Blockchain-Based Mobile Digital Identification for Older Adults in Peru

Wilver Arana
Department of Engineering Faculty, Software Engineering, Universidad Peruana de Ciencias Aplicadas, Lima, Peru
u202023992@upc.edu.pe

Aldo Pastrana
Department of Engineering Faculty, Software Engineering, Universidad Peruana de Ciencias Aplicadas, Lima, Peru
u20211c186@upc.edu.pe

Juan Lopez
Department of Engineering Faculty, Information Systems Engineering, Universidad Peruana de Ciencias Aplicadas, Lima, Peru
juan.lopez@upc.edu.pe (corresponding author)

Received: 18 December 2025 | Revised: 29 January 2026 and 12 March 2026 | Accepted: 23 March 2026

 DOI: https://doi.org/10.48084/etasr.17039

ABSTRACT

The transition of key services to digital platforms has increased demand for secure, accessible digital identification mechanisms. Older adults, particularly in rural and low digital literacy contexts, face important barriers to adopting such systems. This study presents the design, implementation, and pilot validation of a blockchain-based mobile digital identification system tailored for older adults. The solution integrates a Flutter mobile application, a Spring Boot backend, and Ethereum smart contracts to ensure secure identity registration and auditability. A user-centered design methodology was applied, followed by iterative pilot evaluations. Usability was assessed using the System Usability Scale (SUS) with older adults (n = 16), obtaining a mean score of 60.78 (SD = 13.68), indicating acceptable usability. In post-use evaluations (n = 41), participants completed 100% of planned tasks with high satisfaction (5/5 in the second round; NPS +100). From a performance perspective, system latency met the non-functional requirement of under 2 s, with observed p50 ≈ 500 ms and p95 ≈ 1500 ms under good network conditions. Blockchain anchoring successfully generated verifiable transaction hashes for identity registration and audit events, ensuring traceability and integrity. The results demonstrate the technical feasibility, usability, and auditability of a blockchain-based digital identification system designed specifically for older adults, contributing to digital inclusion in rural municipal contexts.

Keywords-blockchain; digital identification; older adults; mobile application; usability; accessibility; digital inclusion

I. INTRODUCTION

Increased digitization and the integration of emerging technologies have significantly transformed many aspects of daily life, providing fast and effective access to essential services in key areas such as health, education, and public services. However, this technological evolution has led to growing digital exclusion of vulnerable groups, particularly older adults, who face technological and cognitive barriers that hinder their full integration into the digital society [1, 2]. Digital identification, as a central component of digital inclusion, plays a crucial role in ensuring the security and privacy of online interactions [3]. In this context, the development of accessible and reliable solutions for the digital authentication of older adults has become a goal not only of technology but also of social development, particularly due to the potential of decentralized technologies such as blockchain to offer total control over user identity and minimize risks associated with traditional centralized systems [4]. Blockchain is a technology that ensures that, once recorded, it is virtually impossible to alter a transaction without the network detecting it.

Despite the great potential of blockchain technology to offer a robust solution for decentralized identity management, the implementation of these solutions in the context of older adults still presents multiple challenges. The main obstacles include unfamiliarity with digital technologies, low digital

literacy, and concerns about privacy and security [5]. As digitization continues to advance, it is essential to address these gaps by developing mobile applications that are easy to use, secure, and accessible to this age group [6]. In addition, although various initiatives have proposed blockchain-based digital identity solutions, many of them are not specifically geared toward the needs of older adults, implying a significant gap in the research and development of accessible systems tailored to this population. The present study addresses these discrepancies.

The primary objective of this study is to develop a mobile application for digital identification using blockchain, designed specifically for older adults [6]. The study explores the technical, social, and design aspects necessary to create an effective solution that facilitates older adults' access to digital services, while also protecting user privacy. The analysis focuses on the implementation and design of architecture that combines ease of use with the robustness of the security mechanisms inherent in blockchain technology [7]. The methodological approach adapted in this research combines agile development techniques and user-centered design frameworks, with a specific focus on digital inclusion and accessibility [8]. Theories of interface design and human-computer interaction are used to ensure that the application interface is intuitive and appropriate for the cognitive and technological capabilities of older adults [9]. In addition, blockchain is used not only to guarantee the authenticity of identities but also to provide a transparent, secure, and decentralized system that allows users to control data without relying on centralized entities [10].

This study provides an overview of how emerging technologies can be effectively applied to improve the digital inclusion of older adults in rural contexts [11]. The study promotes the development of new mobile applications focused on digital identity and provides a framework for future research in this field, promoting equitable access to digital services and ensuring privacy and security in the use of advanced technologies [12]. In particular, this work focuses on rural municipalities in Peru, where older adults face structural barriers to accessing both traditional and digital identification systems. The findings suggest that a blockchain-based digital identification mobile application, designed specifically for older adults, has the potential to address these limitations and contribute to digital inclusion in the Peruvian public service ecosystem.

II. MATERIALS AND METHODS

A. Methodological Context

The project adopts an applied engineering approach to design and implementation, with a specific focus on older adults in rural areas. The choice of a decentralized model responds to the limitations of traditional identity schemes (single points of failure, lack of user control, limited traceability) and the advantages of Self-Sovereign Identity (SSI) and Distributed Ledger Technology (DLT) approaches to ensure the integrity, authenticity, and verifiability of credentials across multiple public and social service domains.

Blockchain provides immutability, resistance to manipulation, and distributed governance for identity management. In addition, SSI gives people back control over the lifecycle of their attributes and identifiers, with authentication, integrity, privacy, trust, and simplicity as the design pillars of a Modern Digital Identity Management System (IDMS) [1]. The comparisons of decentralized approaches underscore the usefulness of combining DLT for transactional events and distributed storage for volumetric data, as well as the performance challenges in DIDs, which must be mitigated through architecture and user experience [5]. In terms of authentication, Web3 mechanisms on Ethereum illustrate benefits over centralized OAuth2 by eliminating intermediaries, giving users greater control over their data, and allowing proof of possession with signatures instead of passwords, all with modern interfaces to improve usability [13].

