. 각 요소 별 전동킥보드 상태에 따라 점수를 부여한다. 각 요소에서 전동킥보드의 센서들을 통해 수집된 값이 올바르게 주차된 상태에 해당되면 1점을 부여하고 그렇지 않으면 0점을 부여한다. 첫 번째 요소는 주차 금지구역에 전동킥보드를 주차했는지 여부에 대한 것으로 GPS 값을 통해 판단할 수 있다. 여기서 주차 금지구역은 서울시에서 발표한 즉시견인구역인 차도 및 자전거차도, 버스 정류장 전면 5m, 지하철역 출구 전면 5m, 점자블럭 및 교통섬 위 등이 해당된다[3]. 반납 시점에서 공유 전동킥보드 GPS 값이 주차 금지구역 범위 내에 있을 경우, 주차가 올바르게 되지 않은 것으로 판단한다. 또한 지하 주차장에 전동킥보드를 주차하여 반납하는 경우, GPS 추적이 불가능하여 전동킥보드 회사가 킥보드의 위치를 파악하기 어렵다. 이 경우, 전동킥보드의 카메라 센서를 통해 주차 상태를 파악할 수 있다. 이용자가 전동킥보드 주차구역에 주차했는지 확인할 수 있도록 주차 구역에 관련 표지판을 두어 전동킥보드 카메라가 표지판 촬영할 수 있도록 한다. 회서 서버는 머신러닝 기반 객체 탐지 모델을 적용하여 주차상태를 판단한다. 이용자가 전동킥보드를 지하 주차장 내 정해진 전동킥보드 주차구역에 주차한 경우에는 올바르게 주차했다고 볼 수 있으니 그렇지 않은 경우, 해당 요소에서 점수를 받을 수 없다. 두 번째 요소는 주차된 전동킥보드의 기울기로 전동킥보드가 똑바로 세워있지 않고 쓰러져 있다면 보행 및 주행에 방해가 되기 때문에 전동킥보드의 기울기도 평가 요소가 될 수 있다. [13]을 참고하여 틸트 센서와 같은 기울기 센서를 전동킥보드에 부착하여 기울기 센서 값이 90° 이상으로 클 경우, 회사 서버는 해당 전동킥보드를 잘못된 주차 상태로 판단한다. 세 번째 요소는 보행 방해 여부에 대한 것으로 주차금지지역이 아니더라도 주택 입구 앞, 좁은 골목 등에서 사람들의 보행에 방해가 되도록 주차가 될 경우, 해당 요소에서 낮은 값을 부여한다. 이는 공유 전동킥보드에 부착된 카메라 센서로 판단 가능하다. 예를 들어, 머신러닝 기반 분류 모델을 통해 공유 전동키보드가 도보 한가운데에 있는지 또는 도보 사이드에 있는지 여부를 판단할 수 있다. 마지막 요소는 전동킥보드의 훼손 여부이다. 공유 전동킥보드는 다수가 사용하기 때문에, 대여 중, 전동킥보드가 훼손이 될 경우, 훼손한 이용자를 추적하기 어렵다. 따라서 이용자가 전동킥보드 사용을 마친 후, 공유 모빌리티 회사에서 제공하는 모바일 어플리케이션을 통해 현 전동킥보드 상태를 사진으로 찍어 회사에 전송함으로서 이용자가 공유 전동킥보드를 훼손 없이 이용했는지 확인할 수 있다. 전동킥보드 훼손의 종류가 많고 그 범위가 다르기 때문에 이는 사람이 직접 육안으로 확인한다고 가정한다.

Table 1의 각 요소들에 대한 평가 값을 순서대로 α_1, α_2, α_3, α_4, 라고 한다면 전체 주차 상태 평가 점수 E는 아래 Equation (1)과 같다. 이때 x,y,w, 그리고 z는 각 요소들 값의 가중치이며 $x+y+w+z=1$을 만족한다. 이때 스마트 컨트랙트를 작성할 때 사용하는 언어인 솔리디티에서는 소수점자리 아래 수를 지원하지 않기 때문에 100을 곱하여 E의 범위가 0이상 100이하가 되도록 설정한다.

