KIPS Trans. Comp. and Comm. Sys.
Vol.9, No.12 pp.315~320
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2020.9.12.315

A Decentralized Face Mask Distribution System Based on the Decentralized Identity Management

Siwan Noh† · Seolah Jang†† · Kyung-Hyune Rhee†††

ABSTRACT

Identity authentication is an important technology that has long been used in society to identify individuals and provide appropriate services. With the development of the Internet infrastructure, many areas have expanded into online areas, and identity authentication technologies have also expanded online. However, there is still a limit to identity authentication technology that relies entirely on trusted third parties like the government. A centralized identity management system makes the identification process between agencies with different identity management systems very complex, resulting in a waste of money and time for users. In particular, the limits of the centralized identity management system were clearly revealed in the face mask shortage in the 2020 COVID-19 crisis. A Decentralized Identity (DID) is a way for users to manage their identity on their own, and recently, a number of DID platform based on blockchain technology have been proposed. In this paper, we analyze the limitations of the existing centralized identity management system and propose a DID system that can be utilized in future national emergency situations such as COVID-19.

Keywords : Blockchain, Decentralized Identity, Identity Authentication

블록체인 분산신원증명에 기반한 탈중앙화된 마스크 중복구매 확인 시스템

노 시 완† · 장 설 아†† · 이 경 현†††

요 약

신원인증은 오래전부터 사회에서 개인을 식별하고 그에 맞는 서비스 등을 제공하기 위해 사용되던 중요한 기술이다. 인터넷 인프라의 발전으로 사회의 많은 부분이 온라인 영역으로 전환되며 신원인증 기술 또한 온라인으로 확장되었다. 하지만 여전히 신원인증 기술은 정부와 같이 신뢰하는 제3의 기관에 전적으로 의존하고 있다는 한계가 있다. 중앙화된 신원관리체계는 서로 다른 신원관리체계를 운용하는 기관 사이의 신원인증 과정을 매우 복잡하게 만들고 비용·시간적으로도 매우 비효율적으로 만들고 있다. 특히 2020년 코로나 바이러스로 인한 마스크 품귀 사태에서 사용된 중복구매 방지 시스템의 구축과정에서 중앙화된 신원관리체계의 한계가 여실히 드러났다. 분산신원증명은 사용자 스스로 자신의 신원정보를 관리하는 방법으로 최근에는 블록체인기술을 사용한 분산신원증명 기술이 다수 제안되고 있다. 본 논문에서는 기존의 중앙화된 신원관리체계의 한계를 분석하고 차후 코로나 바이러스와 같은 국가적인 비상상황에서 사용가능한 분산신원증명 시스템을 제안한다.

키워드 : 블록체인, 분산신원증명, 신원인증

1. 서 론

신원(Identity)은 개인을 식별할 수 있는 정보로서 국내에서는 주로 주민등록번호, 운전면허번호, 여권번호 등 정부의 인가된 발급기관이 개인 식별자(Identifier)와 함께 개인의 정보(이름, 주소 등)인 속성(Attribute)을 플라스틱 카드 등의 형태로 발급한 오프라인 신분증을 신원인증의 수단으로 사용하고 있다. 하지만 인터넷 산업의 발전으로 온라인을 통한 신원 인증의 필요성이 제기되자 정부는 2000년대 초 전자정부법과 함께 온라인에서의 신원인증 수단인 전자서명을 도입하고 개인의 키(Key)를 정부 기관(금융결제원)이 발급하고 관리하는 공인인증서 제도를 도입하였다. X.509 인증서 관리 표준을 따르는 공인인증서는 사용자마다 고유한 비밀키, 공개키 쌍을 생성하고 이 공개키와 사용자의 신원을 공인인증기관이 인증한 정보를 포함하고 있다. 온라인에서의 신원인

