mathematics

MDPI

Article

Connect2NFT: A Web-Based, Blockchain Enabled NFT Application with the Aim of Reducing Fraud and Ensuring Authenticated Social, Non-Human Verified Digital Identity

Jagger Bellagarda [1,*] and Adnan M. Abu-Mahfouz [1,2]

[1] Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0028, South Africa
[2] Council for Scientific and Industrial Research (CSIR), Pretoria 0001, South Africa
* Correspondence: u15165702@tuks.co.za

Abstract: As of 2022, non-fungible tokens, or NFTs, the smart contract powered tokens that represent ownership in a specific digital asset, have become a popular investment vehicle. In 2021, NFT trading reached USD 17.6 billion and entered mainstream media with several celebrities and major companies launching tokens within the space. The rapid rise in popularity of NFTs has brought with it a number of risks and concerns, two of which will be discussed and addressed in this technical paper. Data storage of the underlying digital asset connected to an NFT is held off-chain in most cases and is therefore out of the NFT holders' control. This issue will be discussed and addressed using a theoretical workflow developed and presented for a system that converges NFTs and verifiable credentials with the aim of storing underlying NFT digital assets in a decentralized manner. The second issue focuses on the rise of NFT infringements and fraud within the overall NFT space. This will be discussed and addressed through the development of a practical application, named "Connect2NFT". The main functionality of this practical application will enable users to connect their Twitter social media accounts to the NFTs they own, thus ensuring that potential buyers or viewers of the NFT can comprehensively conclude who is the authentic owner of a specific NFT. An individual performance analysis of the proposed solution will be conducted in addition to being compared and evaluated against similar applications. Thorough development, implementation, and testing has been performed in order to establish a practical solution that can be tested and applied to current NFT use cases. The theoretical NFT storage solution is a minor but equally important contribution in comparison.

Keywords: non-fungible tokens; digital identity; verifiable credentials; blockchain technology; smart contract; social media; Twitter; IPFS

MSC: 68-04

Citation: Bellagarda, J.; Abu-Mahfouz, A.M. Connect2NFT: A Web-Based, Blockchain Enabled NFT Application with the Aim of Reducing Fraud and Ensuring Authenticated Social, Non-Human Verified Digital Identity. *Mathematics* **2022**, *10*, 3934. https://doi.org/10.3390/math10213934

Academic Editor: Ximeng Liu

Received: 3 October 2022
Accepted: 18 October 2022
Published: 23 October 2022

1. Introduction

Non-fungible tokens and verifiable credentials are two fairly new technologies. Verifiable credentials, as defined by the W3C, represent statements made by an issuer in a tamper-evident and privacy-respecting manner. It allows for the digital watermarking of claims made about data using public key cryptography and privacy-preserving techniques to prevent association. The verifiable credentials data model version 1.1 was officially published on 3 March 2022 [1]. A non-fungible token, or NFT, is a unique, non-interchangeable cryptographic token of data that is stored on a blockchain. NFTs are used to identify and prove the authenticity of a digital or physical object and its ownership [2]. The authors have identified two main issues related to NFTs, namely, the storage of underlying digital assets and fraud within the NFT space. Per an IBM report, the blockchain is not designed to store large amounts of data [3]. In the case of NFTs, the underlying digital assets they

represent, such as digital artworks, collectibles, video, and music, are just some of the data formats that require a relatively large amount of storage. Therefore, the actual NFT data object is held off-chain and is referenced in the NFT smart contract. Data can currently be stored either centrally, on a hosted server of the minter, via InterPlanetary File System (IPFS), or through decentralized storage [4].Therefore, the token component of an NFT is truly decentralized, but the media and digital metadata that the NFT points to is stored at the discretion of the user or entity who minted it. A research gap is identified here, focusing on which, if any, data storage solutions are appropriate to ensure true data ownership and if there is a new solution that can be developed to address this issue. NFT fraud has rapidly become an issue, with many scams being set up whereby users claim to be well-known artists and sell NFT infringements. Buyers are under the assumption that they are purchasing an NFT from the original artist but there is no guaranteed way to authenticate digital identity every time. Therefore, the convergence of NFTs and digital identity, through the use of social media, can be used to authenticate the identity of users creating, selling, and buying NFTs. A research gap is identified here, focusing on which, if any, identity authentication solutions are appropriate to reduce the likelihood of NFT infringements and fraud and if there is a new solution that can be developed to address this issue. In this paper, a theoretical and practical approach is taken. A theoretical workflow is presented for a system that converges NFTs, verifiable credentials, and IPFS with the aim of storing underlying NFT digital assets in a decentralized manner. Furthermore, a practical application is developed and presented that allows users to connect their Twitter account to the NFTs they own, thus ensuring that potential buyers or viewers of the NFT can comprehensively conclude who is the authentic owner of a specific NFT. The authors start by presenting a brief overview of NFTs, verifiable credentials, and digital identity and then describe the system design together with how it will address the identified requirements. This research paper will focus on contributing towards the following research questions (RQ), propositions (RP), and hypotheses (H):

- RQ1: Can verifiable credentials be used in conjunction with IPFS to theoretically enforce authenticated identity and storage of underlying NFT digital assets?
- RP1: Verifiable credentials allow for increased privacy, security, and longevity of data.

Hypothesis 1 (H1). *The mechanisms of verifiable credentials are highly correlated with the secure storage of NFT underlying digital assets.*

- RQ2: Can social media (specifically Twitter) be used in conjunction with NFTs to practically reduce the likelihood of digital asset infringements and fraud?
- RP2: IF a smart contract can be coded to leverage Twitter's social, non-human user verification process and connect that already established identity authenticity with NFTs, THEN a reduced likelihood of NFT fraud and infringements would occur.

Hypothesis 2 (H2). *The mechanism of verified social identity supported by social media platforms are highly correlated with the digital authenticity of NFT ownership.*

The following implementations will be carried out to address the above research questions:

- Design a theoretical architecture that converges NFTs ,IPFS, and verifiable credentials with the aim of storing underlying digital assets in a decentralized manner;
- Design and develop a practical web-based application that has the functionality to link NFTs to an authenticated digital identity through the use of social media (i.e., Twitter).

The rest of this research paper is structured in the following manner: Section 2 focuses on the related work and describes the background of verifiable credentials, non-fungible tokens, ERC721 smart contracts, and social media; Sections 3 and 4 explore the proposed solutions for digital identity and data storage, respectively; Section 5 compares and discusses the proposed solutions described in the previous two sections against similar solutions;

and, finally, Section 6 focuses on identifying research gaps and developing a future research direction, before drawing to a conclusion.

2. Related Work and Background

In this section, related work will be explored. Furthermore, the background of the following subsections will be described in order to establish a clear understanding of each concept:

- Verifiable Credentials
- Non-fungible Tokens
- ERC721 Smart Contract
- Social Media

2.1. Related Work

The authors of [5] present a distributed IPFS-based blockchain storage solution for healthcare patient information. The solution addresses the risk of storing sensitive patient data in a central manner. Furthermore, it allows for consistency, integrity, and availability of data to be achieved. This article highlights that secure storage and access to patient data is becoming an increasingly important aspect, but further research into this topic is required in order for blockchain technology to be mass established in the healthcare industry. Another article by the authors of [6] highlight a similar issue, focusing on using IPFS and blockchain technology to store sensitive patient data in an attempt to reduce the risk of ransomware and distributed denial of service attacks that increased during the coronavirus pandemic. However, the cost-effectiveness of the various solutions highlights a potential drawback. Finally, the security of cloud computing environments in relation to Internet-based services is explored. The authors of [7] explore various intrusion detection system (IDS) selection methods to increase the accuracy of the classifiers in detecting intrusion. It was identified that a hybrid ant-bee colony optimization (HABCO) method presented the highest accuracy compared with other methods.

The authors of [8] present a decentralized academic credential system. The blockchain powered system, called "CredeneceLedger", aims to store compact data proofs of digital academic credentials in the blockchain. Furthermore, these credentials can be easily verified by third parties, such as future employers. However, further research of blockchain technology and the impact it has in real-world use cases, such as academic certifications, is required in order for mass adoption to be achieved.

The authors of [9] present a literature review focusing on NFTs. Specifically, the issue of NFT security is presented, and they discuss the fact that NFTs can be lost if the underlying digital asset they are connected to becomes corrupted or removed from its storage location. Furthermore, digital works of value can be stolen and generated as fraudulent NFTs without the consent of the original creator. The authors of this article present several problems with NFTs that require practical solutions. This is an identified research gap that will be addressed in this research paper.

The authors of [10] present a novel blockchain-based distributed identity system called SmartDID. It aims to converge blockchain technology with self-sovereign identity in order to achieve privacy preservation in IoT devices. IoT devices are initially built as light nodes and then configured with a zero knowledge proof dual-credential model designed to protect the privacy of sensitive on-chain data and credentials. The design is Sybil-resident, continuously linked to a distributed identity, and does not rely on centralized identity providers. This is a novel system and therefore requires further development and comprehensive testing in order to establish the viability and overall long-term effect. In another article by the authors of [11], a decentralized identity management system is presented as an alternative to the W3C decentralized identity standard presented in this paper. The system presented makes use of tagging user information with their public key, thus allowing them to easily share any information with a third party by presenting their public key. Although this solution is well researched and presented in a comprehensive

manner, the use of public keys does not ensure that the holder of the public key is entitled to the information they possess. There is a need for further research into authenticated digital identity to be connected to components within the blockchain technology environment, such as NFTs, in order to ensure true data ownership and reduce the risk of fraud and infringements. These research gaps are addressed in this research paper.

The authors of [12] present a decentralized solution that uses NFTs for improving the track and trace capabilities of standard pharmaceutical serialization. Due to the nature of the pharmaceutical industry and the stricter regulations to increase the quality assurance of their processes, this solution presents potential commercial viability. However, the presentation of a use case with a prototypical application should be further developed in order to establish it in a real-world environment.