$$E=(x\alpha_1+y\alpha_2+w\alpha_3+z\alpha_4)\times 100 \tag{1}$$

제안 모델에서는 공유 전동킥보드 회사가 이용자 관리용 스마트 컨트랙트에 각 요소들의 값을 임력하고 스마트 컨트랙트 내에서 주차 상태 평가 점수가 계산된다. 이용자의 신뢰점수 T는 현재 주차 상태 평가 점수와 이전에 누적된 평가 점수에 더해진 값으로 Equation (2)에 따라 계산된다. 여기서 β는 기존 신뢰점수 반영 비율이고 T^{-1}는 신뢰점수를 업데이트하기 직전 이용자의 신뢰점수이다.

$$T=\frac{\beta T^{-1}+E}{\beta+1} \tag{2}$$

3.3 블록체인 기반 공유 전동킥보드 이용자 관리 모델

Fig. 2는 제안하는 블록체인 기반 공유 전동킥보드 이용자 관리 모델의 전체 프로세스를 보인다. 구체적인 모델의 각 단계는 다음과 같다.

1) 이용자 등록

제안 모델에 참여하고자 하는 이용자 U_i는 임의의 비밀값 $sk_i \in Z_q^*$를 선택한다. 여기서 q는 소수이다 이용자 U_i는 $pk_i = sk_iP$를 계산하여 공개키-개인키 쌍 (pk_i, sk_i).를 생성한다. 이때 P는 덧셈 순환군 G_q의 생성자이다. U_i는 자신의 공개키 pk_i와 운전면허증을 이용자 등록기관에 전송한다. 이용자 등록기관은 이용자 U_i가 이전에 이미 등록된 이용자가

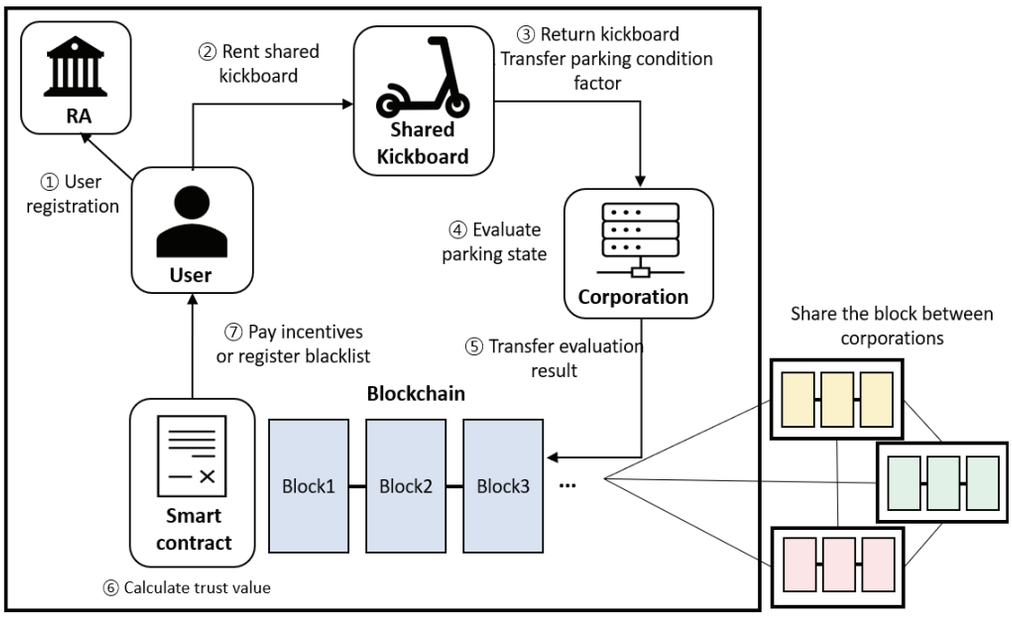

Fig. 2. Overall Process

아닌지 확인한 후, pk_i 정보가 포함된 DID document를 생성하고 이를 이용자 신원관리 블록체인에 등록한다. 이용자 등록기관은 U_i의 DID document의 위치를 나타내는 분산 ID(분산 식별자)를 U_i에게 전달한다. U_i는 발급된 분산ID를 통해 회사에 제공하는 모바일 어플리케이션에 로그인을 할 수 있다.

2) 공유 전동킥보드 대여

이용자 U_i는 도로에 있는 공유 전동킥보드를 이용하기 위해 공유 전동킥보드 회사의 모바일 어플리케이션에 로그인을 한다. 이때 결제수단은 어플리케이션에 사전에 등록되어 있다고 가정한다. U_i는 사용하려는 공유 전동킥보드의 QR 코드를 스캔하여 전동킥보드의 잠금을 해제한 뒤, 전동킥보드를 사용한다.

