Soulbound Token Applications: A Case Study in the Health Sector

ANDREA PINNA, MARIA ILARIA LUNESU, ROBERTO TONELLI, and SIMONE SANSONI,
Department of Mathematics and Computer Science, University of Cagliari, Cagliari, Italy

This article focuses on the concept of blockchain soulbound tokens, their potential applications, and their implementation in Ethereum-based blockchains. Soulbound tokens add an important piece to blockchain technology, as they could be the key to building Web3 and a trustworthy decentralized society. Issued and strictly linked to an account, representing the soul of a user, the soulbound token makes it possible to represent a property that only the user can have and that cannot be transferred, but only removed, which enhances security. To evaluate their impact on blockchain development, we first examine the concept of soulbound tokens, their potential applications, and their effective adoption. The application sectors include the creation of digital identity certificates, ownership certificates, reputational certificates, governance, and the healthcare sector. We then report and describe relevant blockchain token standards, including soulbound token standards, provided in the form of Ethereum Improvement Proposals. Finally, to study the efficacy of the implementation of soulbound tokens, we propose a case study that includes the design and development of a decentralized vaccine certification prototype based on soulbound tokens. In our system, the vaccination data produced by the health authority is fully decentralized and implemented as the issuance of soulbound tokens for the benefit of a citizen's soul account. As a result, the citizen is the only owner of the vaccination data.

CCS Concepts: • **Software and its engineering → Distributed systems organizing principles**;

Additional Key Words and Phrases: Soulbound token, blockchain, web3, health sector, self-sovereign identity, non-fungible token

ACM Reference format:
Andrea Pinna, Maria Ilaria Lunesu, Roberto Tonelli, and Simone Sansoni. 2025. Soulbound Token Applications: A Case Study in the Health Sector. *Distrib. Ledger Technol.* 4, 3, Article 25 (August 2025), 15 pages.
https://doi.org/10.1145/3674155

1 Introduction

The term "soulbound" first appeared in the context of online role-playing video games, specifically in the 2004 video game "**World of Warcraft (WoW)**." An object owned by a character with the soulbound property cannot be traded, sold, or given to another character. In 2018, Vitalik Buterin et al. [34] proposed introducing this same

This work was partially funded by the "W.E. B.E.S.T. Wine EVOO Blockchain Et Smart ContracT" PRIN 2020 financed by the Italian Ministry of University and Research (MUR), CUP: F73C22000430001, and by the "Analysis of innovative Blockchain technologies: Libra, Bitcoin and Ethereum and technological, economical and social comparison among these different blockchain technologies" project funded by Fondazione Di Sardegna, CUP: F72F20000190007. This work was partially supported by the Project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.
Authors' Contact Information: Andrea Pinna, Department of Mathematics and Computer Science, University of Cagliari, Cagliari, Italy; e-mail: pinna.andrea@unica.it; Maria Ilaria Lunesu (corresponding author), Department of Mathematics and Computer Science, University of Cagliari, Cagliari, Italy; e-mail: ilaria.lunesu@unica.it; Roberto Tonelli, Department of Mathematics and Computer Science, University of Cagliari, Cagliari, Italy; e-mail: roberto.tonelli@unica.it; Simone Sansoni, Department of Mathematics and Computer Science, University of Cagliari, Cagliari, Italy; e-mail: s.sansoni@studenti.unica.it.

This work is licensed under Creative Commons Attribution International 4.0.

© 2025 Copyright held by the owner/author(s).
ACM 2769-6480/2025/8-ART25
https://doi.org/10.1145/3674155

idea to the blockchain with the goal of satisfying the need for **Non-Fungible Tokens (NFTs)** with the property of non-transferability.

Soulbound Tokens (SBTs) represent significant progress in the blockchain landscape, aiming to permanently bind certain information to a blockchain account, which can potentially be used to specify particular features or properties of that account. For this reason, they represent the fundamental building blocks of a new Web3 trend known as the Decentralized Society.

According to the proposers' view [2, 34], SBTs will be widely adopted to create and manage Digital decentralized Identities for individuals and organizations in a decentralized society, and applications of SBTs would allow people to have more control over how their data is used.

There are many foreseeable use cases where tokens enabling the unique identification of a user are of fundamental importance [22]. This may be particularly important for applications dealing with documents containing confidential information, such as personal data, bank account data, or records about personal health [13]. SBTs can facilitate numerous applications in a decentralized society [34], including decentralized identity [5, 29], governance and **Decentralized Autonomous Organizations (DAOs)** [11], ownership proofs [3], and interaction in products such as metaverses and video games. For example, a SBT may reference a user's personal identity to establish unambiguous and legitimate ownership of an NFT representing virtual real estate or rare digital artwork in the metaverse. Similarly, a SBT can certify personal individual skills in both the virtual and real-worlds.

Recent research indicates that NFTs can be configured to meet privacy-preserving requirements characteristic of healthcare data management [29]. Furthermore, data tokenization through NFT can be a solution for data governance and management of healthcare institutions and patients [30].

In this study, we concentrate on the applications of SBTs in the health sector because they have the potential to broaden the applicability of NFTs in that realm, including the use of Digital Decentralized identities. In particular, we focus on the tokenization of health certifications, specifically vaccinations. Vaccinations typically involve both the health system and individual citizens. In recent years, we have witnessed major vaccination campaigns against COVID, and governments have explored protocols allowing for various restrictions on those who refuse vaccination. Similar restrictions apply to travel vaccinations or to workers belonging to specific categories.

In this article, we extend the preliminary study conducted in a previous work [16], where we addressed the issues related to confirming COVID vaccination and used a **Soulbound Token (SBT)** to provide the citizen with a soulbound certification of data present in the centralized database of the health authority.

The article is structured as follows: Section 2 describes some applications of SBTs, and Section 3 reports and describes the recognized standards of the tokens involved in this study along with some of their features and implications. Section 4 presents the design of the case study for decentralized vaccination certification. Section 5 describes the implementation of the case study; Section 6 presents the results and discusses findings, and Section 7 concludes the article.

2 SBT

SBTs are a novel typology of blockchain tokens that contribute to the implementation of the so-called Web3. The term Web3 refers to a group of emerging internet applications for blockchain technology, including fungible tokens (cryptocurrencies), NFTs, DAOs, and metaverses. In the context of Web3 applications, SBTs play a key role as essential components of the Decentralized Society, which offers a more decentralized online experience, allowing users to regain ownership over their data and information, monetize the content they create, and easily organize with those who share the same interests and aims [20].

