



AlphaNotary

Versione: 1.0.0

Autore: Adnan Latif Gazi
Data: 8 luglio 2022

Sommario

Abstract	3
Introduzione.....	4
Descrizione	4
Obiettivi.....	4
Suddivisione del lavoro.....	5
Progettazione.....	8
Schema	8
Organizzazione	10
Linguaggi	11
Tecnologie	11
Realizzazione	13
Struttura	13
Back-end.....	14
Front-end.....	14
Esecuzione	15
Avvio.....	15
Installazione	15
Esecuzione di test.....	15
Esecuzione locale	16
Distribuzione	16
Pagina di presentazione.....	18
Pagina di notarizzazione	29
Analisi tecnica	41
Mantenimento	42
Sviluppo.....	42
FAQ	42
Utili	44
Glossario.....	44

Abstract

Questa è la documentazione di AlphaNotary, il progetto di stage curriculare di Adnan Latif Gazi, svolta in data dal 23 maggio 2022 al 22 luglio 2022 nell'azienda Venicecom per conto dell'Università degli Studi di Padova.

Questo documento ha l'obiettivo di presentare il prodotto finale del progetto in ogni suo aspetto: a partire dall'introduzione, alla progettazione, realizzazione, esecuzione, e infine mantenimento, con lo scopo di avviare l'utente al suo utilizzo e colmare ogni eventuale interrogativo.

Il capitolo relativo all'introduzione descrive il funzionamento e le caratteristiche del sistema, quello della progettazione divulga gli schemi, i linguaggi e le tecnologie alla base dell'impianto, quello della realizzazione rivela la procedura di sviluppo rispettivamente della struttura, del back-end e del front-end, quello dell'esecuzione mostra tutti i passaggi da compiere per la configurazione e l'avvio del programma, con una nota di analisi tecnica per esaminare la qualità del prodotto finale, e infine quello del mantenimento spiega lo sviluppo e l'integrazione di future componenti, e le modalità di commercializzazione del sistema, nel caso in cui si volesse espandere ulteriormente l'apparato in futuro e pubblicarlo.

Si rammenta però, che AlphaNotary è solamente un progetto di stage; pertanto, è il frutto di poche settimane di lavoro individuale di uno studente universitario alle prese con un prodotto prima del suo tirocinio ancora completamente da concepire, e quindi vincolato a realizzarne ogni suo aspetto: ciò costringe a ridurre la qualità di dettaglio del lavoro a favore di un risultato visibile e funzionante, e fa sì che tale risultato sia qualitativamente all'altezza solamente di un progetto di stage, ma non oltre, come ad esempio un sistema utilizzato ufficialmente da un'azienda, creando quindi dipendenze pericolose. Se inoltre si considera che la messa focale dell'apprendistato era istruire lo studente sui domini del progetto e introdurlo nel mondo lavorativo, si realizza subito come il programma sia inadatto, anche se pienamente possibile, da essere sviluppato, integrato o commercializzato. Considerando invece, il prodotto per ciò che è, ovvero un progetto di stage, il risultato è notevole: tutti gli insegnamenti, sia quelli acquisiti durante gli anni di studio che quelli recepiti durante il tirocinio, sono stati messi in pratica, ottenendo una qualità finale molto elevata. Il motivo del rammento risiede nel fatto che lo studente non dispone di conoscenze, tempi o esperienze sufficienti a compiere l'ulteriore salto di qualità. Per raggiungere tale obiettivo, il prodotto dovrebbe essere più solido, e ciò richiederebbe rivederne la progettazione e la realizzazione da capo pensando preventivamente a tutti i fattori legali, tecnici ed economici che costituiscono la differenza suddetta. Pertanto, lo studente non si assume la responsabilità nel caso in cui il suo prodotto dovesse essere utilizzato al di fuori delle cerchie sopra denotate, causando problemi di qualunque genere.

In ultimo, si ricorda che alcuni dei termini meno comuni e più caratteristici del progetto sono descritti approfonditamente nel glossario alla fine del documento.

Introduzione

Descrizione

L'azienda utilizza un'applicazione non proprietaria per la notarizzazione, ovvero l'autenticazione di documenti. Quando si carica un nuovo documento nel sistema, viene ricavata da esso una chiave poi memorizzata nella Blockchain. Quando invece si vuole verificare l'autenticità di un documento precedentemente caricato, esso deve essere un'altra volta aggiunto al sistema, così da potervi calcolare nuovamente una chiave di cui controllare la presenza nella Blockchain. Se il documento sarà stato modificato nel tempo, verrà restituito esito negativo, segnalando il fallimento dell'autenticazione e avvertendo della modifica del documento, poiché la chiave prodotta al momento del caricamento iniziale sarà diversa da quella ricavata al momento dell'autenticazione, in quanto documenti minimamente diversi producono chiavi diverse.

Si vuole creare una dApp, ovvero applicazione distribuita online, di notarizzazione analoga a quella già in uso dall'azienda, ma di essa proprietaria, in modo da eliminare le dipendenze dai sistemi esterni, riducendo così i costi e semplificando la gestione dell'infrastruttura. Si vuole inoltre arricchire tale dApp con un'interfaccia di monitoraggio, ovvero una piattaforma in grado di eseguire le funzionalità dell'applicazione principale e visualizzarne i risultati al fine monitorare il loro corretto funzionamento. Successivamente, si desidera espandere la dApp di una serie di funzionalità complementari di gestione dei documenti, in grado di permettere di gestire in modo completo i documenti coinvolti nel sistema.

Questo progetto serve anche per l'interesse dell'azienda di formare lo studente sugli argomenti del lavoro, in modo non precludere la possibilità di future collaborazioni per proseguire lo sviluppo del sistema. Infatti, L'azienda vuole espandere l'uso della Blockchain in molteplici contesti d'uso. Viene quindi richiesto allo studente di produrre anche una serie di documentazioni in merito allo sviluppo del progetto, in particolare per ogni obiettivo prefissato, facilitando la comprensione e quindi la realizzazione di progetti futuri.

Obiettivi

Lo studente svilupperà i seguenti prodotti finali:

1. DApp di notarizzazione: progettazione e realizzazione di un'applicazione che ha il compito di eseguire notarizzazione sulla Blockchain al fine di mettere a disposizione un sistema per autenticare i documenti aziendali.
2. Documentazione della dApp di notarizzazione: stesura della documentazione tecnica che ha compito di presentare la dApp di notarizzazione, nonché di descriverne la progettazione e la realizzazione.
3. Interfaccia di monitoraggio: progettazione e realizzazione di una piattaforma che ha compito di arricchire l'applicazione principale eseguendone le funzionalità e visualizzandone i risultati al fine di monitorare il loro corretto funzionamento.
4. Documentazione dell'interfaccia di monitoraggio: stesura della documentazione tecnica che ha compito di presentare l'interfaccia di monitoraggio, nonché di descriverne la progettazione e la realizzazione.

Conseguito questi prodotti e per quanto possibile nel tempo rimanente, lo studente svilupperà i rispettivi prodotti finali e facoltativi:

1. Funzionalità complementari di gestione dei documenti: progettazione e realizzazione di una serie di funzionalità che hanno il compito di arricchire l'applicazione principale per permettere di gestire in modo completo i documenti coinvolti nel sistema.
2. Documentazione delle funzionalità complementari di gestione dei documenti: stesura della documentazione tecnica che ha compito di presentare le funzionalità complementari di gestione dei documenti, nonché di descriverne la progettazione e la realizzazione.

Si prevede il raggiungimento dei seguenti obiettivi:

- **Obbligatori**
 1. formazione sui domini coinvolti nel progetto;
 2. progettazione e realizzazione del protocollo Smart Contract;
 3. progettazione e realizzazione della dApp di notarizzazione;
 4. progettazione e realizzazione dell'interfaccia di monitoraggio.
- **Desiderabili**
 1. documentazione del protocollo Smart Contract;
 2. documentazione della dApp di notarizzazione;
 3. documentazione dell'interfaccia di monitoraggio.
- **Facoltativi**
 1. progettazione e realizzazione delle funzionalità complementari di gestione dei documenti;
 2. documentazione delle funzionalità complementari di gestione dei documenti.

Suddivisione del lavoro

Lo stage prevede 8 settimane di lavoro a tempo pieno, per un totale di 320 ore collocate in un periodo di 9 settimane di lavoro, per lasciare margine di sicurezza, comprendente le seguenti attività così distribuite:

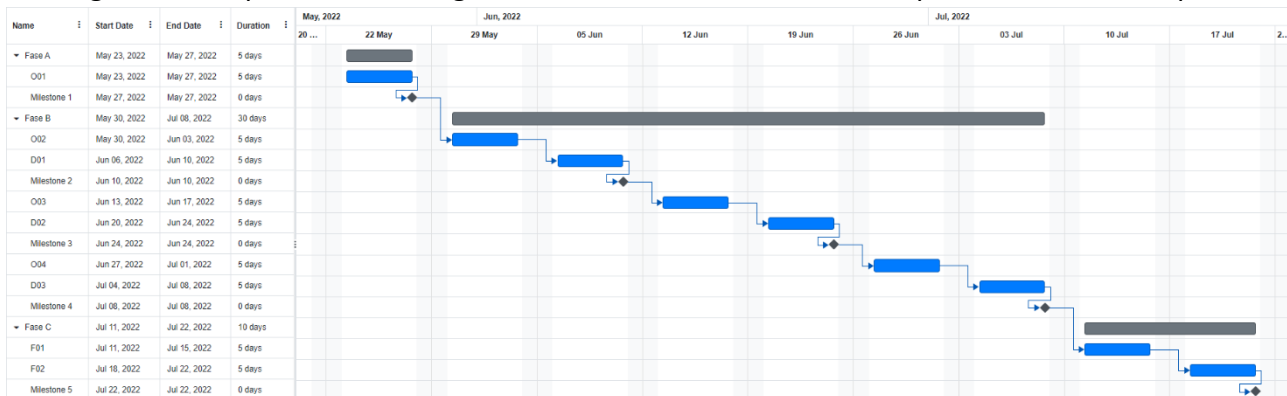
- **Prima Settimana - introduzione e formazione sui domini coinvolti nel progetto (35 ore):**
 - presa visione dell'infrastruttura aziendale (5 ore);
 - configurazione dell'ambiente di lavoro discussione al dettaglio del progetto (10 ore);
 - formazione sui domini coinvolti nel progetto: Blockchain, notarizzazione, Blockchain Ethereum compatibili e crittografia (wallet e chiavi) (20 ore);
- **Seconda settimana - progettazione e realizzazione del protocollo Smart Contract (35 ore):**
 - studio del protocollo Smart Contract (7.5 ore);
 - progettazione del protocollo Smart Contract (7.5 ore);
 - realizzazione del protocollo Smart Contract (20 ore).
- **Terza settimana - documentazione del protocollo Smart Contract (35 ore):**
 - verifica e collaudo della dApp di notarizzazione (7.5 ore);
 - documentazione della dApp di notarizzazione (7.5 ore);
 - sviluppo e distribuzione della dApp di notarizzazione (20 ore).
- **Quarta settimana - progettazione e realizzazione della dApp di notarizzazione (35 ore):**
 - studio della dApp di notarizzazione (7.5 ore);

- progettazione della dApp di notarizzazione (7.5 ore);
- realizzazione della dApp di notarizzazione (20 ore).
- **Quinta settimana - documentazione della dApp di notarizzazione (35 ore):**
 - sviluppo e distribuzione della dApp di notarizzazione (20 ore);
 - verifica e collaudo della dApp di notarizzazione (7.5 ore);
 - documentazione della dApp di notarizzazione (7.5 ore).
- **Sesta settimana - progettazione e realizzazione dell'interfaccia di monitoraggio (35 ore):**
 - studio dell'interfaccia di monitoraggi (7.5 ore);
 - progettazione dell'interfaccia di monitoraggi (7.5 ore);
 - realizzazione dell'interfaccia di monitoraggi (20 ore).
- **Settima settimana - documentazione dell'interfaccia di monitoraggio (35 ore):**
 - sviluppo e distribuzione dell'interfaccia di monitoraggi (20 ore);
 - verifica e collaudo dell'interfaccia di monitoraggi (7.5 ore);
 - documentazione dell'interfaccia di monitoraggi (7.5 ore).
- **Ottava settimana - progettazione e realizzazione delle funzionalità complementari di gestione dei documenti (35 ore):**
 - studio delle funzionalità complementari di gestione dei documenti (7.5 ore);
 - progettazione delle funzionalità complementari di gestione dei documenti (7.5 ore);
 - realizzazione delle funzionalità complementari di gestione dei documenti (20 ore).
- **Nona settimana - documentazione delle funzionalità complementari di gestione dei documenti e conclusione (40 ore):**
 - sviluppo e distribuzione delle funzionalità complementari di gestione dei documenti (20 ore);
 - verifica e collaudo delle funzionalità complementari di gestione dei documenti (7.5 ore);
 - documentazione delle funzionalità complementari di gestione dei documenti (7.5 ore);
 - dimostrazione e consegna del prodotto finale (5 ore).

La pianificazione, in termini di quantità di ore di lavoro, sarà così ripartita:

Durata in ore	Descrizione dell'attività
65	Formazione sui domini coinvolti nello sviluppo del sistema
60	Progettazione e documentazione
10	<i>Analisi del problema e del dominio applicativo</i>
15	<i>Progettazione della soluzione e relativi test</i>
5	<i>Pianificazione del lavoro</i>
30	<i>Documentazione sulla progettazione, realizzazione e presentazione</i>
160	Realizzazione dei sistemi e implementazione delle funzionalità
85	<i>Realizzazione dei sistemi</i>
80	<i>Implementazione delle funzionalità</i>
35	Verifica, collaudo e dimostrazione
20	<i>Verifica della progettazione e del codice</i>
10	<i>Collaudo dei sistemi realizzati e delle funzionalità implementate</i>
5	<i>Dimostrazione del sistema finale agli stakeholders</i>
Totale ore	320

Di seguito è riportato il diagramma di Gantt relativo al piano di lavoro previsto.