3) 공유 전동킥보드 반납

공유 전동킥보드 사용을 마친 이용자 U_i는 전동킥보드를 주차한 후, 모바일 어플리케이션을 통해 사용 완료 처리를 한다. 이때 전동킥보드는 킥보드에 부착된 카메라, 기울기 센서, GPS 센서들을 통해 주변 정보를 수집한다. 수집된 정보는 공유 전동킥보드 회사 서버로 전송된다.

4) 주차 상태 평가 및 이용자 신뢰점수 업데이트

회사 서버는 공유 전동킥보드가 전송한 데이터를 토대로 Table 1에서 정의한 각 주차 상태 평가 요소를 평가한다. 회사 서버는 각 요소별로 올바른 주차 상태에 부합할 경우는 1, 그렇지 않을 경우 0을 부여한다. 각 공유 전동킥보드 회사는 하루 동안 서비스를 이용한 이용자들의 요소별 평가 값들을 모아서 이용자 관리용 스마트 컨트랙트에 트랜잭션으로 전송한다. 공유 전동킥보드 회사는 각 요소별 평가 값을 이용자 관리용 스마트 컨트랙트에 트랜잭션으로 전송한다. 이때 전송하는 트랜잭션의 구조는 아래 Fig. 3과 같다. 여기서 논스(Nonce)는 메시지 재사용 방지를 위한 일련번호, 가스 가격(Gas price)는 1 가스당 지불해야하는 이더 금액, 가스 한도(Gas limit)는 해당 트랜잭션에서 사용가능한 가스의 최댓값이다. 컨트랙트 주소(Contract address)와 함수 선택자(Function selector)는 각각 실행할 이용자 관리용 컨트랙트 주소와 신뢰점수 계산을 위해 호출할 함수를 의미한다. Fig. 3에서 $\alpha_1^i, \alpha_2^i, \alpha_3^i$, 와 α_4^i는 U_i의 요소별 평가 값을 의미한다. 이용자 관리용 스마트 컨트랙트는 입력된 데이터를 이용하여 Equation (1)과 Equation (2)에 따라 U_i의 신뢰점수를 계산하고 업데이트한다. 이때 x, y, w, 그리고 z는 스마트 컨트랙트 배포 때, 공유 전동킥보드 회사에 의해 값이 사전에 설정된다. 업데이트 된 신뢰점수는 블록체인에 참여하는 모든 공유 전동킥보드 회사들이 확인할 수 있다.

5) 인센티브 지급 및 블랙리스트 등록

이용자용 스마트 컨트랙트에서는 주기적으로 신뢰점수가 인센티브 지급을 위한 임계값 θ_{high}이상인 이용자에게 인센티브로 1 토큰을 지급한다. 반대로 블랙리스트 선정을 위한 임계값 θ_{low} 이하의 신뢰점수를 갖는 이용자는 스마트 컨트랙트 상에서 블랙리스트로 등록이 되며 공유 전동킥보드 서비스 이용이 일정 기간동안(일주일 또는 한달) 제한된다. 서비스 이용 제한 이후에는 블랙리스트에서 이용자 정보가 삭제되어

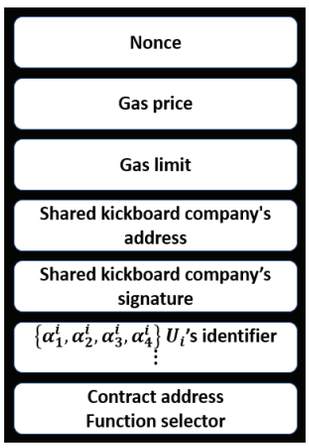

Fig. 3. Transaction Component

해당 이용자는 신뢰점수가 초기화가 되고 다시 서비스를 이용할 수 있다. 이때 인센티브 지급 및 블랙리스트 등록 단계는 정확한 신뢰점수 판단을 위해 인센티브 지급 주기 동안 인센티브를 받기 위한 이용횟수 임계값 τ 이상 공유 전동킥보드 서비스를 이용한 이용자를 대상으로 한다.