The concept of SBTs originates in the context of video games in the Web2 gaming arena, particularly in games like WoW. Soulbound items, e.g., are items that a player can obtain in-game but cannot be transferred to another player. Soulbound objects are valued since they provide players with exclusive items as well as additional perks such as increased experience or bonuses when utilized in particular activities. In 2018, Vitalik Buterin et al. [34]

proposed introducing this same idea to the blockchain with the goal of satisfying the need for NFTs with the property of non-transferability.

In this section, we report the main potential uses of SBTs in different fields of application.

2.1 Identity Management Through Identity-Related SBTs

Within the domain of digital identity in the Web3 landscape, SBTs are closely associated with the notion of Identity Management [8]. More precisely, this association finds a specific expression in the concept of **Self-Sovereign Identity (SSI)**, where individuals have complete control over their own identity, allowing them to choose which aspects of themselves to reveal to others, depending on the context [21]. SSI is a core principle that gives people complete control over their digital identities and can provide more efficient access to services and applications while also improving confidence between people, corporations, and governments around the world by leveraging blockchain technology.

SBTs connect user behaviors, personal data, authentication, and permissioned sharing, allowing individuals' characteristics to be represented in both Web3 and the real-world.

The use of SBTs in digital identity management enables the implementation of three categories of services: legacy identities, pseudonymous identities, and Proofs of Personhood. The first category involves the use of SBTs to implement and enhance existing digital identity systems where a central authority issues identity certificates and the interoperability between systems is improved. In the second category, individuals can interact with each other or with services without revealing their personal details, only their pseudonym (e.g., their blockchain address). Finally, with Proof of Personhood [34], individuals use SBT properties to prove their existence and access services that provide only the tokens necessary for that service. The use case shown in Section 5 falls under this last category.

The SSI implemented through SBTs presents no entry barriers compared to other digital identity systems, as seen in the case of **Verifiable Credentials (VCs)**. It is easy to adopt and promotes interoperability. The adoption of SBTs responds to the collective need for cooperation in fostering a decentralized society. For instance, Chaffer et al. in [5] investigate a paradigm for encoding trust-based social interactions using a mechanism powered by SBTs. In Masa [19], a first mover in the context of SBT initiatives, SBTs are used to express users' qualities, credentials, and reputation in Web3. A person can establish provenance and reputation in Web3 by linking and verifying any identity or reputational data, on- or off-chain, thanks to the primitives provided by the Masa Protocol for Web3 public or private identity management. In the Masa environment, Soulbound Identity intends to become a digital passport for Web3 users—for DeFi, dapps, communities, games, and more.

2.1.1 Design Choices for Attributing SBTs to Identities. SBTs must be designed with two main issues in mind: preserving privacy and avoiding false attributions.

The privacy issue concerns the management of people's personal information. Since SBTs are intended to be attributed by a specific *community* (i.e., an administration in a decentralized society) to a specific person, it is necessary for the community to know the person's personal data for correct attribution. However, sensitive information should be kept off the blockchain to ensure privacy. Only the hash of the information should be used in the blockchain system, with zero-knowledge protocols preferred.

The "false attribution" issue refers to the need to unmask individuals or groups that pretend to belong to a community, obtaining SBTs by secretly using another wallet as the first account. Proposed solutions include limiting the issuing of SBTs only to those who are well known within a community, punishing abnormal behavior by members of the community, and encouraging other members to identify any "scammer" trying to exploit belonging to a community [34]. The token implementation could include additional features to implement a decentralized reputation system to limit the "false attribution" issue.

2.1.2 Comparison with VC. VC is a World Wide Web Consortium standard for digital certificates that aid in the identification of an individual or system [26].

The VC system relies on a "triangle of trust" between the three key parties involved. These include the Issuer, Holder, and Verifier [15]. The Issuer is the entity in charge of issuing VCs. It authenticates credentials using a digital signature issued with its private key. In a decentralized setting, the Issuer is responsible for entering a reference to the freshly generated VC into a data structure known as the "Verifiable Data Registry." The Holder is the entity that keeps and displays the VCs. An Issuer issues an VC to the Holder, who then presents it to a Verifier as needed. The Verifier validates the Verifiable Credentials provided by the Holder. The Verifier verifies the authenticity and validity of VCs using cryptography. VCs represent a key element for implementing SSI. They are personal and securely maintained by the credential holder (such as in a wallet). By keeping verified credentials private, the holder has control over the timing and context in which a credential is shared, and this may be done without involving the authority.

VCs enhance safeguards and privacy when implemented on the blockchain, offering an immutable and globally verifiable decentralized identity [14, 24]. Since they offer a dependable and standardized way to validate the information, VCs are designed for online authentication and digital identity. Deterministic methods can be used to verify the VC after it has been granted, separate and apart from the issuing organization. This indicates that the credential is independent when it is issued and doesn't need to be used again unless it is revoked.

Despite the relative similarities in functionalities and purposes, VC differ from SBTs due to several important factors. First, the architecture of an VC system is more complex. Specifically, it requires the use of a verifiable registry to prove the existence and validity of the credential. With SBTs, this existence is tied to the token's presence in the user's account. In addition, VCs involve the use of asymmetric key cryptographic systems to protect the VC document transmitted off-chain and for its verification. SSI based on SBTs does not require transmitting data outside the blockchain since the credential is linked to the user's account. Furthermore, the transaction size for creating an VC is more burdensome compared to SBTs, as it requires sending more metadata than token creation.

2.2 Further SBT Applications

2.2.1 Governance. Governance tokens represent one use case for SBTs; proof of identification may be another for non-cryptocurrency users. Within the Ethereum ecosystem, several initiatives have emerged that utilize a de facto soulbound structure. BrightID and Proof of Humanity are two examples of projects that employ a SBT model to verify that the owners of accounts are indeed actual individuals.

With the proliferation of DAOs, in 2021, the state of Wyoming recognized DAOs as independent legal entities through an amendment to the legislation regulating limited liability corporations. Consequently, numerous projects have been registered as DAOs in 2021 and 2022. Reputation DAOs utilize SBTs as reputation systems for utilities such as credit scores, proof of identification in the play-and-earn space, and proof of identity for council members across various ecosystems. By employing this technique with SBTs, blockchain may be able to bring more transparency to user on-chain activity [11]. To demonstrate that account owners are real people, token IDs are not transferable in a SBT paradigm, as on-chain assets are soulbound to each verified human.

