

## Self-Sovereign Identity (SSI: 자기주권신원) 연구 동향 분석: 사회경제, 법률, 기술적 고찰을 중심으로\*

손영진\*\* · 박민정\*\*\* · 박정숙\*\*\*\* · 황화정\*\*\*\*\* · 채상미\*\*\*\*\*

### 〈목 차〉

I. 서론	3.2 연구 설계
II. 본론	IV. 결론
2.1 사회경제 분야 연구동향	4.1 연구 결과
2.2 법률 분야 연구동향	4.2 연구 논의
2.3 기술 분야 연구동향	참고문헌
2.4 주요 선행 연구	Appendix.
III. 연구 방법	<Abstract>
3.1 연구 방법	

### I. 서론

4차 산업혁명 시대, 디지털이 중심이 되는 사회를 맞이하며 각종 디지털 기기들을 사용하여 다양하게 만들어 내는 데이터가 부를 만들어내는 중요한 자원이 되었다. 데이터 자체는 일종의 공공재로 더 많은 사람이 사용하고 활용하는 것이 미덕으로 여겨졌다. 그러나 최근 AI 및

빅데이터 등 정보기술의 발달로 인해 데이터는 산업화 시대의 원유와 같이 산업 성장의 핵심적인 자원으로 여겨지게 되었다. 또한 개인의 신원정보나 금융정보와 같은 개인정보는 온라인 기반의 새로운 비즈니스를 가능하게 할 수 있는 매우 전략적으로 가치 있는 데이터로 자리매김하게 되면서 온라인 기반으로 사업을 확장하고자 하는 기업들에 의해 적극적으로 수집되고 있다. 사용자가 서비스를 이용하고자 할

\* 이 논문 또는 저서는 2019년 대한민국 교육부와 한국연구재단의 인문사회분야 중견연구자지원 사업의 지원을 받아 수행된 연구임(NRF-2019S1A5A2A01050610)

\*\* 이화여자대학교 경영학과, teumdal@ewhain.net(주저자)

\*\*\* 이화여자대학교 경영학과, mjpark6767@ewha.ac.kr

\*\*\*\* 고려대학교 정보보호학과, 한국인터넷진흥원, finjspark@kisa.or.kr

\*\*\*\*\* 이화여자대학교 경영학과, LG CNS, hjhwang@lgcns.com

\*\*\*\*\* 이화여자대학교 경영학과, smchai@ewha.ac.kr(교신저자)

때 회원가입이라는 절차와 함께 이름, 주소뿐만 아니라 다양한 정보를 입력하게 되며, 간편한 결제를 위해 카드 번호와 같은 금융정보도 웹사이트에 제공하는 등 사용자의 편의를 위해 제공하는 개인정보(김종기, 김지윤, 2019)가 나날이 늘어나고 있는 실정이다. 실제 금융정보나 주민등록번호 등의 개인정보는 유출 시 개인에게 상당한 피해를 끼치게 되는 정보임으로 기업이 이를 수집하고 저장·관리하는 데 특별한 주의 및 노력을 기울여야 함에도 개인정보 유·노출로 인한 피해는 매년 증가하고 있는 추세이다.

개인정보보호위원회(2021)의 개인정보 침해 신고·상담 분석을 살펴보면 통계 자료가 제시된 2007년 총 25,965건에서 시작하여 2020년 총 177,457건으로 증가하였으며, 2010년 이후 매해 10만건 이상의 개인정보 침해건수가 보고되고 있다. 가장 많은 개인정보 침해 유형은 ‘주민등록번호 등 타인 정보의 훼손·침해·도용에 관한’ 것이며 2010년 이후 전체 침해의 52% 이상을 차지하고 있다. 일례로 보이즈 피싱과 같이 개인의 신상정보가 없다면 실행되기 힘든 범죄에 2020년 한국에서 발생한 피해 사례만 3만여 건, 피해액은 7,000억원에 달한다(천민아, 2021). 그 다음으로 많은 것이 ‘고지·명시한 범위를 넘어선 이용 또는 제3자 제공 침해’이다. 인공지능(AI) 대화 서비스인 ‘이루다’의 경우, 대화를 위한 학습에 사용한 개인 대화 기록의 비식별화 작업 미비로 인한 개인정보 유출 및 타 서비스 이용자들의 개인정보를 무단으로 이용하고 해당 이용 내용의 미고지 및 민감 개인정보의 무단 보관 등으로 서비스가 중단되고, 과징금을 부여받았다.

전세계적으로도 개인정보 유출로 인한 사회적 논의가 계속되고 있다. 2013년 11월 타깃 미국 1,797지점에서 약 4,000만 명의 개인정보가 유출됐고, 2014년 9월에는 Home Depot 미국 1,977매장, 캐나다 180매장에서 개인정보가 해킹되는 사고가 발생하였다(문진욱, 2014). 타깃은 이로 인해 총 1850만 달러의 배상금을 피해자들에게 배상하였으며, 우버는 2016년 60만 명의 운전기사 면허번호를 포함해 총 5,700만 명의 개인정보를 해킹당한 것을 승객이나 운전자에게 알리지 않고 숨겼다가 사건 1년 후 개인정보 유출 사실을 발표했으며 이로 인해 1억 4,800만 달러의 벌금을 지불하였다(문가용, 2018). 페이스북은 2019년 개인정보 유출로 인한 사용자 프라이버시 침해로 미국 연방 거래위원회에서 50억달러(약 5조 9,000억원)의 벌금을 부과받았다(우고운, 2019).

그러나 페이스북이 2019년 낸 벌금은 사용자들의 개인정보인 공개 프로필과 ‘좋아요’ 버튼을 누른 페이지 내용 및 타임라인 글 등을 이용하여 얻은 매출의 9%에 불과하다. 구글이 유튜브에서 광고 수입으로 얻은 매출은 2020년 한 해만 151억 달러이다. 이 광고는 구글이 사용자들의 검색 내용, 유튜브 영상 시청 정보, 방문 페이지 등을 분석하여 각 사용자의 특성에 맞게 송출하도록 하는 알고리즘을 통해 제공된다. 넷플릭스가 창업 후 빠른 속도로 자리를 잡을 수 있었던 것도 고객이 어떠한 영화를 보고, 어떤 평가를 내렸는지를 분석하는 시스템을 구축하고, 개인별 맞춤형 페이지를 제공할 수 있었기 때문이다.

컴퓨터나 휴대폰이 없이 일상생활을 할 수 없을 만큼 디지털화 된 사회에서 개인 정보 유

출로 인한 피해 때문에 웹이나 모바일 서비스를 이용하지 않을 수는 없다(전양 등, 2020). 또한 이미 많은 사람들이 언급했듯이 이미 현대 사회는 데이터 경제 시대로 전환되었고, 이러한 시대에서 데이터는 산업혁명 시대의 원유와 같이 없어서는 안 될 중요한 자원이 되었다. 데이터를 더욱 잘 활용하기 위해, 사용할 수 있는 데이터와 보호해야 할 데이터를 명확히 구분할 필요성이 점점 증대되었고 이를 위한 논의가 새롭게 시작되었다.

유럽연합(EU)의 일반 개인정보보호법(GDPR: general data protection regulation)(2018년 시행), 미국 캘리포니아 주의 소비자보호법(CCPA: california consumer privacy act)(2020년 시행), 한국의 데이터 3법 개정안(2019년 시행)은 개인정보에 대한 이전과는 다른 논의점을 제시한다. 개인 정보 사용에 대한 권한을 명시하고, 데이터 주권을 데이터 생성자 주체인 개인에게 돌려주려 하고 있다는 점이다.

유럽연합의 일반 개인정보보호법(GDPR)의 경우, EU 국민 또는 거주자의 데이터를 사용하는 모든 기업에 적용되며(박민정 등, 2019), 이들에게서 얻는 개인정보 데이터에 대해 컨트롤러, 프로세서 및 데이터 주체를 구분하며, 각자의 역할에 따른 법적 요구사항을 적용한다. 데이터를 생성하는 주체는 권리와 보호에 귀속되지만 데이터 컨트롤러와 프로세서-주로 사업체-에게는 이전보다 강화된 의무와 제재를 부과한다(Hardjono, 2019; Naik and Jenkins, 2020b). 만약 데이터를 사용하는 기업이 이를 어기게 되면 중대 위반의 경우 기업 전 세계 연 매출의 4% 또는 2천만유로 중 높은 금액(박민

정 등, 2018), 일반 위반의 경우 연매출 2%나 1천만유로 중 높은 금액에 해당하는 벌금을 부과할 수 있다. 실제로 구글은 프랑스로부터 개인정보에 대한 적법처리 근거부족을 이유로 5,000만 유로의 벌금을 부과 받았으며, 2020년 H&M 도 같은 이유로 독일에서 3,500만 유로의 벌금을 부과 받았다(원병철, 2021). 유럽과 달리 미국은 개별법주의의 법률체계를 가지고 있어 각 주 별로 적용되는 법이 다른 경우가 많다. 데이터와 관련된 법 중에는 캘리포니아주 소비자보호법(CCPA)의 경우 주 법률체계 중 개인정보와 관련된 데이터 사용에 대한 가장 광범위하고 포괄적인 규제를 담고 있다. 캘리포니아주의 경우 주민의 개인정보를 사용하고자 할 때, 기업은 소비자보호법(CCPA)을 준수해야 한다. 캘리포니아주 소비자보호법의 경우는 캘리포니아 거주민들에게 개인정보에 대한 폭 넓은 통제권을 부여한다는 점에서 GDPR과 유사하지만, 거주민들은 직간접적인 소비자의 위치에서 개인정보에 대한 통제권을 가진다는 점에서 차이가 있다. 또한 CCPA는 데이터 사용에 대한 사전 동의를 요구하지 않는다. 단, 사업자는 소비자들의 권리를 명확하게 제시하고, 이를 소비자들이 확인하여 자신의 정보의 제공, 삭제, 제 3자 판매거부 등을 할 수 있도록 해야 하며, 소비자는 사업자가 이를 위반한 경우 각각의 위반행위에 대해 민사소송을 제기할 수 있다(한국인터넷진흥원, 2021).

한국의 데이터 3법 개정안에서는 개인정보를 특정 개인에 관한 정보, 개인을 알아볼 수 있게 하는 정보로 한정하고 가명정보나 익명정보의 개념을 도입하여 데이터 사용의 분석, 이용의 법적 근거를 명확히 하였다. 개인 정보 처

리자의 책임성 강화 및 법 위반시의 과징금 도입 등 처벌도 강화하였다.

GDPR, CCPA, 데이터 3법 개정안 모두 주요한 쟁점은 정보주체가 자신의 데이터에 대한 제공, 삭제, 제3자 이용 등을 직접 제어, 관리할 수 있는 통제권을 가질 수 있어야 한다는 것이다. 현재의 데이터 시스템은 데이터를 수집, 이용하는 기관이나 기업이 그 통제권을 가지고 있는 중앙집중화된 시스템이다. 이러한 시스템은 서비스 제공자가 모든 사용자의 민감한 정보를 일괄적으로 저장, 관리한다는 측면에서의 편리성은 존재하지만, 항상 개인정보 유출의 위험성이 상존하며 정보주체가 본인의 데이터에 대한 통제권을 가지지 못한 채 서비스 제공자에게 종속될 수밖에 없다. 중앙집중화 관리 방식의 한계점을 개선하기 위한 다양한 기술 중에서도 특히 개인의 신원 정보 등과 같은 민감 정보를 중앙시스템이 아닌 블록체인과 같은 분산 시스템을 이용하여 제공하는 방식의 분산신원증명(DID: decentralized identifier)에 대한 관심이 높아지고 있다.

분산신원증명 기술은 자기주권신원이라 불리는 Self-sovereign identity(SSI) 개념을 바탕으로 하고 있는데, 이는 2016년 크리스토퍼 프레임워크에 의해 처음 제시되었다. 앨런은 디지털 아이덴티티와 자기 주권에 관한 10가지 원칙을 제시하며 사용자가 디지털 아이덴티티를 사용함에 있어 그 통제권이 사용자에게 있어야 함을 주장한다(Allen, 2016). SSI와 관련하여 가장 잘 알려진 소버린 재단은 SSI를 "어떤 중앙 당국에 의존하지 않고 절대 빼앗길 수 없는 평생 휴대 가능한 디지털 아이덴티티"(Tobin and Reed, 2016, p. 8)라고 정의하고 있다. 이러

한 SSI 개념이 주목받고 확산하기 시작한 원인은 다양하게 존재하나, 데이터 소유권 및 데이터 통제권 등 데이터 주권과 관련된 개인의 인식이 증가한 최근의 사회적 환경에서 기인하였다고 볼 수 있다(Der et al., 2017). 이러한 사회적 환경의 조성은 개인의 데이터 보호 활동을 넘어 특정 서비스 등을 이용하기 위하여 기업 및 기관에 데이터를 제공하는 등의 개인의 적극적인 데이터 활용에도 영향을 줄 수 밖에 없다. 따라서, 향후 데이터를 바탕으로 이루어지는 다양한 서비스 확산에 따른 데이터의 가치는 지속적으로 증가할 것으로 예상됨에 따라 (Benoti et al., 2020), 개인의 데이터 주권을 보장하면서 데이터를 적극적으로 활용과 보호할 수 있는 균형 유지의 방법이 필수적이다. 과거와 달리, 개인의 데이터 주권, 데이터 통제권 등의 보장 없이 무분별하게 개인의 데이터를 요구하거나 데이터를 활용하고자 하는 경우, 데이터 주체인 개인의 활발한 데이터 제공 활동을 유도하기 어렵기 때문이다. 이에 데이터를 기반으로 서비스를 개발 및 운영하기 위한 기업, 기관 등은 데이터 주체에게 개인정보 등을 비롯하여 정보에 대한 관리 권한 제공 등 데이터 주체의 소유권 보장의 방식을 바탕으로 데이터 주체로 하여금 적극적으로 데이터를 제공 및 활용의 동의를 유인하기 위한 전략 마련의 필요가 증가하였다. 따라서 사회적으로 SSI 개념의 역할과 의미에 대하여 현재 시점에서 살펴볼 필요가 있다. 그럼에도 불구하고 처음 SSI 개념을 제시한 앨런의 언급과 같이, 아직 통용되는 SSI의 정의나 규칙이 명확하지 않다. 이에 본 연구는 SSI에 대한 기존 연구를 검토하고 분석하여 다음과 같은 문제를 해결하고자 한다.

