Global Report

대중교통에서 자기신원검증 사례 기반의 블록체인 지원 분산식별 관리방법

1. 개요
2. 이론적 배경_ID 유형
3. 블록체인 기반
   SSI 디지털 아이덴티티의 개념화
4. 통합 모빌리티의 발전방향
5. 결론

KAIA 국토교통 과학기술진흥원

작 성 자 | 박 세 환

1. 개요

수년에 걸쳐 인터넷은 사회전반에 걸쳐 일상생활의 근본적인 변화를 가져온 변화의 원동력이 되었다. 개방적이고 분산된 통신 네트워크로 시작된 인터넷은 세계화와 상호연결을 추진하고 강화하는 수많은 응용프로그램의 핵심으로 발전했다. 아울러 인터넷의 파급효과는 운송 및 모빌리티 산업을 포함한 거의 모든 산업부문에서 분명하게 드러나고 있다. 이 중심에 ITS(Intelligent Transport Systems : 지능형 운송 시스템)가 확산되면서 교통 혼잡과 이산화탄소 배출을 줄이면서 도시 안팎의 교통관리 시스템을 획기적으로 개선하고 있다. 특히 UN의 지속가능한 개발목표11은 대중교통 개선의 필요성을 포함한 지속가능한 도시의 필요성을 인식하고 있으며, 교통관리 시스템의 중요성을 강조하고 있다. 이후 교통 및 이동성에 대한 관심이 높아지면서 모빌리티와 같은 새로운 지속가능한 교통 개념을 가속시키고 있다[1]. 다양한 유형의 모빌리티 모드가 단일 서비스에 통합되어 있다. 이 개념에는 승차 공유, 대중교통 및 Uber와 같은 승차서비스 등이 포함되어 있다. 그러나 이러한 서비스 제공은 특히 도시의 대중교통 시스템을 관리하는 플랫폼의 경우, 상호운용성을 제공하지 않는 격리된 서비스로 작동하는 것처럼 보인다.
특히 발권시스템은 도시나 국가와 연결된 단일 운송사업자에 의존한다. 이로 인해 유럽연합(EU)은 2050년까지 유럽전역의 대중교통 당국 간의 상호운용성을 제공하는 스마트 발권 솔루션 개발을 계획하고 있다[2]. 이 스마트 발권 솔루션을 사용하려면 사용자가 유럽 내 모든 대중교통 시스템에 단일 진입점을 가질 수 있어야 한다. 현재의 대중교통 환경은 다양한 솔루션, 가격 모델, 언어 및 데이터 형식 등 매우 세분화되어 있다. 일부 시스템은 국가 내의 다양한 운송모드에 대한 통합솔루션을 제공하는 반면, 다른 시스템은 도시 또는 지역의 특정 네트워크 내에서만 작동하는 경우도 있다. 발권 솔루션은 종이 티켓과 스마트 카드(smart cards)에서 계정 기반 청구에 이르기까지 매우 다양하다. 이 같은 단편화의 주요과제 중 하나는 전반적인 대중교통 시스템에 대해 독립적인 사용자 계정을 관리하는 것이다. 범유럽 또는 글로벌 운송시스템을 원할 경우 데이터 무결성, 개인정보 보호 및 데이터 소유권과 같은 문제가 중요한 고려사항이다.
