한국정보전자통신기술학회논문지(jkiiect)'20-12, Vol.13 No.6
논문 20-13-06-575 http://dx.doi.org/10.17661/jkiiect.2020.13.6.575

자기주권신원기술의 국내 서비스 사례 및 연구 과제 분석을 통한 개인정보 주권 강화 방안연구

이정현*, 김지원*, 김철수*, 양진홍**

A Study on Strengthening Personal Information Sovereignty through Analysis of Domestic Service Cases and Research Projects of Self-Sovereign Identity Technology

Jeong-Hyeon Lee*, Ji-Won Kim*, Chul-Soo Kim*, Jin-hong Yang**

요 약 데이터를 기반으로 한 비즈니스가 폭발적으로 성장함에 따라 개인정보가 포함된 데이터의 중요성이 확대되고 있다. 국내의 경우 데이터 3법이 시행됨에 따라 개인정보가 포함된 데이터 활용 시의 규제 개선 및 명문화를 통해 기업들이 개인정보를 보다 적극적으로 활용할 수 있게 되었다. 이러한 상황에서 서비스 이용에 따른 실명 인증 및 개인정보 제공과 관련해 개인정보 제공을 최소화할 수 있는 자기주권신원기술이 주목받고 있다. 특히, 최근 개인정보 이용에 따른 기록의 명확성 및 증명을 위해 자기주권신원 기능 이용 시 블록체인을 활용한 서비스 및 연구들이 활발하게 이루어지고 있다. 본 논문에서는 국내 자기주권신원 서비스의 특징 및 블록체인 기반 자기주권신원기술과 관련된 연구 현황 및 내용을 분석함으로써 향후 데이터 3법 시대의 개인정보 주권을 강화하기 위한 자기주권신원기술 기반 연구 방향을 제시하고자 한다.

Abstract Along with the exponential growth of data businesses, the importance of data containing personal information of use have also increaseing. Particularly, in Korea, as the Data 3 Act was implemented, companies can use personal information more actively through regulatory improvement and stipulation in case of using data containing personal information. In this situation as per the service use, self-sovereign identity technology has emerged that can minimize the provision of personal information in relation to real name authentication and provision of personal information. Recently, services and studies using blockchain have been actively conducted in case of using the self-sovereign identity function for clarity and verification of records according to the use of personal information. In this thesis, by analyzing the characteristics of domestic self-sovereign identity service and the current status and contents of research related to blockchain-based self-sovereign identity technology and we suggest a research direction based on self-sovereign identity technology to reinforce the sovereignty of personal information in the era of the 3rd Data Act do.

Key Words : Blockchain, Data 3 Act, DID, Privacy, Self-Sovereign Identity

1. 서론

최근 다양한 분야에서 개인 또는 기업의 데이터를 모아 활용하는 사례가 증가하고 있으며, 이에 따라 데이터에 포함된 개인정보의 무분별한 노출 및 활용에

This Paper was supported by Institute of Information & communications Technology Planning & Evaluation & grant funded by the Korea government (MSIT) (No: 2018-0-00261, GDPR Compliant Personal Identifiable Information Management Technology for IoT Environment) in 2020.
*Department of Computer Engineering, INJE University
**Corresponding Author : Department of Healthcare IT, INJE University (jinhong@inje.ac.kr)
Received November 05, 2020 Revised November 14, 2020 Accepted November 16, 2020

따른 침해들이 발생하고 있다.[1] 이러한 예기치 못한 문제점 등의 발생으로 인해 정보 주체인 개인들은 자신의 개인정보에 대한 인식의 향상 및 적법적 활용에 대한 요구가 증대되고 있다.[2][3]

관련해 개인정보에 대해 시대적 흐름을 바탕으로 그 범주를 살펴보면 초기 산업사회에서 프라이버시는 남에게 방해받지 않을 소극적 권리로 정의되었다면, 정보화 사회에서의 프라이버시는 개인이 자신의 정보를 직접 통제할 수 있는 권리로 확장되었다. 현재에는 사물인터넷(IoT), 증강·가상 현실, 인공지능(AI) 등과 같은 ICT 기술을 기반으로 모든 산업, 사물, 사람이 인터넷으로 연결 및 융·복합되어, 프라이버시의 의미가 내 정보의 가치를 보호받을 수 있는 권리로 정의되고 있다.[4] 이러한 변화에 따라 개인정보의 영역이 점차 확대 및 활용 범위가 확장되고 있으며, 기존에는 개인정보로 인정되지 않았던 정보 또는 포함되지 않았던 정보들이 개인정보로 인정되고 있다.[4]

국내의 경우, 데이터 이용에 있어 개인정보 활용 시 관련 규제 혁신과 개인정보보호 거버넌스 체계 정비의 문제를 개선하기 위한 데이터 3법이 개정되었다.[5] 개인정보 관련 법안의 개정을 통해 데이터의 활용 시 개인정보의 범위를 명확히 하고, 활용의 가이드를 제시함으로써 데이터 산업의 활성화를 꾀하고 있다. 그중에서도 개인 신원인증을 위한 공인인증서의 경우 2020년 5월 20일에 폐지법안이 통과하였다.[6] 신원인증의 경우 온라인 서비스상에서 개인정보 데이터를 수집 및 활용에 있어 첫 단계이며, 최근 다양한 개인정보 노출의 문제를 일으키고 있다.[7]

따라서, 기존 방식인 공인인증서를 대체 방안으로 개인정보를 최소한으로 노출하기 위한 새로운 인증 방식인 디지털 신분증 분야가 화두로 떠오르면서 많은 기업들이 해당 시장으로 뛰어들고 있는 추세이다.[8][9] 그중에서 개인정보의 정보주체가 자신의 정보에 대한 주권을 가지고 신원인증을 가능하게 하는 블록체인 기반 자기주권신원인증(Self-Sovereign Identity) 기술로 문제를 해결할 수 있는 방안으로 제안되고 있다.[10][11] 이 기술은 블록체인의 특성을 기반으로 개인정보 활용에 대한 무결성과 투명성을 보장하여, 이를 가능하게 하는 것이다.[12][13]

본 논문에서는 자기주권신원기술과 관련해, 블록체인을 활용한 기술을 종적으로 살펴보고, 개인정보 주권강화를 위한 연구 방향을 제시하고자 하였다. 본 논문에서의 구성은 2장에서는 자기주권신원기술 개요를 통해 데이터 3법이 자기주권신원에 미치는 영향과 블록체인을 통한 활용성을 서술한다. 3장에서는 국내 자기주권신원 서비스 현황과 Alliance 들의 특징을 정리하였다. 4장 국내 블록체인 기반 자기주권신원기술 관련 연구 동향 및 논문을 정량적 지표로 분석하여, 5장에서 자기주권 강화를 위한 블록체인 기반 DID 연구 제언을 제시한다. 그리고 6장에서는 본 논문의 결론 및 향후 연구 활용성을 제시함으로써, 향후 자기주권신원기술을 활용한 개인정보 주권강화 방안을 제시하고자 한다.

