Discover Data

Brief Report

NFTs enabled federated digital identity data representation and management

Memoona Javeria Anwar[1] · **Asif Qumer Gill**[1]

Received: 3 November 2024 / Accepted: 7 May 2025
Published online: 19 May 2025

Abstract
Digital identity data management is a significant challenge for businesses and individuals who wish to interact online in the increasingly digital economy, government, and society. Most recently, non-fungible tokens (NFTs) have been proposed as a solution to represent digital identities and underlying data. NFTs are stored on a blockchain based data management system and seem useful for representing digital identity data stored in independent data systems. The idea of using NFTs to represent digital identities and their associated data is promising, but it also raises significant concerns regarding data privacy and compliance. This article examines the NFT-enabled digital identity data representation and management, highlighting associated privacy risks and mitigation strategies. This study employs a qualitative desk research approach, reviewing industry reports, academic papers, and policy documents to analyze trends, technological advancements, and regulatory considerations. It concludes with recommendations for leveraging programmable privacy to address these challenges, providing valuable insights for researchers and practitioners in privacy-preserving digital identity and NFT-enabled identity management.

Keywords Digital identity · Data management · Data sharing · Non-fungible tokens · Blockchain · Privacy-by-design · Regulatory compliance

1 Introduction

Digitization of data assets and interactions is impacting all aspects of digital economy, government and society across the globe [1–3]. Digital identity is a representation of identity data such as name, address, photo, biometrics etc., which needs to be managed and shared for verifying individuals during digital interactions [4]. Digital identity data assets and their ownership are tied to the corresponding natural person, such as an individual possessing digital identity documents like a driver's license or passport. Blockchain technology has been widely explored as a means to enhance digital identity management [5] by providing decentralized, tamper-resistant, and verifiable identity records. Several blockchain-based identity solutions exist, including Self-Sovereign Identity (SSI) frameworks [6], Decentralized Identifiers [7], and Verifiable Credentials [8]. SSI enables individuals to have full control over their identity data, reducing reliance on central authorities. Decentralized Identifiers, built on blockchain networks, facilitate identity verification without exposing personal data, while verifiable credentials provide cryptographic proofs of identity attributes. Despite their advantages, these solutions face challenges such as interoperability limitations, scalability concerns, and reliance on trusted issuers for credential verification. Non-Fungible Tokens (NFTs) provide a solution for representing digital assets and their ownership, which is

✉ Asif Qumer Gill, asif.gill@uts.edu.au; Memoona Javeria Anwar, memoona.anwar@uts.edu.au | [1]University of Technology Sydney, Sydney, Australia.

stored on a blockchain or digital ledger [3, 9–11]. Unlike traditional blockchain identity solutions, NFTs provide immutable proof of ownership, transferability, and programmability, making them particularly suited for applications involving sensitive personal data [12–14] NFTs have been used in various fields for representing digital assets such as healthcare data [15], academic credentials data [8], and patents [16].

Recently there has been an increasing interest in using NFTs for representing digital identities and their data [16]. NFTs as digital identity can be used for online interactions and transactions [16, 17], however, there are also several risks that must be considered [14, 18, 19] such as the digital identity data privacy and regulatory compliance concerns [20]. Blockchain transactions are considered transparent and immutable, embedding personal identity attributes directly into NFTs could lead to unintended exposure, loss of user control, and compliance challenges with regulations such as the General Data Protection Regulation (GDPR). Therefore, it is crucial to carefully evaluate these implications and develop appropriate safeguards to mitigate any risks associated with the use of NFTs for digital identity data handling.

This paper is organised as follows. Firstly, it presents the NFTs enabled digital identity data workflow. Secondly, it presents the associated data privacy risks. Finally, it concludes with programmable privacy as a recommended solution to address these privacy risks.

2 NFT enabled digital identity data workflow

NFTs have a wide range of potential applications, particularly in settings where a digital representation of ownership is necessary [21]. NFTs are currently being considered to capture and establish ownership of digital data assets such as videos, songs, tweets, artwork, virtual land, and collectibles [21]. Despite these developments, it is important to consider the broader implications of NFTs for digital identity handling. Thus, this paper aims to investigate the following research question:

- RQ: Could NFTs be used to represent and securely verify the identity data of individuals during online interactions?