4. 공유 전동킥보드 이용자 관리를 위한 스마트 컨트랙트 설계 및 구현

4.1 이용자 관리용 스마트 컨트랙트 구성요소

이용자 관리용 스마트 컨트랙트에서 사용하는 주요 변수의 정의는 Table 2에서 보인다. 먼저 각 주차 평가 요소의 값 fact1, fact2, fact3, 그리고 fact4는 uint 형 변수로 정의하였으며 0 또는 1의 값을 갖게 된다. 이 평가 요소들을 바탕으로 주차 상태 평가 결과 값인 Evaluationresult 값이 결정된다. 변수 Trustvalue[], Balances[], Blacklist[]는 mapping 형 변수로 사용자의 식별자 정보를 키 값으로 갖으며 키의 대한 값은 각각 사용자의 신뢰점수, 인센티브 잔액, 블랙리스트 등록 여부를 기록한다. 본 논문에서 설계한 스마트 컨트랙트에서는 사용자의 계좌주소를 식별자로 사용하였다.

이용자 관리용 스마트 컨트랙트에서 사용하는 주요 함수는 Table 3에서 설명한다. setTrustvalue 함수는 처음 등록한 이용자의 신뢰점수의 초기값을 설정해주는 함수이다. 본 논문에서는 초기 신뢰점수를 50으로 한다. EvaluationParking 함수는 이용자가 반납한 공유 전동킥보드의 주차 상태 평가 값을 계산하며 변수 Evaluationresult가 이 함수의 출력 값이 된다. Trustvalueupdate 함수는 이용자의 계좌주소, 주차 상태 평가 결과 값을 입력 값으로 받아 이용자의 신뢰점수를 업데이트 한다. Incentive 함수는 인센티브를 받을 조건을 만족한 이용자에게 인센티브를 지급하는 함수이다. 그리고 AddBlacklist 함수에서는 반대로 신뢰점수가 임계값 미만인 이용자의 계좌주소를 블랙리스트에 기록한다. setTrustvalue, EvaluationParking, Trustvalueupdate, Incentive, AddBlacklist 함수는 공유 전동킥보드 회사들의 계정으로만 실행할 수 있다. 이용자는 Readtrustvalue 함수를 통해 현재 스마트 컨트랙트에 기록된 자신의 신뢰점수를 조회할 수 있다.

Table 2. Variables for a Smart Contract

No.	Variables	Description
1	fact1, fact2, fact3, fact4	The value of each parking evaluation factor
2	Trustvalue[]	A trust value of users
3	Balances[]	An incentive balance of users
4	Evaluationresult	Parking condition evaluation result
5	Blacklist[]	Blacklist of malicious users
6	UsageNum[]	The number of times each user used the service

Table 3. Functions for a Smart Contract

No.	Functions	Description
1	setTrustvalue(address user)	Initializing trust value
2	EvaluationParking(uint factor1, uint factor2, uint factor3, uint factor4, address user)	Calculating parking condition evaluation result
3	Trustvalueupdate(address user, uint Evaluationresult)	Updating Trust value
4	Incentive(address user)	Updating incentive balances
5	AddBlacklist(address user)	Adding a user's address to the blacklist
6	Readtrustvalue[address msg.sender]	Readding the trust value of user(msg.sender)

