

논문 2024-1-4 <http://dx.doi.org/10.29056/jsav.2024.03.04>

SBT와 NFT를 활용한 디지털휴먼의 신원 및 소유권 통합 인증 연구

김동완*, 홍두표*, 노창현*, 신동명*†

An Integrated Authentication Study of Digital Human Identity and Ownership Using SBT and NFT

Dong-Wan Kim*, Dupyo Hong*, ChangHyun Roh*, Dong-Myung Shin*†

요 약

디지털휴먼은 디지털 신원 인증 대상인 사용자의 개성과 신원을 메타버스 내에서 시각화하여 사용자 간의 상호작용을 통해 경제활동 및 사회참여를 구현한다. 이 같은 디지털휴먼은 사칭 및 도용 문제를 방지하기 위해 사용자에게 대한 신원 인증 과정이 필수적이다. 하지만 대부분의 메타버스 플랫폼은 중앙 서버 의존에서 비롯된 보안 취약점이 존재하거나, 분산화된 블록체인 환경에서 신원과 관련된 정보가 공개될 수 있다는 잠재적인 문제가 발생한다.

따라서 본 논문에서는 메타버스환경에서 디지털휴먼의 신원 인증 및 소유권 증명 문제를 해결하기 위해 SBT와 NFT를 활용한 통합 인증 시스템을 제안한다. 제안 시스템에서 사용자는 KYC인증을 통해 플랫폼으로부터 SBT를 발급받으며, 디지털휴먼에 대한 신원 인증은 스마트컨트랙트를 통해 이루어진다. 이는 한 번의 스마트컨트랙트를 통해 소유권과 신원 인증을 처리함으로써 인증 과정의 효율성을 높인다. 제안 시스템을 통해 안전하고 효율적인 디지털 신원 관리 시스템의 구축할 수 있을 것으로 기대한다.

Abstract

Digital Human visualizes the personality and identity of users subject to digital identity authentication within the metaverse and realizes economic activities and social participation through interaction between users. For these digital humans, an identity authentication process for users is essential to prevent impersonation and theft issues. However, most Metaverse platforms have security vulnerabilities resulting from reliance on central servers, or potential problems arise in which identity-related information may be disclosed in a decentralized blockchain environment.

Therefore, in this paper, we propose an integrated authentication system using SBT and NFT to solve the problems of identity authentication and ownership proof of digital humans in the metaverse environment. In the proposed system, users receive SBT from the platform through KYC authentication, and identity authentication for digital humans is performed through smart contracts. This increases the efficiency of the authentication process by processing ownership and identity authentication through a single smart contract. We expect that the proposed system will allow us to build a safe and efficient digital identity management system.

한글키워드 : 메타버스, 디지털휴먼, NFT, SBT, 신원 증명

keywords : Metaverse, Digital Human, Non-Fungible Token, Soulbound Token, Identity Verification

* 엘에스웨어(주) 소프트웨어연구소 연구개발본부 접수일자: 2024.03.06. 심사완료: 2024.03.17.

† 교신저자: 신동명(email: roland@lsware.com) 게재확정: 2024.03.20.

1. 서론

최근 가상 현실(Virtual Reality) 기반의 메타버스 시장 규모가 증가하고 있다. 아울러 업무, 소셜 네트워킹, 엔터테인먼트 등 오프라인 서비스가 가상세계로 전환됨에 따라 사용자가 자신임을 표현할 수 있는 수단의 필요성이 대두되고 있다[1]. 디지털휴먼은 인공지능, 그래픽스, 가상 현실 기술 등을 활용하여 만든 사용자 인터페이스 또는 아바타이다[2]. 디지털휴먼은 사용자가 메타버스 세계에서 상호작용을 수행하는 주요 수단으로, 사용자의 개성과 신원을 표현하며 개인의 정체성을 드러내는 역할을 수행한다. 이에 따라 사용자의 개성과 신원을 나타내는 디지털휴먼에 대한 소유권 인증의 필요성이 대두되고 있다[3].

사용자가 메타버스 내에서 자신의 개성과 신원을 시각적으로 표현하는 것은 매우 개인적인 행위인 만큼, 소유권을 명확히 인증함으로써 해당 디지털휴먼이 특정 사용자의 유일한 신원과 독특한 개성을 대표한다는 것을 보장해야 한다. 이는 타인에 의한 사칭이나 도용을 방지하기 위해 필수적이다. 또한, 소유권 인증은 디지털휴먼이 참여하는 거래의 정확성과 투명성을 보장하는데 중요한 역할을 한다. 사용자가 자신의 디지털휴먼을 통해 상품이나 서비스를 구매, 판매 또는 교환할 때, 디지털휴먼과 소유권 인증을 기반으로 경제활동을 수행하기 때문이다.

따라서 NFT(Non-Fungible Token)를 활용한 소유권 증명에 관한 연구가 활발히 진행되고 있지만[4][5][6], NFT 인증서가 신원 인증에 관한 정보를 충분히 제공하지 못한다는 한계가 있다[7]. NFT의 주된 초점은 자산 자체에 맞춰져 있으며 소유주의 신원에 대해서는 다루지 않는다. 이는 NFT가 특정 블록체인 지갑 주소에 의해 디지털휴먼이나 다른 자산이 소유되고 있음을 명확하게 증명할 수 있지만, 블록체인 지갑의 특성

으로부터 비롯되는 가명성 제공 때문에 정확한 신원 인증의 어려움이 있다[7].

플랫폼 기반의 가상세계에서 디지털휴먼에 대한 사용자의 신원 인증 방식은 크게 중앙 집중 방식과 탈중앙화 방식으로 구분한다[8]. 중앙 집중 방식은 단일 실패 지점(Single Point of Failure)에 대한 보안 취약점을 갖는다. 단일 실패 지점은 모든 데이터가 중앙 서버나 데이터베이스에 저장된 구조로, 사용자의 신원 정보, 금융 정보 등 민감한 정보가 대규모로 노출될 위험이 있다[9]. 일례로, 메타버스 플랫폼인 로블록스는 2020년 5월에 해킹 사고로 인해 사용자 1억 명 규모의 개인 정보가 유출되는 사건이 있었다[10]. 따라서 탈중앙화의 원칙을 준수하며 강력한 보안과 프라이버시를 제공하고 사용자의 주도권을 보장할 수 있는 새로운 디지털 신원 검증 방식이 필요하다.