※ 본 연구는 과학기술정보통신부 및 정보통신기기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었으며(IITP-2020-2015-0-00403) 일부는 2019학년도 부경대학교 연구년 교수 지원사업에 의하여 연구되었음(C-D-2019-0318).
※ 이 논문은 2020년 한국정보처리학회 춘계학술발표대회에서 "블록체인 분산신원증명에 기반한 공적마스크 중복구매 확인 시스템에 대한 연구"의 제목으로 발표된 논문을 확장한 것임.
† 준 회 원 : 부경대학교 정보보호학과 박사과정
†† 준 회 원 : 부경대학교 인공지능융합학과 석사과정
††† 종신회원 : 부경대학교 IT융합응용공학과 교수
Manuscript Received : August 3, 2020
Accepted : August 21, 2020
* Corresponding Author : Kyung-Hyune Rhee(khrhee@pknu.ac.kr)

증은 사용자가 비밀키를 사용한 전자서명을 생성하고 이를 정부가 공인한 인증서에 포함된 공개키로 검증함으로서 이루어진다.

이렇듯 사용자들의 모든 신원정보와 인증수단을 정부가 관리하는 중앙화된 신원 관리 체계는 높은 안전성과 효율성을 보장해줄 수 있다. 하지만 중앙화된 신원 관리 체계는 사용자가 자신의 신원정보에 새로운 속성 정보를 추가하거나 기존의 속성을 변경하는 것에 많은 제약사항을 만들 수 있다. 예로 국내의 신원 관리 체계에서는 관리체계에서 보장하는 속성의 범주 내에서는 관련 기관을 통해 속성의 추가 및 변경이 가능하다(주소지 이전, 주민등록번호 변경, 혼인신고 등). 하지만 이는 신원 관리 체계 시스템의 구축 당시 예상한 속성의 추가 및 변경 건에 대해서만 지원이 가능하고 이후 발생하는 특수한 사례를 지원하는 속성의 추가에는 모든 유관기관의 시스템을 업데이트해야 하는 등의 많은 어려움이 존재한다.

대표적인 예로 2020년 초, 코로나 바이러스 감염증(COVID-19)의 유행으로 인한 마스크 품귀 현상으로 인해 한시적으로 시행된 공적마스크 판매 사례가 있다[1]. 공적마스크 판매제도는 부족한 마스크 공급 상황에서 각계각층에 마스크의 공정한 분배를 위해 정부가 마스크 판매과정에 개입하여 일주일에 공적채널을 통해 구입 가능한 마스크의 수를 제한하는 제도이다. 정부는 시민들에게 새로운 속성인 마스크 구매 여부를 부여하고 마스크 구매 시 신원인증을 통해 이 속성을 검증하고자 하였다. 하지만 기존의 신원관리체계에서 새로운 속성을 추가하는 것은 어려웠고 결국 건강보험심사평가원에서 운용하던 HIRA 시스템을 통해 구매여부 확인 후 마스크를 구매할 수 있도록 하였다. 하지만 마스크 품귀현상이 발생하기 시작한 1월 말에서 약 한 달이 지난 3월 초에서야 제도가 도입되거나 외국인등록증 소지 및 건강보험 가입자 제한으로 인한 주한외국인의 구매는 약 2개월 후인 4월 말 5부제 적용이 완화되는 시점에서야 이루어지는 등 유연하지 못한 신원관리체계로 인한 문제가 두드러졌다.

본 논문에서는 블록체인기술을 사용하여 사용자가 스스로 자신의 신원정보를 관리할 수 있는 분산신원증명 시스템을 제안한다. 제안하는 분산신원증명 시스템은 마스크 중복구매 여부와 같이 기존의 신원관리체계에서 지원하지 않는 사용자의 속성을 사용자 스스로 자신의 신원정보로 등록하고 관리할 수 있도록 지원하고 이를 쉽게 검증할 수 있는 신원관리체계이다.

