A Blockchain-Based System Proposal for management and monitoring Historical Heritage

Gavina Baralla, Luisanna Cocco and Roberto Tonelli
Department of Mathematics and Computer Science,
University of Cagliari, Italy

Marco Di Francesco
NetService spa Bologna, Italy

I. Introduction

Blockchain technology, initially developed for financial transactions, now plays a crucial role in digital transformation across various industries, including the civil sector. Its integration with the Internet of Things (IoT), Artificial Intelligence (AI), and robotics is revolutionizing data management, offering unprecedented levels of security, transparency, and efficiency. Despite its widespread adoption in several sectors including finance, health or logistic, the civil construction industry remains relatively behind in digitalization efforts.

This paper introduces a Blockchain-based system designed to manage and monitor Italy's historical defense heritage, addressing the civil industry's specific challenges. It aims to digitize and secure the management process, overcoming the traditional reliance on paper documents that leads to information dispersion and inefficiencies inbuilding management and maintenance. This system leverages the Self Sovereign Identity (SSI) paradigm, enabling stakeholders to sign transactions on the Blockchain using their Decentralized Identifiers (DIDs). These identifiers provide a secure and immutable way to authenticate users and their permissions, managed by a Permission Manager through smart contracts. Each building is modeled by a smart contract, which not only store the fingerprints of documents but also implement the logic necessary for certifying all related information, including maintenance activities. The adoption of Blockchain, in concert with Building Information Modeling (BIM), IoT, and AI, targets the transformation of outdated and paper-based information handling in the construction sector. This transformation is critical for tackling the inefficiencies that plague project management, from outdated blueprints to delays and coordination problems among teams. The proposed system is part of the IMASSCHAIN [1] project, aligned with the National Military Research Plan, which seeks to develop a comprehensive governance system for historical real estate through collaboration with defense authorities.

II. System Architecture

The system architecture, presented in Fig. 1 is designed to manage the information flow of the Defense Administration's historical infrastructure, encompassing construction, maintenance, and management projects, and stakeholder-generated information, including IoT device data. Information is stored in an off-chain *Repository*, a data lake composed of various databases to handle the heterogeneity of structured and unstructured data and documents. Structured data from surveys are kept in a relational database, IoT sensor data in a NoSQL database, and documents in a Document Management System (DMS). A *Blockchain module* ensures the integrity and reliability of information by storing fingerprints (hashes) of documents and relevant data on-chain, including cadastral deeds and maintenance documentation. This process, known as notarization, allows to verify in the aftermath documents' authenticity, origin, and unaltered state since a specific date. An *IoT module* allows to monitor parameters like temperature and structural integrity, aiding in diagnostics and maintenance automation with the support of an *AI module*. The *BIM module* facilitates interaction with BIM authoring tools, while an *Enterprise Service Bus (ESB)* orchestrates data exchange among modules.

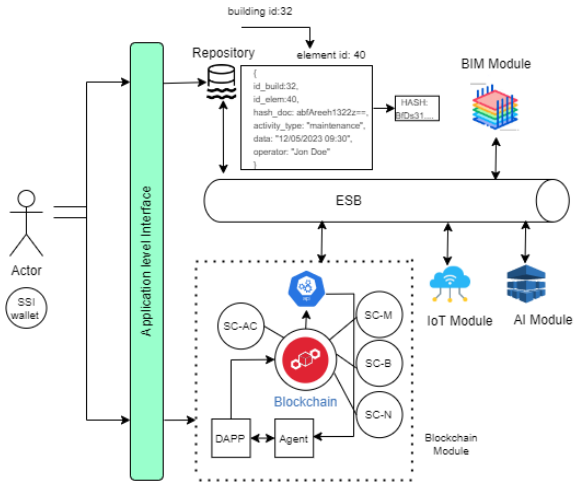

Fig. 1. System Architecture.

A. Blockchain Module development: Methodology

To design the *Blockchain module* the ABCDE method, which is a specific software development process for Blockchain systems, was applied [1]. The main goal of the

[1]Infrastructure Management Support System Chain, under the National Military Research Plan 2020 (CIG: 884399685F - CUP: D84H22001380001)

Blockchain module is to certify all information need to trace the building's state during its entire life cycle. This includes the information flows associated for example with the activities of maintenance or monitoring, but also documents and certificates. The actors of the system are:

- The *system's administrator* that manages the system configuration.
- the *Defence permission Manager* that deploys for each building a smart contract, and associates with each user/stakeholders a precise role in the on-chain subsystem,
- The *Defence authorized users* and stakeholders, such as architects, engineers, and testers, that contribute to associate documents and information with a precise building,
- The *Smart contract(s)* that is the only actor who interacts directly with the blockchain,
- The *Interface* that allows stakeholders to interact with the Blockchain and with the other components of the system.