To address this research question, we employed a qualitative desk research methodology to conduct a review of industry reports, white papers, product analyses, and academic research papers. As a result of this research, we found out that NFTs can possibly be used for representing digital identity documents and related data like a digital concert ticket, which can be programmed with NFTs for unique ownership rights. NFT is stored on a blockchain data management system [7]. In this context, an NFT representing digital identity data can be referred to as a digital identity token (DIT). The DIT can be linked to identity-related data, which may be stored either on-chain (within a blockchain system) or off-chain (in traditional data management systems). The key concepts and terminology of digital identity, in the context of NFTs, are outlined as follows:

- Identity Provider (IdP)—Entities who create ("mint") NFTs and issue ("drop") them to others ("Identity Owners"). IdPs are the actual providers/creators of an NFT. As an example, a singer who mints their music as NFTs and sells it to a buyer.
- Identity Owner (IO)—Individuals or organizations who are issued with NFTs from IdPs
- Relying Party (RP)—Parties who verify NFT ownership by an IO to grant access to digital products and services.

NFTs can be used for securely verifying the identity data of individuals during online interactions. This paper proposed a detailed workflow of NFT enabled digital identity data management, which is mapped in Fig. 1 (based on [22]). The first step, in this workflow, is executed when an IdP digitizes the identity data to create an NFT i.e. DIT. The DIT is then stored (minted) onto the blockchain, where it acts as a verifiable identity credential. Depending on the sensitivity and regulatory constraints of the identity data, different storage configurations are applied:

On-chain storage: Suitable for non-personal metadata, cryptographic proofs, and verifiable identity attestations. Since blockchain transactions are immutable and transparent, only hashed or encrypted representations of identity-related data are stored on-chain to prevent unauthorized access or exposure.

Off-chain storage: Used for sensitive identity data (e.g., full name, biometric templates, government-issued ID details). This data remains in traditional data storage systems, such as secure cloud environments or decentralized storage networks (e.g., IPFS, Arweave, or private databases). The on-chain DIT links to this off-chain data via cryptographic hash pointers, ensuring