표 1. 자기주권신원 10가지 요소
Table 1. Ten elements of self-sovereign identity

Concept	Definition
Existence (실존성)	Users Should be independent
Control (통제권)	Users should have control of their personal information
Access (접근성)	Users must have access to their own data.
Transparency (투명성)	All systems and algorithms must be transparent to users
Persistence (지속성)	The user's personal information should be kept for a long time
Portability (이동성)	The user's personal information and related services should be mobile
Interoperability (호환성)	The user's personal information and related services should be mobile
Consent (동의)	Users must agree to use their personal information
Minimalization (최소화)	The use of information about claims should be minimized
Protection (보호)	The rights of users must be protected

2. 데이터 주권시대의 변화에 따른 자기주권신원

자기주권신원(Self-Sovereign Identity)은 스스로 권한을 가진 신원을 뜻한다. 즉 서비스 제공자 나 중

앙기관의 개입 없이 개인이 자신의 정보를 자신이 자주적으로 소유하고 통제하는 것을 의미한다.[14] 초기 디지털 서비스에서 사용자 신원인증의 경우 여러 기관에서 각각 자신의 ID와 비밀번호를 통해서 신원을 증명하는 개별 신원 모델을 기반으로 하였다.[15] 현재는 OpenID[16], OAuth[17] 등의 기술로 한번 인증한 신원을 통해서 여러 서비스 제공자에게 인증하고 증명 가능한 연합 신원 모델을 사용하고 있다.[15]

이러한 신원인증에 대한 패러다임은 데이터 이용 규제 및 개인정보보호 거버넌스 체계의 변화에 따라서 달라져 왔다. 개인정보를 보호만 하던 시대에서 개인정보를 활용하는 시대로 변함에 따라 사용자는 자기주권 신원을 바탕으로 개인 데이터의 소유권을 추적하고, 개인 데이터가 올바르게 사용되었는지 확인하기 위한 수단을 강구하고 있다. 이와 관련해 자기주권신원 관련해 표1에서와 같은 10가지 요소의 만족이 필요하다.[18]

2.1 자기주권신원 관련 인증 기술의 변화

현재 신원인증 방식의 기술 변화에 따른 방법을 정리하면 다음의 1)~3) 번 순과 같다.

1) 독립형/중앙집중식 인증 기술

독립형/중앙집중식 인증 기술은 인터넷이 나오면서 함께 등장한 개별 신원인증 기술이다.[19] 사용자가 자신의 ID를 관리하는 중앙기관에 신원인증 요청을 보내면 중앙기관이 사용자의 ID를 대신 인증하여 신원증명을 발급하는 형태이다. 그림1과 같이 각 중앙기관이 데이터 주권을 가지고 있게 된다.[20]

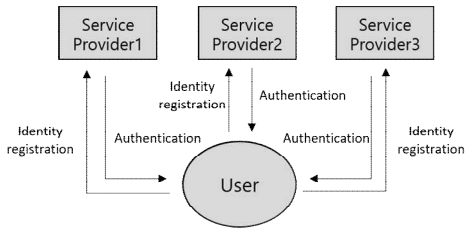

그림 1. 개별 신원인증 모델
Fig 1. Individual identity verification model

2) 연합/사용자 중심 인증 기술

연합/사용자 중심 인증 기술은 그림1에서와같이 각각의 서비스 제공자(Service Provider, SP)에게 신원인증을 하던 방법을 개선한 방식인 SSO(Single Sign On, 통합인증)를 활용한 기술이다.[21][22] SSO는 그림2와 같이 사용자는 자격증명관리자(Identity Provider, IDP)에게 신원을 인증하고, 다른 SP 1, 2, 3에게 IDP의 단일 ID로 신원인증을 가능하게 한다. 연합인증의 핵심기술인 SSO를 구현하기 위한 연구로 SAML(Security Assertion Markup Language)[23], OAuth(Open Authorization), OpenID를 기반으로 신원인증을 하고 있다.

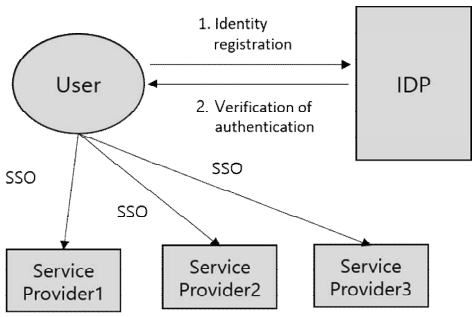

그림 2. 연합인증 모델
Fig 2. Federation authentication model

3) 자기주권신원증명

자기주권신원증명은 탈중앙화 구조를 바탕으로 그림3과 같이 사용자가 직접 자신의 ID를 제출하고 관리하는 권한을 가지며, 기존의 ID 인증 기술과 달리 필요한 정보만 추출하여 제출할 수 있다.

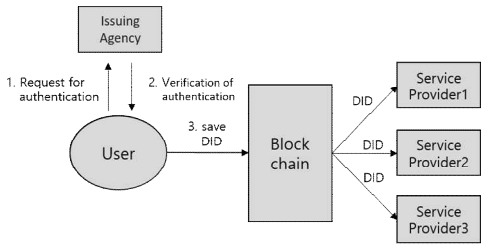

그림 3. 자기주권신원 인증모델
Fig 3. Self-sovereign identity verification model

자기주권신원 이전의 신원인증 패러다임에서 유저는 자신의 개인정보 활용 유/무를 파악할 수 없고, 중앙기관이 자신의 정보를 악용하더라도 유저는 이를 알아차리는 것이 불가능했다.[17] 이러한 점을 개선하기 위해서 자기신원증명기술은 서비스 제공자가 사용자의 개인정보를 투명하게 활용하기 위해 블록체인에 기반한 신원인증 기술로 활용되고 있다.[24]

이때 정보를 공개하지 않고도 신원인증을 가능하게 하는 방법으로 ZKP(Zero- Knowledge Proof, 영 지식 증명)를 활용한 연구가 이루어지고 있다.[25]

2.2 데이터 3법과 자기주권신원

데이터 중심의 디지털전환을 가속화됨에 따라 국내에서는 정보 주체인 개인이 소외되는 정보보호 문제와 데이터 관리 및 활용 미흡 등의 문제점이 대두되고 있었다.[26] 이러한 문제점에 따라서 개인정보에 대한 주체의 권한 강화가 트렌드로 떠오르게 되면서, 금융위원회가 데이터 활용 및 정보보호 종합 방안을 마련하기 위해서 마이데이터 산업 도입 방안을 제시하였다.[27] 마이데이터에서 핵심은 개인이 개인데이터에 대한 관리와 통제 권한을 갖고 자신의 방식으로 활용하는 것을 말하는데, 이때 다양한 기관의 서버에 개인정보 등이 저장되고 공유됨에 따라 개인이 자신의 정보에 접근, 보관을 할 수 있는 방법이 없었다. 이러한 문제를 해결하고자 블록체인 기반 자기주권신원이 조명받기 시작했지만, 이때 개인정보를 보호하기 위한 데이터 이용 규제 및 개인정보보호 거버넌스 체계로 인한 개인정보 활용이 통제되고 있어 활성화를 하지 못했다.[28]