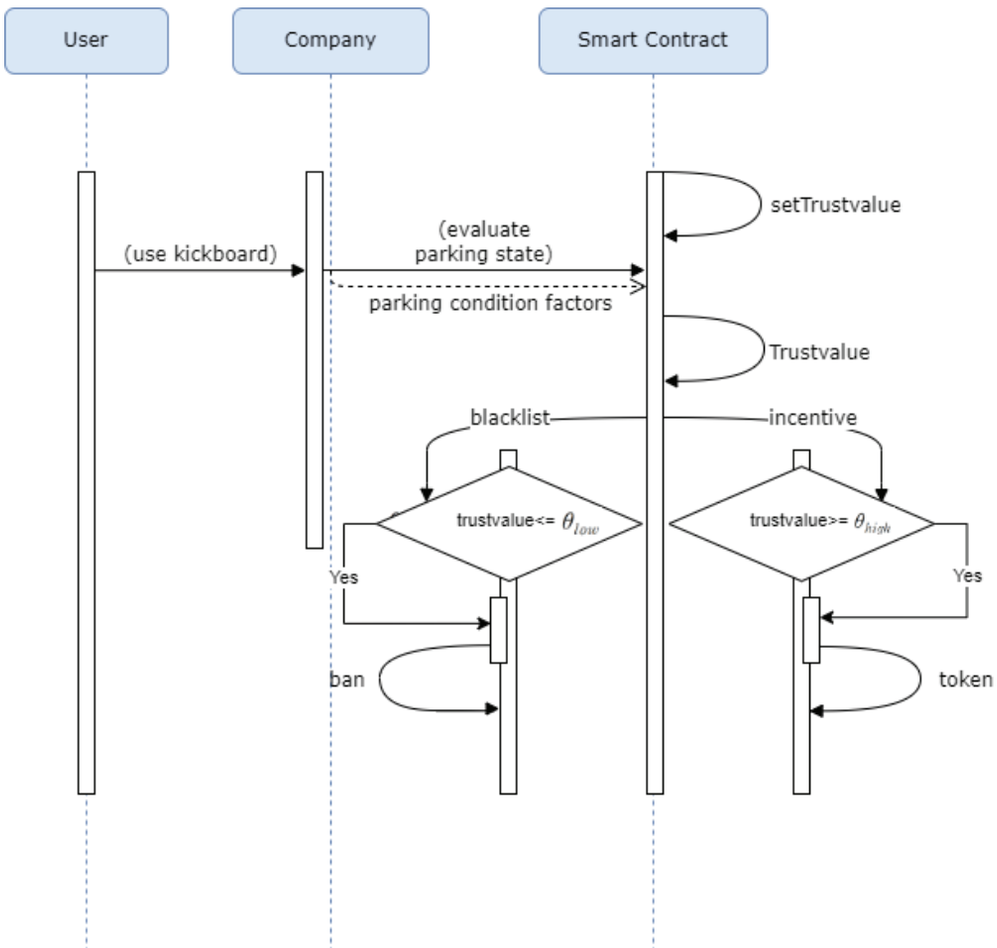

Fig. 4. Smart Contract Operation

4.2 이용자 관리용 스마트 컨트랙트 동작 프로세스

이용자 관리용 스마트 컨트랙트의 동작 프로세스는 Fig. 4에서 보인다. 처음 이용자가 제안 모델에 등록하면 스마트 컨트랙트의 setTrustvalue 함수를 통해 이용자의 신뢰점수 값을 50으로 설정한다. 이용자가 공유 전동킥보드를 이용하기 시작하면 관련 정보는 모바일 어플리케이션을 통해 공유 모빌리티 회사에게 전달된다. 전동킥보드 사용 후, 전동킥보드에 부착된 센서 정보들이 회사 서버로 전달된 후, 회사는 그 센서 정보를 통해 주차 상태를 평가하고 해당 요소 값들을 스마트 컨트랙트에 보낸다. 스마트 컨트랙트 내 Trustvalue 함수로 요소 값을 이용하여 신뢰점수를 계산하여 업데이트한다. 특정 주기(예. 한 달)마다 회사 서버는 AddBlacklist 함수와 Incentive 함수를 실행한다. AddBlacklist 함수는 신뢰점수가 θ_{low}보다 낮은 이용자의 계좌를 Blacklist 변수에서 블랙리스트로 표시한다.

Incentive 함수는 신뢰점수가 θ_{high}보다 높은 이용자 계좌에 대해 토큰을 지급한다.

5. 성능 평가 및 분석

5.1 이용자 관리용 스마트 컨트랙트 가스 수수료 측정

이더리움 플랫폼에서 스마트 컨트랙트를 배포하고 실행하기 위해서는 사용되는 메모리와 연산량에 따라 가스 수수료를 지불해야 한다. 따라서 본 절에서 이더리움 테스트 넷에 이용자 관리용 스마트 컨트랙트를 배포하고 실행할 때 필요한 가스 수수료를 측정하였다. Fig. 5는 이더리움 Sepolia 테스트 넷에 배포한 스마트 컨트랙트를 통해 인센티브를 지급하는 트랜잭션을 실행한 예시를 보인다.