W3C(World Wide Web Consortium)와 같은 서비스 제공 당국에 의해 ID 솔루션에 대한 새로운 개념과 표준이 연구되고 있다. 분산된 식별자를 사용하면 타사에 의존하지 않고 관련 데이터와 사용자를 연결할 수 있다. 따라서 사용자는 데이터에 대한 더 많은 통제권을 확보할 수 있을 뿐만 아니라 기존의 중앙집중식 시스템을 이용하여 전반적인 운영권을 얻을 수 있다. 그러나 데이터 유출 및 오용의 위험에 노출될 수 있다. 개인정보를 제어할 수 있는 능력은 서비스 제공 당국의 핵심원칙 중 하나이며, 이러한 기본은 블록체인 기술(block-chain technology)의 개념에 뿌리를 두고 있다. 특히 블록체인 기술을 기반으로 한 유럽의 대중교통 통합 신원관리 시스템은 다른 나라의 많은 이해관계자들을 포함하여야만 한다. 이러한 시스템은 승차기록, GPS 위치, 계정 잔액 및 기타 계정 관련 개인정보를 통해 민감한 사용자 데이터를 생성하게 된다. 따라서 사용자가 다양한 공공 및 개인 운송회사가 잠재적으로 처리할 수 있는 많은 새로운 데이터 위험에 노출될 수 있다. 이는 대중교통 부문의 신원관리 시스템을 어떻게 구축해야하는지에 대한 전반적인 의문이 제기된다. 유럽위원회의 ITS 지침 2010/40/EU(The ITS Directive 2010/40/EU of the European Commission outlines)은 회원국의 원활한 door-to-door 이동성을 허용하는 유럽의 광범위한 대중교통 시스템 구축목표를 잘 설명하고 있다[3]. 2013년에 결성된 ITS 전문가 그룹에서는 2050년까지 상호운용성이 보장된 대중교통 시스템을 구축할 수 있는 토대를 제공하고 있다[4]. 독립적으로 제어되는 다양한 대중교통 시스템으로 구성된 생태계는 많은 기술적 과제를 안고 있다. 이에 단일 유럽전역의 운송개발을 촉진하려면 가능한 기술솔루션에 대한 철저한 검사가 필요하다. 아울러 다양한 유형의 유럽 대중교통 네트워크를 구현하기 위해서는 환승시스템에서 요금관리와 같은 데이터처리에 관한 많은 과제를 안고 있다. 이러한 과제에는 플랫폼 간 ID관리를 허용하는 적합한 솔루션이 필요하다.
운송네트워크 내 이용자에게 다양한 서비스를 제공할 수 있는 신뢰할 수 있고 투명한 ID관리 시스템을 구축하기 위해 크로스 플랫폼 솔루션(CPS : cross-platform solution)이 개발되었다. CPS의 요구사항은 이해관계자 간 신뢰성을 기반으로 각 엔터티에 대한 투명한 회계 메커니즘을 갖춘 상호운용 가능한 시

