Self-Sovereign Digital Identity System for Smart Cities: A Pilot Project with Trustchain and Hyperledger Indy in the Municipality of Santa Rosa

Carla O. Castanho[1,2], Marcelo P. Chequin[1], 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

carla.castanho@urisantiago.br

Abstract. *In a smart city context increasingly dependent on big tech platforms, this paper presents the implementation and validation of a system integrating Trustchain and Hyperledger Indy for decentralised citizen identification in accessing environmental data in Santa Rosa (RS), Brazil, addressing the need to mitigate centralised data vulnerability while preserving privacy and self-sovereignty. Through a mobile application that requires verifiable credentials, the proposed solution demonstrates the feasibility of the hybrid architecture, consistent performance in digital identity creation and verification metrics, and a stable registration and query workflow, positioning itself as an effective identity management mechanism for smart cities.*

1. Introduction

The incorporation of technology into everyday processes has led to the emergence of smart cities, where areas such as governance, transportation, security, and healthcare are automated, managed, and monitored, often in real time. In a smart city, the Internet of Things (IoT) plays a central role, representing the broad connectivity among sensors, machines, software, and individuals through the Internet to enable interaction, data sharing, and functionality, effectively bridging the physical and digital worlds [Quy et al. 2022]. The connectivity enabled by IoT provides citizens with a wide range of digital products and services derived from urban infrastructure, facilitating access while simultaneously generating a significant increase in the volume of data circulating within this environment.

It is common that, in order to use these digital services, citizens must create accounts within the services themselves that act as centralised local authorities or register with different centralised digital platforms provided by third-party identity providers, such as Google, Facebook, among others. In both cases, citizens are required to submit their data to third-party systems, often repeatedly, or only once when a federated authentication platform is adopted. While the use of digital platforms as identification mechanisms is appealing due to the elimination of the need for multiple registrations, it comes at a high cost: the transfer of personal data to big tech companies. The lack of user control over personal data enables service providers and big tech companies to exploit such data—often inappropriately to generate insights (e.g., consumption habits, leisure preferences, political opinions, etc.) [Sedlmeir et al. 2021]. An approach to mitigate the risks associated with this process involves the adoption of decentralised digital identity systems [Toth and Anderson-Priddy 2019].

In contrast to the traditional centralised model, decentralised identity shifts part of the control from centralised entities to individuals, allowing them to own and manage their digital identity data without relying on intermediaries. In this model, decentralised identifiers (DIDs) and verifiable credentials (VCs) enable the validation of identity attributes without exposing unnecessary personal information, thereby enhancing privacy and reducing dependence on centralised silos [Rellington 2025]. These credentials are typically stored in user-controlled digital wallets and secured through cryptographic mechanisms and distributed technologies such as blockchain [Sedlmeir et al. 2021]. Within this context, the concept of Self-Sovereign Identity (SSI) emerges, in which individuals retain direct control over their digital credentials and decide when and with whom to share their information [Schardong and Custódio 2022].

Although related, the concepts of decentralised identity and self-sovereign identity differ in scope. Decentralised identity primarily refers to a technical architecture that distributes the storage and management of identities across multiple actors, reducing reliance on central authorities [Toth and Anderson-Priddy 2019]. In contrast, self-sovereign identity also encompasses normative principles that position the individual as the primary authority over their personal data [Preukschat and Reed 2021]. Thus, it can be stated that every self-sovereign identity is decentralised, but not every decentralised identity guarantees full user autonomy, as some systems may still involve intermediaries or governance constraints [Mühle et al. 2018].

There is a range of tools available for implementing decentralised identity systems; among them, Trustchain and Hyperledger Indy stand out. Trustchain is a free and open-source software developed by the Alan Turing Institute (United Kingdom) designed for building decentralised digital identity systems [Hobson et al. 2023]. Hyperledger Indy is a permissioned, open-source blockchain platform maintained by the Linux Foundation, specifically designed to provide a secure and decentralised infrastructure for managing self-sovereign digital identities. Its goal is to ensure users have full control over their identities and personal data, removing the traditional dependence on centralised authorities that store and manage sensitive personal information [Baniata et al. 2022].

