논문 22-47-01-17 The Journal of Korean Institute of Communications and Information Sciences '22-01 Vol.47 No.01
https://doi.org/10.7840/kics.2022.47.1.151

프라이버시 보호가 가능한 익명성 기반 차량용 분산 ID

김 현 곤◆

Privacy-Preserving Decentralized Identifiers with Anonymity for Automotive

Hyun-gon Kim◆

요 약

차량통신에 블록체인 기반의 분산 ID(DID)가 상용화될 예정이다. 그러나 DID는 가명성을 제공하지만, 익명성을 제공하지 못함으로 인해 차량 식별자, 운전자 식별 정보, 주행 정보, 위치 정보, 통신 메시지 등이 노출되는 프라이버시 위협이 존재한다. 예를 들어 공격자가 블록체인에서 동일한 DID를 갖는 트랜잭션을 수집하거나, 무선상에서 동일한 DID를 가진 송수신 메시지를 연결하면 차량을 식별하거나 차량의 위치와 차량 주행 정보를 추적할 수 있다. 이와 관련하여 본 논문에서는 차량의 익명성을 제공할 수 있는 프라이버시 보호 기법을 제안하였다. 차량의 소유 증명이나 신원 증명을 위해 짧은 유효기간을 가진 단기 DID를 사용하고, 블록체인의 트랜잭션이나 송수신 메시지의 비연결성을 제공하여 익명성을 보장한다. 표준에 따른 DID 발급 및 검증 절차를 설계하고, 하이퍼레저 인디 블록체인을 활용하여 구현하였으며, 기본적인 성능을 제시하여 제안한 기법의 실현 가능성을 검증하였다.

키워드 : 분산 ID, 익명성, 블록체인, 하이퍼레저 인디, 검증 가능한 크레덴셜
Key Words : DID, Anonymity, Blockchain, Hyperledger Indy, Verifiable Credentials

ABSTRACT

The blockchain-based decentralized identifier(DID) for the automotive industry will be commercialized. However, because the DID provides not anonymity but pseudonymity, leakage of vehicle identifier, privacy threats related to driver-identifying information, vehicle's location, vehicle's driving information, communication message would be vital privacy issues. If an adversary collects transactions based on the same DID in the blockchain and reveled messages through wireless hacking, he or she can identify the vehicle and, track the vehicle's location and driving information. In this paper, a privacy-preserving scheme for vehicles, which provides anonymity. It uses short-term DID for proof of ownership and for pseudonymous through unlinkability of blockchain transactions and communication messages. To verify the feasibility of the scheme, DID issue and verify procedures based on the DID standard are designed and implemented using Hyperledger indy blockchain, also, the results of basic performance analysis are described.

Ⅰ. 서 론

블록체인은 합의를 기반으로 한 공유 분산 데이터베이스이며 탈중앙성, 투명성, 불변성, 가용성을 제공하는 장점 때문에 다양한 산업 분야에 접목되고 있다. 자동차 산업에서는 주행 데이터 공유 플랫폼, 공유 플랫폼을 통한 데이터 마켓, 차량 거래, 차량 식별, 주차료나 통행료 그리고 컨텐츠의 전자지불, 블랙박스 데

◆ First Author : Mokpo National University, Department of Information Security, hyungon@mokpo.ac.kr, 정회원
논문번호 : 202108-216-D-RN, Received August 26, 2021; Revised October 18, 2021; Accepted October 19, 2021

이터 기록, 리스 차량의 운행 거리 기록 등 다양한 비즈니스로 확대되고 있다[1].

블록체인은 참여자 모두에게 정보가 공개되기 때문에 투명성이 제공되지만, 이로 인해 거래 내역이나 개인의 민감한 정보가 노출될 수 있어 프라이버시 보호 측면에서 충돌한다. 신분증의 예를 들면, 신분증 위변조에는 강인하지만, 신분증에 기록된 개인정보의 노출에는 취약하다. 이와 관련하여 블록체인에 기반한 데이터 주권 개념(SSI; Self Sovereign Identity)이 주목받고 있다. 데이터 주권이란 개인에게 정보 권한을 부여해 스스로 자신의 데이터가 어디서, 어떻게, 어떤 목적으로 사용될지를 결정할 수 있는 권리를 말한다. SSI는 탈중앙 아이디로 DID를 사용하며, 영지식 증명(zero-knowledge proofs) 기법을 적용하여 필요로 하는 최소한의 개인정보만을 노출시킬 수 있다. 또한 개인정보에 관련된 내용을 보여주지 않고도 해당 내용이 유효함을 증명할 수 있다. 즉, 내용을 알지 못하지만, 증명자가 제출한 데이터가 유효하다는 것을 증명할 수 있다. SSI는 개인에게 데이터 주권과 프라이버시 보호를 동시에 제공할 수 있다[2].