Table 4는 설계한 이용자 관리용 스마트 컨트랙트를 이더리움 테스트 넷에 배포하고 실행했을 때 소모되는 가스량과 그 값을 Gwei와 달러로 환산한 값을 보인다. 가스 값은 [11]에서 보이는 2022년 12월 17일 평균 가스 값으로 설정하였다. 가장 가스가 많이 측정되는 동작은 스마트 컨트랙트 배포로 약 16달러가 소모되지만 이는 처음 컨트랙트가 블록체인에 올라갈 때 한번만 사용되는 비용이다. 스마트 컨트랙트 배포 후, 제안 모델에서 실행되는 setTrustvalue, EvaluationParking

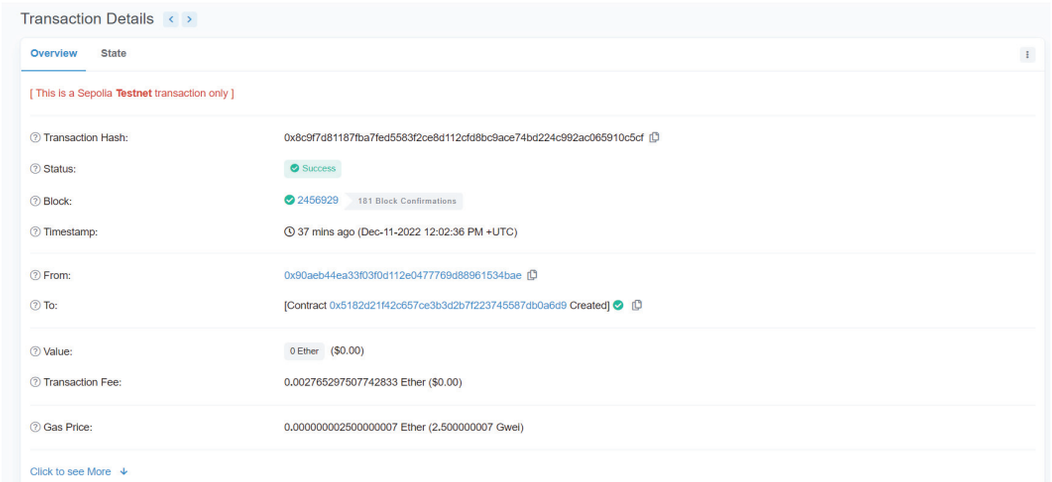

Fig. 5. An Example of Broadcasted Transaction

Table 4. Gas Cost of User Management Smart Contract

No,	Operation	Gas	Gas Price	fee (Gwei)	fee (Dollar)
1	Deployment	624614	17.19Gwei	10,737,114.66	16.60
2	Function setTrustvalue	50514		868,335.66	1.3427
3	Function EvaluationParking	60213		1,035,061.47	1.6005
4	Function Trustvalueupdate	34113		586,402.47	0.906744
5	Function Incentives	27572		473,962.68	0.732880
6	Function AddBlacklist	30028		516,181.32	0.798162

등의 함수들은 실행 시 사용되는 수수료를 달러로 환산하면 1달러 내외로 소요된다. 본 논문에서 가스 금액은 이더리움 메인 넷을 기준으로 하였기 때문에 컨소시엄 블록체인 상에서 스마트 컨트랙트를 실행한다면 이보다 더 낮은 수수료가 사용될 것으로 예상된다. 제안하는 이용자 관리용 스마트 컨트랙트에서는 Mapping 변수를 통해 신뢰점수, 인센티브 잔액 값을 기록하고 있는데 가스 수수료를 줄이기 위해서 해당 값들을 변수로 스마트 컨트랙트에 저장하지 않고 이벤트 로그만 기록하는 방안도 있다.

5.2 악의적인 이용자 신뢰점수 분석

제안 모델에서의 이용자 신뢰점수 산정식은 이용자의 이전 신뢰점수 반영 비율에 따라 다르게 측정될 수 있다. Fig. 5에서는 이전 신뢰점수 반영 비율 β 값이 각각 0.7, 0.5, 0.3 일 때 악의적인 이용자의 신뢰점수 변화를 보인다. 이때 악의적인 이용자는 4가지 주차 상태 평가 요소 중 항상 3가지 요소가 올바른 주차에 부합하지 않는다고 가정하였다. Fig. 6에서 보이듯이 이용자의 초기 신뢰점수가 50점이고 현재 주차 상태에 대한 점수는 항상 그 이하이기 때문에 이전 신뢰점수 비율이 높을수록 신뢰점수가 천천히 감소함을 보인다. 이용자가 주차 상태 평가 점수로 항상 25점을 받으면 그의 신뢰점수는 점차

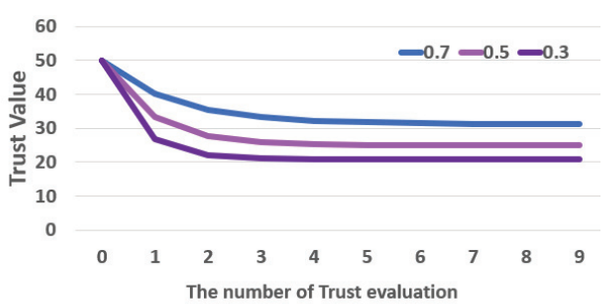

Fig. 6. The Trust Value of A Malicious User According to the Previous Trust Value Reflection Rate

