Decentralized, Quantum-Resistant Identity : The ZK-STARK and IPFS Approach

Khalid Maidine[1,*] **, Ahmed El-Yahyaoui**[1]**, Salima Trichni**[1,2]

[1]Intelligent Processing and Security of Systems (IPSS), Faculty of sciences, Mohammed V University in Rabat, Rabat, Morocco

[2]Department of Interdisciplinary Modules, Faculty of Economics, Legal and Social Sciences of Sale, Mohammed V University in Rabat, Morocco

Emails: khalid_maidine@um5.ac.ma; a.elyahyaoui@um5r.ac.ma; s.trichni@um5r.ac.ma

Abstract

Traditional identity management systems are vulnerable to critical issues, such as privacy breaches and single points of failure, which compromise the security and integrity of user information. These centralized models require the disclosure of sensitive data to third parties, exposing users to heightened risks. To address these challenges and the emerging threat of quantum computing, this paper proposes a novel blockchain-based identity management architecture that employs blockchain's decentralized, immutable ledger to eliminate centralized vulnerabilities, while zk-STARKs enable quantum-resistant, privacy-preserving identity verification without revealing sensitive information.The Framework integrate also InterPlanetary File System protocol for storing users data. This architecture establishes a user-centric, decentralized model that is resilient to both classical and quantum threats, and enhances privacy.

Keywords: Blockchain Technology; ZK-STARK; IPFS; Identity Management; Quantum Computing; Smart Contract

1 Introduction

1.1 Background

The increasing reliance on online services has undeniably improved convenience and interconnectedness for users; however, it has also revealed the inherent weaknesses of legacy identity management systems such as OAuth, OIDC, and SAML. These conventional frameworks depend on centralized authorities[20] and thus create large, singular repositories of sensitive personal information. Such centralization results in a critical vulnerability, making these repositories particularly appealing to cybercriminals. Once these systems are compromised, the consequences can be severe, as vast amounts of personal data become exposed (Table 1).

Recent incidents offer clear examples of the extent of these security gaps. In January 2024, for instance, Spoutible[28] suffered a data breach that impacted roughly 207,000 user accounts. The compromised data set included email addresses, usernames, full names, phone numbers, IP addresses, gender information, passwords, bcrypt password hashes, secrets for two-factor authentication (2FA), and password reset tokens. Investigations revealed that an insecure API endpoint allowed unauthorized access to this data, creating a risk of silent account takeovers by attackers.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

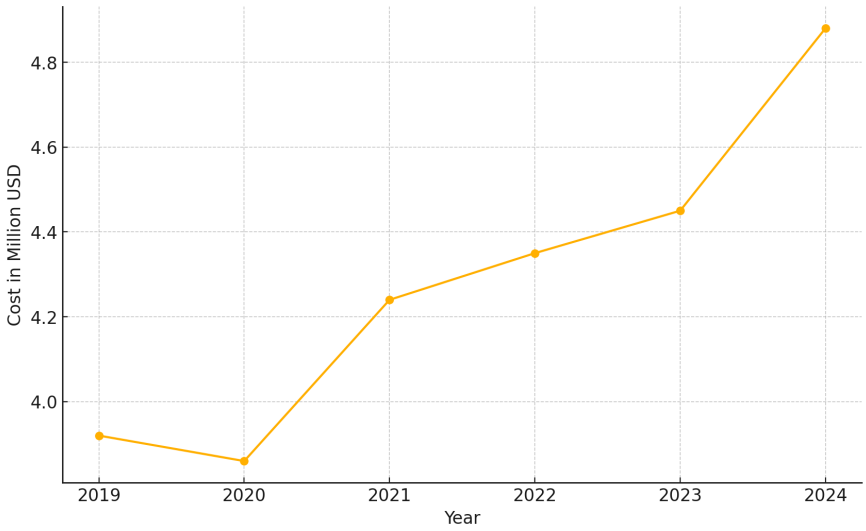

Figure 1: Global Average Cost of a Data Breach (IBM's annual reports)

Similarly, in January 2024, Trello faced a significant data exposure incident affecting around 15 million accounts.[4] Unlike a sophisticated hack, this breach resulted from incorrect configurations of publicly accessible boards and APIs. An individual using the handle 'emo' systematically tested 500 million email addresses against Trello's API to determine if they were linked to existing accounts. Although Trello had implemented IP-based rate limits, the attacker bypassed these defenses by leveraging rotating proxy servers, effectively continuing their data harvesting undetected.

In February 2024, Cutout.Pro experienced a major data breach[25] that revealed sensitive information belonging to 20 million users, including email addresses, hashed and salted passwords, IP addresses, names, and additional personal data. This breach became public when an actor known as 'KryptonZambie' shared 5.93 GB of this stolen data—comprising 41.4 million records—on a well-known hacking forum. Such incidents underscore the significant risks that arise when personal data is stored in large, centralized systems.

Table 1: Major Data Breaches in 2024

Organization	**Date**	**Data Records**	**Type of Data**
National Public Data (NPD)	April 2024	2.9 billion	Names, addresses, Social Security numbers, dates of birth, phone numbers, and historical address data[16]
Financial Business and Consumer Solutions (FBCS)	February 2024	4.2 million	Full names, Social Security numbers, birth dates[3]
Ticketmaster	May 2024	560 million	Names, addresses, phone numbers, customer details[9]
Change Healthcare	June 2024	145 million	Social Security numbers, medical records, addresses[27]
AT&T	July 2024	110 million	Phone numbers, approximate locations, customer data[2]
Dell	May 2024	49 million	Names, addresses, hardware details, order information, and warranty information[26]

Regardless of whether cybercriminals exploit unaddressed software flaws, improper configurations, or employ social engineering techniques such as phishing, they are often able to infiltrate these systems with remarkable ease. This reliance on a single centralized component creates a critical vulnerability; once an intrusion occurs, its impact can extend across millions of user accounts, causing severe reputational damage and financial instability for the organization involved (Figure 1).

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

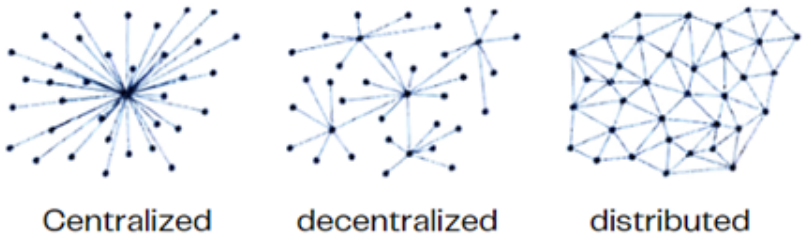

Figure 2: Centralized, decentralized and distributed system

1.2 Motivation

The repeated occurrence of large-scale data breaches, as exemplified by incidents at Spoutible and Cutout.Pro, underscores the urgent need for more robust and decentralized identity management systems. Traditional centralized platforms that store personal information in a single repository are particularly susceptible to both cyberattacks and human errors.[21] These breaches not only result in the unauthorized disclosure of sensitive data but also erode user trust, discouraging individuals from sharing personal details in digital environments. Consequently, digital services are increasingly viewed as insecure, which can hinder the widespread adoption of innovative technologies.

In response to these challenges, decentralized identity management solutions (Figure 2), including those leveraging blockchain technology,[29] offer a compelling alternative. These systems distribute data storage and verification processes, thereby eliminating single points of failure and enhancing overall security. For instance, integrating the InterPlanetary File System (IPFS) into identity management frameworks allows for distributed data storage, making it significantly harder for adversaries to target and compromise sensitive information.