첫째, 최근, 사회경제, 법률 및 기술 분야에서 중요한 신원 인증 모델로 논의되고 있는 SSI에 대한 연구 동향을 제시한다. 둘째, 사회경제, 법률 및 기술 분야의 SSI에 대한 각각의 개념과 정의, 기대역할에 대한 차이점을 분석하여 향후 다양한 산업 분야 및 학문적 관점에서 공통적으로 통용될 수 있는 SSI 개념을 도출한다. 이를 통하여, 최종적으로 SSI 기반 향후 연구 방향의 토대를 제시함과 동시에 SSI 모델을 도입하고자 하는 기업, 기관 등에 시사점을 제공하고자 한다.

## II. 본 론

크리스토퍼 앨런은 “사용자가 자신의 디지털 아이덴티티를 통제할 수 있고 중앙 당국이 아이덴티티에 대한 권한이 없을 때 아이덴티티에 대한 자기 주권이 달성된다”고 말한다(Allen, 2016). 이와 더불어 앨런은 자기 주권에 대한 합의된 정의와 적용 가능한 규칙이 아직 확립되지 않았다고 설명하며, 실존성(existence), 통제권(control), 접근성(access), 투명성(transparency), 지속성(persistence), 이동성(portability), 호환성(interoperability), 동의(consent), 최소화(minimalization/disclosure), 보호(Protection)의 10가지 원칙을 제시하였다(Allen, 2016). 해당 원칙에 대하여 자세히 살펴보면, 먼저 실존성은 디지털 신원을 통제할 수 있는 주체 존재가 독립적이어야 함을 의미한다. 또한, 사용자의 개인정보에 대한 통제 권한을 사용자가 가져야 한다는 통제권과 사용자 본인 이 데이터에 접근할 수 있어야 하는 접근성에

대하여 설명한다. 그리고 사용자의 데이터를 처리하는 모든 시스템과 알고리즘은 사용자에게 투명하여야 함을 의미하는 투명성, 사용자의 개인정보는 중단 없이 보관되어야 하는 지속성, 사용자의 개인정보와 관련 서비스는 이동이 가능하여야 하는 이동성을 제시한다. 사용자의 개인정보는 필요에 따라, 상호 호환이 가능하여야 한다는 호환성, 사용자의 개인정보를 사용하기 위해서는 사용자의 동의가 필요하며 사용자의 정보 사용은 가능한 최소화로 이루어져야 한다는 최소화의 원칙을 준수하여야 한다. 마지막으로 사용자의 개인정보를 활용하는 과정에서 사용자의 권리가 보호되어야 한다는 보호 원칙으로 크리스토퍼 앨런이 제시한 10가지의 원칙은 구성된다. 이러한 디지털 아이덴티티에 대하여 Cameron(2005)은 "하나의 디지털 주체(예: 사용자)가 자신에 대해 또는 다른 디지털 주체에 대해 제기한 일련의 클레임"이라고 정의하여, 한 주체가 복수의 디지털 신분을 가질 수 있음을 암시한다. 카메론은 사용자가 의도된 목적을 위해 정보를 공개해야 한다고 설명하고, 다른 주체에게 제공된 정보만 소유자의 동의를 얻어 사용해야 한다고 하여 이 디지털 아이덴티티를 다루는 시스템은 속임수를 탐지하는 동시에, 즉, 중간에 있는 사람, 피싱, 제약 및 기타 사칭 공격을 막아내어 정보를 안정적으로 전달할 수 있어야 한다고 주장하였다. Sovrin은 SSI를 "어떤 중앙 당국에 의존하지 않고 절대 빼앗길 수 없는 평생 휴대 가능한 디지털 아이덴티티"라고 정의하였다(Tobin and Reed, 2016, p. 8). 이와 같은 SSI를 바탕으로 현재 SSI를 활용한 국내 서비스가 출시되기 시작하였다. 대부분의 국내 서비스는 민간 기업으로 구성된 컨소시엄을

비롯하여 지역자치단체가 참여하여 이루어지는 공공선도 시범사업 및 블록체인 특구 사업을 중심으로 이루어지고 있다(이정현 등, 2020). 이와 같은 SSI 기반 서비스들은 공통적으로 블록체인을 활용한 자기주권신원 증명 방식의 서비스 모델로 개인정보 주체가 원치 않는 정보까지를 제공하는 현존하는 신원 인증 방식을 개선하고자 한다. 따라서 앞서 크리스토퍼 앨런이 제시한 SSI의 10가지 원칙을 준수함에 따라, 최소한의 개인정보만 제공하는 신원 인증 모델 기반의 서비스 제공을 목적으로 한다.

## 2.1 사회경제 연구 동향

### 2.1.1 SSI의 탈중앙화 신원 패러다임 연구

Sovereignty는 사용자가 자신의 디지털 신원을 통제 가능해야 한다는 원칙이다(Baars, 2016). 사용자는 원하는 곳 어디에서나 자신의 신원을 사용할 수 있도록 해야하며, 특정 신원 제공자로부터는 독립적이다(Mühle et al., 2018). 그러나 오늘날 대부분의 신원 관리 체계는 기업, 기관, 조직과 같은 단일 주체가 시스템을 소유하고 제어하는 중앙 집중식이다. 시스템을 사용하기 위해서는 해당 주체가 제공하는 신원을 사용할 수밖에 없으며, 시스템을 벗어나면 해당 신원을 사용할 수 없다(Dunphy and Petitcolas, 2018). 세계은행그룹에 따르면 2018년 전 세계적으로 10억명에 이르는 사람들이 본인의 신원을 증명하는데 어려움을 겪는다(World Bank Group(2018). ID4D Annual Report). 현재의 신원 증명은 국가, 정부와 같이 신뢰할 수 있다고 믿는 중앙기관에게 사용자의

신원을 보증받는 시스템이다. 반대로 말하면 정부가 제대로 된 신원 인증 체계를 가지지 못하는 경우, 개인은 신원을 인증받을 수 있는 기회 자체를 잃기도 한다.

Der et al.(2017)는 국가기관 또는 온라인 서비스 제공업체 같은 ID 중앙제공자에 초점을 맞춘 접근방식에서는 개인이 이민과 같이 자신이 태어난 나라를 벗어나 거주지를 변경하는 경우, 이전 국가에서 사용하던 신원에 대한 액세스 권한을 잃고 새로운 신원을 부여받아야 했으나, 디지털 ID 관리나 SSI를 통해서 개인이 궁극적으로 자신의 신원을 완전히 제어할 수 있고 필요시 선택적 신원의 제공이 가능하다. 이처럼 SSI와 신원에 대한 연구는 신원관련 정보를 통제, 소유하는 주체가 학력증명의 경우 대학, 출생의 경우 출생국가의 정부, 경력 증명의 경우 회사와 같은 자격 증명 발급자에게 있다는 전통적인 관점(Zwitter et al., 2020)에서 벗어나 개인은 다양한 층의 신원 정보를 가질 수 있으며(Cameron, 2005), 중앙 조직의 여부와 상관없이 사용자가 직접 신원 데이터를 제어, 관리 할 수 있다는 새로운 패러다임과 탈중앙화의 특성과 통제권을 가장 잘 뒷받침 할 수 있는 기술인 블록체인을 바탕으로 한 분산ID 기술을 바탕으로 논의되고 있다.

신원은 각 식별자가 한 개인을 고유하게 식별하는데 사용된다는 “단일성”, 과 각 개인이 특정 도메인에서 하나의 식별자를 소유하는 “특이점”의 속성을 가진다. 중앙 집중식 시스템은 이러한 단일성과 특이점을 보장하기 위해 개인 정보를 수집해야 하며 이로 인해 시스템을 유지하고 관리하는데 많은 비용을 지불해야 하고 높은 수준의 개인정보 보안 시스템을 갖

출 것을 요구받는다. 그러나 분산 ID 기술을 사용하면 신원의 단일성과 특이점을 보장하는 중앙 시스템이 없더라도 신원 사용 사례와 자격 증명의 조합을 통해 다양한 신원을 선택적으로 부여받을 수 있으며(Wang and De Filippi, 2020), 불안정한 네트워크 연결 상황, 국가 신원보증 기관의 미비 및 시스템 인프라 부족의 경우에도 사용할 수 있다.

이민자나 난민과 같이 어떤 국가에서 아직 합법적 신분을 가지지 못해 사회적으로 소외된 사람들에게도 분산화된 신원 증명 기술을 통해 법적 신분과는 별개의 신원을 부여함으로써 개인의 의료 서비스와 같은 기본권을 제공받을 수 있으며(M. Shuaib et al., 2021), 어느 국가에서도 법적으로 인정되는 신분이 없어 사회에서 보이지 않는 사람들도 SSI를 통해 자신의 신원을 선택적으로 공유할 수 있고 이를 통해 구급, 추방의 위협에서 벗어나 Covid-19 검사, 의료 시스템의 접근 및 긴급재정지원을 받을 수 있도록 해야한다고 주장한다(Gans et al., 2021). UN 기구 전반에 걸쳐 식량 원조, 안보를 증진하고자 하는 WFP(world food programme)의 'Building Blocks'의 요르단에서의 사용 예시는 개별 신원을 부여하는데 있어 블록체인과 홍채 인식이 결합된 시스템을 통해 일정 수준 이상의 인터넷 연결과 스마트폰 등의 고도화된 기기를 지원 대상자 모두가 소유하지 않아도 식량이나 기금과 같은 자원에 접근할 수 있음을 보여주었다(Wang and De Filippi, 2020).

국가 신원보증 기관의 미비나 시스템 인프라를 자기주권으로 해결하고자 하는 연구흐름도 있다. Freytsis et al.(2021)은 서남 아프리카의 낮은 출생 신고율을 해결하려는 방법으로 케냐

에서 블록체인 기술을 통한 신원 부여 방식을 고안하였다. 아프리카의 부족한 인프라로 인해 많은 아이들이 출생신고조차 하지 못한 채 자라나 사회적인 신원을 가지지 못한다. 아이가 태어남과 동시에 산모와 아이, 보증인을 함께 블록체인에 등록시키는 방법으로 영구적인 신원을 부여하고자 했다. 금융서비스에서 요구하는 신용과 같은 신원은 신뢰받을 수 있는 확인자를 더욱 요구한다. 시에라리온에서 진행된 Kiva 프로젝트는 정부나 인프라의 미비로 법적으로 증명 가능한 신용정보를 만드는 것이 어려워 이를 서비스 요구자에게 제공할 수 없는 경우 신용 기반의 서비스를 이용하는 것은 거의 불가능한 사람들이 SSI를 이용하여 신원을 보장받고 소액 대출과 같은 은행 서비스에 편입할 수 있음을 보여준다(Wang and De Filippi, 2020).

에스토니아의 e-residence 시스템은 SSI를 이용하여 에스토니아에서 태어나지 않았더라도 에스토니아의 가상 거주자가 될 수 있게 한다. 가상 거주자들은 에스토니아의 디지털 국가에 합류하여 EU 국가에 자유롭게 투자할 수 있다(<https://e-resident.gov.ee/become-an-e-resident/>). 이는 자기주권을 이용해 다양한 신분을 부여할 수 있음을 이용해 새로운 법적 신원을 부여한 것이다.

### 2.1.2 기존 데이터 생태계와 SSI 연구

개인이 가진 데이터 중 개인이 경험하거나 이미 가지고 있어 추후에도 변하지 않는 사실들과 관련한 데이터의 이용, 예를 들면 자신이 졸업한 학교, 기간 제한이 있지 않은 자격증의 소유나 퇴직한 회사, 수술 병력과 같은 사실들에 대한 이용과 관련하여 사용자가 직접 자신

의 정보를 관리할 수 있다면 불변하는 정보를 인증받기 위해 각각의 기관에 요청할 필요가 없다. Grech et al.(2021)은 사용자가 받은 교육 및 학습에 대한 인증을 교육기관을 거치지 않고 확인할 수 있는 블록체인 바탕 디지털 자격 증명 생태계를 제안했다.

의료 데이터는 개인의 극히 민감한 정보를 담고 있기에 정보 이용에 있어 많은 법적 제약을 받는다. 의료분야에서 건강/의료 데이터의 정보주체는 개인이나 본인의 의료 데이터에 대한 권리주장 방법이 미흡하다(오현택, 양진홍, 2020). 때문에 본인의 의료 데이터를 활용하기 어렵고, 각 기관에서는 충분한 활용 가치가 있는 데이터가 제대로 활용하지 못하고 폐기된다. 이러한 문제를 개선하기 위해 개인의 건강/의료 정보와 관련하여 환자의 극히 민감한 정보가 담긴 디지털 데이터를 효과적으로 보호하면서도 다른 기관으로의 이동을 가능하게 하고, 상호 운용가능한 의료 생태계를 구현할 수 있는 방법으로 SSI를 통한 환자 본인의 정보 통제 방안을 제시한다(Mohammed Shuaib et al., 2021). Houtan et al.(2020)는 의료 빅데이터의 활용에 SSI를 통한 환자 자신의 의료 데이터 통제력 부과, 의료 데이터 공유를 위한 어플리케이션 제안 및 탈중앙화 수준과 개인정보보호 수준의 균형 조사를 통해 블록체인기반 디지털 아이덴티티의 사용이 환자 데이터 관리 및 환자의 데이터 자주권을 구현하는 유용한 방법임을 제시하였다. 그러나 Siqueira et al.(2021)의 연구에서는 의료 전자 건강 기록(EHR)을 처리하는데 있어 SSI를 제안한 많은 연구들을 분석한 결과 블록체인 기술은 현재의 시스템의 실현 가능한 대안이나 데이터 소유나 자기주권과 같은 개념

이 아직 의료 환경에서 정의되지 못해 SSI가 채택되지 못하고 있음을 밝혔다.

데이터 통제가 강해질수록 사장되는 데이터가 많아진다. 이를 해결하기 위해 SSI를 통한 데이터 통제권을 개인에게 제공하면서도 개인에게는 인센티브를 제공하고, 기업은 허용된 데이터 사용을 통해 이익을 얻을 수 있는 데이터 이코노미 모델이 연구된다. Wittek(2020)는 특정 커뮤니티 내에서 특정 소비 행동에 대한 개인 데이터를 제공하는 경우 인센티브 토큰을 받는 형태의 기술 모델을 제안하여 데이터 사용에 대한 허가 뿐 아니라 그로 인한 이익까지 공유할 수 있는 모델을 제시하였다. Kim(2021) 또한 웹에서 개인이 데이터 제어권을 가지지 못하는 구조를 벗어나 데이터 자산 생성자와 구매자 간의 비대면 신뢰성을 확보하고 생성자가 데이터 유통시 통제권을 가질 수 있는 데이터 유통플랫폼 구조를 제안하였다.