In this paper, we present a system developed as part of a pilot project in the municipality of Santa Rosa (Brazil) for citizen identification and controlled access to an environmental data repository of the city of Santa Rosa (RS). The system aims to ensure secure access to urban digital services while preserving user privacy and adhering to the principles of data self-sovereignty, as well as increasing system resilience. We setup a hybrid DID infrastructure and developed a mobile app that provides access to environmental services, as well as we collected configuration and digital identity creation metrics to evaluate our solution. We validate the practical feasibility of the model for identity management in urban environments, positioning it as an effective mechanism for citizen empowerment in the context of smart cities. The remainder of this paper is structured as follows: Section 2 discusses related work; Section 3 describes the implemented system; and Section 4 presents conclusions and directions for future work.

2. Related work

Several recent studies explore decentralised digital identities and verifiable credentials across different contexts, generally grounded in the self-sovereign identity paradigm. In the IoT domain, Zhao et al. [Zhao et al. 2023] present a model for smart homes in which users and devices are identified through DIDs, and a decentralised access control mechanism is employed to mitigate single points of failure and enhance residents'

privacy. In the context of smart cities, Albugmi [Albugmi 2025] proposes a Hybrid Detection and Prevention Framework for IoT (HDPIoTF) based on blockchain for security in smart cities. The architecture integrates IoT sensors, gateways, blockchain networks, smart contracts, security analytics, and real-time notifications, aiming at continuous monitoring and automated response mechanisms. Both works provide a relevant conceptual foundation for integrating blockchain and IoT in the protection of critical infrastructures. They reinforce the potential of DIDs and SSI across multiple domains; however, they are generally tightly coupled to specific vertical use cases and do not focus on the design of a generic API for smart city-oriented applications, as is the case in our study..

Regarding infrastructure and tooling, Aidoo [Aidoo 2024] proposes the Trust Coalition Agent, a modular system built on the Hyperledger ecosystem (Aries Cloud Agent Python, Indy tails server) that exposes a lifecycle API to manage connections, credential issuance, verification, and revocation within a digital trust coalition composed of multiple domains. Similarly, the open-source project AcaPy-Cloud provides a FastAPI-based application that encapsulates ACA-py and offers a high-level REST API, reducing the number of calls required to perform SSI workflows such as wallet creation, public DID publication, schema creation, credential issuance, and proof verification [Acapy Cloud 2024]. Furthermore, recent works focused on adopting Trustchain as a decentralised PKI infrastructure in smart cities point to additional alternatives for public key registration and validation in digital urban environments [Castanho et al. 2025]. The aforementioned works support the relevance of the chosen technological approach, providing a solid foundation for the development of the system proposed in this paper.

3. Implemented System

This section presents the architecture of the system developed to support decentralised digital identities in a smart city scenario. The solution adopts the self-sovereign identity (SSI) model, allowing users to access urban services through decentralised Identifiers (DIDs) and Verifiable Credentials (VCs), ensuring properties such as decentralisation, verifiability, and access control. To this end, the system integrates a mobile application with a distributed identity management infrastructure, enabling user authentication and authorisation without reliance on centralised providers.

3.1. System Architecture Overview

The proposed integration has two complementary objectives: to deploy Trustchain in a real-world scenario, with mobile users accessing data from urban sensors, and to compare its behaviour and operational requirements with an arrangement based on Hyperledger Indy. By executing both approaches in parallel, we aim to assess the feasibility of Trustchain as a preferred stack for issuing, resolving, and verifying DIDs/VCs, while Indy serves as a reference baseline and an alternative verification path. Figure 1 summarises the component arrangement and the main data and verification flows.