하지만 최근 이를 활성화하기 위한 데이터 3법 개정안이 2020년 1월에 국회를 통과, 2020년 8월에 시행되었다. 데이터 3법은 3가지 법률(개인정보 보호법, 정보통신망법, 신용정보법)을 통합하여 개정된 것으로 주요 내용은 표2에서의 요약본과 같다. 1) 데이터를 이용 및 활성화를 하기 위한 가명 정보 개념 도입, 2) 유사 중복 법률의 규정을 정비하고 추진체계의 통일을 바탕으로 개인정보보호 거버넌스 체계의 효율화, 3) 데이터 활용을 기반으로 개인정보 처리자의 책임 강화

표 2. 데이터 3법 개정안
Table 2. Revised data 3 Act

Data 3 Act	Content
Personal information protection act	• Improving the utilization of data through the introduction of alias information–The use of alias information is processed and utilized for the purpose of statistical preparation, scientific research, and preservation of records for the public interest • Streamlining personal information that can be processed without consent–Allows additional use and provision of personal information as provided under the Presidential Decree to the extent that it is reasonably related to the purpose of collection • Clearing the scope of personal information – establishing a standard for judging information that can easily be combined with other information among personal information to identify a specific individual – Clarifying the exclusion of the application of (anonymous information) from the law • Unifying the privacy system. the elevation of the Personal Information Protection Committee to a central administrative agency belonging to the Prime Minister • The Personal Information Protection Act and the Information and Communication Network Act are readjusted to unify the regulations into the Personal Information Protection Act
Information and communication network act	• Matters related to personal information protection are transferred to the Personal Information Protection Act • Regulations related to personal information protection online • Changed to the Personal Information Protection Committee of the Supervisor
Credit information act	• Readjustment of similar or overlapping clauses with the Personal Information Protection Act • Introduction of a new right to self-determination of personal information • Improvement of the consent system for the use of information, the right to send personal credit information, and the right to request explanation from credit information entities for automated evaluation, etc • Financial field – Establish legal grounds for utilizing big data analysis – Introduce MyData industry – Strengthen personal information protection

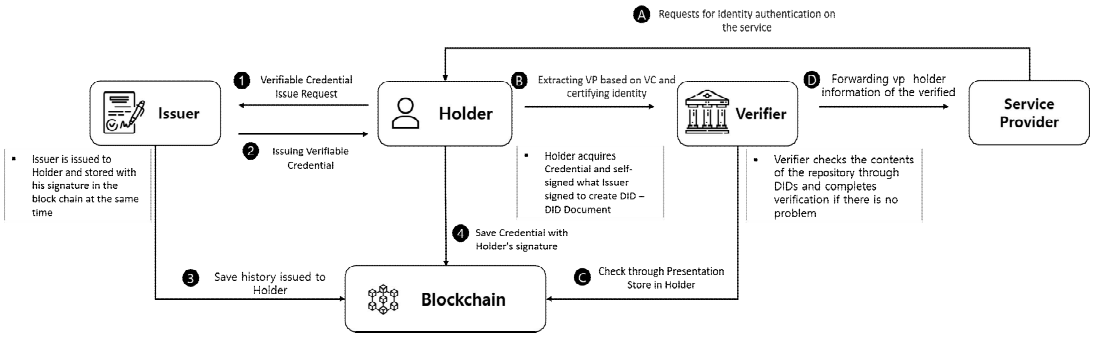

그림 4. 검증 가능한 자격증명 데이터 모델
Fig 4. Verifiable Credentials Data Model

및 모호한 개인정보 판단 기준 명확화를 다루고 있다.[5]

데이터 3법을 통해, 자신의 데이터 소유 및 통제를 위한 자기 정보결정권과 함께, 자신의 정보를 제3자에게 제공하기 위한 자기 정보이동권이 개정되면서 자기주권신원에 대한 데이터의 이용 및 활용성이 증가하게 되었다.

2.3 블록체인을 활용한 자기주권신원

기존의 자기주권신원증명을 할 때 1) 내 정보 중에서 원치 않는 정보까지 제공하고, 2) 인증을 하기 위해서는 많은 시간과 비용이 소요되는 점을 개선하고자 블록체인 기반 자기주권신원연구가 시작되었다.[29] 특히, 앞서 표1에서 언급된 주요 요소 중 지속성, 호환성, 투명성이 구조적으로 만족할 수 있도록 블록체인의 특성인 분산성, 지속성, 확장성, 투명성 등을 활용할 수 있다.

블록체인 기반 자기주권신원기술은 일반적으로 DID(Decentralized Identifier, 탈 중앙 식별자)와 VC (Verifiable Credential, 검증 가능한 자격증명)로 구현한다. 신원인증 및 자격증명 시 사용자가 증명 목적에 따라 필요한 정보만을 선택하여 검증 기관에 제공함으로써, 개인정보를 강화할 수 있는 디지털 신원 확인체계이다. 현재 자기주권신원의 서비스 모델은 W3C에서 정의한 검증 가능한 자격 증명 데이터 모델을 기반으로 사용되고 있으며, 서비스 모델에서의 사용되는 용어는 표3과 같으며, 그 과정은 그림4에서와 같다. 자기주권신원 서비스 모델에 사용되는 Verifiable Data Registry(검증 데이터 저장소)는 블록체인의 수정 불가능한 특성(Immutable)을 이용해

표 3. 검증 가능한 자격증명 데이터 모델 용어
Table 3. Verifiable credentials data model terms

Term	Definition
Issuer (발행인)	Person or institution that issues Verifiable Credential
Holder (사용자)	A person who has a decentralized id and who creates a presentation for his identification and provides it to the verifier.
Verifier (검증인)	Role to validate by receiving at least one verifiable credential
Verifiable Data Registry (검증 데이터저장소)	Trusted repository distributed with roles that the system can perform by mediating identifiers, keys and verifications
Credential	Any information relating to a particular subject (people, organizations, animals, things, everything)
Verifiable Credential (검증 가능한 자격증명, VC)	Any kind of ID attribute value that can express oneself, including identification, graduation certificate, or relationships with others
Verifiable Presentation (검증 가능한 제공 ID 집합, VP)	Value machined only the attribute values needed to prove itself in Verifiable Credential

신뢰 가능한 저장소 기능을 구현하는 것이 일반적이다. 이때, Issuer(발행인) 또는 Holder의 서명 검증을 신뢰 된 환경에서 가능하게 한다.

그림 4에서 1~4번까지는 신원등록을 위한 사전작업과정을 나타낸 것으로 각각의 단계는 아래와 같다.

① Holder가 신원을 증명하기 위해서 Issuer에게 VC 발급 요청을 한다.

② Issuer는 자신 또는 기관의 서명과 함께 VC를 Holder에게 발행하고 전달해준다.

③ Issuer는 Holder에게 VC를 발급하는 동시에 자신의 서명과 함께, Holder의 검증정보를 블록체인(분산 저장소)에 저장한다.

④Holder는 VC를 취득 후 Issuer가 서명 한 내용에 자기 서명을 하고 블록체인(분산 저장소)에 DID를 저장한다.

a~d번까지는 Holder가 Service Provider에게 신원인증을 하는 과정을 나타낸 것이다.