신원 확인의 과정은 꼭 필요하지만 불필요한 개인정보가 노출되거나 제3자의 신원 도용과 같은 문제가 발생하기도 한다. Ahmed et al. (2020)에서는 은행이 서비스를 제공하거나 개인이 은행서비스를 사용하기 위해 고객 신원을 확인할 때 전화나 메시지, 이메일과 같은 수단에서 확인 당사자가 아닌 사기꾼과 같은 제 3자의 정보 도용이 일어날 수 있으며, 사기나 신원 도용의 문제의 해결을 위해 분산 데이터 저장 및 디지털 지갑과 같은 블록체인이 제공할 수 있는 장점을 이용한 SSI 솔루션을 도입할 것을 제안하였다. 유럽의 대중교통 시스템은 여러 국가의 서로 다른 사업자에 걸쳐있다. 기존 신원 체계에서는 각 운송업체마다 하나씩 여행카드가 필요하나 SSI 프레임워크에서는 분산 ID를

통해 표준화된 여행자격 증명을 활용할 수 있다(Stockburger et al., 2021).

### 2.1.3 SSI 패러다임 변화 연구

오히려 분산원장기술기반 ID가 새로운 통제 기구를 만들어낼 것이라는 연구도 있다. Gstrein and Kochenov(2020)는 디지털 신원의 확대에 대한 목표는 좋은 신원에 대한 희망이지만 이미 존재하는 정체성과 국력에 따른 시민권 사이의 불평등을 해결하지 못한다면 디지털 신원은 오히려 선진국의 특권적 지위를 보강하고 전통적인 신분 관리 시스템에서 나타난 유리천장을 강화할 것이라고 주장하였다. 예멘 분쟁에서 세계식량계획(world food programme)은 홍체인식 등록 시스템 도입을 거부한 후티 반군이 통제하는 예멘 지역에 대한 식량 지원을 중단하였다. SSI를 통한 탈중앙 신원부여와 생체인식 시스템은 소외된 사람들을 위해 사용되어 중앙기관의 권력을 분산시키는 것처럼 보였지만 WFP의 지원 중단은 결국 이러한 시스템도 식별, 확인 권한이 있는 기관이 리소스에 대한 액세스 권한을 결정할 권한도 있다는 점을 보여주며 신원 데이터베이스의 구축이 새로운 권력을 창출하는 것과 연관될 수 있음을 암시한다(Martin and Taylor, 2019). 마찬가지로 당장 개인에게 디지털 아이덴티티의 통제권을 주는 것이 이득인지, 기술 제공은 어떻게 할 것인지의 문제에 있어서도 사용자의 데이터 통제권이 현재의 데이터 활용 생태계와 사용자 중심 데이터 생태계와의 충돌되는 논의가 되는 만큼 SSI는 더욱 현재의 데이터 생태계 및 사용자들에게 받아들여질 충분한 이해를 제공해야 하며(Lockwood, 2021) 기술적인 부분에 있어

서도 신뢰 가능한 방안을 제시해야 한다.

사회 경제와 관련한 연구에서는 신원 관리 체계와 관련하여 전통적으로 신뢰받는 국가나 정부, 구글과 페이스북, 인스타그램과 같은 거대 데이터 독점 기관으로의 집중화를 벗어나 개인이 자신의 신원의 다양한 속성 중 하나를 선택하여 생성, 제공할 수 있는 SSI의 특징을 새로운 패러다임으로 수용하여 신원부여 및 확인 기관의 독점화, 개인 데이터 사용을 통한 경제적 이득에서 데이터 주체가 소외되는 문제, 개인정보 유출과 같은 문제를 해결하고자 한 사례들의 효과를 분석하거나 향후 SSI를 적용하여 이러한 문제를 해결할 경우 사회에 미칠 잠재적 효과를 논의하였다. 또한 사회 패러다임 변화 과정에서 나타날 수 있는 SSI와 기존 데이터 사용 생태계와의 공존가능성 또는 상충의 문제와 이 과정에서 사용자들이 겪게 될 혼란에 대해 논의한 연구도 진행되고 있다. SSI의 개념적인 탐구보다는 실증적 사례 연구를 통해 SSI가 가진 사회/경제적 파급효과 검증 및 발생 가능한 문제와 해결책이 있는지 살펴보는 연구가 진행중이며, 개인의 통제권이 배제된 데이터 생태계가 가진 다양한 사회문제를 해결할 수 있는 장점을 SSI가 가지고 있으며, 점차 개인의 데이터 주권을 보장하는 데이터 생태계로 사회적 패러다임이 이동하고 있음을 보여준다.

## 2.2 법률분야 연구 동향

### 2.2.1 법제도 관점에서의 SSI

정보주체의 개인정보들은 많은 기업이나 기관에 중앙집중화 되어 있는 구조였으나 최근에는 점차적으로 정보주체가 자신의 개인정보를

통제하고 소유권을 찾아가는 방향으로 패러다임이 전환되고 있는 시점이다. 법제도 측면에서 유럽연합(EU)은 일반 개인정보 보호법(GDPR, 2018), 미국은 캘리포니아 소비자 프라이버시법(CCPA, 2019) 등으로 개인의 데이터 소유권을 강화하고 있는 추세이며, 데이터 소유권과 관련한 법·제도를 마련하고 있다(여기호 등, 2020). 한편, 국내에서는 마이 데이터(MyData) 산업으로 통칭되는 금융분야의 새로운 데이터 서비스 사업에서 시작하여 데이터 3법(개인정보 보호법, 정보통신망법, 신용정보법)의 개정을 통해 본인의 특정 데이터, 데이터 전부에 대해 사용 또는 활용 여부를 기업에서 직접 요구할 수 있는 권리를 가지게 되었다(데이터 3법, 2020).

최근 코로나19 사태로 인해 급격한 비대면 디지털 사회로의 전환이 이뤄지고 있으며 이로 인한 개인 데이터 중앙집중화의 부작용과 보안 문제들이 불거질 가능성도 높아지고 있다(박진아, 2020). 이에 대한 해결책으로 정보주체가 개인 데이터에 대한 열람·제공 범위·접근 승인 등을 직접 결정함으로써 개인의 정보 활용 권한을 보장하고 데이터 주권을 확립하는 패러다임인 SSI가 점차 주목받고 있다. SSI는 블록체인 기술 발전으로 대두된 개념으로 개인이 직접 자기의 정보를 보유하고 신원을 인증하는 방식을 말한다(고영미, 2021).

### 2.2.2 법과 SSI의 상충 연구

블록체인 기반의 신원인증이나 범용성 문제는 SSI가 개인정보에 대해 기존과는 다른 서비스 모델로 구축되기 때문에 발생한다. 기존 신원 인증은 서비스 제공 기관을 통해 이뤄졌다면 SSI는 정보주체의 결정권과 통제권을 보장

해야 하기 때문에 신원 인증 기술의 중심이 정보주체에게 있어야 한다. 이러한 변화는 기술적 안정성뿐만 아니라 그 척도로서 규범성의 확보가 전제되어야 한다. SSI에 대한 법적 평가를 하기 위해서는 법적 사실이 있어야 하고, 블록체인 기술에 따른 법적 행위는 이미 존재하는 현실이지만 그에 대한 규범성 부여는 우리의 법이 과학기술의 개발을 보장한다는 측면에서도 더욱 세심한 접근이 필요하다(송영현, 2021). 따라서, 블록체인과 같은 개인 데이터의 자기주도적 관리 기술의 사회적 및 법적 수용에 지속적으로 관심을 가져야 하며(박진아, 2020), 블록체인 기술이 각종 사회적 위험성을 제거하고 보안성과 투명성을 보장받기 위해서는 블록체인의 고유한 특징을 확인하고, 이 특징이 블록체인의 상용화 및 국내 개인정보 보호 법제와 어느 면에서 상충되는지를 고려하여 법안을 만들어야 한다(고영미, 2021).

SSI는 그 실현을 위해 블록체인을 바탕으로 한 DID를 사용한다. DID 시스템은 ID 관리 환경에서 중요한 역할을 하고 SSI 시스템은 신원에 대한 통제권을 개인에게 되돌려 주려고 약속했으나 여전히 기존 규제 프레임워크에 대해 평가되고 있다(Penedo, 2021). 현재의 법률은 아직 단일 조직이나 서비스 제공자가 ID 를 설정하고 관리하는 중앙 집중 ID 시스템을 바탕으로 논의되고 있으며, 때문에 개인이 자신의 신원을 직접 제어하여 서비스를 사용할 때 본인의 자격을 원하는 방식으로 증명하는 블록체인 DID의 탈중앙화, 분산화 등의 특성과는 상충되는 부분이 존재한다. 그러나 GDPR은 자연인(natural person)에 관한 개인정보 보호권을 보장하는 동시에 유럽연합(EU) 역내에서의 개

인정보의 자유로운 이동을 보장하기 위해 제정되면서 보다 강력하고 통일된 개인정보 보호 규제가 가능하게 되었다(GDPR 대응지원센터, 2020). GDPR에서는 유럽연합(EU) 데이터 주체의 개인 데이터가 처리되는 경우에만 적용되므로 개인 데이터가 없는 경우에는 적용되지 않으나(Naik and Jenkins, 2020b), 개인이 데이터 컨트롤러에게 개인정보 처리에 관한 정보와 데이터 이동·처분을 요구할 수 있도록 하고, 컨트롤러는 법적 요구가 있을 때마다 이를 수행할 수 있는 시스템을 강제로 보유하도록 하는 등 개인의 데이터 통제권을 상당한 수준으로 강화할 것을 회원국에게 강제하면서 개인의 데이터 주권 강화의 법률 제정에 선도적인 흐름을 만들었다(권현영, 2020).

블록체인 기술은 중앙 관리자가 아닌 데이터를 제공하는 주체들이 직접 신원을 관리하는 기술이기 때문에 관념상 데이터 주권 확보를 위한 다양한 모델 구현에 대한 시도가 가능하지만(권현영, 2020), SSI의 어떤 데이터 구성요소가 개인 데이터를 구성하는지, GDPR이 어떻게 적용되는지, 누가 컨트롤러로 간주되는지 그리고 어떤 정당성이 존재하는지를 결정하기 위해 사용된 시스템과 사용 사례에 대한 상세 분석 논의가 필요하다(Kondova and Erbguth, 2020). GDPR은 주로 정의된 역할이 있는 중앙 집중식 네트워크 설계에 초점을 맞추고 있고 SSI는 주로 모든 사람이 동등한 액세스 권한을 갖는 분산네트워크 설계인 블록체인 기술을 기반(Naik and Jenkins, 2020b)으로 하고 있다. ID 속성 자체는 개인 데이터로 간주될 수 있고, 식별되거나 식별 가능한 자연인과 직·간접적으로 식별할 수 있는 사람도 개인 데이터로

GDPR 규칙의 적용이 가능하다. 또한 Penedo (2021)는 SSI 시스템이 제대로 작동하면 요청된 데이터에 대해 자세히 알 수 있기 때문에 개인 데이터 사용 방식에 대해 제어가 가능하여 DID는 GDPR 구현에 사용이 가능함을 밝혔다.

하지만, 불변형 블록체인에 일부 데이터를 저장할 때는 블록체인에 저장된 데이터가 개인 데이터를 구성하지 않거나, 데이터 주체가 컨트롤러로 간주되거나, 사용자에게 대한 면제가 적용되는지 또는, 블록체인에 지속적으로 저장될 수 있는 영구적 정당성이 존재하는지 확인하여야 한다(Kondova and Erbguth, 2020). 블록체인의 속성상 삭제와 파기가 힘든 문제, 정보보호책임자 지정 등 관리 책임 귀속의 어려움은 현재 개인정보 보호법 체계와 상충되는 점이 많다(권현영, 2020).

### 2.2.3 법과 SSI의 상호보완 제안

개인정보를 보호하면서 적극적으로 활용할 수 있도록 하려면 데이터를 데이터의 주인이 완벽히 통제할 수 있는 제어 가능성이 중요해질 것이다. 블록체인 기반의 SSI 기술을 활용한 새로운 산업 발전을 지원하고 개인정보를 보호하기 위해서는 데이터 통제권에 대한 적절한 법률체계 구축을 위한 법제 정비가 필요하다. 통제권의 관점에서 현행 법체계의 사전 고지·동의 요건은 거래비용을 높이고 오히려 데이터 소유권 행사를 방해하는 잘못된 규제이며 이해상충의 핵심을 이루는 형식적인 규제이다(박상철, 2018).