이러한 문제를 해결하기 위해 본 논문은 SBT(Soulbound Token)와 NFT를 활용한 통합 인증 시스템을 제안한다. SBT는 전송이나 거래 행위가 불가능하며 사용자의 신원 정보를 담은 토큰으로, 개인 신원을 증명하는 데 사용된다[11]. 제안 기법은 스마트 계약을 통해 소유권 확인과 신원 인증을 동시에 처리하여 인증 과정을 간소화한다.

제안 기법은 블록체인 네트워크상에서 진행되므로, 기존의 중앙화된 시스템에 대한 의존도를 낮추며 신원 인증의 안정성을 높인다.

본 논문의 구성은 다음과 같다. 2장에서는 디지털휴먼의 개념과 소유권 및 신원 인증에 관한 이슈를 다룬다. 3장에서는 SBT와 NFT의 개념 및 특성과 표준을 설명하고, 비교 분석한다. 4장에서는 SBT와 NFT를 적용한 소유권 및 신원 인증 통합관리 기법을 설명한다. 5장에서는 결론과 본 연구의 한계점 및 향후 연구 방향에 대해 제시한다.

2. 디지털휴먼

2.1 디지털휴먼의 개념

디지털휴먼은 사람의 신체 구조와 움직임을 가상공간에서 재현하는 디지털 기술로 제작하여 사람과 동일한 외형을 갖추고 있는 가상 인간이다. 디지털휴먼의 역할과 중요성을 강조하기 위해 메타버스를 ‘디지털로 구현된 공유 공간에서 아바타(디지털휴먼)로 활동하는 실감 기술 바탕의 플랫폼’으로 정의하기도 한다[12].

대한민국에서 디지털휴먼이 최초로 등장한 사례는 1998년 1월, 사이버 가수 ‘아담’이다. 하지만 ‘아담’은 고도의 그래픽 작업에 대한 큰 비용 등 여러 이유로 인해 활동을 중단했다[13]. 그러나 컴퓨터 그래픽 기술, AI 기반의 렌더링 기술, 실시간 모션 캡처 기술 등이 크게 발전하면서 디지털휴먼의 모델링과 움직임을 더욱 자연스럽게 만들어 인간과 상호작용하는 것이 가능해졌다. 디지털휴먼 생성 기술 중 하나인 블류메트릭 캡처는 다수의 카메라를 사용해 객체를 사실적인 3차원으로 촬영하는 방식이다. 단일 이미지 기반 3D 휴먼 모델링 기술은 한 장의 사진으로부터 3차원 전신 모델을 생성하여 애니메이션화한 3D 캐릭터를 만드는 기술이다. 영상 합성 기반 휴먼 렌더링은 사람의 다양한 표정을 학습해 새로운 표정을 생성하는 기술로, 실존하지 않는 인물이나 표정, 동작 등을 생성할 수 있다[14].

이 같은 디지털휴먼을 사실적으로 표현하는 기술은 메타버스와 같은 가상 환경에서 사용자가 가상세계에서의 사회적 상호작용과 몰입감을 극대화하는 데 중요한 역할을 한다[15]. 또한, 대부분의 메타버스 이용자는 현실감 있는 디지털휴먼을 통해 메타버스에서 자아정체성을 형성하며, 현실 또는 또 다른 삶의 모습을 구현하고자 한다[16]. 가상공간에서 자신의 이상적인 이미지를 추구하는 사람은 디지털휴먼과의 일치감이나 메타

버스 공간 내 몰입도가 높게 나타나는 것으로 알려졌다[17].

2.2 디지털휴먼의 소유권 증명 문제

메타버스 내에서 사용자가 생성한 디지털휴먼은 사용자의 디지털 정체성과 창의력을 확장하는 수단이다. 웹 도메인, 컴퓨터 게임의 아이템, 그리고 아바타가 재산으로 인정받아 온 것처럼, 메타버스에서 아바타의 소유권 관리 역시 필수적인 기술로 자리매김하고 있다[3]. 이러한 디지털 자산에 대한 명확한 소유권 규정은 사용자의 창작물을 보호하고, 무단 복제 및 도용을 방지하는데 중요한 절차이다. [3]의 연구에서는 디지털휴먼의 3D 모델링 관련 파일 형식이 소유권 정보를 크게 고려하지 않고 있음을 지적한다. 표 1은 Autodesk에서 사용하는 3D 모델링에 대한 파일 정보이며, 디지털휴먼의 대한 제작자, 디지털휴먼을 사용하는 이용자 정보 등 소유 정보에 대한 정보가 존재하지 않는다. 이는 디지털휴먼에 대한 소유권 및 사용자 인증에 관한 내용이 부족함을 나타낸다.

표 1. FBX 파일에서의 File Information [3]
Table 1. File Information in FBX File [3]

구분	설명
File Version	파일 버전
File Unit	단위
System Axis Direction	시스템 축 방향
...	...

2.3 디지털휴먼의 신원 인증 문제

디지털휴먼에 소유권 문제와 정보의 부재는 단순히 소유권 증명 넘어서 사용자의 신원을 인증하는 데에도 한계가 있음을 시사한다. 메타버스 플랫폼에서 디지털휴먼에 대한 신원 인증이

부재할 경우, 소유권을 확인하기 어렵게 되어 사기, 사칭, 위조와 같은 범죄 행위가 가상 환경 내에서 증가할 위험이 따른다. 또한, 블록체인 기술을 기반으로 하는 웹3 메타버스 플랫폼은 사용자들이 여러 가명이나 공개 주소를 사용하여 참여할 수 있는 분산된 관리 환경을 제공한다[18]. 이러한 환경은 일부 사용자들이 의도적으로 이전의 신원을 폐기하고 사기 범죄를 저지를 가능성을 제공함으로써, 악의적인 활동의 추적 및 제재를 어렵게 만든다[19]. 따라서, 메타버스 플랫폼에서 디지털휴먼을 안전하게 사용하기 위해 분산형 또는 블록체인 기반의 시스템에서 신원 관리 문제를 해결해야 할 것이다.

이러한 문제를 해결하기 위해 사용자의 신원 인증을 위한 다양한 연구가 진행되었다. [20]의 연구는 NFT를 활용한 신원 인증 방법을 제안하였다. 사용자의 신원 정보는 NFT의 메타데이터로 기록되며, 블록체인상에서 고유하고 변경 불가능한 형태로 저장함으로써 사용자가 자신의 신원을 증명할 수 있다. 그러나 NFT는 거래가 가

능한 특성을 가진 토큰이기 때문에 신원 인증 정보를 포함할 경우, 거래 후 신원 정보의 부정확성 또는 오용이라는 심각한 문제를 초래할 수 있다. 즉, 신원 정보가 담긴 NFT가 거래되어 다른 사용자에게 넘어가 신원 정보의 오용 및 불일치를 초래한다. 따라서 신원 정보를 포함한 NFT의 거래는 신원 인증의 목적과 상반되는 결과를 초래하여 사용자의 디지털 자산과 신원 보호에 부정적인 영향을 미칠 수 있다.

