블록체인 분산신원증명에 기반한 공적마스크 중복구매 확인 시스템에 대한 연구

노시완*, 장설아*, 이경현**
*부경대학교 일반대학원 정보보호학과
**부경대학교 IT융합응용공학과
nosiwan@pukyong.ac.kr, seolahh1020@gmail.com, khrhee@pknu.ac.kr

A Study on Face Masks Distribution System based on the Blockchain Decentralized Identity

Siwan Noh*, Seolah Jang*, Kyune-Hyune Rhee**
*Department of Information Security, Graduate School, Pukyong National University
**Department of IT Convergence and Application Engineering, Pukyong National University

요 약

2020년 1월 국내에 신종 코로나 바이러스의 확산으로 인해 보건 마스크의 수요가 급증하고 이에 따라 마스크의 가격이 폭등하자 정부가 건강보험정보를 기반으로 보건용 마스크 판매에 관여하는 공적 마스크 5부제를 시행해 왔다. 하지만 건강보험 가입정보에 의존적인 신원 인증 시스템으로 인해 유학생 등 건강보험 미가입자의 경우 마스크의 구입이 어렵고 개인정보 접근 문제 등으로 판매채널의 확장이 어려운 문제가 있었다. 본 논문에서는 건강보험과 같은 특정 신원정보 시스템에 의존하지 않고 중앙기관이 발행하는 신뢰할 수 있는 모든 신원정보(여권, 외국인등록증 등)에 기반하여 사용자가 스스로 자신의 신원정보 속성을 블록체인을 통해 관리하는 방법을 제안한다. 또한 제안 방법에 대해 디지털신원 기법을 평가할 수 있는 지표를 기반으로 자체 평가를 수행한다.

1. 서론

2020년 1월 국내에서 첫 번째 코로나 바이러스 감염증(COVID-19) 환자가 발생하고 점차 확진자가 증가함에 따라 보건 마스크 수요가 급증하였고 이에 따라 시중의 마스크의 가격이 폭등하는 상황에서도 여전히 마스크 품귀현상이 빚어질 정도로 공급이 수요를 쫓아가지 못하는 상황이 발생하였다. 이 과정에서 지나친 매점매석으로 시중에서 보건 마스크를 구하기 더욱 어렵게 되자 정부가 개입하여 마스크 공급량을 대폭 늘리고 판매 채널을 제한하는 공적마스크를 도입하였다. 초기에는 농협 하나로마트와 우체국을 공적판매처로 마스크를 판매하였으나 곧 출생년도에 따른 마스크 5부제를 도입하여 현재까지 시행 중에 있다. 마스크 5부제는 기존에 건강보험심사평가원에서 제공하던 의약품안전사용서비스(Drug Utilization Review, DUR)을 사용하여 공적마스크 구매를 1인당 1주일 2매로 제한하여 중복구매를 방지한다. 본래 의사 및 약사가 환자에게 처방된 의약품의 정보를 제공받아 부적절한 약물사용을 사전에 방지하는 것을 목표로 하는 서비스이나 정부에서는 이 항목에 마스크를 추가하여 사용하고 있다.

하지만 현재 사용하고 있는 공적마스크 판매에는 몇 가지 문제점이 존재한다. 첫째, DUR은 건강보험심사평가원에 등록된 건강보험 가입자 DB에 의존하기 때문에 외국인 등과 같이 건강보험에 가입되지 않은 사용자에게 적용이 어렵다. 둘째, DUR 시스템에 접근하기 위한 권한을 약사 외에 다른 일반인에 부여하기에는 많은 문제가 발생할 수 있기에 판매처를 확장하기 어렵다. 공적마스크 판매 초기에 판매 물품의 유통관리가 효율적인 편의점을 판매처로 추가하는 것에 대한 논의가 있었으나 마스크 수급이 불안정한 시점에서 판매처를 늘리는 것은 의미가 없다고 판단되어 불발되었다. 하지만 편의점을 판매처로 추가하였더라도 DUR과 편의점의 POS(Point of Sales) 시스템의 연동이 어렵고 편의점 직원에게 건강보험 가입자 정보에 접근할 수 있는 DUR 시스템의 관리를 맡기기는 어렵기 때문에 문제가 되었을 것으로 보인다. 마지막으로 마스크 구매자의 프라이버시 노출 문제가 있다. 현재 DUR에 기록된 정보를