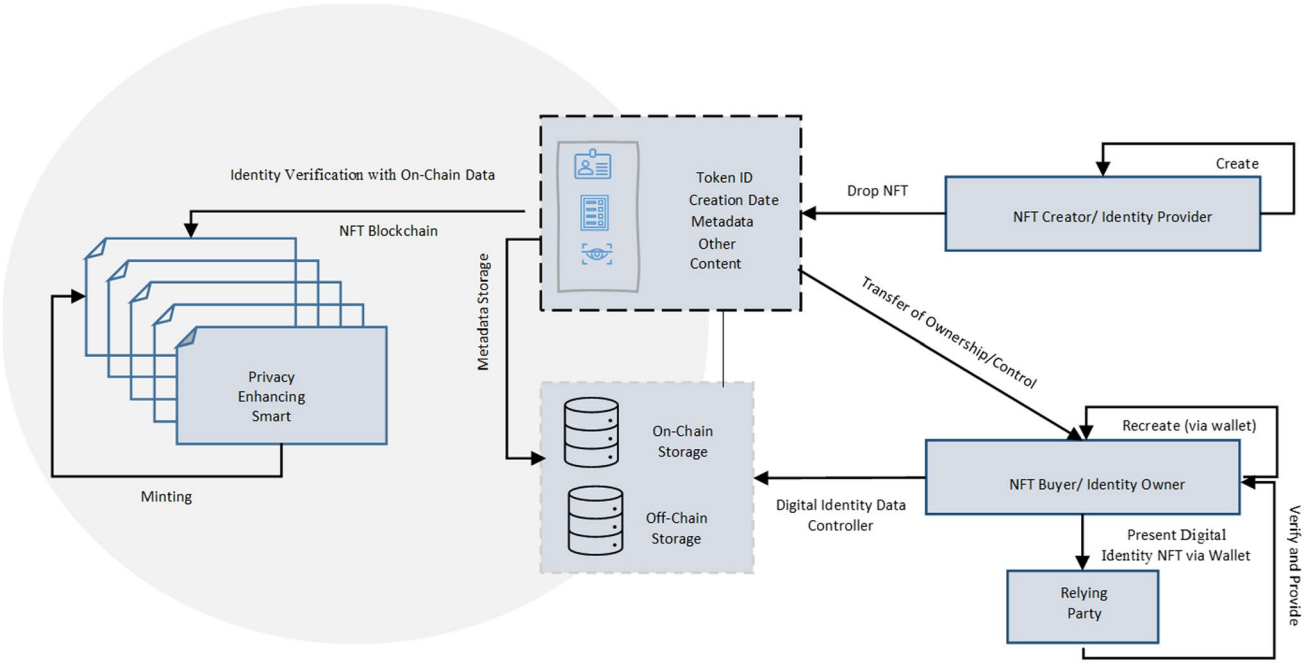

Fig. 1 NFT-enabled digital identity data workflow

data integrity without directly exposing personal information on the blockchain. In this model, the DIT and metadata are stored separately and are decoupled form the original identity data ensuring the secure verification of digital identity data. At the time of identity verification, only DIT and metadata are shared with the RP without exposing the personal identity data. The DITs are minted by IdP in such a waythat ensures the issuance of verifiable digital identity data and proof of ownership by IO. The proof of ownership accompanied by identity data is presented to RP for verification.

This entire workflow is enabled by an IdP by providing a marketplace to conduct DIT-enabled transactions. While Fig. 1 outlines one possible implementation, various configurations of digital identity workflows can be designed based on specific industry requirements, regulatory considerations, and interoperability needs.

2.1 Evaluation and practical implementation

To conduct this research, the NFT-enabled digital identity ecosystems were evaluated by comparing their technical architecture, governance models, and real-world use cases. The analysis focused on Blockchain platforms, identity use cases and On-Chain vs. Off-Chain storage approaches. From a technical perspective, NFTs rely on several core components that enable secure identity management as detailed in Table 1. These components are building blocks that come in different versions and can be assembled in various ways for NFT-enabled digital identity data management and sharing architecture and solutions. While the use of NFTs for digital identity appears promising, it also raises significant privacy concerns, which must be carefully addressed. Table 2 highlights key privacy challenges and proposed mitigation strategies to ensure compliance with data protection regulations and secure identity management in an NFT-enabled ecosystem.

3 Privacy

While the use of NFTs for representing digital identity and related data can be promising, however, it is equally important to address the associated challenges and limitations [14]. These challenges stem from the fundamental difference between ownership and identity itself. While NFTs can be used for enabling digital data ownership and de-coupling, they do not necessarily establish a person's identity and pose some privacy related challenges [14, 23–25]. Before choosing NFT for representing digital identity data, these privacy challenges and possible solutions should be considered as noted in Table 2. NFTs have four main features: they are unique, indivisible, transferable and capable of proving their scarcity. In this section we will analyze the proportionality of these characteristics with privacy risk and regulatory compliance.

Table 1 Building blocks of non-fungible tokens and data handling

Element	Description
Blockchain	Distributed data storage system or register, a.k.a. as digital ledgers. NFTs are typically built on a blockchain, such as Ethereum, which provides a decentralized and transparent way to verify ownership and transfer ownership of the digital asset pr data. Examples of such blockchain are Ethereum, Polygon, Solana, Avalanche, Polkadot, Tezos
Metadata	NFTs often include additional information about the digital asset such as the creation date, the artist's name, and even the provenance of the digital asset. This Metadata linked with the NFTs can be stored in multiple ways such as on a blockchain or Interplanetary File System (IPFS)
Smart contracts	Smart contracts are used to automate the transfer of ownership and ensure that the terms of the sale are met
Digital wallet	NFTs can be stored and transferred using a digital wallet, which is a software wallet
Token IDs	Token IDs are used to identify and differentiate NFTs within a smart contract on a blockchain. Each token ID is associated with a distinct address and metadata, enabling various parties to easily locate and interact with one another, while also taking advantage of the immutable properties of blockchains
Token standard:	NFTs are built on a token standard, such as ERC-721 or ERC-1155, which defines the specific characteristics of the token and how it can be used on a blockchain
Marketplaces:	NFTs can be bought, sold, and traded on various marketplaces, such as OpenSea, Rarible, SuperRare, etc.
Cryptographic keys	The use of cryptographic keys grants control over NFTs and enables essential functions such as encryption and authentication