한편, BMW나 포드 등 주요 자동차 제조사는 블록체인 기반 DID를 적용하여 차량의 변조 및 유지 관리 내역을 기록하며 확인할 수 있는 자동차 출생증명서를 도입할 계획이다[1]. 그러나 블록체인에 차량의 주행 정보나 통신 정보 등에 대한 프라이버시 정보 노출의 위험은 여전히 존재한다. 여기서 유의할 점은 DID를 사용하면 익명성이 제공될 것으로 생각할 수 있으나, 정확하게는 다른 정보와 결합하면 식별이 가능한 가명성이 제공되는 것이다. 예를 들어 하나의 차량에 장기적인 가명(DID)을 사용하여 데이터를 저장한다고 가정하자. 누군가 악의적으로 동일한 차량의 DID로 저장된 데이터를 수집한 다음, 데이터 간에 연결점(linkability)을 찾아 차량을 특정할 수 있는 것이다. 따라서 차량용 DID를 위해 익명성을 제공할 수 있는 기술적인 대응 방안이 필요하다.

차량 프라이버시 보호를 위해 중요하게 다루어야 할 데이터는 차량 식별자, 운전자 식별 정보, 주행 정보, 위치 정보, 통신 정보 등이 있다. 특히, 주행 중인 차량의 위치 정보를 연속으로 획득하여 차량의 동선을 파악할 수 없도록 해야 한다. 차량통신 표준인 WAVE(Wireless Access in Vehicular Environment)에서는 차량 익명성을 제공한다. 차량의 장기 식별자인 VIN(Vehicle Identification Number)을 사용할 경우, 의도와 무관하게 유·무선상의 데이터를 수집하고 분석하면 차량을 특정할 수 있어 프라이버시가 침해될 수 있다. 이를 고려하여 짧은 기간에 유효한(short-lived) 인증서의 공개키를 단기 식별자로 사용하여, 동일 차량으로부터 수집한 메시지들을 서로 연결하기 어려운 비연결성(unlinkability)을 제공한다[3].

본 논문에서는 차량용 DID에 익명성을 제공하여 프라이버시 보호 수준을 높일 수 있는 기법을 제안하였다. 차량은 소유권을 증명할 수 있고 짧은 유효기간을 가진 단기 DID를 사용하여 익명성을 제공한다. 차량용 단기 DID를 효율적으로 생성하고 관리하기 위해, 차량통신에서 사용하는 단기 인증서의 공개키를 단기 DID를 생성하는 데 활용한다. 단기 DID를 적용하기 때문에 동일한 차량으로부터 수집한 메시지 간에 연결을 어렵게 하여 익명성을 제공하는 것이다. 또한, 추후 차량에 분쟁이 발생하였을 때를 대비하여, 차량통신과 연동하여 단기 DID로부터 장기 DID를 매핑할 수 있는 추적성(traceability)을 제공한다.

본 논문의 구성은 다음과 같다. 서론에 이어 2장에서는 관련 연구로 차량통신에서의 익명성 제공 기술, 차량에 블록체인과 DID를 적용한 관련 연구, 하이퍼레저 인디를 소개한다. 3장에서는 제안한 차량용 단기 DID를 설계하고, 4장에서는 하이퍼레저 인디를 기반으로 한 구현 구조를 설계한다. 5장에서는 구현한 소프트웨어의 기본적인 성능을 분석하고 마지막으로 결론을 맺는다.

Ⅱ. 관련 연구

2.1 WAVE 표준의 익명성

WAVE에서는 차량의 익명성을 보장하기 위해서 유선의 X.509와 같은 장기 인증서를 사용하지 않고, 차량통신 전용의 공개키 방식의 단기 인증서를 사용한다[3]. 만약, 차량통신 메시지에 전자서명과 검증을 위해 X.509 인증서가 첨부된다고 가정해보자. 인증서의 소유자(subject name)가 공개되므로 연속된 메시지를 수집하면 메시지 간에 연결점을 찾고 해당 차량의 주행 경로를 추적할 수 있다. 이를 막기 위해 차량통신에서는 단기 인증서를 적용하고 자주 변경시킴으로써 차량을 추적하기 어렵게 한다. 인증서는 1주일에

PSYNYM-Provider ID	PSYNYM Lifetime
Public Key (Pseudonym)	
Public-Provider Signature	

그림 1. WAVE 인증서
Fig. 1. WAVE Certificate

20개의 셋을 리필하고, 5분마다 하나의 인증서를 사용하도록 권고하고 있다[4]. 한 셋에 포함된 인증서의 수는 익명성 제공 수준에 따라 결정할 수 있다. 본 논문에서 활용하고자 하는 WAVE 인증서는 그림 1과 같이 공개키와 발급자의 서명 값이 첨부되어 있다.

2.2 차량용 블록체인

전 세계 주요 자동차 회사의 약 70%가 MOBI(Mobility Open Blockchain Initiative)라는 컨소시엄을 구성하고, 블록체인을 기반으로 차량용 ID 단일화, 실시간 교통정보나 차량의 주행 데이터를 공유, 수집된 데이터를 거래할 수 있는 데이터 마켓 구축 등을 추진하고 있다[1]. 차량통신에 블록체인을 적용하는 관련 연구로, LEI 등[5]에서는 다수의 기지국 단위의 도메인을 관리하는 SM(Security Manager) 노드들을 블록체인으로 연결한다. 블록체인에서 인증서를 셔플링하여 재사용하고 인증서 취소에 활용한다. Noureddint Lasla 등[6]에서는 기지국들을 블록체인 노드로 연결하고, 블록체인을 통해 차량간 인증을 수행한다. 기지국은 차량 대신에 블록체인 연산을 수행하여 차량의 연산 처리부하를 줄인다. Ze Wang 등[7]에서는 차량통신에서 발급되는 인증서와 인증서 취소목록을 블록체인에 기록하여 인증서 발급과 취소 정보를 투명하고 공개적으로 관리한다.

