

A Study on DID-based Vehicle Component Data Collection Model for EV Life Cycle Assessment

Jun-Woo Kwon[†] · Soojin Lee^{††} · Jane Kim^{††} · Seung-Hyun Seo^{†††}

ABSTRACT

Recently, each country has been moving to introduce an LCA (Life Cycle Assessment) to regulate greenhouse gas emissions. The LCA is a mean of measuring and evaluating greenhouse gas emissions generated over the entire life cycle of a vehicle. Reliable data for each electric vehicle component is needed to increase the reliability of the LCA results. To this end, studies on life cycle evaluation models using blockchain technology have been conducted. However, in the existing model, key product information is exposed to other participants. And each time parts data information is updated, it must be recorded in the blockchain ledger in the form of a transaction, which is inefficient. In this paper, we proposed a DID(Decentralized Identity)-based data collection model for LCA to collect vehicle component data and verify its validity effectively. The proposed model increases the reliability of the LCA by ensuring the validity and integrity of the collected data and verifying the source of the data. The proposed model guarantees the validity and integrity of collected data. As only user authentication information is shared on the blockchain ledger, the model prevents indiscriminate exposure of data and efficiently verifies and updates the source of data.

Keywords : Decentralized Identity, Self-Soverign Identity, Life Cycle Assessment

전기차 전과정평가를 위한 DID 기반 차량부품 데이터수집 모델 연구

권 준 우[†] · 이 수 진^{††} · 김 제 인^{††} · 서 승 현^{†††}

요 약

최근 세계 각국은 온실가스 배출을 규제하기 위해 전과정평가(LCA, Life Cycle Assessment)를 도입하려는 움직임을 보이고 있다. 전기차 전과정평가의 차량의 전체 수명주기에 걸쳐 발생하는 온실가스 배출량을 측정하고 평가하는 수단이다. 전과정평가 결과의 신뢰성을 높이기 위해서는 전기차 부품별로 신뢰성 있는 데이터가 필요하다. 이를 위해 최근 블록체인 기술을 적용한 전과정평가 모델에 대한 연구들이 수행되었다. 그러나 기존 연구들은 주요 제품 정보들이 다른 참여자들에게 그대로 노출되어 프라이버시 보호가 되지 않는 문제가 있고 부품데이터 정보가 업데이트될 때마다 트랜잭션 형태로 블록체인 원장에 기록해야 해서 비효율적이다. 따라서 본 논문에서는 효율적으로 전기차 차량부품 데이터를 수집하고 유효성을 검증하기 위해 전과정평가를 위한 DID 기반의 데이터수집 모델을 제안한다. 제안하는 모델은 수집된 데이터의 유효성과 무결성을 보장하며 블록체인 원장에는 사용자 인증 정보만 공유되어 데이터의 무분별한 노출을 방지하고 데이터의 출처를 효율적으로 검증 및 업데이트할 수 있다.

키워드 : 분산신원증명, 자기주권신원, 전과정평가

1. 서 론

기후변화와 환경문제로 인해 차량, 해운, 에너지 등 많은 분야에서 온실가스 배출량을 줄이기 위한 목표를 세우고 있다. 특히, 차량 분야에서는 여러 기업이 온실가스 배출량을 줄이기 위한 전기차 개발을 진행하고 있으며, 그 이용자 역시 꾸준히 증가하고 있다. 전기차의 경우 운행 시 내연기관 자동차처럼 직접 온실가스를 배출하지 않아 친환경적인 것처럼 보

지만 원자재 운반 및 차량제조 과정에서 내연기관 자동차들보다 많은 온실가스를 배출한다[1]. 그러나 현재 시행 중인 차량 온실가스 관리제도는 차량 운행 시 배출되는 온실가스에만 초점을 맞추고 있다. 따라서 근본적인 온실가스 감축을 위해서는 차량의 생산부터 폐차까지 전 생애주기에 걸친 온실가스 배출량을 고려한 평가가 필요하다. 이에, 세계 국가들은 차량의 온실가스 배출량 총합을 평가하는 차량 전과정평가(LCA, Life Cycle Assessment) 도입을 검토 중이다.

유럽연합 집행위원회(EC, European Commission)는 EU 평균 승용차의 탄소 배출 기준 목표를 2030년까지 1990년 대비 55% 감축한다는 것을 목표로 하고 있으며, 이를 평가하기 위해 전과정평가를 바탕으로 한 차량 온실가스 배출량 규제에 대한 논의를 진행하고 있다[2]. EU뿐만 아니라 중국은 2025년 국가 규제 도입을 목표로 차량 분야 전과정평가 도입을 검토

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터 육성지원사업의 연구결과로 수행되었음(IITP-2023-2018-0-01417).

† 준 회 원 : 한양대학교 전자공학과 석사

†† 준 회 원 : 한양대학교 전자공학과 박사과정

††† 총신회원 : 한양대학교 ERICA 캠퍼스 전자공학부 정교수

Manuscript Received : March 15, 2023

Accepted : May 6, 2023

* Corresponding Author : Seung-Hynn Seo(seosh77@hanyang.ac.kr)

중이며, 일본 역시 '2030년 승용차 연비기준'을 통해 차량 전 과정에서 발생하는 온실가스 배출을 고려한 전과정평가가 기반 신연비 규제를 도입하기로 하였다. 전과정평가를 전기차 분야에 적용할 경우 원자재 운반 및 차량제조, 부품교체 및 폐기, 에서 소모되고 배출되는 에너지가 평가와 규제의 대상이 된다. 일반적으로 전기차는 12,000여 개의 부품으로 구성되어 있으며[3], 각 부품은 여러 종류의 소재로 구성된다. 즉, 전기차에 대한 전과정평가를 수행하기 위해서는 수많은 부품별로 데이터수집 절차를 거쳐야 하며, 각 전과정평가 단계별로 수많은 데이터와 데이터베이스가 필요하다.

차량 전과정평가를 통해 온실가스 배출정보를 요구하는 규제가 시행된다면, 전과정평가에 사용되는 데이터의 신뢰도가 매우 중요한 요소가 될 것이다. 즉, 차량제조 전반에서 사용되는 소재 또는 부품이 언제 어디서 생산되었는지를 확인하고 이를 반영한 적합한 데이터를 사용했는지에 대한 검증이 필요하다. 또한, 전과정평가의 신뢰도를 높이기 위해서는 올바른 데이터 수집 절차와 데이터에 대한 유효성 검증이 이루어져야 한다.

