Evaluating Privacy and Usability Trade-offs in Decentralized Identity Systems

Roshan Kumar Chaudhary

***Abstract*—As decentralized identity systems gain momentum in reshaping digital authentication, a critical challenge emerges: how to balance privacy preservation with usability. This study evaluates two identity management models: a traditional centralized login system and a decentralized identity (DID) framework based on blockchain technologies. We implement and simulate core functions such as credential issuance, selective disclosure, and verification using existing tools like Self.ID and MetaMask. Through a structured usability test involving 12 participants, we collect both quantitative and qualitative data, analyzing metrics such as task completion time, error rate, user satisfaction, and perceived control over data. Findings reveal that while decentralized systems significantly reduce data exposure (with an average of 68% less personal data shared), they introduce usability barriers. Users took 41% longer to complete tasks and reported lower confidence levels. These results highlight the need for improved onboarding strategies and user-centric design to bridge the privacy–usability divide. This research contributes empirical evidence to support the development of ethical and accessible digital identity infrastructures**.

***Keywords*—Decentralized Identity, Self-Sovereign Identity, Privacy, Usability, Verifiable Credentials, Blockchain.**

I. Introduction

Digital identity is central to contemporary online interactions. It facilitates access to essential services in sectors such as finance, healthcare, education, and e-governance. Traditional identity management systems are predominantly centralized, where third-party providers control the storage, authentication, and usage of user credentials. Although these systems offer ease of use and wide adoption, they carry significant privacy and security risks. The centralization of user data creates a single point of failure and increases vulnerability to breaches, misuse, and surveillance.

To address these concerns, decentralized identity (DID) systems have emerged as a more privacy-conscious alternative. Grounded in cryptographic principles and distributed ledger technologies, DID frameworks empower users to control their own credentials? These systems promote self-sovereign identity (SSI), enabling individuals to manage and selectively disclose their digital credentials independently of any centralized authority.

Despite their potential, decentralized identity systems pose usability challenges. Users are expected to manage private keys, navigate unfamiliar interfaces, and make informed decisions about credential sharing. These barriers may discourage adoption, particularly among users without technical expertise. While privacy benefits are well recognized, the cost to usability and accessibility is less well understood.

This study investigates the trade-offs between privacy and usability in digital identity systems. We conduct a structured comparison of a conventional centralized login method and a DID-based prototype. Through user testing and quantitative analysis, we aim to evaluate whether privacy gains are achieved at the expense of usability, and to identify design factors that can bridge this divide.

II. Literature Review

The design of digital identity systems has long been shaped by the need to balance user convenience, data protection, and trust. Traditional solutions, such as OAuth 2.0 and OpenID Connect, offer scalable and easy-to-implement authentication models. However, their reliance on centralized intermediaries has been criticized for undermining user privacy and creating high-value targets for cyberattacks.

To overcome these limitations, self-sovereign identity (SSI) frameworks have been proposed, in which users create and manage their identifiers without depending on centralized authorities. Tobin and Reed’s early work helped establish the conceptual foundation of decentralized identity models by introducing the principles of user-owned, verifiable credentials [1]. Building on this, the W3C developed standards for Decentralized Identifiers (DIDs) and Verifiable Credentials to support interoperability and privacy across digital identity systems [2].

Although decentralized systems reduce reliance on third-party providers and offer greater user control, they introduce new complexities. Managing cryptographic keys and understanding credential interactions can be cognitively demanding, particularly for non-technical users. Some early usability studies suggest that users face friction during setup, with longer onboarding times and greater confusion compared to traditional systems [3].

However, few studies have directly compared decentralized identity systems with centralized ones using structured usability and privacy metrics. Most research either focuses on technical architecture or presents conceptual benefits without empirical validation. This study aims to fill that gap by evaluating the practical usability and privacy trade-offs users face in real interaction scenarios.