Similar to the Ethereum case, within the Polkadot and Kusama ecosystems, and developed with the metaverse and GameFi in mind, RMRK, a reputation-based project, created a SBT called **Soulbound 2.0 (SBT2)**. It can be considered dynamic SBTs because RMRK's SBT2 will acquire qualities dependent on how long a user participates in a blockchain-based game or remains in a metaverse.

In the same governance context, accessing loans using the data of the tokens in the soul wallet [13] as a guarantee of reliability, instead of the bank credit score and internal reliability system, represents another use of SBTs, such as the use of SBTs for Know-Your-Customer processes [7].

2.2.2 Reputation. In the Web3 scenario, individuals may receive SBTs based on specific criteria that communities deem appropriate. For example, in the scientific community, publishing metrics directly affect a scientist's reputation. A specific set of tokens might represent contributions with a verifiable digital reputation. As a result,

scientists and groups of people may share a wallet, resembling a decentralized laboratory, with a sort of reputation CV [27, 32].

2.2.3 Healthcare. The use of SBTs in healthcare is the subject of our case study. The healthcare sector is one of the most relevant sectors for the application of blockchain technology, and the scientific community has studied numerous solutions to problems concerning, among others, the management of patients' health data (**Personal Health Record (PHR)**) and the management of hospital and drug supply chains. Our case study focuses on a specific aspect related to PHR, namely vaccination certifications. In our case study, patients' vaccination certificates are modeled as a set of SBTs received by the patient, of which they alone are the owner. PHRs are sensitive data, for the conservation of which we currently rely on centralized systems. This is surmountable, as described by Madine et al. [17], who propose a decentralized system for the management of PHR, respecting privacy and guaranteeing security.

In the global healthcare system, medical equipment plays a crucial role, and their exorbitant cost has led to an increase in the use of reconditioned medical devices as a sustainable alternative for hospitals and patients worldwide. In order to address the issues related to all the difficulties in repositioning reconditioned gadgets into the market (issues about quality and safety, or counterfeiting), Senay et al. show that initially, an NFT-based system has been used for managing and preserving the quality and safety of devices. Refurbished medical equipment produces a secure, transparent, and verifiable record of the process using NFTs as digital representations of medical equipment, with replacement components and certificate papers incorporated into the NFTs. By building a secure and verifiable traceability system and offering a method for ownership management and certification of medical devices throughout the refurbishing process, they employed SBT to assure the integrity and authenticity of refurbished medical equipment. The initial idea in the use of NFTs in general and SBTs specifically was to prevent counterfeiting and provide a safe and reliable manner of trading medical devices [10].

2.2.4 Ownership. The aspects related to digital identity associated with SSI have been under investigation since 2016, but recently, with the diffusion of SBTs, the focus has shifted toward the interactions between SSI and SBTs. In particular, issues related to digital inheritance have been analyzed, such as the plan that would be implemented if the testator, executors, guardians, and beneficiaries had SBTs produced by the testator and transferred to the users' wallets. This procedure might establish the presence of all users while also increasing the protection of the testator's digital assets.

Many of the new platforms are driven by distributed ledgers (i.e., blockchains), which utilize cryptocurrencies and NFTs, allowing for the creation, ownership, and monetization of a new type of decentralized digital asset. The metaverse promises to be one of the biggest employers of the future [28].

To avoid system manipulation, the synergy underlying the combination of SBTs and the metaverse enables the provision of non-repudiable evidence of ownership and protection of personal identity. In fact, SBTs become another basic element in the digital inheritance framework; protocols and networks that consider SBTs may provide privacy and security to their users as they develop their digital inheritance plans.

Furthermore, individuals have the capability to build their digital legacy through SBTs. As NFTs advance within the Web3 domain, users might have the opportunity to establish a perpetual SSI for individuals who are mindful of mortality and wish to oversee inheritance arrangements [11].

3 Blockchain Tokens Standards

A blockchain token is a digital signature embedded in blockchain data that represents or indicates a fact. For example, a token can signify a wide range of facts, from ownership of a specific amount of cryptocurrency to authorship of an artwork.

On programmable blockchains such as Ethereum, token creation is possible by implementing a smart contract. To create a token, the smart contract must include functions enabling transfer and emission (also known as

minting), as well as defining the token's primary features such as its symbol, total supply, ownership, and allowance list. Tokens are typically created using the Solidity programming language on Ethereum-like blockchains.

In the following section, we will discuss the characteristics and standards of blockchain tokens, followed by an examination of SBTs.

3.1 Fungible Token and Non-Fungible Standards

The blockchain community has established technical token standards to simplify the development of custom tokens. Standards in Ethereum are typically denoted as **Ethereum Request for Comments (ERC)** or **Ethereum Improvement Proposal (EIP)**, with the most popular token standards being ERC-20 [31] and ERC-721 [9]. Another standard, ERC-1155 [23], was conceived to implement multiple tokens of different symbols within the same smart contract. Generally, the process of token creation is referred to as "minting."

Tokens can be classified as fungible or non-fungible. The characteristics of these two types of tokens are discussed below.

A fungible token is one that can be "duplicated" in identical and interchangeable copies (hence the term "fungible"), with the common feature being the symbol. In other words, there are no characteristics of a single token that differentiate it from all others of the same symbol. Fungible tokens are assigned to blockchain accounts based on the number of tokens that the account owns. Similar to cryptocurrencies, an account can send and receive a specific amount of tokens with a particular symbol. In a sense, fungible tokens are secondary cryptocurrencies, created primarily for exchange purposes. The majority of fungible tokens in Ethereum adhere to the ERC-20 standard.

Fungible tokens are utilized for creating new cryptocurrencies without necessitating the development of a new blockchain, as well as for generating utility coins to access specific services (referred to as "utility tokens"). Additionally, fungible tokens are employed in the creation of stablecoins (cryptocurrencies pegged to fiat currencies), branded currencies, and reputation tokens for the sharing economy.

An NFT is a blockchain token crafted to be unique and distinguishable from other copies bearing the same symbol. Essentially, each individual token possesses specific distinctive elements (such as a set of attributes), setting it apart from other tokens sharing the same symbol. Consequently, these tokens are not interchangeable. Similar to fungible tokens, NFTs are assigned to blockchain accounts, and they can be transferred from one account to another. In Ethereum, the majority of NFTs are created following the ERC721 standard [9].