확인하기 위해 개인 신분증(주민등록증, 여권, 면허증 등)을 제시하여야하나 이 과정에서 출생년도를 확인하고 DUR에 등록하기 위한 주민등록번호를 제외한 나머지 정보(주소 등)가 판매자에게 노출되는 문제가 존재한다.

본 논문에서는 언급한 문제점들을 해결하고 차후 유사한 상황이 발생 시에 빠르게 구축 및 적용이 가능한 분산신원증명 시스템에 대한 연구를 제안한다.

2. 분산신원증명(DID)

신원(Identity)은 개인을 식별하는 유일한 값으로 주민등록증, 여권 등은 개인의 신원과 속성(Attribute)의 관계에 대해 발급기관이 정의한 전통적인 오프라인 신원인증 수단이다. 반면에 온라인 신원인증은 신뢰기관이 보증한 사용자의 공개키와 오프라인 신원 정보의 결합인 공인인증서를 기반으로 이루어지는데 인증서 발급과정의 불편함이 존재하고 인증과정에서 서비스제공자에게 제공되는 정보에 대한 통제가 발급기관에 존재하는 문제가 있었다.

이에 따라 탈중앙화된 시스템에 대한 관심이 높아지는 가운데 블록체인을 이용한 탈중앙화된 신원(Decentralized Identity, DID)이 제안되었다[1-3]. DID는 사용자의 신원정보를 신뢰기관 없이 스스로 비가역적인 블록체인을 통해 관리하고 신원증명을 중앙화된 기관을 거치지 않으면서도 가능하도록 하여 다양한 분야에서 사용자인증을 제공할 수 있다

.

<표 1> [5]에서 정의한 신원관리 기법 평가기준

평가기준	설명
사용자 자기제어	사용자를 식별할 수 있는 신원정보는 사용자의 동의하에서만 공개되어야함
제한된 사용	인증에 필요한 정보만 수집되어야 함
정당한 취급자	신원정보는 적합한 접근권한을 가진 사용자들 사이에서만 공유되어야함
신원의 방향성	시스템은 공적인 개체에 대한 단방향 식별자와 사적인 개체에 대한 양방향 식별자를 모두 지원해야 함
다원화 설계	시스템은 다른 신원관리·자격증명 기법과 상호작용할 수 있어야함
사용자 통합	명확한 인간-기계 통신 메커니즘을 통해 사용자를 시스템의 컴포넌트로 정의해야 함
일관된 사용자 경험	시스템은 사용자에게 간단하면서 일관적인 사용자 경험을 제공해야함

[4]에서 Paul과 Fabien은 블록체인 기반 신원관리 기법 중 ShoCard[1], Sovrin[2], uPort[3]를 선택하여 [5]에서 정의하는 신원관리 기법의 평가기준에 기반하여 각각을 평가하였다. 정의된 평가기준은 표 1과 같다. 3장에서는 기존의 신원관리 기법을 기반으로 한 공적마스크 중복구매 확인 시스템을 설계하고 [5]의 평가기준을 토대로 자체 평가를 실시한다.

