CertiChain

Requirement Analysis Document

Riferimento	
Versione	1.0
Data	
Destinatario	Prof. Alfredo De Santis, Prof. Christian Esposito
Presentato da	Matteo Ercolino

Introduzione

Contesto e Dominio

Il progetto mira a sviluppare una **piattaforma decentralizzata** per l'emissione, la gestione e la verifica di certificati digitali, sfruttando la tecnologia blockchain di **Ethereum**. L'obiettivo è fornire una soluzione innovativa, sicura e trasparente, che permetta agli **enti certificatori** di rilasciare certificati autenticabili in modo pubblico e decentralizzato, senza la necessità di intermediari centralizzati.

L'adozione della tecnologia blockchain garantisce **immutabilità** e **trasparenza**, eliminando il rischio di frodi, contraffazioni e alterazioni dei dati. Grazie alla verifica immediata e accessibile da qualsiasi parte interessata, la piattaforma fornisce una maggiore fiducia e tracciabilità lungo l'intero ciclo di vita del certificato.

Questa soluzione risulta particolarmente vantaggiosa per settori quali il mondo accademico, le certificazioni professionali e l'industria, dove l'affidabilità e l'autenticità delle credenziali rappresentano elementi fondamentali per la crescita e la credibilità degli utenti.

Obiettivi del Progetto

L'obiettivo principale del progetto è la creazione di una piattaforma decentralizzata che consenta a istituzioni accademiche e organizzazioni di emettere certificati digitali sulla blockchain, garantendo autenticità, immutabilità e verificabilità pubblica.

I certificati digitali saranno emessi come **NFT (Non-Fungible Tokens)** su una blockchain pubblica o privata e saranno collegati ai relativi metadati, che includono informazioni come il nome del corso, l'istituzione emittente e la data di rilascio. Questi metadati saranno memorizzati in modo sicuro e decentralizzato tramite **IPFS (InterPlanetary File System)**, garantendo la disponibilità dei dati senza rischio di manomissione o perdita.

La piattaforma dovrà essere user-friendly, offrendo strumenti intuitivi per l'emissione, la verifica e la gestione dei certificati, con un focus su sicurezza, scalabilità e facilità di adozione da parte degli utenti finali.

Sistema corrente e sistema proposto

Sistema corrente

Attualmente, la gestione e la verifica dei certificati digitali avviene principalmente attraverso sistemi centralizzati, come database gestiti da istituzioni accademiche, enti di formazione e aziende certificatrici. Questi sistemi presentano numerose limitazioni, tra cui la dipendenza da intermediari per l'emissione e la verifica dei certificati. Gli utenti devono necessariamente rivolgersi agli enti certificatori per ottenere copie ufficiali dei certificati o per dimostrarne l'autenticità, il che comporta tempi di attesa e costi amministrativi elevati.

Un altro problema significativo riguarda la contraffazione. I certificati cartacei e digitali, se non adeguatamente protetti, possono essere facilmente alterati o falsificati, compromettendo la credibilità degli istituti e dei beneficiari. La verifica dell'autenticità di un

certificato avviene spesso tramite richieste manuali o l'accesso a database privati, i quali non sono sempre facilmente accessibili né aggiornati in tempo reale.

La condivisione dei certificati rappresenta un'ulteriore sfida, poiché gli utenti sono costretti a inviare documenti cartacei o digitali in formato PDF, che possono essere smarriti, danneggiati o alterati senza lasciare traccia. Inoltre, la conservazione dei dati in sistemi centralizzati espone le informazioni a rischi di perdita o violazioni della privacy a causa di attacchi informatici. Un'altra limitazione è la scarsa interoperabilità tra i diversi enti certificatori, che spesso adottano formati e procedure differenti, rendendo complesso il riconoscimento delle credenziali in ambito internazionale o su diverse piattaforme.

Sistema proposto

Il sistema proposto introduce una piattaforma decentralizzata basata sulla tecnologia blockchain di Ethereum per l'emissione, la gestione e la verifica dei certificati digitali. L'obiettivo è eliminare la dipendenza da autorità centralizzate, offrendo un sistema sicuro, trasparente e accessibile a tutti gli attori coinvolti. I certificati digitali saranno emessi come NFT (Non-Fungible Tokens), garantendo un'identità univoca e non modificabile per ciascun certificato.

Attori e Stakeholder

Gli attori principali coinvolti nel sistema sono:

- **Enti Certificatori**: Università, enti di formazione e aziende che emettono certificati digitali. Sono responsabili della creazione, gestione e revoca dei certificati, garantendo che solo informazioni verificate vengano registrate sulla blockchain.
- **Beneficiari**: Studenti e professionisti che ricevono i certificati digitali. Devono poter accedere facilmente ai loro certificati, condividerli e dimostrarne l'autenticità in qualsiasi momento.
- **Verificatori**: Aziende, istituzioni accademiche e terze parti che verificano la validità dei certificati. Necessitano di un sistema rapido e affidabile per confermare l'autenticità dei certificati.