그러나 차량부품 데이터베이스 구축 한계로 인해 자동차를 구성하는 수많은 소재와 부품에 대한 데이터베이스를 찾기가 어렵다. 더욱이 소재와 부품을 생산하는 지역과 시기에 맞는 데이터베이스를 찾기는 훨씬 어려우며, 실제로 데이터베이스의 명칭만 동일하면 지역과 시기에 상관없이 사용하는 경우가 빈번하다[4]. 우리나라의 경우 기 구축된 LCI(Life Cycle Inventory) 데이터베이스에 등록된 DB 개수는 약 500여 개 수준에 불과하며, 이를 확대 세분화할 필요가 있다.

최근, 위와 같은 문제를 해결하기 위해 전과정평가에 위해 블록체인 기술이 활용되고 있다. [5-7]의 저자들은 제품의 생애주기에 걸쳐 발생하는 정보들을 블록체인에 기록하였으며, [8]은 제품의 환경적 영향 정보를 블록체인 저장하여 제품의 전과정평가를 위한 정보 접근성을 높였다. [9]는 사물인터넷 센서들을 통해 실시간으로 제품의 환경정보를 수집하고 블록체인에 기록하는 블록체인 기반의 전과정평가 모델을 제안했다. 기존 블록체인 모델들은 제품의 전과정평가 정보를 블록체인 또는 클라우드 서버에 저장하여 공유한다. 그러나 전과정평가를 위한 데이터들을 모두 블록체인이나 클라우드 서버에 저장할 경우, 전과정평가 내용에 변경이 있을 때 수정이 어렵고 데이터가 업데이트될 때마다 계속하여 블록체인에 업데이트하여야 한다는 단점이 있다. 또한, 블록체인 또는 클라우드 서버상에 제품 정보가 참여자들에게 무분별하게 공개되어 정보의 프라이버시 보호 방안이 추가적으로 필요하다.

본 논문에서는 전기차 전과정평가의 신뢰도를 높이기 위해 데이터제공자에 대한 인증 및 데이터제공자가 제공하는 차량부품 데이터의 무결성, 유효성을 검증하는 DID(Decentralized Identity) 기반의 차량부품 데이터수집 모델을 제안한다. DID는 블록체인 기반의 탈중앙화 신원증명체제로 블록체인상에서 사용자의 신원을 확인할 수 있게 해준다. 데이터제공자와 데이터수집자는 각각 고유의 DID를 발급받거나 소유하고 있으며, 본 모델에서는 전기차 부품업체들이 데이터제공자,

OEM (Original Equipment Manufacture) 기업이 데이터수집자 역할을 한다. 데이터제공자는 차량부품 데이터를 데이터수집자에게 제출할 때 본인의 서명 및 DID 식별자를 함께 데이터수집자에게 제출한다. 데이터수집자는 DID 식별자를 통해 블록체인 상에서 데이터제공자의 DID 문서를 조회하여 데이터제공자의 신원을 확인하고, 서명과 유효기간 검증을 통해 차량부품 데이터의 무결성 및 유효성을 검증한다. 또한, 차량 전과정평가 특성상 국가별 온실가스 규제 정책 및 전과정평가를 평가하는 기관에 따라 데이터제공자가 제출해야 하는 전기차 차량부품 데이터가 변경될 수 있다. 본 논문에서 제안하는 차량부품 데이터수집 모델은 DID를 기반으로 하기 때문에 데이터의 주권이 사용자에게 있으며, 데이터 내용 변경이 필요할 시, 언제든지 부품데이터 내용 변경이 가능하다.

우리는 uPort[10]의 ethr-did 라이브러리를 이용하여 차량부품 데이터를 JSON(Javascript Object Notation) 데이터 포맷 형태로 생성하고 이를 암호화된 토큰 형태로 주고받았다. 또한, 차량부품 데이터를 검증하는데 걸리는 시간을 측정하였으며, 데이터사이즈나 데이터의 내용이 변경되더라도 검증속도에 크게 영향을 미치지 않는 것을 확인하였다.

본 논문의 2장에서는 관련 연구를 3장에서는 제안하는 모델을 4장에서는 전기차 전과정평가를 위한 데이터수집 시나리오 및 시뮬레이션을 5장에서는 성능분석을 6장에서는 토의를 7장에서는 결론을 기술한다.

2. 관련 연구

2.1 DID (Decentralized Identity)

분산신원증명은 자기주권신원 구현을 위해 온라인상에서 블록체인을 기반으로 사용자가 스스로 신원, 개인정보 등에 대한 증명관리, 신원정보 제출범위 및 대상 등을 통제·수행할 수 있도록 하는 '탈중앙화 신원관리 체계'이다. 사용자는 자신의 신원정보에 대해 주권을 행사할 수 있으며, 분산원장의 암호학적 특성을 기반으로 한 신뢰된 ID 저장소를 이용하여, 제3의 기관의 통제 없이 분산원장에 참여한 누구나 신원정보의 위변조 여부 검증이 가능하다. 사용자(Holder)는 본인의 DID를 통해 자격증명 발행인(Issuer)에게 본인임을 증명하고, 발행인으로부터 자격증명을 획득할 수 있다. 또한, 사용자는 본인이 소유한 자격증명을 조합하여 가공한 후 검증인(Verifier)에게 제출한다. 검증인은 일반적으로 서비스를 제공하는 기업이나 기관이며, 사용자가 제출한 자격증명을 검증한 후 서비스를 제공한다. Fig. 1은 사용자의 자격증명 획득 및 검증 절차이다.

- 사용자는 발행인에게 자격증명 발급요청을 하고 신원확인을 위해 본인의 DID 식별자를 제출한다.
- 발행인은 ID 저장소에서 사용자의 DID 문서를 검증한다.
- 발행인은 사용자에게 자격증명을 발행하고, 해당 자격증명에 서명한다.
- 발행인은 사용자에게 자격증명을 발행하고, 해당 자격증명에 서명한다.

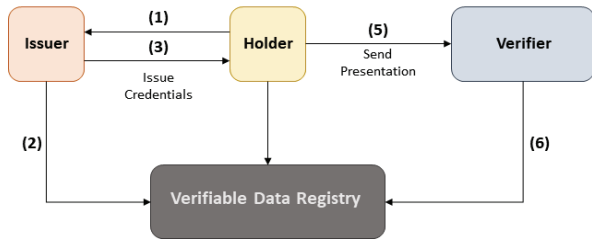


Fig. 1. Verifiable Credential Issuance Process

- 사용자는 본인이 소유하고 있는 자격증명 중 검증인이 요구하는 수준의 정보를 조합한 프레젠테이션(Presentation)을 생성한 후 서명한다.
- 사용자는 생성한 프레젠테이션을 검증인에게 제출한다.
- 검증인은 사용자가 제출한 프레젠테이션의 내용을 확인하고 검증한다.