The authors of [13] present the recent NFT feature developed by social media platform Twitter. While this is not a peer reviewed research article, it is an important development in the NFT space that needs to be discussed for the purposes of this research paper. Users of the Twitter social media platform are able to connect their Ethereum digital wallet and allocate any NFTs that reside within it as their profile picture on the platform. Once an NFT is selected, the feature will authenticate that the asset standard selected is an accepted NFT and set it as the users profile picture. In order for other users to identify the profile picture as an NFT, it will appear in a hexagon shape and be assigned a small Ethereum symbol next to it. It is important to highlight the authentication mechanism of this feature and explain how it works. When a user selects an NFT to be displayed as their profile picture, the feature will check that the NFT is of an accepted standard, such as Ethereum ERC721. The feature does not have the capability to check if the NFT should belong to the holder based on other contributing factors, such as if the digital asset the NFT points towards was created by the original creator and that it is not an infringed upon piece.

The authors of [14] present a similar solution, a decentralized framework for patents as NFTs. However, the article focuses the generation of patents as NFTs specifically and does not discuss other intellectual property solutions. Furthermore, although the article presents a comprehensive layered framework, focusing on multiple imperative aspects such as decentralized authentication, decentralized verification, and storage, the solution presented is created on a conceptual and theoretical level. Therefore, it requires further practical application to be developed.

The authors of [15] present an application feature developed by Unstoppable Domains and Chainlink. Unstoppable Domains is a decentralized blockchain-based protocol for creating and hosting domain names on the Internet as NFTs in the Ethereum ERC721 standard. The feature discussed was developed together with Chainlink, a blockchain oracle platform, and allow users to connect their Twitter account to the domain name they own, thus making it easier to identify the user's public digital wallet address. The proposed solution in this paper will use the idea as a foundation for developing a similar functionality but with further utility beyond the registering of domain names.

It is important to note that there exists a need for further education in the NFT sector. The authors of [16] present a survey conducted in Croatia in 2021 with the aim of understanding the familiarity of respondents with the concepts of the blockchain and NFTs in particular. The results of the survey established that further education is required in order to increase the average individual's knowledge of NFTs. This is an important aspect to note in evaluating whether or not NFTs could achieve mass adoption in the future.

In this research paper, several research gaps noted above will be addressed. All of the articles presented above focus on using NFTs in a particular use case, such as academic credentials or patents. In addition, various articles present conceptual or theoretical frameworks. Furthermore, several articles present solutions using decentralized digital identity but for other technologies, such as IoT, and not NFTs. This research paper will present a theoretical data storage workflow and a practical digital identity linked NFT prototype that has a multitude of real-world use case implementation potential. Furthermore, both

the aspects of ensuring true data ownership and reducing NFT fraud through the use of converging digital identity and NFT technology will be presented.

2.2. Verifiable Credentials

There are three participating users in the verifiable credentials data flow, namely, the issuer, prover, and verifier [1]. In order to simplify the process, the following example is presented. The issuer, a university, for example, creates a data claim about the prover, a student who graduated with a degree, for example. The issuer will sign the data claim with their public decentralized identifier (DID) and issue it via the blockchain to the prover. The prover can then present the proof obtained from the issuer to the verifier, a potential employer, for example. The verifier will check the decentralized identifier of the issuer in order to verify the validity of the claim. Therefore, the verifier never has to confirm the authenticity of the claim directly with the issuer and can instead rely on the digital public DID signature that is attached to the claim.

2.2.1. Elements

There are twelve elements that make up a verifiable credential.

- Data claim—A piece of data representing a statement made about a subject. Example: "Bob graduated from the University of Pretoria".
- Metadata—Attributes of the data claim such as the issuer, expiry date of the credential, an illustrative image representing the credential, and a public verifiable key.
- Proof—Information about the prover that allows other parties and users to verify the validity of the data claim held, that it has not been altered in any way, and that it has not been revoked by the issuer.
- DID—A DID, or decentralized identifier, is a type of uniform resource identifier (URI—a standard identifier format for all resources on the World Wide Web) and is composed of the scheme DID, method identifier, and a unique, method-specific identifier specified by the DID method. It should be noted that DIDs are resolvable to DID documents.
- DID subjects—The subject of a DID is the entity identified by the DID. This can be a person, organization, thing, or concept. The DID subject can also be the DID controller.
- DID controllers—The controller of a DID is the entity that has the ability, as defined by the DID method, to make changes to the DID document. This ability is controlled through the ownership of a set of cryptographic keys. It should be noted that a DID might have more than one controller.
- Verifiable data registries—In order to be resolvable to DID documents, DIDs have to be recorded on an underlying network. This can be any specific technology that supports the recording and returning of DID documents, such as decentralized file systems and ledgers, databases of any kind and peer to peer networks.
- DID documents—DID documents containing information relating to a DID.
- DID methods—DID methods are the mechanisms by which a DID and the associated DID document are created, resolved, updated, and deactivated.
- DID resolvers and DID resolution—The process of DID resolution entails a DID resolver using a DID as input and produces an associated DID document.
- DID URL dereferencing—The process of DID URL dereferencing entails taking a DID URL as input and produces a resource.
- Private wallets—In order to implement verifiable credentials, manage DIDs, and store private keys, digital "wallets" are used. They come in several formats, including mobile phone applications, software, cloud storage, and hardware. Aside from the type of digital wallet used, an imperative element maintained is that it is under the ownership and control of the end user.

2.2.2. Advantages

Verifiable credentials present the following advantages:

- Privacy—The concept of selective disclosure allows the prover the ability to only reveal certain attributes of a specific data claim they hold. Regarding an identity document, for example, the prover can choose to only reveal the year of birth. Furthermore, the prover can choose who they share data claims with and can revoke the sharing of data claims at any time. The prover therefore has full control over their data. Verifiable credentials are stored on an edge or cloud wallet under the control of the prover. Therefore, no personal identification data are stored externally, be it decentralized or centralized.
- Security—Security of data is enforced by cryptography via the blockchain. Furthermore, the verifiable credential resides in the cloud or edge wallet of the prover and not centrally in the location of the issuer. Only the public DID would reside on the blockchain.
- Longevity—Verifiable credentials will never be involuntarily removed from the network, even in the case where the issuer is not operating anymore. Once a verifiable credential is created, the DID linked to it will exist on the blockchain in a decentralized manner and not be linked to any centralized server or location that can be shut down.

It is important to note that, although verifiable credentials have several advantages, there are still drawbacks. One of the major disadvantages is that the validity of the claim is one-sided. The issuer has full control to revoke a claim that has been issued at any time, thus removing all benefits to the prover as they have no direct control [17].

2.3. Non-fungible Tokens

NFTs are created through a process called "minting", often in return for an amount in cryptocurrency. NFTs are usually created in batches with a limited quantity, thus ensuring a finite supply exists. Therefore, the value of an NFT is calculated based on its scarcity. The process of minting an NFT includes the creation and execution of an underlying smart contract [2].

NFT Smart Contracts

A smart contract is best defined as a self-executing piece of code that automatically controls or stores data and actions when a pre-determined set of instructions are met [18]. NFT smart contracts contain information about the NFT such as the name of the creator, the title, and description of the NFT. In most NFTs, the underlying digital asset that the NFT points to is stored off-chain. This is due to the cost and energy consumption required to store fairly large amounts of data on the blockchain [3]. Therefore, an NFT smart contract will usually contain a URL link to the storage location of the underlying digital asset.

2.4. ERC721 Smart Contract

There are multiple smart contract standards that have been developed by various cryptocurrencies, but for the purposes of this paper, the Ethereum ERC721 open standard will be used. This standard aims to track and trace the transfer and ownership of NFT smart contracts. The ERC721 standards define several functions that are in compliance with the ERC20 standard for the purposes of enabling existing digital wallets to display token information [19]. The following describes the set of ERC20-like functions, ownership functions, and metadata functions that exist within the ERC721 standard.

2.4.1. ERC20-like Functions

- name—Defines the token name for other applications and smart contracts;
- symbol—Defines the token symbol;
- totalSupply—Defines the total number of tokens that exist on the blockchain;
- balanceOf—This function returns the number of NFTs owned by a specific wallet address.

2.4.2. Ownership Functions

- ownerOf—This function returns the owner of a specific NFT. Due to the ERC721 standard representing tokens that are unique and non-fungible, these are represented as an ID on the blockchain. Users and smart contracts on the network can use this to identify the owner of the token.
- approve—This function will approve the ability for the owner of the token to transfer it to another user or entity.
- takeOwnership—This optional function can be executed by an outside party to transfer tokens out of another user's account. Therefore, this function can be used when a user has been approved to own a specific amount of tokens and wants to transfer these tokens from another user's or entity's balance.
- transfer—This is another transfer-based function similar to the approve function that allows an owner to transfer tokens to another user or entity, just like other digital tokens or coins.
- tokenOfOwnerByIndex—This optional function allows an owner to hold more than one NFT at a time. Due to each NFT being represented by a unique ID, the smart contract stores these IDs in an array and the function allows for the retrieval of these IDs from the array.

2.4.3. Metadata Functions

- tokenMetadata—This function is an interface that allows users to identify the link to the tokens metadata.

2.4.4. Events

- Transfer—This event is triggered when ownership of an NFT is changed from one user to another. It describes which account transferred and received the token and the token ID that was transferred.
- Approve—This event is triggered when the approve function is executed. It describes which account currently owns the token, which account is approved to take ownership in the future, and the token ID that is approved to have its ownership transferred.

2.5. Social Media

Social media can be defined as a set of websites and mobile applications that allow users to engage in social networking by creating and sharing various digital content with others. Some of the major social media platforms include Twitter, Facebook, and Instagram [20].