Furthermore, advanced cryptographic methods, such as Zero-Knowledge Proofs (ZKPs), can bolster privacy within these decentralized frameworks. ZKPs enable individuals to confirm their identity without disclosing their personal information, thus adding an additional layer of protection against unauthorized access. When combined, blockchain, IPFS, and ZKP technologies have the potential to create a more resilient and secure identity management infrastructure, reducing dependence on centralized entities and addressing emerging threats, including those posed by quantum computing.

Additionally, IPFS ensures that personal data is stored in an encrypted and fragmented manner across a distributed network, substantially minimizing the risk of large-scale data leaks. This distributed and secure data storage approach also aligns with efforts to future-proof systems against quantum computing, which poses a significant threat to conventional encryption algorithms. The integration of blockchain, IPFS, and ZKP technologies represents a promising pathway for the evolution of identity management, enhancing security, transparency, and resilience.

By combining these innovations—blockchain, ZKP, and IPFS we can create identity management systems that not only address current security challenges but also anticipate and mitigate future threats, including those introduced by quantum computing.

1.3 Contribution

The principal contributions of this study can be summarized as follows. It proposes a novel identity management framework that integrates blockchain technology, zk-STARKs, and the InterPlanetary File System (IPFS) to enhance both security and privacy. By decentralizing and distributing data storage while employing zk-STARKs for privacy-preserving verification, the framework mitigates the vulnerabilities typically associated with centralized identity management systems. This approach allows users to authenticate identity attributes without disclosing sensitive data. Furthermore, the proposed solution is designed to be resilient to emerging threats, including those posed by quantum computing, providing a comprehensive and future-proof system for secure digital identity management.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

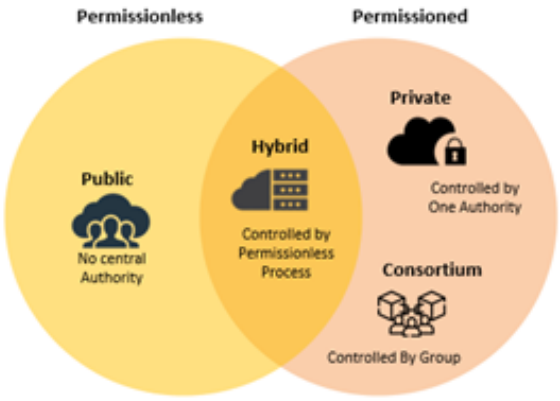

Figure 3: Type of Blockchain

2 Preliminaries

2.1 BLOCKCHAIN

Since the release of Bitcoin's whitepaper in 2008 by Satoshi Nakamoto[31] and the subsequent launch of Bitcoin in 2009,[23] cryptocurrencies have had a profound impact on traditional financial systems. At the core of Bitcoin is blockchain, a form of distributed ledger technology. Blockchain organizes transactions in a sequence of linked blocks, using cryptographic methods to secure data integrity and ensure immutability. Unlike traditional systems that rely on intermediaries, blockchain transactions occur directly between participants, resulting in a transparent and tamper-resistant record. This decentralized architecture fosters a trust model independent of centralized authorities.

Blockchains can be classified based on whether peers require explicit authorization to participate in the network (Figure 3). Permissionless or public blockchains[13] operate without restrictions on participant entry, relying on consensus protocols among potentially unknown users to validate transactions and maintain security. This model enables a fully decentralized trust framework, granting all participants equal rights to interact with the system.

Conversely, permissioned blockchains[30] include consortium and private blockchain models. Consortium blockchains are governed by a collective of institutions that determine the degree of network access and transparency based on their specific use cases. These networks often employ alternative consensus algorithms—such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT)—to reduce the resource consumption associated with Proof of Work (PoW). Private blockchains restrict access to a single organization or a select group of participants, making them particularly suitable for applications with limited or specialized membership. While these permissioned systems enhance control and security, they inherently limit decentralization and have a narrower application scope than public blockchains.

2.2 SMART CONTACTS

Smart contracts are autonomous, self-executing programs that implement agreements directly on the blockchain, thereby eliminating the need for intermediaries.[22] They play an essential role in a range of applications, including financial services and identity management, by automating processes such as identity attribute verification (e.g., citizenship status or educational qualifications) based on predefined logic. For example, a smart contract can confirm a user's citizenship by validating a passport without revealing additional personal information, thereby increasing accuracy and minimizing the risk of human error.

Moreover, smart contracts can autonomously manage Decentralized Identifiers (DIDs) by updating or revoking credentials such as expired professional licenses in real time. This ensures that only valid records are retained

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

within the system. The importance of securing and auditing smart contracts has grown significantly due to past vulnerabilities, such as those exposed in the 2016 DAO attack.[33] To address these concerns, advanced techniques including formal verification, symbolic execution, and fuzz testing have emerged as critical safeguards. Formal verification provides mathematical assurance that the contract adheres to its specifications, while symbolic execution systematically examines all execution paths to identify vulnerabilities. Fuzz testing,[17] in use since 2018, complements these approaches by feeding random inputs to smart contracts, uncovering potential weaknesses that may not be evident through traditional testing.

Future developments in these areas aim to enhance performance, refine the accuracy of bug detection techniques (test oracles), and improve the quality of input data used in testing. These advancements will help ensure that smart contracts are more secure and efficient, supporting broader adoption of decentralized applications in a range of fields.

2.3 DECENTRALIZED IDENTIFIERS (DIDS):

Decentralized Identifiers (DIDs) represent a substantial innovation in blockchain enabled identity management, offering a self-sovereign alternative to traditional identifiers typically controlled by centralized authorities.[19] Unlike conventional identifiers that depend on third-party entities such as governmental bodies or corporate service providers DIDs empower users to independently create and manage their own identifiers. This approach eliminates intermediary dependence and places full ownership and control of identity credentials into the hands of individuals.

These identifiers are securely stored on blockchains and can be verified using smart contracts, ensuring both authenticity and efficiency in the credential validation process. The decentralized nature of DIDs also addresses the vulnerability of single points of failure, which commonly afflict centralized systems, thereby enhancing user privacy and strengthening data security within digital environments.

2.4 ZERO-KNOWLEDGE PROOFS (ZKPS):

Zero-Knowledge Proofs (ZKPs) are a type of cryptographic protocol that allow a prover to convince a verifier that a certain statement is true without revealing any further information about the statement itself.[10] This is achieved through three key properties: completeness, which ensures that if the statement is true, the verifier will accept the proof; soundness, which prevents a dishonest prover from creating a false proof that could deceive the verifier into accepting an incorrect statement; and zero-knowledge, which ensures that the verifier learns nothing beyond the fact that the statement is true. A classic example of a zero-knowledge proof is the Σ-protocol, a three-step interactive protocol that demonstrates zero-knowledge under the assumption that the verifier is honest. For instance, using the notation:

$$ZKP(\alpha : y = g^{\alpha})$$

we express that the prover can demonstrate knowledge of a secret α such that $y = g^{\alpha}$, where g and y are elements of a group G. Moreover, by applying the Fiat-Shamir heuristic, these interactive protocols can be converted into non-interactive ones, maintaining their zero-knowledge property even in less controlled environments. This makes ZKPs incredibly useful for privacy-preserving systems, particularly in blockchain.

2.5 VERIFIABLE CREDENTIALS (VCs):

Verifiable Credentials (VCs) are cryptographically signed digital documents that allow users to prove certain facts about their identity or attributes, without revealing unnecessary details. Developed as part of the World Wide Web Consortium (W3C) standards,[19] VCs are fundamental to decentralized identity systems, offering secure, privacy-preserving solutions for identity verification. They allow for the issuance, holding, and verification of credentials by different entities in a trusted and efficient manner.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

At the core of Verifiable Credentials is the use of digital signatures to ensure that the credential issued by a trusted issuer (such as a university or government) signs the credential using their private key, and ensures that the credential has not been tampered with and is verifiable by another entity. This process is mathematically represented by the Elliptic Curve Digital Signature Algorithm (ECDSA):

$$\sigma = (r, s) = (kG, H(C) + r \cdot sk \mod n)$$

where:

- G is the base point on the elliptic curve.
- $H(C)$ is the cryptographic hash of the credential.
- sk is the issuer's private key.
- k is a randomly generated nonce.
- r and s are the signature's digital components.
- n is the order of the elliptic curve.