2. 관련 연구

2.1 공적마스크 판매제도

2020년 초, 코로나 바이러스 감염증으로 인해 시장의 보건용 마스크 수요가 폭증, 공급량이 부족해지며 마스크 품귀현상이 발생하였다. 이를 해결하기 위해 정부는 국내 마스크 생산량의 일부를 공적 물량으로 확보하여 의료기관과 감염병 특별관리지역 등에 우선배분하고 나머지는 공적판매처를 통해 판매하고자 공적마스크 제도를 시행하였다. 2020년 2월 26일 마스크 및 손소독제 긴급수급 조정조치로 공적 채널을 통한 판매를 시작하였다. 하지만 중복 구매 등 마스크 분배문제가 제기되자 같은 해 3월 5일 마스크 수급 안정화 대책을 발표하고 9일부터 공적 채널을 통해서는 일주일에 2개의 마스크만을 구입할 수 있도록 하는 공적 마스크 5부제를 도입하였다. 5부제는 마스크 생산이 확대되어 수요가 안정되는 같은 해 7월 12일까지 약 5개월간 시행되었다.

서울특별시약사회 정책위원회가 실시한 설문조사에 따르면 공적마스크가 마스크 공급 안정 및 코로나 바이러스 감염증 예방에 크게 기여하였다고 생각한다는 결과가 나왔다. 마스크 분배 문제가 해결되지 못했다면 안정적인 감염병 관리가 이루어지지 못했을 것이라는 의미이지만 5부제는 국내에서 확진자가 폭증하는 시점인 2월 중순에서 약 2주가 넘게 지난 3월 9일에 시작되었다. 즉, 이렇듯 감염병 관리에 중요한 역할을 수행하는 제도가 신속하게 도입되지 못했는데 이는 마스크 중복구매방지를 위한 전산시스템 구축의 어려움에서 기인한다.

최초 정부는 마스크의 중복구매를 방지하기 위해 기존에 건강보험심사평가원에서 약물의 오남용이나 잘못된 처방으로 인한 부작용을 막기 위해 약사가 손님이 이미 처방받은 내역을 확인할 수 있도록 하는 의약품안전사용 서비스(Drug Utilization Review, DUR)[2]를 기반으로 중복구매를 방지하는 시스템을 구축하고자 하였다. 하지만 이 경우 판매채널이 제한되고 시스템 과부하 등의 실효성 문제로 건강보험심사평가원의 HIRA 시스템의 요양기관업무포털에 공적마스크 판매이력 관리시스템을 추가하여 운영하게 되었다[3]. 요양기관업무포털은 건강보험의 심사 및 평가와 관련된 데이터를 수집·처리·분석·활용할 수 있는 응용시스템으로 판매이력 관리시스템은 건강보험 가입자 정보와 등록된 마스크 구매기록을 기반으로 중복구매 여부를 검증하게 된다. 여기서 검증자(판매자)는 정부로부터 인가된 판매자(약사 등)로 한정되며 공인인증서를 통해 판매이력관리시스템에 로그인하여 중복구매 여부를 검증하고 마스크 판매 후 구매자의 구매여부를 갱신한다.

하지만 5부제의 운용과정에서 중앙화된 시스템으로 인한 중복구매방지시스템의 한계를 보였다. 문제는 크게 시스템의 유연성, 가용성으로 정의할 수 있다. 시스템의 유연성은 시스템이 다양한 상황에서 유연하게 대응할 수 있는지를 나타내고 가용성은 시스템이 정상적으로 사용 가능한 정도를 의미한다. 공적마스크 판매이력 관리시스템은 외국인 및 대리구매 문제에 대해 기존 시스템 변경의 어려움 등으로 빠른 대처를 하지 못해 시스템의 유연성의 한계를 보여주었다. 또한 우체국 등 판매처의 확장으로 인한 접속 과부하로 시스템 가용성이 저하되는 문제가 발생했다. 실제로 마스크 중복구매 확