Given that the target population is older adults, the methodology also draws on technology adoption frameworks (TAM/UTAUT) to guide design decisions toward perceived usefulness, ease of use, and enabling conditions (e.g., support from providers/authorities), factors that predict intention and effective use in this group [6, 7]. Evidence on barriers/enablers in older adults (digital literacy gaps, physical/cognitive limitations, privacy concerns, and the critical role of healthcare personnel or local actors) informs co-design, training, and accessibility strategies incorporated into the method [3, 2]. Finally, usability requirements for senior-friendly apps (readability, simple navigation, recoverable errors, voice commands) are integrated as design criteria [8].

B. Selection of Techniques and Tools

1) Blockchain and Smart Contracts

Ethereum is used to record and verify digital identities and access/query audits, taking advantage of its decentralization, immutability, and mature support for smart contracts. Integration is performed through the Web3 interface from the API, storing the transaction hash as irrefutable proof of registration. The Web3 literature supports increased security and user control in decentralized authentication schemes [13].

2) Mobile Platform

The frontend is developed with Flutter for its native performance, agile development cycle, and ability to generate accessible and consistent interfaces on Android/iOS, which are critical for older adults. Senior-friendly design recommendations (large text, high contrast, shallow menus, clear error messages, voice support) guide the components [8].

3) Backend and API

Spring Boot (Java) is used with a layered architecture (REST controllers, domain services, JPA repositories), due to their robustness, scalability, and ease of maintenance. Endpoint security is managed with Spring Security and JSON Web Tokens (JWT); roles restrict critical functions (e.g., service management by local authority).

4) Data and Storage

Operational information (e.g., essential service catalog, user metadata) resides in MySQL due to its ability to handle large volumes with high availability and scalability, while critical events (ID creation, authority queries) are backed up on the chain for traceability.

5) Domain Design Methodology

Domain-Driven Design (DDD) is adopted to align the software model with the language and rules of the social and municipal domain, segmenting the system into defined contexts and promoting consistency between frontend and backend.

C. Implementation Environment: Local Governance and Technology Stack

The pilot project is being carried out with the Municipality of Canta as a collaborating entity and uses Scrum for iterations with early validation, addressing connectivity and adoption risks through community awareness and training. Table I summarizes the technology stack implemented in the digital identification system, highlighting the main technologies used in the frontend, backend, and data storage. In addition, it details the key experimental parameters that guide its development, with special emphasis on accessibility, security, and usability, adapted to the needs of older adults.

TABLE I. TECHNOLOGY STACK AND EXPERIMENTAL PARAMETERS OF THE SYSTEM

Layer/ Module	Main technologies	Key experimental parameters
Mobile frontend	Flutter	Senior-friendly guidelines: large font size, high contrast, simplified navigation, and clear error messages
API/Backend	Spring Boot (Java), Spring Security, JWT, JPA	Layered architecture: roles for critical functions, target latency < 2s with good connectivity
Data	MySQL	Relational schema for catalog and metadata: high availability and scalability
Blockchain	Ethereum, Web3 (from API)	ID registration/verification and auditing: transaction hash storage as proof
Domain	DDD	Delimited contexts; ubiquitous language; aggregates: Resident, Identification, Authority, Service
Process	Scrum	Iterations with early validation: mitigation of connectivity and adoption risks through training

D. Methodological Procedure

1) Requirements Elicitation and Context Analysis

Functional requirements (blockchain registration/verification, digital ID generation, access to services, traceability of queries) and non-functional requirements (response time < 2s on a good network, accessible design) were identified.

2) Domain Modeling

This stage defines key entities (Resident, Identification, Authority, and Service), aggregates, and policies, and establishes a ubiquitous language in agreement with local experts.

3) Architecture Design

This stage involves the decomposition into a mobile client (Flutter), a REST API (Spring Boot), a relational database (MySQL), and smart contracts on Ethereum. It also includes the specification of components, context diagrams, and containers.

4) Development and Integration

This stage involves backend implementation with JPA services and repositories, security with JWT/roles, frontend with accessible widgets and state management, Web3 integration for contract invocation (registration/verification), and transaction hash storage.

5) Iterative Testing

Unit, integration, and functional tests were performed on critical cases (on-chain registration, digital ID authentication, service registration, ID display/filtering) with defined acceptance criteria.

6) Deployment and Training

The deployment and training stage involves installation, use, and management guides. It also includes training sessions and audiovisual materials to mitigate digital literacy gaps in the target population, aligned with best practices for generational inclusion [2].

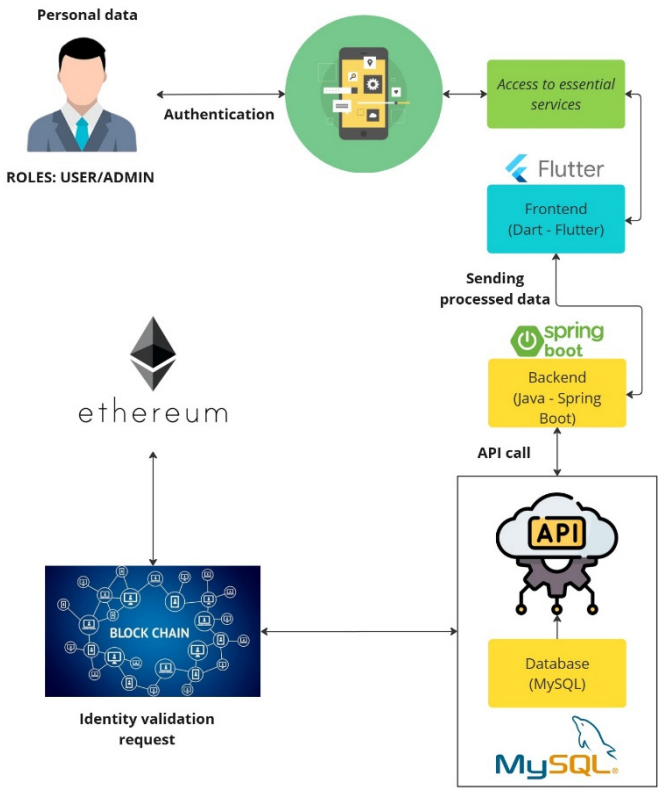


Fig. 1. High-level logical diagram of the system architecture.