한편, [21]은 DID(Decentralized Identifier)를 활용한 신원 증명 연구들을 소개하였다. DID는 사용자가 자신의 신원 정보를 직접 관리하고, 신원 정보의 공개 수준을 조정할 수 있게 하는 탈중앙화된 신원 확인 시스템에서 사용되는 식별자이다. 그림 1은 DID의 발급 과정과 인증 개요를 나타낸 것이다. 사용자는 DID를 발급받기 위해 신뢰할 수 있는 발급 기관에 발급 요청을 한다. 발급자인 신뢰 가능한 기관은 소유자의 신원 검증을 수행하고, 문제가 없다면 신원 정보인 DID를 발급한다. 또한, 분산ID 신뢰 저장소에 사용자

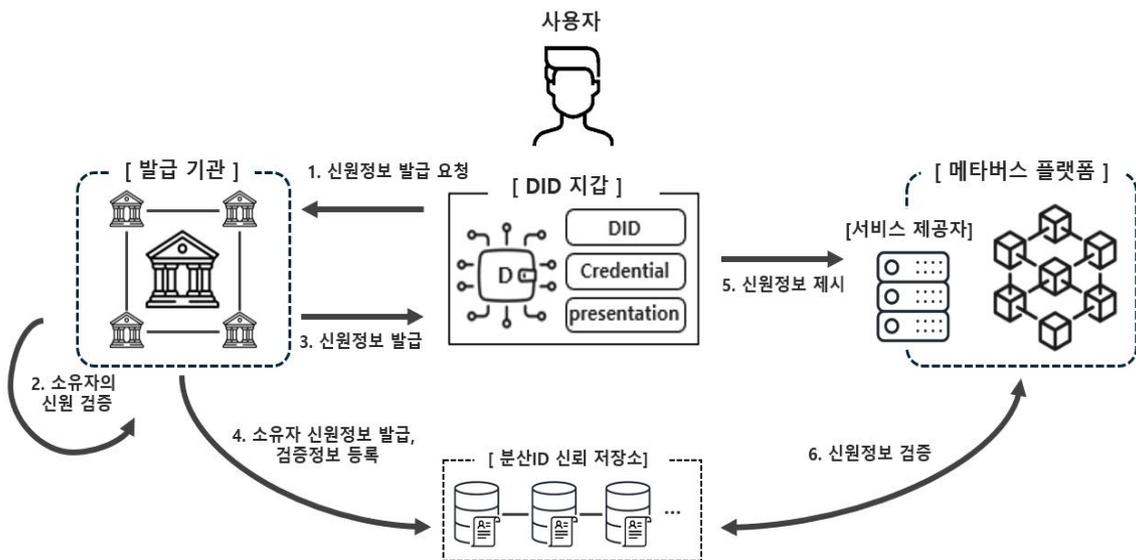


그림 1. DID 개요
Fig. 1. Overview of DID

의 신원 정보 발급에 대해 검증할 수 있는 정보를 등록한다. 사용자는 메타버스 플랫폼을 이용하기 위해 서비스 제공자에게 신원 정보를 제시한다. 서비스 제공자는 분산ID 신뢰 저장소에서 신원 정보를 검증한다. 이 같은 구조를 지닌 DID는 그림 1과 같이 사용자의 신원을 최초로 검증할 수 있는 최소한의 신뢰 기관이 필요하다. 신뢰 기관 같은 중앙 인증기관의 의존성은 완전한 탈중앙화를 구현하지 못한다는 한계가 있다. 또한, 블록체인 기반의 메타버스 플랫폼과 별도로 DID를 인증하고 관리하기 위해 별도의 분산된 환경과 DID 지갑이 필요하다. 반면에 SBT는 기존 사용자 지갑에 종속시킬 수 있으며, 신원 정보를 저장할 수 있고, 네트워크를 필요로 하지 않는다. 따라서 본 논문에서는 SBT와 NFT를 결합한 통합 인증 방식을 제안한다.

3. SBT

3.1 SBT 개념 및 특성

SBT(Soulbound Token)는 블록체인 기술을 기반으로 한 새로운 개념의 토큰으로, 사용자의 신원 인증 및 개인적인 속성과 자격을 불변의 형태로 증명하는 데 사용한다[11]. ‘Soulbound’라는 용어는 토큰이 발행된 개인에게만 영구히 속하고, 전송이나 거래 행위가 불가능하다는 특성을 의미한다. SBT는 토큰화된 디지털 자산이지만, 일반적인 NFT와 달리 사용자의 지갑이나 특정 계정에 영구히 묶여 있어 이를 바운딩(Bounding)된 토큰이라고도 한다. 이 같은 SBT의 개념은 사용자의 디지털 신원과 밀접한 연관관계를 가진다. 따라서 개인의 학력, 자격증, 경력 등과 같은 신원 정보를 블록체인에 등록하여 블록체인 네트워크상에서 신원 인증을 위한 정보로 활용할 수 있다. 표 2와 같은 특성을 가진 SBT는 신원 인

증의 관점에서 사용자가 메타버스 내에서 다양한 활동을 안전하게 수행할 수 있도록 한다[11]. 예를 들어, 마켓에서 발행한 특정 에셋의 라이선스 이용권을 SBT로 변환하면, 해당 라이선스의 진위를 메타버스 내에서 즉시 검증할 수 있다. 또한, 소유권 증명을 위한 신원 정보, 디지털 자산 거래를 위한 본인 인증 정보, 자격증이나 인턴십, 근무 경험과 같은 개인의 이력도 SBT로 기록될 수 있어 메타버스 내에서 신원을 증명하고, 특정 커뮤니티나 활동에 참여할 자격을 부여받을 수 있다.