3.1 NFTs enabled digital identity data handling and privacy risks

It is important to consider the potential privacy risks of NFTs and develop appropriate safeguards to mitigate these risks. This can include a combination of technological, regulatory, and legal measures. There are existing ways to improve privacy for non-fungible tokens (NFTs) such as Zero Knowledge Proof [20, 29]which enables individuals to prove ownership of an NFT without revealing any other information about the NFT or the individual's personal identity data. This ensures that personal data remains undisclosed while maintaining verifiable proof of ownership on-chain. However, while NFTs establish digital ownership, they do not inherently verify that the claiming individual is the actual owner of the digital identity, raising concerns around identity theft or misuse.

To address this, privacy-preserving smart contracts (as illustrated in Fig. 1) can be employed, integrating advanced cryptographic mechanisms such as ring signatures, zero-knowledge proofs (ZKPs) [20, 27], and threshold cryptography [30]. Ring signatures allow a transaction to be signed by a group of users, concealing the true identity of the signer, while ZKPs enable verification of identity claims without exposing sensitive details [31, 32]. Additionally, techniques like secure multi-party computation (SMPC) and homomorphic encryption can further enhance confidentiality in NFT-enabled digital identity transactions, ensuring secure authentication and privacy-preserving verifications [32].

3.2 Regulatory compliance

The inherent design of NFTs and underlying data management system (e.g. blockchain data storage system) also need to consider regulatory challenges in a broad range of areas [33, 34]. These challenges extend beyond storage of sensitive personal data and cross-border transfer of data to include privacy, compliance, security, and governance of data. Before utilizing NFTs to represent and store sensitive personal data, such as digital identities, it is crucial to conduct a comprehensive regulatory analysis and assess potential legal implications.

Key global regulations such as GDPR, EU raises concerns over data subject rights, such as the right to be forgotten (Article 17), which conflicts with blockchain's immutable nature. eIDAS Regulation (EU Regulation 910/2014) governs electronic identification and trust services, posing challenges for NFT-enabled digital identity verification within European legal frameworks. California Consumer Privacy Act (CCPA, USA) grants consumers rights over personal data deletion and control, which may be difficult to enforce in blockchain-based NFT systems. Global anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Regulations, financial compliance frameworks such as the Financial Action Task Force (FATF), Travel Rule and EU's AMLD5/6 raise concerns regarding anonymous NFT transactions and identity verification. China's Personal Information Protection Law (PIPL, 2021) imposes stringent rules on cross-border data transfers, which could impact NFT-enabled identity data stored on international blockchain nodes. US SEC and FINCEN guidelines on digital assets may classify certain NFT-enabled identity tokens as securities or financial instruments, subjecting them to financial regulations and consumer protection laws.