인 시스템 구축 전 포털 시스템 일별 최대 시간당 동시사용자 수는 348~360명, 일 누적 호출건수는 1,445,903~1,523,651건 이였으나 구축 후 일별 최대 시간당 동시사용자 수는 5,829~7,060명, 일 누적 호출건수는 25,310,646~29,567,602건으로 20배 이상 증가하여 이후 3차에 걸친 서버 증설 조치를 취했다. 건강보험심사평가원에서는 시행된 중복구매 확인시스템의 문제를 인지하고 코로나19 위기대응지원 마스크 중복구매 확인시스템 구축 용역사업을 통해 이러한 문제를 해결한 새로운 시스템의 구축을 추진 중이다.

2.2 분산신원증명

전통적인 신원인증 기술은 신뢰하는 기관(Trusted Third Parity, TTP)이 사용자에게 발급한 신원인증 수단(신분증, 공인인증서 등)을 기반으로 이루어져왔다. 하지만 현존하는 대부분의 중앙관리 신원관리체계는 대표적으로 다음과 같은 문제점을 지니게 된다.

- **상호운용성:** 신원의 발급 기관마다 다른 신원관리체계를 사용하는 경우 서로 다른 신원관리체계 간의 신원인증은 제한적이거나 불가능하다.
- **사용자제어:** 한번 발급받은 신원인증 수단에 포함된 속성들은 인증 시 선택적으로 노출시키는 것이 제한적이거나 불가능하다.
- **유연성:** 발급된 신원인증 수단에 새로운 속성을 추가하거나 기존의 속성을 제거하는 것은 제한적이거나 불가능하다.

본 논문에서 다루는 블록체인 기술 기반의 분산신원증명(Decentralized Identity, DID)은 중앙화된 신원관리체계에서 벗어나 사용자 중심의 신원관리체계로서 제안되었다[4-7]. DID는 탈중앙화된 플랫폼인 블록체인 상에서 신원관리체계를 구축한 것으로 TTP 없이 사용자 스스로 자신의 개인키를 사용하여 자신의 신원정보를 관리할 수 있다. 최초로 이 개념을 구현한 것이 탈중앙화된 DNS 서버로서 제안된 네임코인(Namecoin)[4]이다. 네임코인은 누구든지 자신의 개인키로 웹사이트 IP(신원정보)와 도메인네임(속성)을 정의하고 필요하다면 다른 사용자와 도메인네임을 거래할 수 있는 것이 특징이며 이 모든 과정이 TTP 없이 사용자들 사이에서만 이루어진다. 최근에는 이를 실제로 신원증명에 적용하는 기술들이 제안되었는데 Paul과 Fabien은 분산신원증명 개념에 블록체인을 적용한 기술들[5-7]을 분석하고 이들을 다음과 같은 두 분류로 구분하였다[8].

- **자기주권신원(Self-Sovereign Identity):** TTP의 참여 없이 사용자가 스스로 자신의 신원과 속성을 정의하고 관리함
- **분산된 신뢰신원(Decentralized Trusted Identity):** 기존에 TTP가 발급한 신원(주민등록증, 여권 등)에 대해 탈중앙화된 방식의 검증 서비스를 제공함