DID는 키와 값(Key & Value) 형태로 DID 식별자(DID Identifiers)와 DID 문서(DID document)로 구성된다. DID 생성자는 DID 식별자와 DID 문서를 함께 생성한 후 DID 문서는 신뢰된 ID 저장소에 저장한다. 검증자는 DID 식별자를 통하여 DID 문서를 조회할 수 있다. DID 식별자는 URN(Universal Resource Name)형식으로 DID 스킴(DID Scheme), DID 메소드(DID Method), DID 메소드 세부식별 값(DID Method-Specific Identifier)으로 구성되며, DID 문서가 저장된 위치를 알 수 있는 일종의 주소이다. Fig. 2는 DID 식별자 예시이다[11].

DID 문서에는 DID 소유자의 공개키 등 DID의 소유권을 증명할 수 있는 인증수단이 포함되어 있다. 검증자는 시도응답(Challenge & Response) 형식으로 DID 문서에 포함된 공개키를 이용하여 사용자의 Response 검증한다. DID 문서에는 id, publicKey, authentication, service 등의 구성요소들이 포함된다.

VC(Verifiable Credential)는 검증가능한 자격증명으로 각종 데이터, 증명서, 특정인과의 관계 등 모든 정보를 포함할 수 있다. 사용자는 본인의 DID를 통해 본인임을 증명하고 발행인에게 VC를 발급받을 수 있다. 또한, 발행인에게 VC를 발급받는 것이 아닌, 사용자 본인이 스스로 특정 데이터나 정보 등을 VC 형태로 생성하여 상대방에게 전달하는 것도 가능하다.

VP(Verifiable Presentation)는 검증가능한 프레젠테이션으로 하나 이상 VC들의 집합이다. 또한, VP에 포함된 VC들의 출처 검증이 가능한 형태이다. 사용자는 본인이 소유하고 있는 VC 중 하나 이상을 선택하여 VP로 가공할 수 있다. 예를 들어, 학생은 입학증명서 VC, 졸업증명서 VC, 성적증명서 VC 등을 조합하여 이력서 VP를 만들 수 있다.



Fig. 2. DID Identifiers

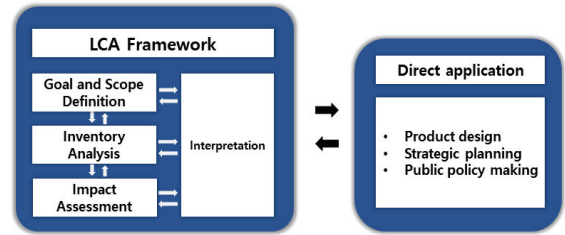


Fig. 3. LCA Framework

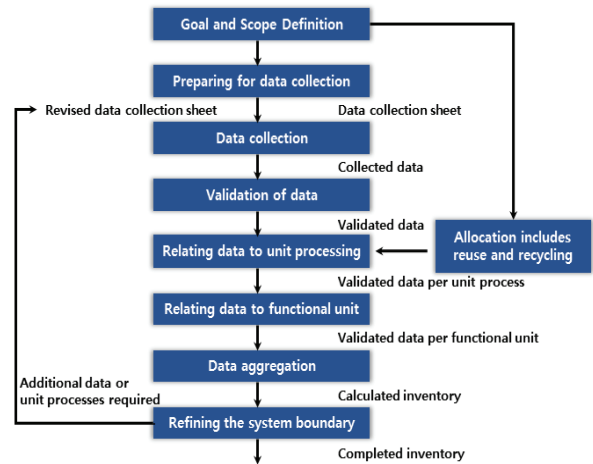


Fig. 4. Life Cycle Inventory Analysis

2.2 현재 전과정평가 (LCA, Life Cycle Assessment)

Fig. 3은 전과정평가 프레임워크이다. 전과정평가는 목적 및 범위 정의, 전과정 목록분석, 전과정 영향평가, 전과정 해석의 4단계로 구성된다. 이중 데이터수집은 전과정 목록분석 단계에서 이루어진다.

Fig. 4는 전과정 목록분석 절차이다. 전과정평가를 위한 데이터는 데이터 품질 요구를 지키며, 전과정평가 수행자가 아닌 현장에 일하는 작업자로부터 수집되어야 한다. 데이터수집자는 데이터베이스나 현장자료 등을 이용해 데이터를 수집할 수 있으며, 특히 전과정평가 연구 대상제품의 제조공정 데이터는 현장데이터를 사용해야 한다. 수집된 데이터는 가공되기 전에 단위공정 또는 전과정 단계별로 검증을 거쳐야 한다[12].

하지만 제품 공급망에는 많은 기업(공급자, 배송, 제조, 소재, 원자재)이 참여한다. 특히, 차량부품과 같이 여러 노드와 복잡한 연결이 있는 공급망에서 신뢰할 수 있는 데이터수집에 어려움을 겪는 경우가 많다.

2.3 블록체인 기반 전과정평가

최근 블록체인 기술을 적용하여 생산품에 대한 정보를 관리하고 추적하는 연구들이 진행되고 있다. [5]의 저자들은 제품의 마케팅부터 디자인, 물류, 유지, 재활용 등 제품의 전 생애 주기 동안 발생 되는 정보들을 관리하기 위한 블록체인 기반의 제품 생애주기 관리 프레임워크를 설계하였다. 제품에 대한 정보의 원본은 클라우드 저장소에 저장되며 원 정보의 해시값이 블록체인에 기록된다. 제품 생산 및 사용에 관련 있는 참여자들은 블록체인을 통해 제품 정보를 검증할 수 있다. [6]

Table 1. A comparison Between the Existing System and the Proposed Model

Classification	[5]	[6]	[7]	[8]	[9]	ours
Decentralized	O	O	O	O	O	O
Integrity	O	O	O	O	O	O
Availability	O	O	O	O	O	O
Traceability	O	O	O	O	O	O
Data privacy	X	X	X	O	X	O
Efficient data proof	X	X	X	X	X	O