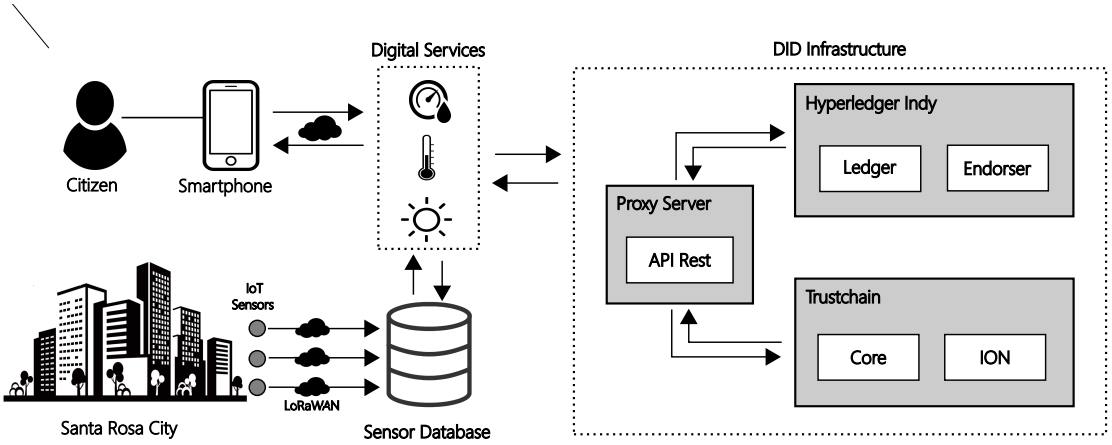

Figure 1. Trustchain and Hyperledger Indy Integration Architecture.

From an architectural perspective, the Proxy Server (REST API) acts as the integration point between the decentralised identity system and the urban data infrastructure. The user's mobile app requests access to environmental data, presenting a Verifiable Presentation (VP) that contains only the attributes required for the request, in accordance with the principle of selective disclosure. This process defines a credential-based authentication flow, where the API validates credentials before granting data access.

To achieve this, two independent verification mechanisms are employed. In the case of Hyperledger Indy, validation involves querying the permissioned ledger, which stores DIDs, schemas, and credential definitions, as well as interacting with the Endorser component, which is an authorised entity that validates and records transactions on the network. In the Trustchain-based approach, Trustchain Core manages identities and credentials off-chain, while Trustchain ION (Identity Overlay Network) anchors decentralised identifiers on a public blockchain for immutable, globally verifiable records.

The complete authentication flow can be described as a sequence of four main stages. First, in the presentation stage, the mobile application sends the Verifiable Presentation (VP) to the API via an HTTPS request, containing only the necessary attributes. Next, the verification stage takes place, prioritising the Trustchain approach, in which the API queries the Trustchain/ION resolver to obtain the DID document, cheques the revocation status of credentials stored in IPFS, and validates the cryptographic binding between the public key and the identifier controller. Once the identity is validated, the authorisation stage is performed based on the access policies defined for the service, considering roles, scope, and data usage constraints. Finally, in the delivery stage, the API queries the sensor database and returns to the user only the authorised data.

In both flows (user and device), the Trustchain-based approach presents relevant operational advantages, such as the use of a decentralised public key infrastructure (DPKI) with public timestamping anchored in Bitcoin through the ION network, as well as the distributed storage of DID documents and status lists in IPFS. Additionally, the architecture supports cryptographic key rotation and recovery, as well as the use of pairwise DIDs, reducing the risk of correlation across different domains and strengthening the privacy properties inherent to the self-sovereign identity model.

3.2. Results and Discussion

The comparative analysis was conducted based on three main metrics: setup time, DID creation time, and DID verification time. Regarding the installation process, both Hyperledger Indy and Trustchain exhibit high initial technical complexity. In the case of Hyperledger Indy, prior knowledge of containers, permissioned ledger configuration, genesis files, and wallet management is required; however, in a controlled environment with an experienced user, the process can be completed in approximately 2 to 6 hours. Trustchain requires technical expertise to run and manage a network node and to understand its transaction model and data anchoring. Full network synchronization is also needed, which in Testnet3 can take 3–4 days. While Testnet4 aims to reduce this time, dependence on global infrastructure still causes significant initial setup latency.

For DID creation, Hyperledger Indy showed stable performance, averaging about 500 ms for full ledger registration. Its permissioned design enables fast, predictable confirmations. Trustchain uses a hybrid model: logical DID creation is fast (50–300 ms) because it is local, but final publication depends on Bitcoin blockchain inclusion, averaging around 10 minutes and incurring transaction fees, unlike Indy. Thus, immediate creation and finalization must be distinguished, with finalization being much slower. For DID verification, both systems performed similarly: about 150 ms in Indy and 50–300 ms in Trustchain, depending on node access, showing that read operations are efficient in both models, even when using a public blockchain.