E. System Architecture

The proposed architecture is based on a high-level vision that helps understand the main components and their interactions. Figure 1 shows the general logical diagram of the proposed solution, which represents the overall dynamics. The main layers that make up this architecture are:

1) Mobile App (Flutter)

Mobile app provides an accessible UI, data entry/query, a lightweight wallet for signature (when applicable), credential reading mode, HTTPS communication with API, and read caches for tolerance to intermittent connectivity.

2) API/Backend (Spring Boot)

API/Backend includes REST controllers, domain services for rules (creation of unique 8-digit ID, validations), persistence with MySQL, security with JWT, and role-based authorization.

3) Blockchain Layer (Ethereum)

The Ethereum smart contract records minimum digital ID attributes and audit events, transaction hash return, and verification queries.

4) Database (MySQL)

The database manages essential services, operational profiles, catalogs, and metadata, with a focus on horizontal scalability.

F. Validation

1) Strategy and Types of Testing

To ensure end-to-end reliability between API–DB–Blockchain and avoid regressions, a risk-based validation plan was adopted that combines unit, integration, functional, and acceptance testing on critical flows. Table II summarizes this plan and incorporates the key cases: CP-001 (on-chain resident registration), digital ID authentication with access to options, registration/consultation of essential services with observable criteria (e.g., HTTP 201 and valid Tx Hash), and behavior verification in the UI.

G. Metrics and Criteria

To evaluate non-functional and usage quality, metrics and thresholds were established in line with the risks of the pilot and ISO/IEC 25010 (usability) and senior-friendly guidelines [9]. Table III operationalizes parameters such as performance (UI < 2 s on a good quality network; NF-1), integrity/verifiability (presence and storage of Tx Hash in on-chain operations), security (JWT, role-based access control, traceability in blockchain; NF-5–6), usability/accessibility (readability, contrast, simplicity; formative testing with older adults), and scalability (controlled degradation with concurrency and low connectivity, with specific mitigations).

1) Functional and Traceability Results of the Pilot

The test results showed correct on-chain registration with hash, login with digital ID, and ID display/filtering, demonstrating functional and traceability compliance.

H. Comparison with Previous Work

The methodology aligns with evidence on decentralized ID and SSI as a way to overcome centralization failures and improve user control/privacy. The proposed work explicitly incorporates the five key components (authentication, integrity, privacy, trust, simplicity) proposed by the IDMS literature on blockchain [1]. It complements decentralized approaches by incorporating performance decisions (off-chain processing in MySQL + critical on-chain events) and role-based access controls, responding to latency and throughput challenges documented for DIDs [5].

TABLE II. E2E VALIDATION MATRIX BY LAYERS AND CRITICAL FLOWS

Item	Description (scope)	Success criteria
Unit tests	Services and DAOs	Coverage of critical components: assertions and error handling
Integration tests	API – DB –Blockchain	Fault-free E2E flow: data consistency between layers
Functional testing	Main use cases	Compliance with UI/API requirements
Acceptance testing	Critical flows with stakeholders	Approval in representative scenarios with real/synthetic data
CP-001 on-chain resident registration	Registration via API on blockchain	HTTP 201 created, and a valid transaction hash returned by the API

TABLE III. CATALOG OF QUALITY METRICS AND ACCEPTANCE CRITERIA

Dimension	Indicator/criterion	Expected evidence
Performance (NF-1)	Response time in UI < 2 s (on a good quality network)	Measurement with network profiles: p50/p95 percentiles below threshold
Integrity/verifiability	Presence and storage of the Tx Hash in on-chain operations	Persistent and recoverable hash: cross-verification on- chain/off-chain
Security (NF-5– 6)	JWT, role-based access control: traceability in blockchain	Token expiration/rotation: auditing of access and traceable queries
Usability/accessibility	Readability, contrast, simplicity: testing with older adults according to ISO/IEC 25010 and senior-friendly guidelines [8]	Documented findings and improvements: compliance with usability thresholds
Scalability	Controlled degradation with concurrent users and limited connectivity	Load/resilience testing: mitigations (data optimization, operation with low connectivity)

Compared to purely web-based Web3 authentication, the solution integrates native mobile (Flutter) and enterprise backend (Spring Boot) for rural environments and low-end devices, prioritizing response times and API robustness, in line with recommendations for accessible design and acceptance by older adults [13, 8]. In contrast to technology adoption studies that point to literacy gaps and mistrust, the project introduces co-design with the municipality, local training, and transparent

traceability (chain audits), factors that the evidence identifies as facilitators [2-4]. In addition, TAM/UTAUT constructs (utility, ease of use, facilitation conditions) are operationalized, linking them to requirements and the accessible interface, which the literature associates with greater intention to use among older adults [6, 7].

However, most of the previous works remain at a conceptual/prototype level or target general populations, with limited validation in real public-service settings and limited focus on accessibility constraints for older adults. The proposed work addresses this gap by reporting an end-to-end municipal pilot with a prototype, API, and on-chain anchoring. In addition, it also operationalizes senior-friendly design and adoption factors (TAM/UTAUT) into measurable requirements and iterative improvements.

In summary, the proposed methodology integrates the technical basis of decentralized identity with principles of senior-centered design and empirical validation of performance, security, usability, and traceability, in a real-world context of low connectivity and municipal support.

