UNIVERSITÀ DI PARMA

Dipartimento di Ingegneria e Architettura

Corso di Laurea in Ingegneria Informatica, Elettronica e delle Telecomunicazioni

---

Sistema di Certificazione Covid-19 basato su Blockchain

Blockchain-based Covid-19 Certification System

Relatore:
Prof. Francesco Zanichelli

Tesi di Laurea di:
Federico Pappani

ANNO ACCADEMICO 2021/2022

La presente tesi tratta la progettazione, lo sviluppo e l'implementazione di un sistema di gestione e verifica di certificati Covid-19 basato su blockchain. Il sistema consente a uno o più enti certificatori autorizzati di creare certificati Covid-19 per vaccinazioni, guarigioni e negatività al test. I certificati vengono poi rilasciati ai pazienti sottoforma di codice QR, che possono essere scannerizzati da un'apposita app per smartphone che ne verifica l'autenticità. Tutti i dati relativi al sistema (certificati ed enti autorizzati) vengono salvati all'interno di una rete blockchain, in questo caso una testnet di Ethereum. Il sistema è costituito dalle seguenti componenti: uno smart contract, una piattaforma web di amministrazione, una REST API, un app per smartphone. Lo smart contract provvede alla gestione dei dati all'interno della blockchain e alle transazioni di dati da scambiare con i vari utenti del sistema. Lo smart contract viene creato dall'amministratore, che ha il permesso di autorizzare e revocare enti certificatori. Questi ultimi possono a loro volta creare certificati Covid-19, ma non autorizzare altri enti. L'amministratore può inoltre revocare eventuali certificati malevoli o invalidi. La piattaforma web di amministrazione mette a disposizione all'ente certificatore o all'amministratore le funzioni necessarie ad un uso semplice e veloce del sistema. L'utente si autentica con la piattaforma tramite un plugin browser, e attraverso transazioni di criptovaluta registra certificati all'interno della blockchain. Per verificare la validità dei certificati è stata creata un'applicazione per smartphone che legge i QR code tramite fotocamera e interroga un'apposita REST API, che restituisce all'applicazione il risultato della verifica. La REST API gira su un server NodeJS ed è sviluppata tramite l'ausilio della libreria ExpressJS. La piattaforma di amministrazione è sviluppata con il framework ReactJS, e si interfaccia con lo smart contract tramite la libreria Web3JS, che ne gestisce ogni aspetto legato alla blockchain. L'app per smartphone è scritta in React Native, e distribuita tramite la suite Expo. Il deploy dello smart contract è avvenuto sulla rete Rinkeby, con tecnologia Ethereum, mentre l'hosting della piattaforma di amministrazione e dell'API sono gestite rispettivamente da Vercel ed Heroku. Il sistema è facile da usare, funzionale e veloce nelle operazioni, risultando scalabile in termini di utenti e traffico, nonché future-proofed dal punto di

vista delle funzionalità. L'intero sistema implementa strategie per garantire la sicurezza dei dati trattati e preservare la privacy dei cittadini, come l'anonimizzazione dei dati salvati, comunicazioni crittografate end-to-end, ed alcuni accorgimenti implementativi. Il sistema è molto rapido, impiegando circa un secondo per verificare un certificato, e una decina di secondi per creare un nuovo certificato, in base al corrente utilizzo della rete.