ⓐ Service Provider는 Holder에게 서비스상에서의 신원인증을 요구한다.

ⓑ 이때, Holder는 Verifier에게 신원증명에 필요한 VC를 VP로 속성값을 추출한 후 제출한다.

ⓒ Verifier는 Holder에게 받은 VP를 기반으로 블록체인(분산 저장소)에 서명을 확인하고 문제가 없으면 검증을 완료한다.

ⓓ 이후 과정으로 Verifier는 검증된 Holder의 VP를 Service Provider에게 전달함으로써, Holder의 신원인증은 완료된다.

이와 관련된 연구들이 표준화를 위해 W3C(World wide web consortium)[30], DIF(Decentralized Identity Foundation)[31]를 중심으로 표준화 작업이 이루어지고 있으며, 국내는 DID Alliance를 주축으로 하고 있다.[32]

표 4. 국내 얼라이언스 특징
Table 4. Alliance features in Korea

	Initial Association	DID Alliance	MyID Alliance	MyKeepin Alliance
Features of Participating Companies	Mobile Carriers, large companies	International IT	Financial sector	International IT
Concept	Mobile Electronic Certificate Issuing Platform	Development of distributed ID standardization framework	Self-Sovereign Identity information platform	DID Commercial Service Development Platform
No. of Member	Mobile network operator (3), bank (5), card (2), IT service provider (3), terminal manufacturer (1)	Financial companies (3), securities firms (1), banks (10), credit card companies (5), IT service providers (44), handset manufacturers (3), Internet shopping malls (2), Blockchain Development (7), others (4)	News agencies (1), banks (6), card (1), securities firms (13), IT service providers (23), terminal manufacturer (1), insurance companies (7), travel agencies (1), Internet shopping malls (1), others (11)	Carrier (3), Media (3), Financial Services (10), IT Service (27), Media (3) Terminal Manufacturer (1), Consulting (1), Blockchain (15), Law Firm (1), Other (3)
Launch service	Mobile Electronic Proof Initials Launch	Omnione - Mainnet Launch	MyID service Launch	Metadium-based launch of DID kaibokippin
Relevant government departments	Ministry of Science and ICT, KISA	Ministry of Science and ICT, KISA	Finance committee	KISA
Blockchain Development Company	SK Telecom	Laonsecure	Iconloop	Coinplug

3. 국내 자기주권신원 서비스 현황

3.1 Alliance 현황

국내 자기주권신원 서비스들은 각각의 컨소시엄 또는 Alliance의 형태로 서비스가 진행되고 있다. 현재 국내 규제샌드박스의 승인받은 자기주권신원 서비스는 크게 DID Alliance Korea[33], MyID Alliance[34], Initial DID Association [35], Mykeepin Alliance[36] 4곳이 있으며, Alliance들의 특징은 표4에서 나타난다. 현재는 민간 주도하에 각각의 Alliance들과 지자체, 민간, 기업 등이 협동하여 상용화를 위해서 서비스가 이루어지고 있다. 하지만 Alliance별로 자기주권신원 서비스를 진행함에 따라 표준화 문제점이 발생하게 되는데, 이를 해결하고자 기관(한국인터넷진흥원, 금융보안원)에서 정책, 기술연구 및 표준화 추진 등을 위한 업무 협약과 가이드라인을 마련하고 있다.[37] 각각의 Alliance 주요 내용을 살펴보면 아래와 같다.

1) Initial DID Association

2019년 7월에 과학기술정보통신부와 함께 한국인터넷진흥원(KISA)이 주관하는 2019년 블록체인 민간주도 국민 프로젝트를 계기로 통신 3사(SK, KT, LG), 금융업체, 삼성전자 등이 참여한 DID 연합이다. 주 서비스는 컨소시엄형 블록체인 네트워크로써 모바일 전자증명 서비스 개발을 우선적으로 진행하고 있다.[38] 현재 서비스는 SK 텔레콤 주축으로 현재 상용화된 서비스는 'Initial' 이다. 이 서비스는 모바일 전자증명 앱에서 발급 및 제출을 원하는 기관에 접속해 원하는 증명서(통신사, 은행, 대학제증명 서비스 등)를 선택해 기관별 웹서비스에서 QR코드를 이용해서 증명서를 발급하고 제출할 수 있다. 다른 서비스와 차이점으로 Hyperledger Fabric[39] 기반으로 사용을 하고 있으며, Off-Chain[40]과 Selective Disclosure[41]를 접목하였다.

2) DID Alliance Korea

2019년 10월 DID Alliance 공식 활동을 시작으로, 분산 ID 서비스를 위해 설립된 비영리 재단이며, 금융결제원과 한국전자서명포럼, 한국FIDO산업포럼이 주축으로 서비스를 하고 있다. 특히, 글로벌 인증 표준화 및 국내 표준 DID 보급 확산을 주도하여 블록체인 기반 탈중앙화 신원인증 인프라 구축을 목표로 하고 있다. 현재 국내 참여기관으로는 금융결제원, 신한은행, NH농협은행 등 46개 기업이 있으며, 국외 파트너로는 소버린(Sovrin)과 시빅(Civic), 영국령 저지섬 정부 등이 있다. 현재 국내 서비스는 국내 보안 기업인 라온시큐어가 개발한 DID 기술인 옴니원을 기반으로 하고 있으며, 상용화한 서비스는 병무청- 인증서 없는 민원서비스 블록체인 플랫폼[42]에 DID(Decentralized Identity)[43], FIDO(Fast Identity Online)[44] 기술이 적용되었다.

3) MyID Alliance

2019년 6월 금융위원회로부터 아이콘루프의 마이아이디 플랫폼이 혁신 금융서비스 금융규제 샌드박스에 지정되었다.[45] 이러한 지정을 통해서 2019년 11월에 출범하여 자기주권형 디지털 ID 생태계를 구축하기 위해 마이아이디 플랫폼을 중심으로 운영되고 있다. 특히 기존시장의 문제점과 사용자들의 불편함을 해결하고자 아이콘루프를 주축으로 연구가 이루어지고 있다. 참여기관으로는 시중은행, 증권사, 등 다양한 분야의 73개의 기관과 기업이 참여 중이다. 현재 국내 서비스 '쯩'은 금융권에서 시행 중인 비대면 계좌 개설 과정에서 생성된 신원인증 정보를 사용자의 단말기에 저장해 두었다가 다시 비대면 계좌를 개설 시 저장된 정보를 제출할 수 있도록 한다.[46] 이때 상세한 정보 확인을 위해서 FIDO 또는 PIN 입력을 통해서 열람할 수 있게 한다. 마이아이디의 차별화된 전략은 범 금융권에 사용할 수 있는 유일 DID 서비스라는 점이다.