스템을 만드는 것을 목표로 블록체인 기반 솔루션으로 개발되었다. 따라서 블록체인 네트워크의 모든 다른 엔터티에 대한 개인정보보호 및 신뢰성을 제공할 수 있어야 한다. 아울러 악의적인 개인정보 도용으로 인한 피해를 최소화하기 위해 승차기록 및 개인정보와 같은 중요한 사용자 데이터가 어떻게 이용되고 있는지에 대해 완전한 제어능력이 필요하다. 이는 SSI(Self-sovereign Identity : 자기 주권 신원)과 관련이 있다. 즉, 시스템구현 및 유럽 운송영역의 목표를 감안할 때 ID관리 및 블록체인 기술의 새로운 SSI 표준에 부합하는 실행가능한 ID 솔루션을 설계하는 것이 우선적이다.

2. 이론적 배경_ID 유형

2005년 Windley는 디지털 ID관리는 다양한 ID의 기록을 관리하는 개념으로, 대표 에이전트의 실명과 같은 특정 ID에 연결된 레코드를 생성/관리/사용/삭제 등의 관리가 포함될 수 있다고 하였다. 디지털 ID로 표시되는 외부 에이전트에는 개인뿐만 아니라 장치, 조직 및 응용프로그램도 포함된다. 따라서 디지털 ID관리는 시스템 내에서 특정 작업을 실행하기 위한 권한을 처리하는 전체 계층을 의미한다. 디지털 ID를 제어하는 사람은 디지털 ID로 인코딩된 규칙 및 권한으로 정의된 시스템 내의 특정 작업에 액세스할 수 있다. 따라서 보안 및 액세스 관리는 모든 ID관리 시스템의 중요한 작업이다. 일반적으로 ID소유자는 다양한 작업을 승인받는 데 필요한 자격증명을 통해 ID에 액세스할 수 있다. 또한 디지털 ID시스템은 점점 더 이질화되어가는 기술 환경에 대한 액세스를 제공해야하기 때문에 더욱 복잡해지고 있다. 따라서 디지털 ID시스템은 중앙집중식 시스템에서 분산솔루션으로 이동하고 있는 추세이다. Christopher Allen에 따르면, 분산 ID시스템은 다른 응용프로그램에서 보다 향상된 휴대성(이동성)과 사용자제어 이점을 제공한다고 했다[5]. 디지털 ID는 사용자 제어 및 휴대성의 차원에 따라 3가지 클래스(중앙집중식/사용자중심/자기 주권 신원)로 분류할 수 있다. 특히 SSI(Self-sovereign Identity : 자기 주권 신원)는 사용자에게 해당 ID를 완전히 제어할 수 있도록 설계되었다. 사용자가 지정된 ID공급자에 의존하도록 요구하는 다른 시스템과 달리 ID 자격증명을 차단/변경/삭제할 수 있는 중앙집중식 서비스와 자율적으로 분리된다. SSI에 대한 10가지 지침 원칙을 <표 1>에 나타낸다.

<표 1> SSI에 대한 10가지 지침 원칙

지침 원칙	주요 내용
보안 차원	
보호	- 개별 사용자의 자유와 권리가 최우선 과제임
원칙	- 사용자ID는 사용자가 원하는 만큼 유지되어야 함 - 기본정보(공용 및 비 공개 키)가 변경되더라도 사용자ID는 동일하게 유지되어야 함
최소화	- 사용자 데이터의 공개는 최소화되어야 함 - 클레임을 확인하는 데 필요한 데이터만 노출되어야 함
제어 가능성 차원	
존재	- ID는 디지털영역 외부의 사용자들과 연결되어야 함 - 따라서 사용자는 디지털영역 밖에서 독립적인 존재를 가져야 함
제어	- 사용자는 자신의 신원과 개인정보 설정에 대한 완전한 제어 및 궁극적인 권한을 가져야 함
승인	- 데이터공유는 사용자가 동의를 제공하는 경우에만 발생할 수 있음
이식성 차원	
상호 운용성	- ID는 모든 유형의 시스템에서 작업할 수 있어야 함 - 사용자제어를 잃지 않고 전 세계적으로 사용할 수 있어야 함
투명성	- ID를 작동하고 관리하는 시스템은 완전히 투명해야 함
접근성	- 사용자는 자신의 신원과 관련된 모든 클레임 및 데이터에 액세스할 수 있어야 함
이식성	- ID는 단일 엔터티에서 보유할 수 없음 - 다른 유형의 시스템으로 전송할 수 있어야 함

* 자료 : Lukas Stockburger et al., “Blockchain-Enabled Decentralized Identify Management: The Case of Self-Sovereign Identity in Public Transportation”, Blockchain: Research and Applications, p.6.

3. 블록체인 기반 SSI 디지털 아이덴티티의 개념화

운송 및 모빌리티 부문과 관련하여 단일 디지털 플랫폼을 사용하여 대중과 민간 운송사업자 간의 격차를 해소하여 운송서비스에 대한 통합 액세스를 달성하기 위해 모빌리티-서비스로서의 새로운 개념이 제안되었다. 블록체인 및 DLT(Distributed Ledger Technology) 기술은 또한 서비스로서 모빌리티에 초점을 맞춘 개방형 플랫폼을 제공하기 위해 연구되었다. 그간 연구사례를 시계열적으로 요약하면 다음과 같다.