III. RESULTS AND DISCUSSION

A. Results

1) Technical Implementation

The DDD architecture in the backend (Spring Boot) and the frontend in Flutter were deployed with JSON/HTTPS API calls and main persistence in MySQL, complemented by a traceability layer in blockchain for critical operations (identity queries by authorities and resident registration). The container diagram and functional modules (digital ID authentication, registration, ID card, services, and administration) were defined and validated in interactive prototypes. Acceptance testing included recording queries from authorities on the list of IDs (traceability) on the Ethereum blockchain and verifying the authentication and identification of residents. During the pilot, the Transaction Identifier (TxID) was generated in the backend, verifiable on Etherscan when the identifier is shared.

Figure 2 illustrates the validation flow of the senior citizen registration process, from initial data capture to on-chain confirmation of the registration event. This flow summarizes the key stages verified during technical implementation and the pilot.

2) System Performance, Latency, and Scalability

Regarding system latency (UI/API), a non-functional requirement of less than 2 s on a good quality network was set, start and end times per request were measured, and p50 and p95 were calculated with latencies between 500 ms and 1500 ms, meeting the objective. In line with comparative evaluations of smart contracts on Ethereum for health records (latency, throughput, and gas cost), the observed performance pattern is consistent with previous implementations of certificates and on- chain verification [14]. The validated critical cases, with expected/observed inputs and outputs, are summarized in Table IV.

Low connectivity behavior was outside the scope of the pilot, as offline support was explicitly excluded. The application is not compatible with devices without internet access, so in poor connectivity environments, timeouts and/or retries without local fallback are anticipated. In terms of scalability, the system's capacity to absorb situational increases in users and services without degrading response is supported by the separation of design responsibilities by domain and the API layer architecture, which preserves functional independence between components and facilitates the horizontal expansion of services.

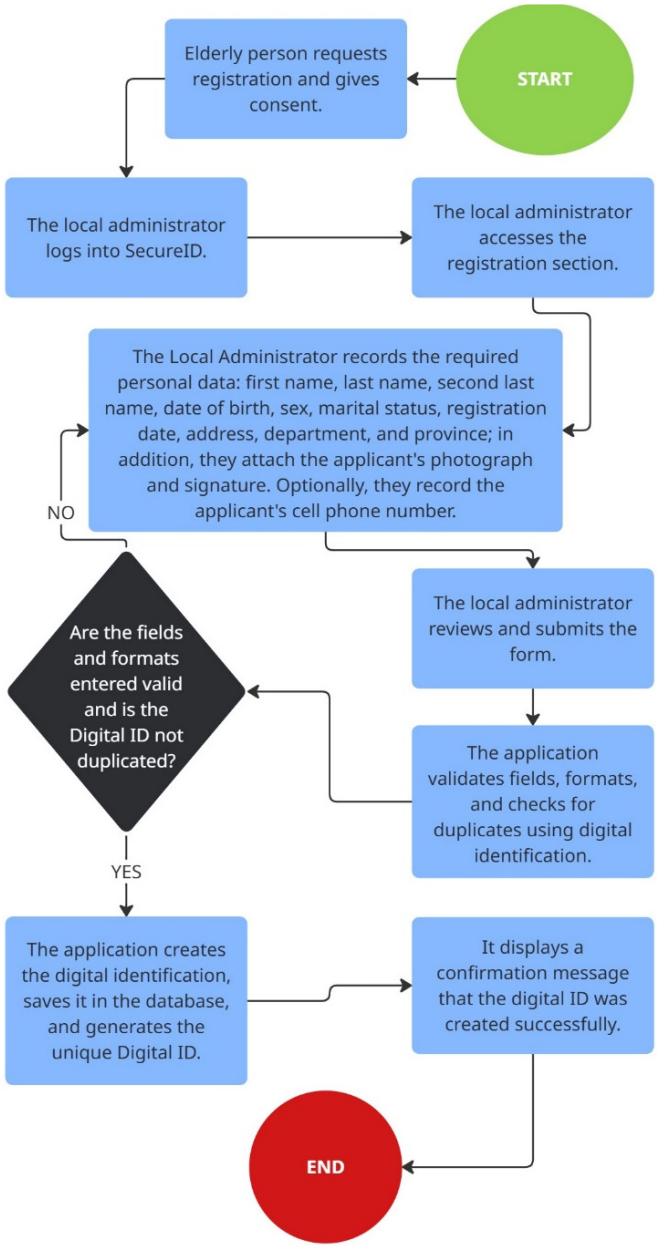


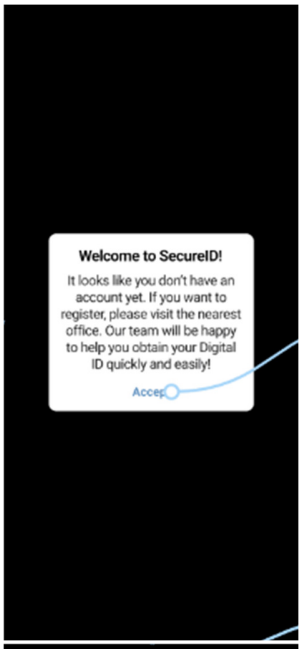
Fig. 2. Registration process validation flow.

TABLE IV. VALIDATED CRITICAL CASES

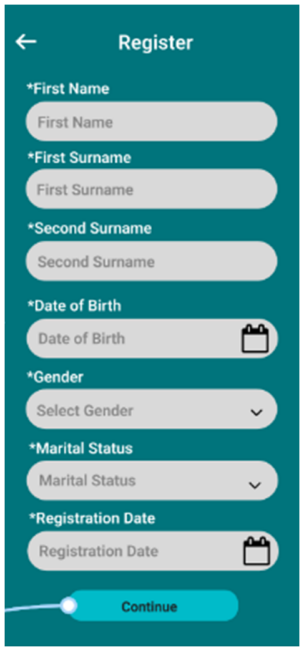
Case	Description	Input	Expected result	Observed result
CP-001 resident registration and on-chain anchoring	Resident registration with photo and signature: registration/consultation event in blockchain	POST/API/ resident	Resident created: event recorded with verifiable TxID	Successful registration: TxID generated
Authentication (digital ID)	Access by digital ID (authority/user role)	Valid/invalid digital ID	Access if valid: error if invalid	Compliant behavior (validated screens and validated flows)
Consultation/services	View/filter older adults and services	GET list + filter by name/ID	List loaded < 2 s p50; exact filtering	Correct display and filtering: latencies between 500 ms and 1500 ms.