4) Mykeepin Alliance

2020년 4월에 출범한 Mykeepin Alliance는 코인플러그를 주축으로 블록체인 분산신원(DID) 기반 전자서명 및 비대면 본인 인증서비스 기반의 기업 연합체이다. 참여기관들은 예스24, 엘지유플러스, 파이낸셜뉴스, 디지털투데이 한빗코, 등 67개의 기업들이 참여하고 있다. 현재 국내 서비스 중인 마이키핀은 간편 본인확인/인증서비스로, 사용자가 DID 기반으로 제3자

의 개입 없이 직접 비대면 본인확인 및 인증요청을 처리할 수 있다. 이를 기반으로 THEPOL(온라인 투표, 여론조사 서비스), 가상자산 거래소한빗코, 부정거래 정보 조회 서비스, 부산시민 모바일 신분증 등을 나타내고 있다.[47]

이러한 4곳의 Alliance 특징에 따라서 서비스를 상용화하고 있고, 그 해당 서비스는 현재 금융권 위주로 출시가 되고 있다. 현재 연합체를 구성하고 있는 참여기업의 숫자가 계속 증가함에 따라 금융권뿐만 아니라 다양한 산업군으로 서비스를 확대하고 있는 추세이다.

3.2 데이터 3법 연계 금융권 서비스 현황

국내에서 데이터 3법이 개정되면서 가장 활발히 개인 데이터를 활용하는 곳은 금융권이다. 데이터 3법 중에서 신용정보법이 개정되면서 은행, 보험회사, 카드회사 등 흩어져 있는 개인 신용 정보를 모아 금융서비스를 제공하는 마이데이터 산업을 통해 지급 결제뿐 아니라 데이터 분야로 오픈뱅킹의 외연을 확장할 수 있게 되었다.[48] 이를 통해 기업들은 데이터 제공에 그치지 않고 분산 되어있는 데이터를 결합해 보다 의미 있는 정보를 창출할 수 있게 되었다. 국내 자기주권신원 기반으로 현재 진행 중인 금융권 서비스는 신한은행의 '쯩' 서비스와, 이동통신사 3사의 '모바일 신분증' 서비스로 표5에서와 같이 블록체인을 이용한 DID 방식을 이용하고 있다. 현재 시장 선점을 우위를 차지하기 위해 116개사가 마이데이터 허가를 위한 수

표 5. 국내 자기주권신원 금융권 서비스 현황
Table 5. Domestic self sovereign identity financial Services

Service	Agency	Contents
zzeung	Iconloop	ID card service (certificate, non-face-to-face account opening, etc.) using the block chain DID (identification) standard
Mobile ID card	Mobile carrier	A service that enables driver's license, renewal, identification, etc. with a blockchain-based mobile license through a simple personal identification app

요조사서를 제출했으며, 이를 기관별로 살펴보면, 금융회사 55개사, 핀테크 20개사, 비금융회사 41개사가 신청했다.[49] 이러한 서비스는 각 금융권 마다 출시 또는 출시 예정으로 현재 개발을 진행하고 있고, 향후에는 각 금융권마다 플랫폼을 통합하여 서비스를 진행하고자 목표를 두고 있다.

3.3 지자체 주도 서비스 현황

국내에서 지자체를 주도로 하는 자기주권신원 서비스 현황은 공공선도 시범사업과 블록체인 특구 사업으로 나누어서 진행 중이다.

먼저, 국내 지자체 공공서비스에 적용한 사업은 '2020 블록체인 공공선도 시범사업'으로 과학기술정보통신부와 한국인터넷진흥원(KISA)이 총괄하였으며, DID 플랫폼을 적용한 최초의 사례로 주목받고 있다.[50] 현재 라온시큐어에서 경상남도와 세종특별자치시에 DID 플랫폼을 시범 적용 중에 있다. 1) 경상남도와 라온시큐어가 손잡고 블록체인 기반의 분산신원증명(DID) 공공서비스를 통해서 스마트 도민(시민) 카드, 스마트 학생증 등 공공서비스 플랫폼을 각각 개발할 계획이다.[51] 2) 세종특별자치시에서는 블록체인 기반 자율주행 자동차 신뢰 플랫폼 구축 시 필요한 차량의 신원확인을 위한 블록체인 기반 DID를 사용하여 서비스할 예정이다.[51]

부산시에서 진행 중인 블록체인 규제 자유 특구의 사업 중 하나로 '부산블록체인체험'앱 사업을 통해서 코인플러그가 DID 기반 모바일 신분확인 체험서비스

표 6. 국내 서비스 현황
Table 6. Domestic service status

Group	Domestic service
Government	ID card (public official, driver's license), Self-certification (MMA)
Municipality	Citizenship card (Busan city, Gyeongsangnam-do), Blockchain-based self-driving car trust platform (Sejong Special Self-Governing City)
The private sector	Employee ID(Financial settlement agency), Driver's license

표 7. 2019-2020년 국가 R&D 과제 현황
Table 7. Status of national R&D challenges for 2019-2020

No	Supervising agency	Project Title	Research Objective
1	Ministry of Science and ICT	Blockchain-based on- and off-line and electronic signature service development	Compatible with international standards development of Mutual Authentication DID Service
2		Blockchain technology based Community operation and non-face-to-face decision-making technology development	Establishment of non-face-to-face meetings and communication platforms for DID-based non-face-to-face communication and operation of multi-family housing and local communities
3		Research on Blockchain based Decentralized Identifier(DID) Platform	Blockchain-based digital identification platform that stores personal information on your device and allows you to select and submit only the information you need to authenticate
4		Core Technologies for 5G-Aware Blockchain Networks	Development of blockchain technology for wireless terminals for 5G ultra-low latency service
5		Development of On-chain-based Electronic Contract Application Platform Using Zero-Knowledge Proof	Development of on-chain electronic contract application platform technology based on territorial knowledge certification technology for the management of contrasts between individuals and institutions
6		Development of Smart Contract Visualization Platform for User Convenience	Development of an application platform that supports smart contract visualization technology to improve the usability of blockchain services
7		Decentralized self-sovereign identity information management using blockchain Technology development	Development of blockchain-based decentralized self-sovereign identity information management technology that is not dependent on blockchain and can protect privacy
8	Ministry of SMEs and Startups	Blockchain-based cold chain trust platform	Blockchain platform for DID for autonomous sovereign identity verification of IOT sensors
9		Development of a safe remittance system using a blockchain-based proof-of-stake consensus algorithm	Interface development that can be linked with various authentication systems
10		Access control authentication system using blockchain-based distributed ID	Blockchain-based distributed ID platform construction
11	Ministry of Health and Welfare	Development of clinical data security management and dynamic agreement system platform using block chain technology	Development of user applications and server programs for storing clinical trial data and protecting personal information in patients, hospitals, and blockchain

를 제공하고 있다. 부산 시민 카드는 별도의 신분증, 증명서 제출을 하지 않고도 부산시민 신분확인 및 인증이 가능하다.[52] 이외에도 정부와 민간에서 진행 중인 서비스 현황은 표6과 같이 사원증, 모바일 면허증 서비스를 진행 예정이다.