As of January 2021, there were 4.66 billion active Internet users in the world. This translates to 59.5 percent of the global population [21]. Regarding the impact of social media use among adults, as reported by the American Psychological Association, the number of adults in the United States of America using social media has increased from 5 percent in 2005 to 70 percent in 2019 [22]. Furthermore, as of 2022, the average adult in the world spends 147 minutes a day on social media, an increase from 90 minutes per day in 2012 [21].

The authors of [23] present a focus on how social media affects identity construction. The authors suggest that social media enables individuals to achieve identity expression, exploitation, and experimentation. Another article, by the authors of [24], explores the meaning of digital identity and describes it as being the combination of (i) official forms of identification, such as IDs and passports, issued by governments and governmental agencies, (ii) identities issued by third parties in the private and public sectors, such as banks, and (iii) digital identities that individuals gather online, such as through various social media platforms. In addition, the authors of [25,26] discuss the process of verifying accounts on the Twitter social media platform. Once an account on the Twitter platform has complied with a variety of guidelines and achieved a certain level of popularity, an internal manual verification process is conducted. If successful, the Twitter account will be officially verified and awarded a blue tick animation next to the account name. This verification

allows other users on the Twitter platform to confirm the authenticity of the account and therefore reduce the level of fraud occurring. These articles present a case that digital identity created using social media platforms is an important aspect in the identity of many individuals and in the authentication of individuals by others.

3. Proposed Solution: Digital Identity

In this section, a practical application, named "Connect2NFT" is presented as a proposed solution to NFT infringements and fraud by connecting digital identity to NFTs. The following subsections are explored:

- Authentication
- NFT Linkage
- NFT Lookup Functionality
- Limitations

When an NFT is created, it is linked to a public digital wallet address. The holder of the digital wallet's private keys has access to the cryptocurrency tokens and NFTs stored within it. However, there are no identifiable attributes that describe the holder's identity apart from the sequence of letters and numbers that make up the wallet address. This anonymity has an advantage in that it ensures the privacy of the wallet holder; however, a disadvantage is that buyers of NFTs do not know if they are purchasing an authentic NFT from the true creator or an infringement copy created by a fraudulent user.

The following example best describes the issue at hand: Artist "A" is an independent animator who creates unique digital artwork pieces. Artist "A" shares these artworks in .JPEG format on their social media channels. Fraudulent User "B" notices the work of Artist "A" on their social media channel and decides to save these images to their local device (i.e., mobile phone). Fraudulent User "B" then decides to mint these images as NFTs via a third party marketplace and advertise them as the original artist, Artist "A". Buyers of these NFTs are under the assumption that they are purchasing an authentic NFT and that all funds are going to the original artist, where in this case they are not. This example highlights the need for NFTs to be linked to the true creators of the NFT and the underlying data it points to.

In this section, a practical web-based, blockchain enabled application called "Connect2NFT" will be presented with the aim of allowing users to connect their Twitter account to the NFTs they hold in their digital wallet, thus enforcing a level of authentic social, non-human verified digital identity while still maintaining a level of privacy. The application has been built with the following development stack:

- Express—A framework that runs within Node.js and allows developers to create and maintain servers;
- React—A JavaScript library used for building user interfaces;
- Node.js—An open-source, cross-platform JavaScript runtime environment;
- Passport.js—An authentication middleware for Node.js.

3.1. Authentication

In order for a user to connect their Twitter account to an NFT they hold, a dual connection to both the user's digital wallet and Twitter account will be required. The authentication layer details these steps.

3.1.1. Connect to Digital Wallet

The first step requires a user to connect to the digital wallet containing the NFTs they wish to link to their Twitter account. A user will need to install a web browser extension for the digital wallet they will be connecting to. For the purposes of this application, MetaMask, a cryptocurrency wallet and blockchain gateway application, will be used. Figure 1 displays the successful connection to a MetaMask wallet. In order to prevent malicious users from creating a link to an NFT, the developed smart contract will check if the user creating the

link owns the NFT on the blockchain. If they do not own the NFT, they will not be allowed to create a link. Figures 2 and 3 displays the successful connection to MetaMask.

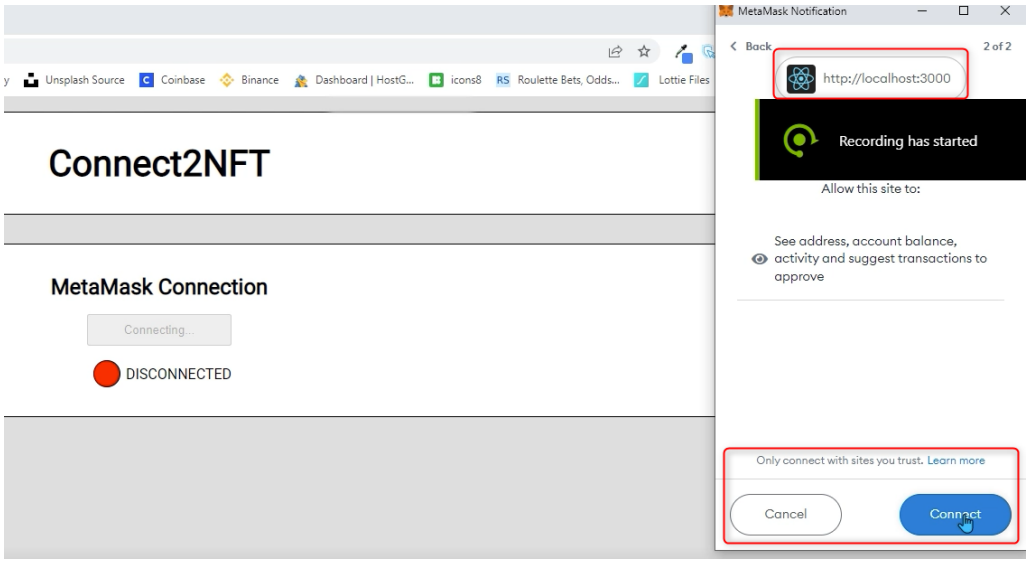

Figure 1. Connection attempt to MetaMask wallet.

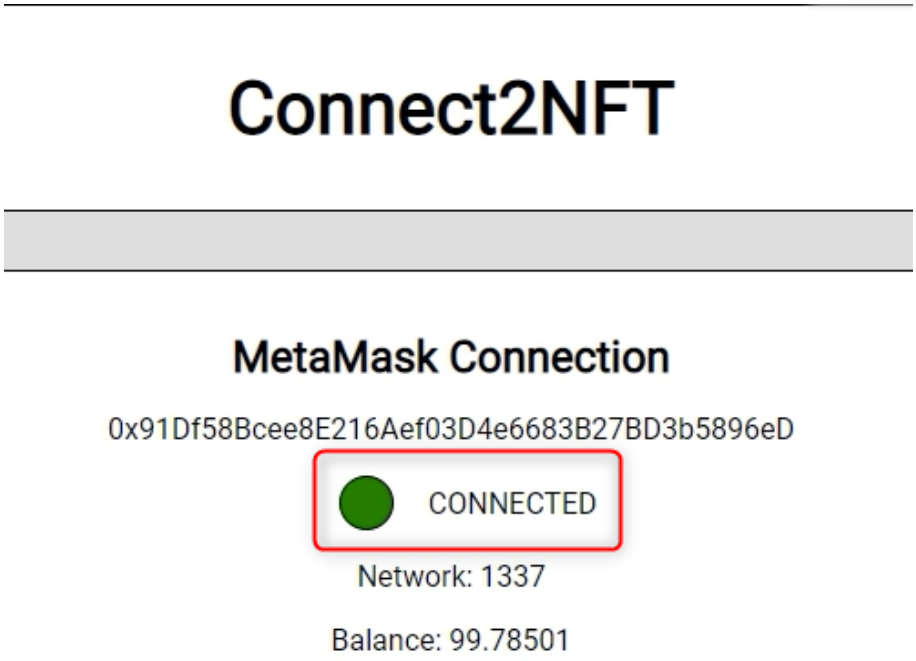

Figure 2. Successful connection to MetaMask wallet.

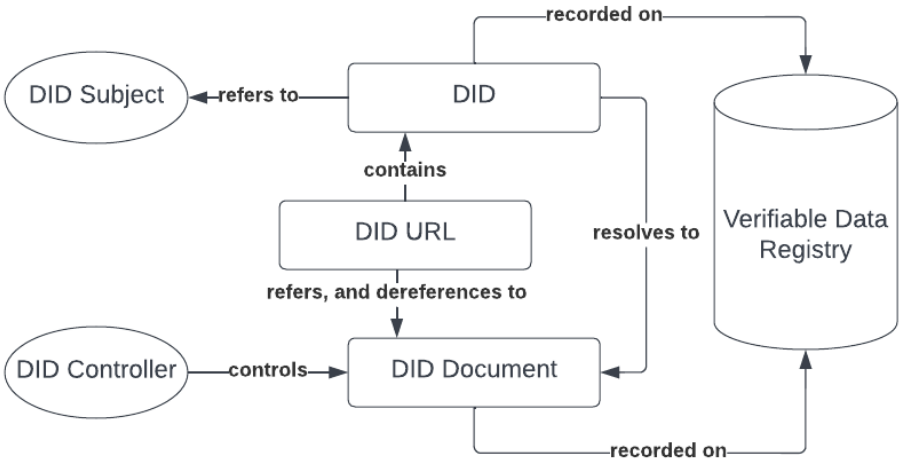

Figure 3. Decentralized identifier architecture [1].

3.1.2. Login to Twitter

The second step requires a user to login to their Twitter account using an API embedded into the application. The Twitter API is used to authenticate users on the front end. It requires users to login and provides an account ID. This ID will be used to secure the link between the user and the blockchain. Figures 4–6 display the successful login to Twitter.