- 2018년 Buccafurri 등은 비대칭 암호화키와 트랜잭션에 서명하는 사용자ID 사이의 직접적인 링크를 허용함으로써 ID 기반 암호화를 사용하여 ID개념을 역할과 연결시킨바 있다. ID 기반 암호화의 일부로 개인키 생성기을 사용하여 제3자가 ID값을 기반으로 공개키를 생성할 수 있도록 한 것이다. 이를 통해 신뢰성이 보장된 제3자 공개키에 해당하는 개인키를 생성할 수도 있게 하였다.
- 2019년 Bothos 등은 다양한 운송제공업체와 이용자를 원활하게 통합하여 통합된 이동성을 가능하게 하는 블록체인 기술을 어떻게 사용할 수 있는지 조사한바 있다.
- 2020년 Bhushan 등은 스마트 시티와 스마트 커뮤니티 이니셔티브에 따라 운송, 스마트 그리드 및 기타 부문에서 블록체인 기술의 유용성을 조사한 다음 다양한 애플리케이션 도메인의 발전을 위한 분산 응용프로그램을 활성화하고 개발하기 위한 몇 가지 연구 과제를 제시한바 있다.
- 2020년 Xu 등은 특정 유형의 블록체인 기술을 사용하여 무선 모바일 네트워크에서 사용자ID를 관리하기 위한 자체 주권 기반 ID 및 인증체계를 제안한바 있다. 이는 블록체인 기반 기술을 이용한 인증 및 ID관리는 네트워크 운영자와의 ID정보의 중앙집중식 관리에 대한 대안으로 무선 모바일 네트워크에서도 연구되었다.

아이덴티티 및 ID관리 시스템에 대한 위에서 언급한 연구 외에도 특히 익명성과 의사익명성을 얻기 위해 공공 디지털 ID시스템의 보안을 강화한 블록체인 기술을 제안한 것도 있다. 지금까지의 연구는 블록체인의 네이티브 의사익명을 포함하여 다양한 익명 계획을 통해 정보유출을 방지함으로써 신원인식이 필요한 응용프로그램을 지원하여 왔다. 이를 통해 공공 디지털 ID시스템을 개선하는 데 초점을 맞추고 있다.

4. 통합 모빌리티의 발전방향

이 연구에서 개발된 저 충실도 프로토타입은 블록체인 기술을 사용하여 분권화의 원칙에 따라 EMC(Euro Mobility Card)를 발행하는 프로세스 즉, 두 가지 핵심원칙(사용자제어/휴대성)에 따라 평가될 수 있다. EMC는 사용자의 완전한 통제 하에 사용자 개인 미디어기기에 저장된 검증 가능한 자격증명으로서 높은 수준의 사용자제어가 가능하다. 또한 EMC는 사용자ID의 일부로 ID카드와 같은 다양한 자격증명을 구현할 수도 있다. 카드를 발급하는 경우, 발급자의 확인에만 의존하고 ID공급자의 영업권에 의존하지는 않는다. 따라서 ID공급자의 독립성이 보장됨으로써 사용자가 자신의 신원을 완전히 제어할 수 있는 장점이 있다.

제안된 시스템의 실용성을 평가하기 위해 기술역량검증 과정에 대한 평가를 수행하였다. 이는 제안된 시스템을 기존 발권시스템에 통합하여 완전한 운영통합 운송이 될 수 있는 기술적 과제를 조명할 수 있을 것으로 기대하고 있다. 개발된 프로토타입은 식별된 문제에 대한 솔루션의 하위집합을 구성하며, 이는 ID 및 서비스공급자 측면에서 많은 기술적 노력을 필요로 한다. 대중교통의 맥락에서 이러한 이니셔

티브는 최종솔루션을 지원하기 위해 현재 발권시스템과 터미널을 업그레이드하는 데에 대한 개선을 요구한다. 특히 EMC카드와 같은 승객에게 제공되는 ID는 발권 단말기에서 확인할 수 있는 형태로 제시되어야 하며, 원활한 방식으로 여행 시 체크인 및 체크아웃할 수 있어야 한다. 또한 검사장치가 제시된 모빌리티 카드를 효과적으로 판독할 수 있도록 인프라를 업그레이드 할 필요가 있다. 따라서 유럽수준에서 국경 간 여행을 용이하게 하는 ID관리 시스템의 전체적인 구현을 평가할 수 있는 보다 철저한 기술 타당성 조사가 필요하다.