Progettazione

Schema

Il sistema presenta un'infrastruttura molto complessa, vale pertanto la pena di analizzarne il funzionamento. Molti sistemi sono coinvolti, sia dentro il prodotto, che fuori. Per quanto concerne l'insieme delle interazioni esterne, si comincia ovviamente dall'applicazione che comunica con una crypto wallet, ovvero un portfolio digitale che permette di gestire il proprio account, le configurazioni di rete, il portafoglio cripto (ovvero del mondo delle Blockchain), e confermare le transazioni. In questo caso viene usato MetaMask, un'estensione da installare in un browser compatibile, per poi creare un proprio account con denaro e configurare le reti di Blockchain interessate. MetaMask sarebbe in grado di comunicare direttamente con le Blockchain, ma essendo queste molto vaste, è difficile che le transazioni vengono correttamente effettuate tutte le volte, perché con una rete configurata normalmente, si conosce l'indirizzo della Blockchain interessata ma non l'indirizzo dell'area precisa in cui sono stati salvati i precedenti blocchi di una stessa applicazione. Si sfrutta quindi, il servizio offerto dai provider, come Infura, che permettono di creare un nodo intermedio che si pone tra MetaMask e le Blockchain: inizializzando un account e avviando un abbonamento, anche gratuito se sotto una determinata soglia giornaliera di blocchi di Blockchain consumati con le transazioni (sufficienti per lo sviluppo del sistema ma non in caso si voglia usare professionalmente il prodotto), il servizio mette a disposizione configurazioni per diverse reti di Blockchain che si può importare su MetaMask, in modo che quest'ultima inoltri al provider le transazioni, e poi sarà essa ad accedere correttamente alla porzione di Blockchain in cui tutti i dati del sistema sono salvati, assicurando le possibilità di completamento della transazione tanto quanto velocizzando l'intero processo.

Per la successiva tecnologia bisogna fare un'importante distinzione: una Blockchain è una struttura dati a forma di lista concatenata in cui dati vengono criptati, suddivisi e inseriti in pacchetti chiamati blocchi, e accodati all'ultimo blocco della Blockchain. È una struttura non reversibile, nel senso che non è possibile togliere un dato, che quindi rimane per sempre, in quanto per questa operazione sarebbe necessario eliminare tutti i blocchi ad esso successivi, rimuovere il blocco d'interesse, e infine di inserire gli altri blocchi tolti (operazione non ammessa, soprattutto perché, essendo una struttura condivisa, nel frattempo altre transazioni potrebbero cercare di inserire nuovi blocchi, e non è ammissibile pensare di bloccare l'intera Blockchain per esso). Una Blockchain è gestita da sé stessa, pertanto non sono permesse eccezioni o interventi umani da parte di amministratori. Una piattaforma decentralizzata Web3.0 è invece un sistema per amministrare uno o più Blockchain, che a loro volta possono essere usate da più piattaforme.

Una piattaforma è quindi in grado, ricevuto una transazione, di ricavarne i dati e sfruttare una Blockchain indicata per salvarne i dati secondo la modalità descritta. In questo caso viene sfruttato la piattaforma Ethereum, in quanto una delle poche, e soprattutto la più famosa, utilizzata, supportata e sviluppata, che permette di salvare qualunque tipo di dato, a differenza di molte altre che invece lavorano solo con dati relativi alle proprie criptovalute. Ganache è l'equivalente di Ethereum per le piattaforme locali, in quanto ne crea una analoga in stile Ethereum, con relativa Blockchain in locale. Le ultime tecnologie sfruttate, sono appunto le Blockchain: in questo caso il sistema mette a disposizione tutte quelle comuni tra Infura ed Ethereum, ovvero:

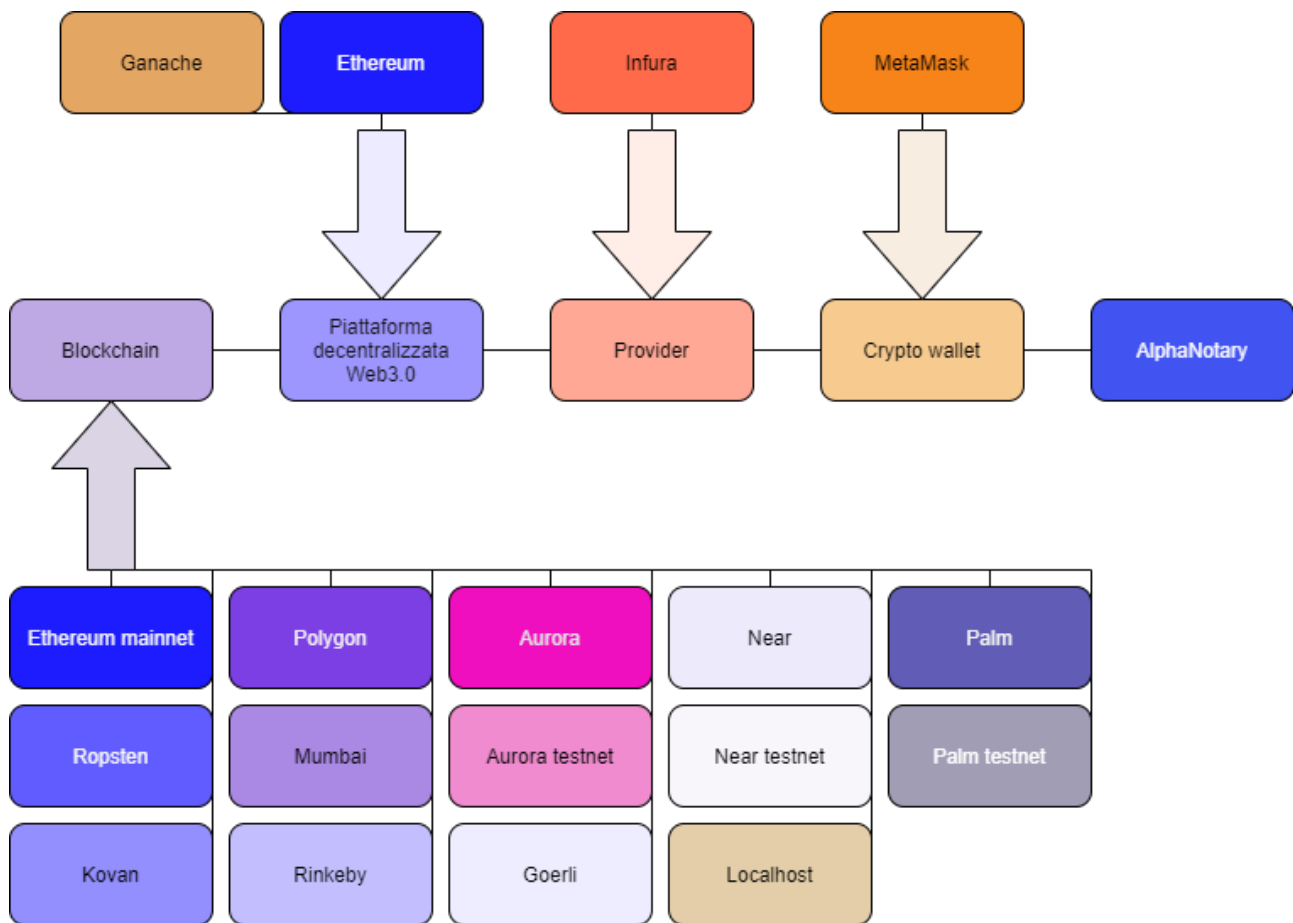
- **Ethereum mainnet:** Blockchain principale di Ethereum.

- **Ropsten:** Blockchain di prova principale di Ethereum.
- **Polygon:** Blockchain secondario di Ethereum.
- **Palm:** Blockchain secondario di Ethereum.
- **Aurora:** Blockchain secondario di Ethereum.
- **Near:** Blockchain secondario di Ethereum.
- **Mumbai:** Blockchain di prova principale di Polygon.
- **Localhost:** Blockchain di prova locale di Ganache.
- **Kovan:** Blockchain di prova secondaria di Ethereum.
- **Rinkeby:** Blockchain di prova secondaria di Ethereum.
- **Goerli:** Blockchain di prova secondaria di Ethereum.
- **Palm testnet:** Blockchain di prova primaria di Palm.
- **Aurora testnet:** Blockchain di prova primaria di Aurora.
- **Near testnet:** Blockchain di prova principale di Near.

Questo descrivere l'insieme delle interazioni per eseguire una transazione dell'utente a partire dal sistema. Ci sono però altre interazioni che il sistema può eseguire senza il coinvolgimento dell'utente: questo sono quelle per migrare lo Smart Contract sulla Blockchain. Uno Smart Contract definisce tutte le operazioni inerenti alla Blockchain che il sistema può effettuare e offre una gamma di funzioni che possono emettere dati dalla o alla Blockchain. Lo Smart Contract è quindi il modello logico del programma. Essa deve essere messo a disposizione sia al front-end, che in questo modo conosce i prototipi delle funzioni da chiamare, sia alla Blockchain, così che questa conosca, avendone il riferimento, lo Smart Contract comunicante. Quindi deve esserci, prima di usare l'applicazione, una iniziale migrazione univoca dello Smart Contract alla Blockchain: questa transazione segue il processo di interazioni descritto, il cui però il passaggio per la crypto wallet è automatizzato.

Senza queste tecnologie esterne all'applicazione, sarebbe molto più complesso sviluppare un sistema come AlphaNotary mettendo in dubbio la fattibilità realizzativa dell'applicazione perché bisognerebbe gestire tutti questi processi internamente al sistema, aumentando il carico di lavoro necessario per costruire il prodotto, la difficoltà realizzativa, e diminuendo al tempo stesso l'efficienza.

Il seguente grafico riassume il funzionamento descritto:



Organizzazione

La realizzazione effettiva dell'intera applicazione è stata preceduta da una lunga fase di progettazione, in cui sono state definite tutte le caratteristiche strutturali che il sistema avrebbe dovuto avere, al fine di garantire uno sviluppo semplice del programma, ma anche una buona manutenibilità e possibilità di sviluppo e integrazione futura. Tutta la progettazione aiuta ovviamente anche a creare un prodotto efficace ed efficiente.

Innanzitutto, si è deciso di adottare il design pattern architetturale MVC (Model View Controller) che suddivide il programma in tre macro-componenti: il modello (fornisce i metodi per accedere ai dati utili all'applicazione), il controller (riceve i comandi dell'utente attraverso la view e li attua modificando lo stato degli altri due componenti), e la view (visualizza i dati contenuti nel model e si occupa dell'interazione con utenti e agenti). Le interazioni partono sempre dalla view e scendono al controller per arrivare infine al modello. I risultati vengono poi restituiti alla view ma solamente dopo essere prima passati per il controller: questo fa intuire che sia stata rispettata anche un'architettura a layer, in cui ogni macro-componente ne costituisce uno. Essendo una dApp, è necessario che il programma abbia anche un'architettura monolitica, ovvero in cui tutto il codice dell'applicazione risiede nella stessa cartella di lavoro. Svariati altri design pattern vengono usati, come il Event-base asynchronous (per eseguire tutte le operazioni possibili e aventi inizio da eventi, in modo asincrono al fine di aumentare l'efficienza del funzionamento), l'Observer (per osservare determinati elementi ed eseguire azioni al loro cambiamento, usati sottoforma di ascoltatori di eventi messi a disposizione da JavaScript), il Facade (per semplificare l'interazione tra le componenti

in modo che ogni componente comunichi con una sola interfaccia che gestirà l'input, e il Factory (per costruire le componenti di modo automatico).

Sono anche state rispettate prassi di buona programmazione come la Single Responsibility Principle, per cui ogni componente del programma esegue solo funzioni relative a ciò per cui è stato concepito, programmazione procedurale, funzionale e ad oggetti, per garantire massima possibilità di riuso di codice, modularità, estensibilità e praticità, e infine attenzione ad algoritmi e strutture per essere congrui e con complessità algoritmica e computazione minima, e pertanto garantendo massima efficienza. Ovviamente tutto il codice è ben documentato al fine di potervi lavorare da altre persone e in futuro.

Le operazioni principali, che quindi vedono un'interazione con la Blockchain, che vengono messe a disposizione dal sistema sono le tre seguenti:

- **Upload:** caricamento di un NFT, ricavato da uno o più documenti con l'aggiunta di informazioni ad esso relative.
- **Check:** notarizzazione di un NFT a partire dai documenti che l'avevano composta al momento del caricamento.
- **Remove:** è una funzionalità aggiuntiva, offerta per avere una gamma completa di operazioni a disposizione e pertanto poter amministrare i propri NFT in modo completo. Permette di rimuovere un NFT dalla Blockchain a partire dai documenti che l'avevano composta al momento del caricamento.

Linguaggi

Di seguito sono riportati tutti i linguaggi di programmazione coinvolti nello sviluppo del progetto, con la descrizione del loro utilizzo:

- **HTML:** per definire la struttura delle pagine utente.
- **CSS:** per definire lo stile delle pagine utente.
- **JavaScript:** per definire il comportamento delle pagine utente.
- **Node.js:** per eseguire lo Smart Contract e la libreria Web3.js, l'avvio del servizio, e la modalità test.
- **Solidity:** per sviluppare lo Smart Contract.
- **Bootstrap:** per usare stili preconfigurati degli elementi delle pagine utente.
- **Web3.js:** libreria per comunicare con lo Smart Contract.
- **Batch:** per creare lo script per avviare comodamente l'applicazione da icona.

Tecnologie

Di seguito sono riportati tutti i linguaggi di programmazione coinvolti nello sviluppo del progetto, con la descrizione del loro utilizzo:

- **Git:** in particolare GitHub, per versionare il codice.
- **Truffle Suite:** libreria per gestire l'ambiente di sviluppo dello Smart Contract.
- **Ganache:** piattaforma decentralizzata Web3.0 locale per esecuzione locale e di test.
- **Ethereum:** piattaforma decentralizzata Web3.0 per esecuzione in modalità reale.