자주적으로 개인의 신원을 증명하기 위한 다양한 기술적 진보와 함께 SSI 플랫폼이 급속도로 성장하고 상용화되면서 암호화 프로토콜 및

사용자의 프라이버시를 강화하는 체계에 대한 인식과 연구도 증가하고 있다(Soltani et al., 2021). SSI은 무허가, 상호 운용 가능하고 분산된 디지털 신원 프레임워크를 만드는데 분산원장기술이 제공하는 기회를 완전히 실현하기 위한 전제조건으로 간주되고, 채택된 접근방식에 있어 확실성·예측가능성·투명성을 창출하는데 그 핵심이 있다. Lim(2020)의 연구는 크리스토퍼 알렌이 고안한 SSI의 10가지 기본원칙을 반영하는데 있어 기술과 정책의 상호작용이 중요함을 강조하고 있다. 예를 들면, 인터넷 프로토콜(TOIP) 스택을 검토하는데 있어서도 법률준수의 필요성을 반영할 필요가 있으며, SSI를 기술적으로 실현하는데 있어 관련된 법적 확실성을 확보하는 것은 중요하다고 논의한다. 이를 위해서는 관련 데이터 및 개인정보 보호법을 적용한 SSI를 위한 신뢰 정책 프레임워크(TPF) 개발이 필요하며, 기본 법률 원칙의 구현과 함께 관찰권 간 데이터 및 개인정보 보호법을 고려하여 정책 프레임워크를 만드는 것이 필요하다고 논의한다. 또한 신뢰할 수 있는 디지털 신원을 소개하는 정책 입안자는 근본적이고 지속적인 정책 결함을 해결하기 위한 법적 원칙과 가치의 적용을 고려하여야 한다고 지적한다(Lim, 2020). Soltani(2021)의 연구에서 SSI 모델은 개인에게 자신의 ID 속성을 제어할 수 있는 권한을 부여하고 개인정보 보호 및 신뢰를 유지하면서 네트워크의 ID 보유자와 기타 엔티티 간에 자격증명을 간소화하여 교환을 허용하는데 이는 개인정보를 취급하고 소비자를 보호한다는 측면에서 GDPR의 목표와 일치한다

법률 분야에서는 SSI가 신원에 대한 권한을 사용자가 스스로 관리하고 통제할 수 있는 디

지탈 신원인증 체계이며, 사용자의 프라이버시를 강화하는 체계(Soltani et al., 2021)라는 인식과 연구가 증가하고 있다. SSI의 패러다임을 법률에서 어떻게 수용할 수 있을지, 현행 법체계와는 어떠한 점에서 상충되는지에 대한 연구가 지속적으로 이뤄지고 있으며, 법·제도 측면의 거래 기반 조성없이 SSI 기술만 활성화된다면 우리 산업과 경제의 혼란이 가중될 것으로 예상하고 법적인 측면과 과학기술의 발전을 고려하여 상호 보완적으로 발전해 나아가야 한다고 논의하고 있다. SSI 기술을 활용한 새로운 산업 발전을 지원하고 개인정보를 보호하기 위해 법·제도적 측면에서 국·내외적으로 SSI 기술의 발전에 상충되지 않는 통합적인 시각과 이에 대한 입법적인 보안을 고민해야 한다.

## 2.3 기술분야 연구 동향

### 2.3.1 초기 SSI 기술 연구(2016~2017)

SSI 개념을 기술적으로 해결하려는 노력은 사회적 환경과 정보기술의 발전에 따라 꾸준히 변화해왔다. 2016년 SSI 개념을 제안한 앨런의 연구를 기점으로 초창기에는 앨런이 제기한 10대 원칙에 대한 해석과 추가 및 원칙의 기술적 구현에 필요한 컴포넌트를 논의하는 연구부터 2021년 현재 의료 등 다양한 분야 적용에 이르기까지 매우 많고 다양한 측면에서 이루어져왔다. 이에 따라 기술 분야에서는 SSI 관련 기술적 연구가 시기별로 어떻게 변화했는지 검토하여 SSI가 개념에 그치지 않고 이를 실제 서비스로 구현, 제공하기 위해 어떠한 기술적 노력들이 있었는지 및 향후 어떠한 기술들이 연구될지를 살펴보았다.

크리스토퍼 앨런은 SSI의 비전을 공유하였지만 스스로도 Self-sovereign identity가 무엇인지, 어떤 규칙을 가져야 하는지에 대해 명확하게 제시하지 못하였다(Allen, 2016). 2016년 앨런의 제안 이후 초기 SSI에 대한 연구는 SSI의 정의와 이를 구성하는 기술 요소들을 다루는 논문들로 이뤄져 있다. Baars(2016)는 앨런이 제시한 SSI의 10가지 원칙을 달성하고 디지털 아이덴티티를 구현하는데 있어 블록체인 기술을 기반으로 하는 DIMS(decentralized identity management system)의 PoC를 제안하였다. 엔티티가 단일 중앙 기관에 의존하지 않고 속성을 교환하고 클레임을 확인할 수 있도록 분산된 ID 관리 아키텍처를 설계하는 방법을 연구하였으며, 다소 이른 논의이지만 블록체인 프로토콜이 다양해질 경우 상호운용성의 필요성 또한 언급하고 있다. Andrew Tobin과 Drummond Reed은 Sovrin 재단의 백서에서 인터넷 아이덴티티의 진화는 세 가지 기본 요구사항(security, control, portability)을 충족시키려는 노력의 결과라고 하며, SSI를 정의하기 위해 크리스토퍼 앨런의 자주권 정체성의 10가지 원칙을 10개의 단어로 요약하고 이를 세가지 기본 요구사항에 매핑하였다(Tobin and Reed, 2016). 세가지 기본 요구사항이란 첫째, 신원정보는 의도하지 않는 노출에서 보호되어야 하고, 둘째, ID 소유자는 자신의 데이터를 알고 접근할 수 있는 통제권이 있어야 하며, 셋째, 자신의 신원 데이터는 원하는 곳 어디서나 사용 가능하고 서비스 제공자에 종속되어서는 안되는 휴대성이 있어야 한다는 것이다. SSI를 위한 신뢰할 수 있는 새로운 인프라의 필요성을 제기하며, DLT(분산원장기술)는 이를 가능하게 하는

획기적인 기술이라고 언급한다. 분산원장기술은 얼마동안 사용되었지만 bitcoin 및 ethereum과 같은 새로운 DLT가 분산 키 관리 및 암호화된 클레임의 Peer-to-Peer 공유와 결합될 때 DLT는 최종적으로 SSI를 가능하게 한다고 하며, 블록체인을 탈중앙화의 파워를 가진 SSI의 핵심 기본 기술로 설명하고 있다(Tobin and Reed, 2016).

### 2.3.2 SSI와 블록체인, DID (2018~2020)

2018년의 논문으로 현재 기준 피인용횟수가 가장 높은 Mühle et al.(2018)의 연구에서는 SSI는 아직 느슨하게 정의된 개념으로 본질적으로 개인이 자신의 디지털 ID를 완전히 소유하고 관리할 수 있도록 하는 ID 관리 시스템이라고 정의하며, 기존의 ID 관리 시스템에서 등록 기관을 대체하는 역할로 블록체인 기능을 식별자 레지스트리(identifier registry)라고 칭한다. SSI 시스템에 필요한 컴포넌트로 identification, verification, authentication, VC(verifiable credentials)와 attribute storage 등을 기본 구성 요소로 제시, 그 작동원리를 통해 SSI의 아키텍처 제시 및 데이터 모델, 시스템의 필수적인 요소들에 대한 분석을 제공하였다. 특히 Self-sovereign identity system을 구현하는 시스템인 uPort, Sovrin 등에서 사용자 ID를 식별할 수 있는 DID에 대한 메소드와 규격 등 본격적인 논의를 하며 다양한 메소드 간 상호운용성을 위한 기술 개발을 언급하였다.

2019년~2020년까지는 SSI의 기술적 구현에 필수적인 아키텍처이자 핵심 기술로 탈중앙 분산원장기술인 블록체인을 연구하면서 블록체인 프로토콜에 대한 평가와 SSI의 기술적 메커

니즘을 프로세스화하고 도식화하여 정립하려는 시도가 나타난다. 이들은 크리스토퍼 앨런이 제시한 SSI의 속성들을 평가의 기준으로 삼아 이에 대한 재조합과 재정립을 하고자 하였다. Toth and Anderson-Priddy(2019)는 실생활에서 사용되는 물리적 ID카드와 같이 직관적으로 사용하기 쉽도록 자기주권 디지털 아이덴티티(SSDI)의 요구사항을 명확히 하고, 사용자의 수용을 촉진할 수 있게 하기 위한 목적으로 기존 SSI에 관한 정의와 속성을 검증하고 IDM과 상호운용성 속성을 추가한 총 14가지의 SSI 속성을 제안하였다. Ferdous et al.(2019)는 SSI에 대한 다른 시각들이 존재하나 방법론적이지도 포괄적이지도 않다고 지적하며, SSI 용어에 대한 다른 관념까지 연구, 수학적인 모델을 사용한 최초의 공식적이고 매우 엄격한 개념정립으로 SSI에 대한 공동의 이해를 제안하였다. uPort, Jolo, Sovrin, Blockerts 시스템을 5개 그룹, 17개 속성으로 나누어 비교한 결과, 현존하는 블록체인기반 SSI 시스템은 17개 속성을 만족하여 사용된 케이스가 없다는 결론을 제시한다.

Schäffner(2019)는 SSI를 확립하는 데 필요한 기본 기술, 프로세스 및 구성 요소를 중점적으로 현존하는 DID 메소드와 관련 시스템을 분석 및 평가하였다. DID method 간 차이를 비교하는 기준으로 시스템 현황, 시스템 설계, 신뢰 아키텍처, 관리 및 수수료 구조를 사용하였고, DID 기술은 최상위 프로토콜이 구축되지 않았을 경우 기본 원장에 크게 의존한다는 것을 발견하였다. 소브린은 하이퍼레저 인디의 개발을 통해 다른 기술보다 더 많은 기능의 제공이 가능하고, 이는 시스템에 대한 신뢰를 강화하고

시스템 개발을 목표로 하기 위해서는 거버넌스 모델이 필요하다는 점을 보여준다(Schäffner, 2019).

SSI 개념이 기술적으로 구현된 블록체인 기반의 DID method들을 실제 원칙의 부합성과 적용을 통해 평가하면서 표준에 관한 이슈와 필요성이 부각되었다. DID의 표준화를 위해 월드와이드웹컨소시엄(W3C)는 분산식별 기술 관련 데이터 모델 및 표현방식에 관한 표준문서를 개발 중이며, decentralized identity foundation(DIF)은 분산 ID생태계를 구축하고자 MS, IBM 등의 IT 회사, 금융사인 Mastercard와 Sovrin, uPort 등이 참여하여 분산ID 관련 기술과 규격을 개발 중이다. 이외에도 International Telecommunication Union Telecommunication Standardization Sector 에서는 분산 원장 상에서도 공개키 기반의 인증서를 이용할 수 있도록 표준을 개발하고 있다.

Kuperberg(2020)는 전통적인 신원관리 시스템과 블록체인 기반의 IAM 솔루션을 비교하며 전문가 인터뷰를 통해 75개의 기준으로 구성된 평가 프레임워크를 개발하고 43개의 요구사항을 제시하여 평가 기준을 수립하였다. 설계자 엔지니어의 관점을 포함한 설문조사 분석과 문헌분석으로 블록체인 기술과 DLT의 IAM 사용성을 평가한 결과, 어떠한 솔루션도 시장 가용성, 기업 준비상태, 비용 및 성숙도의 범주를 모두 만족하는 기술이 없다고 판단, 모든 기술이 초기 단계에 있으며 대부분의 요구사항에 서비스 공급업체가 통합할 수 있는 OAuth 또는 SAML과 같은 표준 호환 인터페이스가 없어 표준에 대한 필요성과 시급성을 지적하였다.

Naik and Jenkins(2020a)은 SSI의 요구사항

과 표준이 매우 빠르게 진화하고 있다고 문제를 제기하며 20가지 SSI 원칙을 제안, 비허가형 ethereum 블록체인인 uPort와 퍼블릭 허가형 하이퍼렛저 인디 기반의 Sovrin을 비교하였다. 두 가지 모두 주권, 데이터 접근 통제, 저장 제어 등 근본적인 요건은 만족하고 있으나 복구, 비용, 개인정보 보호 등에서 지원의 정도는 차이를 보이며 두 시스템 모두 상호운용성과 휴대성 등의 SSI 원칙에서는 개선이 필요한 상황임을 밝혔다. 특히 공통 프로토콜이나 표준기관에 의한 표준정립이 필요하다고 지적하였다.

### 2.3.3 최근 SSI 기술 연구(2021~)

2021년은 아직 진행중이나 DID 시스템의 문제를 제기하고 이를 대비하는 방법이나 실제 산업 현장에서 적용되는 사례를 분석한 연구 트렌드들이 나타났다.

Kim et al.(2021)은 블록체인 기반 DID시스템의 큰 잠재력 대비 전반적인 보안이 철저히 조사되지 않은 것에 대해 문제를 제기하며 DID시스템의 주요 구성 요소를 체계적으로 탐색하고, DID 기술 적용시 발생할 수 있는 취약성을 분석하여 DID 시스템에 발생가능한 공격에 대해 연구하였으며 Mohammed Shuaib et al.(2021)은 healthcare 산업에서 사용자 기록 개인 정보 보호 및 보안은 모든 의료 정보 시스템에서 중요한 요소이므로 의료는 SSI 솔루션이 환자 정보 개인 정보 보호 및 보안 위협에 대응할 수 있는 영역이라고 보고, 블록체인 기반 SSI 솔루션의 헬스케어 적용 가능성, 장점 및 요구사항을 모델 사용 사례를 통해 검토하였다.

Stockburger et al.(2021)는 여러 국가의 여러 운영업체에 걸쳐있는 대중교통 부문에서 자주적 신원 관리가 어떻게 사용될 수 있는지 조사하였다. 블록체인 기반 분산 ID 관리 시스템을 활용하여 대중교통 생태계의 모든 관련 당사자에게 높은 수준의 보안과 투명성을 SSI 프레임워크에서 제공하는 방법을 탐구하여, 기존 대중교통 발권 솔루션과는 달리 유럽의 다양한 운송 네트워크에서 유효한 표준화된 여행자자격증을 어떻게 활용할 수 있는지 보여주고 있다.

또한 Soltani et al.(2021)는 SSI는 사용자 중심적이고 개인정보를 존중하는 디자인 사고를 향한 주요 디딤돌이지만 아직 초기 단계에 있다고 지적하고, SSI 모델이 디지털 신원 및 개인 정보 보호의 모든 문제에 대한 만병통치약 또는 완전한 솔루션이 아니라고 하였다. 새로운 프로토타입, 아이디어가 자주 등장하면서 활기차고 빠르게 확장되고 있는 SSI 생태계의 품질을 강조하여 SSI의 사회적, 기술적 정착에는 다양한 요소가 고려되어야 함을 시사한다.

2016년 크리스토퍼 앨런의 SSI 개념 제시를 기점으로 SSI를 구현하고자 사용된 기술에 대한 문헌을 살펴보았다. SSI의 속성을 규명하고 정의하여 이에 대한 기술적인 해결 도출을 위한 다양한 논의와 시장에 존재하는 시스템의 평가, 해당 시스템의 상호운용성과 표준에 대한 논의, 그리고 다양한 산업분야에의 적용에 있어 리스크와 효과 등에 대한 논의가 거론되고 있다. 향후 기술적 연구는 실제 산업과 생활에 적용에 있어 어떠한 효과가 있었는지를 다루는 연구와 보안 등 리스크에 대한 더 넓은 연구가 필요하며, 신뢰 프레임워크와 같은 통합적인 시각의 기술적 연구 또한 이루어져야 할 것이다.

