Comunicação:

Real Estate Documentation Authentication with Blockchain and Self-Sovereign Identity

João Luís[1], João Santos[2], Tiago Dias[2], and Miguel Correia[1]

[1] INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Lisboa, Portugal
[2] Unlockit, Lisbon, Portugal

Abstract. In recent years, the Portuguese real estate market has expanded, leading to increasingly complex property transactions. The initiation of property transactions involves a significant number of documents, obeyingregulations such as GDPR [2] and AML6 [4]. Access to legal services has also become tougher, requiring communication with several entities. The current solution for document authentication involves traditional methods such as manual verification and reliance on central databases, which are time-consuming and prone to errors. This document proposes a solution to facilitate a streamlined and secure authentication process. The proposed solution not only mitigates the identified challenges in real estate document authentication but also aligns with the current trends in decentralized identity and blockchain technologies. This new approach uses Polygon ID [6], a cutting-edge blockchain-based identity management solution, and the web3 principles. With these, it means a promising transformation in the authentication process, providing increased security, trust, and efficiency.

Keywords: Real Estate · blockchain · Polygon ID · Verifiable Credentials · Decentralized Identifiers

1 Introduction

Real estate has been a trending sector in the Portuguese economy for many years. Starting a property purchase or selling process is long and bureaucratic, involving many documents, contracts, permits, and licenses issued by different authorities and obeying strict regulations regarding due diligence, GDPR, and anti-money laundering, for instance. Due to the increased complexity of regulation over the years, having easy access to legal services is challenging and involves communication with different entities. Real estate professionals, property buyers, and sellers are looking for new solutions to access these services.

Blockchain technology facilitates the validation and tracking of complex transactions. This technology can provide secure transactions, reduce compliance costs, and speed up data transfer processing. Many use cases in the industry have already been validated in the areas of digital identity, real estate, supply chain, and many others. Companies and governments alike are now investing heavily in Distributed Ledger Technology (DLT) to offer better services and products.

This paper focuses on using a Self-Sovereign Identity (SSI) framework [5], Polygon ID, to support the *authentication of documents relevant to the processes of selling and buying a property*, executed with the support of the Blockchain system. Polygon ID is a decentralized identity management solution that leverages selective disclosure [7] to ensure privacy and security. Using Polygon ID, it is possible to verify the authenticity of documents and signatures without exposing sensitive information. This type of authentication aims to prove that a document (and the corresponding signature) is genuine. Polygon ID offers a scalable, secure, and privacy-preserving framework, making it an ideal solution for the real estate sector. Its integration can streamline the document verification process, making it easier and faster for real estate agents to verify information. In the future, real estate agents may have the potential to verify information in an easy and expedited manner, enhancing trust and efficiency in property transactions.

2 Background

2.1 Real Estate

Real estate transactions involve the purchase and sale of properties, where document authentication is crucial. Verifiers must meticulously check documents issued by various authorities to ensure their authenticity. Fraudulent activities and misrepresentations are common issues [11], compromising the privacy of sensitive data. The current trust mechanism relies on direct contact with the issuers, which does not allow for a seamless trust mechanism [3].

2.2 Blockchain

A blockchain, a DLT technology, consists of an immutable record of transactions organized into blocks, chronologically ordered, maintained by a group of nodes that replicate and approve data without relying on a central authority. This system is known for secure transaction processing, cost reduction, and simplification in data processing [1].

2.3 Self-Sovereign-Identity

Self-Sovereign Identity (SSI) is a form of identity management that allows individuals to fully own and manage their digital identity [5]. Users store their identity data in digital wallets, enabling secure, private, and portable use of their credentials. SSI systems rely on Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs). VCs are digital versions of physical credentials that are cryptographically secure and machine-verifiable [9]. DIDs are unique identifiers under the control of the DID subject, independent of any central authority, usually accompanied by cryptographic keys for secure authentication and signing of documents [8].

A blockchain provides a decentralized and immutable ledger where identities and credentials can be registered and verified. It ensures that the identities are tamper-proof and can be validated by any participant in the network. The issuer is a trusted entity (e.g., a government or legal authority) that creates and issues VCs to the user. The issuer registers its identity on the blockchain and can issue VCs that are verifiable by any verifier. The verifier is an entity that needs to verify the credentials presented by the user. The verifier can validate the authenticity of the VC and the DID through the blockchain, ensuring that the credentials are legitimate and not tampered with.

