Instituto Tecnológico
y de Estudios Superiores de Occidente

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación del 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática

Especialidad en Sistemas Embebidos

Implementation of an Embedded IoT Blockchain System to Increase the Security of a Healthcare Institution Network

---

TRABAJO RECEPCIONAL que para obtener el **DIPLOMA** de
ESPECIALISTA EN SISTEMAS EMBEBIDOS

Presentan: **MARCO ANTONIO MARES MEJÍA,**
CÉSAR EDUARDO INDA CENICEROS

Asesor: **LUIS JULIÁN DOMÍNGUEZ PÉREZ**

Tlaquepaque, Jalisco. 11 de agosto de 2024.

Implementation of an Embedded IoT Blockchain System to Increase the Security of a Healthcare Institution Network

Marco Antonio Mares Mejía
Departamento de Sistemas Informáticos
ITESO
Guadalajara, Jalisco, México
marco.mares@iteso.mx

César Eduardo Inda Ceniceros
Departamento de Sistemas Informáticos
ITESO
Guadalajara, Jalisco, México
cesar.inda@iteso.mx

Luis Julián Domínguez Pérez
Departamento de Sistemas Informáticos
ITESO
Guadalajara, Jalisco, México
luisjdominguezp@iteso.mx

***Abstract*—Embedded blockchain emerges as an alternative to protect sensible data due to its decentralized network strategy. The objective of this paper is to propose a proof of concept to improve the security of the Mexican Social Security Institute (IMSS) using an IoT embedded blockchain technology. The implementation consists of a smart contract deployed to the Ethereum Testnet to store medical data, and an IoT embedded system interacting with the contract. By adding a blockchain abstraction layer, the embedded system CPU load is reduced. Low-cost and accessible hardware and software parts were utilized. Results demonstrated that blockchain provides more data security when storing patient medical data based on the IMSS network infrastructure. Blockchain can be a feasible and beneficial alternative to traditional cybersecurity networks and applications.**

Keywords: Blockchain, embedded system, smart contract, healthcare, security, IMSS, Web3.

I. Introduction

Blockchain technology refers to an open, decentralized and immutable database that keeps a record of all transactions in a Peer-to-Peer network. An algorithm analyzes new transaction data and verifies its security and validity; then a new block is added to the database chain. Blockchain can provide certainty and security for any data transfer. In this context, blockchain can be considered as a new paradigm for cybersecurity related applications. For instance, Ethereum blockchain provides smart contracts, which are informatic programs that execute a logic algorithm over the network using test nets with simulated money. Smart contracts replace traditional security-related applications with blockchain technology allowing anonymous, decentralized, transparent and inexpensive data transactions.

Many countries use blockchain to store critical information and automate bureaucratic processes. For instance, Stampery is a Spanish mobile app that certifies documents [1]. This app can be used to automate notarized documents at a lower cost. The cost of the app service is around $0.5 USD compared to the lowest notary fee in Mexico City, which is around $240 USD [2].

Considering the network security provided by blockchain technology, the healthcare sector can obtain benefits from implementing blockchain with its IT infrastructure. One of the uses of blockchain technology in the healthcare industry is to keep patient data safe and secure. The U.S. Federal Agency known as Centers for Medical and Medicaid Services (CMS) calculates that for 2031, the National Health Expenditure will increase to 19.6% of Gross Domestic Product (GDP) [3]. Technology experts fear that this investment increase will perpetuate inefficient practices like data breaches. According to the U.S. Department of Health and Human Services Office for Civil Rights (OCR) report in 2023, more than 540 organizations and 112 million individuals were implicated in healthcare data breaches [4]. Therefore, investing in blockchain systems can help mitigate these risks.

Presently, there are several companies investigating the applications of blockchain in healthcare. One example is the Danish company, Novo Nordisk. This company invented a finger-prick device called the Electronic Patient Interactive Device (ePID), a small electronic instrument that collects data from blood samples and sends it to the attending physician [5]. The ePID connects to the cellphone via an app and the data is stored using a blockchain approach. Another company is ProCredEx, which provides services for validation and verification of medical certificates using blockchain techniques [6]. Both companies provide a different approach to secure a healthcare system. The first company collects data, stores and sends data, and the second, validates certificates. These approaches are not limited to private companies; thus, they can also be implemented within the Social Security healthcare system.