표 2. SBT의 특성
Table 2. Characteristics of SBT

요소	특성
불변성	SBT는 발행되면 변경과 삭제가 불가능하여 신원 인증 정보의 신뢰성을 보장함
비전송성	SBT는 전송할 수 없어 신원 정보가 당사자 이외의 제 3자에게 전달되는 것을 방지함
개인화	각 SBT는 개인의 신원 인증 및 자격 증명과 같은 특정 속성을 나타냄
인증가능성	SBT에 포함된 정보는 공개적으로 검증할 수 있어 메타버스 상에서의 신원 증명에 활용됨

이 같은 SBT의 적용은 여러 사례에서 신원 또는 자격 인증의 수단으로 활용되고 있다. 일례로, 연세대학교 학술문화처는 세미나에서 우수 참여자들에게 SBT 발급을 통해 학생들의 세미나 참여를 인증하고 독려하는 효과를 얻었다[22]. 학생들은 오픈씨 (OpenSea)와 같은 NFT 플랫폼을 통해 본인이 소유한 SBT를 확인할 수 있으며, 소셜 미디어를 통해 이를 공유할 수 있다. 한편, 암호화폐 거래소인 바이낸스(Binance)는

KYC(Know Your Customer) 인증을 완료한 사용자에게 SBT를 발행하는 등[23] 신원 및 자격 인증을 위한 SBT의 활용이 확대되고 있다. KYC는 금융기관이 고객의 신원을 확인하는 인증 과정으로, SBT를 발급하기 위한 인증으로 사용될 수 있다[7].

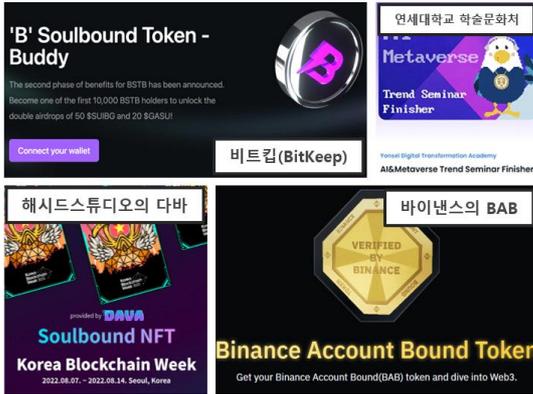


그림 2. SBT 사용 사례
Fig. 2. Examples of SBT Usage

메타버스 플랫폼 내에서 사용자가 생성한 디지털휴먼, 디자인 예셋, 배경, 음악 등 모든 개체는 해당 창작자에 의해 제작되며, 이들 각각의 모델링 정보와 창작자의 소유권은 NFT를 통해 증명할 수 있다. 이와 더불어, NFT에 기록된 저작권자 또는 창작자의 신원은 SBT와의 연결을 통해 추가적으로 인증할 수 있으며, 이는 창작물의 실제 소유주 및 창작자의 신원을 명확하게 하고, NFT로 증명된 소유권과 함께 통합적인 인증 체계의 구성이 가능하다.

3.2 NFT 및 SBT 표준

이더리움의 토큰은 EIP(Ethereum Improvement Proposals) 제안과 ERC(Ethereum Request for Comments) 표준에 따라 제정되며, 이를 통해 이더리움의 발전 방향이 결정된다. 개

발자들은 이더리움의 한계를 개선하기 위해 지속적으로 새로운 제안을 하고 있으며, NFT나 SBT와 관련된 여러 개선 사항이나 새로운 개발이 진행 중이다. 표 3과 표 4는 각각 NFT와 SBT의 주요 표준을 나타낸 것이다.

ERC-5192는 SBT를 구현하기 위해 필요한 기본 인터페이스를 정의하는 표준이다. 이 표준은 ERC-5192가 제안되기 전, 여러 SBT 구현에서 전송 기능 사용 시 발생하는 오류를 해결하기 위해 제안되었다[24]. 이 같은 ERC-5192는 기존 ERC-721 표준에 Locked 이벤트와 Unlocked 이벤트를 다루는 Event 속성과 locked 함수 및 locked 여부를 체크하는 함수가 추가되었다. locked 속성이 true인 경우, 전송과 관련된 기능은 모두 무시되어야 한다는 점을 명시하였다.

표 3. NFT의 주요 표준
Table 3. NFT Key Standards

구분	명칭	설명
ERC-20	Fungible Token	대체 가능 토큰
ERC-721	Non-Fungible Token	대체 불가능 토큰
ERC-777	Token Standard	토큰 표준
ERC-1155	Multi Token Standard	다중토큰 표준
ERC-4519	Non-Fungible Tokens Tied to Physical Assets	NFT의 물리적인 자산연결 표준
ERC-5023	Shareable Non-Fungible Token	공유 가능한 NFT 표준
ERC-6220	Composable NFTs utilizing Equippable Parts	장착 가능한 NFT 표준

표 4. SBT의 주요 표준
Table 4. SBT Key Standards

구분	명칭	설명
ERC-165	Standard Interface Detection	표준 인터페이스 정의
ERC-721	Non-Fungible Token	대체 불가능 토큰
ERC-1238	Non-transferable Non-Fungible Tokens	양도 불가능한 대체 불가능 토큰
ERC-5192	Minimal Soulbound NFTs	SBT의 전송 가능 여부 체크 인터페이스
ERC-5484	Consensual Soulbound Tokens	SBT 표준 (ERC-721 확장)
ERC-6239	Semantic Soulbound Tokens	SBT에 메타데이터를 삽입한 표준확장

3.3 SBT와 DID의 비교 분석

SBT와 DID는 디지털 신원 문제를 다루기 위한 기술로 분산 원장을 기반으로 하며 신원 인증을 하기 위해 활용된다. 표 5는 SBT와 DID를 비교 분석한 것이다. NFT의 변형인 SBT의 특징은 사용자의 지갑에 귀속되어 양도가 불가능하다는 점이다. 또한, NFT와 같이 변하지 않는다는 특징을 갖는다. 이로써, 소유자의 고유한 특성을 영구적으로 표현하여 신원 인증이나 업적 등을 나타내는 데 사용된다. 이러한 SBT는 스마트컨트랙트를 통해 토큰 형식으로 발행하고 블록체인 네트워크상에서 관리되어 커뮤니티 단위의 인증 절차를 수행한다. 이 같은 구조를 가진 SBT는 사용자의 프라이버시 보호 관점에서 추가적인 조치가 필요할 수도 있다. SBT를 제안한 논문에서 SBT는 개인 정보 보호에 대한 기술적인 수단을

언급하지만[11], 블록체인의 퍼블릭 네트워크와 SBT 자체에 의존하는 것만으로는 이상적인 프라이버시 보호 달성하기 어려운 한계가 있다[27].