2.3 차량용 DID 확산

DID가 자동차나 운전자의 소유 증명이나 신원 증명에 접목되고 있다. DID를 식별자로 사용하는 MOBI에서는 차량통신 네트워크의 계층적 구조를 고려하여 로컬 DID와 글로벌 DID를 두고 상호 연동한다. Manas P. B 등[8]에서는 SSI를 활용하여 보호해야 할 데이터에 민감도를 매겨 관리하는 모델을 제시하였으며, 피어 SSI 엔티티들 간에 중간자 공격을 완화할 수 있도록 하였다. 국내에서는 '블록체인 기반 자율주행차 신뢰 플랫폼 구축' 시범사업을 통해 DID 기반 V2X(Vehicle to Everything) 통신의 인증서비스를 제공할 계획이며, 제시한 DID 구조는 그림 2와 같다[9]. 차량-차량, 차량-관제센터, 차량-서비스 간 송수신되는 정보에 대한 보안을 강화하고, 위변조가 불가능한 스마트 컨트랙트(Smart Contract) 기반 자율주행 블록체인 플랫폼을 통해 실시간 공유되는 자율주행 정보에 대한 신뢰성을 보장한다. 운전자의 DID와 차량의 DID는 각각 별도의 식별자로 사용하며, 차량의 운행정보는 블록체인에 저장된다.

DID의 참여 주체는 크게 발행기관(Issuer), 정보주체 Holder), 검증기관(Verifier)으로 구성된다. 발행기관은 정보주체가 요구하는 증명서를 발급하는 기관이다. 정보주체는 DID가 지칭하는 실제 객체를 의미한다. 사람이 될 수도 있고, 특정 기관, 사물 등이 될 수 있다. 검증기관은 주체가 제출하는 증명서를 검증하는 기관으로, 정보주체가 교통정보센터, 소방서, 경찰서, 보험사, 교통정보 활용 포털 서비스 업체 등에 제출하는 증명서의 진위를 검증해주는 DID 서비스 제공자로, 기업이나 기관이 될 수 있다. 블록체인은 DID와 관련된 모든 데이터를 신뢰성 있게 저장하는 저장소이다. 이 외에 DID 컨트롤러(Controller)는 정보주체의 인증을 대행해주거나 DID에 연결된 문서를 변경해주는 역할을 대행한다.

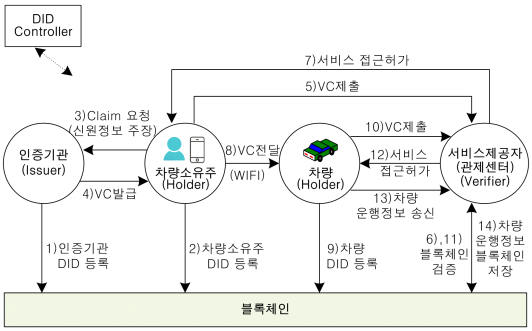

그림 2. V2X를 위한 DID
Fig. 2. DID for V2X Communications

2.4 하이퍼레저 인디

분산원장 구현을 목표로 하는 초기의 하이퍼레저 패브릭은 탈중앙화된 식별자를 구현하는 데 한계가 있었다. 이를 고려하여 도입된 하이퍼레저 인디(Hyperledger Indy)는 분산원장을 처리하는 블록체인 노드들에게 독립적인 식별자를 제공할 수 있으며, 관련된 도구, 라이브러리, 재사용 가능한 요소들을 제공한다[10]. 따라서 하이퍼레저 인디는 DID를 구현하는 데 적합하다. 특히 식별자와 관련된 인증에 특화된 패브릭이며, 분산된 환경에서 약속된 암호화 체계를 통해서만 인증이 가능하므로 신뢰성을 높일 수 있다. DID는 설명하고자 하는 개체, 식별자에 대한 공개키, 서비스 등을 JSON 개체로 표현한다.

Ⅲ. 제안한 기법

3.1 설계 원칙

제안한 기법의 주요 목표는 블록체인 기반의 DID를 사용하는 환경에서 차량의 익명성을 제공하는 것

이다. 이를 위해 차량의 소유 증명이나 신원 증명과 차량 익명성을 제공하기 위해 짧은 유효기간을 가진 단기 DID를 사용한다. 따라서 동일한 차량으로부터 수집한 메시지 간에 연결을 어렵게 하여 익명성을 제공하는 것이다. 설계 원칙은 아래와 같다.

□ 단기 DID 발급과 삭제 등 관리가 효율적이어야 한다. 이를 위해 차량통신 WAVE 시스템에서 사용하는 단기 인증서를 제공받아 제안한 기법에서 활용한다.
□ 차량 정보의 주인이 블록체인에 저장된 정보 중, 응용서비스에 따라 꼭 필요한 정보만을 선택하여 제삼자에게 제공할 수 있어야 한다.
□ 블록체인에는 차량의 운행정보, 사고 정보, 교통정보 등 차량과 관련된 모든 정보가 트랜잭션 형태로 저장되며, 트랜잭션의 식별자로 단기 DID를 사용한다.
□ 추후 차량에 분쟁이 발생하였을 때를 대비하여, 블록체인에 저장된 단기 DID와 차량을 매핑하는 추적성을 제공해야 한다.