Applications of NFTs include supply chain traceability (where a token could represent a good in the supply chain) [1], decentralized energy markets [18], digital identity management, digital twins, collectibles (NFTs designed solely for collection purposes), artwork ownership, DRM (Digital Rights Management), and authenticity certification.

By restricting the transfer of tokens from one account to another at the implementation level, it is possible to create what are known as non-transferable tokens.

3.2 SBT Standards

SBTs are based on NFTs and on the concept of non-transferable tokens, ensuring that the carried information is unique and forever belongs to the identity (the account) owning the SBTs [12, 33]. A number of official proposals of SBT standards have been released by the Ethereum community since the original idea was published. Proposals are collected and commented in the famous *EIP* web page. Two are the SBT proposals that currently arrived at the *Standar Track*, namely ERC-5192 and ERC-5484.

The ERC-5129 standard focuses on the minimal requirement for "soulbinding" a common ERC-721 token, allowing a wallet to check for permanent non-transferability. The proposed interface adds two events that acknowledge the locking and unlocking operations and a Boolean function to query, for a given token id, the token's locking status [6].

The second standard, ERC-5485, centers around the scenario where a soulbound authorization token is issued and subsequently, the transferability features of the token are "burned." This standard outlines an interface that specifies and indicates who was authorized to burn the token at the time of issuance, whether it was the issuer, the owner, both, or neither [4].

Two other proposals are currently under review before they could become standards. The ERC-5114 called *Soulbound Badge* defines the interface of a badge token to be linked to an existing NFT token at the time of minting adding them the SBT constraints. This proposal was the first created [35].

The ERC-5516 focuses on the possibility of combining multiple SBTs, providing double signature and multi-ownership features. The proposed interface specializes the existing ERC-1155 interface for multi-token standards [25].

Two other proposals, namely ERC-5727 (Semi-Fungible SBT) and ERC-5633 (Composable Soulbound NFT, EIP-1155 Extension), are still in their early stages.

4 Design of a SBT-Based System for Vaccination Certification

In this section, we describe the design of a vaccine certification system that leverages blockchain SBTs.

The system's objective is to generate a vaccination certificate issued by the health authority and assigned to a citizen.

As previously noted, SBTs play a pivotal role in the healthcare sector. This case study serves as a prime example of the practical application of SBTs, demonstrating their ability to facilitate the public attribution of certificates without requiring personal identification. By integrating SBTs with the provision of blockchain accounts that are detached from individuals' identities, this approach ensures the independent issuance of certificates, separate from the off-chain components in use.

In the scenario we are about to describe, two actors are involved: the health authority and the citizen.

- —Citizen: who has received a vaccine and will be able to receive and view the vaccine certificates issued to him by the health authority. The citizen can always receive certificates at the designated address. However, he cannot transmit a certificate to another citizen.
- —Health authority: this could represent the local health department, issuing vaccination certificates to citizens, with the option of adding and reading vaccine and citizen data to and from the database.

More specifically, once logged in, the health authority will be able to see vaccines that can be certified for citizens. The administrator will also be able to view the list of citizens and potentially issue certificates to them. The health authority can send a certification by performing the "Issue certification" action. If the operation is successful, citizens who have obtained the certification will be able to find their certification in their soul wallet. We assume that the citizen has communicated the designed address to the health authority and that he has the private key of the corresponding account.

4.1 Development Tools

For the purposes of this work, we have utilized a set of free and open-source tools that are easily accessible from any machine. The vaccine certification system was built with a wallet, an IDE and a DBMS.

- —Wallet: It simplifies accounts management and the development of decentralized applications. We adopted Metamask, an open-source wallet that can function as a blockchain service provider by connecting the application and the blockchain network. Metamask was utilized in our system to create blockchain accounts for the issuance and management of SBTs.
- —Integrated development environment: For writing and deploying the smart contract, we used Remix, an open-source, web-based IDE designed for the implementation, compilation, deployment, and debugging of smart contracts. We used it to write the SBT smart contracts in the Solidity programming language.

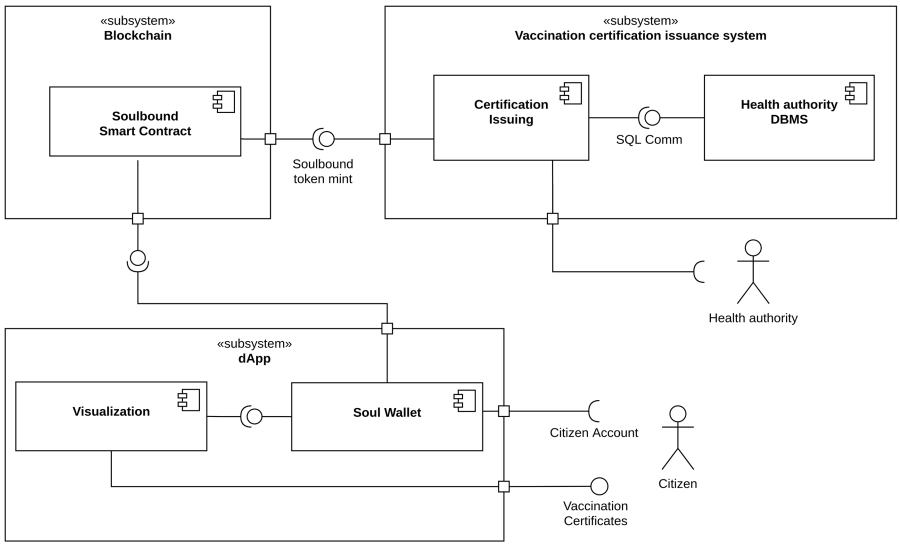

Fig. 1. Component diagram of the three main subsystems underpinning the SBT-based vaccination certification system. Upon issuing a request, the system verifies the accuracy of citizen and vaccination data, and retrieves from the database the "soul" address of the citizen and the address of the SBT corresponding to the vaccination.

—DBMS: To simulate a cloud-based architecture, we utilized the "Free SQL Database," a web-based service offering a free-to-use Database Management System for SQL-based databases. We employed this service as the database component in the "Vaccination Certification Issuance System." The utilization of a remote database enabled us to mimic real working conditions.

The logic and interfaces of both the dApp subsystem and the Vaccination Certification Issuance System subsystem were developed in JavaScript. For this purpose, we utilized WebStorm JetBrains, an integrated development environment.