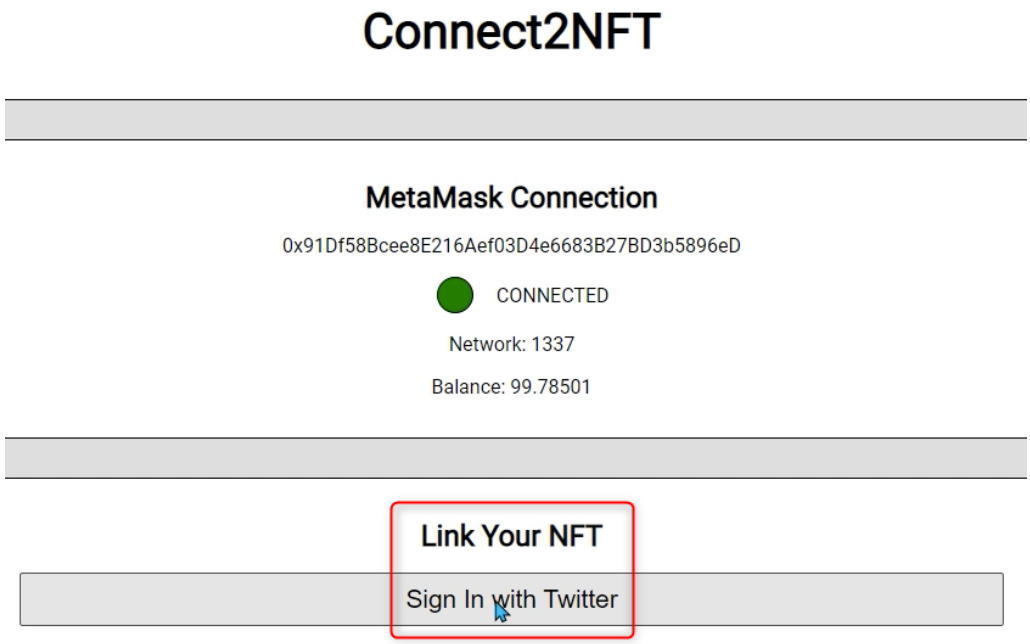

Figure 4. Login attempt to Twitter account.

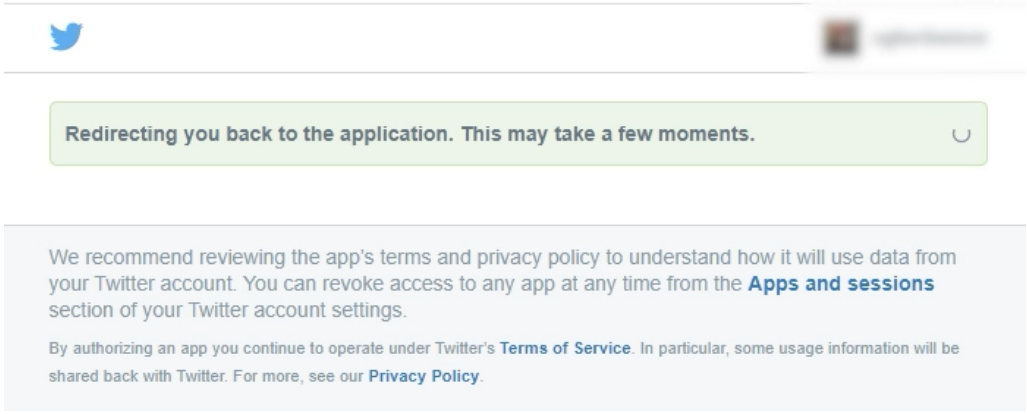

Figure 5. External Twitter connection window.

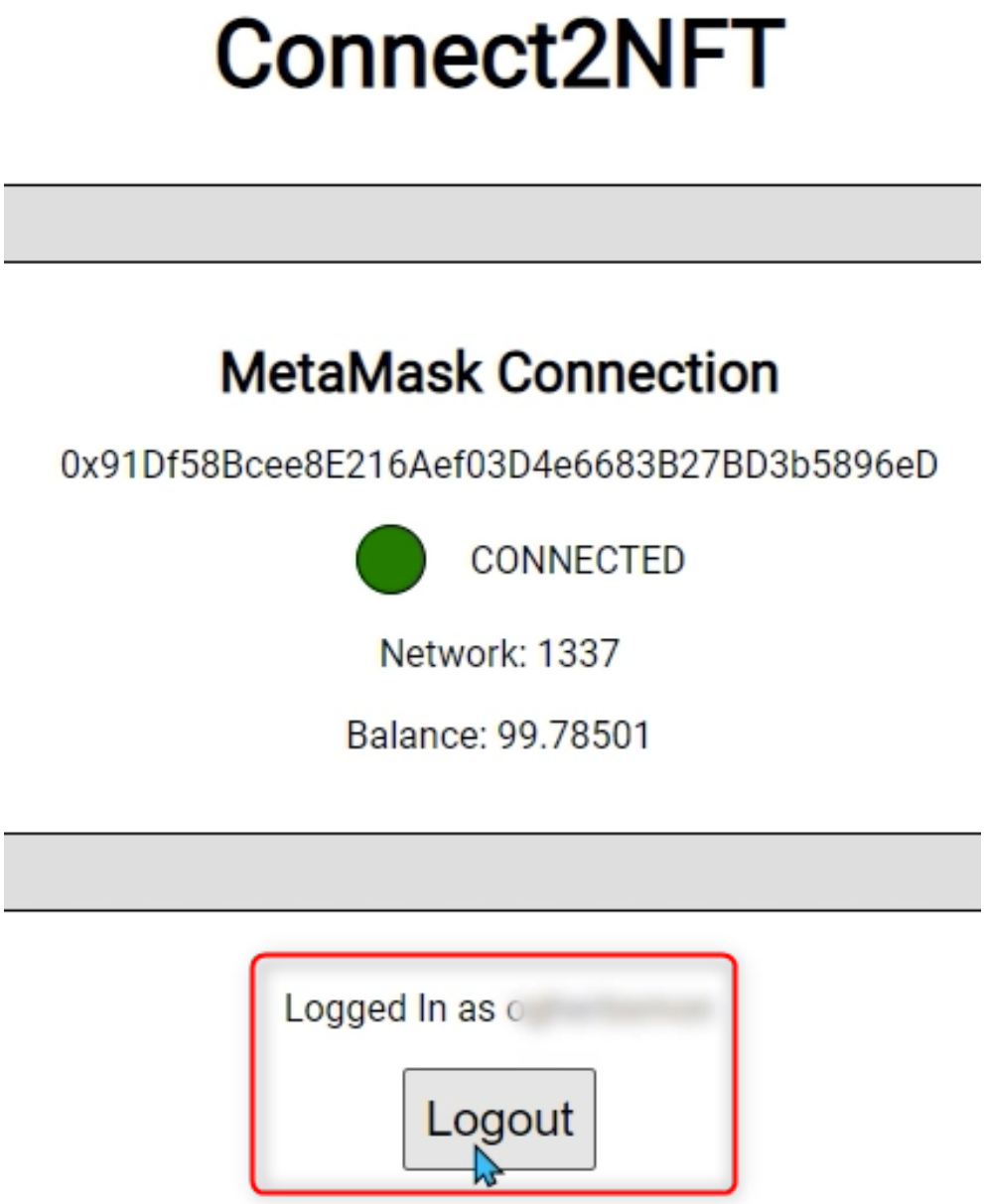

Figure 6. Successful Twitter login.

3.2. NFT Linkage

This section details the selection of a specific NFT by the user and the linking of the NFT to the user's logged-in Twitter account.

3.2.1. NFT Selection

Once the user has connected to their digital wallet, the application will display all of the NFTs held within the wallet. The user will be prompted to select the specific NFT they wish to connect to their Twitter account.

3.2.2. NFT Connection

Once a specific NFT has been selected, the user will select to link the NFT to the logged-in Twitter account on the application. Once this step has been executed, the underlying code will save the link between the token address and Twitter account to a separate smart contract. This smart contract is of an Ethereum standard and is stored entirely on the blockchain, thus ensuring a high level of decentralized security is maintained. Refer to Figure 7 for an example of an NFT being linked. As an input, the user would click on the displayed "Link" button and then confirm the blockchain transaction. Finally, the successfully linked NFT will be displayed as an output. It should be noted that a local blockchain is needed for development in order to verify if the user actually owns the NFT they are linking to. This is a very important security feature. Forking the Ethereum mainnet allows this application to access data on the mainnet that otherwise would be inaccessible without deploying on an actual mainnet blockchain.