3.2 단기 DID 설계

단기 DID는 짧은 주기로 발급과 삭제 그리고 관리되어야 하므로 계산 부하가 매우 커질 수 있다. 만약 통신할 때마다 매번 새로운 DID를 사용한다면 매우 높은 수준의 비연결성을 제공할 수 있으나 성능저하와 고비용이 요구되어 비효율적이다. 이를 고려하여 제안한 기법에서는 차량통신에서 사용하는 인증서의 공개키를 시드로 하여 단기 DID를 발급하고 활용한다. 즉, 차량통신에서 인증서가 짧은 주기로 변경되어 사용된다는 점에 착안하여, 인증서 공개키를 시드로 하여 단기 DID를 만들어 사용하는 것이다. 따라서 기본적으로 차량통신에서 제공하는 익명성 수준을 제공한다. 단기 DID를 발급하는 방법은 인증서의 공개키 첫 16바이트를 그대로 사용한다. 차량통신에서는 인증서가 주기 t(ex; 5분)마다 변경되므로 이를 이용해 t, $2t$, $3t$,..nt와 같이 원하는 만큼 주기를 늘려서 단기 DID를 발급한다. 즉, 익명성 제공 수준에 따라 DID 발급 주기를 변경하여 설정할 수 있도록 한다.

추후 차량에 분쟁이 발생하여 차량을 추적할 필요가 있을 때는 블록체인에 저장된 단기 DID와 차량을 매핑하는 작업이 필요하다. 본 논문에서는 WAVE에서 이 기능을 수행하는 MA(Misbehavior Authority)와 연동을 통해 처리하는 것으로 가정한다.

3.3 기본 절차 설계

이 절에서는 W3C DID 표준문서[11]를 기초로 하여 제안한 기법의 기본적인 절차를 설계한다. 발급자인 CA(Certificate Authority)는 DID에 필요한 신원, 소유, 자격 증명을 발행하며, DID의 소유자는 차량이며, SP(Service Provider)는 검증 기관, DID 컨트롤러는 차량의 DID 연산 부하를 줄이기 위해 차량을 대신한 연산을 하는 엔티티이다.

단기 DID(short-term DID; 이하 sDID)의 발급과 검증 흐름을 그림 3에 나타내었다. (1) 차량통신 WAVE 시스템으로부터 인증서가 변경된다. (2) 차량은 컨트롤러에게 인증서의 공개키를 전달하면서 sDID를 발급받는다. (3) CA에게 VC(Verifiable Credentials) 발급을 요청한다. (4) CA는 VC를 발급한다. (5) CA는 발급된 VC 정보 ($sDID$, $issuer's\ P_k$)를 블록체인에 저장한다. (6) 차량의 인증서 공개키($pseudonym$)가 지정된 sDID를 블록체인에 저장한다. (7) 이후, 검증자인 SP가 차량의 sDID를 검증할 때, VP(Verifiable Presentations)를 요청한다. (8) VP를 제출함과 동시에 DID 컨트롤러에게 sDID Auth를 요청한다. (9) 컨트롤러는 차량 대신에 sDID Auth를 대행한다. (10) 차량의 sDID가 인증되면 SP는 블록체인으로부터 그 차량의 sDID 문서를 획득하여 Proof를 검증한다. 검증에 성공하면 SP는 해당 sDID에 연관된 인증서를 확인할 수 있다. (11) 추후, 분쟁이 발생할 때 WAVE 시스템과 연동하여 인증서로부터 차량을 추적한다.

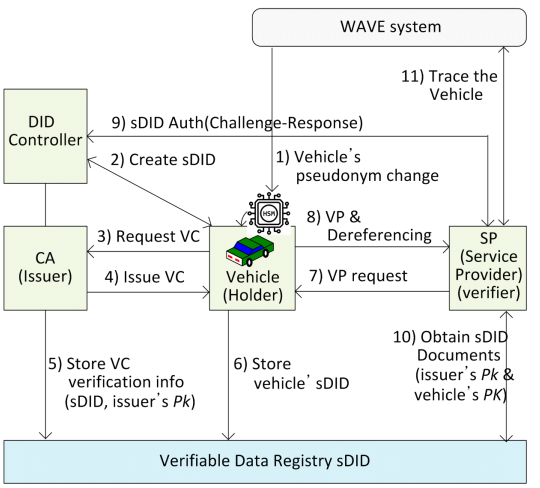

그림 3. sDID를 위한 VC 발급 및 검증
Fig. 3. VC Issue and Verify for sDID

3.4 VC와 DID 문서 설계

차량에서 사용하는 VC는 응용서비스가 제공하는 서비스 특징에 따라 다양한 형태를 가질 수 있다. 제안한 기법의 VC를 그림 부록-1에 나타내었다. VC의 차량정보에는 인증서의 공개키로 구성되며 더 많은 항목을 추가할 수 있다. VP를 구성할 때는 차량 응용서비스의 요구에 따라 VC에서 정의된 항목 중, 필요한 항목을 선택적으로 제공한다. 영지식증명을 적용하여 필요한 항목이 어떤 조건에 부합하는지만을 표현한다.