(a)

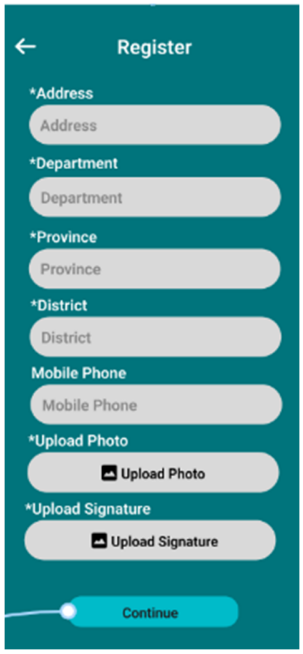
(b)



(c)



(d)



(e)

(f)

(g)

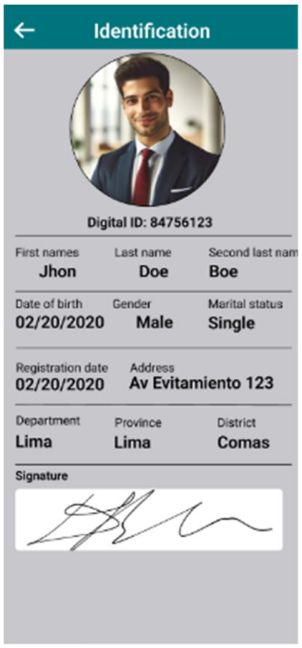


Fig. 3. Interface for identification registration: (a and b) welcome page, (c and d) registration form, (e) registration confirmation, (f) main menu, (g) identification.

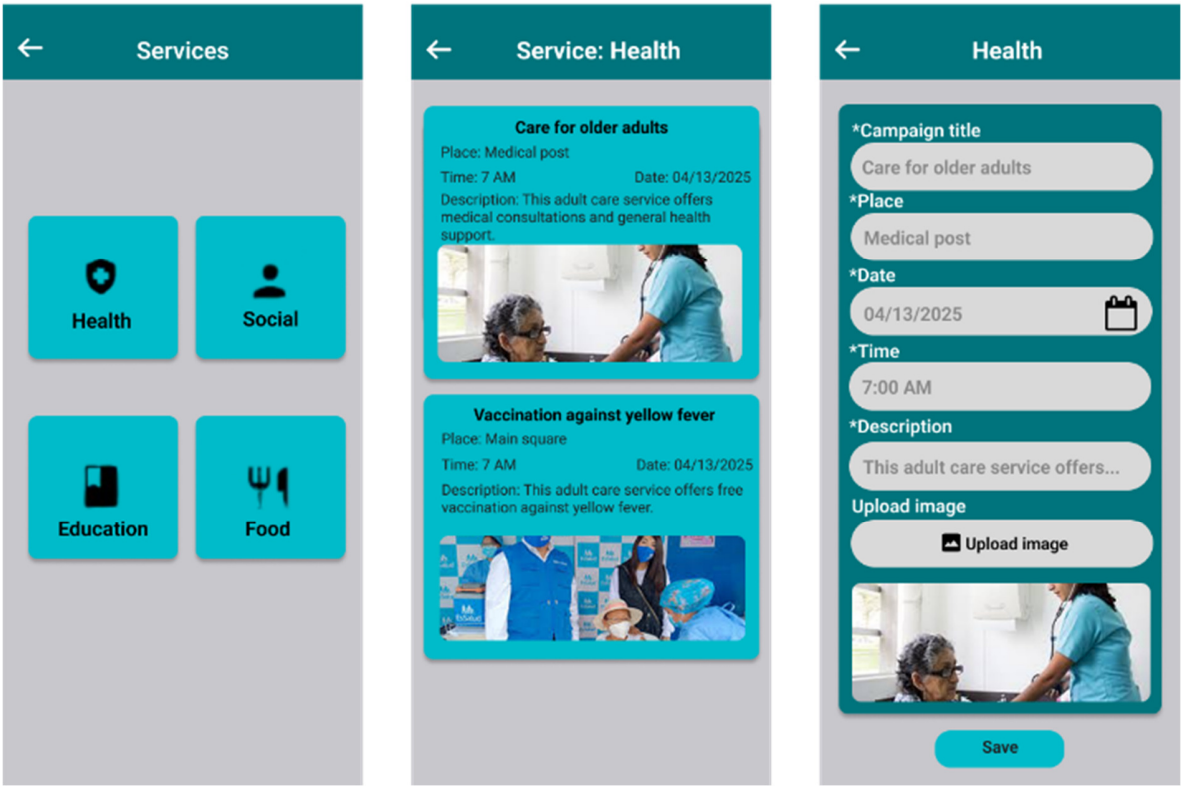


Fig. 4. Interface for essential services.

3) Usability and Accessibility

In a training phase, usability was evaluated with mockups and navigable flows in Figma with older adults (n = 16), applying the System Usability Scale (SUS) with a mean of 60.78 and an SD of 13.68, a result consistent with acceptable usability. Observations on visual hierarchy, labeling, and initial orientation guided subsequent design adjustments. Figures 3 and 4 display the registration, authentication, and identity

verification flows considered. With the functional mobile application now complete, two validations were performed on different days to introduce improvements between rounds; in both cases, the sessions were conducted on the participant's personal phone, with assistance available from the local authority in accordance with the campaign protocol.