The logic and the interfaces of the dApp subsystem and the Vaccination Certification Issuance System subsystem have been developed in JavaScript. For this purpose, we used WebStorm JetBrains, an integrated development environment.

To assess our system's performance under real working conditions, we deployed the smart contracts on the Ethereum Seopolia testnet. This network allows us to simulate delays and transaction costs on a public blockchain. Additionally, private and permissioned blockchain systems can be employed to simulate the system's operation with custom blockchains.

4.2 System Design

The component diagram in Figure 1 comprises three main components. The two actors interact with different parts of the system. The health authority accesses the "Vaccination Certification Issuance Subsystem" to issue a certificate. This subsystem consists of the Health Authority DBMS and the Certification Issuing component, which interacts with the smart contract for minting a new SBT. The citizen interacts with the dApp subsystem, consisting of the citizen's "soul" (i.e., its wallet) and a web-based interface.

At the core of the system is the blockchain subsystem, which includes a distinct smart contract for each vaccine in the DBMS. Specifically, each smart contract represents a specific SBT.

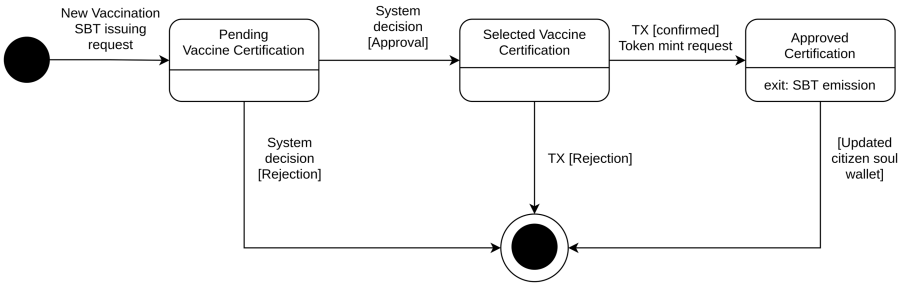

Fig. 2. UML state diagram of the SBT vaccine certification system. The health authority initiates a new certification request via a SBT, providing the citizen and vaccine identifier. The system processes the request. If the citizen exists in the database, the system retrieves the citizen's "soul" address and the smart contract address from the database, and submits the transaction to mint a new SBT. The blockchain component mints a token by recording the issue date and assigning it to the citizen. At this stage, the citizen will be able to view the token-certificate in their soul wallet.

As represented in Figure 1, the system is structured as a blockchain application, with a blockchain component comprising Ethereum smart contracts and two off-chain components. The first component resides on a remote database, while the second is an issuing component located within a web-based application, encompassing both the user interface and the user's wallet.

All three system components have been implemented to realize the system. The implementation details of each individual component are provided below.

The UML state diagram in Figure 2 The system describes various states, primarily focusing on vaccine certification. When the health authority initiates a new request for certification via a SBT, inputting the citizen and vaccine identifier, the system transitions to the "Pending vaccine certification" state. Subsequently, the system attempts to retrieve the citizen's "soul" address and the smart contract address from the database. If both are found, the system moves to the "Selected Vaccine Certification" state and initiates a transaction to mint a new SBT. Upon confirmation of the transaction, the blockchain component mints a token by recording the issue date and assigning it to the citizen, leading the system to the "Approved Certification" state. At this juncture, the citizen possesses the soulbound-token certificate in their soul wallet.

5 Implementation of System Components

The implementation was developed using Solidity for the blockchain component and Python for the dApp and Vaccination Certification Issuance System components. The database was created and populated in MySQL, with Python being utilized for this purpose as well. The code, excluding the creation and population of the database, amounts to just 186 lines of code for the backend and smart contracts. The code is available on GitHub.[1]

5.1 Blockchain Subsystem

The blockchain component of the system consists of a blockchain infrastructure and a set of smart contracts implementing SBT-based vaccination certificates.

The system is intended to function on public blockchains. For evaluating the case study implementation, we utilized the public Ethereum test blockchain, Sepolia, and the Polygon mainnet.

As previously discussed, to create a contract implementing SBTs, one can refer to the EIP standards currently in effect. Unlike the ERC-5129 standard, the vaccine SBT does not require blocking or unblocking activities, as the token is directly linked at the time of issuance. Similarly, unlike the ERC-5484 standard, the vaccine SBT does not need specific rules for authorization, as the authorization is implicit.

[1] https://github.com/AndreaPinna/sbt-health/

```
function safeMint(address to, uint _administrationDate) public onlyOwner {
      uint256 tokenId = _tokenIdCounter.current();
      tokenIdCounter.increment();
      safeMint(to, tokenId);
      administrationDate[tokenId] = _administrationDate; //timestamp
  }
```

Fig. 3. The function safeMint of the SBT smart contract.

```
function _beforeTokenTransfer(address from,  address to, uint256 tokenId) internal override virtual {
        require( from == address(0) || to == address(0), "You are not authorized to transfer the token.");
    }
function _afterTokenTransfer(address from, address to, uint256 tokenId) internal override virtual {
            if(from == address(0)){
                emit Attest(to, tokenId);
            }
            else if (to == address(0)){
                emit Revoke(to, tokenId);
            }
    }
```

Fig. 4. The _beforeTokenTransfer and _afterTokenTransfer functions of the SBT smart contract.

For implementing the soulbound vaccination certification tokens in our case study, we chose to begin with the NFC ERC-721 standard and then implement the necessary constraints to comply with the non-transferability and emission requirements. Specifically, we satisfied the non-transferability and issuance requirement by the creator (or owner) of the smart contract by overriding certain functions of the ERC-721 token implementation provided by OpenZeppelin.

In our case study, each type of vaccine listed in the health authority database entries corresponds to a smart contract for a vaccination SBT on the blockchain.

Each vaccination soulbound token inherits three OpenZeppelin contracts: ERC721.sol for NFT standards, Counters.sol for useful functions for tracking issued tokens, and Ownable.sol, which contains basic access control functions. These functions can be used to grant the contract owner (in this case, the health authority) the ability to issue SBTs.

We describe three smart contract functions created or specialized to implement the SBT. The “safeMint” function is defined to issue (and thus assign) a SBT to a citizen. This function requires the address to which the token will be soul bound, as well as the date of the vaccination administration.. This function’s code is shown in Figure 3.