sDID Document는 차량이 해당 DID의 소유권을 가지고 있음을 증명할 수 있는 인증수단이 포함된다. 차량이 SP에게 did:sov:sdid_vehicle1이 자신의 sDID라고 주장하면, SP는 블록체인에서 차량의 sDID가 저장된 위치를 확인하여 sDID 문서를 획득한다. 이후, SP는 차량에게 해당 sDID가 그 차량의 sDID라는 것을 인증해보라는 Challenge-Response를 실행한다. Response를 수신한 SP는 차량의 문서에 포함된 공개키를 이용하여 요청자의 Response를 검증한다. 이 절차를 sDID Auth라 한다. DID 컨트롤러가 소유자인 차량을 대신해서 sDID Auth를 수행할 때는 그림 부록-2와 같이 컨트롤러를 지정해야 한다.

Ⅳ. 하이퍼레저 인디 블록체인 구현

분산원장기술에 독립적인 식별자를 지원하는 하이퍼레저 인디의 SDK[11]를 사용하여 제안한 기법을 구현하였다. 구체적인 절차는 문헌[12]을 참고하였으며, 그림 3에 표현된 DID Auth는 인증 주체가 DID 컨트롤러에서 CA로 변경될 수 있어 단순화하기 위해 구현에서는 제외하였다.

4.1 스키마와 크레덴셜 정의

CA가 VC 처리를 위해 셋업 과정을 시작하면서 VC의 내용을 스키마(schema) 형태로 등록한다. 스키마에는 VC의 요소들이 $m_1, m_2, \ldots, m_n$의 형태로 포함된다. 여기서 m_1과 m_2는 특별하게 지정되는데, m_1은 차량이 VC의 주인임을 증명할 수 있는 *link secret*이 지정되고, m_2는 revocation context가 지정된다. 스키마는 인디 노드의 *SCHEMA* 트랜잭션을 사용한다.

이후 CA가 크레덴셜 정의(credential definition)를 등록한다. 여기에는 어떤 스키마를 사용할지에 대한 정보, 해당 크레덴셜 정의로 발행된 VC 검증과 폐기

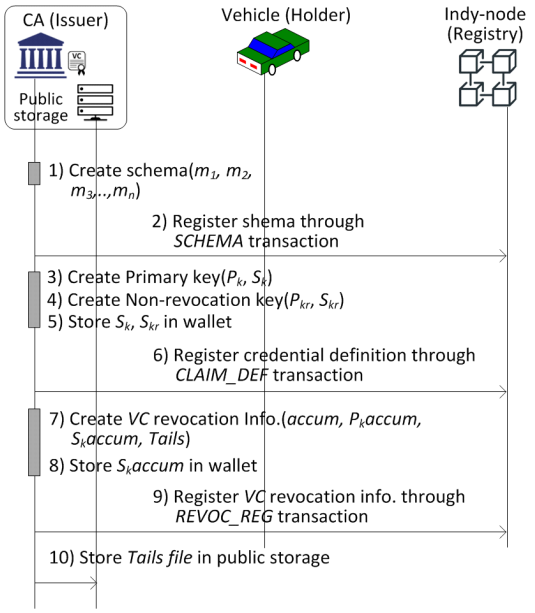

그림 4. 발행자 셋업 절차
Fig. 4. Issuer Setup Procedure

검증에 필요한 공개키가 포함된다. CA는 필요한 키 쌍을 생성한 후, 비밀키는 안전한 장소에 보관하고, 공개키는 크레덴셜 정의에 포함시켜 *CLAIM_DEF* 트랜잭션을 통해 블록체인에 등록한다.

CA는 크레덴셜 정의에 해당하는 VC 폐기 정보를 이용하여 자신의 VC가 폐기되지 않았음을 증명할 수 있는 데이터를 생성한다. 추후에 SP는 이 데이터를 근거로 수신한 VC가 폐기되었는지 검증할 수 있다. CA는 VC 폐기 정보를 담은 $accum$를 수정하고 VC 폐기 여부를 검증할 수 있는 키 쌍인 $P_k accum$과 $S_k accum$을 *REVOC_REG* 트랜잭션을 통해 블록체인에 등록한다. 이때 VC 폐기 목록의 원본 데이터인 *Tails file*은 블록체인에 등록하기에는 용량이 크므로 CA가 관리하는 공개 저장소에 따로 등록한다. *Tails file*이 위치한 URI도 *REVOC_REG* 트랜잭션에 포함되어 블록체인에 저장된다.

4.2 VC 발행

차량이 CA로부터 VC를 발행받는 과정이다. 차량은 나중에 영지식증명을 바탕으로 VC의 소유권을 증명할 때 사용하는 *link secret*을 생성한다. 발행하는 VC의 공개키 값들 즉, P_k, P_{kr}이 포함된 크레덴셜 정의를 블록체인으로부터 획득한다. 랜덤 값 $vPrime$과 $vrPrime$을 생성한 뒤, *link secret*,

P_k, P_{kr}, $vPrime$, $vrPrime$을 연산하여 *blinded secret*을 생성한다.