표 5. SBT와 DID 비교 분석
Table 5. Comparative of SBT and DID

이름	SBT	DID
정의	- 개인에게 귀속되는 블록체인기반 디지털 토큰	- 사용자가 직접 관리하는 분산형 신원 인증 시스템
용도	- 신원 인증 - 자격 증명 - 신뢰 네트워크 구축	- 신원 인증 - 자격 증명 - 자기 주권 신원 실현
특징	- 양도 불가능 - 변형 불가능 - 커뮤니티에 의한 인증	- 사용자 주도의 신원관리 - 프라이버시 보호 강화 - 다 플랫폼 호환
기술 구현	- 블록체인 기반 - 스마트컨트랙트를 통한 발행	- 분산원장(DLT) 기술 기반
개인 정보 보호	- 개인정보 과도 노출 위험 - 선택적 정보공개 제한	- 사용자 선택적 정보 공개
전송 가능성	- 전송 불가능	- 전송 가능
장점	- 개인 특성 명확 표현 가능 - 커뮤니티 기반의 신뢰 구축	- 사용자가 신원 정보를 직접 관리 및 통제 - 향상된 프라이버시
단점	- 유연성 제한 - 프라이버시 보호 강화 필요	- 복잡한 관리 시스템 - 인증 기관 의존 - 키 복구 어려움

또한, SBT는 양도와 변경이 불가능하다는 점에서 유연성이 제한된다. 이는 정보의 업데이트로 인해 사용자 신원 정보를 변경해야 할 때 제약 사항으로 작용한다.

반면, DID는 사용자가 자신의 디지털 신원을 통제하고, 다양한 온라인 서비스에 접근할 목적으로 설계되었다. 이 같은 DID는 누구나 필요한 신원 정보를 언제든지 생성하여 이용할 수 있고 신원 정보의 활용처를 파악할 수 있다는 장점이 있다. DID는 다양한 블록체인 및 분산원장 기술 기반으로 구현될 수 있으며, W3C(World Wide Web Consortium)[28]에 의해 표준화된 규격을 따른다. DID는 신뢰 가능한 인증기관이 발행하고, 분산 원장 기술(Distributed Ledger Technology)에 의해 관리된다. DID는 사용자에게 의해 각각 다른 정보가 담긴 여러 DID를 가질 수 있으며, 사용자가 자신의 신원 정보를 직접 관리하고 통제할 수 있다. 또한, 프라이버시 보호 강화를 위한 별도의 프로그래밍에 대한 제약이 없다. DID 자체는 신원 정보를 위한 식별자 역할을 하지만, 사용자의 필요에 따라 제 3자에게 전송이 가능하다. 하지만 이 같은 DID는 구조상 복잡한 관리 시스템을 가진다는 문제점이 있다. 또한, 메타버스와 같은 타 플랫폼에서 DID를 채택할 때, 기존 블록체인 네트워크와 다른 별도의 신원 인증 및 관리를 위한 분산원장이 필요하다는 단점이 있다. 뿐만 아니라, 사용자 입장에서 자신의 신원 정보를 직접 관리한다는 개념은 이론적으로는 매력적이지만, 실제로는 기술적 지식이 필요한 경우가 많아 접근성이 낮을 수 있다는 우려가 있다. DID 사용자는 자신의 디지털 신원을 안전하게 관리해야 하는 책임이 있으며, 커뮤니티에 의한 복구 매커니즘이 있는 SBT와 달리, 자신의 개인 키를 분실하면 해당 DID와 연결된 모든 정보와 자격증명에 대한 접근이 어렵다. 또한, DID는 복잡한 구조의 시스템 때문에 환경 구

성 및 개발과 관리가 난해하다는 문제점이 있다. 따라서 본 논문에서는 이 같은 문제를 해결하기 위해 NFT 및 SBT 기반의 통합 인증 개념을 제안한다.

4. NFT 및 SBT 기반의 소유권 및 신원 인증 통합 증명 개념

4.1 전체 개요

메타버스 플랫폼에서 사용하는 디지털휴먼에 관한 디자인 정보는 사람의 신체 구성과 유사한 모델링 데이터로 구성된다. 외형뿐만 아니라 착용가능한 헤어 등의 액세서리 같이 디자인된 모델링 데이터가 합쳐져 하나의 디지털휴먼의 외형을 이룬다. 이러한 특징에서 소유권 정보를 포함하는 NFT 적용은 일반적인 ERC-721 및 ERC-6220 표준을 기반으로 적용해야 한다. 또한, NFT의 소유권을 증명 과정 시 필요한 신원 인증 정보는 대체 불가능해야 하며, 조작의 위험성이 없고, 투명해야 하며, 정보의 거래가 불가능해야 한다. 따라서 SBT는 ERC-721과 ERC-1238을 바탕으로 ERC-5192, ERC-5484의 표준을 적용해야 한다.

기본적으로 SBT는 사용자의 신원을 증명하는 도구이며, 전송이나 거래 행위가 불가능해 소유자에게만 귀속되는 특성을 가진다. 그러나 신원 인증에 필요한 정보나 자격을 증명하는 시스템은 필요에 따라 정보의 업데이트가 가능하도록 설계되어야 한다. 따라서 불변속성을 가진 SBT에 NFT와 같은 다른 디지털 토큰과의 연동이나 레코드를 통해 구현되어야 한다.

본 논문의 소유권 및 신원 인증 통합 증명을 위한 SBT 적용 예시는 사용자가 신원과 관련된 SBT를 보유하고 있어, 다른 메타버스 서비스에 접속할 때 사용자의 지갑에 SBT를 보유하고 있



그림 3. 디지털휴먼의 SBT 및 NFT 통합 인증 적용 전체 시나리오
 Fig 3. Integrated Authentication Scenario for Digital Human Using SBT and NFT

음을 증명하기만 하면 된다. 따라서 별도의 자격 증명 또는 ID 정보를 각각의 메타버스 서비스 공급자에게 전송할 필요가 없다. 그림 3은 디지털 휴먼의 SBT 및 NFT 통합 인증 적용 전체 시나리오를 나타낸 것이다. 본 장에서는 그림 3의 절차에 따라, 사용자의 신원 인증 및 디지털휴먼의 소유권을 증명하기 위한 통합 인증 방법에 대해 설명한다.