- **IPFS:** protocollo usato dalla libreria Web3.js per gestire la comunicazione con lo Smart Contract.
- **Lite-server:** pacchetto npm per gestire autonomamente l'esecuzione del programma.
- **Polygon:** Blockchain principale del sistema. È possibile impostare anche tutte le altre Blockchain indicate.
- **Infura:** provider per l'accesso alla Blockchain.
- **MetaMask:** estensione per browser per la gestione della crypto wallet.
- **Windows:** sistema operativo di sviluppo principale.
- **Linux:** sistema operativo di sviluppo secondario.

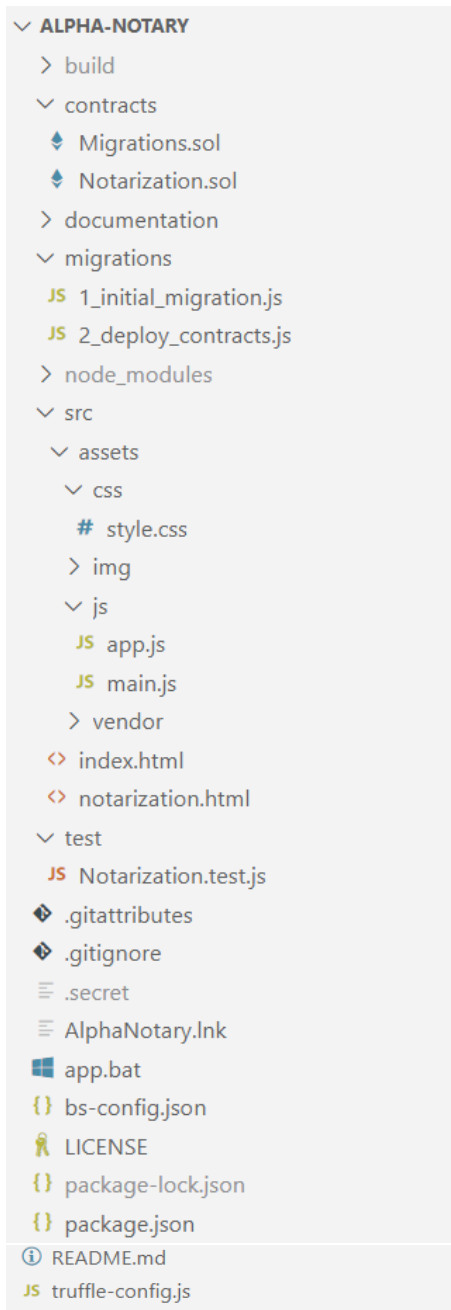
Realizzazione

Struttura

Conviene spiegare la struttura della cartella del progetto affinché sia semplice proseguire con sviluppi futuri. Nella cartella `contracts` sono presenti due file, uno per Smart Contract: il primo definisce quello necessario al sistema, mentre il secondo viene creato automaticamente da Truffle Suite e serve alla Blockchain per tracciare lo sviluppo dello Smart Contract principale. Ogni Smart Contract è un unico file perché lo Smart Contract è per definizione una classe contenente tutte le funzionalità per il sistema vuole offrire inerente alla Blockchain. La cartella di `documentation` contiene la documentazione, tra cui la seguente. La cartella di `migrations` contiene due file generati automaticamente da Truffle Suite, uno per lo Smart Contract di migrazione, e uno per tutti gli altri, in questo caso uno solo. Sono degli script JavaScript necessari per la migrazione sulla Blockchain degli Smart Contract.

La cartella `src` contiene tutto il front-end: sono presenti alla radice di questa cartella le pagine html finali visualizzate dall'utente. Sono anche presenti una cartella `css` contenente il foglio di stile css delle pagine, una cartella `js` contenente un primo file di script JavaScript `app` contenente il controller e la view dell'applicazione, e un secondo file di script JavaScript `main` contenente le animazioni del programma. La cartella `img` contiene le immagini del sistema, mentre la cartella `vendor` contiene invece, una serie di cartelle, ognuno relativo ad una libreria grafica usata, contenente diversi file css e JavaScript. Nella cartella `test` è presente un file di script JavaScript contenente i test di unità del back-end. Alla radice della cartella di lavoro sono presenti i seguenti file:

- **.gitattributes:** necessario per il versionamento tramite GitHub. È un file facoltativo.
- **.gitignore:** esclude alcuni file dall'essere versionati su GitHub. È un file facoltativo.
- **.secret:** informazioni personali dell'utente: se non esiste, deve essere creata. In tale file nella prima riga è da immettere lo mnemonic (codice segreto delle crypto wallet), e nella seconda riga la chiave generata dal provider.
- **AlphaNotary:** collegamento all'eseguibile dell'applicazione. È un file facoltativo.
- **app:** eseguibile dell'applicazione. È un file facoltativo.
- **bs-config:** definisce struttura della cartella.
- **package-lock:** definisce il compilato della cartella.
- **package:** informazioni generiche e dipendenze da installare al momento della configurazione del programma.
- **README:** utile a presentare il progetto su GitHub. È un file facoltativo.
- **LICENSE:** licenza repository GitHub. È un file facoltativo.
- **truffle-config:** configurazione di tutte le reti di Blockchain supportate.



Back-end

Il back-end è costituito dallo Smart Contract. L'unico punto da sottolineare sulla sua realizzazione è che è completamente testata, con test di unità, raggiungendo una code coverage del 100%.

Front-end

Qui vi sono presenti sia il controller che la view. È rilevante citare che la grafica è responsive, accessibile (contro disabilità e a favore della separazione tra struttura, presentazione e comportamento), ottimizzato per SEO (Search Engine Optimization, risultati del motore di ricerca, tramite attributo keyword, title e separazione tra struttura, presentazione e comportamento) e SERP (Search Engine Result Page, risultati di ricerca, tramite attributo description e separazione tra struttura, presentazione e comportamento).

Esecuzione

Avvio

Installazione

Si necessita di avere a disposizione localmente del codice sorgente dell'applicazione. Ciò può essere raggiunto, se non lo si ha già e se non vi sono altri metodi per averlo, effettuando il fork o scaricando il repository GitHub (raggiungibile cliccando <https://github.com/adnangazi/alpha-notary>), di cui si dispone il link alla fine del documento. Una volta in possesso del codice sorgente, sarà necessario aprire la cartella da un terminale ed eseguire i seguenti comandi:

```
truffle compile  
npm install
```

Essi, rispettivamente, eseguono il back-end, in particolare compilano lo Smart Contract producendo una cartella build che sarà necessario al front per conoscere i prototipi delle funzioni offerte dallo Smart Contract, e installando infine, tutti pacchetti di dipendenze, che invece verranno messe nella cartella node_modules che verrà creata, necessari per poter eseguire il sistema. Verrà anche prodotto il file JavaScript package-lock.

Prima di tutto sarà necessario avere le seguenti configurazioni sul proprio dispositivo:

- **MetaMask**
- **Truffle suite**
- **Node.js**

Esecuzione di test

L'esecuzione in modalità di test permette di verificare che il sistema sia stato sviluppato adeguatamente, ma soprattutto di controllare che l'ambiente sia correttamente configurato. L'esecuzione in modalità di test non implica alcun'interazione da parte dell'utente, in quanto il programma automatizza tutte quelle possibili, eseguendoli (test di unità), e visualizzandoli sottoforma di lista di test passati. L'esecuzione in modalità di test non è obbligatoria.

Per avviare il programma in modalità di test, bisogna aprire il progetto con un terminale ed eseguire i seguenti comandi:

```
truffle test
```

I test eseguiti sono divisi in quattro sezioni, uno per ogni operazione principale messo a disposizione dal sistema, con l'aggiunta dell'iniziale fase di distribuzione delle specifiche del sistema.

Prima di tutto sarà necessario avere le seguenti configurazioni sul proprio dispositivo:

- **Ganache**

Verrà quindi, visualizzato come segue, ed è l'unico risultato ammissibile per accertare la correttezza del programma e della configurazione dell'ambiente:

```
PS D:\GitHub\adnangazi\alpha-notary> truffle test
Using network 'development'.

Compiling your contracts...
=====
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Notarization.sol
> Artifacts written to C:\Users\adnan\AppData\Local\Temp\test--10964-D8lcBjegTPKU
> Compiled successfully using:
  - solc: 0.5.16+commit.9c3226ce.Emscripten.clang

Contract: NOTARIZATION
  ✓ DEPLOY (231ms)
  ✓ UPLOAD (4116ms)
  ✓ CHECK (1909ms)
  ✓ REMOVE (2550ms)

4 passing (9s)

PS D:\GitHub\adnangazi\alpha-notary> █
```

Esecuzione locale

L'esecuzione locale significa eseguire il programma su una propria rete locale, e quindi usando una propria Blockchain. Ciò permette di far funzionare il sistema in fase di sviluppo, per verificare il prodotto finale, o per usare il sistema premesso che si sia disposti sempre ad avere l'infrastruttura per l'esecuzione in locale a disposizione, senza però spendere denaro reale per usare una vera Blockchain o incorrere nei rischi ad essi collegati. L'esecuzione in modalità di test non è obbligatoria. Bisogna pertanto, aprire il progetto con un terminale ed eseguire i seguenti comandi:

```
truffle migrate
npm start
```

Il primo comando esegue la migrazione dello Smart Contract nella Blockchain locale, ed è da eseguire solamente la prima volta. Se in precedenza era già stato caricato lo Smart Contract in tale Blockchain, e si desidera cancellarlo per caricarlo nuovamente, basterà aggiungere al comando l'opzione --reset. Il secondo comando avvia il sistema.

Prima di tutto sarà necessario avere le seguenti configurazioni sul proprio dispositivo:

- **Ganache**

Distribuzione

Il processo di distribuzione deve essere eseguito una volta certi che il sistema funzioni e quando si desidera caricare lo Smart Contract su una Blockchain vera e cominciare ad usare il prodotto condiviso tra tutti gli utenti. Il processo di distribuzione è identico a quella di esecuzione locale, solamente che bisogna specificare durante il comando di migrazione dello Smart Contract, quale

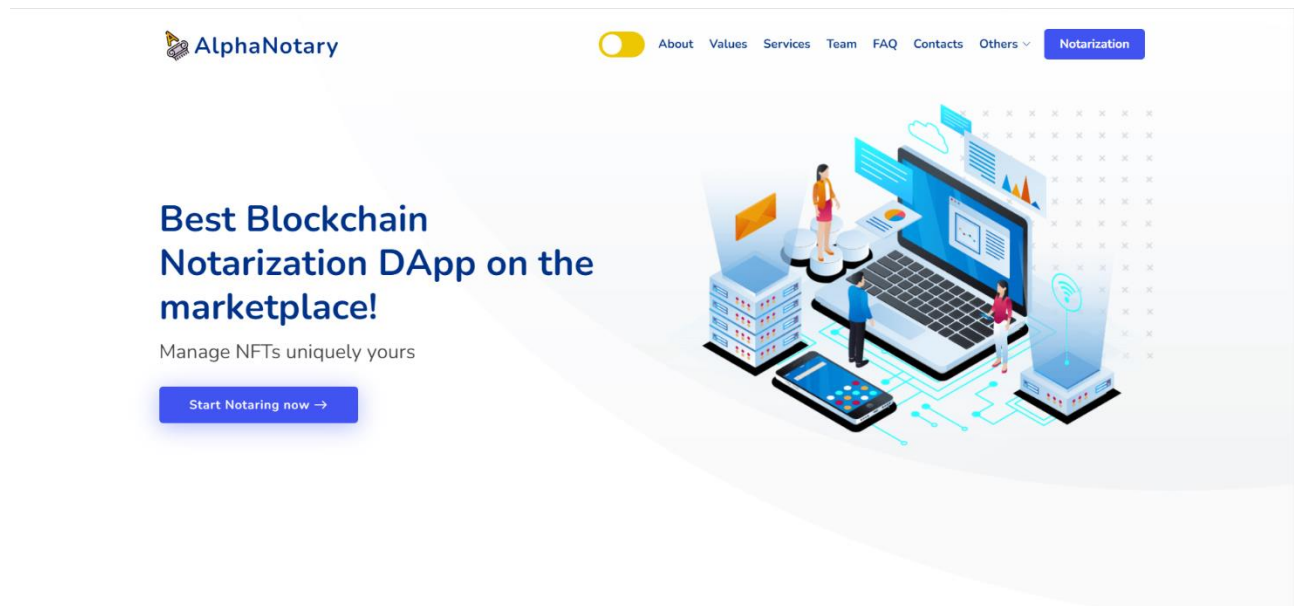
Blockchain si intende effettuarla, con il seguente comando:

```
truffle migrate --network <your_network>
```

È anche possibile accedere al prodotto cliccando al seguente link <https://alpha-notary.vercel.app/src/index.html>. Ma a causa di un problema di configurazione della porta, visualizza solamente l'interfaccia grafica del sistema. In ultimo, sapendo che lo Smart Contract è stato migrato nella rete d'interesse, si può semplicemente aprire il file .batch di nome app, oppure il collegamento di nome AlphaNotary, quest'ultimo con la possibilità di essere spostata ove di preferisce, entrambe nella cartella del progetto.