차량은 나중에 *blinded secret*에 매치되는 *link secret*를 알고 있음을 증명할 수 있으므로 VC에 대한 소유권을 증명할 수 있다. 마지막으로 차량은 CA에게 VC에 대한 소유권 증명을 위한 *blinded secret*과 발행받을 VC의 크레덴셜 정의를 발행인에게 전달하면서 VC 발행을 요청한다.

VC 발행 요청을 받은 CA는 차량 정보를 스키마에 채워 넣고, 발행할 VC 폐기 관리를 위해 *Tails file*에 정의된 인수 중 하나를 선택한다. 이후, 차량으로부터 받은 *blinded secret* 값과 블록체인으로부터 획득한 $accum$, P_kaccum, P_k, P_{kr}을 이용해 pre-VC와 pre-VC 폐기 증명을 생성한다. 폐기 정보에 새롭게 생성된 VC가 추가되었으므로 $accum$을 업데이트한 후, *REVOC_REGUPDATE* 트랜잭션을 통해 업데이트한 $accum$을 등록한다. 마지막으로 CA는 pre-VC, pre-VC 폐기 증명을 차량에게 전송하고, 차량은 $vPrime$과 $vrPrime$을 기초로 하여 pre-VC와 pre-VC 폐기 증명을 VC, VC 폐기 증명으로 업데이트한 후 자신의 지갑에 저장한다.

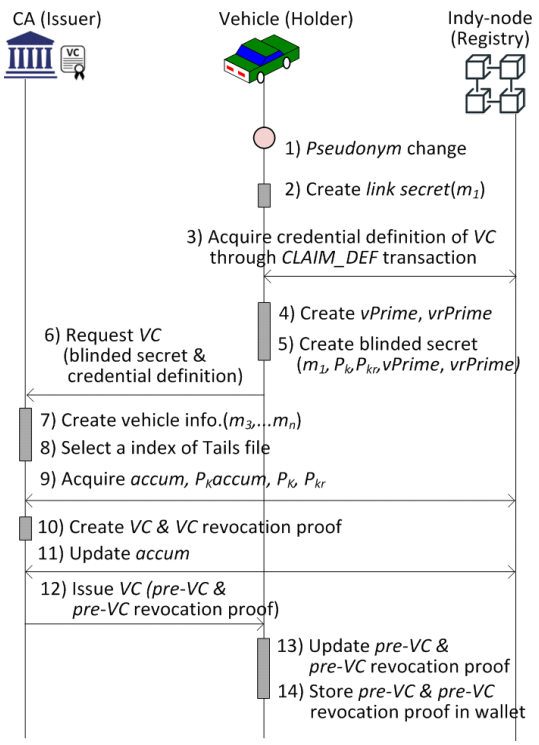

그림 5. VC 발행 절차
Fig. 5. VC Issue Procedure

4.3 VP 검증

SP가 차량에게 VP를 요청한다. SP가 원하는 VC에는 sDID 소유주로서 제공되는 인증서의 공개키 속성과 차량이 VP를 생성할 때 사용할 난스(nonce) 값이 포함된다. 이를 수신한 차량은 VP 생성을 위해 블록체인으로부터 P_k, P_{kr}, P_kaccum을 획득하고, CA의 공개 저장소로부터 *Tails file*을 획득한다. 이후, 획득한 값을 기초로 하여 SP가 요청한 sDID 속성만 확인할 수 있도록 VC를 VP로 가공한 후, VP를 전송한다. 마지막으로 SP는 VP 내에 포함된 VC에 해당하는 크레덴셜 정의와 VC 폐기 정보를 획득한 후, VP 검증을 완료한다.

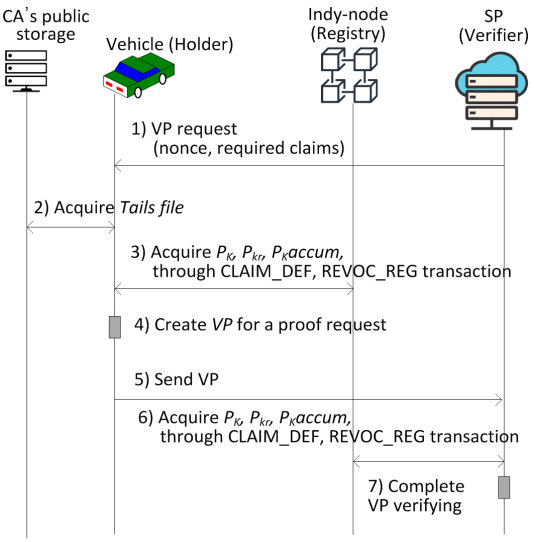

그림 6. VP 검증 절차
Fig. 6. VP Verify Procedure

V. 성능 분석 및 고찰

앞 장에서 설계하고 구현한 소프트웨어의 기본적인 성능을 측정·분석하였다. 성능은 초기 sDID를 발급하는 시간과 서비스 제공자에 의해 시작된 VP 검증 시간으로 분리하여 측정하였다. 구현환경은 다음과 같다.