The verifier uses the issuer's public key to validate the signature, ensuring that the credential is both authentic and untampered. One of the key advantages of VCs is their ability to support selective disclosure, where the holder can reveal only specific parts of the credential as needed. This is often achieved through cryptographic commitment schemes, such as Pedersen Commitments, which enable privacy-preserving proofs:

$$C = g^r h^m \mod p$$

where:

- m is the identity attribute being committed (e.g., age or citizenship).
- r is a random value (nonce) that ensures the commitment is hidden.
- g and h are generators of a group of prime order p.

This technique allows the holder to prove that they possess valid information without exposing the actual data itself. The verifier can then check the validity of the disclosed information without learning more than necessary, ensuring both privacy and integrity.

2.6 ZK-STARKs

ZK-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge), introduced in 2018[1] by Eli Ben-Sasson and colleagues, represent a significant advancement in cryptographic proof technologies. Designed to overcome the limitations of earlier zero-knowledge systems such as ZK-SNARKs, ZK-STARKs eliminate the need for a trusted setup phase—a component that historically introduced a potential vulnerability. By removing this dependency, ZK-STARKs ensure greater system transparency and resilience against single points of failure.

At their core, ZK-STARKs employ probabilistic proof concepts, particularly leveraging the Fast Reed-Solomon Interactive Oracle Proofs of Proximity (FRI) algorithm. This mathematical foundation enables the generation of succinct, scalable proofs that can be verified in sublinear time. Such efficiency is particularly valuable in systems that handle large volumes of data, like blockchain-based identity management platforms.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

A key distinction between ZK-STARKs and ZK-SNARKs lies in quantum resistance.[11] ZK-STARKs are designed to withstand quantum computing threats, thereby enhancing their long-term viability in security critical applications. As a result, ZK-STARKs are increasingly seen as a transformative technology for scalable, privacy-preserving, decentralized applications,[14] especially where the protection of sensitive data, such as user identities, is paramount.

Their innovative algorithmic approach and scalability make ZK-STARKs a foundational tool for secure digital identity frameworks in the evolving technological landscape. The Table 2 presents a comparative overview of ZK-STARKs and ZK-SNARKs, outlining key differences. The following subsections detail the procedures for proof generation and verification as described in.[1]

Table 2: Comparison between ZK-STARKs and ZK-SNARKs[15]

Feature	ZK-STARKs	ZK-SNARKs
Trusted Setup	Does not require a trusted setup phase	Involves a trusted setup phase
Transparency	Entirely transparent with no need for third-party trust	Depends on a trusted third party to establish initial parameters
Proof Size	Proofs are generally larger	Produces smaller, more compact proofs
Verification Speed	Enables sublinear time verification	Generally fast, though verification can be longer
Quantum Security	Inherently resistant to attacks from quantum computing	Exposed to vulnerabilities from future quantum computers
Scalability	Exceptionally scalable, particularly for large datasets	Scalability is somewhat limited when compared to ZK-STARKs
Underlying Mathematics	Relies on probabilistic proof techniques such as FRI (Fast Reed-Solomon IOPP)	Uses elliptic curve operations and pairing-based cryptography
Computational Efficiency	Well-suited for verifying complex computations efficiently	Performs best for smaller-scale or simpler computational needs
Use Cases	Applicable to systems requiring decentralization and scalability, like secure voting or identity frameworks	Typically implemented in platforms like Zcash, Filecoin, and Loopring due to its minimal storage footprint and concise proofs

2.6.1 ZK-STARK Proof Generation:

1. **Problem Definition and Requirements**

   - The purpose of a ZK-STARK proof is to produce a verifiable demonstration that a computation C has been correctly performed on a dataset D without revealing the data itself, thus preserving privacy.
   - In this scenario, the prover P (such as an entity managing sensitive information) must demonstrate a claim, such as the non-existence of a specific record within D. This proof should reveal nothing beyond the truth of the statement.
   - A single output α from C (for instance, a "no match" for a DNA profile p)[1] is shared, while the prover ensures that the entire computation accurately reflects the dataset D, avoiding the need for trusted intermediaries or exposure of confidential details.

2. **Arithmetization – Converting Computation to Algebraic Form**

   To enable rigorous verification, ZK-STARK reformulates computational steps as algebraic statements. This transformation involves:

   - **Algebraic Intermediate Representation (AIR)**
     AIR describes each computation step using polynomials $P_i(X, Y)$. In this framework, X and Y represent the input and output states of the computation step, respectively. Each transition is represented as:

$$P_1(X, Y) = 0, \quad P_2(X, Y) = 0, \quad \ldots, \quad P_s(X, Y) = 0$$

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

This ensures that each step of the computation adheres to well-defined polynomial constraints.

- **Low-Degree Extension (LDE)**
  LDE extends a function f, defined over a smaller domain S, to a larger domain S'. This extension preserves the structure of the original function, allowing verification over a broader domain. By broadening the polynomial representation across a larger field, ZK-STARK ensures the extended dataset remains faithful to the original. The article highlights the use of the Fast Fourier Transform (FFT), particularly the additive FFT for binary fields, to compute these extensions efficiently.

3. **Commitment to Data and Computation Steps**

   At this stage, the system commits to all inputs, intermediate states, and final outputs, ensuring they cannot be modified retroactively. This establishes integrity and supports scalable verification.

   - **Reed-Solomon Encoding**
     Reed-Solomon codes encode the data and intermediate states, forming a mathematical commitment to the entire computational process. This approach secures the computational trace, enabling verifiers to check targeted elements rather than the full dataset, thereby improving scalability.
   - **Merkle Tree**
     A Merkle tree structures encoded data as a binary tree, with each node representing a hash of its child nodes. The root hash functions as a tamper-evident commitment to the dataset, so any change in data can be traced through the authentication path back to the root.

     $$\text{Commit}(D) = \text{MerkleRoot}(f(D))$$

   - **Authentication Paths**
     To prove the correctness of specific data elements, each element is accompanied by an authentication path that connects it securely to the root of the Merkle tree.

4. **Interactive Oracle Proof of Proximity (IOPP)**

   - **Randomized Queries**: Rather than evaluating the entire dataset, the verifier randomly selects points within the dataset, achieving high-confidence verification while avoiding exhaustive checks.
   - **FRI (Fast Reed-Solomon IOP of Proximity)**: This protocol ensures that the function f closely approximates a low-degree polynomial g, verifying that the dataset is consistent with a polynomial structure.

     $$f \in RS[F, S, \rho] \quad \text{such that} \quad f(x) \approx g(x)$$

5. **Proof of Knowledge and Soundness**

   ZK-STARK proofs guarantee three essential properties:

   - **Completeness**: If the assertion is true (e.g., the DNA profile is not found in the database), the prover can reliably convince the verifier.
   - **Soundness**: If the claim is false, the probability of the prover misleading the verifier is negligible.
   - **Zero Knowledge**: The protocol ensures that no details beyond the final outcome α are revealed. This is accomplished through randomized queries, safeguarding the confidentiality of all other dataset elements.