Table 2 Privacy challenges and solutions for NFT based digital identity

Challenge/limitation	Description	Solution
Authenticity	When a user mints or sells NFTs, a harmful attacker may take advantage of authentication vulnerabilities or take the user's private key to illegitimately transfer ownership of the NFTs	To mitigate this risk, it is important to implement robust security measures such as two-factor authentication and secure storage for private keys. Additionally, implementing smart contract-based access controls can ensure that only authorized individuals are able to mint or transfer ownership of NFTs
Data storage	As per the report by IBM [26], blockchain cannot store large amounts of data, therefore digital identity data associated with NFT needs to be stored off-chain	The Digital Identity NFT data Object (e.g., government issued ID documents, VCs, biometric) should be stored off-chain. Only reference to data can be added in smart contract
Data ownership	The token aspect of NFTs is fully decentralized, however, the digital identity data and metadata associated with the NFT is held at the responsibility of the owner or entity who created it. It remains uncertain which data storage options are suitable to guarantee genuine ownership of data. Additionally, possession of an NFT does not necessarily imply full ownership of all underlying data	Clear and transparent ownership rights for the underlying data could be established and enforced through smart contracts, so that the possession of an NFT also grants full ownership rights to the associated data
Fraud	There is no certain method to authenticate digital identity of the person presenting/selling/claiming ownership of the NFT	Adding a mandatory identity check in the smart contract before interacting with any NFT owner
Integrity	The integrity of the metadata and ownership of NFTs is protected once the transaction is confirmed, however, the data stored outside of the blockchain may be tampered with	Both the hash data as well as the original data should be sent to the NFT buyer when transferring/selling/exchanging NFTs or related assets
Recovery model	Users store NFTs on blockchain using a wallet with a seed phrase, a password needed to access the wallet and assets. If the seed phrase is lost, access to the wallet and its assets is lost, which could be an issue if Digital identity data is stored as NFTs, and the seed phrase is the only copy of the data	Using a recovery phrase that allows users to recover their wallet using a set of specified recovery words in a specific order
Non-repudiation	The transfer of an NFT from one user to another cannot be denied due to the security of the blockchain and the use of a signature scheme. However, the data linked to the NFT, such as a hash, may be manipulated by a malicious attacker or linked to their own address	A multi-signature (multi-sig) smart contract can mitigate risks of tampered hash data or attacker-controlled NFT bindings by requiring multiple cryptographic signatures for transaction approval. Implementing threshold signatures (e.g., TSS, Schnorr signatures) or multi-party computation (SMPC) ensures that no single entity can unilaterally modify NFT ownership or metadata, enhancing security and integrity
Confidentiality	The transparency of NFTs in the blockchain makes it easy for malicious actors to access and leverage the link ability of the NFT's hash and transaction	Privacy-enhancing smart contracts can strengthen confidentiality in NFT-enabled identity systems by implementing advanced cryptographic techniques. Zero-Knowledge Proofs (ZKPs) [20] [27] (e.g., zk-SNARKs, zk-STARKs) enable identity verification without revealing sensitive data. Homomorphic encryption [7] allows computations on encrypted data, ensuring confidentiality even on-chain. Secure Multi-Party Computation [27] distributes cryptographic processes across multiple entities, preventing any single party from accessing complete identity data. Stealth Addresses [28] generate unique, one-time addresses per transaction, preventing traceability. By integrating these techniques, NFT-enabled identity frameworks can enhance privacy, security, and regulatory compliance, mitigating risks associated with data exposure and transaction linkability

Table 2 (continued)

Challenge/limitation	Description	Solution
Digital footprints	NFTs can be used to track and monitor individuals' behavior and preferences. For example, an NFT could be used to represent a digital asset, such as a social media post or a website visit, which could reveal information about the individual's interests and online activity	Use Tor-like mixnets (e.g., Nym, HOPR) to anonymize NFT-related web activity. Privacy-focused NFT platforms can integrate zk-Rollups to batch transactions, hiding individual user activity from public blockchain explorers
Authorization	In the NFT system, the ability to sell is controlled by a smart contract	A formal verification on the Smart contracts can address this limitation

Discover Data (2025) 3:19 | https://doi.org/10.1007/s44248-025-00058-y

In this section, we analyze the use of NFTs for digital identity data from a regulatory perspective as detailed in Table 3.