Sovrin은 자기주권신원 형태의 분산신원증명 플랫폼으로 서비스제공자에 의해 인증된 참여자들만 참여 가능한 허가형 블록체인(Permissioned blockchain)상에 구현된 오픈소스 프로젝트이다[5]. 일반 사용자들이 단말 클라이언트를 통해 자신의 신원정보(식별자, 공개키, 메타데이터)를 관리하고 이 정보를 신뢰하는 기관들(은행, 대학, 정부 등)의 합의에 기반하여 블록체인 데이터베이스에 기록한다. 사용자는 여러 키를 사용하여 복수의 식별자-속성 조합의 신원정보를 사용할 수 있다. uPort는 분산된 신뢰신원 형태의 분산신원증명 프레임워크로 이더리움 블록체인 상에서 스마트 컨트랙트로 구현된 오픈소스 프로젝트이다[6]. 사용자는 컨트롤러(Controller) 컨트랙트로 키를 초기 등록하고 이후 컨트롤러 컨트랙트를 참조하는 프록시(Proxy) 컨트랙트들을 생성해 복수의 식별자-속성 조합의 신원정보를 관리할 수 있다. ShoCard는 분산된 신뢰신원 형태로 신뢰기관이 발급한 신원정보를 암호학적 해시함수형태로 비트코인 블록체인에 저장하여 누구든지 검증가능한 신원증명 서비스를 제공한다[7]. 블록체인에 기록되는 신원정보는 최초에 신뢰하는 제3자인 인증자(Certifier)에 의해 기록되지만 기록된 신원정보는 누구든지 쉽게 검증할 수 있다.

본 논문에서 제안하는 시스템은 ShoCard와 같이 분산된 신뢰신원 형태의 신원증명 서비스를 제안한다. 대부분의 사회영역에서 여전히 중앙화된 신원관리체계를 사용하는 것을 고려했을 때 기존 신원관리체계와 연계하고 현시점에서 적용하기 쉬운 중간형태로서 적은비용으로도 구축하기 쉽고 기존 시스템과의 연계도 용이할 것으로 보인다.

3. 분산신원증명 설계

3.1 제안시스템 설계

이 장에서는 마스크 중복구매 방지에서 판매이력관리시스템으로 사용될 수 있는 분산신원증명 시스템을 설계하고 제안한다. 제안시스템에서 중앙기관(발급기관, Issuer)은 사용자(Holder)에게 검증가능한 자격증명을 부여한다. 사용자는 발급받은 자격증명을 블록체인에 기록하고 인가된 판매자(Verifier)를 통한 마스크 구입 시 신원에 대한 검증 및 새로운 속성(마스크 구매여부)을 구매자의 신원정보에 새로운 검증가능한 자격증명으로 생성하여 전달한다. 여기서 판매자는 사용자에게 새로운 속성을 부여하는 인증기관(Certifier)의 역할을 수행한다. 각 참여자들의 역할 그리고 제안시스템의 세부적인 절차는 Fig. 1과 같으며 Table 1은 제안 시스템에서 사용하는 표기이다.

- **발급자(Issuer, CA):** 일반적인 신원증명의 발급기관으로 신뢰하는 기관이다. 사용자에게 자격증명을 발급하고 해당 자격증명을 검증하기 위한 기관의 서명을 전달한다.
- **사용자(Holder, U):** 사용자는 발급자로부터 자격증명을 발급받고 스마트계약을 생성하여 이를 관리한다.
- **검증자(Verifier, V):** 검증자는 제안 시나리오에서는 마