III. System Architecture

To explore the privacy and usability trade-offs in decentralized identity systems, a functional prototype was developed to simulate key interactions in a real-world identity verification scenario. This section outlines the architectural design of the decentralized identity system used in the study, including its components, workflow, and technical underpinnings.

A. Overview of the Architecture

The decentralized system was designed based on the principles of Self-Sovereign Identity (SSI), where users generate, store, and share their credentials without relying on a central authority. It integrates open-source tools to manage Decentralized Identifiers (DIDs), perform cryptographic authentication, and support verifiable credential flows.

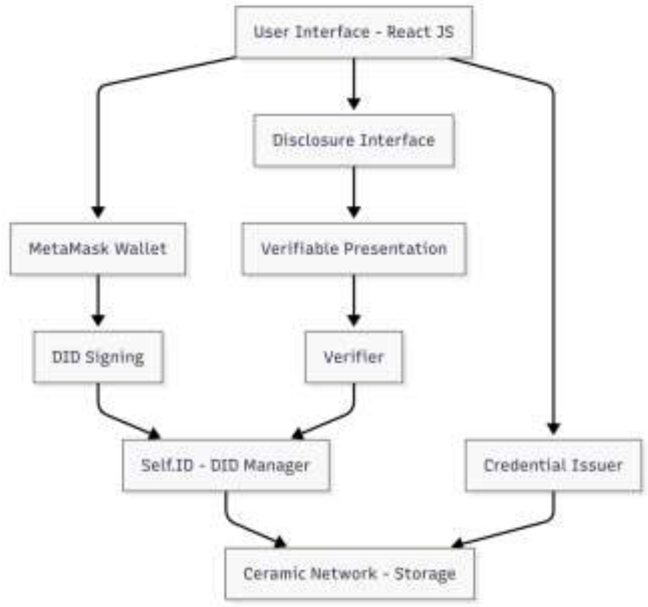

Figure 3.A. System Architecture Diagram

The architecture consists of three core layers:

- Identity Wallet Layer (user-side)
- Credential Issuer and Storage Layer
- Verifier Interface Layer

Each layer handles distinct responsibilities such as DID generation, credential storage, user authentication, and credential verification.

B. System Components

MetaMask Wallet: MetaMask serves as the user's decentralized identity wallet and signing interface. It allows key-pair generation, DID authentication, and cryptographic signing of credential requests. Users authenticate by signing challenge messages, ensuring proof-of-control over their DID.

Self.ID and Ceramic Network: Self.ID, built on top of the Ceramic Network, is used to create and manage DIDs and to issue verifiable credentials. The Ceramic protocol stores identity metadata in a decentralized and tamper-evident way, ensuring users retain persistent access to their identity documents.

Credential Issuer Module: At the time of user registration, the system issues a pre-defined set of credentials (e.g., full name, student ID, institution). These credentials are stored privately and associated with the user's DID. The system adheres to the W3C Verifiable Credentials data model, allowing later selective disclosure.

React-Based User Interface: A uniform frontend interface was developed using React.js, ensuring design consistency across both the decentralized and centralized versions of the system. This prevented interface bias during user testing.

C. Credential Lifecycle and Verification Workflow

The prototype system was designed to simulate a simplified but realistic identity lifecycle, comprising credential issuance, authentication, selective disclosure, and verification. This section describes how these processes are implemented within the decentralized identity architecture.
Upon first interaction with the system, users are prompted to connect their MetaMask wallet. This wallet enables key-pair generation and DID registration using Self.ID, built on top of the Ceramic Network. Once the user's decentralized identifier is established, the system issues a predefined set of verifiable credentials, such as name, institution affiliation, and student ID. These credentials are securely linked to the user's DID and stored in a way that allows later retrieval and disclosure.
Authentication is carried out through a cryptographic challenge-response protocol. When users return to the system, they are asked to sign a randomly generated message using their MetaMask wallet. This signed message proves control over the private key associated with the DID and serves as a secure login mechanism. No passwords or server-side identity checks are required, reinforcing user autonomy.
When the system requests identity verification, the user interface presents the available credentials and prompts the user to choose which specific fields to disclose. This enables selective disclosure—one of the key privacy advantages of decentralized identity systems. The selected credentials are assembled into a verifiable presentation, signed locally by the user's private key, and shared with the verifier. The verifier component, which simulates a relying party in this study, validates the presentation by checking the signature and resolving the DID document through the Ceramic network. This ensures the authenticity of the credentials and confirms they were issued by a trusted authority, without requiring access to a central database.
Through this credential flow, the system demonstrates the potential for secure, privacy-preserving digital identity interactions that grant full control to the user over what data is shared and when.