4) Post-Use Survey

The post-use survey of older adults was conducted in two rounds, with a sample size of 31 and 41 for Survey V1 and V2, respectively. Overall, participants completed all planned tasks and reported high usability and satisfaction, with improvement observed between V1 and V2 following adjustments to onboarding, in-app messages, visual guidance, and synchronization. Figure 5 depicts the overall post-use satisfaction, and Table V outlines the quantitative results of the sample, the context of use, and the performance and usability metrics.

5) Post-Use Survey: Local Authorities

The post-use survey with local authorities was also conducted in two rounds (V1: $n = 2$; V2: $n = 3$). In both rounds, the service management flow was completed, with high satisfaction and a positive assessment of the usefulness and simplicity of the application, despite occasional connectivity limitations. Table VI summarizes the quantitative results of completed tasks, perceived connectivity, and key strengths and recommendations for this user profile.

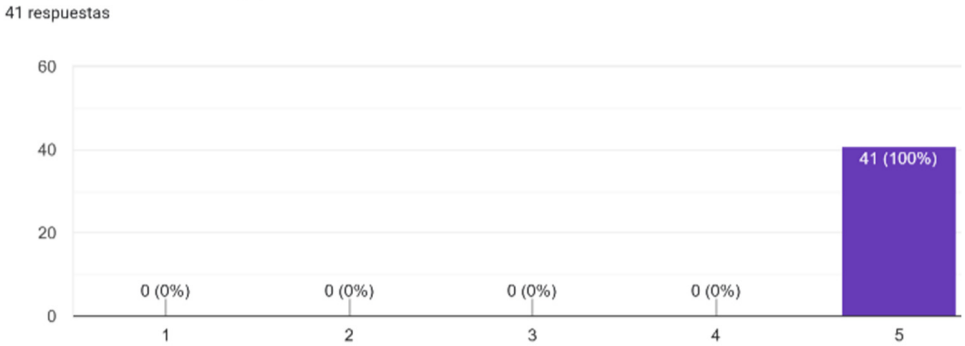


Fig. 5. Overall satisfaction level of older adults after using the application.

TABLE V. POST-USE SURVEY RESULTS: OLDER ADULTS ($n = 41$)

Variable	Result
Age range (cumulative)	60–64 (7), 65–69 (10), 70–74 (10), 75–80 (10), >80 (4)
Device and support	Participant's personal phone: assistance available under the campaign protocol
Connectivity	Fair/good
Tasks completed	Registration, login, ID display, service consultation, and logout (100%)
Likert scale (usability)	V1: 3.8–4.5 and V2: 5.0/5.0 on all items
NPS	+100
Positive aspects	Clarity of buttons and text, font size, navigation
Observations	Increased autonomy in V2: support available per protocol; perceived improvement in connectivity
Recommendation	Clearer in-app messages and persistent guidance: strengthen synchronization and resilience in contexts of variable connectivity

TABLE VI. POST-USE SURVEY RESULTS: LOCAL AUTHORITIES ($n = 3$)

Variable	Result
Age range	30–34 and >40
Tasks completed	Log in, check ID, register/update service, edit service, and log out (100%)
Connectivity	Fair/good
Satisfaction	5/5
NPS	+100
Positive aspects	Useful for management and simple design
Problems	Weak signal, delays in logging
Recommendation	Strengthen synchronization and resilience in the face of limited connectivity

6) Qualitative Findings and Design Adjustments

In terms of design, large buttons, high contrast, sans serif fonts, and visual delimitation of interactive elements were incorporated, reinforcing immediate feedback through brief pop-up messages. These decisions are consistent with established guidelines for older adults, which propose increasing the size and spacing of controls, adding text labels to icons, using simple language, and avoiding controls near the edge to minimize accidental touches [15].

Qualitative observations collected during testing indicated a significant improvement in the memorability of workflows thanks to the implementation of step-by-step flows and confirmations. A preference was also observed for short, clear messages over long texts and navigation through service cards with familiar iconography. These improvements address the challenges documented in mHealth for older adults, such as complex menus, small fonts, and cognitive overload, and

comply with specific usability and accessibility recommendations for this group [16, 17].

7) Security and Privacy

The system applies access control using JWT and role assignment (authority/user), with authentication performed with a digital ID issued/derived from the flow supported in blockchain. Traceability is guaranteed by recording authority queries about identifications on the blockchain, providing immutability and external verification of the access history for auditing [14]. The rationale for these controls is aligned with the confidentiality, integrity, and availability approach proposed for digital identity in healthcare, as authentication and role management restrict access to sensitive data, on-chain records preserve the integrity of events and enable external verification, and the separation of responsibilities in the architecture favors service availability, in accordance with the guidelines reported in [18].

B. Discussion

1) Comparison with Prior Work

The proposed work lies at the intersection between decentralized digital identity and access to essential services for the elderly in rural contexts. Compared to the past studies, it provides end-to-end functional validation from prototypes to API to on-chain anchoring, with an emphasis on interface accessibility. In digital identity and blockchain, previous studies highlight blockchain for integrated identity management, access control, and immutable logging in health/IoT [18, 19]. The present study confirms that blockchain-based traceability mechanisms can be effectively applied in real-world public service scenarios, extending prior approaches beyond conceptual or prototype-level implementations. The comparison with related works is summarized in Table VII. Overall, prior studies emphasize blockchain's benefits for integrity and auditability, but frequently under-report usability evidence for older adults and deployment constraints in rural/low-connectivity environments. The results complement these works by providing empirical usability/satisfaction evidence and an operational traceability workflow in a municipal scenario, while also identifying remaining limitations (e.g., low-connectivity behavior and additional authentication mechanisms) as key requirements for future large-scale adoption.

