

Descrizione tecnica della piattaforma YourCompany

DizMe - Hackathon_21

Michele Bonini
Martino Simonetti

2021

Indice

Introduzione	2
1 Il caso d'uso	3
2 Implementazione	5
2.1 La blockchain di Algorand	5
2.2 Il sito e il framework di DizMe	6
2.3 Interazioni fra DizMe Wallet e YourCompany	7
2.4 Interazioni fra YourCompany e Algorand	7
2.5 Il database	7
2.6 L'interfaccia grafica	8
2.7 YourCompany e GDPR	11
3 Manuale d'uso	12
4 Sviluppi futuri	14
4.1 Sezioni da implementare	14
4.2 Nuovi casi d'uso	15

Introduzione

YourCompany è un sito web che propone un'interfaccia semplice ed intuitiva, che permette di interagire con la blockchain di **Algorand** attraverso un wallet collegato univocamente ad una persona fisica tramite il **DizMe wallet**. Questa corrispondenza univoca fra persona fisica, certificata da **infoCert**, e wallet Algorand è fondamentale per la soluzione che proponiamo. Il caso d'uso che ci siamo impegnati ad affrontare: lo sviluppo di un **passaporto vaccinale**.

YourCompany propone l'utilizzo degli Algorand Standard Asset (ASA) come rappresentazione digitale di una dose vaccinale. Avere un wallet univocamente collegato ad una persona fisica permette al legislatore di inviare le dosi alla persona fisica alla quale la dose è stata somministrata.

Capitolo 1

Il caso d'uso

Realizzazione di un sistema che permetta di rilasciare un attestato di vaccinazione o passaporto vaccinale, sotto forma di credenziale digitale. La suddetta credenziale dovrà essere verificabile da una terza parte.

Diagramma casi d'uso:

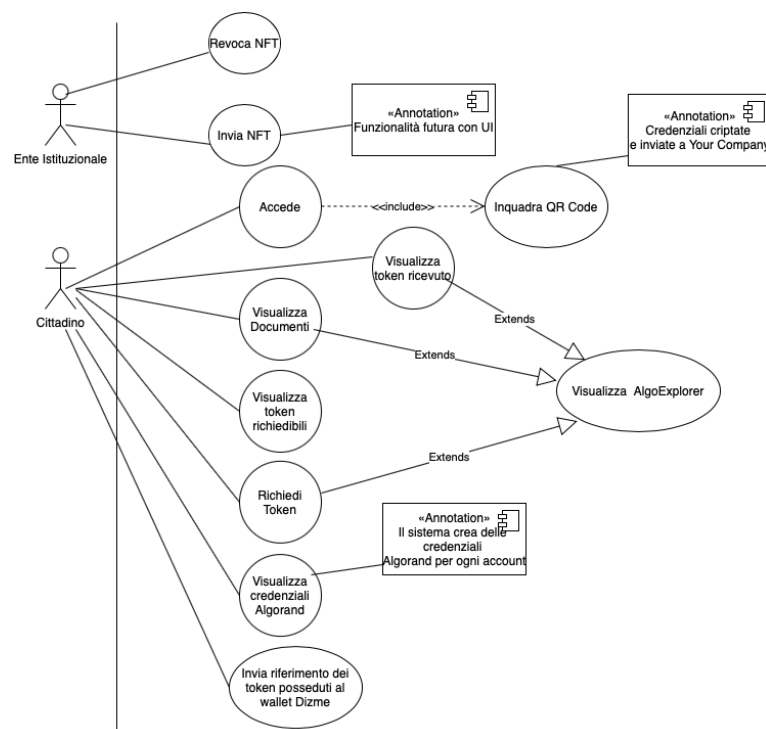


Figura 1.1: Diagramma dei casi d'uso.