- ☐ CPU : Intel(R) Core i7-9700 3.00GHz
- ☐ OS : Ubuntu 16.04TLS 64bits
- ☐ Library : Hyperledger fabric and indy, libsodium, libindy, indy crypto
- ☐ Database : rocksdb
- ☐ Num. of indy-node : 4(CA, vehicle, SP, orderer)

☐ Num. of channel : 1
☐ Chaincode language : go, java sscript, java

5.1 성능 측정

첫 번째 실험에서는 sDID 발급 횟수를 변화시켜 가면서 하나의 VC 발급과 VP 검증에 소요되는 평균 시간을 측정하여 Table 1에 나타내었다. VC 발급에는 평균 851.4ms가 소요되고, VP 검증에는 평균 85ms가 소요되었다.

이 실험에서는 블록체인을 구성하는 인디 노드의 수가 4개밖에 되지 않아, sDID가 증가하여도 VC 발급과 VP 검증시간에 크게 영향을 주지 않았다. 그러나 실제 운영 환경에서 블록체인의 노드의 수가 많아지면 이에 비례해서 증가할 것이다. 두 번째 실험에서는 VC 발급 횟수와 VP 검증 횟수를 증가시키고 소요시간을 측정하여 그림 7에 나타내었다. 첫 번째 실험과 유사하게 VC 발급이 VP 검증보다 약 10배 정도 선형적으로 증가한다. VC 발급에는 트랜잭션 생성, 합의 알고리즘 수행, 체인코드의 실행, 전자 서명 및 검증, 트랜잭션 쓰기 등으로 인해 VP 검증보다 더 많은 시간이 소요된다. 8,192개의 VC 발급에는 7,299sec가 소요되고, VP 검증에는 733sec가 소요되었다.

세 번째 실험에서는 VC 발급 횟수와 VP 검증 횟수를 1,024로 고정하고, sDID 문서의 데이터 사이즈를 10K 바이트에서 100K 바이트까지 변화시키면서 추이를 살펴보았다. 그림 8과 같이 VC 발급은 VP 검증보다 약 8.61배에서 13.3배까지 점진적으로 증가하는 반면, VP 검증에는 데이터 사이즈가 증가해도 일정한 시간이 소요되어 크게 영향을 주지 않는 것으로 나타났다.

표 1. VC 발행과 VP 검증에 소요되는 평균 시간
Table 1. Average Elapsed Time for VC Issue and VP Verify

Number of sDID	Throughput(msec)	
	Elapsed time per VC issue	Elapsed time per VP verify
64	826.6	87.2
128	839.3	84.7
256	841.2	86.0
512	837.5	84.4
1,024	855.0	81.5
2.048	862.9	82.8
4,096	857.3	83.7
8,192	891.0	89.5
mean avg.	851.4	85.0

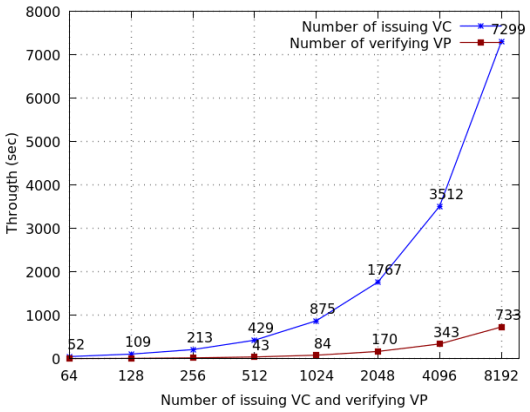

그림 7. VC 발행과 VP 검증 소요 시간
Fig. 7. Elapsed Time for VC Issue and Verify

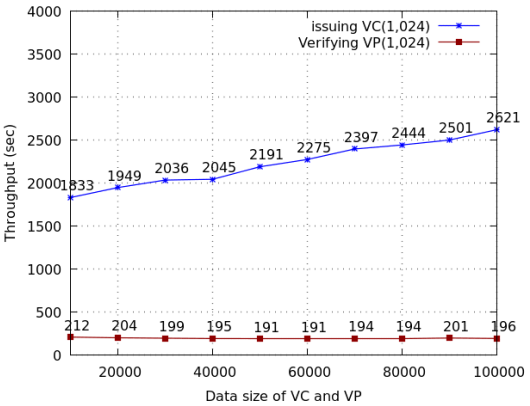

그림 8. 데이터 크기에 따른 VC 발행과 VP 검증 소요 시간
Fig. 8. Elapsed Time for VC Issue and Verify according to Data Size

5.2 기능 분석

설계한 기법을 구현하고, 주요 기능인 WAVE로부터의 단기 공개키 획득, 차량에서 DID 생성, CA를 통해 VC 발급, 하이퍼레저 인디에 정보 저장, 서비스 제공자의 VP 검증 요청과 검증이 이루어지는지 확인하였다. 또한 VC와 VP 검증에 소요되는 시간을 측정한 결과, 본 논문에서 제공하고자 하는 기능들이 정상적으로 동작하고 실현 가능성이 있음을 확인하였다.