은 제품 중심(Product-Centric) 정보를 블록체인과 스마트 컨트랙트를 이용해 통합적으로 관리하는 방안을 제안하였다. 스마트 컨트랙트에 제품의 생애주기 동안 발생하는 정보를 스마트 컨트랙트를 통해 기록, 변경한다. [7]의 저자는 순환 경제(Circular Economy)를 위한 블록체인 기반의 공급망 관리(Supply Chain Management) 모델을 제안하였다. 자원 낭비를 줄이기 위해, 제품의 생산 전부터 생산 이후까지의 과정 동안 자원 재활용 이력 정보를 블록체인에 기록한다. [8]에서는 블록체인 기반의 제품 전과정평가 모델을 제안하였다. 탄소배출량 등 제품의 환경적 영향과 관련된 정보를 블록체인으로 저장하여 모든 블록체인 노드들은 제품의 전과정평가 계산을 할 수 있다. 이때 데이터의 프라이버시를 보호하기 위해 제품명은 암호화된 상태로 공유할 수 있다. [9]의 저자도 전과정평가를 위한 사물인터넷(IoT, Internet of Things) 기술을 결합한 블록체인 시스템을 제안하였다. IoT 센서들을 통해 제품 또는 서비스의 환경 관련 정보를 실시간으로 수집하고 이를 블록체인에 기록하여 보다 정확하고 효율적인 전과정평가 계산이 가능하다. [5-9]에서 수행된 연구들은 블록체인을 통해 제품의 생애주기 동안 발생하는 정보들을 블록체인에 기록함으로써 제품 관련 정보의 접근성을 높이고 이력 정보를 안전하게 관리할 수 있도록 하였다. 그러나 전기 차량의 경우, 부품이 약 12,000개로 전기 차량의 전과정평가를 위해 관련 부품정보를

블록체인에서 일일이 조회하는 것은 비효율적이다. 또한, 블록체인에 기록된 부품정보를 업데이트할 때, 많은 양의 트랜잭션이 발생하므로 긴 트랜잭션 처리 시간이 필요하다. 추가적으로 [5-7, 9]처럼 부품데이터들이 모두 블록체인 상에서 공개될 경우, 제조사, 제조일자 등의 정보가 블록체인 참여자에게 모두 노출되어 데이터 프라이버시 보호가 되지 않는 문제가 발생할 수 있다. Table 1은 기존 블록체인 기반 제품 전과정평가 모델과 제안하는 모델을 비교하였다. 기존 연구들은 블록체인의 특성에 따라 분산성, 무결성, 접근성, 그리고 추적성을 가지고 있다. 그러나 [5-9]는 제품 정보가 블록체인 원장 또는 클라우드 서버에서 공개되어 프라이버시 보호가 되지 않았다. 또한, 기존 연구들은 효율적인 정보 증명 방안을 고려하지 않았다. 따라서 본 논문은 DID 모델을 적용하여 전과정평가를 위한 각 부품의 환경정보를 블록체인이 아니라 사용자의 지갑에서 관리하여 무분별한 정보 노출을 막고 해당 정보를 증명하기 위한 정보를 블록체인에 관리함으로써 효율적인 전과정평가를 위한 데이터수집 모델을 방안을 제시한다.

3. DID 기반 전기차 차량부품 데이터수집 모델

본 장에서는 전기차 전과정평가를 위한 DID 기반 차량부품 데이터수집 모델을 제안한다. 본 모델은 최상위 신뢰기관, DID 발급·등록 및 전과정평가 신뢰저장소 운영 주체인 OEM (Original Equipment Manufacturer), 전기차 부품업체, 검증기관, LCA 평가기관으로 구성된다.

전기차는 약 12,000개의 많은 부품으로 구성되어 있으며, 조립과정에서 수많은 부품업체를 거친 후 최종적으로 완성차 기업인 OEM에 의해 조립된다. 각각의 전기차 부품업체는 전과정평가를 위한 데이터수집자 역할을 하며, OEM과 전기차 부품업체는 DID를 기반으로 전기차 전과정평가 기준에 부합하는 차량부품 데이터를 VC, VP 형태로 생성하여 주고받는다. Fig. 5는 DID 기반 전기차 차량부품 데이터수집 모델 개요도이다.

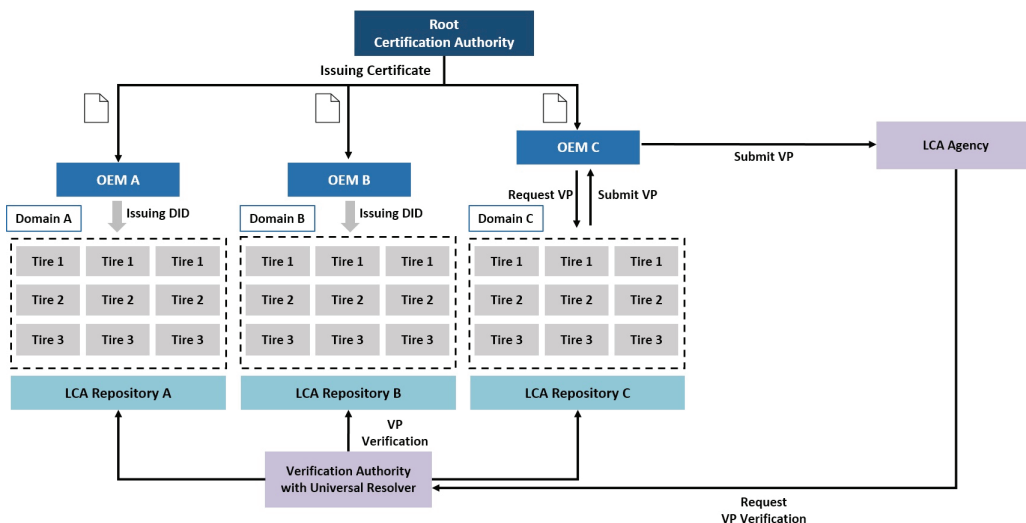


Fig. 5. Proposed Model

3.1 최상위 신뢰기관

최상위 신뢰기관은 가장 높은 신뢰 수준을 바탕으로 OEM의 가입, 제명, 권한 부여 및 정지 등에 대한 사항을 결정한다. 최상위 신뢰기관은 각 OEM에게 OEM 인증서를 발급하며, 해당 인증서에는 등록기관, 보장등급, OEM 명칭, OEM 검증정보, 유효기일 등이 포함되어 있다. OEM은 인증서를 통해 전과정평가 신뢰저장소의 운영관리 권한 등을 얻을 수 있으며, OEM은 이를 통해 해당 본인에게 차량부품을 납품하는 전기차 부품업체들에게 전과정평가 신뢰저장소 운영관리 권한을 증명할 수 있다.

3.2 OEM (Original Equipment Manufacturer)

OEM은 각 OEM 별로 전기차 차량부품 데이터수집을 위한 전과정평가 신뢰저장소를 운영·관리한다. 또한, OEM은 본인이 운영하는 도메인에 참여하는 전기차 부품업체에게 DID를 발급 및 등록해주는 역할을 한다.