2) Implementation Challenges

In LTC/AAL, evidence shows an abundance of Ethereum prototypes for service/consent management but little evaluation in real scenarios and barriers to adoption (infrastructure, inter-institutional coordination, organizational change, acceptance) [20]. This work's contribution takes the form of a rural municipal case with a closed operational flow (registration, authentication, consultation) and validated traceability, still pending large-scale evaluation.

TABLE VII. COMPARISON WITH PRIOR WORK

Prior work	Approach	Limitations	Contribution
On-chain medical certificates [14]	Smart contracts (Ethereum): latency, throughput, gas	Does not evaluate vulnerable groups	The logic of immutable logging is transferred to queries by authority
Review of IoT, block chain, and digital ID in healthcare [15]	Review of 112 studies: focus on CIA and identity management	Highlights scalability and access gaps	This operational study implements traceability in a municipal case with UI accessible
Blockchain in LTC/AAL [16]	Ethereum dominance: service management and consent	Prototypes: low real- world validation	Real-world case of identification and access to local services; emphasis on simple access
Scoping review of mHealth usability [17]	Critical measures (SUS, memorability, errors)	Lack of objective measurement of memorability	Memorable prioritized with step-by-step flows
Design guidelines for older adults [18]	Control size, contrast, simple language	Heterogeneo us guides: limited validations	Concrete implementation in the prototype and final screens

3) On-chain Security and Smart Contracts

Work on verification/medical certificates reports manageable latencies and costs, and value in auditing and immutability, which supports the recording of critical events such as consultations [14]. In terms of usability with older adults, evidence-based guidelines propose simplicity, large controls, high contrast, step-by-step assistance, and warn of memorability/mental load as underrated dimensions [15, 16]. The proposed design adopts these recommendations and discusses their implications for continuity of use.

C. Limitations and Future Directions

1) Limitations of the Study and Pilot

The proposed solution strengthens traceability and access security within the specific regulatory, infrastructural, and socio-digital context of rural municipalities in Peru by incorporating blockchain technology only where it adds value (query auditing), avoiding overloads in the flow of older adults. The pilot met usability requirements (SUS = 60.78, SD = 13.68, $n = 16$) and UI/API latency requirements (p50 ≈ 500 ms, p95 ≈ 1500 ms, < 2 s), with on-chain event verification via Etherscan, which supports the technical feasibility and auditability of the approach. However, some limitations remain, such as the absence of two-Factor Authentication (2FA), the persistence of session artifacts in SharedPreferences in the prototype (insecure storage at the device level), and gaps in quantitative evidence regarding TAM/UTAUT models and low connectivity conditions, which limit comparability with LTC/AAL environments [20].

2) Future Scope of Development and Evaluation

Future plans include the incorporation of interoperability based on DID/SSI standards (e.g., DID methods and verifiable credentials) to promote portability and inter-institutional integration. There are also plans to strengthen client-side security by migrating from SharedPreferences to secure operating system storage (Android Keystore/iOS Keychain via secure storage), using short-lived access tokens with server rotation/renewal, and incorporating 2FA (TOTP/SMS or

WebAuthn). In addition, it is planned to continue with instrumented measurement of latency under load, complemented by stress tests, consolidating a degraded mode with encrypted local storage and synchronization queues for limited connectivity scenarios. A future study will also conduct a large-scale evaluation, incorporating TAM/UTAUT models and pre-post memorability tests targeting older adults. Finally, there are plans to coordinate with public policies to facilitate adoption in municipalities and LTC centers, considering organizational, technological, and infrastructural barriers [16, 18, 20].

IV. CONCLUSION

This study has demonstrated that the integration of blockchain technology with mobile applications for the digital identification of older adults is not only technically feasible but also an effective solution for improving the digital inclusion of this population group in rural contexts. Through the implementation of a decentralized architecture, which uses Ethereum for transaction recording and identity validation, the study offers a robust system that guarantees privacy and security without relying on centralized entities.

The results of usability tests with older adults indicate that, although challenges related to digital literacy and cognitive limitations remain relevant, user-centered design and simplified authentication processes allow for a satisfactory user experience. In particular, the intuitive interface and controls tailored to older adults improved accessibility, with an acceptable average usability score (System Usability Scale (SUS) = 60.78). From a technical perspective, the system meets performance and security requirements, with response times of less than 2 S under optimal network conditions and effective access control using JSON Web Tokens (JWT) and digital authentication. In addition, blockchain traceability provides a transparent audit of identity queries, reinforcing user confidence in the proposed application.

However, the study also identified areas for improvement, such as the need to incorporate additional authentication measures, such as two-Factor Authentication (2FA), and optimization of the solution for environments with limited connectivity, which represents an opportunity for expansion and strengthening of the system in future iterations. Finally, the successful implementation of this system in collaboration with the Municipality of Huaros underscores the importance of integrating local actors and community training to ensure the effective adoption of disruptive technologies among older adults. This collaborative approach should be replicated in future research and development to promote digital inclusion in other rural and vulnerable communities.

This work demonstrates the feasibility of blockchain-based digital identification for older adults and introduces a user-centered framework for rural, low digital literacy contexts. In doing so, it lays the groundwork for future research and development to expand digital inclusion in vulnerable communities, contributing to a transition toward a more equitable and digitally inclusive society.

CONFLICTS OF INTEREST

Not applicable to this work.

ACKNOWLEDGMENT

The authors would like to thank the research team at the Peruvian University of Applied Sciences for their ongoing support and resources during the development of the study. Special thanks go to the local collaborators and authorities in Huaros, who allowed the conduction field tests and provided valuable feedback. The authors would also like to acknowledge the health and technology professionals for their valuable suggestions, which were essential in ensuring the safety and accessibility of the developed application. In addition, the authors express their gratitude to the participants in the usability tests, whose willingness and patience were key to improving the functionality and design of the platform.

DATA AVAILABILITY

Not applicable to this work.