5. 결론

이 연구에서는 개인 신원의 자기 주권 원칙에 따라 사람들이 여러 운송제공업체 관할권에 걸쳐 여행할 때 다양한 여행카드의 사용을 최소화할 수 있는 분산된 신원관리시스템을 제안하였다. 이에 주요 요구사항을 도출하고 개념증명을 통해 “Hyper-ledger Indy” 라는 block-chain을 사용하여 저 충실도 프로토타입을 개발하였다. 이는 개인이 유럽전역에서 상호운용 가능한 발권시스템 이용을 보다 더 용이하게 제어할 수 있는 방법을 보여준 것이다. 제안된 시스템은 2050년까지 회원국 간 단일 운송시장을 달성하는 EU의 목표와 일치한다. 대부분의 ID관리 솔루션에서 사용자는 ID공급자에게 자신의 ID제어를 위임한다. 사용자가 자신의 ID를 완전히 제어하기 위해서는 검증자/발급자/ID홀더 간에 네트워크 신뢰성이 보장된 블록체인 기반 ID관리 시스템을 사용하여 분산원칙에 따라 설정되어야 한다. 이에 신뢰할 수 있고 투명하며 불변성이 보장된 네트워크와 암호화 증명은 사용자에게 완전한 제어를 부여하는 데 필요한 기본 요건이다. 이 연구에서 프로토타입은 유럽의 대중교통 네트워크 전반에 걸쳐 신분증 역할을 할 수 있는 검증 가능한 자격증명, 유로 모빌리티 카드로 자리 잡을 수 있을 것이다.
지난 몇 년 동안 개인정보유출로 인한 반복적인 신원도용 사건이 사회적 혼란을 야기시켜 왔다. 이를 해소하기 위해 블록체인 기술의 분산원장을 이용한 새로운 사용자 신원관리시스템(SSI : Self-Sovereign Identity)이 개발되었다. 이 연구에서는 여러 국가의 대중교통에서 사용자 신원관리 방법들을 제시하고 있다. 이 연구결과는 국내 대중교통에서 효율적인 사용자 신원관리를 위한 밴치마킹 자료로 활용할 수 있을 것이다.

[참고문헌]

[1] Holmberg, P., Collado, M., Sarasini, S., & Williander, M., (2016). Mobility as a service - MAAS: describing the framework. Technical Report. Viktoria Swedish ICT AB, Sweden.
<https://www.viktoria.se/sites/default/files/pub/www.viktoria.se/upload/publications/final_report_maas_framework_v_1_0.pdf>
[2] ITS Expert Group. (2013). Smart Ticketing Guidelines for ITS Deployment in Urban Areas. Technical Report. Urban ITS Expert Group.
<https://ec.europa.eu/transport/sites/transport/files/themes/its/road/action_plan/doc/2013-urban-its expert_group-guidelines-on-smart-ticketing.pdf>
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040&from=ENJournal Pre-proof
[4] ITS Expert Group. (2013). Smart Ticketing Guidelines for ITS Deployment in Urban Areas. Technical Report. Urban ITS Expert Group.
<https://ec.europa.eu/transport/sites/transport/files/themes/its/road/action_plan/doc/2013-urban-its expert_group-guidelines-on-smart-ticketing.pdf>
[5] http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

<원문제목> Blockchain-Enabled Decentralized Identify Management: The Case of Self-Sovereign Identity in Public Transportation
<원문출처> Blockchain: Research and Applications