본 논문에서는 OEM과 해당 OEM에게 차량부품을 납품하는 모든 전기차 부품업체가 한 도메인에 속해있다고 가정한다. 부품업체의 경우 하나의 OEM에게만 부품을 납품하는 것이 아닌, 여러 OEM에게 차량부품을 납품할 수 있으므로 타 OEM이 운영하는 도메인에 동시에 참여할 수 있다. OEM은 자신에게 차량부품을 납품하는 부품업체들에게 해당 도메인에서 사용 가능한 DID를 발급해주고, DID와 쌍을 이루는 DID 문서는 OEM이 운영하는 전과정평가 신뢰저장소에 등록한다.

OEM은 완성된 전기차에 대한 전과정평가가 필요한 경우, LCA 평가기관에 전기차 전과정평가를 요청하고 전과정평가에 필요한 차량부품 데이터 VC를 부품업체들로부터 수집한다. OEM은 부품업체들로부터 수집한 차량부품 데이터 VC를 전기차 전과정평가 데이터 기준에 부합하는 VP로 가공하여 LCA 평가기관에 제출한다.

3.3 전기차 부품업체

Fig. 6는 차량부품 납품구조이다. 차량부품 납품구조는 일반적으로 하위 부품업체가 상위 부품업체로 부품을 납품하는 피라미드 구조이다. 각 부품업체는 해당 업체가 납품하는 물품에 따라 1차 부품업체에서 3차 부품업체로 구분된다. 예를 들어, 소재, 원자재 업체는 3차 부품업체, 엔진, 제동, 조향 전장 등 부품업체는 2차 부품업체, 모듈 및 시스템 업체는 1차 부품업체로 구분된다. 부품업체들은 OEM으로부터 DID를 발급받으며, 본인들이 납품하는 차량부품에 대한 데이터를 VC로 발행한다. 부품업체는 상위 부품업체나 OEM에 부품을 납품하면서 차량부품 데이터 VC를 함께 전달하며, 최종적으로 OEM은 모든 차량 부품데이터 VC를 수집하여 취합한다.

또한, 차량제조 특성상 수많은 부품업체가 존재하며, 부품업체는 한 OEM뿐 아니라 여러 OEM에게 부품을 납품할 수 있다. 따라서, 부품업체는 한 도메인이 아닌 여러 도메인에 속할 수 있다. 검증기관은 부품업체가 새로 DID를 발급받지 않더라도 기존의 DID를 이용해 새로운 도메인에서 활동할 수 있도록 해준다.

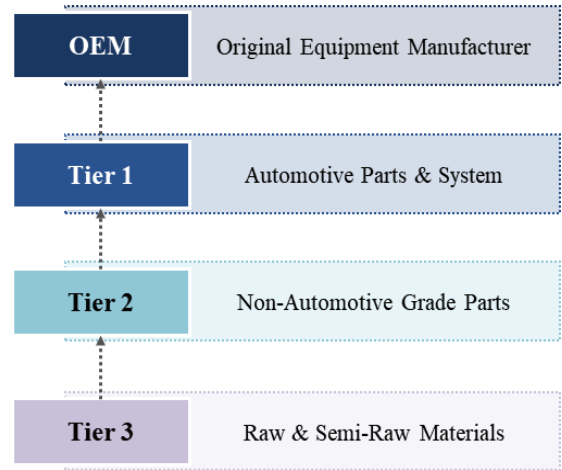


Fig. 6. Automotive Supply Chain

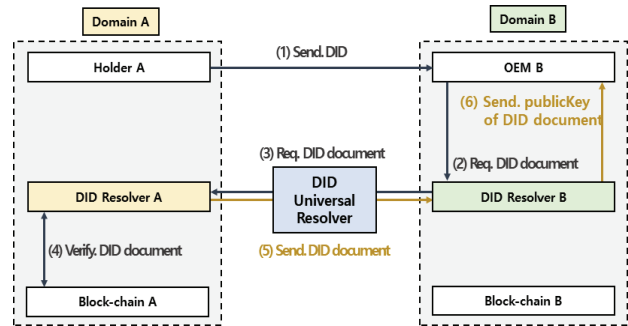


Fig. 7. Verification Authority

3.4 검증기관

검증기관은 최상위 신뢰기관으로부터 운영되며, VC나 VP의 진위를 확인하기 위해 저장소를 통해 DID를 검증하는 역할을 한다. 제안하는 모델의 경우 부품업체가 여러 도메인에 참여할 수 있다. 하지만 각 OEM은 개별적인 저장소를 운영하면서 독자적인 생태계를 구축하고 있다. 따라서, 부품업체들이 여러 도메인에서 활동하기 위해 DID 상호운용을 지원하는 검증기관이 필요하다. 검증기관은 OEM의 부품업체 DID 검증을 돕기 위해 유니버설 리졸버(Universal Resolver)의 기능을 수행할 수 있어야 한다. Fig. 7은 유니버설 리졸버를 이용한 검증기관의 타 도메인 간 DID 검증과정이다.

3.5 LCA 평가기관

LCA 평가기관은 전기차 전과정평가를 수행하는 기관이다. OEM 업체는 전기차 전과정평가를 LCA 평가기관에 요청하고, LCA 평가기관에서 요구하는 수준의 전기차 차량부품 데이터를 VP로 가공하여 LCA 평가기관에 제출해야 한다. OEM은 부품업체들로부터 전기차 차량 부품데이터 VC를 수집하여 이를 VP로 가공한 후 LCA 평가기관에 제출한다. LCA 평가기관은 검증기관의 도움을 받아 OEM이 제출한 VP의 유효성 및 진위를 검증하고 VP에 포함된 정보가 전과정평가 데이터 요구사항에 부합하는지를 확인한 후 전과정평가를 진행한다.

4. 전기차 전과정평가를 위한 데이터수집 시나리오 및 시물레이션

본 장에서는 전기차 전과정평가를 위한 차량부품 데이터수집 시나리오를 보여준다. 전기차 전과정평가는 LCA 평가기관에 의해 수행된다. 전기차에 대한 전과정평가가 필요한 OEM은 LCA 평가기관에 전과정평가 요청을 하게 되고, LCA 평가기관에서 요구하는 수준의 차량부품 데이터를 VP로 가공하여 제출해야 한다. OEM은 VP 생성을 위해 전기차 부품업체들로부터 차량부품 데이터 VC를 발급받은 후, 이를 가공하여 VP를 생성한다. Fig. 8은 차량 부품데이터 수집 및 제출 절차이다.