2.6.2 ZK-STARK Proof Verification:

1. **Merkle Root Validation**

   - Initially, the verifier confirms that the Merkle root, as provided by the prover, correctly represents the original data commitment.
   - This validation ensures the integrity of the computation trace T, where the root R is computed as:

     $$R = \text{hash}(T)$$

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

2. **Low-Degree Extension (LDE)**

   - The verifier performs a Low-Degree Extension to interpolate the polynomial corresponding to the computation trace, verifying that it maintains a low degree.
   - For a given function f defined on a field F with subsets $S \subset S'$, the extended polynomial f' is given by:

$$f'(x) = \sum_{i=0}^{d} a_i x^i$$

   - The Fast Fourier Transform (FFT) is employed to optimize the LDE process, reducing the computational workload to approximately $3 \cdot |S'| \log |S'|$.

3. **Reed-Solomon Interactive Oracle Proof of Proximity (FRI Protocol)**

   - The verifier uses the FRI protocol to assess whether the polynomial $f(x)$ provided by the prover indeed approximates a low-degree polynomial.
   - This involves sampling random evaluation points $x_1, x_2, \ldots, x_k$ and confirming that $f(x)$ is close to a polynomial of degree less than $\rho|S|$:

$$f(x) \approx g(x)$$

4. **Random Sampling with Merkle Path Validation**

   - For every randomly chosen query point x_i, the verifier checks the Merkle paths from leaf to root to ensure consistency with the initially committed trace.
   - Each verification step requires confirming:

$$\text{hash}(x_{i-1}, x_i) = x_{\text{parent}}$$

   - These paths must align with the Merkle tree's structure, confirming the trace's integrity.

5. **Final Consistency Verification**

   - After completing polynomial proximity and Merkle path validation, the verifier performs a final check to ensure that all constraints for the queried polynomial evaluations are consistent with the initial data commitments.
   - This step validates the overall correctness and soundness of the ZK-STARK proof.

Finally, the efficiency of ZK-STARK verification can be described by the following ratios for runtime and communication size:

$$\rho_{\text{time}} = \frac{T_V}{T_C} \quad \text{and} \quad \rho_{\text{size}} = \frac{CC}{|D|}$$

2.7 Decentralized Applications (DApps)

Decentralized Applications (DApps)[34] represent a transformative approach to application development and deployment by utilizing a decentralized network infrastructure, thereby eliminating the reliance on traditional intermediaries such as centralized servers or institutions. Built on blockchain technology, DApps ensure a high level of transparency, security, and immutability, as all transactions and data are maintained by a distributed network of participants rather than a singular controlling entity. This decentralized governance fosters trustless environments where interactions are governed by predefined rules embedded in smart contracts. DApps can operate on either public or permissioned blockchain networks, providing varying levels of privacy and scalability. The decentralized nature of DApps mitigates risks related to single points of failure and censorship, empowering users with direct engagement in the platform's processes. This paradigm shift enables DApps to offer robust, resilient systems that uphold the core principles of decentralization, making them particularly suited for sectors requiring high levels of trust, transparency, and security.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

2.8 InterPlanetary File System (IPFS)

The InterPlanetary File System (IPFS) is increasingly adopted across diverse domains for its decentralized, peer-to-peer data storage capabilities.[12] Beyond identity management, one significant application is in content delivery systems such as Filecoin, a decentralized storage network built upon the IPFS protocol. Within Filecoin, users store and retrieve data without depending on centralized servers, thereby enhancing data availability and reducing vulnerability to censorship or outages by distributing files across multiple participating nodes.

Another noteworthy application is DTube, a decentralized video-sharing platform modeled after traditional platforms like YouTube. DTube utilizes IPFS to host its video content, ensuring that no single entity exercises control over the data. This decentralized approach enhances user autonomy and privacy by spreading video files across a peer-to-peer network rather than relying on a central server.

IPFS is also employed in decentralized web hosting scenarios, where websites are maintained across a network of nodes instead of a single server, guaranteeing continuous availability even if some nodes become inaccessible. These implementations illustrate how IPFS bolsters the robustness, privacy, and decentralized nature of modern web services.

From a technical standpoint, IPFS fragments data into smaller components, each assigned a unique cryptographic hash known as a content identifier (CID).[8] These fragments are then distributed across various nodes within the network. When a file is requested, the system locates and retrieves the relevant pieces using the CIDs, reassembling them to reconstruct the complete file. As the system uses content-based addressing rather than location-based addressing, the data's integrity is inherently preserved—any modification to the content would produce a new hash, signifying a distinct version of the file. This immutable structure makes tampering evident through straightforward hash verification. IPFS also employs a distributed hash table (DHT) to track which nodes possess specific data fragments, enabling efficient and scalable file retrieval within the decentralized network.

3 Related Works

The rapid evolution of blockchain-based identity management systems (IDMS) has garnered significant attention, especially in the context of privacy and scalability challenges. Despite various efforts to leverage blockchain and zero-knowledge proofs (ZKPs) to secure identity verification processes, existing approaches face critical limitations that hinder their widespread adoption. This section examines related works, focusing on their shortcomings and how zk-STARKs provide a more advanced solution.

One prominent work is BIDaaS (Blockchain-based Identity as a Service) introduced by Lee et al. (2017),[18] which proposes a decentralized identity service that utilizes blockchain to authenticate users without pre-shared credentials. While BIDaaS addresses some of the inefficiencies in centralized identity systems, it still relies on a model where certain identity attributes are managed by a central entity (the BIDaaS provider), reintroducing risks of single points of failure. More critically, it does not fully explore the potential of zero-knowledge proofs, leaving user privacy exposed during identity verification processes. This work highlights the need for systems that not only decentralize identity but also preserve privacy more robustly, as achieved through zk-STARKs.

Yang and Li (2020) presented BZDIMS,[32] a zero-knowledge-proof-based identity management system that leverages zk-SNARKs to ensure privacy and integrity during identity verification. Although zk-SNARKs have been widely praised for their ability to verify information without revealing underlying data, they come with inherent limitations such as the need for a trusted setup. This trusted setup creates a vulnerability in which a compromised initial setup could undermine the entire system's security. Moreover, the high computational costs associated with zk-SNARKs make them less scalable for larger networks, limiting their practical use in high-throughput environments. In contrast, zk-STARKs eliminate the need for a trusted setup, offering greater transparency and security, and they are more efficient at scale, making them better suited for widespread adoption.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

In the realm of social networks, Zhu et al. (2023)[35] proposed a decentralized identity management protocol based on range proofs, designed to protect user privacy without requiring a trusted setup. While range proofs represent a significant step forward in terms of privacy protection, they are still limited in their ability to scale and handle more complex identity verification scenarios. For instance, they are more effective at proving a simple condition, such as whether a user's age is within a certain range, rather than managing more intricate identity attributes. zk-STARKs, with their ability to prove complex statements efficiently and without trusted setups, offer a more versatile solution to the challenges highlighted in this work.

In the healthcare sector, Barros et al. (2021)[7] demonstrated the use of self-sovereign identity (SSI) combined with blockchain and zero-knowledge proofs to create a privacy-preserving vaccination pass. This system allows users to prove their vaccination status without revealing sensitive personal details, showcasing the practical applications of blockchain and ZKPs in privacy-critical environments. However, the use of zk-SNARKs in this system, as with other similar solutions, introduces limitations related to computational complexity and the risk of trusted setup compromise. Furthermore, while it addresses the immediate need for privacy in health-related data, the system does not account for the long-term scalability and quantum threats that zk-STARKs are uniquely designed to mitigate. By employing zk-STARKs, the solution could not only improve privacy but also future-proof the system against emerging quantum computing risks.

A broader survey of blockchain-based identity management systems by Ahmed et al. (2022)[5] provides a comprehensive review of existing solutions, highlighting the transition from centralized to decentralized models. While this shift represents a critical advancement in digital identity management, the paper also notes that many blockchain-based IDMSs still struggle with scalability and privacy concerns, particularly when handling large networks or diverse user bases. The review underscores the importance of adopting solutions that can balance privacy, security, and efficiency, pointing to zk-STARKs as a promising avenue for future research.