4.2 사용자 지갑 생성 단계

사용자는 메타버스 플랫폼을 이용하기 위해 그림 4와 같이 지갑을 생성한다. 메타버스 플랫폼에서 사용되는 디지털 지갑은 NFT, 배지 같은 디지털 자산만 저장할 수 있다. 따라서 본 논문에서의 적용 예시에서는 신원에 대한 자격 증명, SBT, NFT를 관리하기 위해 BIP-44(Bitcoin Improvement Proposal 44)[26] 주소체계 기반의 HD 지갑(Hierarchical Deterministic Wallet)을 사용한다. HD 지갑이란, 하나의 마스터 시드(seed) 키를 사용하여 무수히 많은 주소를 생성할 수 있는 암호화폐 지갑이다[29]. 사용자의 지갑은 키 파생 알고리즘을 통해 고유의 단일 시드 값에서 개인 키를 파생하고, ECDSA(Elliptic Curve Digital Signature Algorithm)[30]을 통해 개인키에 해당하는 공개키를 생성한다.

4.3 디지털휴먼 생성 및 NFT 주조 단계

메타버스 환경에서 디지털휴먼은 사용자의 가상 대리인으로서, 개인의 신원과 개성을 표현하는 중요한 수단이다. 사용자는 블록체인 플랫폼 내에서 그림 5와 같이 아바타를 생성한다. 아바타의 모델링에 관한 데이터는 데이터의 해시값, 제작자, 사용 플랫폼 등의 파일 정보를 메타데이터화 하여 블록체인에 저장하기 위한 적합한 포맷으로 변환한다. NFT 저장 및 서명은 변환된 메타데이터와 사용자의 지갑 주소를 NFT 스마트 컨트랙트에 입력하여 트랜잭션을 생성한다.

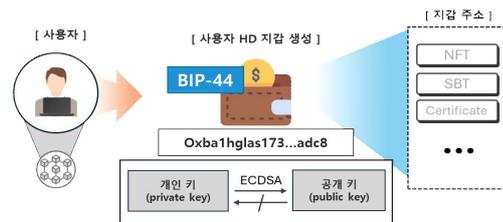


그림 4. 사용자 지갑 생성
 Fig 4. User Wallet Creation

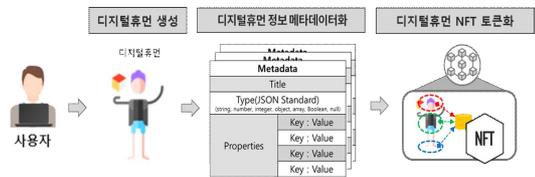


그림 5. 디지털휴먼 생성 및 NFT 주조
 Fig 5. Creation of Digital Humans and Minting of NFTs

트랜잭션 생성자의 서명이 포함된 트랜잭션이 블록체인 네트워크의 규칙을 준수할 때, 트랜잭션 내용이 포함된 블록이 생성되어 NFT가 발행된다.

4.4 사용자 자격 증명 단계

사용자는 ID 카드 정보를 제공하는 것과 유사하게 자격 증명 발급자에게 KYC 발급에 필요한 정보를 제출한다. 이는 사용자의 실명, 생년월일, 국적 등의 개인 정보가 포함될 수 있으며, 디지털 신원의 바탕이 된다. 사용자의 정보가 확인되면 발급자는 신분증 양식과 유사하게 자격 및 ID를 증명할 수 있는 자격 증명을 제공한다. 사용자는 발급받은 자격 증명을 사용자 지갑에 저장한다.

4.5 신원 정보를 포함하는 SBT 발행 단계

제안하는 개념의 메타버스 플랫폼에서는 사용자의 디지털 신원을 안전하게 관리하고 인증하기 위해 SBT의 발행 과정을 도입한다. SBT 발행 과정은 스마트컨트랙트의 생성 및 배포, 사용자 자격 증명의 서명 추가, 트랜잭션 생성 및 검증, SBT의 발행으로 구성된다. 스마트컨트랙트의 생성 및 배포과정에서 메타버스 플랫폼은 사용자에게 발행될 SBT를 관리하기 위해 특정 권한을 가진 스마트컨트랙트를 생성한다. 이 컨트랙트는 사용자의 자격 증명을 확인하고, 해당 증명이 플랫폼의 요구 조건을 충족할 때만 SBT를 생성 및 발행할 수 있다. 생성된 스마트컨트랙트는 블록체인 네트워크에 배포된다. 자격 증명 및 트랜잭션 생성 과정에서는 사용자가 자신의 자격 증명에 서명을 추가한다. 이를 통해 생성된 트랜잭션에는 스마트컨트랙트에서 설정한 조건을 충족하는 증명이 포함된다. 트랜잭션 검증 과정에서의 스마트컨트랙트는 사용자로부터 제출된 트랜잭션 증명을 검증한다. 검증이 완료되면 사용자의

지갑 주소로 SBT가 발행된다. 이 같은 SBT 발행 과정은 사용자의 자격 증명을 검증하는 스마트컨트랙트와 증명이 참(True)으로 검증될 경우에 SBT를 발행하는 두 가지 주요 스마트컨트랙트를 통해 수행된다. 위 과정에서 컨트랙트는 증명 검증(Verify Proof)을 통해 사용자의 주소로 등록하고 SBT 발행을 위한 권한을 확인한다.

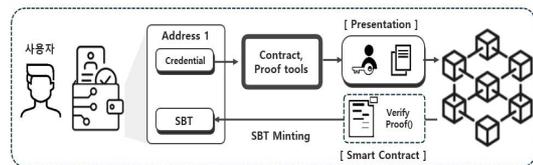


그림 6. 신원 정보를 포함하는 SBT 발행
Fig 6. Issuance of SBTs Containing Identity Information

4.6 NFT 및 SBT 기반의 디지털휴먼 소유권 및 신원 통합 인증 단계

인증 과정을 거쳐 발행된 SBT는 사용자의 지갑에 등록되어 지갑 주소를 통해 메타버스의 디지털 휴먼과 연동된다. 디지털 신원과 직접적으로 연결된 SBT는 디지털 증명서의 역할을 수행한다. 이 증명서는 사용자의 디지털 자산, 경험 및 자격 증명을 보호하고 검증하는 역할을 한다. 사용자는 특정 서비스에 접근하기 위해 자신의 지갑에 연동된 아바타 내에서 SBT의 존재를 확인하고 인증하는 과정을 거친다. 이 같은 인증 과정은 메타버스 내에서 사용자가 이용에 관한 라이선스나 거래 등의 상호작용 서비스를 이용할 수 있는지를 결정짓는다. SBT는 사용자의 개인 정보 보호를 최우선으로 고려하여 필요한 최소한의 정보만을 담고 있으며, 필요에 따라, 영지식증명(zero-knowledge proof, ZKP)[31] 같은 기술을 활용해 사용자의 정보를 은폐하면서도 소유를 증명할 수 있는 방법 등을 고려할 수 있다. 메타버스 사용자가 거래, 소유권 이전, 커뮤니티 참여

등의 다양한 활동을 할 때, 자신의 신원을 증명하는 것은 필수적이다.