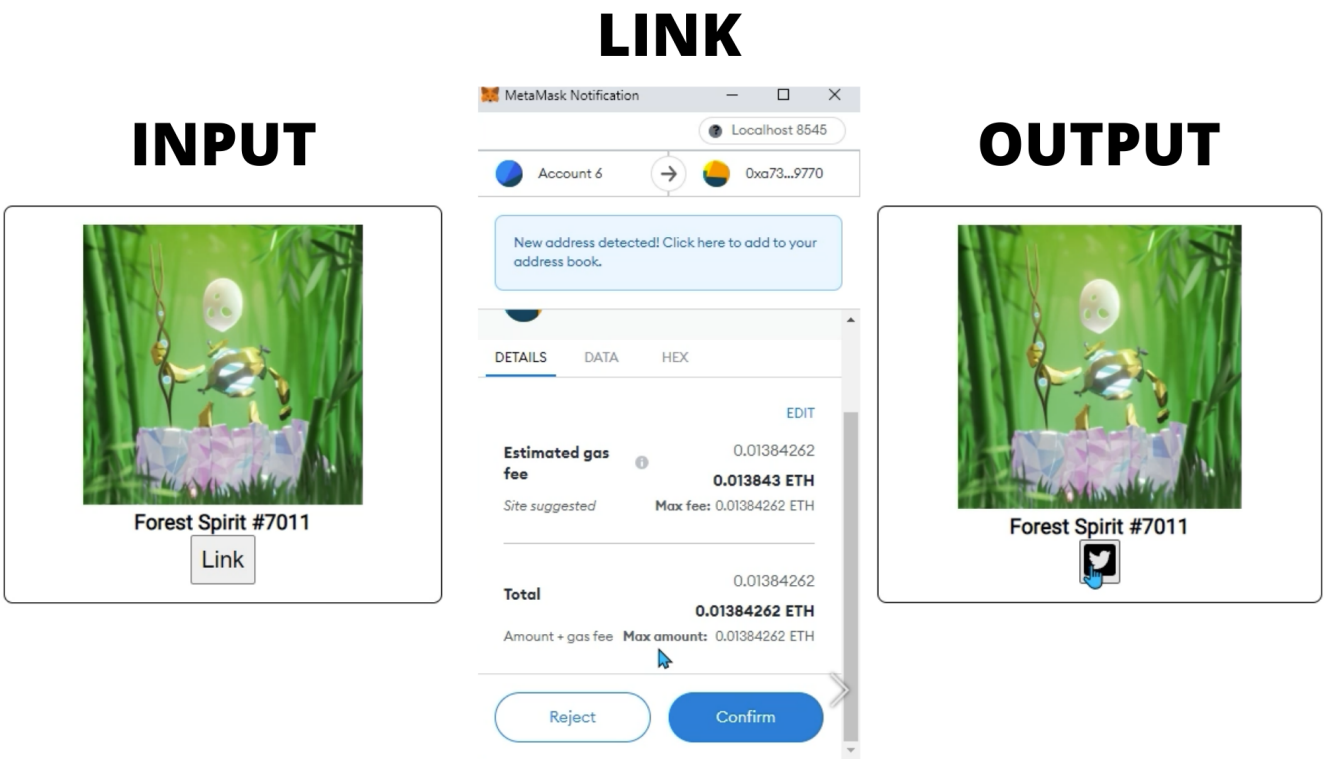

Figure 7. NFT connection to Twitter.

3.3. NFT Lookup Functionality

The underlying smart contract will save every link between an NFT token address and Twitter account. Therefore, it is possible to identify if a link exists between an NFT token address and a Twitter account through the back-end logic of the application and the blockchain. A front-end NFT explorer view will be formally developed at a future point and will allow external users to search for any token address and receive the linked Twitter

account in return. This functionality will allow any third party user to identify whether an NFT they wish to purchase has a linked Twitter account to the original authentic creator or current holder, therefore reducing the potential for NFT infringements to be sold.

3.4. Limitations

This application is limited to Ethereum and layer 2 sidechains. Furthermore, this application is currently limited to only linking NFTs built with a ERC721 token standard.

3.5. Future Development

The following details the features that have been included in the development of the current application:

- MetaMask connection and authentication;
- Twitter connection and authentication;
- Display user NFTs;
- Link NFT smart contract;
- Link verification;
- Display badge if user is the NFT creator.

The following details the features still to be developed. These will be noted as future research points:

- NFT transfers;
- NFT explorer;
- Unlink functionality;
- Front-end design and implementation;
- Mobile responsiveness;
- Smart contract testing;
- Live deployment.

4. Proposed Solution: Data Storage

In this section, a theoretical workflow is presented that details how NFTs can be stored in the holder's domain. Furthermore, other applications and architectures will be described before being compared and discussed against the proposed solution in the next section.

4.1. Verifiable Credentials

Per Figures 8 and 9, the theoretical workflow developed describes how verifiable credentials can be used to create NFTs and store the underlying digital asset of an NFT in the user's domain. This is achieved using W3C's decentralized identifiers (DID) protocol to establish and support NFT ownership and authentication in a diversified and distributed manner. The protocol will enable users to establish a cryptographically secured digital identity that uses DID features such as privacy and security to ensure they have full control over their digital assets. This will also be linked to the practical application described, allowing users to connect their Twitter social media account to the NFT they hold.

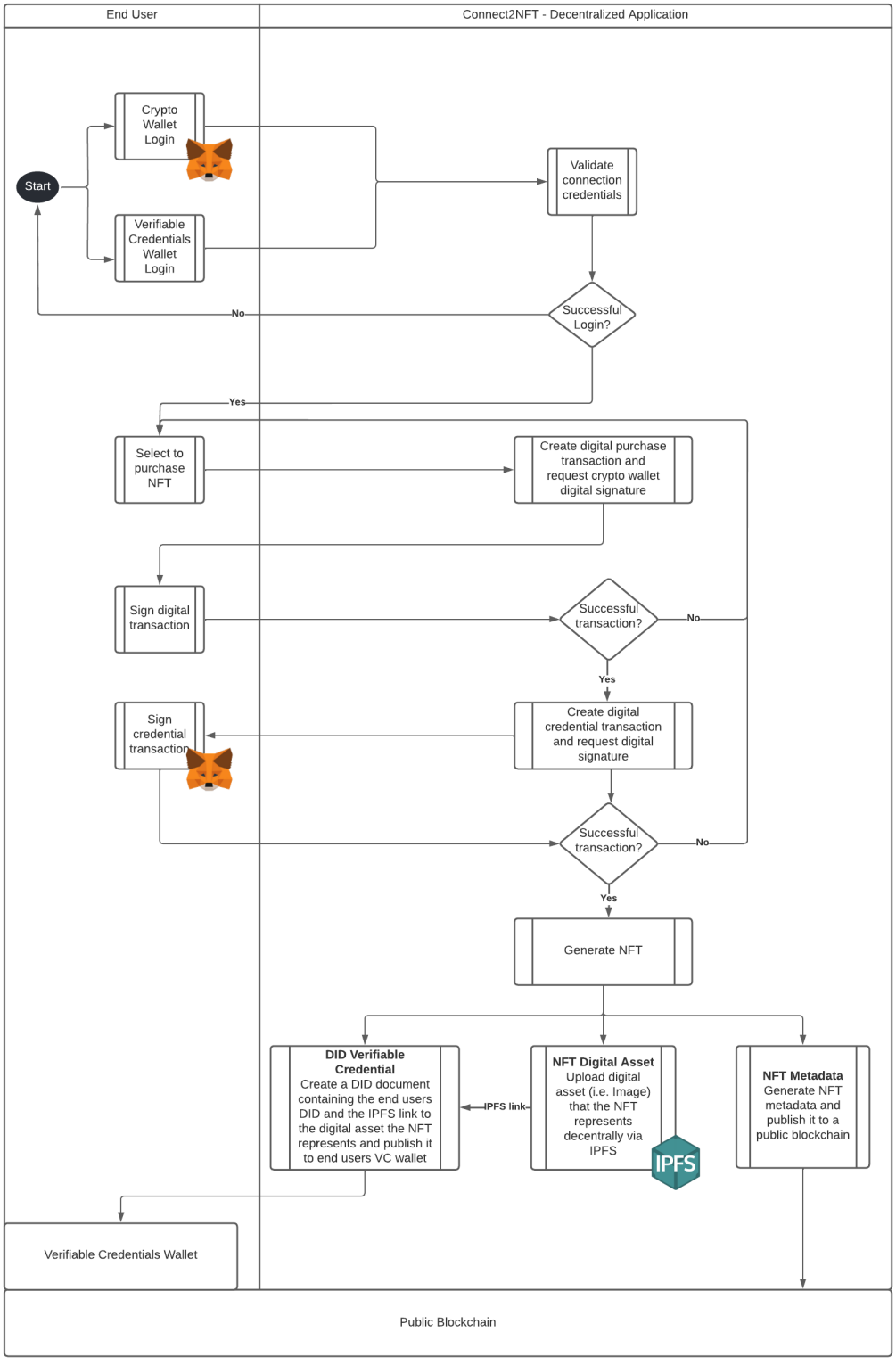

Figure 8. NFT issuing workflow.

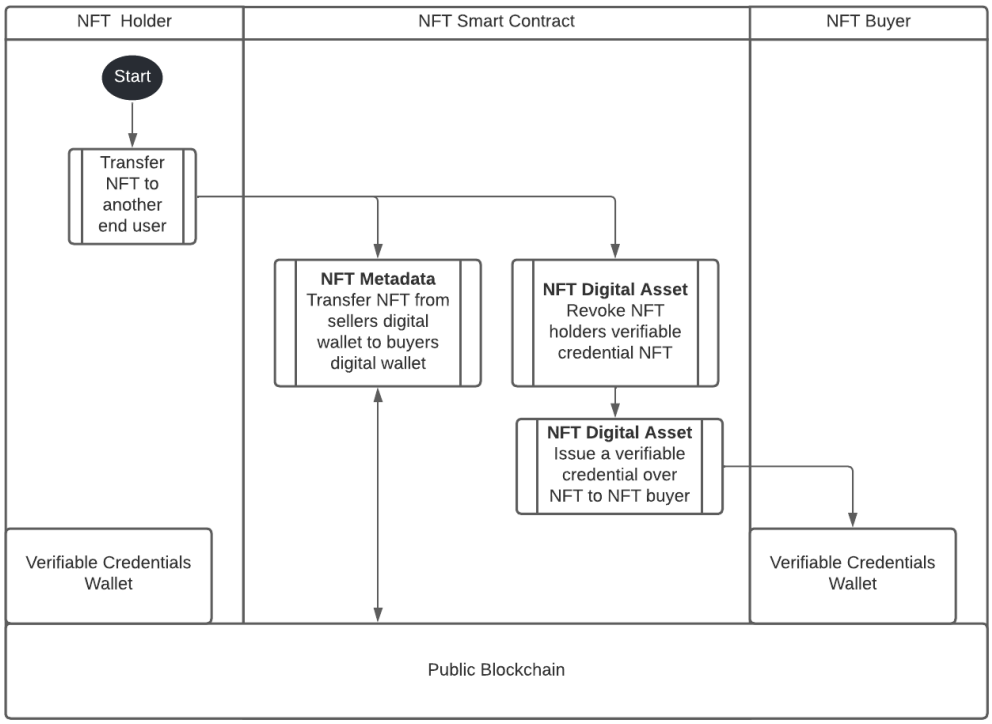

Figure 9. NFT transfer workflow.