Panait and Olimid's[24] study investigates how advanced cryptographic tools, specifically zk-SNARKs and zk-STARKs, can provide privacy in blockchain-based identity management. In public blockchain networks, where data exposure risks are high, their study explores how privacy-preserving tools can verify identities without revealing sensitive information. They compare zk-SNARKs and zk-STARKs, discussing that zk-SNARKs, though efficient and small in size, require a trusted setup. This setup requirement can be a security concern. zk-STARKs, on the other hand, do not need a trusted setup but produce larger proofs. The authors examine the available libraries for zk-SNARKs and zk-STARKs, offering practical insights for using zk-SNARKs today and exploring zk-STARKs as a promising, emerging alternative.

Lohar et al.[19] propose a decentralized identity management system based on SSI principles, using Ethereum blockchain and IPFS. They highlight problems in traditional, centralized identity systems that depend on single trusted entities, suggesting a shift towards a decentralized system that allows users to control their identity information. Using Ethereum smart contracts and zk-SNARKs, their system enables users to prove their identity while keeping other personal details private, following W3C's standards for DID. This setup allows users to selectively reveal identity details, such as proving age without disclosing additional information. By using IPFS for data storage, the authors promote decentralized access to data, supporting GDPR-compliant practices like data minimization.

Anusuya et al.[6] extend the use of zk-SNARKs to electronic health records, proposing a privacy-preserving, blockchain-based EHR management system that ensures secure access and data confidentiality. Their system leverages zk-SNARKs to enable zero-knowledge verification, whereby healthcare providers can verify patient information without exposing sensitive data. This approach minimizes the risk of data breaches by storing hashed health records on the blockchain, allowing only authorized users to retrieve necessary health information. Anusuya et al. highlight that zk-SNARKs provide an efficient mechanism for privacy within EHR systems, showcasing the adaptability of zero-knowledge protocols for high-sensitivity domains such as healthcare.

A key research gap lies in integrating zk-STARKs with IPFS to achieve scalable, privacy-preserving identity management on blockchain. While zk-STARKs enhance transparency without trusted setups, their larger proof sizes challenge real-time use, and efficient pairing with IPFS remains underdeveloped. By integrating zk-STARKs into a decentralized identity management framework and adopting IPFS as a distributed storage of personal data, this paper aims to offer a solution that not only preserves user privacy but also ensures long-term security and scalability.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

4 Architecture Overview

The proposed decentralized identity management framework empowers users to securely and privately oversee their digital identities by leveraging blockchain technology. This architecture integrates zk-STARKs to provide privacy-preserving verification of identity attributes, allowing users to prove claims without exposing any confidential information. Furthermore, the adoption of Decentralized Identifiers (DIDs) and IPFS ensures that users maintain complete autonomy over their identity credentials, eliminating the need for reliance on centralized intermediaries. The subsequent sections detail the core components of this architecture and examine how the incorporation of zk-STARKs and IPFS strengthens the privacy, availability, and security of digital identities. Finally, the processes for user registration and identity verification are outlined in the following sections.

4.1 KEY COMPENENTS:

The primary components of the proposed architecture are as follows:

User: This refers to the individual who interacts with the decentralized application (Dapp) using their cryptographic wallet (e.g., MetaMask). The user provides essential personal information—including name, location, and date of birth—via a sign-up form, and authorizes blockchain transactions by linking their wallet.

Wallet: A cryptographic wallet containing the user's private key, enabling them to sign blockchain transactions securely. The wallet establishes a connection with the Dapp, facilitating user registration and smart contract interactions. Additionally, it provides the wallet address (via the `GetWallet()` function), which is utilized to create Decentralized Identifiers (DIDs).

BLOCKID Dapp: Serving as the client-facing interface, the BLOCKID Dapp enables users to connect their wallets and input personal data (name, location, date of birth) for registration. It interacts with the backend smart contract to perform key operations, including DID creation, data submission, and storage of encrypted data on IPFS.

Smart Contract: Operating on the Ethereum blockchain, this decentralized program handles the application's core logic, performing the following functions:

-Generate DID: Assigns a unique Decentralized Identifier (DID) to each user, linking it to the wallet address to establish a verifiable identity.

-Push DID: Records the generated DID on the blockchain, using the associated wallet address as a reference.

-Submit Data: Encrypts the user's personal information (name, location, and date of birth) using zk-STARKs before submitting it to the contract.

-Store Hash: Once the data is encrypted and stored on IPFS, the smart contract saves the resulting IPFS hash along with the user's DID, ensuring data integrity and verifiability.

IPFS (InterPlanetary File System):[12] A decentralized peer-to-peer storage network that hosts the user's encrypted personal data. After encryption through zk-STARKs, the user's information is stored in a distributed fashion on IPFS. An IPFS hash—uniquely identifying the stored data—is generated and subsequently saved in the smart contract to provide tamper-evident, persistent data availability.

4.2 SIGN UP WORKFLOW

As illustrated in Figure 4, the sign-up process is detailed as follows:

1. The user accesses the BLOCKID **DApp**.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

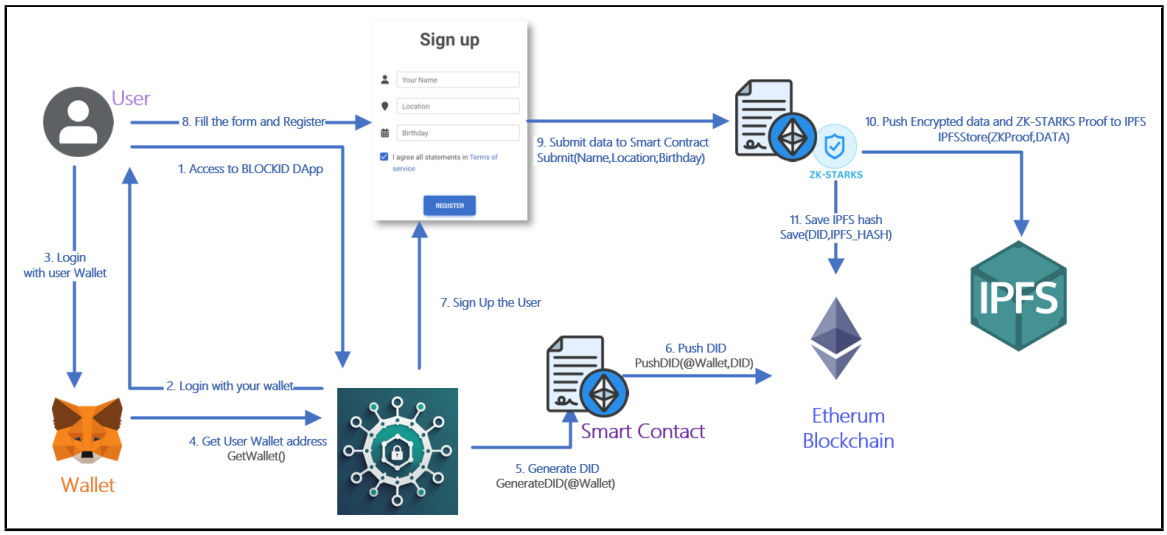

Figure 4: Sign-up workflow

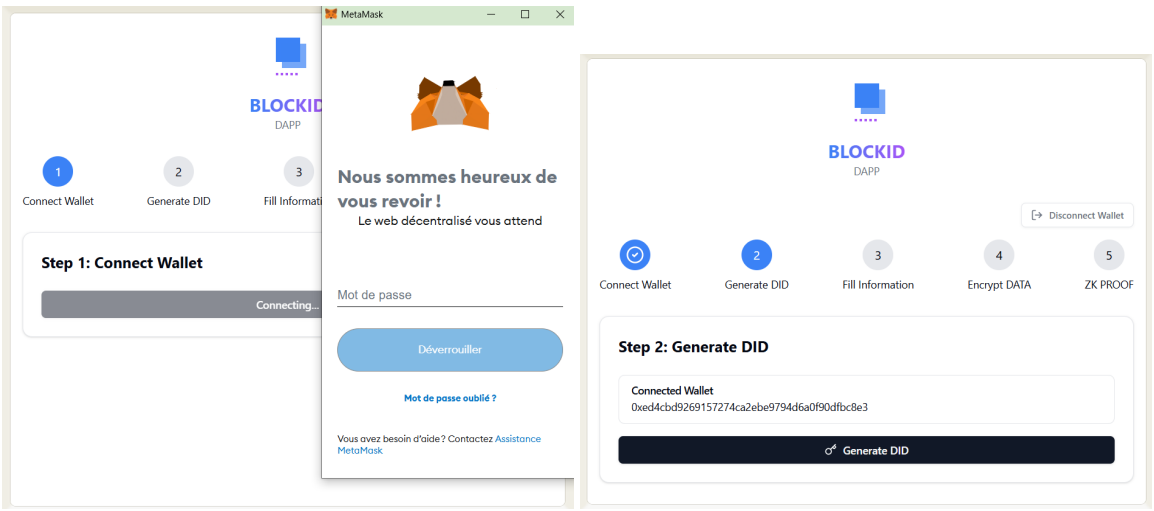

Figure 5: DApp - Front End

DOI: https://doi.org/10.54216/JCIM.160212
Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

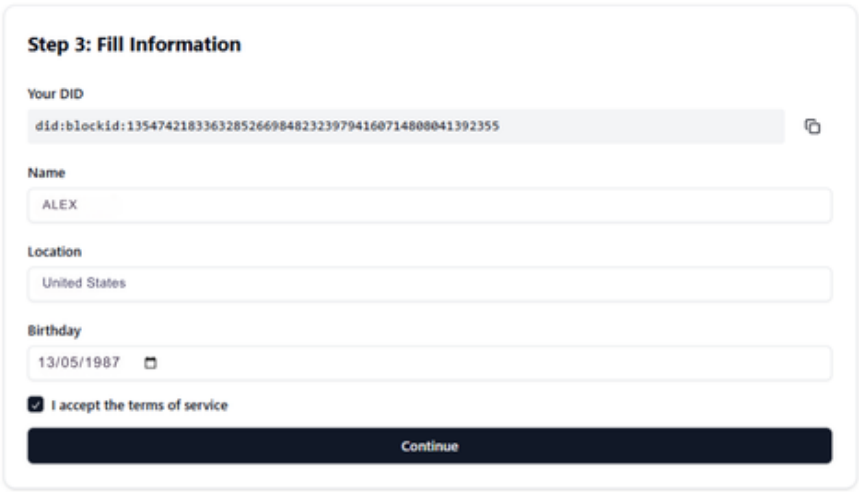

Figure 6: DApp form for collecting user data.

(a) The user begins by accessing the BLOCKID **DApp**.

(b) To authenticate, the user connects their Ethereum wallet (e.g., *MetaMask, TrustWallet*) to the **DApp**. This connection allows the retrieval of the user's Ethereum address, which is then stored locally within the **DApp** as the primary identity anchor Figure 5.

(c) A **DID** is generated by applying the W3C DID specification to the user's Ethereum address and appending a custom prefix (`did:blockid:`) that aligns with Ethereum DID methods.

(d) The **DApp** forwards the newly created **DID** along with the Ethereum address to a smart contract deployed on the Ethereum blockchain. This contract keeps a secure mapping between Ethereum addresses and their associated DIDs.

(e) The user completes the sign-up form by providing personal information, including name, location, and date of birth, and submits it via the **DApp** Figure 6.
For example:

```
{
    "Name": "ALEX",
    "location": "United States",
    "birthday": "1987-05-13"
}
```

(f) The provided personal data (name, location, birthday) is pre-processed for encryption by transforming it into a polynomial form over a finite field, a crucial step for zk-STARK encryption. For instance, the name "Mohammed" is converted into a polynomial representation:

$$P_{\text{name}}(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

(g) Using these polynomial representations, the **DApp** constructs a succinct zk-STARK proof, demonstrating that the submitted data satisfies all required constraints (such as accurate name, location, and birthday) without revealing the actual data itself.

$$zk\_proof = generate\_proof(polynomials)$$

(h) The personal data, together with the zk-STARK proof, is packaged and encrypted to enhance security. This encryption ensures that the data remains inaccessible without the appropriate decryption key.

(i) The encrypted user data is then uploaded to IPFS, and an IPFS Content Identifier (CID) is generated, serving as a unique reference for the stored data.

(j) Finally, the IPFS hash and the zk-STARK proof are linked to the user's DID and recorded on the blockchain. The smart contract maintains the mapping between the DID and the corresponding IPFS hashes, ensuring data integrity and verifiability.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

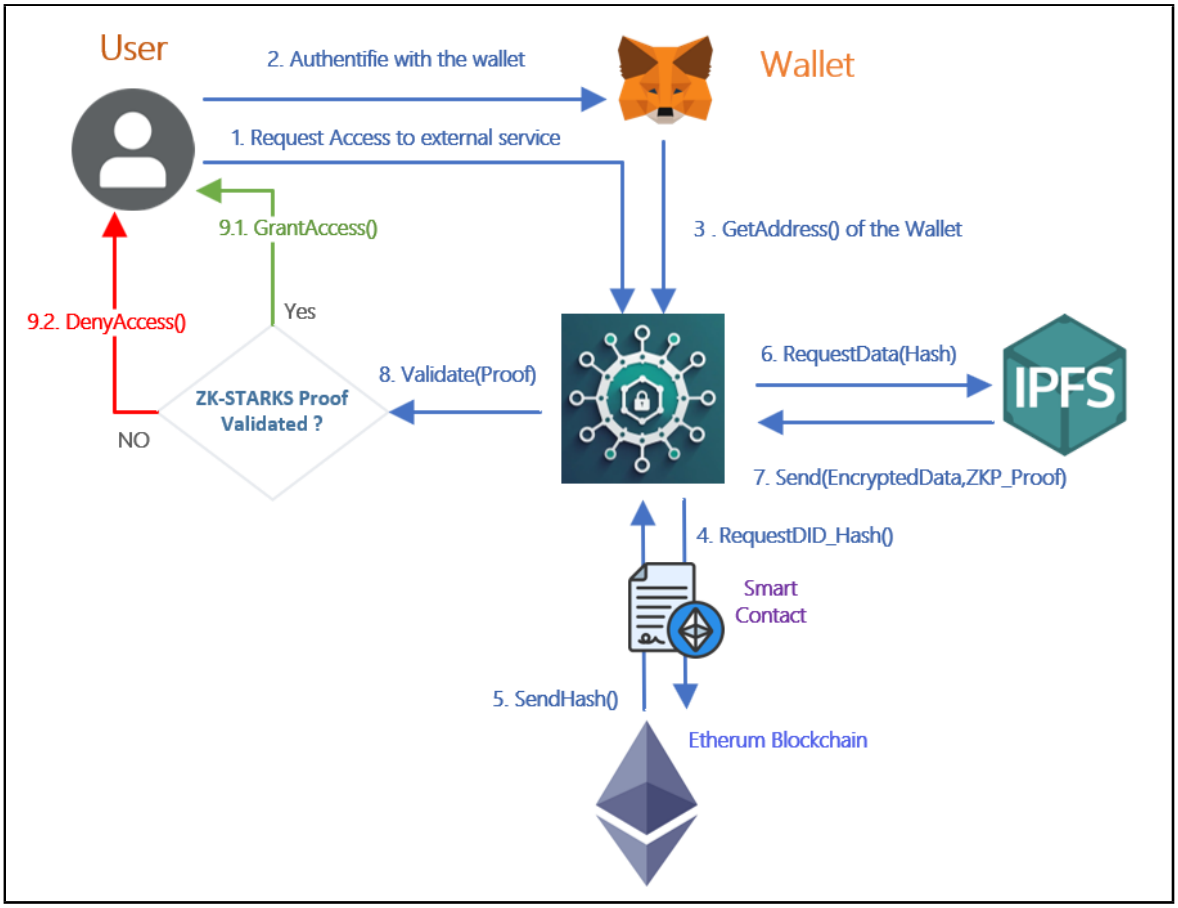

Figure 7: Verification Workflow

4.3 VERIFICATION WORKFLOW

As depicted in Figure 7, the verification process proceeds as follows:

(a) The user begins the verification by submitting a request to an external verifier (e.g., a financial institution, government portal, or similar service).
csharp Copier Modifier

(b) The user then authenticates with the verifier by connecting their blockchain wallet previously used with the BLOCKID application (such as MetaMask).