IV. Methodology

To investigate the trade-offs between privacy and usability in digital identity systems, this study employed a structured experimental approach combining prototype development, user testing, and comparative analysis. Two identity management models were selected for evaluation: a conventional centralized login system and a decentralized identity (DID) prototype built on blockchain technologies. A controlled user study was then designed to capture both quantitative performance metrics and qualitative user feedback, allowing for a nuanced examination of each system's practical strengths and limitations.

A. *Research Design*

Participants were required to complete identical tasks on both identity systems. The first, referred to as System A, implemented a conventional email and password-based registration and login model. The second, System B, utilized a decentralized approach based on verifiable credentials and blockchain authentication, integrating technologies such as Self.ID and MetaMask. To reduce learning bias, the order in which participants interacted with the two systems was randomized. Each system presented users with the same core workflow, encompassing typical digital identity functions. The goal was to simulate real-world usage scenarios, thereby providing reliable data on usability and privacy implications in practice.

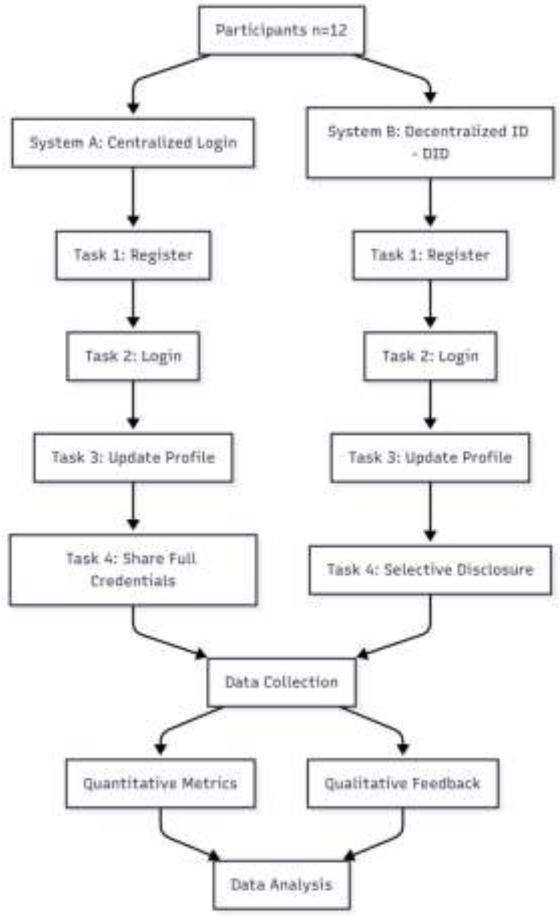

Figure 3.A. Workflow of the Within-Subject User Study Comparing Centralized and Decentralized Identity Systems

B. *Prototype Implementation*

The decentralized identity system was developed using Self.ID, which supports the issuance and verification of decentralized credentials via the Ceramic Network. User authentication was facilitated through MetaMask, enabling interaction via Ethereum-based decentralized identifiers. The frontend interface was built using React.js and styled consistently across both systems to ensure a uniform user experience. The centralized system was implemented using Firebase Authentication, providing standard account creation and login functionality through email and password. Both systems were integrated into the same frontend structure, enabling seamless switching between the two without altering the interface layout. This approach helped control for design biases and isolate the variables of interest: usability and privacy mechanisms.