Table 2는 부품업체가 전기차 차량부품을 납품할 때 함께 제출해야 하는 차량부품 환경정보 데이터 명세 예시이다. 여기에는 지구온난화지수, 부영양화지수 등 차량부품 생산 시 발생하는 환경오염 지표에 관한 내용이 포함되어 있다. 해당 내용은 추가되거나 변경될 수 있으며, DID 시스템 특성상 명세 내용이 바뀌더라도 부품업체는 해당 데이터 명세를 기반으로 쉽게 클레임(Claim)을 추가하거나 제거할 수 있다

본 논문에서는 시물레이션을 위해 uPort[10]에서 제공하는 이더리움 기반의 ethr-did 라이브러리를 이용한다. uPort에서는 ERC-1056을 기반의 DID 저장소를 이더리움 메인넷에 배포하였으며, 사용자는 라이브러리를 통해 DID를 생성 및 조회할 수 있다. ethr-did 라이브러리를 이용하면 VC 및 VP를 JSON (Javascript Object Notation) 데이터 포맷 형태로 생성할 수 있다. 또한, 이를 JWT(JSON Web Token)형태로 생성하여 주고 받을 수 있다. JWT는 JSON 데이터를 Base64 URL-safe Encode를 통해 인코딩하여 직렬화한 것이며, 토큰 내부에는 위변조 방지를 위해 발행인의 개인키를 이용한 전자서명이 포함된다.

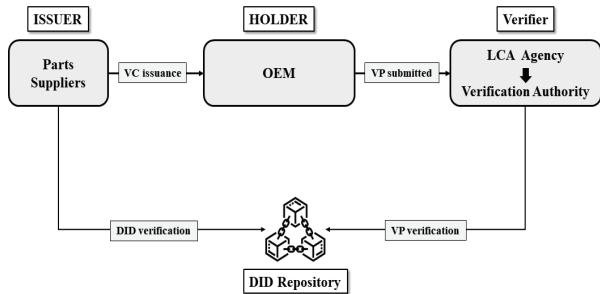


Fig. 8. VC Issuance & VP Verification Process

Table 2. EV Parts Data Statement

Claim
Global Warming
Eutrophication
Acidification
Ozone Depletion
Photochemical Ozone Formation
Abiotic Depletion
Water Depletion
Human Toxicity

4.1 OEM의 DID 생성 및 부품업체 DID 발급

전과정평가 신뢰저장소 운영 주체인 OEM은 해당 도메인에서 사용할 DID를 스스로 생성한다. 부품업체는 OEM에게 본인임을 증명한 후 OEM으로부터 DID를 발급받는다. OEM은 자신에게 차량부품을 납품하는 부품업체들에게 해당 도메인에서 사용 가능한 DID를 발급해주고, DID 식별자와 쌍을 이루는 DID 문서는 OEM이 운영하는 전과정평가 신뢰저장소에 등록한다. DID 문서에는 해당 DID의 소유권을 증명할 수 있는 인증수단이 포함된다.

DID는 EthrDID 함수를 통해서 생성되며, DID 문서는 DID 리졸버(DID Resolver)를 통해 조회할 수 있다. DID 리졸버는 Infura를 통해 본인의 프로젝트를 생성한 후, getResolver 함수를 통하여 가져올 수 있다. DID 문서 조회는 resolve 함수를 통해서 수행되며, Fig. 9는 조회된 DID 문서 예시이다. DID 문서는 크게 id, publicKey, authentication, signature 항목으로 구성되며, Table 3은 DID 문서의 주요항목이다.

4.2 전기차 차량부품 데이터 VC 생성 및 제출

전기차 전과정평가를 위해서, 차량 부품업체들은 전과정평가를 위한 차량부품 데이터를 VC나 VP 형태로 만들어 상위tier의 부품업체나 OEM에게 제출해야 한다. 이때, 부품업체는

```

1  {
2    "@context": "https://www.w3.org/ns/did/v1",
3    "id": "did:storageA:1234CompanyA",
4
5    "publicKey":[{"id": "did:storageA:1234CompanyA#key-1",
6                  "type": "RsaVerificationKey2022",
7                  "controller": "did:example:1234User",
8                  "publicKeyPem": "--BEGIN PUBLIC KEY...END PUBLIC KEY--\n"},
9                  {"id": "did:storageA:1234CompanyA#key-2",
10                 "type": "RsaVerificationKey2022",
11                 "controller": "did:example:1234User",
12                 "publicKeyPem": "--BEGIN PUBLIC KEY...END PUBLIC KEY--\n"}
13                ],
14
15    "authentication":[{"id": "did:storageA:1234CompanyA#keys-1",
16                      "did:storageA:1234CompanyA#keys-2"}
17                    ],
18
19    "signature":[{"type": "RsaSignature2022",
20                 "created": "2022-09-22T16:02:20Z",
21                 "creator": "did:example:1234OEM",
22                 "signatureValue": "QNB13Y7Q9...1tzjn4w=="
23                }
24              ]
25            }
26          }
27        }
28      }
    
```

Fig. 9. Example of DID Document

Table 3. Main Items in a DID Document

Component	Description
id	The id field contains a DID of a parts supplier that is identified through id.
publicKey	The publiKey field contains a variety of types of data required for DID ownership authentication,
authentication	The authentication field specifies the ownership authentication method provided by the DID document
signature	The signature field Includes OEM's signature on the parts supplier's public key.

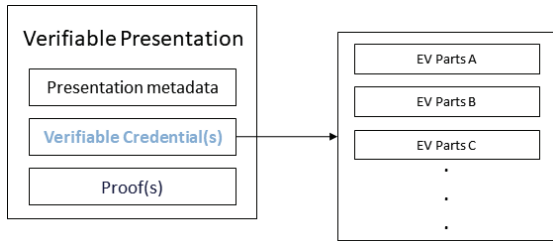


Fig. 13. VP Data Model of EV Parts Data

Table 5. Items of VP that Require Verification

Components	Description
VP Proof	Checking whether the VP is forgery and verifying whether the OEM who submitted the VP is the valid.
Decentralized ID of the holder pointed to by the VC in the VP	Verifying that the holder pointed to by the VC is the submitter.
Proof of the VC in the VP	Checking whether the VC belonging to the VP is forged and verifying that VC issuer is the correct.

어 있다. Fig. 13은 전기차 부품데이터 VP 데이터모델이다. 프레젠테이션 메타데이터(Presentation metadata)항목에는 해당 데이터의 타입, 이용약관 등이 포함되며, 검증가능한 자격 증명(Verifiable Credential(s)) 항목에는 각 부품에 대한 VC들이 포함된다. Proof(s) 항목에는 VP 발행인의 서명, 서명 알고리즘, 서명 생성일, 검증방법 서명 값 등이 포함된다.