Ⅵ. 결 언

본 논문에서는 블록체인 기반의 DID를 사용하는 환경에서 차량의 익명성을 제공하여 프라이버시를 보

호할 수 있는 기법을 제안하였다. 제안한 아이디어의 실현 가능성을 검증하기 위해 W3C DID 표준문서를 기초로 하여 필요한 DID 발급 절차와 검증 절차를 설계한 후, 하이퍼레저 인디의 SDK를 사용하여 구현하였다. 그리고 기본적인 성능을 측정하였다.

제안한 기법에서는 차량의 소유 증명이나 신원 증명을 할 수 있는 짧은 유효기간을 가진 단기 DID를 사용한다. 차량통신에서 인증서가 짧은 주기로 변경되어 사용된다는 점에 착안하여, 인증서 공개키를 시드로 하여 단기 DID를 만들어 사용한다. 이를 통해 기본적으로 차량통신에서 제공하는 익명성 수준을 동일하게 제공할 수 있다. 그리고 영지식증명을 적용하여 정보의 주인이 블록체인에 저장된 정보 중, 응용서비스에 따라 꼭 필요한 정보만을 선택하여 제삼자에게 제공할 수 있다. 또한 추후 차량에 분쟁이 발생하였을 때를 대비하여, 블록체인에 저장된 단기 DID로부터 차량을 특정할 수 있는 추적성을 제공한다.

References

[1] https://dlt.mobi

[2] S. Lee, et al., "Trends and analysis of blockchain privacy protocols," *J. KICS*, vol. 44, no. 12, pp. 2252-2259, Dec. 2019.

[3] IEEE 1609.2-2016, "*IEEE standard for wireless access in vehicular environments-security services for applications and management messages*," IEEE Standard, Mar. 2016.

[4] I. Saini, et al., "Evaluating the effectiveness of pseudonym changing strategies for location privacy in vehicular ad-hoc network," *Wiley Secur. and Privacy*, pp. 1-13, May 2019.

[5] A. Lei, et al., "A blockchain-based certificate revocation scheme for vehicular communication systems," *ELSEVIER Future Generation Comput. Syst.(online available)*, Apr. 2019.

[6] N. Lasla, et al., "Efficient distributed admission and revocation using blockchain for cooperative ITS," in *Proc. NTMS*, pp. 1-5, Feb. 2018.

[7] Z. Wang, et al., "Blockchain-based certificate transparency and revocation transparency," *Financial Cryptography and Data Secur., Spring Berlin Heidelberg*, pp. 144-162 Mar. 2019.

[8] M. P. Bhattacharya, et al., "Enhancing the security and privacy of self-soverign identities on hyperledger indy blockchain," in *Proc. ISNCC*, Montreal, QC, Canada, Dec. 2020.

[9] https://www.boannews.com/media/view.asp?idx=88077

[10] https://hyperledger-indy.readthedocs.io/projects/ sdk/en/latest

[11] https://www.w3.org/TR/did-core

[12] D. Yoon, "Analysis report of self-soverign identities," *Jpub Press book*, www.jpub.kr, Jul. 2020.

김 현 곤 (Hyun-gon Kim)

1992년 2월 : 금오공과대학교 전자공학과 졸업

1994년 2월 : 금오공과대학교 전자공학과 공학석사

2003년 8월 : 충남대학교 전자공학과 공학박사

1994년~2005년 : 한국전자통신연구원 정보보호연구단 선임연구원

2005년 3월~현재 : 목포대학교 정보보호학과 교수

2011년 8월~2013년 7월 : University of Delaware 방문교수

<관심분야> 차량통신 보안, 이동통신 보안, 인공지능 보안

[ORCID:0000-0003-2619-5582]

Verfiable Credential for sDID


```
{
  "@context": [
     "https://www.w3.org/2018/credentials/v1"
     "https://www.koreadmv.org/context"
  ],
  "id": "did:sov:sdid_vehicle1",
  "type": ["VerifiableCredential", "VehicleCredential",
  "issuer": "did:sov:koreadmv1",
  "issuanceDate": "2021-01-01T09:00:00Z",
  "expirationDate": "2022-01-01T09:00:00Z",
  "credentialSubject": {
    "id": "did:sov:sdid_vehicle1",
    "vehicleInfo": {
        "PseudonymPk" : "69156193594462789135"
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2021-01-01T09:00:00Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:vehicle:koreadmv1/keys/1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI ……"
    }
}
```


그림 부록-1. 검증 가능한 크레덴셜의 예
Fig. Appendix-1. An Example of Verifiable Credential

sDID Document


```
{
  "@context": "https://www.w3.org/2018/credentials/v1",
  "id": "did:sov:sdid_vehicle1",
  "authentication": [ {
     "id": "did:sov:sdid_vehicle1#keys-1",
     "type": "RsaVerificationKey2018",
     "controller": "did:sov:sdid_controller1",
     "publicKeyPem": "-----BEGIN PUBLIC KEY …END
                          PUBLIC KEY-----\r\n"
    } ],
   "service": [ {
     "id": "did:sov:sdid_vehicle1",
     "type": "VefifiableCredentialService",
     "serviceEndpoint": "https:koreadmv1.org/vehicle"
   } ]
}
```


그림 부록-2. 검증 sDID 문서의 예
Fig. Appendix-2. An Example of sDID Document