Pagina di presentazione

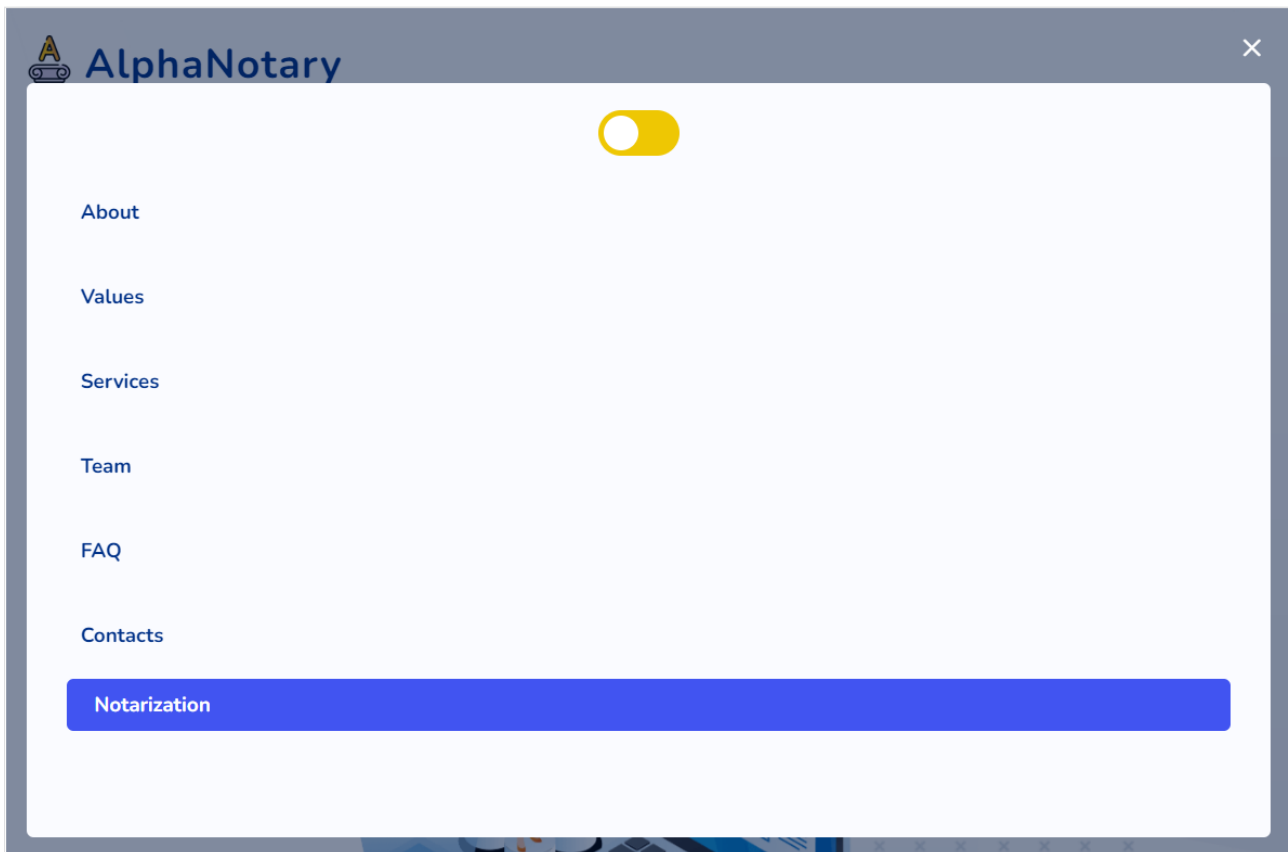
La schermata d'avvio:



La schermata d'avvio mobile:



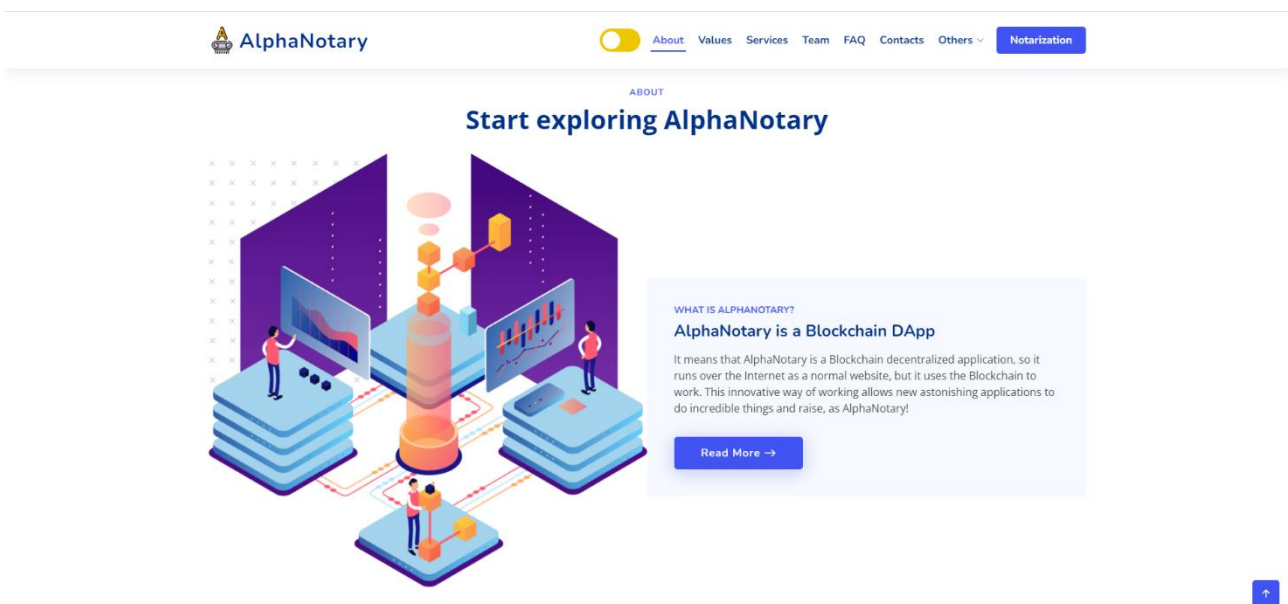
Il menu mobile:




Il breadcrumb:




La sezione della presentazione:



La sezione della descrizione di cos'è:



 [About](#) [Values](#) [Services](#) [Team](#) [FAQ](#) [Contacts](#) [Others](#) [Notarization](#)

BANNER


Discover more about AlphaNotary

WHAT DOES ALPHANOTARY DO?

AlphaNotary permits to notarize your documents on the Blockchain


Notarization is the process that brings to authenticate documents through the time. So, you can know in this way at any time if a document you receive or use is truly what the original was, or if it has been modified by someone. Being able to authenticate documents is very important, especially where files are widely used, where they are shared between many entities, or simply is relevant to guarantee their security. So AlphaNotary is thought for all of these realities, and it uses the Blockchain to embrace the trend of Web3.0, and develop this functionality in the easiest way possible, either!

[Read More →](#)



Pagina 20 di 46

La sezione dei pregi:


 AlphaNotary

AboutValuesServicesTeamFAQContactsOthers

Notarization


VALUES

Values that make AlphaNotary unique across the world




Security

It's absolutely impossible to hack AlphaNotary! It is designed appositely not to expose sensible data, so you can use our system in peace and for relevant files.




Quality

Our team of bright-minds encloses an intransigent way of working, that last no details. The quality we offer is priceless, and it ends up in a better experience for the user.




Solidity

No servers, no downloads, no service interruptions. AlphaNotary is pretty solid thanks to the Blockchain to the base. It will always work!




Efficiency

We have put our best to create a system that does its things exactly how it should be done. For this purpose, nothing better could have been done.



Efficacy

AlphaNotary seems to do magic, but it really does perfectly what it promises: check the product to ensure yourself. You can also visit the source of the work.



Affordability

We are pleased to share our product completely for free! You only have to pay a few cents to the Blockchain every time you make a transaction, to recompense your usage.

La sezione delle funzionalità:

The screenshot shows the AlphaNotary website header with the logo, a navigation menu (About, Values, Services, Team, FAQ, Contacts, Others), and a 'Notarization' button. The main section is titled 'Checklist of AlphaNotary main features' under the 'FEATURES' heading. It displays a grid of eight features, each with a checkmark icon:

- ✓ Lite mode
- ✓ Full mode
- ✓ Light mode
- ✓ Dark mode
- ✓ Upload
- ✓ Check
- ✓ Remove
- ✓ Monitor

To the right of the grid is an illustration of four people interacting with a large digital screen and gears. A small blue button with an upward arrow is located at the bottom right of the section.


La sezione dei pregi:

The screenshot shows the AlphaNotary website header with the logo, a navigation menu (About, Values, Services, Team, FAQ, Contacts, Others), and a 'Notarization' button. The main section is titled 'Main points of merit of AlphaNotary' under the 'MERITS' heading. It features a grid of six points, each with an icon and a brief description:

- Continuous raise**: AlphaNotary can only increase because it's a web always open website.
- No footprint**: Only a public and world-wide infrastructure is used: the Blockchain.
- UI/UX**: Captivating and accessible GUI for the best experience of use build solid clients.
- Extreme simplicity**: Like magic, all stuff work greatly together. And all is needed is just a click: could it be simpler than this?
- Practical**: AlphaNotary is designed for wide use, so it is also a working environment application.
- Requested**: AlphaNotary was born from the need of automate authentication of many industries.

On the left side of the grid is an illustration of a smartphone displaying a user interface, surrounded by gears and a megaphone. A small blue button with an upward arrow is located at the bottom right of the section.

La sezione dei passi compiuti per effettuare la notarizzazione:




AboutValuesServicesTeamFAQContactsOthers

Notarization

SERVICES


The services that AlphaNotary offers



Hashing

A unique key is generated of the documents in the form a hash code thanks to a hash function. Next the documents are uploaded to the Blockchain.


Read More →



Connection

The connection is intermediate by the MetaMask extension, which creates transactions containing your data to the Blockchain directly from your crypto wallet.


Read More →



Transaction

Transactions are managed by the Infura provider, which guarantees them to reach the Blockchain and manages the process to execute them.


Read More →



Executing

An apposite Smart Contract, which is an operative unit that defines the operations a system can do on a Blockchain, manages how the data have to be stored.


Read More →



Saving

Ethereum permits Smart Contracts to be connected and tell how to store data into the Blockchain. So the Blockchain is like a database, and Smart Contracts servers.

Read More →




Notaring

Managing hash codes, upload, checking and removing them creates a notarization system, which AlphaNotary is built around, offering a complete service.

Read More →

La sezione della descrizione di come funziona:



AboutValuesServicesTeamFAQContactsOthers

Notarization

DESCRIPTION

How the system works

Extraordinary system: such simple to use. But how does it work?

VIEWCONTROLLERMODEL


A super rich graphic user interface is just a pleasant decoration to facilitate the interactions with the main functionalities of the system.


- ✓ Usability is the priority of the view.

The view is made of components that simplify and modularize its work, in addition of facilitating other components, too.

- ✓ Facilitate the work of the other components is relevant for the view.

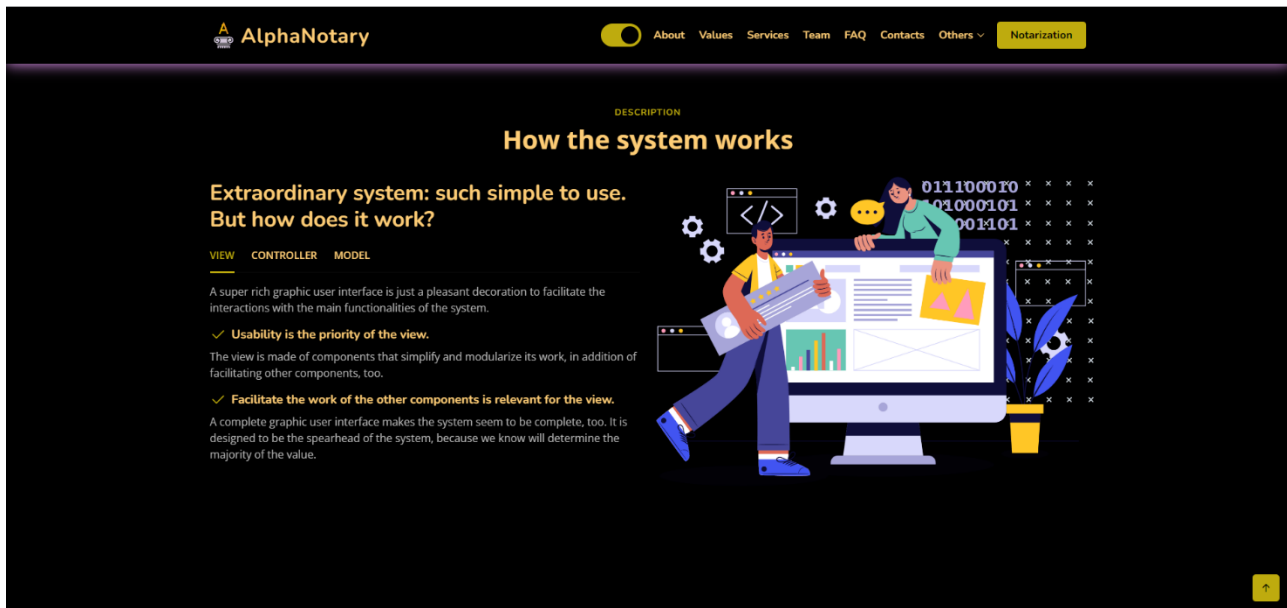
A complete graphic user interface makes the system seem to be complete, too. It is designed to be the spearhead of the system, because we know will determine the majority of the value.