4. 자기주권신원기술 관련 블록체인 기반 국내 연구 동향 분석

4.1 국내 R&D 과제 분석

NTIS(국가과학기술정보서비스)에서 2018년부터 현재까지 3년간 블록체인과 관련된 과제는 총 1015개가 도출되었다.[57] 그중에서 AND 검색식으로 자기주권신원, DID 내용이 포함된 연구로 좁혀보면 2019년 2개, 2020년 연임 과제 2개, 신규과제 11개로 나타났다. 개별 사업을 주관하는 기관은 과학기술정보통신부, 중소벤처기업부, 보건복지부로 3개의 부처에서 주관하고 있다. 각 과제의 수행 기관을 중심으로 보면 중소기업 8개, 연구소 1개, 대학 2개로 구성되어 기업주도형 과제가 많은 특징을 가졌다. 이는 블록체인 기술을 자기주권신원기술 분야에서 산업적 측면으로 활용하고자 하는 것으로 이해할 수 있다.

표7에서 나열되어 있는 국가 R&D 과제를 부처별 특징으로 보면 과학기술정보통신부는 개발(블록체인 융합기술, 기초연구, 비대면 비즈니스) 위주로 진행하

고 있으며, 중소벤처기업부는 시장확대형 과제와, 보건복지부는 의료데이터 관리체계를 중심으로 수행하고 있다. 표8에서는 각 과제별 특징을 그룹화하여 나타낸 것으로, 블록체인 기반 자기주권신원을 구현하기 위한 과제로는 모바일 신분증 및 단말기, 인증 및 인증서, 환자 및 병원 관련 내용이 주된 관련 내용이며 IoT 분야에서 센서의 자율적 주권신원 확인을 위한 기술 등의 연구 과제가 진행되고 있음을 확인할 수 있었다. 그중 기술별 특정을 뽑아내서 숫자 기호로 표현되어 있는 것은 DID의 특징을 나타낸 것이다.

표 8. 2020년도 DID 과제 특징
Table 8. Features of 2020 DID project

Technical feature	Project No	DID Relation
IoT/ 5G	④, 8	Identification certificate
Mobile I./Terminal	①, 3, 4	Distributed identity proof
Contract, Signature	①, ②, ⑤, 6	Distributed identity
Certificate	⑨, 10	Identification certificate
Patient, Hospital	11	-
Standardization	7	Identification certificate

4.2 국내 논문 연구 현황

블록체인 기반 자기주권신원기술과 관련해 국내 연구현황 분석을 위해 국내 학술논문 검색사이트인 DBpia를 활용하여 검색하였다.[53] 검색 조건은 Keyword 1, 2를 AND 조건식에 넣어 결과를 도출한 것으로 표9과 같다. 표9에서 Keyword 1인 Self-Sovereign Identity와 Self-Sovereignty는 공통의 Keyword를 가지고 있어 저널의 연구는 동일한 결과를 보였다. 연구의 특성을 비교하기 위해 국외의 경우 IEEE Xplore를 그 대상으로, 검색 대상은 2015년 이후 연구 결과물을 그 대상으로 한다.[54] 현재 국내의 경우 논문지, 학술대회에서 다루어지는 자기주권신원의 경우, 2019년 이후 데이터만 검색이 되었다. 기초연구와 응용연구를 분류하는 방법은 Keyword를 통해서 산업군의 분류가 포함되어있으면 이것을 응용연구(Applied Research, AR)로 하고 나머지는 기초연구(Basic Research, BR)로 보았다. 전체 연구 내용은 응용연구(DID 기반 홈쇼핑 FIDO 거래 인증 연구[55], 교통사고 센서 데이터 분석을 위한 DID 디지털포렌식 프레임워크[56])에 중점을 두고 있는 것을 확인할 수 있었다.

이는 해외 대비(Digital Identity 9건, Architecture 2건, DID 응용 9건, Digital Wallet 2건, Self-Sovereign Identity 8건, 기타 1건) 충분한 활용의 사례 및 기타 기술들과의 연계에 관해 충분한 연구가 이루어지지 않은 것으로 확인할 수 있었다. 단 현재 국내 연구의 경우 전체적인 논문의 수가 부족하여 데이터의 분석에 충분하지 않은 한계를 가지고 있다.

5. 자기주권 강화를 위한 블록체인 기관 DID 연구 제언

앞서 살펴본 바와 같이 현재 자기주권 강화를 위한

표 9. 국내 자기주권신원 논문 연구 현황
Table 9. Research status of domestic self-sovereign identity thesis

No	Keyword 1	Keyword 2	Domestic paper			International paper		
			Journal		Conference	Journal		Conference
1	Decentralized Identity or DID	-	3		2	3		21
			BR 1	AR 2		BR 1	AR 2	
2	Self-Sovereign Identity	-	1		1	5		31
		Blockchain	-		-	BR 2	AR 3	24
3	Self-Sovereignty	Identity	1		-	3		1
		Blockchain	-			BR 2	AR 1	2

표 10. 자기주권강화를 위한 DID 연구 제언
Table 10. DID research proposal for strengthening self-sovereignty

No	Research items	Research content	Utilityize
1	Selective Disclosure	Zere-knowledge Proof(ZKP)	Minimize personal information exposure
2	FIDO-linked interface	Simple authentication through biometric information without using a password	Electronic signature service
3	Linkage of public and private identifiers	Integrate distributed identifiers	Integrated platform
4	Insufficient Credential Standard	Identify user requirements	Structuraliz ation of Verifiable Credential
5	Certification period	Certificate validity period	Personal Information Protection
6	Domestic Poorly verified cryptographic modules	Poor verification of cryptographic modules of decentralized ID platform	Cryptograp hic module
7	Key management and recovery plan	A Research on the Application of Personal Keys in Mobile Loss	Mobile Terminal
8	Compatibility in case of saving terminal	Compatibility in case of using 2 or more USIMs	

연구는 신원증명 분야와 의료[58] 및 전자서명과 같은 응용 분야에 집중되고 있다. 개인정보보호를 위한 자기주권 강화 연구를 위해 이러한 연구 방향과 더불어 표10에서 제시한 8가지 항목의 연구를 제안하고자 한다.

먼저, 개인정보보호를 위한 핵심 연구로 크리덴셜 표준에 대한 연구가 이루어져야 한다. 이를 통해 사용자의 요구사항을 식별하는 데 있어 일관성 있는 구조를 사용할 수 있고, 선택적 공개를 통해서 모든 개인정보를 제공하지 않고도 서비스를 이용하여 개인정보 노출을 최소화할 수 있을 것이다.[59]

보안을 강화하기 위해 발급하는 인증서에 적정 기간을 두고 업데이트 방안 및 재발급을 받을 수 있도록 하고, 모바일 단말기에 신원증명을 저장할 경우 키를 관리하고 복구 방법을 마련하여 분실 시 개인 키 활용 방안과 관련된 연구가 필요하다. 특히 국내 검증필 암호모듈이 저조하기 때문에 이를 개선하여 분산 ID 플랫폼을 검증할 수 있는 암호모듈의 연구 및 개발이 필요하다.

그리고 자기신원주권기술을 활용하기 위한 연구로 공공 및 민간 식별자 연계 만들어서 분산되어있는 식별자를 통합함으로써, 추후 통합 플랫폼을 구현에 기반을 마련하고, FIDO 연계인터페이스를 통해서 비밀번호를 사용하지 않고 생체정보를 통한 간편인증으로 활용성을 증진하기 위한 방안의 연구가 필요하다. 또한 모바일 기반의 서비스 확산을 위해 2개 이상의 USIM을 사용하는 모바일 단말기에 신원정보를 저장하는 경우 상호 호환성을 제공하기 위한 연구 또한 필요하다.