(c) The verifier collects the wallet address from the connected wallet to establish the user's blockchain identity.

(d) Next, the verifier queries the smart contract on the Ethereum blockchain to obtain the user's DID and the associated IPFS hash corresponding to the wallet address.

(e) The smart contract responds by returning the relevant IPFS hash to the verifier.

(f) Using this IPFS hash, the verifier makes a request to IPFS to retrieve the user's encrypted identity data.

(g) IPFS responds by providing the encrypted user data along with the zk-STARK proof tied to the user's DID.

```
{
    "proof": "zk_stark_proof_data",
    "encrypted_data": {
        "name": Encrypted (ALEX),
        "location": Encrypted (United States),
        "birthday": Encrypted (1987-05-13)
```

DOI: https://doi.org/10.54216/JCIM.160212
Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

```
        }
    }
```

(h) The verifier proceeds to validate the zk-STARK proof off-chain to avoid high gas fees on Ethereum. This verification step confirms the authenticity and integrity of the encrypted data while ensuring that no sensitive information is revealed.

(i) If the zk-STARK proof passes verification, the verifier can confidently authenticate the user's identity and grant them access to the requested service. Should the proof fail, the user's access is denied, as the verifier cannot confirm the identity.

5 Discussion

The Table 3 offers an in-depth comparative analysis of the proposed identity management framework—which integrates Blockchain, zk-STARKs, and IPFS against existing related solutions. Each work is assessed based on its technical characteristics, including privacy protection, scalability, quantum resistance, and data integrity. This comparative evaluation demonstrates how our framework distinguishes itself by delivering a secure, decentralized, and forward-looking identity management system.

Table 3: Comparison between the Proposed Identity Management Framework (Blockchain, zk-STARKs, and IPFS) and Related Approaches

H: High; M: Moderate; L: Low

Feature	**Proposed System**	**32**	**18**	**35**	**19**	**6**
Privacy Preservation	H	M	L	H	M	M
Quantum Resistance	H	L	-	M	M	L
Setup Transparency	H	L	L	H	M	M
On-Chain Data Minimization	H	M	M	M	H	M
Verification Speed	H	M	M	H	M	L
Scalability	H	L	M	M	M	L
User Control & Decentralization	H	M	L	H	H	M
Security	H	M	L	H	H	M
Interoperability	H	M	L	M	M	M
Cost Efficiency	H	L	M	H	M	M
Data Immutability & Integrity	H	M	L	H	H	M

The proposed architecture functions as a prototype that addresses several shortcomings identified in traditional identity management systems. By integrating Blockchain, zk-STARKs, and IPFS, it enhances critical features such as privacy, scalability, and decentralization. While not yet fully deployed or tested, this framework exhibits substantial advantages in key performance areas.

In terms of privacy protection, the system significantly outperforms many existing solutions through the use of zk-STARKs, which provide zero-knowledge verification of identity attributes. This approach eliminates the need for revealing sensitive information during authentication. In contrast, several existing systems that utilize zk-SNARKs or similar cryptographic methods still rely on trusted setups that may expose user data to third parties[18].[32]

A major distinction lies in quantum resistance. The system's reliance on zk-STARKs, which inherently resist quantum-based attacks, sets it apart from alternatives that depend on elliptic curve cryptography, as noted in studies such as.[19] While these related solutions address current security needs, they remain vulnerable to future quantum computing developments. Our system's integration of quantum-resistant cryptography ensures a more durable and future-ready identity management platform.[35]

Setup transparency is another key advantage of our design. By removing the need for a trusted setup phase, the architecture eliminates reliance on centralized trust anchors. This transparent structure, enabled by zk-STARKs, minimizes single points of failure and strengthens overall system trustworthiness. In contrast, many related identity management approaches still depend on trusted setup phases, introducing potential vulnerabilities.[6]

An important feature of our system is the minimization of on-chain data. Only essential information—such as the IPFS hash and the user's DID—is recorded on the blockchain. This approach limits on-chain data exposure and prevents blockchain bloat, offering a distinct advantage over systems

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

that store verifiable credentials or sensitive data directly on-chain[18].[35] Storing user data off-chain on IPFS while maintaining robust on-chain verification strikes an effective balance between security and efficiency.

Scalability is another strength of our framework. By leveraging zk-STARKs, the system can efficiently process large datasets without performance degradation. The distributed nature of IPFS ensures that large files are stored and accessed without burdening the blockchain itself. This scalability is not commonly found in systems using zk-SNARKs, which can face performance issues under high computational demand[32].[18]

User autonomy and decentralization are enhanced through the incorporation of decentralized identifiers and off-chain storage using IPFS, giving users direct control over their data. This approach contrasts sharply with systems relying on centralized infrastructures, as discussed by Anusuya,[6] which restrict user control and introduce additional risks. Our decentralized architecture empowers users to manage their identities independently of third parties.

From a security perspective, the system's use of zk-STARKs delivers robust cryptographic guarantees without requiring a trusted setup, unlike other solutions that still depend on potentially vulnerable trusted setups.[6] This ensures a more resilient security posture against modern and future threats, including quantum attacks.

Our system also excels in interoperability. By incorporating open standards such as DIDs and zk-STARKs, it is compatible with a variety of decentralized applications. In comparison, the BiDaas platform, despite its decentralization, struggles to seamlessly integrate with other ecosystems due to its verification method dependencies. Our framework's flexibility makes it ideal for identity verification across multiple platforms.

Cost efficiency is another important advantage. By reducing on-chain storage through the use of IPFS, we lower transaction costs typically associated with identity verification. Systems that retain significant on-chain data tend to incur higher expenses, particularly for large-scale operations. Moreover, zk-STARKs offer computational efficiency, further reducing the costs of deploying and verifying identity proofs.

Finally, data integrity and immutability are core strengths of this architecture. By combining zk-STARKs for secure cryptographic proofs with IPFS for distributed data storage, our system ensures that once data is submitted, it cannot be altered without detection. This is a critical improvement over centralized systems like those described in,[6] where single points of failure can compromise data integrity. In our design, data immutability and security are inherently decentralized.

In summary, the integration of Blockchain, zk-STARKs, and IPFS within our proposed architecture represents a forward-looking and highly scalable approach to digital identity management. This combination of advanced cryptography, quantum-resistant security, and decentralized storage addresses many challenges inherent in current systems, positioning our framework as a secure, user-centric solution for the evolving digital landscape.