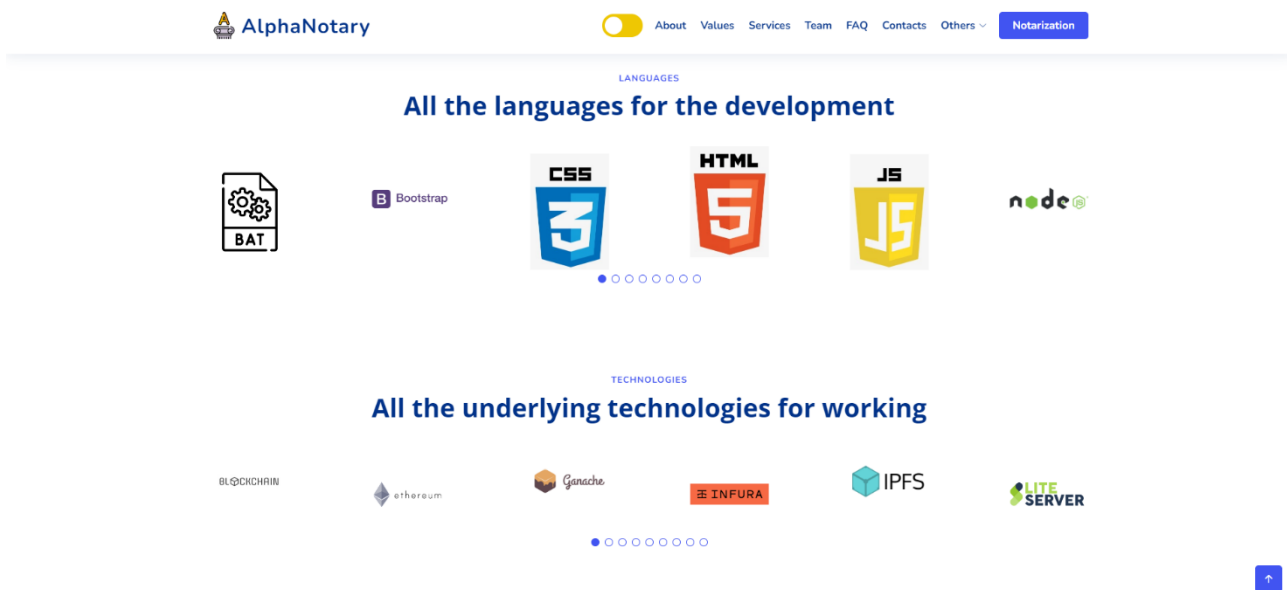


Pagina 23 di 46

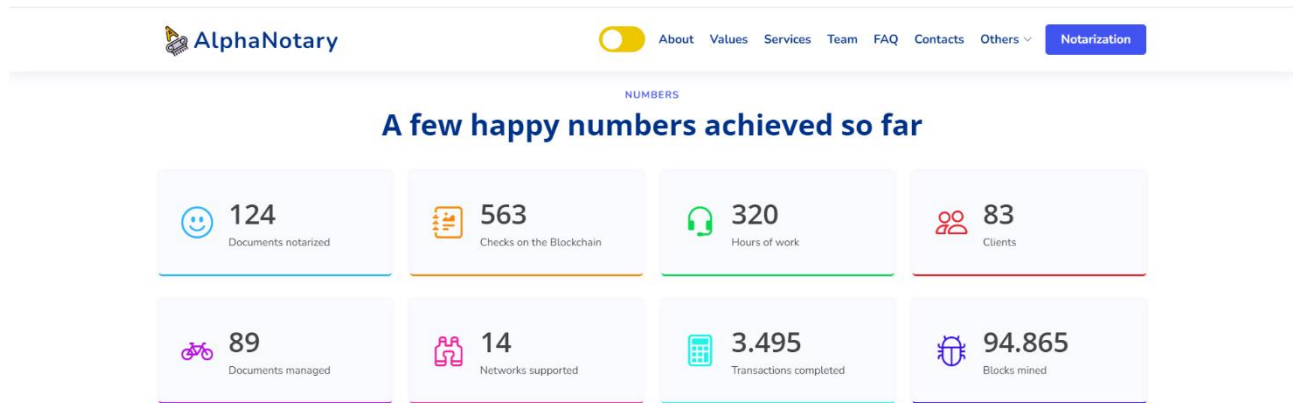
La sezione della descrizione di come funziona, ma con il tema scuro:



La sezione dei linguaggi e tecnologie usate:



La sezione dei traguardi raggiunti finora:



La sezione del profilo dei membri del gruppo:

AlphaNotary


TEAM


Let me present myself

Adnan Latif Gazi
CEO & Founder

I am a student of Computer Science at the University of Padua. I have always been excellent in the relevant courses of my studies, getting top marks among the courses that made me differentiate between professors and colleges. This makes me an exceptional student. I am passionate about algorithms and data structures, programming paradigms, databases and software engineers. I am good and experienced in teamwork, in fact I like to manage, lead and collaborate with teams and projects. I also like to develop clean and efficient code. I have experience with languages such as C ++, Java, JavaScript, PHP, SQL, MATLAB, HTML, CSS, and a little bit of many others. I'm familiar with technologies like Git, QT Framework, Windows, Linux, and more. In my spare time I usually work on my own project or attend online courses, both of IT, to develop my skills and technologies. In the future I want to continue my studies with a Masters in Computer Science to specialize in the field of Artificial Intelligence or Advanced Algorithms.


La sezione delle recensioni ricevuto finora:



[About](#) [Values](#) [Services](#) [Team](#) [FAQ](#) [Contacts](#) [Others](#) [Notarization](#)

TESTIMONIALS


What they say about AlphaNotary



Massimo Zambon
Venicecom developer

It was a pleasure to work with this team to develop AlphaNotary. It is a very interesting and a stimulating experience of work, with a useful way of working able to bring to great results, whatever the goal is. The completeness of the product, which has been taken from zero, conceived, designed, developed, and managed so far as well as in future, demonstrates the authentic and incredible capabilities of the team.


★★★★★



Marco Baraldi
Senior project manager Venicecom

It is incredible how well-done this system is made: everything works perfectly, and it presents itself in the greatest way possible. This product exceeds my expectations, and it is ready to conquer a wide client base and their trust, too. To make things worse, it is also a complete new approach to the Blockchain world, which represent a basis for working on new range of technologies and possibilities!




★★★★★




Fabio Bortoluzzi
System Administrator & Facility Manager Venicecom

I've analyzed the technical part of the product and I have to admit the quality of the development. Each technology used is motivated, and each component's respect patterns, best practices, and programming paradigms. The infrastructure is well-designed, too. All of these things are the awareness of a great project result, leaving out the product for what it is itself, which is awesome, too.

★★★★★





La sezione delle domande frequentemente fatte:

AlphaNotary

About Values Services Team **FAQ** Contacts Others

Notarization

FAQ

Frequently asked questions

What is Lite mode?

What is Full mode?

How do I know my documents are not exposed?

How do I start using AlphaNotary?


How can I check my Blockchain interactions?


How can I contribute to AlphaNotary?

Just giving it a look...

What to do in case of errors?


La sezione dei contatti:





[About](#)
[Values](#)
[Services](#)
[Team](#)
[FAQ](#)
[Contacts](#)
[Others](#)
[Notarization](#)

CONTACTS


All the ways to contact me






Social

Instagram & Facebook
iamadnangazi | Adnan Latif Gazi




Call me

+39 339 322 1343




Address

Via Miranese, 460/A
30174, Chirignago - Venice, Italy




Email me

adnangazi.ag@gmail.com




My projects

GitHub
adnangazi




Open hours

Monday - Friday
9:00AM - 06:00PM



Portfolio


adnangazi.github.io



My works


LinkedIn
adnanlatifgazi

Il footer:



AlphaNotary

AlphaNotary is a Blockchain Notarization DApp to manage NFTs uniquely yours, creating, notarizing, and monitoring your documents! Notarization is solid, practical, and safe thanks to AlphaNotary! Start right now and enjoy a completely new era of NFTs!



PROJECT LINKS

- Home
- Notarization
- Monitoring
- Documentation
- Repository

TOPICS LINKS

- Blockchain
- Notarization
- DApp
- Ethereum
- NFTs

CONTACT ME

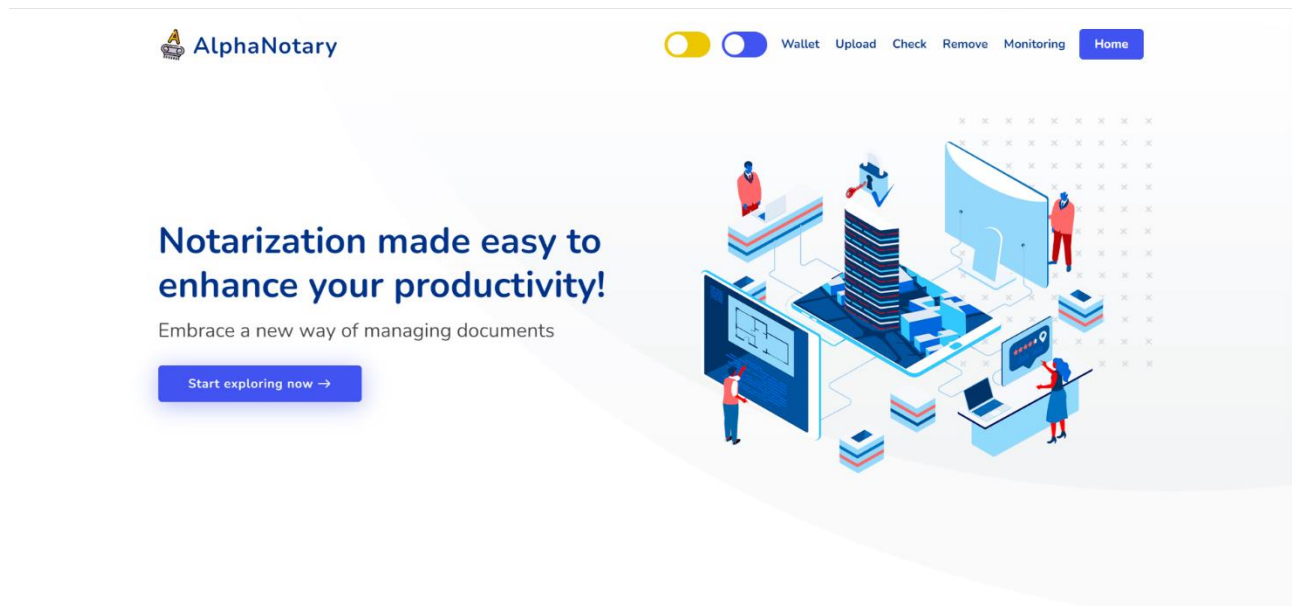
Address: Via Miranese, 460/A
30174, Chirignago - Venice, Italy
Phone: +39 339 322 1343
Email: adnangazi.ag@gmail.com
Open hours: Monday - Friday
9:00AM - 6:00PM

Designed, developed, and managed by Adnan Latif Gazi

© Copyright 2022 - All Rights Reserved

Pagina di notarizzazione

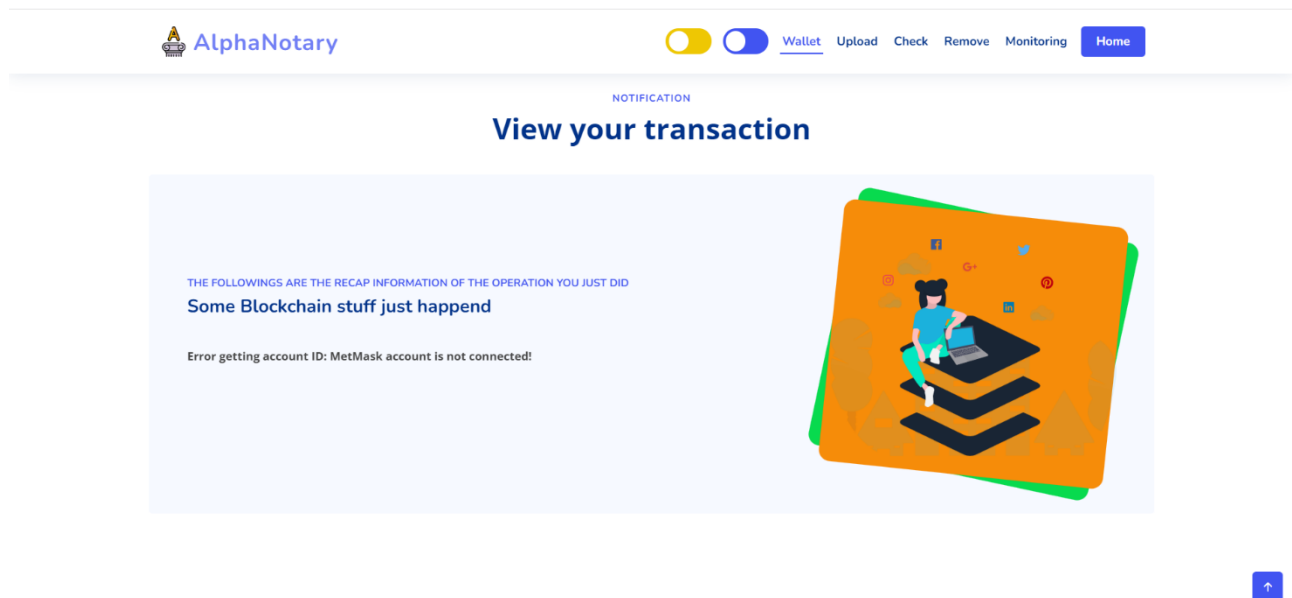
La schermata d'avvio:



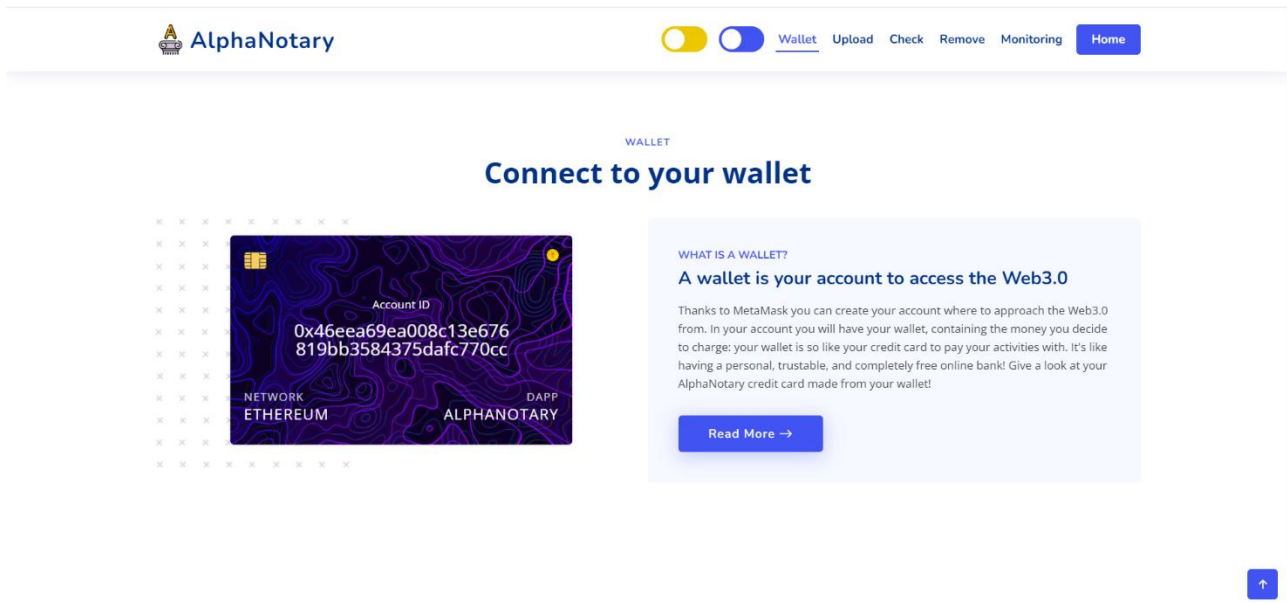
Il breadcrumb:



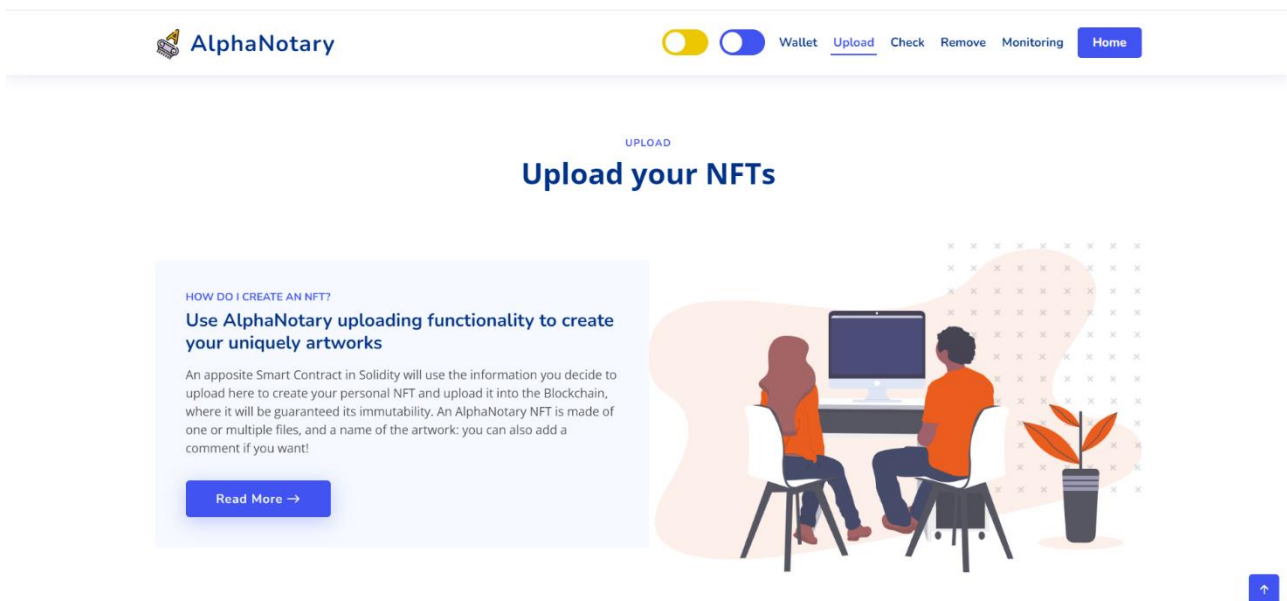
La sezione del banner di errori:



La sezione del wallet:



La sezione del caricamento:



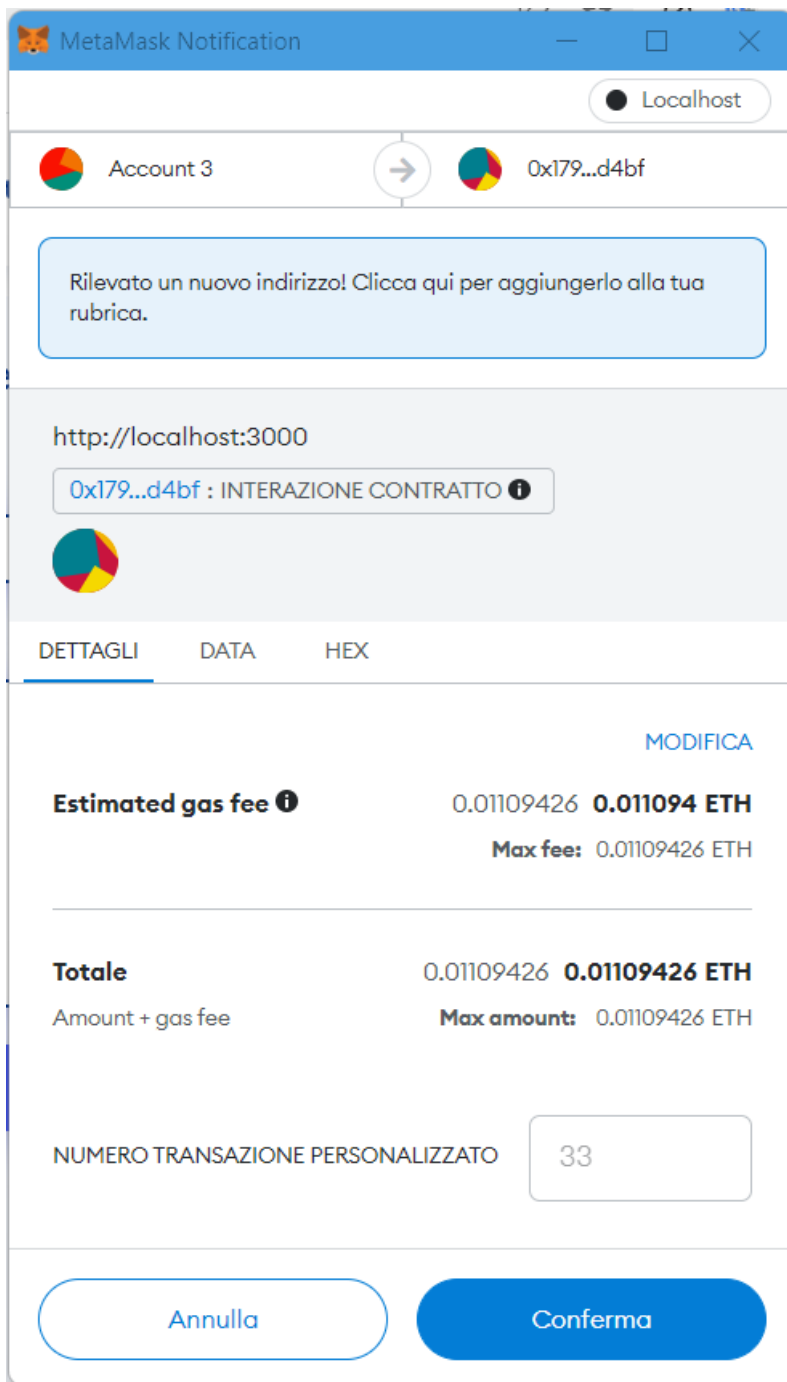
Il form di caricamento vuoto:

The screenshot shows the AlphaNotary web interface. At the top, there is a navigation bar with the AlphaNotary logo, a toggle switch for 'Wallet', and a menu with 'Upload', 'Check', 'Remove', 'Monitoring', and 'Home'. The main content area is divided into two sections: 'Upload your files here' on the left and 'Insert your files info here' on the right. The 'Upload your files here' section contains a dashed box with a cloud icon and an upward arrow, with the text 'Browse or drag & drop' below it. The 'Insert your files info here' section contains a 'Document name' input field with the placeholder text 'Subject', a 'Document comments' text area with the placeholder text 'Message', and an 'Upload' button at the bottom. A small blue square button with an upward arrow is located at the bottom right of the page.

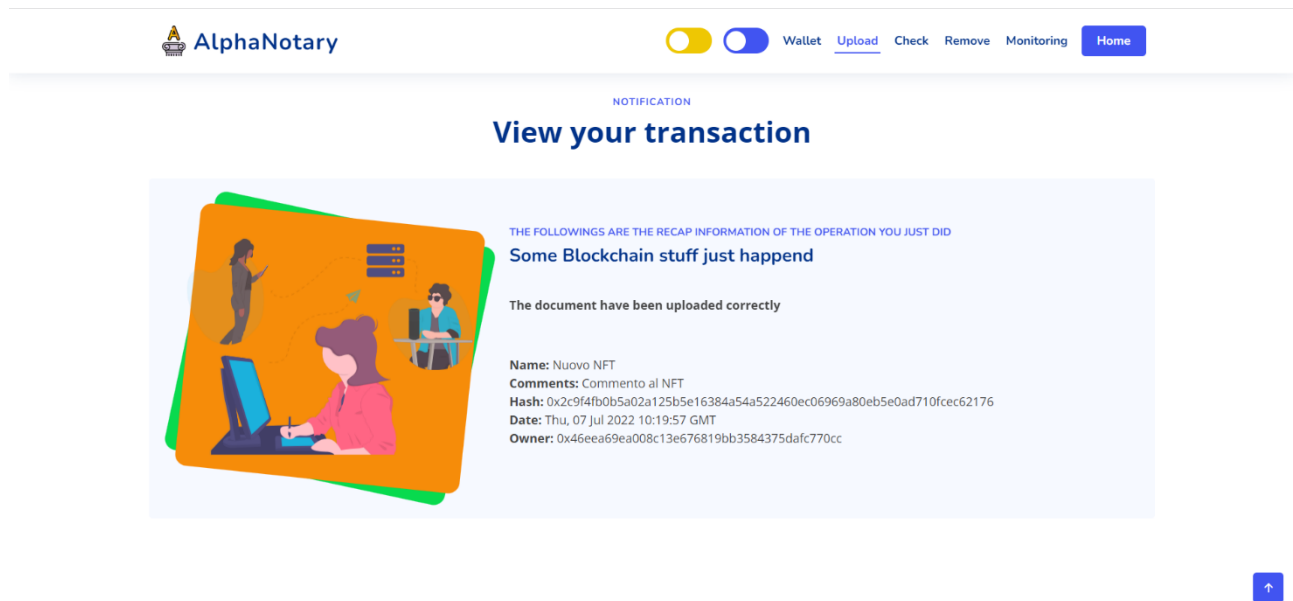
Il form di caricamento pieno e in modalità leggera:

The screenshot shows the AlphaNotary web interface in a 'lite-mode'. The navigation bar is the same as in the previous screenshot. The main content area is divided into two sections: 'Upload your files here' on the left and 'Insert your files info here' on the right. The 'Upload your files here' section contains a dashed box with a cloud icon and an upward arrow, with the text 'Browse or drag & drop' below it. Below this box, there are three file upload progress bars. The first bar is for 'Motivation letter.txt' and is at 95%. The second bar is for 'CERN-CodingChallenge2.md - uploaded' and is at 100%. The third bar is for 'Fellowship.txt - uploaded' and is at 100%. The 'Insert your files info here' section contains a 'Document name' input field with the placeholder text 'Nuovo NFT', a 'Document comments' text area with the placeholder text 'Commento al NFT', and an 'Upload' button at the bottom. A red warning message at the bottom of the page states: '* take care that AlphaNotary is currently on lite-mode, so you will not be able to monitor your transactions!'. A small blue square button with an upward arrow is located at the bottom right of the page.

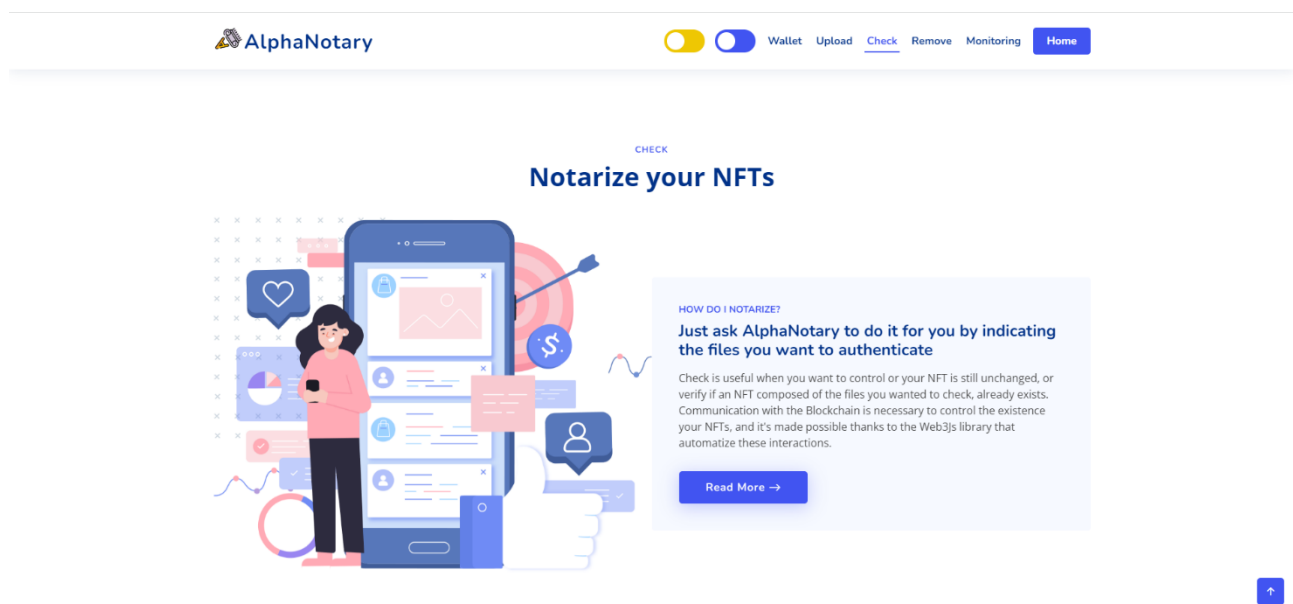
La schermata di conferma su MetaMask:



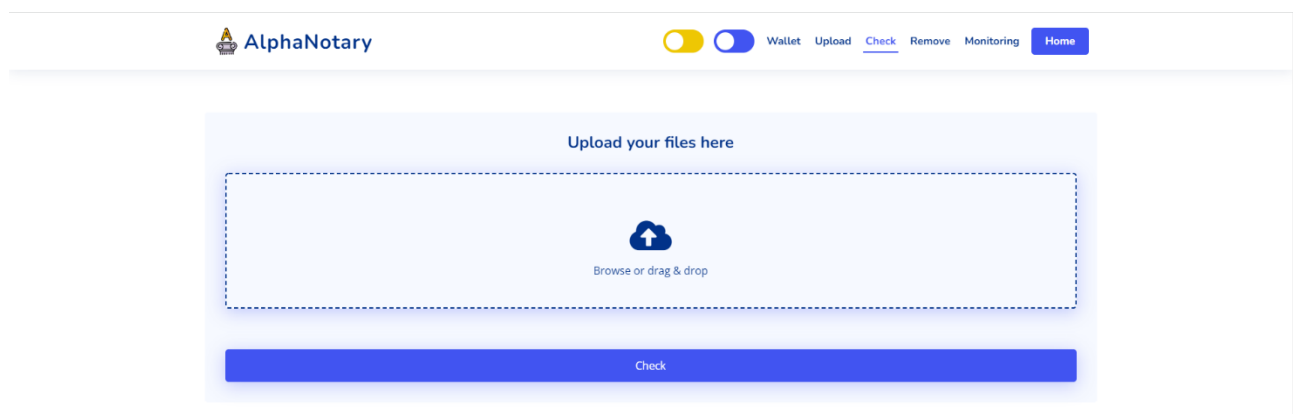
La sezione di banner dei risultati del caricamento:



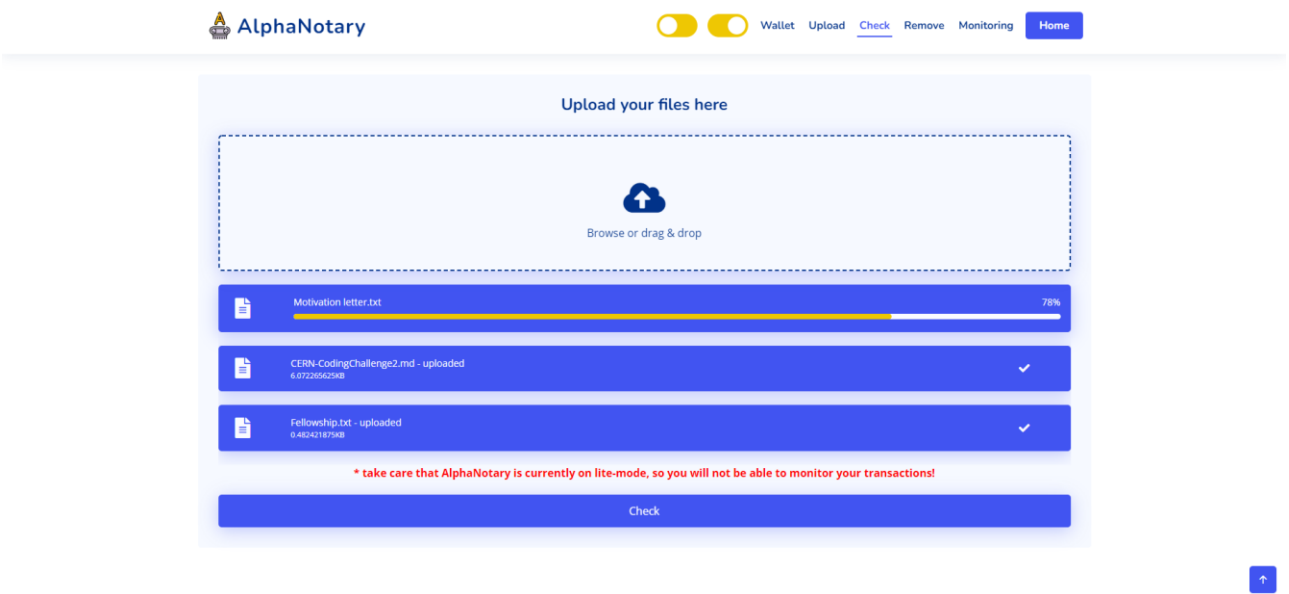
La sezione del controllo:



Il form di caricamento vuoto:



Il form di caricamento pieno e in modalità leggera:



La schermata di conferma della transazione su MetaMask:

MetaMask Notification

Localhost

Account 3

→

0x179...d4bf

Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

http://localhost:3000

0x179...d4bf : CHECK ⓘ

DETTAGLI

DATA

HEX

MODIFICA

Estimated gas fee ⓘ

0.00702294 **0.007023 ETH**

Max fee: 0.00702294 ETH

Totale

0.00702294 **0.00702294 ETH**

Amount + gas fee **Max amount:** 0.00702294 ETH


NUMERO TRANSAZIONE PERSONALIZZATO

34

Annulla

Conferma

La sezione del banner dei risultati del controllo:



Wallet Upload Check Remove Monitoring Home

NOTIFICATION


View your transaction

THE FOLLOWINGS ARE THE RECAP INFORMATION OF THE OPERATION YOU JUST DID

Some Blockchain stuff just happend


The document have been found!

Name: Nuovo NFT
Comments: Commento al NFT
Hash: 0x2c9f4fb0b5a02a125b5e16384a54a522460ec06969a80eb5e0ad710fcec62176
Date: Thu, 07 Jul 2022 10:19:57 GMT
Owner: 0x46eea69ea008c13e676819bb3584375dafc770cc
Interaction date: Thu, 07 Jul 2022 10:21:26 GMT
Interaction owner: 0x46eea69ea008c13e676819bb3584375dafc770cc



↑

La sezione della rimozione:



Wallet Upload Check Remove Monitoring Home

REMOVE


Manage your NFTs

HOW CAN I MANAGE MY NFTS AT ALL?

AlphaNotary offers additional functionalities to bring a complete service, including the removal function


NFTs are meant to stay immutable through the time, but if you want to remove some of them, you can! Take care that removing your files will not bring any advantage, nor to you, neither to AlphaNotary or the Blockchain, because everything is only saved in the Blockchain, where blocks are used only once because it is a one-way chain where new blocks are added to the end. To understand better the Blockchain structure, or to test this function, you can run the application in local using Truffle suite.

[Read More →](#)




↑

Il form del caricamento vuoto:



Wallet Upload Check Remove Monitoring Home

Upload your files here



Browse or drag & drop

Remove

Il form del caricamento pieno e in modalità leggera:

AlphaNotary

Wallet

Upload

Check

Remove

Monitoring

Home

Upload your files here

Browse or drag & drop

Mothivation letter.txt

86%

CERN-CodingChallenge2.md - uploaded

6.07235625KB

Fellowship.txt - uploaded

0.482401875KB

* take care that AlphaNotary is currently on lite-mode, so you will not be able to monitor your transactions!

Remove

La schermata di conferma su MetaMask:

MetaMask Notification

Localhost

Account 3

→

0x179...d4bf

Rilevato un nuovo indirizzo! Clicca qui per aggiungerlo alla tua rubrica.

http://localhost:3000

0x179...d4bf : INTERAZIONE CONTRATTO ⓘ

DETTAGLI DATA HEX

MODIFICA

Estimated gas fee ⓘ

0.00715002 **0.00715 ETH**

Max fee: 0.00715002 ETH

Totale

0.00715002 **0.00715002 ETH**

Amount + gas fee Max amount: 0.00715002 ETH


NUMERO TRANSAZIONE PERSONALIZZATO

35

Annulla

Conferma

La sezione del banner dei risultati della rimozione:



Wallet

Upload

Check


Remove

Monitoring

Home

NOTIFICATION

View your transaction



THE FOLLOWINGS ARE THE RECAP INFORMATION OF THE OPERATION YOU JUST DID


Some Blockchain stuff just happend

The document have been removed!

Name: Nuovo NFT
Comments: Commento al NFT
Hash: 0x2c9f4fb0b5a02a125b5e16384a54a522460ec06969a80eb5e0ad710fcec62176
Date: Thu, 07 Jul 2022 10:19:57 GMT
Owner: 0x46eea69ea008c13e676819bb3584375dafc770cc
Interaction date: Thu, 07 Jul 2022 10:22:55 GMT
Interaction owner: 0x46eea69ea008c13e676819bb3584375dafc770cc

↑

La sezione del monitoraggio vuoto:



Wallet

Upload

Check


Remove

Monitoring

Home

MONITORING

Monitor your actions



HOW DO I CHECK MY TRANSACTIONS?

Monitor your activities in AlphaNotary here or on the scanner for more details


AlphaNotary Smart Contact is made appositely for tracking users activities: this is not for violating your privacy (take care that everything is extremely encrypted and protected so none your data are shared or exposed) but because in this way it is possible a better management of your NFTs. You can also check the status in real time of your transactions on the Blockchain scanner.

[Read More →](#)

No interactions done yet! Start notaring now and monitor your transactions to watch them here!

↑

La sezione del monitoraggio pieno in modalità leggera:



Wallet


Upload

Check

Remove


Monitoring

Home




Remove

Interaction date: Thu, 07 Jul 2022 10:22:55 GMT
Interaction owner: 0x46eea69ea008c13e676819bb3584375dafc770cc
Name: Nuovo NFT
Date: Thu, 07 Jul 2022 10:19:57 GMT
Comments: Commento al NFT
Owner: 0x46eea69ea008c13e676819bb3584375dafc770cc



Check

Interaction date: Thu, 07 Jul 2022 10:21:26 GMT
Interaction owner: 0x46eea69ea008c13e676819bb3584375dafc770cc
Name: Nuovo NFT
Date: Thu, 07 Jul 2022 10:19:57 GMT
Comments: Commento al NFT
Owner: 0x46eea69ea008c13e676819bb3584375dafc770cc



Upload

Interaction date: Thu, 07 Jul 2022 10:19:57 GMT
Interaction owner: 0x46eea69ea008c13e676819bb3584375dafc770cc
Name: Nuovo NFT
Date: Thu, 07 Jul 2022 10:19:57 GMT
Comments: Commento al NFT
Owner: 0x46eea69ea008c13e676819bb3584375dafc770cc

Il footer:



Manage NFTs uniquely yours, by uploading documents, checking their authenticity, and removing them when you want! Monitor the correctness of your transactions as well! Notarization is solid, practical, and safe thanks to AlphaNotary! Start right now and enjoy a completely new era of NFTs!



PROJECT LINKS

Home

Notarization

Monitoring

Documentation

Repository

TOPICS LINKS

Blockchain

Notarization

DApp

Ethereum

NFTs

CONTACT ME

Address: Via Miranese, 460/A
30174, Chirignago - Venice, Italy
Phone: +39 339 322 1343
Email: adnangazi.ag@gmail.com
Open hours: Monday - Friday
9:00AM - 6:00PM

Designed, developed, and managed by Adnan Latif Gazi
© Copyright 2022 - All Rights Reserved

Analisi tecnica

Per l'intero processo di realizzazione, l'attenzione è stata posta tanto sull'ottenimento di un buon risultato finale e che rispettasse tutti i vincoli preventivati, quanto sulla qualità del lavoro, in modo da assicurare che il prodotto ottenuto sia il miglior risultato al quale si potesse ambire. Ciò hanno confluato in prestazioni del sistema che vale la pena analizzare tecnicamente, quale il costo delle transazioni. Di seguito sono riportate i costi delle transazioni per ogni operazione messo a disposizione dell'utente, in ogni sua modalità:

Costo transazioni					
Test	Lite mode	Operazione	Costo	Media totale	Differenza
#1	No	Upload	0,00082326	0,00185042	77%
	No	Check	0,00054228		
	No	Remove	0,00048488		
	Sì	Upload	0,00015754	0,00042755	
	Sì	Check	0,00011982		
	Sì	Remove	0,00015019		
#2	No	Upload	0,00597366	0,01503830	75%
	No	Check	0,00429796		
	No	Remove	0,00476668		
	Sì	Upload	0,00158410	0,00381620	
	Sì	Check	0,00092370		
	Sì	Remove	0,00130840		
#3	No	Upload	0,00614142	0,01512158	75%
	No	Check	0,00429772		
	No	Remove	0,00468244		
	Sì	Upload	0,00158386	0,00381548	
	Sì	Check	0,00092346		
	Sì	Remove	0,00130816		
				Differenza totale	75%

Questo conclude che la modalità leggera diminuisce i costi delle transazioni del notevole 75%, il che rappresenta una differenza colossale, soprattutto considerando la situazione a lungo termine, in cui si prevede un uso intensivo del sistema, con molteplici transazioni ad ogni istante, e il loro costo in una rete vera di Blockchain, in cui sono generalmente più elevati rispetto ad una rete di prova.

È inoltre, necessario sottolineare come i test sui costi delle transazioni siano stati fatti eseguendo il programma in locale, in quanto più stabile: le reti reali sono molto variabili, e pertanto ad ogni istante, anche se presi in momenti consecutivi, presentano costi molto differenti, (dipendenti dalla commissione in tempo reale che la rete richiede, a sua volta determinato dal numero di miners a sorreggerla in quel momento) sfalsando completamente il test.

Mantenimento

Sviluppo

Segue una lista degli sviluppi futuri che sarebbe possibile effettuare al sistema:

- **Versione Express dell'applicazione:** necessario per la distribuzione in un server. Il problema del sistema attuale è l'assenza della configurazione esplicita della porta su cui viene eseguito il programma, in quanto, non essendo un'applicazione Express, ciò viene gestito automaticamente. Questo particolare impedisce il caricamento in un server, che viene effettuato correttamente, ma in fase di esecuzione, non si riesce ad ascoltare il programma.
- **Introduzione framework per il front-end (Angular):** consigliabile nel caso si intenda aumentare le funzionalità del programma. Attualmente la semplicità del sistema non ne costringe l'uso. La scelta di Angular è consigliabile per allinearsi alle tecnologie usate dall'azienda e per la popolarità del linguaggio, che garantisce grande documentazione e supporto.
- **Distribuzione in un server:** consigliabile per evitare di eseguire tutte le applicazioni richieste per l'avvio, per non essere vincolati ad avere tutto l'ambiente configurato, e per mettere a disposizione al pubblico il prodotto.
- **Automatizzazione delle transazioni:** necessario per procedere all'API di AlphaNotary e comodo per evitare all'utente di confermare ogni volta l'avvio di una transazione.
- **API di AlphaNotary:** necessario per integrare il sistema a quello aziendale. Aiuterebbe la modularità dell'infrastruttura per altro, in quanto le componenti logiche sarebbero ancora più separate e intercambiabili.
- **Gestione dell'account e abbonamento per i clienti:** consigliabile se si intende commercializzare il prodotto, rendendolo a pagamento.