3. DID 기반 중복구매 확인 프로토콜

[4]에서 Paul과 Fabien은 분산신원관리 기법을 중앙 기관 없이 사용자가 스스로 자신의 신원과 속성을 정의하고 관리하는 자기주권신원(Self-sovereign Identity)과 기존에 존재하는 중앙 기관이 발급한 신원(여권 등)에 대해 블록체인을 이용한 검증 서비스를 제공하는 분산된 신뢰 신원(Decentralized trusted Identity)으로 구분하였다. 제안하는 시스템은 중앙 기관인 정부가 마스크와 같은 공적 판매가 필요한 물품의 판매과정에서 사용자가 가진 특정 속성(마스크 구매여부)를 탈중앙화된 방식으로 검증하는 것이 목적이므로 분산된 신뢰신원 형태의 설계가 적절하다.

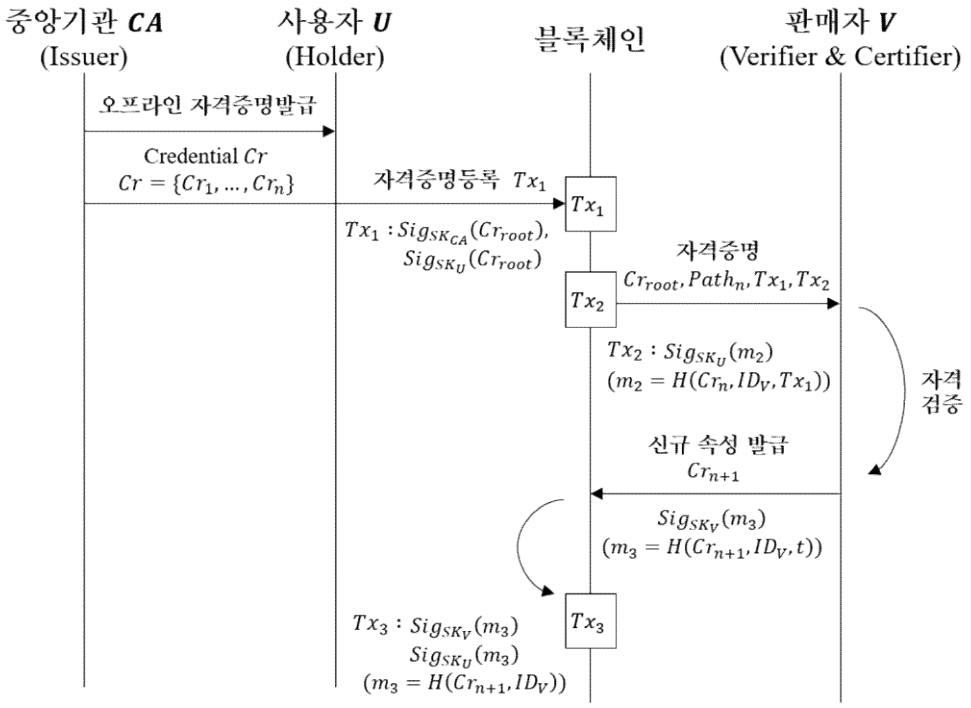
제안시스템에서 중앙기관(정부, Issuer)은 사용자(Holder)에게 신뢰할 수 있는 자격증명을 부여한다. 사용자는 발급받은 자격증명을 블록체인에 기록하고 중앙기관이 인가한 판매자(Verifier)를 통한 마스크 구입 시 신원에 대한 검증 및 새로운 속성(마스크 구매여부)을 신원정보에 추가한다. 여기서 판매자는 사용자에 대한 새로운 속성을 부여하는 기관(Certifier)의 역할을 수행한다. 제안시스템의 세부적인 절차는 그림 1과 같다.

▪ 자격증명등록

사용자(U)는 여권, 운전면허증과 같이 중앙기관(CA)에서 발급하는 오프라인 자격증명을 가지고 있다는 가정 하에 오프라인 자격증명에 있는 각 속성(이름, 주민번호, 주소 등)에 대한 부분집합들(예:[이름],[이름,주소],...)을 선택하고 선택된 부분집합들을 이용하여 머클트리(Merkle tree)를 생성, 머클 루트 값 Cr_{root}를 계산한다. 사용자와 중앙기관은 Cr_{root}에 대한 서명을 생성하여 블록체인에 기록한다(Tx1).