25점에 가까워지게 된다. 블랙리스트를 결정하는 임계값 θ_{low} 이 만약 25점일 경우, 악의적인 이용자를 구분하는 데 시간이 소요될 수 있다. 즉, 임계값 θ_{low}은 악의적인 사용자의 행위를 얼마나 허용해주냐에 따라 그 값이 결정될 수 있다.

5.3 제안 모델 보안성 분석

제안 모델에서 악의적인 이용자는 이용자 관리용 스마트 컨트랙트 운영을 방해하기 위해 의도적으로 많은 양의 트랜잭션을 생성하는 DDoS(Distributed denial of service)를 시도할 수 있다. 그러나 이 경우, 트랜잭션을 수행하는데 이

더 수수료가 소모되기 때문에, 공격자 입장에서는 DDoS 공격을 위해 높은 비용을 지불해야 한다. 따라서 악의적인 이용자가 제안 모델에 DDoS 공격을 하면서 얻는 이득이 없기 때문에 DDoS 공격의 가능성은 낮다. 또한 공유 모빌리티 회사 서버들은 지속적은 트랜잭션 트래픽을 모니터링 하면서 이상 트래픽(예를 들어 짧은 시간동안 특정 이용자 ID에 대한 트랜잭션이 다량 발생할 경우)을 감지할 수 있다.

제안 모델은 블록체인 기술을 통해 다수의 공유 전동킥보드 회사들이 이용자의 정보들을 공유하거 저장한다. 따라서 특정 회사가 해킹, 고장 등의 문제로 서버 내 정보가 소실되더라도 복구가 가능하며 단일 실패점(Single point of failure) 문제가 존재하지 않는다. 또한 블록체인에 기록된 내용은 블록체인의 무결성 특징으로 인해 위·변조가 불가능하다. 그러므로 블록체인 원장에 저장되는 이용자의 신뢰점수, 인센티브 잔액은 안전하게 관리된다.

6. 결 론

본 논문은 공유 전동킥보드의 불법 주차 및 방치 문제를 완화하고 공유 전동킥보드 이용자를 통합적으로 관리하기 위해 공유 전동킥보드 회사들이 참여하는 블록체인 기반의 공유 전동킥보드 이용자 관리 모델을 제안하였다. 제안 모델에서 이용자들은 인센티브를 받기 위해 적극적으로 사용한 전동킥보드를 올바르게 주차하도록 동기가 부여된다. 또한 공유 전동킥보드 회사들은 제안 모델을 통해 기존 불법 주차된 전동킥보드 견인 또는 관리에 대한 비용을 줄일 수 있다. 악의적인 이용자를 통합적으로 관리하고 악의적인 이용자의 서비스 이용을 제한할 수 있어 보다 안전하고 효율적인 공유 전동킥보드 서비스 운영이 가능할 것으로 기대된다. 제안 모델은 공유 전동킥보드 회사들이 참여하고 있으나, 이를 확장하여 공유 자동차, 공유 자전거 등의 다른 공유 모빌리티 회사들과 대중교통 회사들도 참여가능하다. 이 경우, 참여 회사 간의 공유된 인센티브 정보를 토대로 추가시간 이용권 제공, 타 회사의 이동수단 무료 이용 서비스 등 여러 서비스를 제공할 수 있다. 다만, 블록체인의 투명성으로 인해 이용자의 신뢰 점수에 대한 개인정보가 보호되지 못한다는 문제가 있다. 따라서 본 논문의 후속 연구에서는 이용자의 개인정보 보호를 고려한 블록체인 기반 공유 전동킥보드 이용자 관리 모델 설계에 대해 연구할 계획이다.

References

[1] GVR Report, “Personal Mobility Devices Market Size, Share & Trends Analysis Report By Product (Walking Aids, Wheelchairs, Scooters), By Region (North America, Europe, APAC, Latin America, MEA), And Segment Forecasts, 2022 - 2030”. accessed 2022-12-18.

[2] Nielsen [Internet], http://www.koreanclick.com/insights/newsletter_view.html?code=topic&id=599&page=1&utm_source=board&utm_medium=board&utm_campaign=topic&utm_content=20201130, 2020.