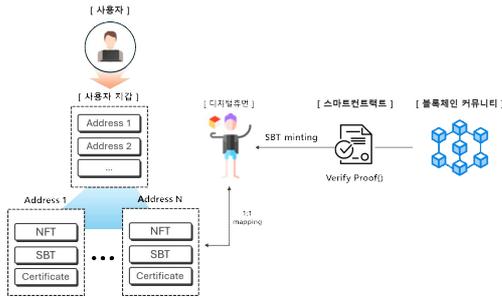


그림 7. 디지털휴먼의 소유권 및 신원 통합 인증
Fig 7. Ownership and Integrated Authentication of Digital Humans

사용자의 지갑에 연결된 SBT는 고유한 신원 정보를 포함하고 있어, 사용자의 디지털휴먼이나 NFT 트랜잭션을 포함한 블록이 블록체인에 기록되면, 해당 정보를 쉽게 조회할 수 있다. 일련의 과정을 통해 NFT와 연관된 SBT의 트랜잭션을 확인함으로써 신원과 소유권을 동시에 검증한다.

5. 결론

그래픽 기술의 발전과 메타버스 시장의 성장으로 사용자 신원을 명확하게 표현할 수 있는 디지털휴먼의 필요성이 점점 커지고 있다. 디지털휴먼은 가상 활동의 신뢰와 안전을 보장하며 개인화된 경험을 가능하게 한다. 이를 위해 소유권 인증이 주로 블록체인 기술을 통해 이루어지지만, 데이터 유출이나 신원 도용 같은 문제가 여전히 존재한다. 메타버스 내에서의 신원 확인은 NFT와 같은 자산 거래뿐만 아니라 디지털휴먼 간 상호작용의 진위 또한 확인해야 한다.

이러한 문제를 해결하기 위해 본 논문에서는

NFT와 SBT를 결합한 통합 인증 방안을 제안했다. 제안 방식은 자격 증명을 통해 발급받은 SBT를 계층적 결정 지갑인 HD 지갑에 담아 NFT의 소유권 및 신원 인증을 수행한다. 이로써, 거래나 요청이 발생할 때마다, 별도의 자격 증명을 전송할 필요 없이 사용자가 신원과 관련된 SBT를 지갑에 보유하고 있음을 증명하기만 하면 된다. 이는 블록체인의 투명성을 활용하고, 중앙화된 시스템에 대한 의존도를 낮추며, 인증의 안정성을 강화한다. 또한, 신원 인증과 소유권 인증을 함께 처리함으로써 전체 시스템의 효율성을 개선하였다. 제안 방안을 통해 사용자는 메타버스에서 자신의 신원을 확실하게 증명할 수 있으며, 소유권이나 자격 증명을 이용하여 다양한 서비스에 접근할 수 있다.

제안 기법을 통해 메타버스 내에서 신뢰할 수 있는 디지털 경제 환경을 조성할 것으로 기대한다.

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. RS-2023-00229451, 이종 플랫폼간 상호호환이 가능한 디지털휴먼(아바타) 연동 기술)

참고 문헌

- [1] Junghyun Yoon, Gaeun Kim, “The Outlook and Innovation Strategy for the Metaverse Virtual World Ecosystem”, STEPI Insight. Vol. 284, pp.1-53, Dec. 22, 2021, URI: <https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE11032833>
- [2] Nah, Ken, et al., “A study on the user experience to improve immersion as a

- digital human in lifestyle content”, Applied Sciences, Dec. 23, 2022, DOI: <https://doi.org/10.3390/app122312467>
- [3] ChangHyun Roh, Shin DongMyung, “A Study on the Application of NFT for Ownership Management of Digital Humans (Avatars) in the Metaverse Environment”, Journal of Software Assessment and Valuation, 19(2), pp.31-40. Jun. 2023, URI: <https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE11601819>
- [4] K. Venugopal, K. S. Anand, N. Lakhinana, N. M., “NFT For Collectibles”, 2023 5th Biennial International Conference on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, 2023, pp.1-5, DOI: 10.1109/ICNTE56631.2023.10146683
- [5] Dowling M. Fertile LAND, “Pricing non-fungible tokens. Finance Research Letters”, Jan. 1, 2022, DOI: <https://doi.org/10.1016/j.frl.2021.102096>
- [6] (Online) “The sandbox”, URI: https://installers.sandbox.game/The_Sandbox_Whitepaper_2020.pdf
- [7] Kim Geunyoung, Jaecheol Ryou, “Digital Authentication System in Avatar Using DID and SBT”, Mathematics 11(20), 2023, DOI: <https://doi.org/10.3390/math11204387>
- [8] Zichichi, Mirko, et al., “Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland”, Proceedings of the Fifth Distributed Ledger Technology Workshop, DLT, 2023, URI: <https://mirkozichichi.me/assets/papers/38protecting.pdf>
- [9] Soohyung Kim, “Decentralized Identity Technology Trends”, ICT Standard Weekly(TTA) No.1114, URI: http://weekly.tta.or.kr/weekly/files/20221426051420_weekly.pdf
- [10] (online) “Roblox Game Hacked, 100 Million Users’ Data Compromised”, May. 7, 2020, URI: <https://www.expresscomputer.in/secURItty/roblox-game-hacked-100-million-user-s-data-compromised-report/55078>
- [11] Weyl, E. Glen, Puja Ohlhaber, Vitalik Buterin, “Decentralized society: Finding web3’s soul”, Available at SSRN 4105763, May. 10, 2022, URI: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763
- [12] Keeyoung Yoon, “What Are the Technological Changes in the Metaverse This Year? What Are the Future Challenges”, Software Policy & Research Institute(SPRi), Dec. 13, 2021, URI: https://spri.kr/posts/view/23352?code=data_all&study_type=industry_trend
- [13] Dokyung Kim, “The Golden Age of Virtual Humans, ‘Virtual Influencers’”, Machinery & Equipment News, Mar. 4, 2022, URI: <http://www.kmecnews.co.kr/news/articleView.html?idxno=24862>
- [14] Hwasup Lim, Jae-In Hwang, “Introduction to Immersive Content Technology in the Non-contact Era Using Digital Humans”, Convergence Research Review, Vol. 7, No. 3, Mar. 8, 2021, URI: https://crpc.kist.re.kr/user/nd49151.do?View&term_id=&uQ=&itemShCd1=&pageLS=10&page=1&pageSC=REGDATE&pageSO=DESC&dmlType=&boardNo=00007346
- [15] Shinae Kim, Kwon Hee-kyung, “Avatar Technology Trends to Improve User Experience in Metaverse”, The Journal of The Korean Institute of Communication Sciences 39(2), pp. 74-83, 2022. URI: <https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE11032346>
- [16] Jihye Lee, Chungmin Joo, “A Study on the Perception of Self-Identity of Metaverse Users : Focusing on Symbolic Interactionist Theory”, Korean Journal of Journalism & Communication Studies, Vol.66, No.3, pp.92-138, 2022, DOI: <https://doi.org/10.20879/kjics.2022.66.3.003>