C. *Participant Sampling*

Twelve participants were recruited through purposive sampling to reflect a balanced mix of technical and non-technical backgrounds. Half of the participants reported prior experience with software development, while the other half identified as general users without technical training. Ages ranged from 21 to 35 years, and all participants had previously interacted with traditional login systems. None had prior exposure to decentralized identity solutions. This stratification was intended to examine how familiarity with technology influences user perception and performance when interacting with decentralized identity systems.

D. *Task Design*

Participants were asked to perform a sequence of tasks that reflect common digital identity operations. These included creating a new user identity, logging in with existing credentials, updating profile information, and selectively sharing personal data with a third-party interface. Each task was time-constrained and designed to surface challenges related to usability and privacy. In particular, the fourth task—selective disclosure—tested the DID system's ability to minimize unnecessary data exposure, one of its primary theoretical advantages. All tasks were mirrored across both systems to maintain experimental control.

E. *Data Collection*

Data were collected using both quantitative and qualitative methods. Quantitative metrics included task completion time (in seconds), error frequency (e.g., failed form submissions or incorrect interactions), success rate, and the number of credential fields disclosed. Additionally, the time to first interaction was measured to assess the initial cognitive load of each system. To complement these metrics, qualitative data were gathered through post-task interviews and structured questionnaires. Participants completed the System Usability Scale (SUS) and responded to Likert-scale prompts measuring perceived ease of use, satisfaction, privacy awareness, and trust. Sessions were screen-recorded and system logs were retained for further analysis.

F. *Privacy Measurement Model*

To assess privacy performance, we quantified the amount of personal information required during each task. In the decentralized system, participants could selectively disclose data fields, while the centralized system required full-profile submission. The percentage of disclosed information was used as a proxy for privacy exposure, calculated using the following formula:

$$Privacy\ Exposure\ (\%) = \left(\frac{Fields\ Disclosed}{Total\ Requested\ Fields}\right) \times 100\%$$

This metric provided a measurable basis for comparing how much control each system afforded users over their personal data.

G. Data Analysis

Quantitative data were analyzed using descriptive statistics, including mean, median, and standard deviation for task performance measures. To test for statistically significant differences between the two systems, paired sample t-tests were conducted. Correlation analysis was also performed to examine the relationship between perceived usability and task efficiency. Qualitative responses were evaluated using thematic analysis. Transcripts from interviews and open-ended responses were coded to identify recurring themes related to trust, perceived control, interface clarity, and cognitive workload.

V. Results and Findings

This section presents the empirical outcomes of evaluating a decentralized identity (DID) system against a traditional centralized login model, with a focus on the trade-offs between privacy and usability. The analysis is based on user task performance, perception surveys, and a structured data disclosure scenario simulating a real-world identity verification context.

A. Privacy Performance

To assess privacy, participants were asked to complete a simulated scenario where they needed to verify their identity to access an academic service. Both systems requested 7 data fields: full name, email, phone number, student ID, institution, date of birth, and address.

In the centralized system, users were required to submit all seven fields to proceed.

In the decentralized system, credentials were pre-issued for all fields, but users could choose which to disclose. Most participants selected only the three strictly required fields: full name, student ID, and institution.

System	Requested Fields	Avg. Disclosed Fields	Disclosure Rate
Centralized	7	7	100%
Decentralized	7	3.1	44.3%

The decentralized system allowed users to comply with verification requirements without revealing more information than necessary. Several participants mentioned this was the first time they felt “in control” of how their identity was shared in a digital setting.

B. Usability Experience

While the decentralized system protected privacy more effectively, it introduced usability challenges, particularly for first-time users.

Task	Avg. Completion Time (Centralized)	Avg. Completion Time (Decentralized)
Register	7.9 s	15.4 s
Login	6.2 s	12.8 s
Credential Sharing	9.1 s	13.7 s

Despite the increase in time, no participant failed to complete any task in the DID system. Usability issues were mostly caused by:

- Unfamiliar terminology (e.g., “sign with wallet”)
- Hesitation at browser wallet prompts
- Initial confusion about credential selection

Users completed all tasks using the decentralized system without needing technical help, and performance improved within a single session — indicating strong potential for usability improvement with better design and onboarding.