The *Instituto Mexicano del Seguro Social* (*IMSS*) is a decentralized organism of the Mexican federal government. It provides social healthcare and social security services to affiliated workers and their families based on their Social Security Number (SSN). The medical consultation process in the clinic is performed in person by the medical staff and the affiliated worker receives proof of attendance. This document is commonly used to obtain medical certification for leave of absence. Blockchain technology can be implemented in IMSS clinics to automate these processes, including the validation of Social Security Numbers (SSN) and proof of attendance documents. Additionally, it can securely store patient medical information and verify the authenticity of these documents.

Therefore, the objective of this paper is to propose a proof of concept for a blockchain healthcare application using IMSS infrastructure as reference.

This paper is organized as follows: Section II describes hardware and software parts used in the implementation. Section III explains the interaction between embedded and blockchain components, additionally, proposes the design of the smart contract. Section IV reports the results stored in the Ethereum blockchain. Section V presents the conclusions and future work.

II. Our Approach: Protection of Medical Data

To address the priority of protecting sensitive data against breaches, an embedded system was established with enhanced security by integrating blockchain services. This approach ensures data integrity and guards against unauthorized access. In addition to the typical optimization of storage resources, the system employs advanced encryption algorithms to safeguard sensitive medical data. This method represents a new paradigm in implementing robust security measures within embedded systems.

Crypto wallets, blockchain services (test networks such as Sepolia), and smart contracts were implemented to the improve the system's functionality and viability by enabling secure transactions, verifying data integrity, and automating trustless interactions.

A. Hardware Components

The implementation of a highly robust, straightforward and scalable prototype was performed using the following low-cost parts:

- ESP32 Board: This microcontroller provides logic flow control over blockchain requests due to its integrated Wi-Fi components. Additionally, it offers comprehensive development tools that facilitate direct programming.
- GME12864-13 Oled Display: This screen functions as the graphic communication with the final user showing recorded medical data and requesting user input.
- MAX30102 Sensor: This sensor reads medical data, such as oxygen in blood, heart rate and blood pressure.
- Matrix Keyboard 4x4: This component records the SSN by the user.

B. Software Components

The following Integrated Development Environments (IDEs), which include a source code editor and a compiler are essential for ensuring a robust and secure development. With the integration of cryptocurrency wallets and blockchain explorers, these IDEs offer a free alternative for blockchain development and are described below:

- Visual Studio Code IDE: Provides a connection with the "Platform IO" extension, tailored for the use of libraries that facilitate functionality with blockchain and Web3 services to interact with smart contracts.
- Web3E: This library enables communication with the blockchain using web functions, there is a repository that has this integration [7].
- Remix Solidity IDE: This online tool facilitates the writing, compilation, and deployment of smart contracts in the Solidity language for use on the Ethereum blockchain
- Sepolia ETH Testnet: This test network allows developers to experiment with blockchain and smart contracts using simulated funds.
- MetaMask: A digital wallet utilized for managing account funds and deploying smart contracts to the blockchain network.
- Etherscan: Blockchain explorer was used to show all the transaction details.

III. Embedded Blockchain in Healthcare

The Sepolia test network was selected to integrate blockchain services into this embedded system architecture. "Fig. 1" delineates the use case diagram of the system. The interaction process between the user and the embedded system leveraging blockchain technology, primarily involves capturing medical data through sensors. The user inputs the Social Security Number (SSN). Then, the data is transmitted through a transaction to the blockchain, and once the process is complete, a block is generated with the recorded data. This block can be accessed at any time using the SSN by printing the previously recorded data to the user [8]. Blockchain interactions generate transactions on the Sepolia network, recording patient data in a smart contract, which is verifiable on Etherscan.

