Building an Inclusive and Sustainable Smart City: A Pilot Project on Decentralized Digital Identity and Data Governance in Santa Rosa

Carla O. Castanho[1,2], Marcelo P. Chequin[1], Fernando M. Neto[2], Paulo C. Vargas[2], Sandro Sawicki[1], Rafael Z. Frantz[1]

[1]Unijuí University – Ijuí, RS – Brazil

{carla.castanho, marcelo.chequin}@sou.unijui.edu.br

{sawicki, rzfrantz}@unijui.edu.br

[2]URI University – Santiago, RS – Brazil

{066918, 102231}@urisantiago.br

Abstract. *This paper presents the initiative to transform the municipality of Santa Rosa into an intelligent and sustainable region. The project is fundamentally guided by the principles of Equality, Diversity, and Inclusion. For its implementation, a smart city pilot lab was built to validate technologies in a real-world environment. The study focuses on exploring decentralized solutions that enable citizens to securely access urban data through digital identification. The experimental evaluation of access control utilizes the concept of Decentralized Digital Identity, supported by Hyperledger Indy and Trustchain technologies. This research aims to advance the debate on the integration of decentralized identity into smart city infrastructure.*

1. Main Objective

Founded in 1931, the municipality of Santa Rosa, with a population of 73,575 inhabitants and a territorial area of 488.42 km², has established itself as an emerging industrial and commercial hub in southern Brazil. Its strategic geographic location, close to the borders with Argentina and Paraguay, gives the city a distinctive geopolitical and economic potential. The municipal administration, determined to capitalize on this position, has set as its central objective the transformation of Santa Rosa into a smart city and the positioning of the region as an innovation hub in the extreme south of the country.

In the context of smart cities, the creation and use of digital identities become fundamental elements for enabling access to public and private services, such as healthcare, transportation, security, and digital governance. Thus, the main objective of this work is the design and validation of a decentralized digital identity model for smart cities. This model aims to ensure secure access to digital services while preserving user privacy and respecting the principles of data self-sovereignty.

2. Beneficiaries of the Proposal

In 2021, a partnership was formalized between the municipal administration and the Applied Computing Research Group (GCA) of Unijuí University, resulting in the successful submission of a joint proposal to a public call issued by the Secretariat of Innovation, Science, and Technology of the state of Rio Grande do Sul. The approval of the proposal secured the funding of BRL 1.3 million, enabling the creation of the SmartLive

Lab [Sawicki et al. 2025] at the University's facilities. This infrastructure is equipped with specialized hardware and software for the prototyping and testing of smart city technologies, in addition to providing facilities for interinstitutional collaboration, such as the ongoing partnership with the University of Cambridge established in 2019.

The SmartLive Lab plays a central role in the methodology of the project, operating in two complementary dimensions. First, it has an operational and validation-oriented role, serving as a pilot platform for the deployment and testing of technologies under real-world conditions and at a controlled scale within the municipality of Santa Rosa. This preliminary phase is crucial for refinement and data collection, mitigating risks prior to large-scale implementation. Second, it fulfills an academic and educational role: the laboratory acts as a hub of knowledge-generation, providing a practical experimentation environment for the development of intellectual capital at multiple levels, ranging from undergraduate research to master's and doctoral studies, as well as international research collaborations.

3. Technologies Used

The proposed solution integrates a mobile application and Self-Sovereign Identity (SSI) components to manage Decentralized Identifiers (DIDs) and Verifiable Credentials. The backend, developed in Python using FastAPI, provides a REST API to query environmental data (temperature and humidity) collected by Netvox R72623 sensors [Netvox Technology 2019], control access, and interact with Hyperledger Indy/Aries agents when required. The data are persisted as time series in a PostgreSQL database, recording both the measured value and the corresponding *timestamp* for each observation.

The development of decentralized digital identities requires a technological ecosystem that combines open W3C protocols (DIDs and Verifiable Credentials) with tools that ensure distribution, verifiability, and security. Two main technologies were adopted. The first, based on Trustchain [Hobson et al. 2023], employs the ION network over Bitcoin for the immutable registration of DIDs, using Rust, Node.js, IPFS, and MongoDB to form a decentralized public key infrastructure. The second, grounded in the Hyperledger ecosystem [Hyperledger 2024], combines the permissioned Indy ledger (and its AnonCreds model) with the Aries toolkit for credential management and peer-to-peer communication (DIDComm), supported by agents such as ACA-Py and relational databases (PostgreSQL). These tools constitute the development ecosystem, enabling the construction of a distributed, verifiable, and interoperable architecture for digital identities. The combination of these technologies ensures that the system is aligned with open W3C standards while promoting security, auditability, and genuine decentralization.

4. Results Obtained

The implementation of a decentralized digital identity system involves a robust set of technologies, tools, and services that support standards for decentralized identifiers, verifiable credentials, and distributed storage. The proposed integration pursues two complementary objectives: (i) to deploy Trustchain in a real-world scenario, with mobile users accessing urban sensor data, and (ii) to compare its behavior and operational requirements with an arrangement based on Hyperledger Indy. By running both tracks side by side, we aim to observe latency, costs, governance, and user experience, maintaining Trustchain as the preferred stack for DID/VC issuance, resolution, and verification, while Indy serves

as a contrasting reference and an alternative verification path. Figure 1 summarizes the component arrangement and the main data and verification flows.