The theoretical workflow for creating an NFT is described as follows:

- An end user will gain access to the decentralized application (DApp) through a mandatory dual login. The first login will require the end user to connect to their cryptocurrency wallet of choice. MetaMask has been used for this example. The DApp will authenticate and validate the user's credentials using the digital provider's (in this case, MetaMask) cryptographically secured login flow. The second mandatory login path requires the end user to connect to their decentralized identifier's (DID) managing platform for verifiable credentials issuing, management, and verification. The DApp will authenticate and validate the user's credentials using the digital provider's secured login flow.
- Once a successful login is obtained, the end user can choose to purchase an NFT from the DApps NFT offerings.
- Once an NFT has been selected, two digital transactions will take place that require the digital signature of both parties involved. The first transaction is the transfer of the NFT from the seller and current holder (DApp) to the buyer and future holder (end user). This transaction entails deducting the listed price of the NFT from the end user's MetaMask wallet balance. The second transaction is the creation of a digital credential transaction that will be issued by DApp, creating a verifiable credential for the end user.
- If the above two transactions are successfully processed, the NFT will then be minted on the DApp platform. This entails executing an underlying NFT smart contract and thus creating a JSON file containing the mandatory metadata, such as the NFT name, description, and the URL to the location of the digital asset that the NFT represents. However, instead of including a general URL as is usually the case, the digital asset will be automatically uploaded in a decentralized manner via IPFS, and the content identifier or CID will be added to the DID document created. A DID URL is then generated and added to the metadata of the NFT on-chain. A DID URL is a network location identifier for specific resources, such as DID subjects or DID documents.

- Once the NFT has been issued, the end user will now have two artifacts in their possession. The first is the NFT metadata that reside on-chain, including the DID URL linking to the credential issued in relation to the NFT, which is stored in the end user's verifiable credentials wallet. The second artifact is the digital asset the NFT represents, which will be stored off-chain via IPFS.

The theoretical workflow for transferring an NFT is described as follows:

- If an NFT is transferred to another user, the underlying smart contract contained within the NFT will revoke the verifiable credential connected the NFT that is held by the seller and re-issue it to the verifiable credential wallet of the buyer.

4.2. Centralized Storage

In many cases, the underlying digital asset is stored on central servers. This creates an issue for holders of NFTs who want to still own and hold their NFTs if the company or entity hosting the centralized servers stops operating and/or shuts the server down. Due to the location-based nature of https URLs, they are deemed to be centralized. An NFT that has an underlying https URL metadata file is not truly owned by the NFT holder, as they need to continuously rely on the operator of the centralized server hosting the data. An example presented is an NFT digital artwork called "Crossroad", minted on Nifty Gateway by well-known artist "Beeple". The digital artwork that is connected to the NFT token is hosted on third party marketplace Nifty Gateway's servers. Therefore, should Nifty Gateway decide to shut their servers down, the NFT token will point to a dead https URL and display an error message. The image and underlying metadata represented by the NFT token are reliant on Nifty Gateway and their servers. The holder of the token, who paid USD 6.6 million for the NFT, has no control over the storage of the NFT data [27].

4.3. IPFS

IPFS, or InterPlanetary File System, is a distributed peer-to-peer file storage and sharing file system that allows for more security over how NFTs are stored [28].

4.4. Decentralized Storage

Decentralized storage aims to store data files permanently across a decentralized network of computers [29]. Through the issuing of a cryptocurrency linked to this service, users can buy and sell decentralized storage space using these tokens. Some of the well-known decentralized data storage providers include Filecoin, Sia, and Arweave. A specific focus will be placed on Arweave and its "blockweave". This is a chain of blocks structured in such a way that each block is linked to two earlier blocks, thus forming a chain. Transactional data are then stored in a graph of these blocks. Arweave makes use of a proof-of-access consensus algorithm, thus ensuring that computers that are on the network can verify and validate transactions are accurate and that past transactions have not been altered in any manner [30].

5. Smart Contract Testing

This section will explore the smart contract that was developed for the practical digital identity solution "Connect2NFT". In order to establish that the developed smart contract is operating as intended, a series of tests were run by calling the function of the smart contract within a virtual environment against a series of data arrays. The results were then compared to the expected outputs, with any errors or bugs flagged. In order to perform this testing, Mocha was used. Mocha is a feature-rich JavaScript test framework running on Node.js and in the browser, allowing for asynchronous testing. Furthermore, Mocha tests run serially, allowing for flexible and accurate reporting, while mapping uncaught exceptions to the correct test cases [31].

The testing for this smart contract, named "TwitterLink", focused on establishing whether the functions called would successfully create an on-chain link between an NFT

and the user's Twitter account username. For the purposes of this test, the following NFT and Twitter test data were used (refer to Figure 10):

- Twitter user name: "username";
- NFT holders digital address: "signer";
- NFT token address: "contract".

Figure 10. TwitterLink test data.

The function "createLink" was executed for each of the six existing arrays:

- getLink (refer to Figure 11);
- getLinks (refer to Figure 11);
- getAllLinks (refer to Figure 12);
- getUserLinksByAddr (refer to Figure 12);
- getUserLinksByID (refer to Figure 13);
- Remove (refer to Figure 13).

Figure 11. TwitterLink contract testing.

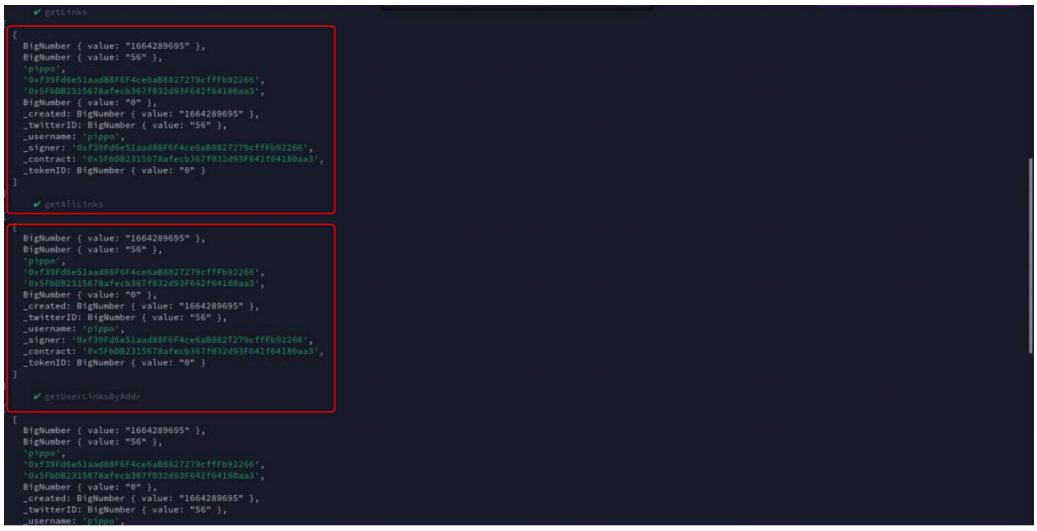

Figure 12. TwitterLink contract testing.

As a result, per Table 1, five of the six tests passed successfully. However, the test gaining information from the "Remove" array failed. The failure highlighted missing ownership requirements in the smart contracts code, thus allowing external users to potentially remove the link between an NFT and Twitter account without the approval of the original user. This failure is deemed a programming security error and will be noted as a future research point to be further developed and potentially corrected. To conclude, the smart contract has the ability to establish a link between an NFT and Twitter account on-chain but does not showcase the security requirements to restrict external users from potentially removing that link.

Figure 13. TwitterLink contract testing.

Table 1. Digital identity: smart contract testing.

Array	Pass or Fail
getLink	Pass
getLinks	Pass
getAllLinks	Pass
getUserLinksByAddr	Pass
getUserLinksByID	Pass
Remove	Fail

6. Comparison and Discussion

An exploratory qualitative case study data analysis was performed following a deductive approach. A walkthrough study of each system was conducted multiple times over a set period with the data being summarized, categorized, and commented on in an iterative manner.

- Acquire the data—Thorough research was conducted to determine which existing solutions and a developed proposed solution could potentially address the research question presented.
- Establish criteria for comparison—The following categories have been determined as the main analysis factors in determining if the solution supports the detailed hypotheses. These criteria aspects were determined through an iterative walkthrough comparison of each existing and proposed solution as part of the case study.
- Analyze the data—A walkthrough study was performed of each existing solution and of the proposed solution that was designed and/or developed.
- Conclusion—A conclusion is drawn in Section 6 for the case study comparison. Furthermore, future research points are detailed.

It should be noted that the checklist plan by the authors of [32] was followed for the design and data collection in order to ensure plan validity. Furthermore, a timeline for the comparison and discussion section is detailed below in Figure 14.

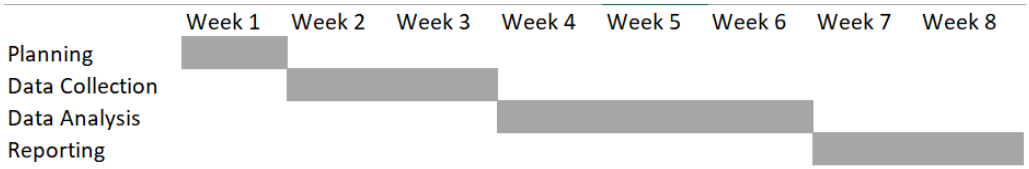

Figure 14. Comparison and discussion timeline.