이러한 연구를 기반으로 신원확인 기술의 개인정보 노출 및 오남용 사용문제를 해결하고, 자기 주권강화를 통해서 보다 신뢰할 수 있는 사용자 중심의 신원정보관리 기능을 제공할 수 있을 것이다.

그리고 마지막으로 현재 서비스의 경우 각 Alliance 별로 각자만의 특징을 가지고 자기주권신원을 강화하기 위한 서비스가 이루어지고 있다. 빠른 확산으로 인한 활용성 증가 측면이 있으나, 연합인증 때와 마찬가지로 여러 가지 앱을 사용해서 등록하고 사용을 하는 체계를 벗어나지 못하는 문제가 발생할 수 있다. 개선하기 위한 방안으로 특정 블록체인에 종속적이지 않고 프라이버시 보호가 가능한 자기주권신원 공통 플랫폼 개발을 통해서 관리가 필요하다. 특히, 국내의 DID 상용화는 금융권 분야를 위주로 이루어지고 있는데, 국제 표준화 기구인 W3C에서도 관련 de-factor 표준이 이루어지고 있어, 향후 호환성의 이슈가 예상된다. 따라서 국내에서도 관련된 표준이슈에 대한 논의 및 금융권 이외의 산업 분야들이 함께 논의를 통해 확장성 및 범용성을 가진 기술 개발이 이루어져야 한다.

6. 결론

본 논문에서는 자기주권신원기술 기반 국내 서비스 사례 및 연구 과제 분석을 통해서 개인정보 주권 강화를 위한 연구 방향을 도출하고자 하였다. 국내 자기주권신원기술 서비스들과 논문 및 연구 현황을 살펴본 바 현재까지 자기주권신원 관련 연구는 기초연구보다는 응용연구에 중점을 두고 있는 것으로 확인할 수 있었다.

최근 국제 표준화 기구인 W3C에서도 관련 de-factor 표준이 계속 진행됨에 따라 국내도 이에 대한 대응 및 관련 논의가 필요한 것으로 판단된다. 특히, 현재 국내 금융권 이외의 산업 분야들도 함께 논의를 통해 확장성 및 범용성을 가진 기술 개발이 이루어져야 한다.

본 논문에서는 자기주권강화를 하기 위한 핵심 연구 주제로 영 지식증명방법 및 크리덴셜 표준을 바탕으로 개인정보 노출을 최소화하고, 생체인증과 더 많은 암호 모듈 검증을 통해서 보안성을 향상시키고, 분산되어 있는 식별자를 통합함에 따라 통합플랫폼을 사용했을 때의 문제를 해결하고, 모바일 단말기 키 관리 및 복구방안 마련과 호환성 해결이 요구된다. 따라서 근본적인 자기주권강화와 관련된 문제점을 해결할 수 있을 것으로 예상된다. 향후 연구에서는 제안한 각 연구 요소들에 대한 추가적인 연구가 필요할 것이다.

REFERENCES

[1] Sang-kwang Kim, Sun-kyung Kim, The Effect of Personal Information Regulation Level and Data Combination on Big Data Utilization, KOTIS, Vol.23 No.2, pp. 305-323. Apr. 2020

[2] Min-chul Lim, KISA "Personal Information Paradigm, Protection + Utilization Change", ZDNetKorea, May. 01. 2017

[3] In-soon KIm, Change the paradigm of privacy and utilization, PRESS9, May. 07. 2017

[4] Privacy Protal, Understanding personal information, Retrieved Oct. 26. 2020 from https://www.privacy.go.kr/nns/ntc/inf/personalInfo.do

[5] Policy Briefing on the Republic of kore,Data 3 Law policy Brieging, Retrieved Oct. 9. 2020 from http://www.korea.kr/special/policyCurationView.do?newsId=148867915

[6] Jong-ho Han, Good!Bye, 'public certificate'the passage of a repeal bill by the National Assembly, Seoul Economy, May. 20. 2020

[7] Min-cheol Lim, public certificates that are about to be abolished, 46,000 cases leaked in the last two months... Most in history, Aju economy, Sep. 27. 2020

[8] Jae-hee Han, Competition to dominate the "digital ID card" market is heating up, seoul press, Jun. 21.2020

[9] Tae-yeong Jeong, Opening the Digital Identity Era, Safety Journal, Jul. 03. 2020

[10] Heon-young Kwon, The Possibility and Development of Blockchain Technology in the data Sovereignty Era, pp.17-27, IITP, Jul. 2020

[11] H. Gulati and C. Huang, "Self-Sovereign Dynamic Digital Identities based on Blockchain Technology," 2019 SoutheastCon, Huntsville, AL, USA, pp. 1-6, Apr. 2019

[12] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, Jul. 2019

[13] G. Malik, K. Parasrampuria, S. P. Reddy and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, pp. 1-6, Mar. 2019

[14] Sovrin, What is self-sovereign identity, Retrieved Oct. 26. 2020 from https://sovrin.org/faq/what-is-self-sovereign-identity/

[15] Security Technology Research Team (Security Research Division), Comparison of Identity Management Types and Characteristics, pp.1-6, Financial Security Agency, Mar. 2017

[16] H. Oh and S. Jin, "The Security Limitations of SSO in OpenID," 2008 10th International Conference on Advanced Communication Technology, Gangwon-Do, pp. 1608-1611, Apr. 2008

[17] N. Hossain, M. A. Hossain, M. Z. Hossain, M. H. I. Sohag and S. Rahman, "OAuth-SSO: A

Framework to Secure the OAuth-Based SSO Service for Packaged Web Applications," 2018 17th IEEE International Conference TrustCom/BigDataSE, New York, NY, pp. 1575-1578, Sep. 2018

[18] Christopher Allen, The Path to Self-Sovereign identity, Retrieved Oct. 26. 2020 from http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

[19] J. Fang, C. Yan and C. Yan, "Centralized Identity Authentication Research Based on Management Application Platform," 2009 First International Conference on Information Science and Engineering, Nanjing, pp. 2292-2295, Dec. 2009

[20] Security Research Department Security Technology Research Team, Comparison of characteristics and changes in identity information management types, pp.1-6, Financial Security Agency, Mar. 2020

[21] Dae-seon Choi, Sang-rae Cho, Seung-hyun Kim, Seung-hun Jin, Kyo-il Chung, "Internet ID Management Service", 14(5), pp. 32-43, Oct. 2004

[22] D. Choi, S. Jin and H. Yoon, "Trust Management for User-Centric Identity Management on the Internet," 2007 IEEE International Symposium on Consumer Electronics, Irving, TX, pp. 1-4, Nov. 2007

[23] T. Komura, Y. Nagai, S. Hashimoto, M. Aoyagi and K. Takahashi, "Proposal of Delegation Using Electronic Certificates on Single Sign-On System with SAML-Protocol," 2009 Ninth Annual International Symposium on Applications and the Internet, Bellevue, WA, pp. 235-238, Sep. 2009