## 2.4 주요 선행 연구

<표1> 주요 선행 연구

분야	문헌 제목 및 저자	제시된 SSI 개념	연구 주제 (연구 문제)
사회 경제	“Self-Sovereign Identity - Opportunities and Challenges for the Digital Revolution” Der et al.(2017)	사용자 중심의 identity. 사용자 의 개인 데이터 제어에 더욱 초점을 맞추고, ID 관리를 서비스 사용과는 독립적으로 구현해야 함	사람, 서비스, 장치의 상호 연결성을 위해 안전하고 법적으로 규정된 보안 디지털 ID 관리를 실현하기 위해 SSI를 이용하여 개인의 독립적 디지털 ID 유지
	“Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion” Wang and De Filippi (2020)	다양한 도메인과 환경에서 개인의 정체성과 그 구성요소의 다양한 측면을 선택적으로 주장할 권리. 정체성과 구성요소는 특정 정부, 기업 또는 조직을 통한 발행과는 무관해야 하며, 개인은 관리 시스템 내에서 자신의 개인 데이터와 신원 표현에 대한 통제권을 가져야 함.	현실세계의 SSI 관리 시스템을 연구하여 개인이 통제권을 가진 자격증명과 생체 측정방식의 신원지표로 신원 인증의 대체 접근 방식을 설명하고, 사례연구를 통한 자기주권 정체성이 경제적 포용성을 증진할 수 있는가라는 논의
	“Exploring Value Propositions to Drive Self-Sovereign Identity Adoption” Lockwood(2021)	사용자 중심 데이터 생태계에서 SSI는 상호작용의 표준화된 집합으로 참여자와 네트워크 간의 은유적 연결고리. 사용자는 신원, 관계, 자격증명, 데이터제어에 대한 통제가 가능함	SSI 기술 채택이 사용자 중심 데이터 생태계에서 가질 수 있는 가치 탐구
법률	“Self-Sovereign Identity on Public Blockchains and the GDPR” Kondova and Erbguth(2020)	사용자(개인 또는 조직)가 중간자를 가지지 않고서도 제 3자에게 즉시 제공할 수 있는 신뢰할 수 있는 자격증명(실제 ID)	SSI는 데이터 주체의 프라이버시를 기술적으로 보호하고 GDPR을 준수하지만, GDPR을 적용하는 방법 및 컨트롤러로 간주되는 사람 및 정당성이 존재하는지를 결정하려면 사례별 사례분석과 기존의 법적 불확실성에 대한 법적 근거의 필요성 논의
	“Self-Sovereign Identity Systems and European Data Protection Regulations: An Analysis of Roles and Responsibilities” Penedo(2021)	개인을 신분시스템의 중심에 두고 신분과 관련된 모든 행동이 본인에 의해 승인되어야 함. 개인이 국가 또는 제3의 신분제공자의 의존과는 무관하게 신원을 가질 권리가 있다는 믿음에서 기반함	분산형 ID 관리 시스템이 신원 관리에 핵심적인 역할을 수행하게 되면서 기존 규제 프레임워크와 GDPR 과 같은 일반데이터 보호규정이 적용될 수 있는지에 대한 탐색
	“Self-Sovereign Identity: The Harmonising of Digital Identity Solutions Through Distributed Ledger Technology” Lim(2020)	정부나 중앙집중식 조직에 의존하지 않고 개인의 신원소유 및 통제 권리를 인정하는 프레임워크와 이와 관련한 디지털 운동을 모두 칭함	분산된 디지털 신원 프레임워크를 만드는데 분산원장기술이 제공하는 기회를 완전히 실현하기 위한 전제조건으로 SSI를 검토하고, 크리스토퍼 앨런이 고안한 10가지 기본원칙을 통해 법률 준수의 필요성을 분석

기술	<p>“A Survey on Essential Components of a Self-Sovereign Identity”</p> <p>Mühle et al.(2018)</p>	<p>아직 느슨하게 정의된 개념. 본질적으로 SSI는 개인이 자신의 디지털 ID를 완전히 소유하고 관리할 수 있도록 하는 ID 관리 시스템</p>	<p>SSI의 개념과 최신 기술에 대한 개요와 이해를 제공하는 것. 신원확인, 인증, 검증가능한 요청 및 속성 스토리지의 4가지 시스템 기본 구성요소의 검토와 이들 기본 구성요소가 가져야 하는 필수요건을 논의</p>
	<p>“Analysis and Evaluation of Blockchain-based Self-sovereign Identity Systems”</p> <p>Schäffner(2019)</p>	<p>SSI는 사용자에게 그들의 신원과 관련한 완전한 통제권을 제공하여 신원관리의 복잡성을 줄여주며 기능을 향상시켜 온라인 신원을 보다 높은 수준으로 만드는 것</p>	<p>SSI를 확립하는 데 필요한 기본 기술, 프로세스 및 구성 요소를 중점적으로 다루고 상호 작용하는 방식을 설명</p>
	<p>“Self-Sovereign Digital Identity: A Paradigm Shift for Identity”</p> <p>Toth and Anderson-Priddy(2019)</p>	<p>사용자가 자신의 디지털 신원을 통제할 수 있으며, 중앙 당국이 신원에 대해 권한을 갖지 못하는 정체성</p>	<p>Web에서의 신원 관리가 위기에 처해 있으며, 디지털 신원을 실생활에서 사용되는 물리적 ID처럼 직관적이고 사용하기 쉽도록 가상화하여 사용자가 수용하게 하는 방안 탐색</p>
	<p>“A Security Analysis of Blockchain-Based Did Services”</p> <p>Kim et al.(2021)</p>	<p>사용자가 개인정보와 청구권의 최소한의 공개로 신원을 통제하고 관리할 수 있으며, 여러 맥락에 걸쳐 일관된 사용을 할 수 있음</p>	<p>DID 시스템의 다양한 구성 요소 및 타 시스템 구성요소와의 상호작용에 대한 포괄적인 논의를 제공하고, 사용자부터 대상 DID 문서의 실제 획득 및 사용에 이르기까지 경로의 DID 시스템의 취약성을 탐색하여 기본 7가지 보안 공격 도메인을 식별. DID 시스템의 각 보안 공격 벡터에 대해 가능한 대응책과 방어책을 제시</p>

체계적 문헌 연구를 통해 사회/경제, 법률, 기술 분야별로 각 분야의 연구동향을 알아볼 수 있었다. 표 1은 이와 관련한 주요 선행 연구 논문들을 선정, 제안한다. 이들 논문은 SSI와 관련한 주요 개념을 제시하였거나 새로운 아이디어를 제공하여 향후 연구에 도움이 될 수 있는 연구들이라 할 수 있다. 찾아낸 논문들은 피인용횟수 확인을 통해 한번 더 검증하였다. 피인용횟수는 해당 논문이 이후 연구에 얼마나 많이 언급되었는지를 나타내는 객관적인 지표 중 하나이다. 피인용횟수가 높을수록 연구자들이

해당 논문에 대해 많이 검토하고 의견을 받아들였다는 의미도 되므로 연구동향과 같이 논문에 대한 영향력을 살펴볼 때 반드시 고려해야 한다. 그러나 SSI는 비교적 최신의 연구이며 아직은 그 개념에 대해서도 연구가 진행되고 있는 상황이다. 때문에 피인용횟수가 없는 논문이 많은 상황이었으며 피인용횟수가 해당 연구의 가치를 말해주는 것은 아니기에 저자들의 논의를 거쳐 새로운 아이디어가 제시되었거나 실증적 연구를 통해 의미가 있는 연구도 포함하였다.

사회/경제 분야에서는 실사례를 분석하여 SSI가 어떠한 방식으로 적용 가능한지를 보여주는 연구와 사회적 패러다임의 변화로 인한 관점의 변화를 보여주는 논문을 제시하였다. Der et al.(2017)의 논문은 디지털 ID와 ID의 자주적 정체성에 대한 초기 논의들을 제시하여 이후 연구들에 다양한 시사점을 제공하였으며, SSI가 새로운 패러다임으로 자리 잡고 현실에서 사용된 이후 실사례를 분석하여 SSI가 어떠한 방식으로 적용 가능한지에 대해 연구한 논문들에서는 Wang and De Filippi(2020) 논문이 가장 많이 언급되었다. Lockwood(2021)의 논문은 비록 피인용횟수는 없지만 사회적인 패러다임의 변화와 현재 SSI 패러다임이 어떠한 논점과 가치를 중심으로 발전해야 하는지를 제안한 점에서 SSI의 향후 연구에 도움이 될 것이다.

법률 분야에서는 SSI라는 새로운 개념의 등장과 함께 SSI를 법제도에 맞게 분석하고 관계를 조명한 Kondova and Erbguth(2020)의 연구와 GDPR과 같은 현재의 법률체계나 규제 프레임워크를 분석하여 분산형 DID 시스템이 현재의 법률과 어떠한 부분에서 상충되고 문제가 되고 있는지에 대해 논의한 Penedo(2021)논문, 법과 기술의 발전은 상호보완적이어야 함을 논의한 Lim(2020)의 논문을 제안한다.

기술 분야는 기술의 끊임없는 발전에 따라 새로운 기술적 제안들이 현재도 다양하게 연구되고 있으며 SSI와 블록체인 기술을 다룬 논문도 가장 많았다. 그러나 Mühle et al.(2018)의 연구와 같이 SSI에 대해 개요 및 기본이 될 수 있는 기술 시스템의 주요 구성요건을 모아 논의한 논문은 시간이 지날수록 더욱 중요성을

더할 것이다. 마찬가지로 Schöffner(2019)는 SSI와 관련된 방대한 기본 기술과 구성 요소들을 잘 정리해 향후 연구에 많은 도움이 되고 있다. SSI를 이루는 속성들을 다양한 방식으로 검증하고 구현한 다양한 연구 논문들 및 다양한 DID 플랫폼들이 등장하면서 이들 간의 상호운용성을 높이기 위한 기술 표준에 대한 제안과 관련한 연구들이 활발히 이뤄지고 있으며 이 중 Naik and Jenkins(2020a)의 논문을 살펴보았다. 최근 SSI와 DID의 적용에 있어 시스템을 공격할 수 있는 다양한 취약점을 분석하여 보안점이나 해결책을 제시한 Kim et al.(2021)의 논문을 발견하였다.

SSI의 개념은 가능한 연구자들이 논문에서 제시한 개념을 그대로 사용하고자 하였으나 저자가 SSI에 대해 따로 개념을 정의하지 않았거나 명확하게 제시하지 않은 경우, 저자가 논문에서 인용하거나 언급한 SSI의 개념을 명시하였다. SSI의 개념 및 정의와 관련된 논의에 있어서 사회/경제에서 SSI는 개념을 명확히 정의하려 하기보다는 기존에 앨런이 제시한 SSI의 개념을 제시하고 이에 포함된 정체성, 신원 등의 사회적 논의에 대해 분석하고 이들의 사회적 논의가 어떻게 변화하고 있는지에 더욱 관심을 두었다. 법률 분야에서는 개인의 통제권을 통한 개인정보주권의 확보에 더욱 중심이 맞춰진 SSI의 개념이 나타난다. SSI가 가진 통제권은 블록체인 DID 시스템이 가진 기술적 특징 때문에 아직은 법률과 충돌이 생기지만 이 문제가 해결되면 결과적으로는 개인정보를 보호하는데 필수적인 요건이 될 것임을 시사한다. 기술분야에서는 SSI가 가진 원칙을 기준으로 SSI를 DID의 기술적 구성요소와 속성에 비추

어 정의하고자 하였다. SSI는 실제 신원을 통제 하는데 사용될 DID 기술의 개념적 바탕이 되기에 관리 속성에 조금 더 중점이 되어 필요한 개념들이 포함된다.

세 분야에서 SSI의 개념에 대해 공통적으로 논의하고 있는 점은 탈중앙화된 신원이다. 모든 분야의 SSI의 개념에서 신원의 생성과 관리에 있어 중앙집중화 방식으로 관리되던 기존의 시스템이나 제 3자의 개입 또는 의존에서 벗어난 개인이나 정보 주체를 언급하고 있다.

### III. 연구방법

#### 3.1 연구 방법

메타연구는 이전에 진행된 연구 성과를 역사적으로 검토함으로써 기존의 연구 경향에 대한 규칙성을 밝혀내는 연구 방법이다(성욱제, 2012). 체계적 문헌 고찰(systematic reviews)은 지금까지 학술연구 문헌으로 발표된 논문을 대상으로 합리적 판단에 근거하거나 객관적 기준에 따라 분석하여, 해당 주제의 변화 흐름, 특성을 파악하는 것으로(이중정 등, 2020) 이와 같은 분석을 통해 하나의 연구 결과로부터는 얻기 힘든 큰 수의 연구대상에 대한 연구나 다년간에 걸친 연구 결과를 종합적으로 제시할 수 있다. 같은 문제를 연구한 기존의 연구 출판물들을 탐색하고 이들의 결과를 비판적으로 평가하고 분석하여 다양한 결과들을 안정된 결론으로 제시할 수 있고, 요약된 결과를 일반화시킬 수 있는 근거를 마련, 다양한 종류의 연구에 광범위하게 적용될 수 있다는 것은 메타분석의

장점 중 하나이다(신태범, 권상희, 2013). 또한 특정 분야에 대한 동향을 탐색하거나 특정 주제에 대한 다양한 연구 문헌들을 탐색하여 세부 연구 문제의 차이, 해결 방안 주장의 차이들을 비교 검토하여(Siqueira, Rocha, 2021) 모호한 주제를 더욱 명확히 드러내는데 도움을 줄 수 있다.