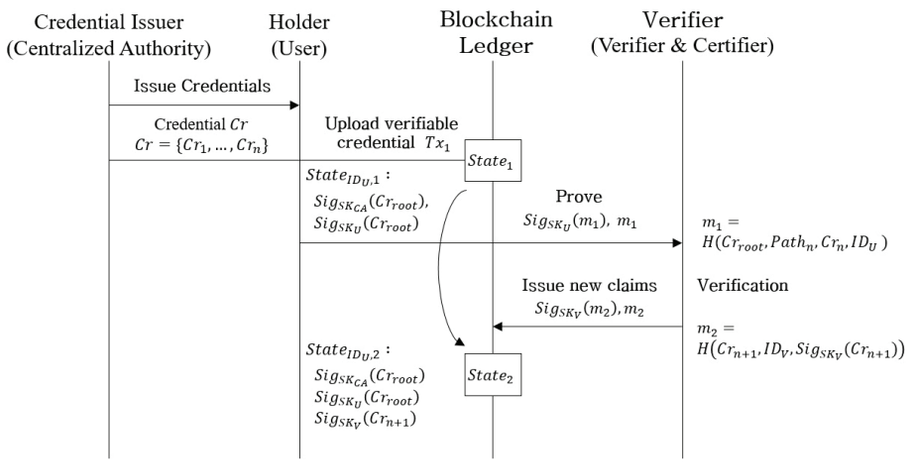

Fig. 1. Identification Process in Proposed System

Table 1. Notations

Notations	Description
Cr	A set of user's credentials
Cr_{root}	A merkle root generated from a subset of user's credentials($Cr_1, \ldots Cr_n$)
Sig_{SK_x}	A digital signature generated by a secret key of user x
$H()$	A cryptographic hash function
ID_x	Identity of a user x
$Path_x$	A merkle path to verify credential Cr_n

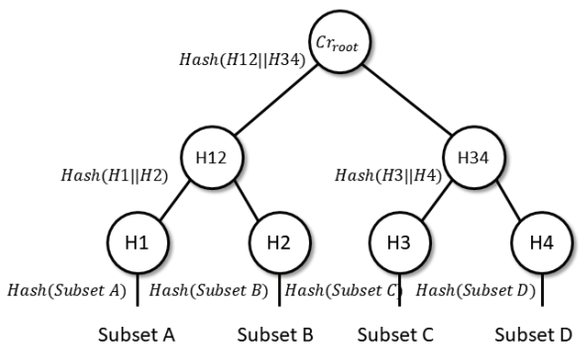

Fig. 2. Merkle Tree in Transaction Tx1

스크 판매자로 블록체인을 통해 사용자의 속성(마스크 구매여부)를 검증한다.

- **인증자(Certifier):** 인증자는 사용자에게 새로운 속성을 부여하는 발급자로부터 인가하는 하위 신뢰기관이다. 제안 시나리오에서 인증자는 공적마스크 판매자들로서 인증자는 사용자의 신원정보에 새로운 속성을 추가한다.

제안 시스템의 시나리오에서 공적마스크 판매자(약국, 우체국 등)은 마스크 구매자의 자격증명을 검증하는 검증자이면서 검증된 사용자에게 새로운 자격증명을 발급하는 인증자의 역할을 수행한다. 발급자와 인증자의 서명 검증은 현재 사용하고 있는 계층적인 신뢰구조에 기반한 PKI (공개키 기반 구조, Public Key Infrastructure)를 사용한다.

(1) **자격증명등록:** 사용자는 여권, 운전면허증과 같이 중앙기관(CA)에서 발급하는 오프라인 자격증명을 이미 가지고 있다는 가정 하에 오프라인 자격증명에 있는 각 속성(이름, 주민번호, 주소 등)에 대한 부분집합들(〈이름〉, 〈이름,주소〉, ...)을 선택하고 선택된 부분집합들을 이용하여 Fig. 2와 같이 머클트리(Merkle tree)를 생성, 머클루트 Cr_{root}를 계산한다. 사용자와 사용자를 인증한 중앙기관은 Cr_{root}에 대한 디지털서명을 생성하여 블록체인에 기록한다($State_{ID_U,1}$). 이 단계에서 블록체인 상태 DB에는 사용자의 속성정보를 포함한 머클루트 Cr_{root}와 이에 대한 최상위 신뢰기관의 서명과 사용자의 서명이 기록된다.

(2) **자격증명검증:** 사용자는 Tx1의 사용자 서명의 생성에 사용된 비밀키와 동일한 비밀키를 사용하여 마스크 구매를 시도한다. 이 과정에서 사용자 인증에 요구되는 자격증명의 부분집합 Cr_n(〈이름, 주민번호〉 혹은 〈이름, 면허번호〉 등)과 이를 검증하기 위한 머클경로(Merkle path) $Path_n$을 판매자에게 제시하고 이에 대한 디지털 서명을 $State_{ID_U,1}$에 사용된 것과 동일한 비밀키로 생성하여 마스크 판매자에게 제시한다. 판매자는 $State_{ID_U,1}$에 사용된 비밀키와 제시된 서명에 사용된 비밀키의 동일성(동일한 공개키로 검증 유무) 및 자격증명(속성)의 유효성(머클트리 검증)을 검증한다.