[3] Namunews [Internet], https://namu.news/article/1579328#gsc.tab=0, 2022.

[4] S. Carrese, F. D’Andreagiovanni, A. Nardin, T. Giacchetti, and L. Zamberlan, “Seek & Beautify: integrating UAVs in the optimal beautification of e-scooter sharing fleets,” *2021 7th International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, IEEE, 2021.

[5] M.-J. Park, N.-H Kim, S. Lee, and S.-H. Seo, “A study on the Blockchain-based Shared Electric Kickboard Management Model for Citizen Participation,” *Proceeding of the Annual Conference of Korea Information Processing Society Conference (KIPS)*, pp.263-265, 2022. https://doi.org/10.3745/PKIPS.Y2022M11A.263

[6] M. Castro and B. Liskov. “Practical byzantine fault tolerance,” *OsDI*, Vol.99, No.1999, pp.173-186, 1999.

[7] O. Dib, K. Brousmiche, A. Durand, E. Thea, and E. B. Hamida, “Consortium blockchains: Overview, applications and challenges,” *International Journal on Advances in Telecommunications*, Vol.11, No.1&2, pp.51-64, 2018.

[8] D. Wang and X. Zhang. “Secure ride-sharing services based on a consortium blockchain,” *IEEE Internet of Things Journal*, Vol.8, No.4, pp.2976-2991, 2020.

[9] M. Baza, N. Lasla, M. M. E. A. Mahmoud, and G. Srivastava, “B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain,” *IEEE Transactions on Network Science and Engineering*, Vol.8, No.2, pp.1214-1229, 2019.

[10] D. Pirker, T. Fischer, H. Witschnig, and C. Steger, “velink-a blockchain-based shared mobility platform for private and commercial vehicles utilizing erc-721 tokens,” *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*. IEEE, 2021.

[11] Ychart, “Ethereum Average Gas Price” [Internet], https://ycharts.com/indicators/ethereum_average_gas_price, Accessed 2022-12-17.

[12] D.-G. Yoon, “Structual Analysis of Self-Sovereign Identity,” Jpub, 2020.

[13] E.-J. Jang and S.-J. Shin. “Proposal of user filtering system for black consumer extraction -focusing on shared electric kickboard users-,” *The Journal of The Institute of Internet, Broadcasting and Communication*, Vol.21, No.4, pp.97-102, 2021, doi:10.7236/JIIBC.2021.21.4.97.

이 수 진

https://orcid.org/0000-0003-1690-8577
e-mail : tssn195@hanyang.ac.kr
2019년 한양대학교 ERICA 캠퍼스 전자공학부(학사)
2021년 한양대학교 전자공학과(석사)
2021년 ~ 현 재 한양대학교 전자공학과 박사과정
관심분야 : Blockchain Security, IoT Security, Privacy Protection

박 민 정

https://orcid.org/0009-0001-4800-9923
e-mail : koalabona01@hanyang.ac.kr
2020년 ~ 현 재 한양대학교 ERICA 캠퍼스 전자공학부 학사과정
관심분야 : Blockchain Security, IoT Security

김 나 희

https://orcid.org/0009-0009-2561-5515
e-mail : skgml5809@hanyang.ac.kr
2020년 ~ 현 재 한양대학교 ERICA 캠퍼스 전자공학부 학사과정
관심분야 : Blockchain Security, IoT Security

서 승 현

https://orcid.org/0000-0002-1150-7080
e-mail : seosh77@hanyang.ac.kr
2000년 이화여자대학교 수학과(학사)
2002년 이화여자대학교 컴퓨터학과(석사)
2006년 이화여자대학교 컴퓨터학과(박사)
2006년 ~ 2010년 금융보안연구원 주임연구원
2010년 ~ 2012년 한국인터넷진흥원 선임연구원
2012년 ~ 2014년 미국 퍼듀대학교 컴퓨터학과 박사후연구원
2014년 ~ 2015년 고려대학교 정보보호대학원 BK21+ 사업단 연구교수
2015년 ~ 2017년 고려대학교 세종캠퍼스 수학과 조교수
2017년 ~ 현 재 한양대학교 ERICA 캠퍼스 전자공학부 정교수
관심분야 : IoT Security, Blockchain, Privacy protection, Post Quantum Cryptography, Cryptographic Protocol Design and Application