[24] S. E. Haddouti and M. D. Ech-Cherif El Kettani, "Analysis of Identity Management Systems Using Blockchain Technology," 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), Rabat, Morocco, pp. 1-7, Jun. 2019

[25] Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, pp. 1336-1342, Jun. 2018

[26] Samjong KPMG economic researcher, The Beginning of the Data Economy, MyData: Focusing on the Financial Industry,samjon Insight, Vol.68, pp. 2-45, Jan. 2020

[27] Finance committee, Announcement of the Introduction of MyData Industry in the Financial Sector, Financial Services Commission Press Release, Jul. 18. 2018

[28] Young-ok Kang, The Role of Spatial Information for the Vitalization of the Data Economy, pp. 2-4, KRIHS, May. 2019

[29] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, Jul. 2019

[30] World ide web consortium, Retrieved Oct. 26. 2020, from https://www.w3.org

[31] Decentralized Identity Foundation, Retrieved Oct. 26. 2020, from https://identity.foundation

[32] DID Alliance, DID Alliance Korea 2019 conference with plenty to see, DID Alliance press Release, Oct. 23. 2019

[33] DiD Alliance, Retrieved Oct. 26. 2020, from https://www.didalliance.or.kr

[34] MyID Alliance, Retrieved Oct. 26. 2020, from https://myidalliance.org

[35] Initial DID Association, Retrieved Oct. 26. 2020, from https://www.initial.id/html/index.html

[36] Mykeepin Alliance, Retrieved Oct. 26. 2020 from https://mykeepin.org

[37] KISA, Kisa-Financial Security Agency, working together to build a digital identification system based on a block chain, KISA press Release, Dec. 17. 2019

[38] Hyun-suk choi, Initial Confirmation of Blockchain Network Service Name, including 3 Mobile Telecommunications Companies and Samsung Electronics, yunhap news, Oct. 20. 2020

[39] S. Kakei, Y. Shiraishi, M. Mohri, T. Nakamura, M. Hashimoto and S. Saito, "Cross-Certification Towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric," in IEEE Access, vol. 8, pp. 135742-135757, Jul. 2020

[40] C. Li, B. Palanisamy and R. Xu, "Scalable and Privacy-Preserving Design of On/Off-Chain Smart Contracts," 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW), Macao, Macao, pp. 7-12, Apr. 2019
[41] T. Balopoulos and S. Gritzalis, "Towards a logic of privacy-preserving selective disclosure credential protocols," 14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings., Prague, Czech Republic, pp. 396-401, Sep. 2003
[42] Laonsrcure, Retrieved Oct. 26. 2020, from https://www.raoncorp.com/ko/solution/omnioneenterprise
[43] Decentralized Identity, Retrieved Oct. 26. 2020, from https://www.w3.org/TR/did-core/
[44] Sang-rae cho, Dae-sun Choi, Seung-heon Jin, Hyung-ho Lee, Authentication technology without password-FIDO, pp.101-109, ETRI, Aug. 2014
[45] Ji-young Lee, Icon loop digital ID service Designated as Financial services commission innovation financial services, Daily economy, Jun. 26. 2019
[46] Zzeung, Retrieved Oct. 26. 2020 from https://www.zzeung.id/#/
[47] Seol-young Lee, Korea`s representative DID MyKeypin Alliance full-scale expansion of ecosystem, Financial News, Sep. 23.2020
[48] Sang-il Lee, Passing the Data 3 Act, raising expectations for the activation of innovative services in the financial sector, Digital Daily, Jan. 1. 2020
[49] Financial Services Commission, Results of MyData Permission Demand Survey (5.14~5.28 days) in Financial Sector - 116 companies in various fields want MyData business, Korea Policy Briefing, Jun. 3. 2020
[50] Ministry of Science and ICT, Report on the launch of the Blockchain pilot project by the Ministry of the Ministry of Science and ICT, Government24, May. 27. 2020
[51] In-sun Jeong, 2020 government-sponsored public institution block chain project general reorganization, KISA open 10 blockchain public-leading pilot projects this year, coindesk, Jan. 18. 2020
[52] Im-sook Lee, Busan City's Blockchain-based Mobile Identity Experience Service Starts, Busan pressRelease, Jun. 9. 2020
[53] DBPIA, Retrieved Oct. 10. 2020, from https://www.dbpia.co.kr/
[54] IEEEXplore, Retrieved Nov. 1. 2020, from https://ieeexplore.ieee.org/Xplore/home.jsp
[55] Hyeop-goo Yeo, Min-goo Kang, Seung-il Sonh, "A Study on the DID based Smart Remocon and FIDO Transaction Certification for Home-shopping", Smart Media Journal, Vol.9, No.1, pp. 60-66, Mar. 2020
[56] Jae-hun Hwang, Min-je Cho, Cheol-hee Yoon, "A Study on the Application of DID Digital Forensic Framework for Traffic Accident Sensor Data Analysis", Digital Forensic Research, Vol.14, No.3, pp. 221-238, Sep. 2020
[57] NTIS, Blockchain task, Retrieved Oct. 26. 2020, from https://www.ntis.go.kr/
[58] B. Houtan, A. S. Hafid and D. Makrakis, "A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare," in IEEE Access, vol. 8, pp. 90478-90494, May. 2020
[59] Seung-wan Chae, A Study on the Utilization of Decentralized ID Information Protection, pp. 74-99, Dong-A InfoSec 2020- Information Security & Privacy Conference, Feb. 2020

저자약력

이 정 현 (Jeong-Hyeon Lee) **[학생회원]**

- 2020년 2월 : 인제대학교 컴퓨터공학 (학사)
- 2019년 9월~현재 : 인제대학교 컴퓨터공학과 석사 재학 중

〈관심분야〉 개인정보보호, 블록체인, Decentralized ID, GDPR

김 지 원 (Ji-Won Kim) **[학생회원]**

- 2018년 2월 : 인제대학교 컴퓨터공학과 (학사)
- 2019년 9월~현재 : 인제대학교 컴퓨터공학과 석사 재학 중

〈관심분야〉 개인정보보호, 블록체인, GDPR, 의료데이터

김 철 수 (Chul-Soo Kim) **[정회원]**

- 2003년 2월 : 부산대학교 컴퓨터공학 (박사)
- 1985년~2000년 : 한국전자통신연구원(ETRI) TDX 개발 운용 SW 과제 책임자
- 2008년~2010년 : 지식경제부 네트워크 PD
- 2001년 9월~현재 : 인제대학교 컴퓨터공학과 교수

〈관심분야〉 네트워크 프로토콜, 트래픽 관리, 개인정보보호, GDPR, 블록체인

양 진 홍 (Jin-Hong Yang) **[정회원]**

- 2019년 2월 : KAIST 정보통신공학 (박사)
- 2017년 2월~2018년 1월 : HECAS 최고기술책임(CTO)
- 2017년 10월~현재: 한국과학기술원 IT융합연구소 겸직교수
- 2018년 3월~현재 : 인제대학교 헬스케어IT 학과 조교수

〈관심분야〉 데이터 컴플라이언스, 마이데이터, 헬스케어 데이터 활용