Figure 2 shows the actors and the user stories below described through a UML Use Case Diagram, where use cases are the user stories.

- The System administrator manages the system configuration ("configure system").
- The Defence permission Manager deploys for each building a smart contract ("deploy smart contract(s))".
- The Defence permission Manager associates with each blockchain address a precise identifier, hence a precise stakeholder, that operates in the system ("create mapping for stakeholders").
- The Defence permission Manager assigns to each actors a role ("assign role").
- The system maps the building's identifier to an address, hence implements the logic to associate a building with a precise Blockchain address, precisely with the smart contract' address associated with the building ("create mapping for buldings").
- Defence authorized users and/or stakeholders certify an activity, hence the system implements the logic need to certify all the information associated for example with the maintenance activity executed ("certify activity").
- The Defence authorized users and stakeholders certify a document, hence the system implements the logic to store on chain the fingerprints of documents ("certify document").

From the user stories just listed is simple proceeding with the division of the system into on-chain and off-chain subsystems. Precisely the on-chain subsystem is composed of four smart contracts, *SC-AC*, *SC-M*, *SC-B*, *SC-N*, while the off-chain subsystem is composed of an interface, precisely an application programming interface (API), and of two blocks. They are the blocks named *DAPP* and *Agent* needed to manage the SSI identities.

B. Building Certification Smart Contracts

The on-chain subsystem is composed of four smart contracts as depicted in Figure 1.

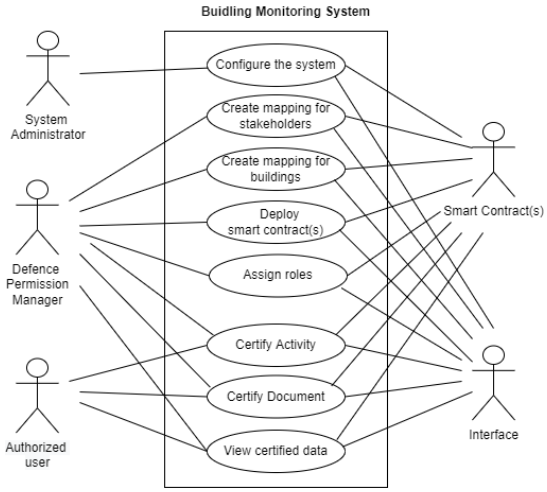

Fig. 2. Use case Diagram

The smart contract, *SC-AC*, associates with each blockchain address a precise identifier, hence a precise stakeholder, that operates in the system. Note that the system in Figure 1 exploits the SSI paradigm's concepts to allow stakeholders to sign their transactions on blockchain. So the blockchain address just mentioned, is the so-called DID that allows to identify an entity within a SSI system.

The smart contract, *SC-M* implements the logic to associate a building with a precise Blockchain address, precisely with the smart contract's address associated with the building.

The smart contract, *SC-N* implements the logic to store on chain the fingerprints of documents not necessarily associated with a building.

Finally the smart contract, *SC-B*, represents the core of the Blockchain subsystem and implements the logic need to certify all the information associated to a precise building. This smart contract manages for example the notarization of json files created by the *Interface* block of the system in Figure 1, and related for example to maintenance activities executed on the building to which *SC-B* refers. Therefore, it includes appropriate data structures for the on-chain storage of the hash of json file, and also appropriate data structures for the on-chain storage of the hash of documents. In addition it also manages the access of the stakeholders to its data structures and to its methods. Stakeholders access has to be managed based on the type of document and based on the user access privileges. For example only users responsible for a given activity has to be able to certify documents relating to that activity. The proposed system can be generalized and adapted to the monitoring and management needs of any building type, offering a scalable and secure solution for the digital transformation of building management across the various property types in real estate.

REFERENCES

[1] L. Marchesi, M. Marchesi, and R. Tonelli, "Abcde—agile block chain dapp engineering," *Blockchain: Research and Applications*, vol. 1, no. 1-2, p. 100002, 2020.