2.4 Polygon ID

Polygon ID is a decentralized identity management solution that leverages blockchain technology to implement the SSI principles [6]. Polygon ID allows users to create and manage their DIDs. These identifiers are registered on the Polygon blockchain, ensuring that they are decentralized and under the user's control. Polygon ID supports the issuance and verification of VCs. Issuers can create VCs that are cryptographically signed and that contain proofs that can be verified by any verifier. These credentials are stored in the user's digital wallet, ensuring privacy and control. Polygon ID utilizes selective disclosure. This means that users can prove the validity of certain attributes in their credentials without revealing the entire credential. By leveraging blockchain's immutability and cryptographic techniques, Polygon ID ensures that the credentials and identities are secure and private.

3 Solution

This section outlines a proposed solution that aims to address the issues discussed earlier. The proposal is a reliable real estate document authentication system that leverages web3 technologies, including DIDs and VCs, and interoperates with services provided by Polygon ID to streamline the process of validating documents in a real estate application.

3.1 User Roles

This system involves three user roles: an issuer, a user, and a verifier.

- The issuer, which represents a legal public entity, registers its identity in the ledger and issues VCs representing documents to a user, to prove the legitimicy of that document.
- The user, which can be a buyer or seller of a property, requests documents from the issuer and consequently stores a proof of that document in the form of a VC.
- The verifier, which requests the necessary data from the user for the documentation process and verifies the authenticity of the proof.

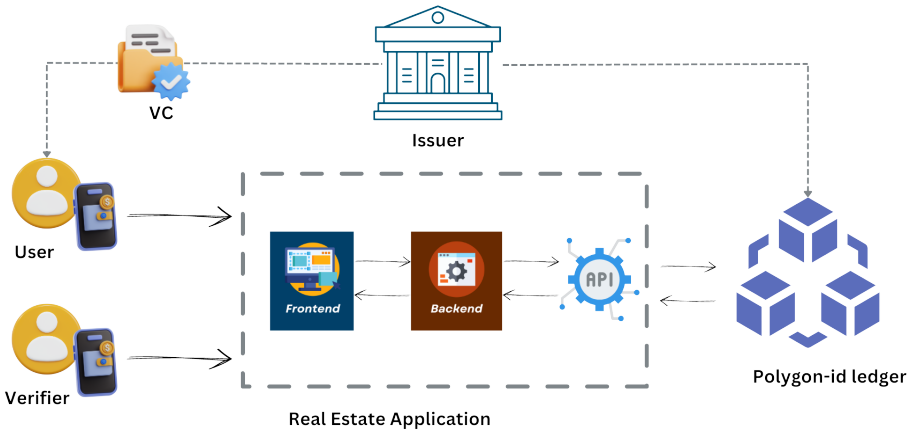

Fig. 1. Solution Architecture

3.2 Architecture

The architecture of the system is presented in Figure 1. The overall system is an application that provides a streamlined interface to facilitate the authentication and verification of real estate documents. This application is backed by a blockchain that provides an SSI framework, which in this case is Polygon ID. The key features and processes supported by the application are the following:

- Initial Page: Lists the necessary documents for buying and selling properties, the associated issuers, and their DIDs to facilitate documentation requirements.
- User Authentication: Each user authenticates using their digital wallet, proving possession of a DID. Unlike traditional methods that rely on identity providers, this method ensures decentralized and secure authentication.
- Verifier Authentication: The verifier must possess a VC containing a credential that legitimizes their access to user data. This ensures that only authorized entities can request and verify document information.
- Document Access and Selective Disclosure: After authentication, users can access information related to their documents. They can select the necessary fields for each document using selective disclosure, which allows them to reveal only the required fields, protecting their private information.
- API-Defined Queries: Queries are defined by an API that verifies the proof sent by the user. The verifier can request specific fields, but only with user consent.
- User Dashboard: Each user can see the status of each necessary document, the fields extracted, and the proofs of verification on their personal dashboard.

This architecture ensures a secure, efficient, and privacy-preserving process for the authentication and verification of real estate documents, leveraging Polygon ID and web3 principles.