#### 3.2 연구 설계

연구 주제와 관련된 키워드로 “Self-Sovereign Identity”를 이용하여 구글 학술검색(google scholar)에서 검색되는 논문 제목을 기준으로 1차 검색을 진행하였다. 또한, government, economy, law, GDPR, DID 와 같이 사회경제, 법률, 기술 카테고리와 연관된 키워드를 검색에 함께 이용하여 각 분야별로 SSI 관련 연구를 추가로 수집하고 피인용횟수가 높은 논문과 해당 논문에 포함된 참고문헌 리스트를 비교 검토하였다. 이와 더불어 SSI를 대중적으로 처음 제시한 Allen(2016)의 연구와 SSI로 검색되지 않지만 디지털 아이덴티티와 블록체인 분산ID 기술을 다룬 논문들을 연구대상에 포함시켰다. 2016년부터 2021년 7월까지 학술 논문, 학위논문, 컨퍼런스에서 정식으로 출판된 연구 논문을 우선 검토 대상으로 선정하였으나 사회경제, 법률분야에서는 최근의 사례 연구의 검토도 필요하다고 판단하여 연구기관 보고서와 법령정보 및 웹페이지도 일부 대상에 포함되었다. 수집된 연구 대상은 논문 및 보고서, 웹페이지로 논문은 초록을 우선 검토하여 분야별로 구분하여 최종적으로 112개의 대상 중 41개의 선행 연구가 사용되었다. 2.4의 표는 각 영역

별로 SSI에 대한 체계적 문헌 연구를 통해 발견한 연구 방향과 관련하여 초기 아이디어를 제공했거나 주요 개념을 제시한 문헌을 소개하고자 하였다.

## IV. 결론

### 4.1 연구 결과

본 연구는 최근 중요한 신원 인증 모델로 논의되고 있는 SSI에 대한 선행연구를 다각적 관점에서 접근하여 각 분야의 특징을 반영한 SSI의 개념과 정의를 제시하는 동시에 통합적 관점에서 포괄적으로 적용 가능한 SSI의 학술적 개념을 제시하는 것에 주된 목적이 있다. 이를 위하여 앞 절에서 제시한 바와 같이, 사회/경제, 법률, 기술적 관점으로 접근한 SSI 관련 선행연구를 종합적으로 검토하여 각 분야별 SSI의 개념과 특징에 대하여 제시하였으며 주요 결과는 다음과 같다.

첫째, SSI는 특정 기업이나 기관의 개입 없이 디지털 신원(digital identity)을 이용하여 스스로 신원을 관리한다는 점에서 현존하는 중앙 집중화된 형태의 신원 관리 체계와는 분명한 차이가 존재한다. 이와 같이 기존 신원 관리 체계와는 상이한 SSI의 특징을 새로운 신원 관리의 패러다임으로 사회에서 수용함에 따라, SSI 구현에 따른 사회적 파급효과를 분석하거나 향후 미칠 영향에 대한 잠재적 효과를 살펴본 사회적 관점에서 접근한 연구가 다수 존재한다.

새로운 사회적 규범(social norms) 혹은 신기술의 등장은 특정 집단 내에 널리 조성된 문화

와 환경적 특징에 따라, 사회와 조직에 영향을 미치고 이를 수용하는 개인의 태도에 다양한 영향력을 행사함이 다수의 선행연구를 통하여 검증되어왔다. 대표적으로, 개인이 속한 사회에 형성된 문화적 특징에 따라 개인의 PC 활용의도에는 차이가 존재하였으며 (Srite and Karahanna, 2006), 특정 기술에 대하여 조성된 사용자의 인식에 따른 사회적 규범은 새로운 어플리케이션에 대한 사용자의 수용 태도와 사용 행동에 영향을 주는 것으로 밝혀졌다 (Beldad and Hegner, 2018). 이와 유사한 맥락에서 SSI의 등장은 사용자의 개인정보에 대한 인식을 비롯하여 개인정보를 활용한 인증 체계 및 인증이 주로 이루어지는 온라인 환경의 태도에까지 영향을 준다. 따라서, 인터넷 등 온라인 환경에 대한 개인의 의존성이 높아짐에도 불구하고 정보 주체의 개인정보 통제가 어려운 현실점에서 SSI는 오늘날 사회에 필수불가결한 개념에 되었다. SSI는 이전과 다르게 제3자 및 기업/기관의 개입 없이 신뢰를 바탕으로 이루어지는 새로운 신원 관리 체계라는 점에서 사회적 영향력을 수반함에 따라, SSI의 잠재적 사회 효과에 대한 다양한 연구가 진행될 필요가 있다. 나아가 SSI는 기존의 중앙 집중화 시스템에서 신원을 관리하고 해당 시스템을 유지하기 위하여 수반되던 상당한 경제적 비용을 감축시킬 수 있는 것으로 예측됨에 따라 (Kubach et al., 2020), 사회/경제적 비용의 변화에 따른 경제 효과에 대한 지속적인 연구가 필요하다. 그러나 이러한 경제적 비용 감축에도 불구하고 과거와는 다른 새로운 신원 인증 체계임에 따라, 사용자들에게 새로운 체계에 대한 적응과 신뢰 확보를 위한 사회적 비용이 추가적으로

수반될 것으로 예상된다. 따라서, SSI의 등장에 따라 기존의 신원 인증 관리 생태계의 사회적 안전성을 무너뜨리지 않으면서 감축된 사회, 경제적 비용 등의 변화에 따른 예상 및 파급효과와 관련된 연구의 필요성이 존재한다. 이에 현재 사회적 관점에서의 SSI 연구 동향을 종합하였을 때, SSI의 정의는 “중앙 집중화 방식으로 관리되던 기존의 신원 관리 체계와는 다르게 개인정보에 대한 관리 권한을 정보 주체가 가질 수 있도록 하는 신뢰 기반의 신원 인증 체계”로 도출할 수 있다.

둘째, 전세계적으로 최근, 데이터 경제 패러다임 등장과 유럽의 GDPR 시행에 따른 개인정보에 대한 통제권, 자율성 등의 보장 필요성이 증가하는 시대적 환경에 발맞추어 법률적 관점에서의 SSI 개념이 주목받기 시작하였다. 이에 정보 주체의 자기 주권 실현을 목적으로 한다는 SSI의 특징에 착안하여 국내를 비롯하여 해외의 개인정보 및 데이터 관련 법률과의 관계를 조명한 연구가 다수 존재한다. 특히, SSI의 의미를 개인정보 주권 개념을 바탕으로 개인의 완벽한 데이터 소유권 및 데이터 통제권의 확보로 규명하였다. 또한, 국내 개인정보보호법, 유럽 GDPR 등의 현행법을 바탕으로 SSI 구현 서비스 및 SSI 기반 비즈니스 모델의 상용화에 따라 발생 가능한 법적 쟁점을 평가하였다. 구체적으로, 블록체인에 저장된 개인정보 데이터의 경우 블록체인의 기술적 특징으로 삭제 및 파기가 어려움에 따라, 이로 인하여 향후, DID 구현에 따라 위반의 소지가 있는 법적 상충 쟁점을 도출하였다. 이러한 법률적 관계 정립 및 법적 상충 소지의 쟁점을 발굴함에 따라, 다수의 선행 연구들은 SSI의 본래 취지 달성을 위해

서는 SSI 구현을 위한 단편화된 기술 개발 뿐만 아니라 해당 기술의 확산을 뒷받침하기 위한 법과 제도의 마련 중요성을 공통적으로 시사하였다. 이에 앞선 선행연구를 종합하였을 때, 법률적 관점에서의 SSI는 “제3자의 개입 없이 정보 주체가 개인정보를 통제할 수 있도록 하여 개인정보의 주권 확보 즉, 개인정보자기결정권을 보장하게 하는 개인정보 관리 방식”으로 정의할 수 있다.

셋째, 기술 분야의 SSI 연구들은 주로 디지털 신원 관리(identity management)를 시작으로 SSI를 기술적으로 구현 가능하기 위한 DID method에 대한 연구가 주를 이루고 있다. 기존의 중앙 집중화된 시스템에서 관리하던 신원 관리 체계와는 다르게 분산화된 시스템에서 구현되는 DID 기술을 이용하여 신원정보의 인증이 가능하다는 점에서 다수의 선행연구들이 DID 기반의 SSI 구현의 프로세스를 설계 및 검증하였다. 구체적으로, DID 등장의 초기에는 DID 구성요소와 DID의 구조(infrastructure)를 중심으로 SSI의 구현 시나리오에 대한 제안 연구가 활발히 진행되었다. 이후에는 DID method에 따른 개인정보보호 지원 수준 등에 대한 평가 관련 연구도 다수 수행되었다. 최근에는 다양한 DID 플랫폼이 상용화됨에 따라, 플랫폼 사이의 상호운용성을 높이기 위한 목적으로 관련 국제 표준 정립의 필요성을 제기하며 다양한 기존 표준의 분석과 신규 표준에 대한 제안의 연구가 활발히 이루어지는 추세이다. 기술적 관점에서 살펴본 SSI 대부분의 선행연구들은 현재, 아직 초기 산업 시장의 특징에 따라 SSI를 구현하기 위한 기술 검증 시나리오 설계 및 관련 서비스의 보안성을 증진시키기 위

한 기술 구성 요소 개선의 연구로 요약될 수 있다. SSI 개념의 확산과 관련 서비스가 증가할 것으로 예상됨에 따라, 향후에는 이를 구현 가능하도록 하는 DID 기술의 무결성과 지체 없이 실시간으로 방대한 양의 신원 정보를 처리할 수 있는 블록체인 원천 기술의 마련을 위한 연구가 수행될 필요가 있다. 이와 같이 기술 분야의 SSI 선행연구를 살펴본 결과, 본 연구는 기술 분야에서의 SSI를 “중앙 집중 시스템에 의존하지 않고 필요에 따른 최소한의 정보를 노출하여 본인 인증을 가능하게 하는 사용자 중심의 신원 인증 모델”로 정의한다.

앞서 제시한 바와 같이, 본 연구는 사회/경제, 법률, 기술의 관점에서 각각 통용되는 SSI의 주된 개념과 정의를 도출하였다. 이를 종합하여 본 연구는 특정 산업 분야를 넘어 포괄적 관점에서 적용 가능한 SSI의 학술적 정의를 “중앙 집중 시스템 혹은 제3자의 개입 없이 개인정보 주체의 자율적 통제에 따라 스스로 신원 인증이 가능한 신뢰 기반의 신원 관리 체계”로 제시한다.

#### 4.2 연구 논의

본 연구는 산업 분야별 특징이 반영된 SSI의 개념을 비롯하여 포괄적 관점에서의 SSI의 학술적 정의를 제시함에 따라, 최종적으로 다음과 같은 연구의 시사점에 따라 논의하고자 한다.

첫째, 본 연구는 현재 혼용되어 사용되고 있는 SSI 개념에 대하여 주요 산업 분야의 특징이 반영된 각각의 개념과 학술적으로 통용 가능한 SSI의 정의를 제시함에 따라, SSI 분야의 산업 활성화 촉진과 관련 학술 연구 범위의 확장에

기여한다. SSI 기반의 비즈니스 모델과 서비스는 최근 이를 구현 가능하도록 하는 DID 기술의 등장과 함께 확산되기 시작하였다. 그럼에도 불구하고 SSI의 본래 의미를 해석하여 수용하는 과정에서 SSI의 개념에 대한 각 산업별 차이가 존재하였다. 이는 각 산업별 중점을 두는 SSI의 주요 속성의 차이에서 기인하였다. 이에 본 연구에서 주요 산업에서 적용된 SSI의 의미를 도출하였다. 나아가 SSI의 산업별 정의 및 기대역할을 제시함에 따라, 본 연구는 SSI 기반 서비스의 개발 및 도입을 계획하고 있는 기업 및 공공 분야에 각 산업별 SSI의 역할과 개념에 대한 이해를 도모하는 동시에 SSI 기반의 다양한 비즈니스 모델을 발굴하기 위한 토대를 제공하였다. 이와 더불어 본 연구는 SSI의 학술적 정의를 제시함에 따라, 이를 바탕으로 SSI 관련 다양한 연구의 기반을 조성하여 SSI 연구 분야의 확장에 기여할 것으로 예상된다.

둘째, 본 연구의 결과는 사회적으로 SSI 개념이 정착되고 SSI 기반 비즈니스 모델의 확산을 위해서는 사회/경제, 법률, 기술 분야의 분리된 발전이 아니라 세 분야 모두의 상호작용을 기반으로 움직여야 함을 시사한다. 사회-기술적 시스템(socio-technical system, STS) 이론에 따르면, 최적화된 산출물을 생성하기 위해서는 기술, 사회, 조직적 다각도의 접근과 상호작용 필요성을 주장한다(Bostrom and Heinen, 1977; Chai and Kim, 2012). 이는 본 연구에서 살펴본 바와 같이, SSI가 구현하고자 하는 본래 취지를 구현하기 위해서는 기술, 법/제도 및 사용자의 인식을 포함한 사회적 환경 등이 각각 독립되어 역할을 수행하는 것이 아니라 다양한 분야 및 관점에서 융합적으로 기반이 조성되어야 한

다. 구체적으로, DID를 통하여 선택적으로 정보 주체가 개인정보를 제공하여 신원을 증명 가능한 동시에 보안성을 담보하기 위한 기술의 개발이 지속적으로 이루어지는 동시에 해당 기술이 국내에서 정착 및 확산되기 위해서 현존하는 국내의 개인정보보호, 정보통신망법 등의 관계 법령과 상충 이슈가 없는지에 대한 검토를 통한 제도적 방안 마련이 필요하다. 이는 기술의 등장과 발전에 따라 해당 기술의 상용화가 현존하는 법률에 위배소지가 있는지에 대한 선제적 검토와 관련 기술의 사회적 과급 효과 등을 고려하였을 때, SSI와 같은 새로운 사회적 규범이 기술과 제도의 뒷받침을 통하여 성공적으로 정착할 수 있다.

앞서 서론에서 제시하였던 국내 인공지능(AI) 대화 서비스인 ‘이루다’의 사례와 같이, 이루다는 대용량의 자연어처리능력(NLP)을 비롯하여 투입된 데이터를 바탕으로 스스로 학습하여 새로운 데이터를 산출 및 예측할 수 있는 딥러닝 알고리즘 등 높은 수준의 기술 역량을 갖추었음에도 불구하고 사회 및 제도적 관점에서 충분한 상호 작용이 발생하지 못하여 서비스의 중단을 초래한 것으로 볼 수 있다. ‘이루다’ 서비스의 잠정 중단 원인을 STS 관점에서 살펴보면, 대표적으로 AI 챗봇에 대한 국내 사용자의 익숙하지 않은 인식에서 발생하는 사회적 거부감과 개인정보보호법 및 사용자의 프라이버시 침해의 위협에 대한 법률적 관점에서의 충분한 고려가 이루어지지 않은 채, 기술만이 단편적으로 개발되었기 때문이다. 즉, 사회-기술-제도가 융합적으로 상호작용하지 못하였다는 것이다. 이러한 ‘이루다’의 사례와 같이, 법, 제도를 비롯하여 사회 및 조직의 견해와 인식의 차이는

해당 기술의 정착과 확산의 극복 대상이다 (Porter and Donthu, 2006). 이에 SSI도 개인정보와 같이 주요한 정보를 처리한다는 점에서 특히, 법/제도와의 상호작용 및 이전에는 존재하지 않은 신규 기술 기반의 신원 인증 관리 체계라는 점에서 사용자의 인식 고려와 기존의 신원 인증 관리 생태계의 안전성을 유지하며 사회적 건전성을 훼손하지 않을 수 있도록 사회/조직-기술-법률의 발맞춘 상호작용 기반의 발전과 추진이 이루어져야 한다.