Considerando quanto sopra citato e il fatto che l'infrastruttura sarà gestita dallo Stato sono stati evidenziate le seguenti caratteristiche come fondamentali per la soluzione da proporre:

- *flessibilità*: le informazioni sul Covid, vaccini e le scoperte scientifiche legate ad esse sono in continuo divenire, ciò comporta che il sistema di rilascio delle credenziali dovrà essere flessibile per adattarsi a probabili evoluzioni legislative;
- *sicurezza*: il sistema dovrà essere sicuro e non manomettibile;
- *trasparenza*: chiunque dovrà poter verificare l'autenticità dei dati rilasciati;
- *privacy*: la sicurezza dei dati degli utenti devono essere una priorità;
- *economicità*: il sistema dovrà essere sostenibile dal punto di vista economico;
- *affidabilità*: il sistema dovrà essere affidabile e scalabile, anche con migliaia di richieste al minuto dovrà rispondere efficientemente;

Capitolo 2

Implementazione

In questa sezione verranno descritte le principali scelte implementative che sono state fatte.

2.1 La blockchain di Algorand

Algorand offre l'infrastruttura sulla quale vengono registrate le somministrazioni dei vaccini. Gli ASA offrono un ottimo strumento per la rappresentazione di un lotto vaccinale, dove:

- un asset rappresenta l'insieme delle dosi di vaccino di un tipo (tipi di vaccino: AstraZeneca, Pfizer, J&J e Moderna) rilasciate da un'unica struttura,
- un'unità di asset rappresenta una dose di vaccino.

Fra le caratteristiche più interessanti che gli ASA offrono e che ci hanno fatto propendere per il loro utilizzo sono i seguenti:

- la possibilità di freeze un account per un determinato asset, ciò impedisce al possessore del wallet di scambiare delle unità di un asset con altri wallet;
- la possibilità di revocare un asset ad un dato wallet, molto utile in caso di errori.

La scelta è ricaduta sulla blockchain per rendere le transazioni il più trasparente possibile. Pensiamo che soprattutto quando si va a gestire la "cosa pubblica" la trasparenza sia fondamentale. Attraverso la piattaforma **Algo Explorer** (<https://algoexplorer.io>) è possibile visualizzare tutte le transazioni che avvengono sulla blockchain, andando a verificare chi è in possesso o meno un determinato token. Attraverso il suo sito YourCompany, analogamente a quanto può fare su Algo Explorer, l'utente potrà vedere visualizzare il suo bilancio di Algo e ASA.

Il riferimento a tali token verrà inviato al wallet Dizme sotto forma di credenziale, in modo da poterle utilizzare come **attestazione di vaccinazione**.

Sarebbe stato possibile salvare le credenziali in un normale DB e utilizzare direttamente gli strumenti che DizMe offre, abbiamo scelto la blockchain per le sue caratteristiche di sicurezza, trasparenza e affidabilità.

2.2 Il sito e il framework di DizMe

Il sito web è stato sviluppato utilizzando i seguenti linguaggi e framework:

- Python,
- Django,
- JavaScript,
- Html,
- CSS,
- SQL

Il framework di DizMe che è stato utilizzato è reperibile al seguente indirizzo <https://github.com/dizme/Foundation>.

2.3 Interazioni fra DizMe Wallet e YourCompany

Le interazioni fra il DizMe wallet e la pagina web di YourCompany sono mediate dal Dizme Stack.

Le principali interazioni presenti sono:

- **Connessione alla propria area personale:** attraverso il widget di DizMe il sito genera un QRCode che se inquadrato dal DizMe wallet permette all'utente di inviare delle informazioni al sito, fra le quali la più importante è il codice fiscale, e loggarsi nella sua area personale del sito YourCompany;
- **Rilascio di credenziali sul DizMe wallet:** attraverso un pulsante sulla pagina è possibile inviare una credenziale al proprio DizMe wallet che l'utente può scegliere se accettare o meno.

2.4 Interazioni fra YourCompany e Algorand

Le interazioni fra la blockchain e il sito YourCompany avvengono attraverso delle funzioni in back-end che attraverso una sandbox comunicano con la Testnet di Algorand.

Le principali interazioni presenti sono:

- **Richiesta del balance:** in diverse occasioni YourCompany richiede il bilancio di un wallet per un determinato token;
- **Opt-in:** per poter ricevere un determinato asset l'utente deve effettuare una "richiesta" che prende il nome opt-in, in seguito alla segnalazione il wallet dell'autorità sanitaria potrà inviare l'unità di vaccino sotto forma di ASA all'accout richiedente.