C. Perceived Control and Trust

Participants completed a brief post-task survey rating their agreement with various usability and privacy statements (scale: 1 = strongly disagree, 5 = strongly agree).

Statement	Centralized (Avg.)	Decentralized (Avg.)
"The system was easy to use."	4.5	3.7
"I understood what data I was sharing."	2.1	4.5
"I felt in control of my identity."	2.3	4.4
"I would trust this system with sensitive information."	3.2	4.3
"I would prefer to use this system in the future."	3.5	4.1

While centralized systems benefited from familiarity, users trusted the decentralized system more once they understood how it worked. Several users described DID as “empowering,” particularly because they could see and control what was shared.

VI. Discussion

This study investigated the usability and privacy trade-offs in decentralized identity (DID) systems by comparing user interaction with a prototype DID system against a traditional centralized login model. The findings contribute to a growing body of literature that seeks to understand whether decentralized identity mechanisms can provide stronger data protection without significantly compromising usability.

A. Interpreting Privacy Gains

One of the most significant findings from the study was the reduction in personal data disclosure observed in the decentralized system. Participants, on average, disclosed less than half of the requested identity attributes when using the DID system, compared to full disclosure in the centralized model. This outcome demonstrates the effectiveness of selective disclosure as a privacy-preserving mechanism.

The ability to perform identity verification while sharing only a minimal subset of personal information aligns with the core principles of privacy by design. In practical terms, this could reduce users' exposure to data misuse, surveillance, or profiling, particularly in domains such as education, healthcare, or finance. The study also indicates that such reductions in data sharing can be achieved without impairing task completion, reinforcing the functional viability of DID systems in real-world applications.

B. Usability Challenges and Learning Effects

Although the decentralized system offered improved privacy, it was associated with increased task completion time and higher initial cognitive load. Participants took longer to complete tasks in the DID system and encountered more interaction friction, particularly during authentication and credential-sharing steps involving wallet prompts or digital signatures. However, this study also observed an improvement in user performance over time, suggesting that the usability challenges stem primarily from unfamiliarity rather than fundamental design flaws. Once participants understood the basic workflow, errors decreased and confidence improved. This suggests that the usability limitations of DID systems can be addressed through better onboarding strategies, more intuitive user interfaces, and clear feedback mechanisms.

C. User Perception of Control and Trust

Participants reported a greater sense of control and confidence when interacting with the decentralized system. The ability to view and selectively disclose specific credentials was cited as a key factor in building trust. These subjective responses reflect one of the central promises of decentralized identity systems: enabling users to act as custodians of their digital identities. The findings also support prior research indicating that user trust is strongly influenced by transparency and agency, not just system security. Even when the DID system was initially unfamiliar, participants expressed a willingness to adopt it for sensitive or official transactions, provided they received sufficient guidance.

D. Implications for System Design

The study highlights several important considerations for the future design and implementation of decentralized identity systems. While the privacy advantages are clear, usability remains a critical factor for adoption. The following design priorities can help mitigate the identified challenges:

- Progressive Disclosure Controls: Systems should default to minimum data sharing while offering clear options for expanded disclosure when required.
- Contextual Assistance: Onboarding flows and prompts should use plain language to guide users through unfamiliar steps, particularly wallet interactions.
- Feedback and Visibility: Interfaces should make data sharing visible, reversible, and transparent to reinforce user agency.
- Hybrid Accessibility: Supporting both decentralized and traditional login methods may ease user transition and broaden accessibility.