(3) **신규속성발급:** 자격검증 후 판매자는 사용자를 위해 마스크 구매 여부에 대한 새로운 속성 Cr_{n+1}(마스크 구매 여부)을 정의한다. 판매자는 Cr_{n+1}에 대한 디지털 서명으로 블록체인 상태 DB에 기록된 사용자 U의 상태를 갱신한다($State_{ID_U,2}$). 마스크 구매 과정이 종료된 후

Table 2. Evaluation Result

Evaluation Law	Result	Description
User Control	High	Only users who have the same private key as the key used in the certificate have control over the issued certificate. This can be verified by anyone with a digital signature created with the corresponding private key.
Minimal Disclosure	Medium	Users can use only the information they wish to disclose in a subset of the attributes contained in the issued credential. Each subset can be verified by the digital signature of the issuing entity.
Justifiable Parties	High	Credentials are recorded only as hash values of Merckle Tree on the blockchain and are not disclosed to third parties. Only justifiable parties can receive the original value of the credential for verification from the user in the user's identity verification process.
Directed Identity	Low	Provides only unidirectional identity
Design for a Pluralism	High	Proposed systems assume to operate on the public blockchain such as Bitcoin and Etherium. It is possible to work with other existing identity management systems by utilizing various APIs already developed.
Human Integration	High	In the proposed system, user terminals can be provided in the form of mobile apps. User authentication is easy without having to view and enter ID cards, and cannot be used to steal other user's ID.
Consistent Experience	High	Through authentication using QR code in the mobile app, the certification process can be simplified to provide services.

블록체인 상태 DB에는 사용자의 최초의 속성정보를 포함한 머클루트 Cr_{root}와 이에 대한 최상위 신뢰기관의 서명 및 사용자의 서명 그리고 판매자가 새로 발급한 속성 Cr_{n+1}에 대한 인증된 판매자의 디지털 서명이 기록된다.

제안 시스템에서 블록체인은 시스템의 모든 참여자들에게 공개된 장부로서 사용자의 초기 신원정보의 상태에 대한 변화 값을 지속적으로 기록하는 상태 DB로서 사용된다. 또한 시스템의 참여자면 누구나 사용자(구매자)와의 대화식 프로토콜 수행으로 등록된 속성의 검증 및 신규속성 부여를 TTP의 참여 없이도 수행하는 것이 가능하다. 그리고 상태 변화의 유효성은 PKI를 통해 인증자의 유효성 검증 및 그 서명 검증을 통해 가능하다.

3.2 제안시스템 평가

제안시스템에 대한 평가는 [9]에서 제안된 디지털신원 시스템에 대한 평가 프레임워크에 기반하여 수행하였다. [9]의 평가 프레임워크는 다음과 같은 7개의 항목으로 구성되어있으며 각 항목에 대한 설명은 다음과 같다.

(1) **사용자 자기제어(User Control and Consent):** 사용자를 식별할 수 있는 신원정보는 사용자의 동의하에서만 공개되어야한다.

(2) **제한된 사용(Minimal Disclosure for a Constrained Use):** 신원인증 과정에서 인증에 필요한 정보만 수집되어야 한다.

(3) **정당한 취급자(Justifiable Parties):** 신원정보는 적합한 접근권한을 가진 사용자들 사이에서만 공유되어야 한다.

(4) **신원의 방향성(Directed Identity):** 시스템은 공적인 개체에 대한 단방향 식별자와 사적인 개체에 대한 양방향 식별자를 모두 지원해야 한다.