4 Programmable contextual data privacy

This paper explored the NFT-enabled digital identity data representation and management and related privacy preserving challenges. Privacy preserving data management is a broad concept with varying interpretations across industries and users. This section focuses on programmable privacy, a framework that enables users to define, enforce, and adapt privacy controls in a structured manner. As per SSI [23], there is a potential to treat privacy as a programmable and composable right, aligning with diverse expectations and agreements. Programmable privacy empowers users and developers to personalize data privacy settings based on individual needs and business context. A proposed protocol in [30] allows users to add privacy to their NFT ownership using zkSNARK proof systems and smart contracts. Authors of [23] define "privacy as a programmable, loosely coupled bundle of rights to permission access, alter or profit from information". This means that there should be a mechanism allowing the IO to define the policy and access rights for accessing digital identity data. This can be achieved by writing privacy-preserving smart contracts, which enable IOs to track and enforce who can access what functions on a smart contract. IOs can add access control to every smart contract function, checking whether the requester has permission to call the function. Authorized requesters (RPs) can be defined as a list of account addresses. At runtime, the transaction sender's (RP's) address is checked against the list of authorized addresses. If there is a match, the rest of the smart contract logic is executed. Otherwise, the function does not execute further. This mechanism ensures that only authorized participants and smart contracts can successfully call corresponding functions. The authorization is implemented in smart contracts running on blockchain, leveraging the properties provided by blockchain.

Furthermore, access-related conditions can be enforced through policies embedded in smart contracts. These policies can be used to control access to the data stored along with the NFT, for example, by setting expiration dates for access. Smart contracts can be designed to enforce time-bound sharing, allowing Identity Owners to specify a subset of data to share, specify who can access the data, and control the duration of access by setting an expiration policy.

To advance this research, future implementations should focus on developing a prototype smart contract framework that integrates programmable privacy functions. A decentralized storage, such as a non-custodial identity wallet, can be used to hold an individual's digital identity data. The prototyping can include designing and testing smart contracts using Solidity, deploying the prototype on Ethereum or a Layer-2 blockchain to assess transaction costs, and evaluating execution performance under different privacy configurations. This could be in the form of an app or browser extension wallet that allows users to create their decentralized identity and manage third-party service

Table 3 Regulatory challenges for NFT based digital identity

Challenge/limitation	Description
Lack of interoperability	NFT enabled digital identity can lead to a lack of interoperability between different platforms, as different platforms may use different standards for creating and storing NFTs. This can make it difficult for individuals to use their digital identity data across different platforms and services
Limited scalability	NFTs are stored on a blockchain, which can have limited scalability. This means that as the number of NFTs and the number of transactions involving NFTs increases, the blockchain may become congested and experience sever performance issues. This can make it difficult for individuals to access and use their digital identity and related data in a timely manner
Privacy concerns	It can raise privacy concerns, as the ownership and transaction history of an NFT that can be publicly viewed. This can reveal sensitive identify data about the individual, such as their name, address, and other personal details
Lack of regulatory oversight	NFTs are relatively new technology, and there is currently a lack of regulatory oversight in place to protect NFT-enabled individuals' digital identities. This can make it difficult for individuals to seek legal recourse if their digital identity is compromised or misused
Security risk	As NFTs rely on blockchain data management system, they are vulnerable to hacking and other forms of cyber-attacks. This can lead to loss or theft of digital identities, or the malicious use of digital identities
Anonymous transactions	NFTs can also be used to facilitate anonymous transactions, which can be problematic in situations where the identity of the parties involved needs to be known, such as in anti-money laundering or counter-terrorism financing regulations

providers' access to it. With this design, users are the sole owners of their respective public and private cryptographic keys. To evaluate effectiveness, future research should measure access control efficiency via permission verification times, scalability through transaction throughput under varying loads, and privacy assurance via security audits and zkSNARK verification.

In addition to technical measures, it is also crucial to amend current privacy laws or introduce new laws specifically designed to address the unique complexities associated with blockchain and the use of NFTs to represent and store digital identity data. These laws should address issues such as data ownership as it relates to privacy, determining whether data stored as NFTs meets the definition of personal data, and guidance around data anonymization or pseudonymization as it relates to health data stored as NFTs.