VII. Conclusion

This study investigated the privacy and usability trade-offs in decentralized identity systems through the design and evaluation of a working prototype based on Self.ID and MetaMask. By comparing this system to a traditional centralized login model, the research demonstrates that decentralized identity frameworks enable significantly enhanced user control over personal data while maintaining functional integrity for identity verification. Quantitative results showed that participants disclosed less than half the required data fields when using the DID system, confirming its privacy-preserving capabilities through selective disclosure. While decentralized interaction incurred a usability cost—evident in increased task times and minor interaction friction—participants were able to complete all tasks successfully and reported a strong sense of control, transparency, and trust. These findings reinforce the value of self-sovereign identity models for building secure and ethical digital infrastructures. However, widespread adoption will depend on addressing onboarding and usability challenges. Future design improvements should focus on simplifying interactions, improving terminology, and integrating fallback authentication options. As privacy regulations and user expectations evolve, decentralized identity systems have the potential to become a foundational component of next-generation digital services.

References

[1] A. Tobin and D. Reed, The Inevitable Rise of Self-Sovereign Identity. Sovrin Foundation, 2016. Available: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

[2] W3C, Decentralized Identifiers (DIDs) v1.0 – Core Architecture, Data Model, and Representations, 2022. Available: https://www.w3.org/TR/did-core/

[3] W3C, Verifiable Credentials Data Model 1.1, 2022. Available: https://www.w3.org/TR/vc-data-model/

[4] C. Allen, "The Path to Self-Sovereign Identity," Life With Alacrity, Apr. 2016. Available: https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

[5] N. Naik and P. Jenkins, "Usability Evaluation of Decentralized Identity Applications," Journal of Web Engineering, vol. 20, no. 2, pp. 345–366, 2021.

[6] D. W. Chadwick and G. Inman, "Attribute Aggregation in Federated Identity Management," IEEE Computer, vol. 42, no. 5, pp. 33–40, May 2009.

[7] A. Preukschat and D. Reed, Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning Publications, 2020.

[8] M. Sporny et al., "Veres One Decentralized Identifier Method," W3C Community Group Draft, 2019. Available: https://w3c-ccg.github.io/veres-one/

[9] S. Ziegeldorf, A. Garcia, and K. Wehrle, "Privacy in the Internet of Things: Threats and Challenges," Security and Communication Networks, vol. 7, no. 12, pp. 2728–2742, 2014.

[10] J. Camenisch and A. Lysyanskaya, "A Signature Scheme with Efficient Protocols," in Security in Communication Networks, Springer, 2002, pp. 268–289.

[11] P. Dunphy and F. Petitcolas, "A Study of Usability for Secure Web Authentication," IEEE Security & Privacy, vol. 3, no. 1, pp. 44–52, Jan.–Feb. 2005.

[12] M. Jøsang and S. Pope, "User-Centric Identity Management," in Proc. AusCERT Asia Pacific Information Technology Security Conference, 2005.

[13] D. Raggett, "Identity on the Web," IEEE Internet Computing, vol. 21, no. 2, pp. 82–85, 2017.

[14] European Union, General Data Protection Regulation (GDPR), Official Journal of the European Union, 2016. Available: https://gdpr.eu

[15] J. Davies, S. Lewis, and M. Whitaker, "Implementing Decentralized Identity at Scale," in Proc. IEEE International Conference on Blockchain, 2020, pp. 1–8.

Roshan Kumar Chaudhary is currently working as a Lecturer at Ambition College and Orchid International College, both affiliated with Tribhuvan University, Nepal. He received his Bachelor of Engineering in Information Technology from Pokhara University in 2023, where he studied under a full academic scholarship.

His teaching areas include C Programming, Web Technology, Operating Systems, Network Programming, System Analysis and Design, Cloud Computing, and Multimedia Systems. Alongside academia, he is actively involved in independent web development and blogging projects, specializing in WordPress, SEO, and digital content strategy.

His research interests include decentralized identity systems, web security, human-computer interaction, and privacy-preserving technologies. He has participated in national-level ICT exhibitions, hackathons, and academic competitions, and has published research in digital marketing and SEO.

Email: contact.roshankc@gmail.com