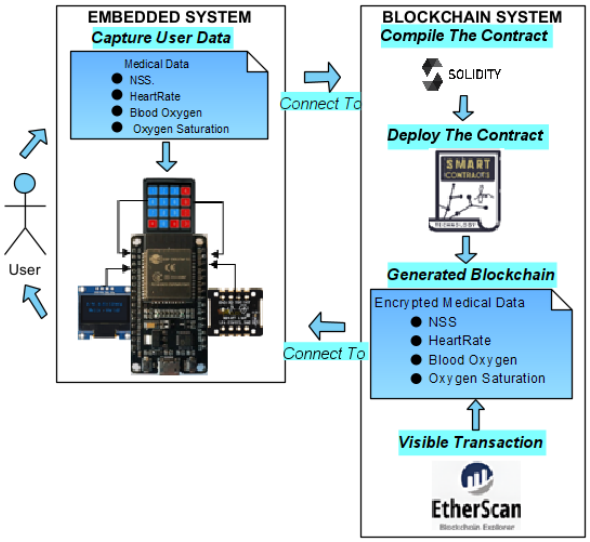

Fig.1 Embedded system use case diagram (UML).

A. *Smart Contract*

The smart contract MedicalData “Fig.2”, operates by using the values obtained from the embedded system. The MedicalRecord structure employs the parameters within the AddMedicaRecord function to create a block containing the user’s data. Subsequently, the GetMedicalRecords function retrieves the stored values, contingent upon the user having the requisite permissions, which are verified by the AuthorizeUser function. This mechanism ensures that access to these data is restricted to authorized user only.

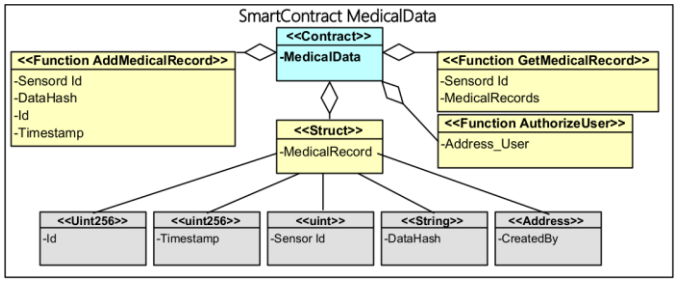

Fig.2 SmartContract MedicalData.

IV. Embedded Blockchain Medical Records

Deployment of Ethereum smart contract on Sepolia Testnet is shown in “Fig. 3”. According to Etherscan, the contract deployment transaction costs around 0.00649 Sepolia ETH ($0.000593 USD). This cost represents a tradeoff between the one-time payment of deploying the contract and the embedded system CPU load.

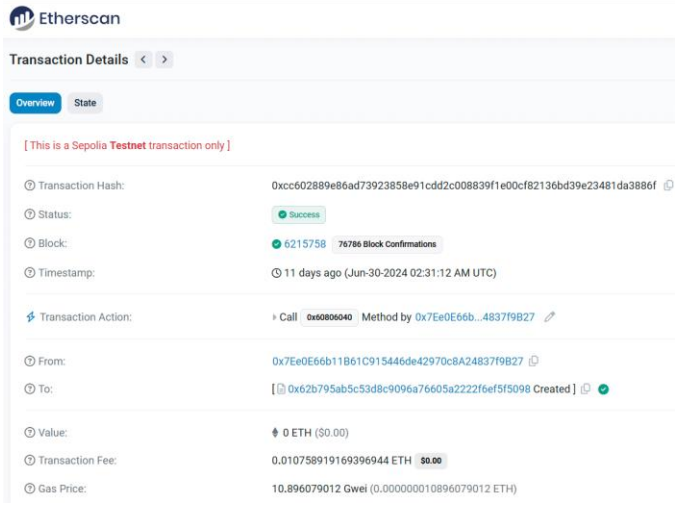

Fig. 3. Medical data smart contract deployment.

The ESP-32 microcontroller is configured with 6575372486 Gwei gas price, 9000000 gas limit and the direction of the cryptowallets and the deployed smart contract. “Fig. 4” shows the transaction of the embedded system calling AddMedicaRecord function.