2.5 Il database

Dal momento che il template messo a disposizione da DizMe utilizza un database PostgreSQL, si è optato per mantenerlo anche per la tabella da noi aggiunta deno-

minata **account**. Questa tabella possiede al suo interno 3 campi: *codice fiscale*, *wallet algo*, *private key*. Per quanto riguarda i codici fiscali, verranno inviati a YourCompany attraverso il widget Dizme e le proof template. Durante la prima connessione da parte dell'utente con la piattaforma verrà creato un nuovo portafoglio algorand ed il suo indirizzo corrisponderà al campo *wallet algo* mentre la chiave privata (la quale verrà comunicata all'utente) al campo *private key*. Ad ogni codice fiscale, prima di essere inserito, verrà applicata una funzione hash, in modo tale da mantenere l'anonimicità dell'utente.

2.6 L'interfaccia grafica

Per quanto riguarda l'interfaccia grafica, dal momento che si tratta di un prototipo, si è deciso di optare per qualcosa di minimale e semplice. Inoltre, tale applicazione è pensata per cittadini ed enti istituzionali. La sezione inerente a quest'ultimi sarà da migliorare ed approfondire aggiungendo funzionalità specifiche e permettendo loro di rilasciare token direttamente dal portale YourCompany. Al momento, il rilascio dei token, è possibile solo da linea di comando. Tornando all'interfaccia della nostra organizzazione, è presente un login mediante il quale è possibile accedere solo se si è in possesso di un proprio wallet sull'applicazione Dizme. Inoltre, in tale wallet, deve essere stato inserito e verificato il proprio codice fiscale. Grazie ad esso sarà possibile accedere a YourCompany attraverso un QRCode che verificherà se l'utente è davvero in possesso del codice fiscale. Anche la sezione dedicata al profilo risulta essere semplice e minimale, proprio per non generare senso di malessere o disorientamento all'interno del portale. Da tale schermata è possibile richiedere uno specifico token oppure inviare al wallet Dizme la prova che si è in possesso del token (attraverso l'utilizzo del rilascio delle credenziali). Per questo caso d'uso, ogni token corrisponderà ad una specifica dose di vaccino. Di conseguenza, qualora l'utente fosse in possesso di due token associati allo stesso **asset id** (il quale identifica un particolare **NFT - Non Fungibile Token**), si potrà assumere che tale persona avrà effettuato entrambe le dosi di vaccino richieste.

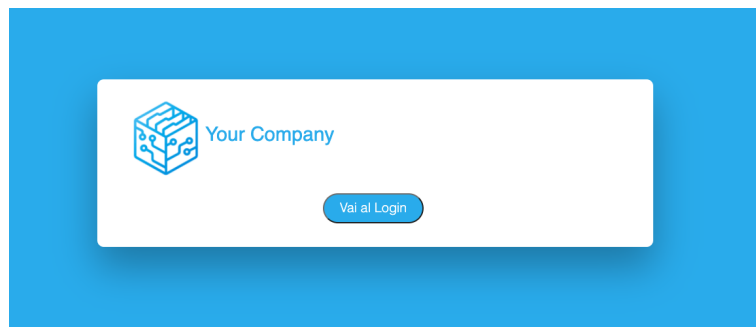


Figura 2.1: Il login.