4.5 전기차 차량부품 데이터 VP 검증

OEM으로부터 전기차 차량부품 데이터 VP를 전달받은 LCA 평가기관은 해당 VP에 대한 검증과정을 거친 후 전과정 평가를 수행한다. LCA 평가기관은 차량부품 데이터 VP에 포함된 Table 5와 같은 항목들을 검증한다. 만약 검증하는 VP에 속한 VC의 발행인이 해당 VP를 제출한 OEM의 도메인에 속하지 않는 경우, VP를 검증하기 위해 검증기관에 검증요청을 하여야 한다.

5. 성능 분석

본 장에서는 전기차 차량부품 데이터 제출 및 검증 시나리오를 시뮬레이션을 통해 분석한다. 시뮬레이션에는 삼성 NT950QDB-K71A 모델이 사용되었으며, 11세대 i7-1165G7 2.8GHz, 16GB RAM이 내장되어 있다.

전기차는 구동/전달 부품 2,280개, 차체 부품 2,880개, 서스펜션/제동 부품 2,880개 기타 부품 3,960개로 약 12,000개의 부품으로 이루어진다. 또한, 1차 기업의 경우 위탁기업이 평균 15.1곳 2차 이하 기업의 경우 평균 13.2 곳 정도이다 [13]. 따라서, OEM이 관리해야 하는 VC의 개수는 12,000개이며, 1차 부품업체에서 관리해야 하는 총 VC의 개수는 약 1,000개 정도로 추정된다.

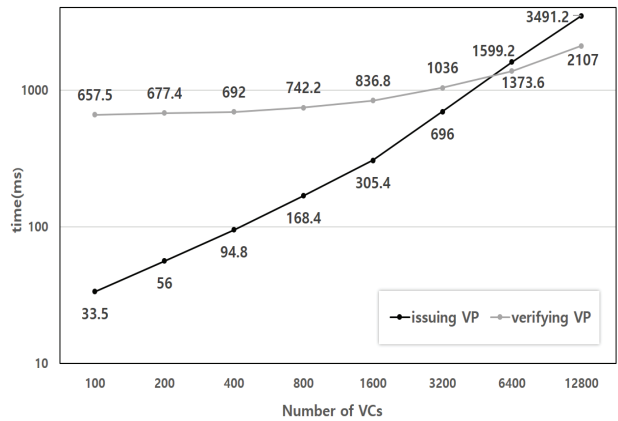


Fig. 14. VP Issuance and Verification Time According to Number of VCs

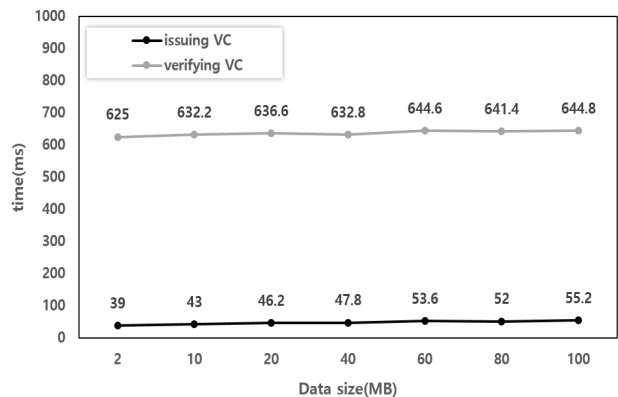


Fig. 15. VC Issuance and Verification Time According to Data Size

첫 번째 실험에서는 전기차에 필요한 총 부품의 개수를 고려하여 VP 생성과 검증에 소요되는 시간을 측정하였다. Fig. 14와 같이 VP에 속한 VC의 개수를 100개부터 12800개까지 변화시켜가며, VP 발행과 검증에 소요되는 평균시간을 측정을 진행하였다. VP 발행에 소요되는 시간은 VP에 속한 VC의 개수에 따라 선형적으로 증가하며, VP 검증에 소요되는 시간은 VP 발행에 비해 증가율이 낮은 것을 확인할 수 있다. VP에 속한 VC의 개수가 12,800개일 경우 VP 생성에는 약 3.4초, VP 검증에는 약 2.1초가 소요되는 것을 확인할 수 있다.

차량제조의 특성상 부품이 변경되거나 제조공장/지역 등에 따라 차량부품데이터가 변경될 수 있다. 이는 VC 데이터 사이즈에 변화를 줄 수 있다. 두 번째 실험에서는 VC 데이터 사이즈에 따른 VC 발급 및 검증시간을 측정하였다. Fig. 15와 같이 VC의 데이터사이즈를 2MB에서 100MB까지 증가시키면서 VC 발행 및 검증에 소요되는 시간을 측정하였다. VC 데이터사이즈가 증가하더라도 VC 발행 및 검증에 소요되는 증가량이 적어 크게 영향을 주지 않는 것을 확인할 수 있다. 따라서 전과정평가에 필요한 차량부품데이터 내용과 데이터 사이즈가 변경되더라도 VC 발행 및 검증에는 영향을 미치지 않는다.

6. 토 의

전기차 전과정평가를 위해서는 올바른 데이터 수집과정과 수집된 데이터의 신뢰성과 유효성을 검증하는 것이 중요하다. 본 장에서는 수집된 전기차 차량부품 데이터의 신뢰성을 위한 토의를 기술한다.

첫 번째 데이터 무결성 문제이다. 제안하는 모델에 참여하는 OEM이나 상위 부품업체는 하위 부품업체에서 제출한 차량부품 데이터 VC/VP의 발행인, Proof(s) 항목을 검증한다. 발행인 항목은 VC/VP의 발행인이 올바른지 확인하는데 이용되며, Proof(s) 항목은 제출된 VC나 VP의 위·변조 여부를 확인하고 데이터의 무결성 검증에 이용된다.

두 번째는 사용자 인증 문제이다. 전과정평가를 위한 데이터 수집 시, 데이터의 출처를 밝히는 것은 매우 중요한 문제이다. 본 모델은 DID Auth를 통해 DID 소유자를 인증하고 데이터의 출처를 밝힌다. 부품업체에 발급되는 DID와 DID 문서는 PKI를 기반으로 하고 있으며, DID Auth는 시도응답(Challenge & Response) 방식으로 수행된다. 검증자는 부품업체 DID 문서에 등록된 공개키와 쌍을 이루는 개인키를 이용하여 사용자 인증을 진행한다. 개인키의 경우 부품업체만 알기 때문에 그 외의 이용자는 Response 값을 생성할 수 없다. 이는 공격자의 데이터 변조, 삽입, 삭제 등을 불가능하게 하며, 중간자 공격과 재전송 공격으로부터 안정성을 제공한다.