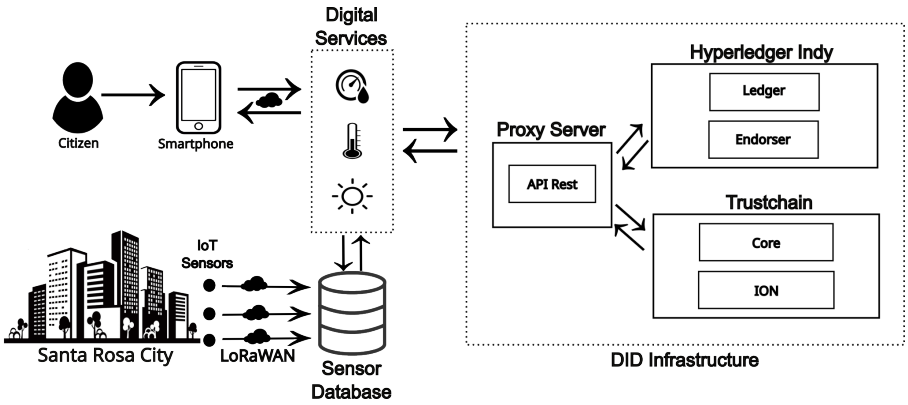

Figure 1. ***Trustchain and Hyperledger Indy Integration Architecture.***

From an architectural perspective, the Proxy Server (REST API) constitutes the qcoupling point between identity and data. The mobile application of the user requests access to the readings of the sensor database and, instead of traditional credentials, presents a Verifiable Presentation (VP) containing only the minimum required attributes (selective disclosure). The API prioritizes validation through Trustchain: it resolves the DID of the holder through ION/Bitcoin, retrieves the DID document and metadata from IPFS, checks signatures, state policies, and revocation status, and then applies the urban service authorization rules. When configured for comparative purposes, the same endpoint can invoke an Indy verifier to validate an equivalent VP, recording time metrics, failures, and audit events across both paths, exactly as indicated by the parallel links in Figure 1.

The complete workflow unfolds in four sequential steps. (1) Presentation: the smartphone application sends the VP to the API over HTTPS. (2) Verification (Trustchain-first): the API queries the Trustchain/ION resolver, obtains the DID document and revocation lists/status from IPFS, validates Bitcoin-anchored timestamping, and confirms the key–controller binding. (3) Authorization: once the identity is validated, the API enforces policy rules (roles, data scope, time window, quotas), recording audit trails. Optionally, in comparison mode, it executes Indy verification in parallel or as a fallback and stores the corresponding metrics. (4) Delivery: the API queries the sensor database and returns only the authorized data (aggregated or anonymized according to policy), preserving data minimization.

The integration also encompasses IoT devices as identity subjects. Sensors may possess DIDs issued by Trustchain or Indy, signing events at the edge; the Proxy Server only accepts authenticated ingestion, reducing the risk of spoofing and improving data traceability. In both user and device flows, Trustchain provides operational advantages: a decentralized public key infrastructure (DPKI) with public timestamping (Bitcoin/ION), distributed documents and status lists (IPFS), key rotation and recovery mechanisms, and encouragement of pairwise DIDs to mitigate cross-domain correlation.

The application provides two visualization screens (temperature and humidity) both that consume authenticated metrics endpoints and display readings from the previous day with on-demand updates. In cases of session expiration or invalid proofs, the app redirects the user to the credential presentation flow, ensuring that only properly verified

profiles can access the data. Finally, the integration was designed following production-grade practices, including short-lived caching of DID/VC resolutions to reduce repeated calls, rate limiting and circuit breakers at the API layer, structured logging, verification metrics (resolution time, success/failure rates, revocation incidence), and full auditing of access decisions. This arrangement demonstrates, with real sensor data and mobile users, that Trustchain can maintain DID/VC-based access control in a smart city context while simultaneously enabling a fair and measurable comparison of its performance and operational characteristics against the Indy-based track.

4.1. Pending Tasks

To advance the proposed decentralized digital identity architecture and transform it into a solution ready for real-world smart city scenarios, our task list includes: systematically evaluating system behavior under load by measuring end-to-end latencies in key operations (DID resolution, retrieval of distributed artifacts, and credential verification) and observing the impact of multiple issuers and verifiers competing for the same resources; introducing caching mechanisms, asynchronous queues, and fault-tolerance strategies to ensure operational continuity and response times compatible with public services; and conducting usability studies with citizens, public servants, and technical operators to assess onboarding flows, access recovery, and selective credential presentation.

In parallel, integrating the proposed architecture with one or more concrete urban services can produce real-world metrics on latency, cost, success rates, and perceived value, supporting informed decisions regarding platform evolution and its potential adoption in production environments.

Acknowledgements

This research was partially funded by the Coordination for the Improvement of Higher Education Personnel (CAPES) and the National Council for Scientific and Technological Development (CNPq), through projects 309425/2023-9 and 402915/2023-2.

References

Hobson, T., France, L., Greenbury, S., Hare, L., and Wochner, P. (2023). Trustchain – trustworthy decentralised public key infrastructure for digital credentials. *IET Conference Proceedings*, 2023(14):31–40.

Hyperledger (2024). Hyperledger indy: Distributed identity framework. https://www.hyperledger.org/projects/hyperledger-indy. Last accessed on 08/24/2024.

Netvox Technology (2019). *R72623 LoRaWAN Wireless Temperature & Humidity Sensor – User Manual*. Last accessed on 01/29/26.

Sawicki, S., Frantz, R. Z., Battisti, G., Roos-Frantz, F., Rasia, L. A., Eder, O., Molina–Jimenez, C., and Crowcroft, J. (2025). Building a smart city that stimulates innovation using open source and decentralised technologies. In *Anais do XXVIII Congresso Ibero-Americano em Engenharia de Software*, pages 356–359, Porto Alegre, RS, Brasil. SBC.