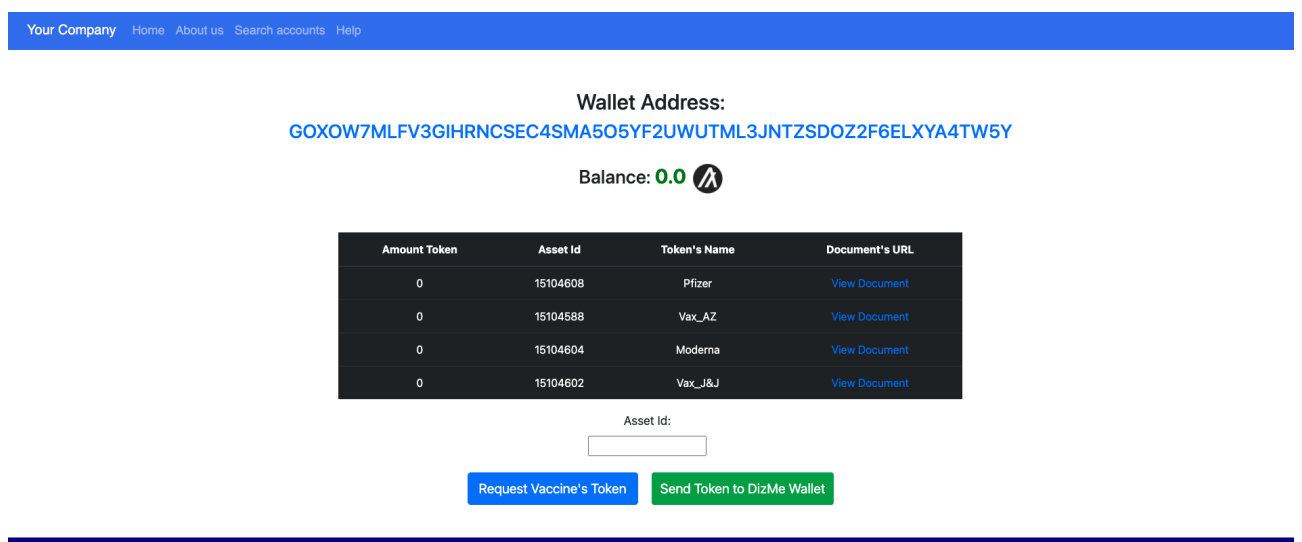


Figura 2.2: La sezione account.



Figura 2.3: Vaccini che mettono a disposizione token.



Figura 2.4: Esempio di una transazione visualizzata su Algo Explorer.

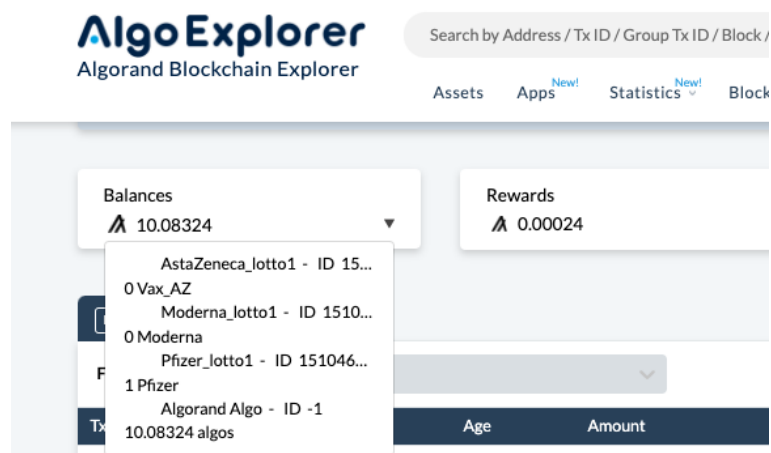


Figura 2.5: Alcune informazioni inerenti l'ammontare di token posseduti da un utente.

Your Company

Wallet Address:
GOXOW7MLFV3GIHRNCSEC4SMA5O5

Balance: 0.0

Amount Token	Asset Id	Token's Name	Document's URL
0	15104608	Pfizer	View Document
0	15104588	Vax_AZ	View Document
0	15104604	Moderna	View Document
0	15104602	Vax_J&J	View Document

Asset Id:

Request Vaccine's Token

Send Token to DizMe Wallet

Available Assets




Figura 2.6: Visualizzazione in modalità responsive.

2.7 YourCompany e GDPR

Il sistema che viene proposto ha da subito avuto l'obiettivo di minimizzare il numero dati personali utilizzati all'interno del sistema. Il sistema non permette conoscere la corrispondenza fra Algo wallet e identità della persona fisica.

Capitolo 3

Manuale d'uso

In questa sezione verrà descritto come poter avviare il progetto.