FAQ

Segue una lista delle domande più comuni porsi sul prodotto, e le relative risposte esaustive:

- **Cos'è la modalità leggera?**
La modalità leggera (Lite mode) passa a uno Smart Contract più leggero, che evita di monitorare le tue transazioni: tutte le funzionalità principali vengono mantenute, solo che non puoi vedere il registro delle tue azioni per una maggiore velocità operativa e minori costi di transazione.
- **Che cos'è la modalità completa?**
La modalità completa è quella predefinita e passa a uno Smart Contract più pesante, che monitora le tue transazioni in modo da poter vedere il registro delle tue azioni per tracciare e controllare la correttezza del flusso di lavoro del processo di autenticazione.
- **Come faccio ora a non esporre i miei documenti?**
I tuoi documenti sono al sicuro perché AlphaNotary non li salva né li conserva. Sul tuo dispositivo e solo lì i tuoi documenti vengono presi, calcolato immediatamente il codice hash e subito rimosso. Gli unici contenuti esposti sono i codici hash, ma vengono crittografati più volte durante i processi di notarile e monitoraggio e, a peggiorare le cose, i codici hash non consentono di ricreare da essi il documento originale.
- **Come inizio a utilizzare AlphaNotary?**

Tutto ciò di cui hai bisogno per iniziare ad annotare è avere l'estensione MetaMask sul tuo browser: installala dal marketplace delle estensioni del browser, quindi crea lì il tuo account. Dovrai anche configurare la rete che desideri utilizzare e infine caricare il tuo portafoglio con le monete come. Verifica anche di avere un browser che supporti queste tecnologie.

- **Come posso controllare le mie interazioni Blockchain?**

Ogni volta che interagisci con la Blockchain, MetaMask crea una nuova transazione che devi confermare. Da quella pagina puoi ottenere il link necessario per accedere al sito Web di scansione Blockchain della tua rete attuale. Nella pagina di scansione vedrai tutti i dettagli in tempo reale delle tue transazioni.

- **Come posso contribuire ad AlphaNotary?**

Sono molto felice di vederti qui, significa che ti è piaciuto molto il nostro prodotto. AlphaNotary è completamente gratuito e open source, quindi basta andare nel repository, studiarne la documentazione ed estrarre una richiesta per contribuire, saremo molto pronti a collaborare! Puoi anche segnalarci se preferisci.

- **Basta dare un'occhiata...**

È abbastanza comprensibile se non vuoi iniziare a usare AlphaNotary. Sugeriamo sempre di dare una possibilità al nostro prodotto, ma se vuoi solo vedere come funziona, puoi fare lo stesso: segui le istruzioni per iniziare ma configura in MetaMask una rete di test o una rete locale invece di utilizzare la rete principale reti. In questo modo non verranno coinvolti soldi veri: per le reti di test è necessario richiedere i faucet (piccola quantità di monete false utilizzabili solo nelle reti di test) all'apposito sito web; per la rete locale suggeriamo di installare Ganache, e automaticamente tutto verrà impostato.

- **Cosa fare in caso di errori?**

La mancanza di un server rende AlphaNotary resiliente agli errori comuni, quindi il sistema dovrebbe sempre funzionare. Ma se ricevi un errore, prova ad aggiornare il sito Web e inoltre MetaMask. Prova anche a controllare i molti log degli errori che il sistema stampa per vedere cosa c'è che non va. Prova a controllare lo stato della tua rete e l'operazione che stavi cercando di fare sono ulteriori passaggi. Infine, non esitare a contattarci se nessuna di queste soluzioni funziona: saremo felici di aiutarti!

Utili

Glossario

Segue una lista di termini, ognuno con una definizione, che si ritiene possano essere utili per la piena comprensione del dominio del progetto:

- **Blockchain:** la blockchain (letteralmente catena di blocchi) è una struttura dati condivisa e immutabile. È definita come un registro digitale le cui voci sono raggruppate in blocchi, concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia. Sebbene la sua dimensione sia destinata a crescere nel tempo, è immutabile nel concetto di quanto. Il suo contenuto una volta scritto tramite un processo normato, non è più né modificabile né eliminabile, a meno di non invalidare l'intero processo. Tali tecnologie sono incluse nella più ampia famiglia dei registri distribuiti (distributed ledger), ossia sistemi che si basano su un registro distribuito, che può essere letto e modificato da più nodi di una rete. Non è richiesto che i nodi coinvolti conoscano l'identità reciproca o si fidino l'uno dell'altro perché, per garantire la coerenza tra le varie copie, l'aggiunta di un nuovo blocco è globalmente regolata da un protocollo condiviso. Una volta autorizzata l'aggiunta del nuovo blocco, ogni nodo aggiorna la propria copia privata. La natura stessa della struttura dati garantisce l'assenza di una sua manipolazione futura. Le caratteristiche che accomunano i sistemi sviluppati con le tecnologie della blockchain e dei registri distribuiti sono: digitalizzazione dei dati, decentralizzazione, disintermediazione, tracciabilità dei trasferimenti, trasparenza/verificabilità, immutabilità del registro e programmabilità dei trasferimenti. Grazie a tali caratteristiche, la blockchain è considerata pertanto un'alternativa in termini di sicurezza, affidabilità, trasparenza e costi alle banche dati e ai registri gestiti in maniera centralizzata da autorità riconosciute e regolamentate (pubbliche amministrazioni, banche, assicurazioni, intermediari di pagamento, ecc.).
- **Notarizzazione:** la notarizzazione è il processo eseguito dal notaio o, nella antica dizione tuttora talvolta usata, notaro (dal latino notare ossia annotare, prender nota), è il soggetto al quale è affidata la funzione di garantire la validità dei contratti, degli atti giuridici civili e dei negozi giuridici, attribuendo pubblica fede agli atti e sottoscrizioni apposte alla sua presenza.
- **DApp:** un'applicazione decentralizzata (DApp, dApp, Dapp o dapp) è un'applicazione che può funzionare in modo autonomo, in genere attraverso l'uso di contratti intelligenti, che viene eseguita su un sistema informatico decentralizzato, blockchain o altro sistema di contabilità distribuita. Come le applicazioni tradizionali, le DApp forniscono alcune funzioni o utilità ai propri utenti. Tuttavia, a differenza delle applicazioni tradizionali, le DApp funzionano senza l'intervento umano e non sono di proprietà di nessuna entità, ma distribuiscono token che rappresentano la proprietà. Questi token vengono distribuiti secondo un algoritmo programmato agli utenti del sistema, diluendo la proprietà e il controllo della DApp. Senza un'entità che controlla il sistema, l'applicazione diventa decentralizzata. Le applicazioni decentralizzate sono state rese popolari dalle tecnologie di registro distribuito (DLT), come la blockchain di Ethereum, su cui sono costruite le DApp, tra le altre blockchain pubbliche. La natura affidabile e trasparente delle DApp ha portato a maggiori sviluppi nell'utilizzo di queste funzionalità all'interno dello spazio della finanza decentralizzata (DeFi). Le DApp sono suddivise in 17 categorie: scambi, giochi, finanza, gioco d'azzardo, sviluppo, archiviazione,

ad alto rischio, portafoglio, governance, proprietà, identità, media, social, sicurezza, energia, assicurazioni e salute.

- **Smart Contract:** gli Smart Contract (in italiano: contratto intelligente) sono protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale. Gli Smart Contract, di solito, hanno anche un'interfaccia utente e spesso simulano la logica delle clausole contrattuali.
- **Wallet:** un Wallet è sinonimo di portafoglio elettronico, ovvero un programma o un servizio web che permette agli utenti di memorizzare e controllare in maniera centralizzata le proprie informazioni personali inerenti agli acquisti online, come login, password, indirizzi di spedizione e dettagli dei propri strumenti di pagamento come carte di credito o altri servizi di pagamento collegati a strumenti o conti bancari o di moneta elettronica. Un portafoglio elettronico fornisce una adeguata, rapida ed agevole tecnologia che permette all'utente di effettuare acquisti di prodotti presso qualunque persona o negozio al mondo.
- **Ethereum:** Ethereum è una piattaforma decentralizzata del Web 3.0 per la creazione e pubblicazione peer-to-peer di contratti intelligenti (Smart Contracts) creati in un linguaggio di programmazione Turing-completo. La criptovaluta a esso legata, Ether, è seconda in capitalizzazione dietro ai Bitcoin.
- **NFT:** un non-fungible token (NFT, in italiano gettone non fungibile o gettone non riproducibile) è un tipo speciale di token che rappresenta l'atto di proprietà e il certificato di autenticità scritto su catena di blocchi di un bene unico (digitale o fisico); i gettoni non fungibili non sono quindi reciprocamente intercambiabili; cioè in contrasto con le criptovalute, come Bitcoin e molti gettoni di rete o di utilità, che sono per loro stessa natura fungibili, ovvero possono essere duplicati infinite volte in copie esattamente identiche ed interscambiabili (non è possibile dunque definire univocamente un'identità del singolo gettone che lo differenzi da tutti gli altri, rendendo perciò tutte le copie equivalenti ed identiche al gettone originale, e anche in relazioni agli usi e funzioni).
- **Miner:** il mining, nel contesto della tecnologia blockchain, è il processo di aggiunta di transazioni al grande registro pubblico distribuito delle transazioni esistenti, noto come blockchain. Il termine è meglio conosciuto per la sua associazione con bitcoin, sebbene altre tecnologie che utilizzano il Blockchain utilizzino il mining. Il mining di bitcoin premia le persone che eseguono operazioni di mining con più bitcoin. Il mining di blockchain comporta l'aggiunta di transazioni al registro blockchain esistente delle transazioni distribuite tra tutti gli utenti di una blockchain. Mentre il mining è principalmente associato al bitcoin, anche altre tecnologie che utilizzano una blockchain utilizzano il mining. Il mining implica la creazione di un hash di un blocco di transazioni che non può essere facilmente falsificato, proteggendo l'integrità dell'intera blockchain senza la necessità di un sistema centrale. L'estrazione viene in genere eseguita su un computer dedicato, poiché richiede una CPU veloce, oltre a un maggiore consumo di elettricità e più calore generato rispetto alle normali operazioni del computer. L'incentivo principale per il mining è che gli utenti che scelgono di utilizzare un computer per il mining vengono ricompensati per farlo. Nel caso di bitcoin, sono 25 bitcoin per hash. Questo è il motivo per cui alcuni hacker utilizzano macchine in cui si rompono per estrarre bitcoin, facendo in modo che una vittima inconsapevole paghi i costi del mining senza trarne alcun vantaggio.

- **Web3.0:** in informatica il Web 3.0 è un termine a cui corrispondono significati diversi, volti a descrivere l'evoluzione dell'utilizzo del web e l'interazione fra gli innumerevoli percorsi evolutivi possibili. Questi includono trasformare il web in un database, cosa che faciliterebbe l'accesso ai contenuti da parte di molteplici applicazioni che non siano dei browser; sfruttare al meglio le tecnologie basate sull'intelligenza artificiale; il web semantico; il geospatial web; l'implementazione di una blockchain distribuita che supporti un linguaggio Turing completo.
- **Faucet:** un crypto faucet è una app o un sito Web che distribuisce piccole quantità di criptovalute come ricompensa per il completamento di attività facili. Viene loro dato il nome di "rubinetti" perché le ricompense sono piccole, proprio come piccole gocce d'acqua che gocciolano da un rubinetto che perde. Tuttavia, nel caso dei criptovalute, piccole quantità di criptovaluta gratuite o guadagnate vengono inviate al portafoglio di un utente. Per ottenere criptovalute gratuite, gli utenti devono completare attività semplici come visualizzare annunci, guardare video di prodotti, completare quiz, fare clic sui collegamenti (attenzione!) o completare un captcha. I crypto faucet non sono certamente uno schema per arricchirsi rapidamente. Più semplice è il compito, minore è la ricompensa. La maggior parte dei siti Web offre una soglia minima di pagamento; quindi, i premi guadagnati completando le attività vengono depositati in un portafoglio online del sito. Un utente può ritirare questo premio solo dopo aver raggiunto la soglia minima impostata. Con i migliori criptovalute, questo potrebbe richiedere solo un giorno, ma spesso può richiedere più di una settimana.
- **Crypto:** il vocabolo criptovaluta o criptomoneta è l'italianizzazione del termine inglese cryptocurrency e si riferisce a una rappresentazione digitale di valore basata sulla crittografia. L'etimologia del vocabolo deriva dalla fusione di cryptography ("crittografia") e currency (valuta): si tratta di una risorsa digitale paritaria e decentralizzata (non chiaro). Al mondo esistono oltre 17.500 criptovalute. Le criptovalute (o criptomonete) utilizzano tecnologie di tipo peer-to-peer (p2p) su reti i cui nodi risultano costituiti da computer di utenti, situati potenzialmente in tutto il globo. Su questi computer vengono eseguiti appositi programmi che svolgono funzioni di portamonete. Non c'è attualmente alcuna autorità centrale che le controlla. Le transazioni e il rilascio avvengono collettivamente in rete, pertanto non c'è una gestione di tipo centralizzato. Queste proprietà, uniche nel loro genere, non possono essere esplicate dai sistemi di pagamento tradizionale. Il controllo decentralizzato di ciascuna criptovaluta funziona attraverso una tecnologia di contabilità generalizzata (DLT), in genere una blockchain, che funge da database di transazioni finanziarie pubbliche. Un sistema decentralizzato potrebbe essere più resistente ad attacchi informatici o a incidenti operativi rispetto a un sistema accentrato perché il primo continua a operare anche quando uno o più nodi smettono di funzionare.