5 Conclusion and future work

This exploratory research examined the use of Non-Fungible Tokens (NFTs) for digital identity data and related privacy concerns. A concrete NFT-enabled digital identity data workflow has been proposed as a reference and foundation for future research and development. The findings of this research suggest that while NFT-enabled digital identity may offer potential benefits for those seeking anonymity and privacy online, there are also several significant threats to privacy that must be addressed. These privacy risks are analyzed, and potential solutions for each individual risk are proposed. The suitability of NFTs for digital identity is also examined from a regulatory compliance perspective. The research suggests embedding privacy into smart contracts by using the programmable privacy technique to address the limitations of NFTs enabled digital identity data representation and management. Future research should implement programmable privacy-based smart contracts and evaluate their effectiveness using measurable benchmarks, including access control efficiency (permission verification times), scalability (transaction throughput under load), and privacy assurance (security audits and zkSNARK verification). Testing these solutions in real-world settings will refine NFT-enabled identity management to balance privacy, security, and compliance effectively.

Author contributions M.J.A proposed the initial draft of the paper. A.Q.G then reviewed and updated abstract, Sects. 1–2 and final conclusion. All authors reviewed the manuscript.

Funding There was no funding received for this work and paper.

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Ethics approval and consent to participate Not applicable.

Consent for publication Not applicable.

Competing interests The authors declare no competing interests.