▪ 자격증명검증 및 신규속성 발급

사용자는 Tx1의 서명에 사용된 비밀키와 동일한 키를 사용하여 마스크 구매를 시도한다. 이 과정에서 마스크 구매에 필요한 자격증명 부분집합 Cr_n과



(그림 1) 제안시스템 세부 과정

이를 검증하기 위한 Cr_{root} 및 머클경로(Merkle path) $Path_n$을 제시하고 이에 대한 서명을 비밀키로 생성하여 마스크 판매자에게 전달한다. 판매자는 Tx1에 사용된 비밀키와 제시된 서명에 사용된 비밀키의 동일성 및 자격증명의 유효성을 검증한다.

<표 2> 제안 시스템 평가결과

평가기준	설명
사용자 자기제어	사용자만이 신뢰기관으로부터 자신에게 발급된 자격에 대한 권한을 가지며 이는 스마트계약에 해당하는 비밀키로 관리됨
제한된 사용	사용자는 오프라인 자격증명에 포함된 자격을 부분집합으로 구성하여 공개하고 싶은 자격만 증명에 사용할 수 있음
정당한 취급자	자격정보는 블록체인 상에서는 해시값으로 기록되고 정보취급자에게만 자격검증을 위한 원본값이 제공됨
신원의 방향성	단방향(unidirectional) 신원만을 제공
다원화 설계	시스템은 비트코인,이더리움과 같은 퍼블릭 블록체인 상에서 동작하는 것을 가정하여 상호운용성을 보장하는 기술을 사용하여 다른 신원관리 시스템과 연동 가능
사용자 통합	모바일 앱 형태로 서비스 제공 가능, 사용자 인증은 신분증을 보고 입력하는 과정없이 간편하게 이루어지며 타인의 신분증 도용 불가능
일관된 사용자 경험	모바일 앱에서 QR코드를 이용한 인증 등을 통해 자격증명 과정을 간소화하여 간편하게 서비스를 제공할수있음

자격검증 후 판매자는 마스크 판매 및 사용자의 속성에 마스크 구매에 대한 속성 Cr_{n+1}을 자신의 서명을 통해 추가한다.

각 과정은 별도의 스마트계약을 통해 이루어지며 사용자의 초기 자격증명을 관리하는 계약 A와 이 계약과 연동되어 사용자의 속성을 관리하는 계약B의 연동으로 동작한다. 제안 시스템에 대한 자체평가 결과는 표 2와 같다.

4. 결론

본 논문에서는 최근까지도 이슈가 되고 있는 공적 마스크 구입에 필요한 자격증명에 대해 블록체인을 이용한 방식을 제안하였다. 제안 시스템은 이더리움 블록체인과 같은 퍼블릭 블록체인 상에서 구현이 가능하고 비밀키 관리 및 서명용 모바일 애플리케이션과 스마트계약만으로 구축이 가능하고 사용자에게 부여가능한 속성에 대해 제약이 없으므로 좀더 유연하게 다양한 상황에 대응할 수 있을 것으로 기대한다.

사사표기

본 연구는 과학기술정보통신부 및 정보통신기기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2020-2015-0-00403)으며 일부는 2018년도 정부(과학기술정보통신부)의 재원으로 한

국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2018R1D1A1B07048944)

참고문헌

[1] “Identity Management Verified Using the Blockchain,” ShoCard Whitepaper, 2017.

[2] A. Tobin and D. Reed, “The Inevitable Rise of Self-Sovereign Identity,” The Sovrin Foundation, 2016.

[3] C. Lundkvist et al., “uPort: A Platform for Self-Sovereign Identity,” 2017.

[4] 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.

[5]K. Cameron, “The laws of identity,” Microsoft Corp, vol. 12, pp. 8 - 11, 2005.