4. Conclusion

This paper presents a software system where access to Santa Rosa's environmental data requires verifiable credentials based on decentralised identity. The solution integrates two decentralised identity systems (Trustchain and Hyperledger Indy) with a mobile app and verification infrastructure that authenticates requests before granting access to the city's environmental data. The results demonstrate the practical feasibility of the approach, as the complete flow of registration, credential presentation, and data querying operated consistently, adhering to the principle of data minimisation by exposing only the information necessary for the service. In terms of performance, Hyperledger Indy exhibited reduced and predictable response times, while Trustchain combines fast logical creation with higher finalisation latency due to blockchain anchoring, maintaining similar verification times across both approaches.

Literature shows SSI adoption is hindered by usability issues and complex key management for non-experts. The Santa Rosa pilot addressed this by using a mobile app that hides technical details, easing citizen onboarding while maintaining cryptographic robustness. The findings suggest SSI must be designed as a socio-technical system that balances security, social acceptance, and regulatory compliance. The choice of the Bitcoin-anchored ION network via Trustchain ensured immutability but introduced higher costs and latency than permissioned ledgers like Hyperledger Indy, underscoring the need for context-sensitive architectural choices. As future work, we plan to evaluate the solution's performance in larger-scale scenarios by measuring latencies in DID resolution, distributed artifact retrieval, and credential verification. We will also conduct usability studies with diverse citizen profiles to assess the user experience of digital wallets and authentication. Integration with other urban services will provide real-world operational and adoption metrics to assess feasibility in production. Finally, we will investigate mechanisms to enhance operational resilience and examine the impact of emerging, including quantum-resistant, cryptographic approaches.

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

Acapy Cloud (2024). acapy-cloud: Cloud-native services and api for managing dids and verifiable credentials. Acesso em: 20 nov. 2025.

Aidoo, A. (2024). Federated governance in a digital trust coalition. Master's thesis, University of Zurich.

Albugmi, A. (2025). Hybrid smart iot detection and prevention framework for smart cities using blockchain technology. *International Journal of Advanced and Applied Sciences*, 12(4):107–115.

Baniata, H., Pflanzner, T., Fehér, Z., and Kertész, A. (2022). Latency assessment of blockchain-based ssi applications utilizing hyperledger indy. In *Nome completo do evento ou anais*, pages XX–XX, Local do evento. Editora.

Castanho, C., Frantz, R., Chequin, M., Sawicki, S., Roos-Frantz, F., Molina-Jimenez, C., Crowcroft, J., and Hobson, T. (2025). Unlocking the potential of decentralised digital identification systems for smart cities. In *Anais do III Colóquio em Blockchain e Web Descentralizada*, pages 7–12, Porto Alegre, RS, Brasil. SBC.

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.

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30:80–86.

Preukschat, A. and Reed, D. (2021). Self-sovereign identity - decentralized digital identity and verifiable credentials. In Co., M. P., editor, *Self-Sovereign Identity livebook*, chapter Why the internet is missing an identity layer—and why SSI can finally provide one, page 504. Manning Publications Co.

Quy, V. K., Hau, N. V., Anh, D. V., Quy, N. M., Ban, N. T., Lanza, S., Randazzo, G., and Muzirafuti, A. (2022). Iot-enabled smart agriculture: Architecture, applications, and challenges. *Applied Sciences*, 12(7).

Rellington, J. (2025). *Self-Sovereign and Decentralized Identity: The Future of Identity Management*. Independently Published.

Schardong, F. and Custódio, R. (2022). Self-sovereign identity: A systematic review, mapping and taxonomy.

Sedlmeir, J., Smethurst, R., Rieger, A., and Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, 63(5):603–613.

Toth, K. C. and Anderson-Priddy, A. (2019). Self-sovereign digital identity: A paradigm shift for identity. *IEEE Security Privacy*, 17(3):17–27.

Zhao, X., Zhong, B., and Cui, Z. (2023). Design of a decentralized identifier-based authentication and access control model for smart homes. *Electronics*, 12(15):3334.