6 Future Work

In the next phase of this research, we plan to develop and implement a prototype of the zk-STARK and IPFS-based identity management system to validate its practical application and performance. The proof-of-concept will showcase how zk-STARK proofs can be integrated with IPFS for secure, decentralized identity management with a distributed storage. Through this PoC, we aim to demonstrate how users can generate and control DIDs, manage verifiable credentials, and interact with service providers without revealing sensitive information. The system's privacy-preserving capabilities will be rigorously tested, particularly in challenge-response scenarios, to assess how zk-STARKs effectively protect user data during verification processes. The prototype will also evaluate key performance metrics such as verification speed, transaction costs, and overall scalability in high-traffic environments. By testing the system's ability to handle large-scale identity verifications, we will assess the benefits of using IPFS for off-chain storage and zk-STARKs for quantum-resistant privacy protection. This future work will provide valuable insights into the real-world potential of this architecture, guiding further refinements and enhancements for secure and scalable identity management solutions.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

References

[1] Eli ben-sasson et al. scalable, transparent, and post-quantum secure computational integrity. *Tech. rep. 046. 2018*, 2018.

[2] ATT Data Breach: Nearly ALL Customers Have Phone Records Stolen. https://news.trendmicro.com/2024/07/15/att-data-breach-110-million/, 2024. [Online; accessed 24-Octobre-2024].

[3] FBCS Breach Exposes Millions, Comcast and Truist Bank Affected. https://socradar.io/fbcs-breach-exposes-millions-comcast-and-truist-bank/, 2024. [Online; accessed 24-Octobre-2024].

[4] Lawrence Abrams. Trello API abused to link email addresses to 15 million accounts. https://www.bleepingcomputer.com/news/security/trello-api-abused-to-link-email-addresses-to-15-million-accounts/, 2024. [Online; accessed 24-Octobre-2024].

[5] Md. Rayhan Ahmed, A. K. M. Muzahidul Islam, Swakkhar Shatabda, and Salekul Islam. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. *IEEE Access*, 10:113436–113481, 2022.

[6] R. Anusuya, D. Karthika Renuka, S. Ghanasiyaa, K. Harshini, K. Mounika, and K. S. Naveena. *Privacy-Preserving Blockchain-Based EHR Using ZK-Snarks*, page 109–123. Springer International Publishing, 2022.

[7] Mauricio Barros, Frederico Schardong, and Ricardo Custódio. Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass, 02 2022.

[8] Insaf Boumezbeur, Karim Zarour, Dounia Keddari, Farah Boutouatou, Yasser Nassim Benzagouta, Imane Harkat, and Seghiri Meriem. Secure ehr sharing using blockchain and ipfs. 42:1–14, 07 2024.

[9] Sopan Deb. Ticketmaster Confirms Data Breach. Here's What to Know. https://www.nytimes.com/2024/05/31/business/ticketmaster-hack-data-breach.html, 2024. [Online; accessed 24-Octobre-2024].

[10] Shalini Dhar, Ashish Khare, Ashutosh Dhar Dwivedi, and Rajani Singh. Securing iot devices: A novel approach using blockchain and quantum cryptography. *Internet of Things*, 25:101019, 2024.

[11] Mohammed El-hajj and Bjorn Roelink. Evaluating the efficiency of zk-snark, zk-stark, and bulletproof in real-world scenarios: A benchmark study. *Information*, 15:463, 08 2024.

[12] Desmond Kong Ze Fong, Vinesha Selvarajah, and M.S. Nabi. Secure server storage based ipfs through multi-authentication. In *2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC)*, pages 1–7, 2022.

[13] Rishabh Garg. *Blockchain Ecosystem*, pages 23–42. 2023.

[14] Giancarlo Giuffra. A summary of scalable, transparent, and post-quantum secure computational integrity, 08 2019.

[15] Yinjie Gong, Yifei Jin, Yuchan Li, Ziyi Liu, and Zhiyi Zhu. Analysis and comparison of the main zero-knowledge proof scheme. In *2022 International Conference on Big Data, Information and Computer Network (BDICN)*, page 366–372. IEEE, January 2022.

[16] Jennifer Gregory. National Public Data breach publishes private data of 2.9B US citizens. https://securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citizens/, 2024. [Online; accessed 24-Octobre-2024].

[17] Bo Jiang, Ye Liu, and W.K. Chan. Contractfuzzer: Fuzzing smart contracts for vulnerability detection. In *2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE)*, pages 259–269, 2018.

[18] Jong-Hyouk Lee. Bidaas: Blockchain based id as a service. *IEEE Access*, 6:2274–2278, 2018.

[19] Shailaja Lohar. Decentralization of identity using ethereum and ipfs. *Communications on Applied Nonlinear Analysis*, 31(4s):378–391, July 2024.

[20] Shengchen Ma and Xing Zhang. Integrating blockchain and zk-rollup for efficient healthcare data privacy protection system via ipfs. *Scientific Reports*, 14:11746, 05 2024.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025

[21] Khalid Maidine and Ahmed El-Yahyaoui. Cloud identity management mechanisms and issues. In *2023 IEEE 6th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, pages 1–9, 2023.

[22] Bhabendu Kumar Mohanta, Soumyashree S Panda, and Debasish Jena. An overview of smart contract and use cases in blockchain technology. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–4, 2018.

[23] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

[24] Andreea-Elena Panait and Ruxandra F. Olimid. *On Using zk-SNARKs and zk-STARKs in Blockchain-Based Identity Management*, page 130–145. Springer International Publishing, 2021.

[25] Vilius Petkauskas. Details of 20M Cutout.pro users exposed on leak forum. `https://cybernews.com/news/cutoutpro-leak-exposed-millions-users/`, 2024. [Online; accessed 24-Octobre-2024].

[26] Tushar Richabadas. Dell: 49 million customer records exposed in 1 automated attack. `https://blog.barracuda.com/2024/05/23/49-million-customer-records-exposed-in-1-automated-attack`, 2024. [Online; accessed 24-Octobre-2024].

[27] Will Schmidt. THE CHANGE HEALTHCARE CYBER ATTACK. `https://www.pcgsoftware.com/ransomware-unitedhealth-group-and-change-healthcare`, 2024. [Online; accessed 24-Octobre-2024].

[28] Twingate Team. Spoutible Data Breach: What How It Happened? `https://www.twingate.com/blog/tips/Spoutible-data-breach/`, 2024. [Online; accessed 24-Octobre-2024].

[29] Atharva Thorve, Mahesh Shirole, Pratik Jain, Crehan Santhumayor, and Soham Sarode. Decentralized identity management using blockchain. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pages 1985–1991, 2022.

[30] Zhiwei Wang, Qingqing Chen, and Lei Liu. Permissioned blockchain-based secure and privacy-preserving data sharing protocol. *IEEE Internet of Things Journal*, 10(12):10698–10707, 2023.

[31] Craig S Wright. Bitcoin: A peer-to-peer electronic cash system. *SSRN Electronic Journal*, 2008.

[32] Xiaohui Yang and Wenjie Li. A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers Security*, 99:102050, 2020.

[33] Xiangfu Zhao, Zhongyu Chen, Xin Chen, Yanxia Wang, and Changbing Tang. The dao attack paradoxes in propositional logic. In *2017 4th International Conference on Systems and Informatics (ICSAI)*, pages 1743–1746, 2017.

[34] Peilin Zheng, Zigui Jiang, Jiajing Wu, and Zibin Zheng. Blockchain-based decentralized application: A survey. *IEEE Open Journal of the Computer Society*, 4:121–133, 2023.

[35] Xinjie Zhu, Debiao He, Zijian Bao, Min Luo, and Cong Peng. An efficient decentralized identity management system based on range proof for social networks. *IEEE Open Journal of the Computer Society*, PP:1–12, 01 2023.

DOI: https://doi.org/10.54216/JCIM.160212

Received: January 01, 2025 Revised: March 03, 2025 Accepted: April 01, 2025