본 연구는 SSI에 대하여 다루어진 주요 학술지 논문, 컨퍼런스 논문, 연구기관 발행 보고서를 연구 분석 대상으로 살펴보았다. 이는 SSI에 대한 모든 문헌을 검토할 수 없는 현실적 제약 사항을 반영하여 공신력 있는 학술지 및 컨퍼런스를 통하여 전문 연구진의 심사에 따라 발간된 연구 논문을 비롯하여 국내외 연구기관에서 발행된 보고서를 대상으로 하였다. 따라서 향후 연구에서는 보다 많은 선행연구의 수집을 비롯하여 SSI를 구현하는 주요 DID의 기술 분석 백서(whitepaper) 및 국가별 관련 보고서를 포함하여 범위를 넓히며 추가 연구를 수행할 필요가 있다. 본 연구는 최근 활발히 연구가 진행되기 시작한 SSI를 다룸에 따라, SSI 분야의 검증된 선행연구를 충분히 수집하는 데 한계가 존재하였다. 또한, SSI 관련 연구 대부분이 통계적 방법론을 적용한 실증 연구가 아닌, SSI의 의미를 탐색하거나 SSI를 구현하기 위한 기술적 아키텍처 및 플랫폼을 분석한 연구가 주를 이룸이 확인되었다. 따라서, 현재 SSI 관련 충분한 양의 문헌 수집이 어려운 점과 더불어 대부분 SSI의 의미와 기술 분석과 관련하여 수행된 SSI의 선행 연구 동향 및 특징을 반영하여

본 연구는 체계적 문헌 고찰의 방식을 채택하였다. 이와 같은 연구 분석의 방법을 수행함에 따라, 본 연구는 다양한 선행 연구를 면밀히 검토하여 SSI의 의미를 체계적으로 종합 및 분석하여 결과를 도출하였다. 이러한 연구 방법은 현재 학술 및 산업적 관점에서 다양한 SSI의 의미와 역할에 대하여 제시하여 도출된 연구 결과를 기반으로 시사점을 제공하고자 하는 본 연구의 주된 목적에 부합하다고 판단되었다. 즉, 본 연구는 SSI 관련 연구를 실증적으로 분석하기 위하여 요구되는 충분한 양의 문헌 수집의 한계로 인하여 정성적 관점에서 문헌을 분석하여 결과를 도출하였으나, 향후에는 SSI 관련 충분한 선행연구의 누적을 통하여 SSI의 의미와 역할에 대한 실증 연구를 수행하여 관련 연구 분야의 확장에 기여할 예정이다.

## 참고문헌

고영미, “탈중앙화 자기주권신원인증 (DID) 에 대한 법적 고찰.”, 법학논총, 제45권, 1호, 2021, pp. 421-447.

권현영, “데이터 주권 시대의 블록체인 기술 활용 가능성과 개발 현황.”, 주간기술동향, 2020.07.22., pp. 17-27.

김중기, 김지윤, “모바일 기기 사용자는 왜 정보 보호에 위험한 행동을 하는가?: 위협행동 결정요인 모델을 중심으로.”, 정보시스템연구, 제28권, 제2호 2019, pp. 129-152.

박민정, 유지은, 채상미, “Isms-P 와 Gdpr 의 개인정보보호 부문 연계 분석.”, 한국IT서

비스학회지, 제18권, 제2호, 2019, pp. 55-73.

박민정, 채상미, 이명준, “개인정보보호법제 관점에서 본 블록체인의 법적 쟁점: GDPR 및 국내 개인정보보호법을 바탕으로.”, Journal of Information Technology Applications & Management 제25권, 제2호, 2018, pp. 133-146.

박진아, “데이터의 보호 및 유통 법제 정립 방안.”, 서강법률논총, 제9권, 제2호, 2020, pp. 3-41.

성욱제, “국내 미디어 다양성 연구에 대한 메타 분석: 미디어 다양성에 대한 개념 및 접근방식을 중심으로.”, 방송통신연구, 2012, pp. 101-139.

송영현, “블록체인 기술의 사회에서의 보편적 활용을 위한 규범성 고찰.”, IT 와 법 연구, 제22권, 2021, pp. 341-70.

신태범, 권상희, “국내 온라인저널리즘 연구에 대한 메타분석: 분석 대상과 주제, 이론 및 방법론적 특성을 중심으로.”, 커뮤니케이션 이론, 제9권, 제2호, 2013, pp. 200-249.

여기호, 박근덕, 염홍열, “분산 Id 보관 및 연계 서비스 모델 제안.”, 정보보호학회논문지, 제 30권, 제3호, 2020, pp. 513-25.

오현택, 양진홍, “마이데이터 환경에서 개인의 전자 건강/의료 데이터 활용을 위한 데이터 거래모델.”, 한국정보전자통신기술학회 논문지, 제13권, 제3호, 2020, pp. 250-261.

이정현, 김지원, 김철수, 양진홍. “자기주권신원

- 기술의 국내 서비스 사례 및 연구 과제 분석을 통한 개인정보 주권 강화 방안 연구.” 한국정보전자통신기술학회 논문지, 제13권, 제6호, 2020, pp. 575-589.
- 이중정, 안재영, 김행미, 김우석, “Ict 기반 공유 경제 발전을 위한 학문적 노력에 대한 고찰: 국내외 Mis와 유관 분야의 학술 연구를 대상으로 메타분석.”, 지식경영 연구, 제21권, 제4호, 2020, pp. 129-56.
- 전양, 박민정, 채상미, “중·노년층의 온라인 개인정보보호 행동에 영향을 미치는 요인에 관한 연구, 한국과 중국 인터넷 사용자를 중심으로.”, 정보시스템연구, 제29권, 제1호, 2020, pp. 51-74.
- 한국인터넷진흥원. 미국 개인정보보호 법 행정 체계 현황 및 주요 위반사례(‘21.1월 기준). 한국인터넷진흥원 개인정보보호위원회 and 개인정보보호국제협력센터, 2021.02.25.
- GDPR대응지원센터. 2020 EU 일반개인정보보호법(GDPR) 가이드북. 한국인터넷진흥원 (2020).
- “개인정보 침해 신고·상담 건수.”, e-나라지표, Updated 2021.07.16.
- “데이터 3법.”, 정책위키, 대한민국 정책 브리핑, Updated 2021.07.20.
- Ahmed, Khaled A. M., Sabry F. Saraya, John F. Wanis, Amr M. T. Ali-Eldin, “A Self-Sovereign Identity Architecture Based on Blockchain and the Utilization of Customer’s Banking Cards : The Case of Bank Scam Calls Prevention.”, 2020 15th International Conference on Computer Engineering and Systems (ICCES), 2020.
- Baars, DS, “Towards Self-Sovereign Identity Using Blockchain Technology.”, Master’s thesis, University of Twente, 2016.
- Beldad, Ardion D, Sabrina M Hegner, “Expanding the Technology Acceptance Model with the Inclusion of Trust, Social Influence, and Health Valuation to Determine the Predictors of German Users’ Willingness to Continue Using a Fitness App: A Structural Equation Modeling Approach.”, *International Journal of Human - Computer Interaction*, Vol. 34, No. 9, 2018, pp. 882-93.
- Benoit, D. F., Lessmann, S., Verbeke, W. “On realising the utopian potential of big data analytics for maximising return on marketing investments.” *Journal of Marketing Management*, Vol. 36, No.3-4, 2020, pp. 233-247.
- Bostrom, Robert P, J Stephen Heinen, “Mis Problems and Failures: A Socio-Technical Perspective. Part I: The Causes.”, *MIS quarterly*, 1977, pp. 17-32.
- Cameron, Kim, “The Laws of Identity.”, Microsoft Corp, 12, 2005, pp. 8-11.
- Chai, Sangmi, Minkyun Kim, “A Socio-Technical Approach to Knowledge

- Contribution Behavior: An Empirical Investigation of Social Networking Sites Users.”, *International Journal of Information Management*, Vol. 32, No. 2, 2012, pp. 118-26.
- Der, Uwe, Stefan Jähnichen, Jan Sürmeli, “Self-Sovereign Identity - Opportunities and Challenges for the Digital Revolution.”, *arXiv preprint arXiv: 1712.01767*, 2017.
- Dunphy, Paul, Fabien AP Petitcolas, “A First Look at Identity Management Schemes on the Blockchain.”, *IEEE security & privacy*, Vol. 16, No. 4, 2018, pp. 20-29.
- Ferdous, Md Sadek, Farida Chowdhury, Madini O. Alassafi, “In Search of Self-Sovereign Identity Leveraging Blockchain Technology.”, *IEEE Access*, Vol. 7, 2019, pp. 103059-79.
- Freytsis, Maria, Iain Barclay, Swapna Krishnakumar Radha, Adam Czajka, Geoffrey H. Siwo, Ian Taylor, Sherri Bucher, “Development of a Mobile, Self-Sovereign Identity Approach for Facility Birth Registration in Kenya.”, *Frontiers in Blockchain*, Vol. 4, 2021.
- Gans, Rachel Benchaya, Jolien Ubacht, Marijn Janssen, “Self-Sovereign Identities for Fighting the Impact of Covid-19 Pandemic.”, *Digital Government: Research and Practice*, Vol. 2, No. 2, 2021, pp. 1-4.
- Grech, Alex, Ira Sood, Lluís Ariño, “Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education.”, *Frontiers in Blockchain*, Vol. 4, 2021.
- Gstrein, Oskar J., Dimitry Kochenov, “Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?”, *Frontiers in Blockchain*, Vol. 3, 2020.
- Hardjono, Thomas, “Federated Authorization over Access to Personal Data for Decentralized Identity Management.”, *IEEE Communications Standards Magazine*, Vol. 3, No. 4, 2019, pp. 32-38.
- Houtan, Bahar, Abdelhakim Senhaji Hafid, Dimitrios Makrakis, “A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare.”, *IEEE Access*, Vol. 8, 2020, pp. 90478-94.
- Kim, Bong Gon, Young-Seob Cho, Seok-Hyun Kim, Hyoungshick Kim, Simon S. Woo, “A Security Analysis of Blockchain-Based Did Services.”, *IEEE Access*, Vol. 9, 2021, pp. 22894-913.
- Kim, Geun-Hyung, “A Design of Self-Sovereign Data Distribution Platform for a Reliable Data Economy.”, *Journal of Digital Contents Society*, Vol. 22, No. 3, 2021, pp. 483-90.
- Kondova, Galia, Jörn Erbguth, “Self-Sovereign

- Identity on Public Blockchains and the GDPR.”, *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 2020.
- Kubach, Michael, Christian H Schunck, Rachele Sellung, Heiko Roßnagel, “Self-Sovereign and Decentralized Identity as the Future of Identity Management?”, *Open Identity Summit 2020*, 2020.
- Kuperberg, Michael, “Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective.”, *IEEE Transactions on Engineering Management*, Vol. 67, No. 4, 2020, pp. 1008-27.
- Lim, Jonathan, “Self-Sovereign Identity: The Harmonising of Digital Identity Solutions through Distributed Ledger Technology.”, *ANU Journal of Law and Technology*, Vol. 1, No. 2, 2020, pp. 98-120.
- Lockwood, Mick, “Exploring Value Propositions to Drive Self-Sovereign Identity Adoption.”, *Frontiers in Blockchain*, Vol. 4, 2021.
- Mühle, Alexander, Andreas Grüner, Tatiana Gayvoronskaya, Christoph Meinel, “A Survey on Essential Components of a Self-Sovereign Identity.”, *Computer Science Review*, Vol. 30, 2018, pp. 80-86.
- Naik, Nitin, Paul Jenkins, “Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems.”, *2020 IEEE International Symposium on Systems Engineering (ISSE)*, 2020a, pp. 1-6.
- Naik, Nitin, Paul Jenkins. “Your Identity Is Yours: Take Back Control of Your Identity Using Gdpr Compatible Self-Sovereign Identity.”, *2020 7th International Conference on Behavioural and Social Computing (BESC)*, 2020b.
- Penedo, Andrés Chomczyk. “Self-Sovereign Identity Systems and European Data Protection Regulations: An Analysis of Roles and Responsibilities.”, *Gi-Edition.*, 2021.
- Porter, Constance Elise, Naveen Donthu, “Using the Technology Acceptance Model to Explain How Attitudes Determine Internet Usage: The Role of Perceived Access Barriers and Demographics.”, *Journal of business research*, Vol. 59, No. 9 , 2006, pp. 999-1007.
- Schäffner, Martin, “Analysis and Evaluation of Blockchain-Based Self-Sovereign Identity Systems.”, Master’s thesis, 2019.
- Shuaib, M., S. Alam, M. Shahnawaz Nasir, M. Shabbir Alam, “Immunity Credentials Using Self-Sovereign Identity for

- Combating Covid-19 Pandemic.”, *Materials Today: Proceedings*, 2021.
- Shuaib, Mohammed, Shadab Alam, Mohammad Shabbir Alam, Mohammad Shahnawaz Nasir, “Self-Sovereign Identity for Healthcare Using Blockchain.”, *Materials Today: Proceedings*, 2021.
- Siqueira, Alexandre, Arlindo Flavio Da Conceição, Vladimir Rocha, “Blockchains and Self-Sovereign Identities Applied to Healthcare Solutions: A Systematic Review.”, *arXiv preprint arXiv:2104.12298*, 2021.
- Soltani, Reza, Uyen Trang Nguyen, Aijun An, “A Survey of Self-Sovereign Identity Ecosystem.”, *Security and Communication Networks* 2021, 2021.
- Srite, Mark, Elena Karahanna, “The Role of Espoused National Cultural Values in Technology Acceptance.”, *MIS quarterly*, 2006, pp. 679-704.
- Stockburger, Lukas, et al. “Blockchain-Enabled Decentralized Identify Management: The Case of Self-Sovereign Identity in Public Transportation.”, *Blockchain: Research and Applications*, 2021, 100014.
- Toth, Kalman C., Alan Anderson-Priddy, “Self-Sovereign Digital Identity: A Paradigm Shift for Identity.”, *IEEE Security & Privacy*, Vol. 17, No. 3, 2019, pp. 17-27.
- Wang, Fennie, Primavera De Filippi, “Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion.”, *Frontiers in Blockchain*, Vol. 2, 2020.
- Wittek, Kevin Lazzati Laura Bothe David Sinnaeve Ann-Julie Pohlmann Norbert, “An Ssi Based System for Incentivized and Selfdetermined Customer-to-Business Data Sharing in a Local Economy Context.”, *2020 IEEE European Technology and Engineering Management Summit (E-TEMS)*, 2020, pp. 1-5.
- Zwitter, Andrej J., Oskar J. Gstrein, Evan Yap, “Digital Identity and the Blockchain: Universal Identity Management and the Concept of the “Self-Sovereign” Individual.”, *Frontiers in Blockchain*, Vol. 3, 2020.
- Tobin, Andrew, Drummond Reed, “The Inevitable Rise of Self-Sovereign Identity.”, The Sovrin Foundation 29, 2016.
- World Bank Group, Id4d Annual Report. 2018.
- Allen, Christopher, “The Path to Self-Sovereign Identity.”, Life With Alacrity, 2016.04. 25., 2016. <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.
- Martin, Aaron, Linnet Taylor, “Biometric Ultimata – What the Yemen Conflict Can Tell Us About the Politics of

Digital Id Systems.”, 2019.06.21. Accessed 2021.08.18. <https://globaldatajustice.org/2019-06-21-biometrics-WFP/>.