- [17] Sonnie Youn, Juyeon Park, Kyu-Hye Lee, “Social Self Image and Avatar Image in the Virtual World: Focus on Ideal-Self Image and Actual-Self Image”, *Journal of the Korean Society of Costume*, Vol. 61, No. 9, pp. 1-14, Nov. 2011, URI: <https://koreascience.kr/article/JAKO2011110334669576.page>
- [18] Duan, Haihan, et al., “Metaverse for social good: A university campus prototype”, *Proceedings of the 29th ACM international conference on multimedia*, pp. 153-161, 2021, DOI: <https://doi.org/10.1145/3474085.3479238>
- [19] Liu, Yang, et al., “Blockchain-based identity management systems: A review”, *Journal of network and computer applications*, Vol. 166, Sept, 2020, DOI: <https://doi.org/10.1016/j.jnca.2020.102731>
- [20] Banaeian Far, Saeed, and Seyed Mojtaba Hosseini Bamakan, “NFT-based identity management in metaverses: challenges and opportunities”, *SN Applied Sciences*, 5(260), Sept. 8, 2023, DOI: <https://doi.org/10.1007/s42452-023-05487-5>
- [21] Buttar, Ahmed Mateen, et al., “Decentralized Identity Management Using Blockchain Technology: Challenges and Solutions”, *Blockchain Transformations: Navigating the Decentralized Protocols Era*, Cham: Springer Nature Switzerland, pp. 131-166, Feb. 13, 2024, DOI: https://doi.org/10.1007/978-3-031-49593-9_8
- [22] (Online) “Yonsei University Office of Academic Culture Issues SBT Certification for Educational Participation”, Dec. 12, 2022, URI: https://www.yonsei.ac.kr/sc/intro/presrel.jsp?article_no=212048&mode=view
- [23] (Online) “What are Soulbound tokens (SBT) and how Binance is integrating them on the BNB chain?”, Feb. 27, 2023, URI: <https://www.binance.com/en/feed/post/255191>
- [24] (Online) “Ethereum Improvement Proposals”, URI: <https://eips.ethereum.org/erc>
- [25] Nadini, Matthieu, et al., “Mapping the NFT revolution: market trends, trade networks, and visual features”, *Scientific reports*, Vol. 11, No. 1, 2021, DOI: <https://doi.org/10.1038/s41598-021-00053-8>
- [26] (Online) “bip-0044.mediawiki”, URI: <https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki>
- [27] Zhang, Yijian, et al., “DSBT: Research on Soulbound Token Mechanism Based on Consortium Blockchain and Decentralized Identity”, *International Conference on Computational & Experimental Engineering and Sciences*. Cham: Springer International Publishing, Feb. 13, 2023, DOI: https://doi.org/10.1007/978-3-031-42987-3_34
- [28] (Online) W3C, “Decentralized Identifiers (DIDs)”, Jul. 19, 2022, URL: <https://www.w3.org/TR/did-core/>
- [29] Gutoski, Gus, Douglas Stebila, “Hierarchical deterministic Bitcoin wallets that tolerate key leakage”, *Cryptology ePrint Archive*, 2014, URI: <https://eprint.iacr.org/2014/998>
- [30] Johnson, Don, Alfred Menezes, Scott Vanstonem, “The elliptic curve digital signature algorithm (ECDSA)”, *International journal of information secURity*, Vol. 1, pp. 36-63, 2001, DOI: <https://doi.org/10.1007/s102070100002>
- [31] Fiege, URIel, Amos Fiat, Adi Shamir, “Zero knowledge proofs of identity”, *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, 1987, DOI: <https://doi.org/10.1145/28395.28419>

저 자 소 개



김동완(DongWan Kim)

2022.02 한국성서대학교 컴퓨터소프트웨어
학과 졸업
2024.02 숭실대학교 컴퓨터학과 석사
2024.01-현재 엘에스웨어 소프트웨어연구소
연구개발본부 주임 연구원
<주관심분야> 클라우드, 인공지능, 빅데이
터, 블록체인, 분산신원인증



홍두표(Dupyo Hong)

2022.02 숭실사이버대학교 ICT공학과 졸업
2024.02 숭실대학교 컴퓨터학과 석사
2024.01-현재 엘에스웨어 소프트웨어연구소
연구개발본부 주임연구원
<주관심분야> 클라우드, 인공지능, 빅데이
터, 블록체인, 분산신원인증



노창현(ChangHyun Roh)

2017.08 순천향대학교 소프트웨어공학과 졸업
2020.02 순천향대학교 컴퓨터학과 석사
2020.05-2022.02 에스지에이퓨처스(주)
컨설팅팀 사원
2022.03-현재 가천대학교 정보보호학과
박사과정
2022.12-현재 엘에스웨어(주) 소프트웨어연
구소 연구개발본부 수석연구원
<주관심분야> 정보보호, CPS 보안, 블록체
인, DID, NFT, 저작권 기술, 메타버스, 디지
털휴먼



신동명(Dong-Myung Shin)

2003.02 대전대학교 컴퓨터공학과 박사
2001-2006 한국정보보호진흥원
응용기술팀 선임연구원
2006-2014 한국저작권위원회
저작권기술팀 팀장
2014-2016 한국스마트그리드사업단
보안인증팀 팀장
2016-현재 엘에스웨어(주) 소프트웨어연구소
연구소장/상무이사
<주관심분야> 오픈소스 라이선스, 저작권기
술, 시스템/네트워크보안, SW취약점분석·감
정, 블록체인 기술, 메타버스