References

1. Schmidt JT, Tang M. Digitalization in education: challenges, trends and transformative potential. In: Führen und Managen in der digitalen Transformation. Springer Fachmedien Wiesbaden; 2020. p. 287–312.
2. Zhao S, Zhang Y, Iftikhar H, Ullah A, Mao J, Wang T. Dynamic influence of digital and technological advancement on sustainable economic growth in belt and road initiative (BRI) countries. Sustainability (Switzerland). 2022;14(23):15782.
3. Scheiding R. Designing the future? the metaverse, NFTs, & the future as defined by unity users. Games Cult. 2022. https://doi.org/10.1177/15554120221139218.
4. Anwar M, Gill A, Beydoun G. Using adaptive enterprise architecture framework for defining the adaptable identity ecosystem architecture. In: ACIS 2019 Proceedings. https://aisel.aisnet.org/acis2019/94. Accessed 1 Jan 2019.
5. Careja AC, Tapus N. Digital identity using blockchain technology. Procedia Comput Sci. 2023;1(221):1074–82.
6. Self-Sovereign Identity - Alex Preukschat, Drummond Reed - Google Books. https://books.google.com.au/books?hl=en&lr=&id=BfQ1EAAAQBAJ&oi=fnd&pg=PA1&dq=self+sovereign+identity&ots=iDGHzy_pSw&sig=64J8hllu6DzZxzcmTLdNnaMgquE#v=onepage&q=self%20sovereign%20identity&f=false. Accessed 16 Feb 2025.
7. Goel A, Rahulamathavan Y. A comparative survey of centralised and decentralised identity management systems: analysing scalability, security, and feasibility. Future Internet. 2025;17(1):1.
8. Arenas R, Fernandez P. CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. In: 2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018 - Proceedings. 2018. https://ieeexplore.ieee.org/abstract/document/8436324/. Accessed 16 Jan 2023.
9. Popescu AD. Non-Fungible Tokens (NFT)-Innovation beyond the craze. Eng Technol J. 2021;66:2021.
10. Pinto-Gutiérrez C, Gaitán S, Jaramillo D, Velasquez S. The NFT hype: what draws attention to non-fungible tokens? Mathematics. 2022;10(3):335.
11. Casale-Brunet S, Zichichi M, Hutchinson L, Mattavelli M, Ferretti S. The impact of NFT profile pictures within social network communities. ACM Int Conf Proc Ser. 2022. https://doi.org/10.1145/3524458.3547230.
12. Park A, Kietzmann J, Pitt L, Dabirian A. The evolution of nonfungible tokens: complexity and novelty of NFT use-cases. IT Prof. 2022;24(1):9–14.
13. Jung Y. Current use cases, benefits and challenges of NFTs in the museum sector: toward common pool model of NFT sharing for educational purposes. Museum Manag Curatorship. 2022. https://doi.org/10.1080/09647775.2022.2132995.
14. Wang Q, Li R, Wang Q, Chen S. Non-fungible token (NFT): overview, evaluation, opportunities and challenges. ArXiv. https://arxiv.org/abs/2105.07447v3. Accessed 16 May 2021.
15. Kumar R, Marchang N, Tripathi R. Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In: 2020 International Conference on COMmunication Systems and NETworkS, COMSNETS 2020. 2020. p. 1–5. https://ieeexplore.ieee.org/abstract/document/9027313/. Accessed 16 Jan 2023.
16. Mojtaba S, Bamakan H, Nezhadsistani N, Bodaghi O, Qu Q. A decentralized framework for patents and intellectual property as NFT in blockchain networks. https://www.researchsquare.com. Accessed 5 Oct 2021
17. Walt.id. Introduction to NFTs for Identity. by walt.id TL;DR What are NFTs? 2022.
18. Nwaeze G. NFTs and metaverse: exploring the challenges and prospects for IP lawyers in the digitalized world. SSRN Electron J. 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4198128. Accessed 17 Jan 2023
19. Far SB, Bamakan SMH, Qu Q, Jiang Q. A review of non-fungible tokens applications in the real-world and metaverse. Procedia Comput Sci. 2022;214:755–62.
20. Song R, Gao S, Song Y, Xiao B. ZKDET: a traceable and privacy-preserving data exchange scheme based on non-fungible token and zero-knowledge. In: Proceedings - International Conference on Distributed Computing Systems. 2022. p. 224–34.
21. Ignoffo Z. Privacy affairs. The use case for NFTs - solving online identity verification. 2022. https://www.privacyaffairs.com/nft-identity-verification/. Accessed 15 Jan 2023
22. Zanjanab AG, Ahadi N, Monametsi G, Sorooshian S, Taghipour A. The Outlook of Non Fungible Tokens (NFTs): an alternative for academic manuscript ownership and scholarly publications. In: 2023 International Conference on Cyber Management and Engineering, CyMaEn 2023. Institute of Electrical and Electronics Engineers Inc.; 2023. p. 245–50.
23. Weyl EG, Ohlhaver P, Buterin V. Decentralized society: finding Web3's soul. SSRN Electron J. 2022. https://doi.org/10.2139/ssrn.4105763.
24. Bellagarda J, Abu-Mahfouz AM. 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(21):3934.
25. Wang Q, Li R, Wang Q, Chen S, Ryan M, Hardjono T. Exploring Web3 From the View of Blockchain. arxiv.org. 2022.
26. IBM. Why new off-chain storage is required for blockchains. Tech Rep. 2018. https://doi.org/10.13140/RG.2.2.34421.22242.
27. Gilbert C, Gilbert MA. Unlocking privacy in blockchain: exploring zero-knowledge proofs and secure multi-party computation techniques. GSJ. 2024;12(10):1368–92.
28. Wahrstatter A, Solomon M, Difrancesco B, Buterin V, Svetinovic D. BaseSAP: modular stealth address protocol for programmable blockchains. IEEE Trans Inf Forensics Secur. 2024;19:3539–53.
29. Chen T, Lu A, Kunpittaya J, Luo A. A review of zero knowledge proofs. 2021.
30. Galal HS, Youssef AM. Aegis: privacy-preserving market for non-fungible tokens. IEEE Trans Network Sci Eng. 2023;10(1):92–102. https://doi.org/10.1109/TNSE.2022.3205428.
31. Flor AML, Rodríguez DDL, Luna DJMS. Distributed cryptographic protocols. Ph.D. thesis. https://riunet.upv.es/handle/10251/198106. Accessed 16 Oct 2023.
32. Jamwal S, Cano J, Lee GM, Tran NH, Truong N. A survey on Ethereum pseudonymity: techniques, challenges, and future directions. J Netw Comput Appl. 2024;1(232): 104019.
33. Johnson KN. Decentralized finance: regulating cryptocurrency exchanges. SSRN Electron J. 2021;62:4–5.
34. Fairfield JAT. Tokenized: the Law of non-fungible tokens and unique digital property. Indiana Law J. 2021;97(4):4.