Per poter eseguire il progetto oggetto di questo lavoro sarà necessario installare ed avviare la sandbox di Algorand, la quale permette di impostare un nodo in un ambiente container. Dopo aver installato il tool **docker-compose**, bisognerà lanciare i seguenti comandi da terminale:

- *git clone https://github.com/algorand/sandbox.git;*
- *cd sandbox;*
- *./sandbox up testnet;*

Con l'ultimo comando, "*./sandbox up testnet*", sarà possibile avviare la sandbox e sincronizzarsi con la rete **testnet** di Algorand. Questo passaggio è fondamentale per il buon funzionamento della piattaforma YourCompany. Bisognerà trovare il proprio indirizzo IP ed assegnarlo agli appositi parametri all'interno del file **generic_organization_conf.env**. Dopo essersi recati nella directory corretta, bisognerà avviare il file **docker-compose-db-redis** mediante il comando: *docker-compose -f docker-compose-db-redis.yaml up*. Successivamente, bisognerà creare il database PostgreSQL eseguendo i seguenti passi:

- Aggiungere un nuovo server utilizzando il proprio indirizzo IP;

- A partire dall'utente *postgres* creare un nuovo database denominato **generic_organization_db** con password **organization_db_password**.
- Aggiungere la tabella **account** con i campi **codice_fiscale**, **wallet_algo**, **private_key**.

Infine, in un'altra finestra del terminale, sarà necessario eseguire il file **docker-compose-dev** attraverso il comando *docker-compose -f docker-compose-dev.yaml up*. Consigliamo di lanciare questo file utilizzando *docker-compose -f docker-compose-dev.yaml up --build* qualora fosse la prima esecuzione in assoluto. La piattaforma sarà raggiungibile da Browser all'indirizzo **http://*"inserire qui il proprio indirizzo IP"*:8015/home/**.

Capitolo 4

Sviluppi futuri

In questa sezione verrà descritto in primo luogo cosa manca al progetto perché possa rispondere a pieno al caso d'uso e in secondo luogo a quali altri casi d'uso si può adattare l'applicazione sviluppata.

4.1 Sezioni da implementare

- Interfaccia grafica per gli istituti che somministrano i vaccini, attualmente questa sezione è funzionante ma senza UI;
- sicurezza, sarà necessario implementare ed aumentare le difese da possibili attacchi;
- aggiungere delle tabelle nel DB dove registrare gli indirizzi degli enti autorizzati a rilasciare NFT e gli ASA correttamente rilasciati;
- attualmente la credenziale sul DizMe wallet punta ad una pagina di Algo Explorer dov'è possibile verificare l'asset, fondamentale sarà cambiare questo puntatore: una volta scansionato il QRCode presente nella credenziale rilasciata sul DizMe wallet si aprirà una pagina di YourCompany che dopo aver effettuato le dovute verifiche permetterà di visualizzare a schermo due semplici messaggi, o "PASSAPORTO VALIDO!" o "PASSAPORTO SCADUTO!".
- implementare la UI implementando suggerimenti che possano aiutare utenti meno esperti.

4.2 Nuovi casi d'uso

Pensiamo che attraverso gli ASA possa passare una vera e propria rivoluzione per quanto riguarda il rilascio di documenti digitali da parte delle autorità, l'enorme potenzialità deriva dal fatto che i wallet di ente pubblico e cittadino possono essere univocamente riconducibili agli stessi. Seguono alcuni esempi di possibili implementazioni

- **Rilascio attestato di negatività al covid 19:** un ospedale che esegue tamponi potrà creare i suoi ASA, dove chiunque possieda un'unità dell'asset potrà essere considerato negativo, sappiamo che spesso i tamponi hanno una validità di qualche giorno, sarà quindi possibile, ad esempio, inviare l'asset e revocarlo automaticamente dopo un numero definito di giorni.
- **Motorizzazione rilascia la patente:** alla patente fisica si associa anche una versione virtuale (ASA), se dovesse occorrere una circostanza per la quale la patente debba essere revocata, l'asset verrà revocato.

Entrambi gli esempi sono di veloce implementazione.

Interessante è notare come tramite la possibilità di revocare un ASA sia superato il concetto di revocation-list.