(5) **다원화 설계(Design for a Pluralism of Operators and Technology):** 시스템은 다른 신원관리·자격증명 기법과 상호작용할 수 있어야한다.

(6) **사용자 통합(Human Integration):** 명확한 인간-기계 통신 메커니즘을 통해 사용자를 시스템의 컴포넌트로 정의해야 한다.

(7) **일관된 사용자 경험(Consistent Experience Across Contexts):** 시스템은 사용자에게 간단하면서 일관적인 사용자 경험을 제공해야한다.

상기의 7개 평가 항목에 대한 제안 시스템의 평가결과는 Table 2와 같다(각 항목에 대해서 결과에 따라 상중하의 3단계로 구분하여 표시함).

4. 결 론

본 논문에서는 공적마스크 중복구매 여부와 같이 기존의 중앙화된 신원관리체계에서는 관리하기 힘든 여러 속성들을 기존에 구축된 신원관리체계 및 여러 인프라를 활용하여 관리할 수 있는 분산신원증명 시스템을 제안하였다. 제안 시스

템은 이더리움 블록체인과 같은 퍼블릭 블록체인 상에서 비밀키 관리 및 서명용 모바일 애플리케이션과 스마트계약만으로 구축이 가능하고 사용자들에게 부여 가능한 속성에 대해 제약이 없으므로 좀 더 유연하게 다양한 상황에서 신속하게 대응할 수 있을 것으로 기대한다.

References

[1] E. T. Kim, How South Korea Solved Its Face Mask Shortage [Internet], https://www.nytimes.com/2020/04/01/opinion/covid-face-mask-shortage.html.

[2] Health Insurance Review & Assusement Service, Drug Utilization Review (DUR) [Internet], https://www.hira.or.kr/dummy.do?pgmid=HIRAA990001000330.

[3] Health Insurance Review & Assessment Service, HIRA System [Internet], https://biz.hira.or.kr/.

[4] A. Loibl, "Namecoin," in *Proceedings of the Seminars Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM)*, pp.107-113, 2014.

[5] A. Tobin and D. Reed, The Inevitable Rise of Self-Sovereign Identity [Internet], https://sovrin.org/.

[6] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, uPort: A Platform for Self-Sovereign Identity [Internet], http://blockchainlab.com/pdf/uPortwhitepaperDRAFT20161020.pdf.

[7] A. Ebrahimi, Identity Management Verified Using the Blockchain [Internet], https://www.pingidentity.com/en/lp/shocard-personal-identity.html.

[8] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security & Privacy*, Vol.16, No.4, pp.20-29, 2018.

[9] K. Cameron, The laws of identity [Internet], https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

노 시 완

https://orcid.org/0000-0003-0261-3444
e-mail : nosiwan@pukyong.ac.kr
2016년 부경대학교 IT융합응용공학과(학사)
2018년 부경대학교 정보보호학과(석사)
2019년 ~ 현 재 부경대학교 정보보호학과 박사과정
관심분야 : Blockchain, ID Management, Cryptographic Algorithm, Access Control

장 설 아

https://orcid.org/0000-0002-4636-5027
e-mail : seolahh1020@gmail.com
2020년 동아대학교 국제경영학과(학사)
2020년 ~ 현 재 부경대학교 인공지능융합학과 석사과정
관심분야 : Blockchain Governance, Artificial Intelligence, Information Security

이 경 현

https://orcid.org/0000-0003-0466-8254
e-mail : khrhee@pknu.ac.kr
1982년 경북대학교 수학교육과(학사)
1985년 한국과학기술원 응용수학과(석사)
1992년 한국과학기술원 수학과(박사)
1985년~1993년 한국전자통신연구원 연구원, 선임연구원
1993년 ~ 현 재 부경대학교 IT융합응용공학과 교수
관심분야 : Information Security, Mobile Communication Security, Blockchain, Artificial Intelligence