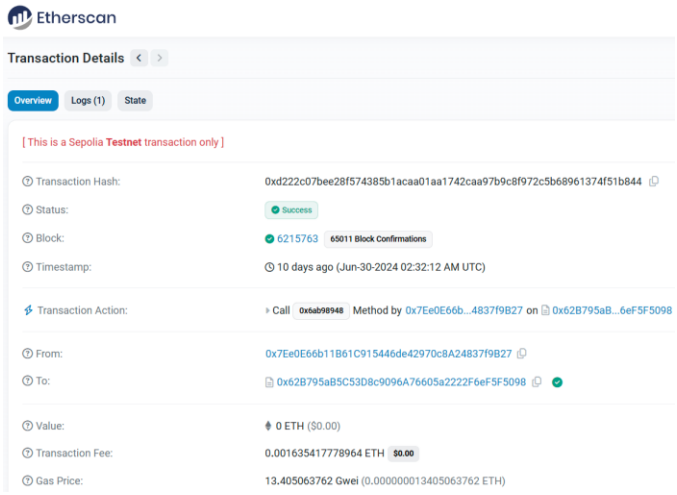

Fig. 4. New medical record creation.

“Fig. 5” shows medical record transaction information. MedicalRecordCount shows that there’s 1 medical record created and GetMedicalRecord shows the ID of the medical record, a sensor reading, embedded system wallet address and the timestamp.

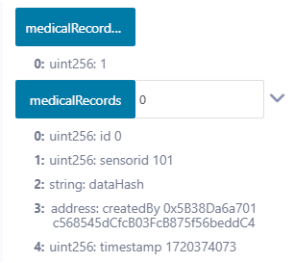

Fig. 5. Reading the medical record.

Medical record containing relevant patient data is stored in a new block on the blockchain. The medical record information is easily readable and permanent, therefore, the user can save the medical record ID for future reference. The blockchain validates the medical record before creating it, thus increasing overall reliability and security of the healthcare institute network. The embedded system CPU load is reduced by handling network operations and memory storage in a decentralized way, therefore, connecting the ESP-32 board to the deployed contract and wait for the response.

V. Conclusion and Future Works

In this paper, the feasibility and benefit of an embedded blockchain application focused on a healthcare institution is presented. Innovations include implementing the ESP-32 board due to its lower price and ease of prototyping in comparison to other hardware platforms. Additionally, using Ethereum as the carrier of data storage, medical records remain immutable, thus assuring integrity, accessibility and non-repudiation of medical data. These three important security attributes can reduce security threats within the healthcare system.

Developing a similar smart contract to address certificates validation is proposed as future work. In addition, a proper prototype can be built and installed in a clinic to test the real performance of the system compared to the consultation process, by monitoring execution time of the system, gas expense and power consumption.

ACKNOWLEDGMENTS

This work was supported by the Jalisco government through the *Secretaría de Innovación, Ciencia y Tecnología* (*SICyT*). The team would like to thank Dr. Luis Julián Domínguez Pérez for his constant support.

REFERENCES

[1] "Stampery: leaders in blockchain-based data certification," Stampery. Accessed: Jul. 07, 2024. [Online]. Available: https://stampery.com

[2] M. N. V. Solano, "Consejería Jurídica Y De Servicios Legales," Ciudad de México, 2024. [Online]. Available: https://consejeria.cdmx.gob.mx/

[3] "NHE Fact Sheet | CMS." Accessed: Jun. 09, 2024. [Online]. Available: https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/nhe-fact-sheet

[4] "U.S. Department of Health & Human Services - Office for Civil Rights." Accessed: Jun. 09, 2024. [Online]. Available: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[5] "Blockchain x Clinical Trials for patient data security." Accessed: Jun. 09, 2024. [Online]. Available: https://techlife.novonordisk.com/cases/epid

[6] "ProCredEx Home ProCredEx." Accessed: Jun. 09, 2024. [Online]. Available: https://procredex.com/

[7] "JamesSmartCell - Overview," GitHub. Accessed: Jul. 07, 2024. [Online]. Available: https://github.com/JamesSmartCell

[8] F. Kabashi, V. Neziri, H. Snopce, A. Luma, A. Aliu, and L. Shkurti, "The possibility of blockchain application in Higher Education," in *2023 12th Mediterranean Conference on Embedded Computing (MECO)*, Jun. 2023, pp. 1–5. doi: 10.1109/MECO58584.2023.10154919.