6.1. Proposed Solution: Digital Identity

In an attempt to identify if the proposed system offers a new, unique contribution, a comparison to other systems will be performed based on the following nine characteristics:

6.1.1. Control

End users should be in full control of their digital identity and have the ability to attach and remove it from the NFTs they hold. This is achieved by all three NFT applications. The proposed system allows users to link their Twitter account to a selected NFT and remove the linkage at any time. Furthermore, should an NFT be sold and transferred to another user, the application will check and remove any links upon login or refresh of the old and new owner.

6.1.2. Provability

The identity of the holder should be able to be verified by trusted third parties. The proposed system allows external third party users to check for a specific NFT token address and identify whether a linked Twitter account exists. The application tool developed by Unstoppable Domains allows users to identify the linked Twitter account of a user when inputting their digital wallet address. The Twitter verification tool does not allow for any true identity verification. When a user selects an NFT to be displayed as their profile picture, the feature will check that the NFT is of an accepted standard, such as Ethereum ERC721. The feature does not have the capability to check if the NFT should belong to the holder based on other contributing factors, such as if the digital asset the NFT points towards was created by the original creator and that it is not an infringed upon piece. The proposed system differs here as only the true creator of the NFT has the ability to login to their Twitter account and create the link to an NFT. Any fraudulent users would not be able to gain access to the creator's Twitter account. It should be noted that the possibility of a original creator's Twitter account being hacked is possible and has been considered.

6.1.3. Transparency

The application providing the ability to link digital identity to NFTs should be transparent around how the application works and how it stores user data. Any algorithms used should be open source and as independent as possible from the organization developing the application. The development stack used to develop the proposed system is explained and the code is openly available to observe. This is not the case with the other NFT applications.

6.1.4. Range

This characteristic refers to whether an the application can be used across multiple types and standards of NFTs. The proposed system allows users to link any NFTs of an Ethereum ERC721 standard. In addition, the Twitter verification tool allows users to set any NFT of an Ethereum ERC721 standard as their profile picture. The NFT application tool by Unstoppable Domains only allows users to connect registered domain names as NFTs. The proposed system widens the type of NFT that can be linked to a Twitter account; however, it should be noted that only one standard of NFT can be linked currently. Further

development is required to extend this to NFTs of other cryptocurrency standards. This will be a future research point.

6.1.5. Security

A secure and private channel should be created for the user when connecting to, selecting, and verifying their NFTs with no information revealed to the application developers. All three NFT applications enable this to occur. The proposed system requires users who intend to link an NFT to their Twitter account to both connect to their digital wallet and login to their Twitter account. Both of these activities require a digital signature and/or password to be entered in order for the connection to be executed. In addition, the dual requirement further enforces the element of security regarding the application.

6.1.6. Tamper-Proofness

Any digital identity credentials shared should be tamper-proof by way of cryptography through the use of blockchain technology. All three NFT applications utilize blockchain technology, thus enforcing the use of digital identity in a tamper-proof manner.

6.1.7. Privacy

End users should be able to protect their real-world identity when authenticating an NFT. In the case of all three NFT applications, users are able to keep their real-world identity private while still achieving a level of digital identity. However, it should be noted that the proposed system enables users to connect their digital identity, through the use of their Twitter account, to the NFTs they hold in an authenticated manner. The application tool developed by Unstoppable Domains and Chainlink also allows for this. However, the Twitter NFT verification tool does not.

6.1.8. Scalability

The application should be scalable and be able to adapt to high incoming network traffic. All three applications are relatively new in comparison to each other and therefore has not been mass adopted. The Twitter verification tool is currently only available for a select group of Twitter users, those paying for the Blue subscription. The application tool developed by Unstoppable Domains and Chainlink has been released, but with the scope of use being limited to just domain names registered on the Unstoppable Domains platform, the need for scalability is limited. Apart from the fact that the proposed system was developed using a fork of the Ethereum mainnet blockchain, it is still in a test environment, and therefore it is difficult to assess scalability in real-time. However, it should be noted that due to the manner in which NFT links to Twitter accounts are stored, the ability for the application to scale is highly possible and probable.

6.1.9. Cost

The cost to issue and link digital identity to NFTs should be within a reasonable range. During testing of the proposed solution, the gas fee required to process a link between an NFT and Twitter account was 0.013843 Ethereum, estimated USD 40. Unstoppable Domains charge 3.17 Chainlink, estimated USD 50 to perform a link between a domain name and a user's Twitter account [33]. The Twitter NFT tool is only available to Blue level users, which costs USD 2.99 per month [34].

Refer to Table 2 for comparison results.

Table 2. Digital identity: application comparison.

Characteristic	Proposed Solution	Unstoppable Domains/Chainlink NFT Tool	Twitter NFT Tool
Control	Y	Y	Y
Provability	Y	Y	N
Transparency	Y	N	N
Range	Y	N	Y
Security	Y	Y	Y
Tamper-proofness	Y	Y	Y
Privacy	Y	Y	Y
Scalability	Y	Y	Y
Cost	0.0138 Ethereum (USD 40)	3.17 Chainlink (USD 50)	USD 2.99 per month

6.2. Proposed Solution: Data Storage

In an attempt to identify if the proposed system offers a new, unique contribution, a comparison to other systems will be performed based on the following eight characteristics:

6.2.1. Longevity, Control

The NFT holder should have full control over the underlying digital asset. Furthermore, the storage of the underlying digital asset should be in the NFT holder's domain. Regarding longevity, the existence of an NFT and specifically the underlying digital asset that it references must be persistent and in the domain of the NFT holder.

All solutions except for centralized storage allow for holders to be in full control of the NFT's underlying digital asset and allow for permanent persistence as it is stored in the domain of the NFT holder. In the case of centralized servers, the operator can decide to shut the server down or remove the digital asset linked to the NFT smart contract. Data files stored via IPFS are hosted by nodes in the network. In the case of NFTs, third party marketplaces can deploy a node on the IPFS network and host the storage of NFT underlying files via a private gateway [35]. The goal for the permanent storage of these data are that other nodes on the network replicate the data, thus creating multiple copies. However, based on this setup, the storage of the NFT's underlying data is specific to at least one node on the network staying online. In most cases, this is the third party marketplace where the NFT was originally minted. However, if the third party marketplace decides to shut down and their node is removed, then the underlying digital asset that an NFT references is at risk of being removed. An example of this risk is presented in reference to an NFT known as "Everydays: The First 5000 Days", which sold for USD 69 million in 2021. The NFT contract data refer directly to an IPFS hash that is accessible via a public IPFS gateway, but the underlying artwork image is stored via third party marketplace Makers' private IPFS gateway. A service known as IPFS2Arweave offers a solution where data are both pinned on IPFS and stored on Arweave [36]. The proposed solution leverages IPFS as a storage protocol but further incorporates verifiable credentials as a layer of identity authentication.

6.2.2. Provability

The identity of the holder of an NFT should be able to be verified by potential buyers. Digital wallet addresses are currently the only way of authentically identifying the holders of NFTs. Although this does offer a level of anonymity, in the cases of users wanting to link their real-world identity to NFTs and the underlying digital assets they point to, there is no solution. Therefore, there is a need for a connection to be established between NFTs and authenticated digital credentials. The incorporation of verifiable credentials with NFT issuing offers a potential solution to this problem. The ability for a digital credential to be issued alongside the creation of an NFT will allow for the validation of ownership to be established in a unique manner.

6.2.3. Transparency, Portability, Tamper-Proofness

The underlying smart contract behind an NFT should be accessible and code transparent. In addition, an NFT should be transportable by the holder. Finally, the metadata and ownership record of an NFT should be tamper-proof by way of cryptography through the use of blockchain technology.

All options allow for the transferring and storage of NFTs built on blockchain-based transparent smart contracts. The characteristics of smart contract transparency, portability, and tamper-proofness are inherent in the characteristics of NFTs themselves. However, the transparency, portability and tamper-proof nature of the storage mechanism for each solution, except for centralized storage, allows for external users to locate and view the digital asset that an NFT references.

6.2.4. Scalability

The application used to mint NFTs should be scalable and able to adapt to high incoming network traffic. In the case of the proposed solution, the protocols of NFT smart contracts and verifiable credentials are both scalable in nature and therefore support the the mass storage of NFTs and the digital assets they reference. The same can be said for all of the other storage solutions used in this comparison.

6.2.5. Cost

The cost of minting an NFT should be within a reasonable range. The service IPFS2Arweave costs USD 0.05 per megabyte to be stored for 200 years. There are multiple applications that can be used to store data on IPFS. Pinata is a well-known application where users can store files up to 1 gigabyte for free, thereafter costing USD 0.15 per gigabyte [37]. There are multiple centralized storage options available. For the purposes of this comparison, Google Drive and Dropbox were selected as options. Google Drive offers users 15 gigabyte for free, and the next plan starts at USD 1.88 per month for 100 gigabytes [38]. Dropbox offers users 2 gigabytes for free, and the next plan starts at USD 9.99 per month for 1 terabyte [39]. A DID document is a JSON-LD object stored centrally in the NFT holder's verifiable credentials wallet and does not incur a cost to the end user [40]. The metadata of the NFT will still reside on-chain and therefore be subject to gas fees. These can be minimal based on the blockchain network used. Furthermore, the proposed solution leverages IPFS as a storage protocol and therefore carries the cost of USD 0.15 per gigabyte.

Refer to Table 3 and 4 for comparison results.

Table 3. Data storage: application comparison.

Characteristic	Proposed Solution	Central	IPFS
Control	End User	Issuer	Network
Longevity	Y	N	Y
Provability	Y	N	N
Transparency	Y	Y	Y
Portability	Y	Y	Y
Tamper-proofness	Y	Y	Y
Scalability	Y	Y	Y
Cost	Minimal gas fees and USD 0.15 per GB	USD 9.99 per month per Terabyte	USD 0.15 per GB

Table 4. Data storage: application comparison.