REFERENCES

[1] F. Wang, Y. Gai, and H. Zhang, "Blockchain User Digital Identity Big Data and Information Security Process Protection Based on Network Trust," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 4, Apr. 2024, Art. no. 102031, https://doi.org/10.1016/j.jksuci.2024.102031.

[2] Md. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 113436–113481, 2022, https://doi.org/10.1109/ACCESS.2022.3216643.

[3] A. Stamate, M.-D. Marzan, M. Velciu, C. Paul, and L. Spiru, "Advancing User-Centric Design and Technology Adoption for Aging Populations: A Multifaceted Approach," *Frontiers in Public Health*, vol. 12, Dec. 2024, Art. no. 1469815, https://doi.org/10.3389/fpubh.2024.1469815.

[4] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-Enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation," *Blockchain: Research and Applications*, vol. 2, no. 2, Jun. 2021, Art. no. 100014, https://doi.org/10.1016/j.bcra.2021.100014.

[5] B. Ma, X. Zheng, C. Zhao, Y. Wang, D. Wang, and B. Meng, "A Secure and Decentralized SSI Authentication Protocol with Privacy Protection and Fine-Grained Access Control Based on Federated Blockchain," *PLOS ONE*, vol. 17, no. 9, Sep. 2022, Art. no. e0274748, https://doi.org/10.1371/journal.pone.0274748.

[6] W. Schirmer, N. Geerts, A. Vercruyssen, and I. Glorieux, "Digital Skills Training for Older People: The Importance of the 'Lifeworld,'" *Archives of Gerontology and Geriatrics*, vol. 101, Jul. 2022, Art. no. 104695, https://doi.org/10.1016/j.archger.2022.104695.

[7] Z. Yan, X. Zhao, Y. Liu, and X. Luo, "Blockchain-Driven Decentralized Identity Management: An Interdisciplinary Review and Research Agenda," *Information & Management*, vol. 61, no. 7, Nov. 2024, Art. no. 104026, https://doi.org/10.1016/j.im.2024.104026.

[8] S. Cucko and M. Turkanovic, "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," *IEEE Access*, vol. 9, pp. 139009–139027, 2021, https://doi.org/10.1109/ACCESS.2021.3117588.

[9] T. Rathee and P. Singh, "A Systematic Literature Mapping on Secure Identity Management Using Blockchain Technology," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, pp. 5782–5796, Sep. 2022, https://doi.org/10.1016/j.jksuci.2021.03.005.

[10] S. Selvarajan *et al.*, "An Artificial Intelligence Lightweight Blockchain Security Model for Security and Privacy in IIoT Systems," *Journal of Cloud Computing*, vol. 12, no. 1, Mar. 2023, Art. no. 38, https://doi.org/10.1186/s13677-023-00412-y.

[11] A. Addo and P. K. Senyo, "Advancing E-Governance for Development: Digital Identification and Its Link to Socioeconomic Inclusion," *Government Information Quarterly*, vol. 38, no. 2, Apr. 2021, Art. no. 101568, https://doi.org/10.1016/j.giq.2021.101568.

[12] S. S. Oh, K.-A. Kim, M. Kim, J. Oh, S. H. Chu, and J. Choi, "Measurement of Digital Literacy Among Older Adults: Systematic Review," *Journal of Medical Internet Research*, vol. 23, no. 2, Feb. 2021, Art. no. e26145, https://doi.org/10.2196/26145.

[13] C. N. Butincu and A. Alexandrescu, "Design Aspects of Decentralized Identifiers and Self-Sovereign Identity Systems," *IEEE Access*, vol. 12, pp. 60928–60942, 2024, https://doi.org/10.1109/ACCESS.2024.3394537.

[14] P. Sharma, S. Namasudra, R. Gonzalez Crespo, J. Parra-Fuente, and M. Chandra Trivedi, "EHDHE: Enhancing Security of Healthcare Documents in IoT-Enabled Digital Healthcare Ecosystems Using Blockchain," *Information Sciences*, vol. 629, pp. 703–718, Jun. 2023, https://doi.org/10.1016/j.ins.2023.01.148.

[15] M. Gomez-Hernandez, X. Ferre, C. Moral, and E. Villalba-Mora, "Design Guidelines of Mobile Apps for Older Adults: Systematic Review and Thematic Analysis," *JMIR mHealth and uHealth*, vol. 11, Sep. 2023, Art. no. e43186, https://doi.org/10.2196/43186.

[16] Q. Wang *et al.*, "Usability Evaluation of mHealth Apps for Elderly Individuals: A Scoping Review," *BMC Medical Informatics and Decision Making*, vol. 22, no. 1, Dec. 2022, Art. no. 317, https://doi.org/10.1186/s12911-022-02064-5.

[17] A. Khamaj and A. M. Ali, "Examining the Usability and Accessibility Challenges in Mobile Health Applications for Older Adults," *Alexandria Engineering Journal*, vol. 102, pp. 179–191, Sep. 2024, https://doi.org/10.1016/j.aej.2024.06.002.

[18] S. K. Jena, R. C. Barik, and R. Priyadarshini, "A Systematic State-of-Art Review on Digital Identity Challenges with Solutions Using Conjugation of IoT and Blockchain in Healthcare," *Internet of Things*, vol. 25, Apr. 2024, Art. no. 101111, https://doi.org/10.1016/j.iot.2024.101111.

[19] H. K. Abdali, M. A. Hussain, Z. A. Abduljabbar, and V. O. Nyangaresi, "Implementing Blockchain for Enhancing Security and Authentication in Iraqi E-Government Services," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 18222–18233, Dec. 2024, https://doi.org/10.48084/etasr.8828.

[20] B. Steurer, B. Trukeschitz, and U. Schneider, "Applications of Blockchain Technology in Long-Term Care: Use Cases, Potentials, and Barriers," *BMC Health Services Research*, vol. 24, no. 1, Oct. 2024, Art. no. 1292, https://doi.org/10.1186/s12913-024-11670-0.