The other two functions were added to implement specific constraints for transferring, attestation, and revocation that must be added to the ERC721 token. Specifically, the _beforeTokenTransfer function overrides the function in OpenZeppelin’s implementation to prevent token transfers. Additionally, the _afterTokenTransfer function overrides the original function to implement the events of attestation and revocation. The code for both functions is listed in Figure 4.

5.2 Vaccination Certification Issuance Subsystem

This subsystem comprises two components: the certification issuing component and the health data database component. It facilitates the exchange of information between these components and communication with the blockchain subsystem. The health authority interacts with this subsystem through a user interface.

For this use case, the Health Authority DBMS is implemented as a centralized remote database. This highlights that the proposed system is effectively applicable to existing systems as well.

The database consists of only two tables representing Vaccine specification data and citizen records. Both tables include an attribute *address*, enabling the system to interact properly with the smart contract and send the certificate to the respective citizen.

—Vaccines: table with attributes $id_{vaccine}$, $name$, $pharma_{company}$, and $sc_{address}$.
—Citizens: table with attributes $id_{citizen}$, $name$, $surname$, $birth_{date}$, tax_{code}, and $soul_{address}$.

We avoid creating a relationship table between the Vaccines and Citizens implementing vaccination records. That information is stored in the blockchain component as a SBT.

This option allows for the fulfillment of two requirements within the web3 paradigm. The first pertains to functionality, prioritizing user centrality by enabling the potential destruction of vaccination certificates (via burning the SBT) without necessitating formal requests. The second addresses the requirement of redundancy avoidance, as the centralized off-chain system gains access to blockchain data efficiently.

We implemented the logic of this subsystem in JavaScript. In particular, the implementation includes a *script.js* file containing the calls to the smart contract functions, and, in particular, contains a function issuing (citizenID, vaccineID, and date), which takes as parameters the address of the citizen to whom the certification is to be issued, the ID of the vaccine in the database, and the date of the vaccination. This function starts the sequence of operations represented in the state diagram in Figure 2.

Every contract interaction can only be performed by the smart contract's owner (the control is directly carried out by the smart contract code). This script makes use of the smart contract's ABI, written in the vaccineSBT.abi.js file. Note that any smart contract implementing a vaccination certification has the same ABI. The implementation also includes the JavaScript code that imports the libraries to work with the remote databases, passing all the necessary data as parameters, performing login checks, and allowing interaction with the online database to fetch data from two tables.

5.3 Citizen dApp Subsystem

We implemented this subsystem using Metamask and a JavaScript module. In particular, the implementation includes a web-based user interface that allows the user to visualize the list of his own vaccination certificates. The application does not require any type of login, as the access credentials are replaced by the accounts that the citizen manages in his soul wallet. In our implementation, the wallet is managed via Metamask. However, the application can be rewritten to allow the use of other ways of managing the wallet (e.g., via a hardware wallet).

6 Results and Discussion

The performance of the implemented system was evaluated in terms of latency time and execution cost on two public blockchain networks, namely the Ethereum mainnet and the Polygon mainnet. Polygon was originally designed to allow the Ethereum ecosystem to scale and greatly reduce costs. The overall performance of the system depends on its architecture. As described in Figure 1, when the Health authority interacts with the issuance system, the Certification issuing subsystem communicates with the DBMS and with the smart contract. In our setup, both are based on remote services: the blockchain network provides a node-based RPC service, while the DBMS system provides a TCP-IP connection.

In this configuration, a direct connection to a blockchain node was favored over utilizing a third-party provider (such as Infura or Alchemy). In this analysis, latency times on the Ethereum network were assessed using its testnet, as the smart contracts were deployed on the testnet. Multiple free RPC servers listed on the chainlist.org website were considered. Servers were selected based on their optimal reliability and privacy protection scores as provided by the website. The chosen servers are: ethereum-sepolia-rpc.publicnode.com and polygon-rpc.com. Table 1 presents the results of our experiments in terms of latency time for data retrieval operations from the remote SQL database and the two blockchains. Both blockchain RPC servers exhibit an average latency time approximately 5–6 times that of the database. Even in the worst-case scenario observed for Polygon, the times remain suitable for the anticipated read operations in the use case. It's worth noting that for write operations, the "block time" of each blockchain must be taken into account, which averages 12 seconds for Ethereum mainnet

Table 1. Latency Time Statistics of the Blockchain and DBMS Components of the System, Based on 100 Samples

Latency time (ms)	Ethereum Testnet	Polygon Mainnet	freeSQLdatabase
max	199	521	48
average	136	192	31
st dev	17	68	22

Table 2. Gas Consumption and Cost in USD of the Contract Deployment, the Issuing and the Burning of a Soulbound Vaccination Certificate in the Ethereum Main Net and in the Polygon Mainnet

Activity	Gas	Cost Ether (USD)	Cost Matic (USD)
Deploy	3,137,985	0.1443 (470.6)	0.1883 (0.179)
SBT Certificate Issuing	119,339	0.0055 (17.90)	0.0072 (0.007)
SBT Burning	32,879	0.0015 (4.93)	0.0019 (0.002)

On February 27, 2024, the costs are computed with a fee equal to 46 GWei and 60 GWei respectively, at the exchange rates of 1 ETH = 3260 USD and 1 MATIC = 0.95 USD.

and approximately 2 seconds for Polygon mainnet. Assuming that a transaction is included in the next block, confirmation is typically received after half the block time, on average.

Cost performance will be considered below. The system requires that a smart contract be deployed for each vaccine in the database. As shown in the Table 2, in the event of deployment on the Ethereum mainnet, the operation would cost approximately 0.14 Ether, that in US dollars, with a value that in February 2024 is around 3,300 USD, corresponds to approximately 470 USD. Each issue of tokens to citizens costs around USD 18, while any burning of the vaccination certificate (the citizen's only expense) costs around USD 5. The issuance of the certificate via the Ethereum public network involves significant costs. This is especially true for certificate issuance because the cost of issuance must be multiplied by the number of citizens vaccinated by the health authority. As a solution, the use of a cheaper public blockchain can result in significant cost savings. Table 2 reports the costs when using the Polygon blockchain. At the time of analysis, the execution costs appear to be more than two thousand times lower.