세 번째는 가용성 문제이다. 제안하는 모델에 참여하는 차량 부품업체들은 OEM이 운영하는 도메인에 참여하는 사용자(OEM, 부품업체 등)의 DID나 제출된 차량부품 데이터에 대한 검증을 언제든 진행할 수 있다. 또한, 사용자들의 인증정보는 중앙화된 기관이 저장하는 것이 아닌, DID 문서 형태로 블록체인의 분산화된 신뢰저장소에 저장되기 때문에 DoS, DDoS 등의 공격을 받아 네트워크 한곳에 장애가 발생하더라도 가용성에 큰 영향을 끼치지 않는다.

7. 결 론

전기차의 경우 운행중에는 온실가스를 배출하지 않지만, 원자재 운송 및 생산과정에서 많은 온실가스를 배출한다는 사실이 알려지면서 관심을 받고 있다. 유럽, 일본, 중국 등 세계 각국은 차량의 온실가스 배출량을 규제하기 위한 수단으로 전과정평가 도입을 논의하고 있다.

전과정평가의 정확성을 높이기 위해서는 신뢰성 있는 데이터사용이 필요하다. 하지만, 차량 전과정평가를 위한 데이터베이스의 부재로 데이터베이스 구축 및 데이터수집의 필요성이 제기되고 있다. 데이터의 신뢰성을 위해 블록체인이 전과정평가 모델에 적용된 사례들이 있으나 제품 관련 정보가 그대로 모든 참여자에게 노출되고 정보의 수정 및 업데이트가 있을 때마다 블록체인에 새로 기록해야 하는 번거로움이 있었다. 이를 개선하기 위해 본 논문에서는 DID 기반의 전기차 전과정평가를 위한 전기차 차량부품 데이터수집 모델을 제안하

였다. 데이터수집자인 OEM은 데이터제공자인 부품업체에게 DID를 발급함으로써 데이터제공자에 대한 인증을 수행한다. 또한, 데이터제공자인 전기차 부품업체는 데이터에 본인의 DID를 삽입한 후 전자서명을 수행하여 데이터의 출처와 무결성을 보장한다. 차량부품 데이터는 개인이 관리하고 공유 원장에는 참여자의 인증 정보만 올라가므로 타인으로부터 데이터 프라이버시를 보호할 수 있고 효율적인 데이터 업데이트와 검증이 가능하다. 본 연구는 추후 전기차뿐만 아니라 타 공급망 분야에서도 적용 가능할 것으로 기대된다.

References

- [1] H. W. Shim and S. S. Kim, "Analysis on a greenhouse gas reduction effect of an electric vehicle by applying the demand side management method," *Korea Society of Transportation*, Vol.36, No.6, pp.403-414, 2018.
- [2] H. C. Kim, "Climate change and life cycle assessment of automobiles," *Auto Journal*, Vol.43, No.5, pp.23-27, 2021.
- [3] Korea energy information center [Internet], <http://www.energycenter.co.kr/news/articleView.html?idxno=1290>, Apr. 2021.
- [4] I. K. Kim, "LCI database for life cycle assessment on vehicle," *Auto Journal*, Vol.43, No.5, pp.28-31, 2021.
- [5] X. L. Liu, W. M. Wang, H. Guo, A. V. Barenji, Z. Li, and G. Q. Huang, "Industrial blockchain based framework for product lifecycle management in industry 4.0," *Robotics and Computer-Integrated Manufacturing*, Vol.63, 2020.
- [6] J. Mattila, T. Seppälä, P. Valkama, T. Hukkinen, K. Främbling, and J. Holmström, "Blockchain-based deployment of product-centric information systems," *Computers in Industry*, Vol.125, 2021.
- [7] B. Wang, W. Luo, A. Zhang, Z. Tian, and Z. Li, "Blockchain-enabled circular supply chain management: A system architecture for fast fashion," *Computers in Industry*, Vol.123, 2020.
- [8] X. Lin, X. Li, S. Kulkarni, and F. Zhao, "The application of blockchain-based life cycle assessment on an industrial supply chain," *Sustainability*, Vol.13, No.23, 2021.
- [9] A. Zhang, R. Y. Zhing, M. Farooque and K. Kang, "Blockchain-based life cycle assessment: An implementation framework and system architecture," *Resources, Conservation and Recycling*, Vol.152, 2020.
- [10] uPort [Internet], "<https://www.uport.me>," Dec. 2022.
- [11] K. H. Lee, S. H. Park, H. J. Kim, T. G. Ha, J. Y. Yoo, and K. B. Kim, "A Proposal of an Inter-Operable Trust Anchor Framework Basic Model for Decentralized Identity (DID) and Public Key Infrastructure (PKI)," *KICS Journal*, Vol.47, No.10, pp.1606-1619, 2022.

- [12] M. N. Nwodo and C. J. Anumba, "Exergetic life cycle assessment: A review," *Energies*, Vol.13, No.11, 2020.
- [13] Korea Labor Institute [Internet], <https://www.kli.re.kr/eia/selectNewReprtView.do?key=476&nttNo=210&pageIndex=2&bbsNo=93&searchYear=&endYear=&searchDepart=&searchNm=&searchResearch=&searchContents=>, 2019.



김 제 인

<https://orcid.org/0000-0002-7635-8653>
e-mail : rean5123@hanyang.ac.kr
2021년 한양대학교 ERICA 캠퍼스
전자공학부(학사)
2023년 한양대학교 전자공학과(석사)
2023년~현 재 한양대학교 전자공학과
박사과정

관심분야 : Blockchain Security, Post Quantum Cryptography



권 준 우

<https://orcid.org/0000-0001-5898-3036>
e-mail : kjw9628@hanyang.ac.kr
2021년 한양대학교 ERICA 캠퍼스
전자공학부(학사)
2023년 한양대학교 전자공학과(석사)

관심분야 : Decentralized Identity, Privacy Protection



서 승 현

<https://orcid.org/0000-0002-1150-7080>
e-mail : seosh77@hanyang.ac.kr
2000년 이화여자대학교 수학과(학사)
2002년 이화여자대학교 컴퓨터공학과(석사)
2006년 이화여자대학교 컴퓨터공학과(박사)

2006년 ~ 2010년 금융보안원 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, Front-end
Design & Verification Methodology



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