3.3 Implementation

The application uses React.js for the frontend, Java Quarkus for the backend, and an API utilizing Polygon ID services. During authentication, the user requests authentication within the application, which then queries the API and sends the request to the user's wallet. The user receives the challenge, signs it with their DID, and proves their identity. The verifier undergoes a similar process, additionally proving possession of the verifier VC.

When verifying documents (represented as VCs), the user selects the necessary fields, and the application queries the API to design a query for those fields. Each query specifies the credential type required, the accepted issuers to prevent fake identities, the user's DID to ensure ownership of the credential, the selected fields using selective disclosure to maintain privacy, and the signature type of the VC. The user then creates a proof in their wallet based on these fields and sends it back to the application, which asks the API to verify. The verification process checks that the credential type matches the request, the user owns the VC, the VC's revocation and validity status are confirmed, and the signature authenticity is validated to ensure the issuer issued the credential and it hasn't been modified.

4 Future Work

The next objective is to evaluate the prototype created. The following metrics will be assessed: throughput and latency of user and verifier authentication; throughput and latency of document verification and field extraction, including varying the number of fields requested and the two types of signatures; the percentage of successful verifications, tested with fake issuers and fake user ownerships, aiming for 100%; and user experience as part of qualitative evaluation, to ensure the process is seamless.

Additionally, ZKPs allow users to prove the validity of their credentials without revealing the underlying data, thereby protecting sensitive information during verification [10]. However, currently, we use selective disclosure because the full value is required to fulfill contracts related to the purchase or sale of properties. In the future, ZKPs could be particularly useful for other situations, such as verifying eligibility without revealing exact details (e.g., confirming the user is over a certain age without revealing their exact age, or confirming residency in a city without revealing the exact address).

5 Conclusion

This paper presented a reliable solution for real estate document authentication, addressing the complexity and inefficiency of current methods. By leveraging

web3 technologies, such as DIDs and VCs, and utilizing services provided by Polygon ID, the proposed system enhances the security, trust, and efficiency of document validation processes. This integration simplifies the verification process for real estate agents, ensuring privacy and authenticity while expediting transactions.

Acknowledgments. This work was financially supported by Project Blockchain.PT – Decentralize Portugal with Blockchain Agenda, (Project no 51), WP 6, Call no 02/C05-i01.01/2022, funded by the Portuguese Recovery and Resilience Program (PPR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program. This work was also supported by national funds through Fundação para a Ciência e Tecnologia (FCT) with reference UIDB/50021/2020 (INESC-ID).

References

1. Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J.: Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering **30**(7), 1366–1385 (2018)
2. European Parliament and European Council: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General data protection regulation (2016)
3. Kalyuzhnova, N.: Transformation of the real estate market on the basis of use of the blockchain technologies: opportunities and problems. In: MATEC web of conferences. vol. 212, p. 06004. EDP Sciences (2018)
4. Kemal, M.U.: Anti-money laundering regulations and its effectiveness. Journal of Money Laundering Control **17**(4), 416–427 (2014)
5. Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C.: A survey on essential components of a self-sovereign identity. Computer Science Review **30**, 80–86 (2018)
6. Polygon Technology: Polygon id: Decentralized identity for the web3. `https://polygon.technology/polygon-id/`, last accessed: 2024-07-10
7. Ramić, Š.B., Cogo, E., Prazina, I., Cogo, E., Turkanović, M., Mulahasanović, R.T., Mrdović, S.: Selective disclosure in digital credentials: A review. ICT Express (2024)
8. Sporny, M., Guy, A., Sabadello, M., Reed, D.: Decentralized identifiers (DIDs) v1. 0 - Core architecture, data model, and representations (Jul 2022), W3C Recommendation
9. Sporny, M., Noble, G., Longley, D., Burnett, D.C., Zundel, B., Hartog, K.D.: Verifiable credentials data model v1.1 (March 2022), W3C Recommendation
10. Sun, X., Yu, F.R., Zhang, P., Sun, Z., Xie, W., Peng, X.: A survey on zero-knowledge proof in blockchain. IEEE Network **35**(4), 198–205 (2021)
11. Tilbury, J.L., de la Rey, E., van der Schyff, K.: Business process models of blockchain and South African real estate transactions. In: 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems. pp. 1–7 (2019)