By forgoing the use of a public permissionless blockchain, the utilization of a permissioned blockchain can be considered. The use of a permissioned blockchain can solve the problem of operating costs, for instance, by setting the gas cost to zero. However, a permissioned blockchain dedicated to a single service would involve operating costs in terms of machines and network maintenance by the health authority and the installation of a dedicated application by the citizen, reducing the possibility for the citizen to manage his soul wallet. As a possible solution, the use of permissioned blockchains dedicated to a set of services for people can be considered. In this way, the operating costs would be distributed among the authorities participants, and the citizen could use the same soul-wallet for multiple services, including health certificates.

Although the case study is limited to vaccination certifications, the approach used can be extended to any type of medical certification. For example, a specific SBT can represent the eligibility to drive a vehicle or the certification of disability for social security purposes. The natural development of this approach can allow the creation of complete PHRs, obtained as a composition of SBTs that the individual citizen can manage as the sole owner of the data in his soul-wallet with one or more addresses.

A results of our case study concerns its implementation. It has been highlighted that with minimal development tools, it is possible to create a decentralized system for issuing SBTs. The case study shows how the citizen, i.e., the end user, gets hold of the certificates directly in his soul-wallet. The attribution of the user's address in the health authority database was not represented in the case study. This has been deliberately omitted from the case study to highlight the next steps without losing the generality of the approach. In particular, it is always the citizen who decides to associate a particular address with his identity. It should be noted that the citizen can at any time create a new account in his soul wallet and use a new address as a soul for another service. In this case, the identity-address association is registered in the company database with the aim of maintaining a "classic" approach to health data management. This highlights the fact that a real centralized system, such as that of healthcare companies, can be easily updated to include the decentralized component for issuing SBTs. However, a purely decentralized system can ensure that the identity-address association is registered on a specific smart contract, using cryptographic techniques for the preservation of sensitive data. Alternatively, by substituting the health authority with a Driver and Vehicle Licensing Agency, it is possible to implement the issuance of SBTs representing a driving license issued by the agency for the benefit of a citizen, who becomes the owner of the non-transferable digital certificate.

7 Conclusions

The concept of SBT adds an important piece to blockchain technology for they could be the key to building a trustworthy decentralized society. Issued and strictly linked to an account, the soul, of a user, the SBT makes it possible to represent a property that only the user can have and that cannot be transferred but only removed. The set of personal documents kept in each person's collection of SBTs would serve as those documents when needed. Additionally, it would describe a citizen's personal history and certify their professional, academic, and life experiences. In this article, we have examined the concept of the SBT, its potential applications, the used standards and its effective adoption. Among the application sectors are the creation of digital identity certificates, ownership certificates, reputational certificates, governance, and the healthcare sector. The proposed case study falls into this latter sector. In particular, the design and development of a decentralized vaccine certification prototype based on SBTs is discussed. In our system, the vaccination data produced by the health authority is fully decentralized and implemented as the issuance of SBTs for the benefit of a citizen's soul account. As a result, the citizen is the only owner of the vaccination data.

The article describes the components of the system and, in particular, the smart contract's characteristics that the SBT implements. The token is implemented as a specialization of the NFT ERC-721 provided by Openzeppelin to make the token compatible with the characteristics of SBTs. The used approach, focused on the definition of the elements and on minimizing the tools necessary for development, can be replicated for the study of other case studies, such as product certification, or the issuance of identity documents. Future studies may include the extension of the types of health data that can be released as SBTs up to the implementation of fully decentralized, complete PHRs with data owned only by the citizen. In real-world applications, implementing a vaccination certification using SBTs may present some barriers to adoption. The most relevant regards the need to make the system in full compliance with the laws in terms of sensible data management (e.g., with the GDPR rules).

Another barrier to adoption is stakeholders' initial reluctance to adopt new approaches or a new system, as well as final users' need to become accustomed to using and trusting such systems. Furthermore, technical adoption challenges may impede the system's real-world application. In particular, while the system described is technically simple, making it compatible with existing and in use systems may not be trivial and would entail costs for the institution. However, the benefits of using the concept of the SBT in this and similar contexts outweigh the drawbacks discussed above. Implementing a system that allows people complete freedom in using credentials and personal information is a challenging step forward in the direction of a decentralized society.

References

[1] Gavina Baralla, Andrea Pinna, Roberto Tonelli, Michele Marchesi, and Simona Ibba. 2021. Ensuring transparency and traceability of food local products: A blockchain application to a Smart Tourism Region. *Concurrency and Computation: Practice and Experience* 33, 1 (2021), e5857.

[2] Silvia Bartolucci, Giuseppe Destefanis, Marco Ortu, Nicola Uras, Michele Marchesi, and Roberto Tonelli. 2020. The butterfly "affect": Impact of development practices on cryptocurrency prices. *EPJ Data Science* 9, 1 (2020), 21.

[3] Benjamin Blau and Shardul Vikram. 2022. Entering a New Era of Decentralized Customer Experience (DCX) Web3 Unlocks the New Market Category of Decentralized Customer Experience with Unforeseen Value Across Industries. *Available at SSRN 4219848* (2022).

[4] Buzz Cai. 2022. ERC-5484: Consensual Soulbound Tokens. Retrieved from https://eips.ethereum.org/EIPS/eip-5484. Ethereum Improvement Proposals, Available online.

[5] Tomer J. Chaffer and Justin Goldston. 2022. On the existential basis of self-sovereign identity and soulbound tokens: An examination of the "self" in the age of Web3. *Journal of Strategic Innovation and Sustainability* 17, 3 (2022), 1.

[6] Tim Daubenschütz and Anders. 2022. ERC-5192: Minimal Soulbound NFTs. Retrieved from https://eips.ethereum.org/EIPS/eip-5192. Ethereum Improvement Proposals, Available online.

[7] Joaquin D. Fernandez, Tom J. Barbereau, and Orestis Papageorgiou. 2022. Agent-based model of initial token allocations: Evaluating wealth concentration in fair launches. (2022).

[8] Paul Dunphy and Fabien A. P. Petitcolas. 2018. A first look at identity management schemes on the blockchain. *IEEE Security & Privacy* 16, 4 (2018), 20–29.

[9] William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs. 2018. ERC-721: Non-Fungible Token Standard. Retrieved from https://eips.ethereum.org/EIPS/eip-721. Ethereum Improvement Proposals, Available online.

[10] Senay A. Gebreab, Khaled Salah, Raja Jayaraman, and Jamal Zemerly. 2023. Trusted traceability and certification of refurbished medical devices using dynamic composable NFTs. *IEEE Access* 11 (2023), 30373–30389.