문가용. “개인정보 유출 숨긴 우버에 1억 4천 8백만 달러 벌금”, 보안뉴스, 2018.09.27. <https://m.boanews.com/html/detail.html?idx=73267>

문진욱, “미국, 잇따른 개인정보 유출사건으로 보안결재 관심 급증.”, 2014. <https://news.kotra.or.kr/user/globalAllBbs/kotraneews/list/2/globalBbsDataAllView.do?dataIdx=136362&column=&search=&searchAreaCd=&searchNationCd=&searchTradeCd=&searchStartDate=&searchEndDate=&searchCategoryIdx=&searchIndustryCateIdx=&page=107&row=100>

Republic of Estonia E-residency, Accessed 2021.08.18. <https://e-resident.gov.ee/become-an-e-resident/>.

우고운, “페이스북 5조9000억원 벌금 낸다...전체 매출의 9%” 조선일보, 2019.07.25. [https://www.chosun.com/site/data/html\\_dir/2019/07/25/2019072500828.html](https://www.chosun.com/site/data/html_dir/2019/07/25/2019072500828.html)

원병철, “지금까지 약 3,628억 벌금 부과한 EU GDPR... 우리나라 기업은 어땠나” 보안뉴스, 2021.04.25. <https://www.boanews.com/media/view.asp?idx=96852&kind=>

천민아, “보이스피싱, 요즘 누가 속냐고?...서울만 매일 6억원 피해.”, 뉴스시스, 2021.03.21. [https://newsis.com/view/?id=NISX20210319\\_0001377085&cID=10201&pID=10200](https://newsis.com/view/?id=NISX20210319_0001377085&cID=10201&pID=10200).

Appendix. 선행 연구 정보

\* 출간연도별 제시

\* Google Scholar에 검색된 논문에만 인용횟수 표기

No.	출간 년도	인용 횟수	저자	논문명	저널
1	2005	397	Cameron, Kim.	The Laws of Identity	Microsoft Corp
2	2016	-	Allen, Christopher,	The Path to Self-Sovereign Identity	Life With Alacrity
3	2016	91	Baars, DS.	Towards Self-Sovereign Identity Using Blockchain Technology	University of Twente
4	2016	118	Tobin, Andrew, Drummond Reed.	The Inevitable Rise of Self-Sovereign Identity	The Sovrin Foundation
5	2017	33	Der, Uwe, Stefan Jähnichen, Jan Sürmeli.	Self-Sovereign Identity - Opportunities and Challenges for the Digital Revolution	arXiv preprint arXiv:1712.01767
6	2017	244	Dunphy, Paul, Fabien AP Petitcolas.	A First Look at Identity Management Schemes on the Blockchain	IEEE Security & Privacy

No.	출간 년도	인용 횟수	저자	논문명	저널
7	2018	125	Mühle, Alexander, Andreas Grüner, Tatiana Gayvoronskaya, Christoph Meinel.	A Survey on Essential Components of a Self-Sovereign Identity	Computer Science Review
8	2018	0	박상철	데이터 소유권 개념을 통한 정보보호 법제의 재구성	법경제학연구
9	2019	53	Ferdous, Md Sadek, Farida Chowdhury, Madini O. Alassafi.	In Search of Self-Sovereign Identity Leveraging Blockchain Technology	IEEE Access
10	2019	2	Martin, Aaron, Linnet Taylor.	Biometric Ultimata – What the Yemen Conflict Can Tell Us About the Politics of Digital Id Systems	Global Data Justice
11	2019	5	Schäffner, Martin.	Analysis and Evaluation of Blockchain-Based Self-Sovereign Identity Systems	- (Master's thesis)
12	2019	25	Toth, Kalman C., Alan Anderson-Priddy.	Self-Sovereign Digital Identity: A Paradigm Shift for Identity	IEEE Security & Privacy
13	2020	0	Ahmed, Khaled A. M., Sabry F. Saraya, John F. Wanis, Amr M. T. Ali-Eldin.	A Self-Sovereign Identity Architecture Based on Blockchain and the Utilization of Customer's Banking Cards : The Case of Bank Scam Calls Prevention	2020 15th International Conference on Computer Engineering and Systems
14	2020	6	Gstrein, Oskar J., Dmitry Kochenov.	Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?	Frontiers in Blockchain
15	2020	34	Houtan, Bahar, Abdelhakim Senhaji Hafid, Dimitrios Makrakis.	A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare	IEEE Access
17	2020	19	Kondova, Galia, Jörn Erbguth.	Self-Sovereign Identity on Public Blockchains and the GDPR	Proceedings of the 35th Annual ACM Symposium on Applied Computing
18	2020	36	Kuperberg, Michael.	Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective	IEEE Transactions on Engineering Management
19	2020	1	Lim, Jonathan.	Self-Sovereign Identity: The Harmonising of Digital Identity Solutions through Distributed Ledger Technology	ANU Journal of Law and Technology

No.	출간 년도	인용 횟수	저자	논문명	저널
20	2020	3	Naik, Nitin, Paul Jenkins.	Your Identity Is Yours: Take Back Control of Your Identity Using Gdpr Compatible Self-Sovereign Identity	2020 7th International Conference on Behavioural and Social Computing
21	2020	4	Naik, Nitin, Paul Jenkins.	Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems	IEEE International Symposium on System
22	2020	52	Wang, Fennie, Primavera De Filippi.	Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion	Frontiers in Blockchain
23	2020	2	Wittek, Kevin Lazzati Laura Bothe David Sinnaeve Ann-Julie Pohlmann Norbert.	An Ssi Based System for Incentivized and Selfdetermined Customer-to-Business Data Sharing in a Local Economy Context	2020 IEEE European Technology and Engineering Management Summit (E-TEMS)
24	2020	8	Zwitter, Andrej J., Oskar J. Gstrein, Evan Yap.	Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual	Frontiers in Blockchain
25	2020	-	권현영	데이터 주권 시대의 블록체인 기술 활용 가능성과 개발 현황	주간기술동향
26	2020	0	박진아	데이터의 보호 및 유통 법제 정립 방안	서강법률논총
27	2020	0	여기호, 박근덕, 염홍열	분산 Id 보관 및 연계 서비스 모델 제안	정보보호학회 논문지
28	2020	0	오현택, 양진홍	마이데이터 환경에서 개인의 전자 건강/의료 데이터 활용을 위한 데이터 거래모델	한국정보전자통신 기술학회 논문지
29	2021	0	Freytsis, Maria, Iain Barclay, Swapna Krishnakumar Radha, Adam Czajka, Geoffery H. Siwo, Ian Taylor, Sherri Bucher.	Development of a Mobile, Self-Sovereign Identity Approach for Facility Birth Registration in Kenya	Frontiers in Blockchain
30	2021	2	Gans, Rachel Benchaya, Jolien Ubacht, Marijn Janssen.	Self-Sovereign Identities for Fighting the Impact of Covid-19 Pandemic	Digital Government: Research and Practice

No.	출간 년도	인용 횟수	저자	논문명	저널
31	2021	0	Grech, Alex, Ira Sood, Lluís Ariño.	Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education	Frontiers in Blockchain
32	2021	0	Kim, Bong Gon, Young-Seob Cho, Seok-Hyun Kim, Hyoungshick Kim, Simon S. Woo.	A Security Analysis of Blockchain-Based Did Services	IEEE Access
16	2021	0	Kim, Geun-Hyung.	A Design of Self-Sovereign Data Distribution Platform for a Reliable Data Economy	Journal of Digital Contents Society
33	2021	0	Lockwood, Mick	Exploring Value Propositions to Drive Self-Sovereign Identity Adoption	Frontiers in Blockchain
34	2021	0	Penedo, Andrés Chomczyk	Self-Sovereign Identity Systems and European Data Protection Regulations: An Analysis of Roles and Responsibilities	Gi-Edition
35	2021	7	Shuaib, M., S. Alam, M. Shahnawaz Nasir, M. Shabbir Alam	Immunity Credentials Using Self-Sovereign Identity for Combating Covid-19 Pandemic	Mater Today Proc
36	2021	6	Shuaib, Mohammed, Shadab Alam, Mohammad Shabbir Alam, Mohammad Shahnawaz Nasir	Self-Sovereign Identity for Healthcare Using Blockchain	Materials Today: Proceedings
37	2021	0	Siqueira, Alexandre, Arlindo Flavio Da Conceição, Vladimir Rocha	Blockchains and Self-Sovereign Identities Applied to Healthcare Solutions: A Systematic Review	arXiv preprint arXiv:210412298
38	2021	0	Soltani, Reza, Uyen Trang Nguyen, Aijun An	A Survey of Self-Sovereign Identity Ecosystem	Security and Communication Networks 2021
39	2021	0	Stockburger, Lukas, Georgios Kokosioulis, Alivelu Mukkamala, Raghava Rao Mukkamala, Michel Avital	Blockchain-Enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation	Blockchain: Research and Applications
40	2021	0	고영미	탈중앙화 자기주권신원인증(Did) 에 대한 법적 고찰	법학논총
41	2021	0	송영현	블록체인 기술의 사회에서의 보편적 활용을 위한 규범성 고찰	IT 와 법 연구

**손 영 진 (Son, Young Jin)**



이화여자대학교 사회학과를 졸업하고, 현재 이화여자대학교 일반대학원 경영학과 석사통합과정 재학 중이다. 주요 관심분야는 블록체인, 인간 행동, 빅데이터 등이다.

**박 민 정 (Park, Min Jung)**



성신여자대학교에서 법학사, 이화여자대학교에서 빅데이터분석학 석사학위, 경영학과에서 박사학위를 취득하였다. 주요 연구 분야는 개인정보보호, 정보보안, AI, 블록체인 등이다.

**박 정 숙 (Park, Jung Suk)**



숙명여자대학교 통계학과와 경영학 석사를 취득하였고, 고려대학교 정보보호학 박사 수료하였다. 현재 한국인터넷진흥원 수석연구원으로 재직하고 있으며, 주요 관심분야는 개인정보보호 및 정보보안 등이다.

**황 화 정 (Hwang, Hwa Jeong)**



국민대학교 영어영문학 학사, 서강대학교 MBA 경영정보시스템 석사 취득 후 이화여자대학교 경영학과 MIS 박사과정 재학 중이다. 현재 LG CNS에서 블록체인 컨설팅과 사업개발을 담당하고 있다. 주요 관심분야는 블록체인, DID, 정보보호와 AI이다.

**채 상 미 (Chai, Sang Mi)**



현재 이화여자대학교 경영대학 부교수로 재직 중이다. 이화여자대학교에서 학사, 서울대학교에서 경영학 석사학위를 취득하였으며, 미국 The State University of New York at Buffalo에서 경영학 박사학위를 취득하였다. 주요 전문분야는 정보기술과 인간 행동에 관한 주요 이슈 IT와 조직 및 전략, 정보보안과 조직, 그리고 최근에는 AI, 블록체인을 비롯하여 빅데이터 분석 기술을 활용한 연구를 진행하고 있다.

<Abstract>

## **Self-Sovereign Identity (SSI): Structured Literature Reviews with Socio-Technical Perspective**

Son, Young Jin · Park, Min Jung · Park, Jung Suk · Hwang, Hwa Jung · Chai, Sang Mi

The concept of Self-Sovereign Identity (SSI) has emerged to overcome the limitations of traditional centralized personal identity management systems in our society. Therefore, in this study, 36 seminal researches out of 112 collected studies were investigated with a systematic literature review method to deliver a core common definition as well as the research trends on SSI in the socioeconomic, legal and technological fields. SSI studies in the legal field have mainly considered the conflicts with relevant laws such as General Data Protection Regulation (GDPR) and privacy protection laws. The study of SSI in the technology field have looked at the trends of the technical components to implement SSI and discussed the necessities of establishing standards to increase interoperability for SSI diffusion worldwide. This study ultimately derived the core definition of SSI from a various academic fields as “a trust-based personal identity management system that enables autonomous self-identification by a identity owner without a centralized system or 3rd party intervention”. The results of this study contribute to the understanding of the essential SSI concept which were varied on different research fields and industries. The results also provide a foundation for discovering various SSI-based business models, applications as well as future research opportunities. Furthermore, this study suggested that SSI must be developed with interdisciplinary manner among the socioeconomic, legal, and technological fields to be practically applicable system to enable autonomous self-identification by a identity owner in our society.

**Keyword:** Blockchain, DID, Self-Sovereign Identity, Systematic Reviews

\* 이 논문은 2021년 8월 26일 접수, 2021년 9월 17일 1차 심사, 2021년 11월 25일 게재 확정되었습니다.