Characteristic	Proposed Solution	Decentralized Storage (i.e., Arweave)
Control	End User	Network
Longevity	Y	Y
Provability	Y	N
Transparency	Y	Y
Portability	Y	Y
Tamper-proofness	Y	Y
Scalability	Y	Y
Cost	Minimal gas fees and USD 0.15 per GB	USD 0.05 per MB

7. Conclusions

In relation to data storage, it is noted that the use of IPFS, decentralized storage, and the proposed solution all present a valid storage method given that they allow a user to store underlying digital assets in a persistent manner at a fairly low cost. In addition, the convergence of decentralized storage and verifiable credentials highlight the characteristics of real-world identity, provability, and consent that can be achieved. However, verifiable credentials are issued and therefore controlled by third parties, thus limiting the degree of decentralization identified in this solution. Finally, it should be noted that the proposed workflow presented is theoretical and still requires further research into how it would be implemented practically. Aspects such as the concept of establishing a connection between the NFT smart contract and the credential issued containing the IPFS link to an NFT digital asset need to be further researched. Furthermore, more investigation is needed into how the revoking and re-issuing of verifiable credentials will operate when an NFT is sold or transferred between users. In relation to the practical solution developed, it is determined that the application provides a solution to authenticating NFT ownership in a private, secure, and cost competitive manner. Further implications of this implementation include a reduction in NFT fraud and an increase in NFT awareness for external users. Further research is required in order to implement and launch a commercial solution. There is a need to widen the range of NFT standards and social media platforms included on the application. Furthermore, additional specifications can be developed such as an NFT explorer in addition to allowing users to follow a creator's social media account via the application and therefore receive any updates to new NFTs that are held by the creator or linked to the creator's social media account. However, it is imperative to note that the authentication method of this proposed solution is determined to be limited to social, non-human verified identity. The proposed solution does not offer a suitable method to authenticate real-world personal identity and verifiable human identity. In addition, per the testing carried out on the smart contract developed, there is a security failure that could allow created links to be removed without the original user's authorization.

Author Contributions: Conceptualization, J.B.; methodology, J.B.; software, J.B.; validation, J.B.; formal analysis, J.B.; investigation, J.B.; resources, J.B.; data curation, J.B.; writing—original draft preparation, J.B.; writing—review and editing, J.B. and A.M.A.-M.; visualization, J.B.; supervision, A.M.A.-M.; project administration, J.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

NFT	Non-fungible Token
VC	Verifiable Credentials
IoT	Internet of Things
DID	Decentralized Identifier
IPFS	InterPlanetary File System
USD	United States Dollar
RQ	Research Question
RP	Research Proposition
H	Hypothesis

References

1. Verifiable Credentials Data Model v1.1. Available online: https://www.w3.org/TR/vc-data-model/ (accessed on 3 March 2022).
2. Wang, Q.; Li, R.; Wang, Q.; Chen, S. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. *arXiv* **2021**, arXiv:2105.07447.
3. IBM. *Why New Off-Chain Storage Is Required for Blockchains Document*, version 1.0; IBM: Armonk, NY, USA, 2018.
4. NFTs Have a Huge Persistence Problem. Available online: https://futurism.com/nfts-have-huge-persistence-problem (accessed on 3 March 2022).
5. Kumar, R.; Marchang, N.; Tripathi, R. Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain. In Proceedings of the 2020 International Conference on COMmunication Systems NETworkS (COMSNETS), Bangalore, India, 7 January 2020.
6. Kumar, S.; Bharti, A.K.; Amin, R. Decentralized Secure Storage of Medical Records Using Blockchain and IPFS: A Comparative Analysis with Future Directions. 2021. Available online: https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.162 (accessed on 3 March 2022).
7. Sangaiah, A.K.; Javadpour, A.; Ja'fari, F.; Pinto, P.; Zhang, W. A hybrid heuristics artificial intelligence feature selection for intrusion detection classifiers in cloud of things. *Clust. Comput.* **2022**. https://doi.org/10.1007/s10586-022-03629-9.
8. Arenas, R.; Fernandez, P. CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. In Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, 17 June 2018.
9. LaGuardia, A.M. NFT—Friend or Foe of Today's Art Market? 2021 Available online: https://digitalcommons.sia.edu/stu_theses/104/(accessed on 4 April 2022).
10. Yin, J.; Xiao, Y.; Pei, Q.; Ju, Y.; Liu, L.; Xiao, M.; Wu, C. SmartDID: A Novel Privacy-preserving Identity based on Blockchain for IoT. *IEEE Internet Things J.* **2022**. https://doi.org/10.1109/JIOT.2022.3145089.
11. Shekar, M.C.; Gururaj, H.L.; Flammini, F. Securing personal identity using blockchain. *Int. J. Crit. Comput.-Based Syst.* **2022**, *10*, 248–267.
12. Chiacchio, F.; D'Urso, D.; Oliveri, L.M.; Spitaleri, A.; Spampinato, C.; Giordano, D. A Non-Fungible Token Solution for the Track and Trace of Pharmaceutical Supply Chain. *Appl. Sci.* **2022**, *12*, 4019.
13. Twitter Users Can Now Add Verified NFTs as Profile Photos. Available online: https://www.bloomberg.com/news/articles/2022-01-20/twitter-users-can-now-add-verified-nfts-as-profile-photos (accessed on 4 April 2022).
14. Seyed Mojtaba Hosseini Bamakan, Nasim Nezhadsistani, Omid Bodaghi et al. A Decentralized Framework for Patents and Intellectual Property as NFT in Blockchain Networks. *Res. Sq.* **2021**, https://doi.org/10.21203/rs.3.rs-951089/v1.
15. Link Twitter to your Domain! Available online: https://unstoppabledomains.com/chainlink (accessed on 17 April 2022).
16. Posavec, A.B.; Aleksić-Maslać, K.; Tominac, M. Non-Fungible Tokens: Might Learning About Them Be Necessary? In Proceedings of the 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 23–27 May 2022.
17. Understanding the Verifiable Credentials (VCs). Available online: https://hackernoon.com/understanding-the-verifiable-credentials-vcs-it1535e9 (accessed on 5 August 2022).
18. Chirtoaca, D.; Ellul, J.; Azzopardi, G. A framework for creating deployable smart contracts for non-fungible tokens on the Ethereum blockchain. In Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Oxford, UK, 3 August 2020.
19. ERC-721 Non-Fungible Token Standard. Available online: https://ethereum.org/en/developers/docs/standards/tokens/erc-721 (accessed on 27 May 2022).
20. What Is Social Media. Available online: https://www.antonymayfield.com/2006/09/27/social-media-ebook/ (accessed on 10 April 2022).
21. Social Media—Statistics & Facts. Available online: https://www.statista.com/topics/1164/social-networks (accessed on 10 April 2022).
22. Social Media's Growing Impact on Our Lives. Available online: https://www.apa.org/members/content/social-media-research (accessed on 10 April 2022).
23. Uğur, G. The Effect of Social Media on Identity Construction. *Mediterr. J. Soc. Sci.* **2017**, *8*, 85.
24. Cheesman, M. Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. *Geopolitics* **2022**, *27*, 134–159.
25. Barsaiyan, S.; Sijoria, C. Twitter Blue Tick—A Study of its Impact on Society. *Indian J. Mark.* **2021**, *51*, 38–52.
26. Kirabo, L.; Namara, M.; Mcneese, N. The Power of the Blue Tick (): Ugandans' experiences and engagement on Twitter at the onset of the COVID-19 pandemic. In Proceedings of the 3rd African Human-Computer Interaction Conference: Inclusiveness and Empowerment, Maputo, Mozambique, 8–12 March 2021; pp. 84–93.
27. The Storage Method of NFT Artworks That You Can't Ignore. Available online: https://www.fio.one/2021/10/25/the-storage-method-of-nft-artworks-that-you-cant-ignore/ (accessed on 27 May 2022).
28. Benet, J. Ipfs-content addressed, versioned, p2p file system. *arXiv* **2014**, arXiv:1407.3561.
29. Benisi, N.Z.; Aminian, M.; Javadi, B. Blockchain-based decentralized storage networks: A survey. *J. Netw. Comput. Appl.* **2020**, *162*, 102656.
30. Arweave Wiki. Available online: https://arwiki.wiki/#/en/main (accessed on 29 April 2022).
31. Mocha. Available online: https://mochajs.org/ (accessed on 2 October 2022).

32. Brereton, P.; Kitchenham, B.A.; Budgen, D. Using a protocol template for case study planning. In Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering, Bari, Italy, 26–27 June 2008.
33. How to Buy LINK Directly from Your Wallet. Available online: https://unstoppabledomains.freshdesk.com/support/solutions/articles/48001199959-how-to-buy-link-directly-from-your-wallet (accessed on 27 May 2022).
34. Introducing Twitter Blue—Twitter's First-Ever Subscription Offering. Available online: https://help.twitter.com/en/using-twitter/twitter-blue (accessed on 2 June 2022).
35. IPFS Gateway. Available online: https://docs.ipfs.io/concepts/ipfs-gateway/#overview (accessed on 17 April 2022).
36. IPFS + Arweave. Available online: https://ipfs2arweave.com/ (accessed on 29 April 2022).
37. What's the Real Cost of IPFS? Available online: https://medium.com/pinata/whats-the-real-cost-of-ipfs-3623f274cfaa (accessed on 15 May 2022).
38. Google One Plans. Available online: https://one.google.com/about/plans (accessed on 15 May 2022).
39. Dropbox Plan Comparison. Available online: https://www.dropbox.com/individual/plans-comparison (accessed on 15 May 2022).
40. Understanding Decentralized IDs (DIDs). Available online: https://medium.com/@adam-14796/understanding-decentralized-ids-dids-839798b91809 (accessed on 15 May 2022).