[11] Justin Goldston, Tomer J. Chaffer, Justyna Osowska, and Charles von Goins II. 2023. Digital inheritance in Web3: A case study of soulbound tokens and the social recovery pallet within the polkadot and kusama ecosystems. arXiv:2301.11074. Retrieved from https://doi.org/10.48550/arXiv.2301.11074

[12] Felix Hildebrandt. 2022. The future of soulbound tokens and their blockchain accounts. In *Konferenzband zum Scientific Track der Blockchain Autumn School 2022*. Hochschule Mittweida, 18–24.

[13] Shrey Jain, Leon Erichsen, and Glen Weyl. 2022. A plural decentralized identity Frontier: Abstraction v. composability tradeoffs in Web3. arXiv:2208.11443. Retrieved from https://doi.org/10.48550/arXiv.2208.11443

[14] Zhiji Li. 2022. A verifiable credentials system with privacy-preserving based on blockchain. *Journal of Information Security* 13, 2 (2022), 43–65.

[15] Zoltán A. Lux, Dirk Thatmann, Sebastian Zickau, and Felix Beierle. 2020. Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. In *Proceedings of the 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS '20)*. IEEE, 71–78.

[16] M. I. Lunesu, R. Tonelli, A. Pinna, and S. Sansoni. 2023. Soulbound token for Covid-19 vaccination certification. In *2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. 243–248.

[17] Mohammad M. Madine, Ammar Ayman Battah, Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi, Sasa Pesic, and Samer Ellahham. 2020. Blockchain for giving patients control over their medical records. *IEEE Access* 8 (2020), 193102–193115.

[18] Michele Marchesi, Andrea Pinna, Francesco Pisu, and Roberto Tonelli. 2019. Crypto-trading. Rechargeable token-based smart energy market enabled by blockchain and IoT technology. In *Proceedings of the European Conference on Parallel Processing*. Springer, 166–178.

[19] Masa. 2023. Masa to Launch Soulbound Token Protocol & Developer Toolkit on Base Blockchain. Retrieved from https://medium.com/masa-finance/masa-to-launch-soulbound-token-protocol-developer-toolkit-on-base-blockchain-71331b6d4ad4

[20] Alex Murray, Dennie Kim, and Jordan Combs. 2023. The promise of a decentralized internet: What is Web3 and how can firms prepare? *Business Horizons* 66, 2 (2023), 191–202.

[21] Razieh Nokhbeh Zaeem, Kai C. Chang, Teng-Chieh Huang, David Liau, Wenting Song, Aditya Tyagi, Manah Khalil, Michael Lamison, Siddharth Pandey, and K. Suzanne Barber. 2021. Blockchain-based self-sovereign identity: Survey, requirements, use-cases, and comparative study. In *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*. 128–135.

[22] Giuseppe A. Pierro, Henrique Rocha, Stéphane Ducasse, Michele Marchesi, and Roberto Tonelli. 2022. A user-oriented model for Oracles' Gas price prediction. *Future Generation Computer Systems* 128 (2022), 142–157.

[23] Witek Radomski, Andrew Cooke, Philippe Castonguay, James Therin, Eric Binet, and Ronan Sandford. 2018. ERC-1155: Multi Token Standard. Retrieved from https://eips.ethereum.org/EIPS/eip-1155. Ethereum Improvement Proposals, Available online.

[24] Tasfia Rahman, Sumaiya I. Mouno, Arunangshu M. Raatul, Abul K. Al Azad, and Nafees Mansoor. 2023. Verifi-chain: A credentials verifier using blockchain and IPFS. In *Proceedings of the International Conference on Information, Communication and Computing Technology*. Springer, 361–371.

[25] Lucas Martín Grasso Ramos and Matias Arazi. 2022. ERC-5516: Soulbound Multi-owner Tokens [DRAFT]. Retrieved from https://eips.ethereum.org/EIPS/eip-5516. Ethereum Improvement Proposals, Available online.
[26] Johannes Sedlmeir, Reilly Smethurst, Alexander Rieger, and Gilbert Fridgen. 2021. Digital identities and verifiable credentials. *Business & Information Systems Engineering* 63, 5 (2021), 603–613.
[27] Sasha Shilina. 2023. Decentralized science (DeSci): Web3-mediated future of science. 2023. Retrieved from https://medium.com/paradigm-research/decentralized-science-desci-web3-mediated-future-of-science-2547f9a88c40.
[28] Carl H. Smith, Judith Molka-Danielsen, Jazz Rasool, Jean-Brunel Webb-Benjamin, and Kyrotech Ltd UK. 2023. The world as an interface: Exploring the ethical challenges of the emerging metaverse. In *Proceedings of the Hawaii International Conference System Sciences*. 6045–6054.
[29] Nigang Sun, Yuanyi Zhang, and Yining Liu. 2022. A privacy-preserving KYC-compliant identity scheme for accounts on all public blockchains. *Sustainability* 14, 21 (2022), 14584.
[30] Zhen L. Teo and Daniel S. W. Ting. 2023. Non-fungible tokens for the management of health data. *Nature Medicine* 29, 2 (Jan. 2023), 287–288. DOI: https://doi.org/10.1038/s41591-022-02125-2
[31] Fabian Vogelsteller and Vitalik Buterin. 2015. ERC-20: Token Standard. Retrieved from https://eips.ethereum.org/EIPS/eip-20. Ethereum Improvement Proposals, Available online.
[32] Fei-Yue Wang, Wenwen Ding, Xiao Wang, Jon Garibaldi, Siyu Teng, Rudas Imre, and Cristina Olaverri-Monreal. 2022. The DAO to DeSci: AI for free, fair, and responsibility sensitive sciences. *IEEE Intelligent Systems* 37, 2 (2022), 16–22. DOI: https://doi.org/10.1109/MIS.2022.3167070
[33] Qin Wang, Rujia Li, Qi Wang, and Shiping Chen. 2021. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv:2105.07447. Retrieved from https://doi.org/10.48550/arXiv.2105.07447
[34] E. Glen Weyl, Puja Ohlhaver, and Vitalik Buterin. 2022. Decentralized Society: Finding Web3's Soul. *Available at SSRN 4105763* (2022).
[35] Micah Zoltu. 2022. ERC-5114: Soulbound Badge [DRAFT]. Retrieved from https://eips.ethereum.org/EIPS/eip-5114. Ethereum Improvement Proposals, Available online.

Received 30 April 2023; revised 8 April 2024; accepted 23 May 2024