Descrizione del Sistema

Requisiti Funzionali

- **FR1 - Emissione dei Certificati**: Gli enti certificatori devono poter emettere certificati digitali associati a un identificativo univoco e all'indirizzo Ethereum del beneficiario. Ogni certificato deve includere informazioni essenziali come nome del corso, istituzione emittente e data di rilascio. L'emissione dovrà avvenire attraverso la creazione di un NFT, garantendo l'unicità del certificato.
- **FR2 - Verifica dei Certificati**: Gli utenti devono poter verificare l'autenticità dei certificati tramite una semplice ricerca sulla piattaforma, utilizzando un identificativo univoco o il wallet address del beneficiario. Il sistema deve fornire accesso immediato ai metadati del certificato memorizzati su IPFS e garantire che il certificato non sia stato alterato o revocato.
- **FR3 - Revoca dei Certificati**: Gli enti certificatori devono avere la possibilità di revocare un certificato in caso di errore, frode o ritiro del titolo. Il certificato revocato deve essere visibile come non valido durante la verifica, con la relativa motivazione della revoca.
- **FR4 - Accesso degli Utenti e Beneficiari**: I beneficiari devono poter accedere ai propri certificati attraverso un'interfaccia utente intuitiva, che permetta loro di visualizzare e condividere i certificati attraverso un link pubblico o un QR code collegato alla blockchain.

Requisiti Non Funzionali

- **Sicurezza**: Il sistema deve garantire la sicurezza dei dati e delle transazioni mediante l'uso di crittografia avanzata e meccanismi di autenticazione sicura come wallet digitali basati su Ethereum.
- **Immutabilità**: Le informazioni registrate sulla blockchain devono essere immutabili, impedendo qualsiasi modifica non autorizzata dei certificati una volta emessi.
- **Usabilità**: L'interfaccia utente deve essere semplice e intuitiva, con una curva di apprendimento minima per enti certificatori e beneficiari. Il sistema deve garantire un'esperienza fluida su dispositivi desktop e mobili.
- **Performance**: Le operazioni di verifica dei certificati devono essere rapide, con tempi di risposta inferiori a 3 secondi. L'accesso ai dati su IPFS e blockchain deve essere ottimizzato per garantire una fruizione immediata.
- **Costi di Transazione**: La piattaforma deve essere ottimizzata per ridurre i costi delle transazioni sulla blockchain, privilegiando l'uso di soluzioni di storage decentralizzate per minimizzare l'uso on-chain quando non strettamente necessario.
- **Manutenibilità**: La piattaforma deve essere facilmente aggiornabile, con un'architettura modulare che consenta miglioramenti futuri senza interruzioni del servizio.

Architettura del Sistema

Panoramica

Il sistema è progettato secondo un'architettura decentralizzata basata sulla blockchain di Ethereum. L'architettura prevede una suddivisione in tre livelli principali.

Livello di Presentazione

- Include l'interfaccia utente web, accessibile tramite browser, che consente a enti certificatori e beneficiari di interagire con la piattaforma.
- Fornisce funzionalità di autenticazione tramite wallet Ethereum come MetaMask.
- Permette la visualizzazione e la condivisione dei certificati digitali.

Livello Applicativo

- Comprende gli smart contract Solidity distribuiti sulla blockchain di Ethereum, responsabili della gestione dei certificati digitali sotto forma di NFT.

Livello Dati

- Memorizza i certificati e i relativi metadati in modo decentralizzato su IPFS (InterPlanetary File System).
- I riferimenti ai dati su IPFS vengono memorizzati negli smart contract per garantire la persistenza e l'accessibilità.

Componenti Principali

Frontend Web Application

La piattaforma web fornisce un'interfaccia user-friendly per l'emissione, la verifica e la condivisione dei certificati digitali.

- Autenticazione tramite MetaMask.
- Dashboard per enti certificatori e beneficiari.
- Funzioni di verifica pubblica dei certificati.

Smart Contract su Ethereum

Implementati in Solidity, i contratti intelligenti consentono la gestione decentralizzata dei certificati digitali. Le funzionalità principali includono:

- Emissione di certificati come NFT.
- Verifica dell'autenticità.
- Revoca dei certificati.
- Controllo delle autorizzazioni per gli enti certificatori.

Storage Decentralizzato (IPFS)

I certificati e i loro metadati vengono archiviati in IPFS, garantendo accesso distribuito e affidabile. L'hash generato viene memorizzato negli smart contract per garantirne l'integrità.

Wallet Ethereum

I wallet digitali, come MetaMask, vengono utilizzati per gestire le credenziali di accesso e interagire con gli smart contract, consentendo l'emissione e la verifica dei certificati.

Backend API (Opzionale)
Un backend basato su Node.js e Express può essere implementato per gestire operazioni non critiche come notifiche, analisi e reportistica.

Flusso di Dati e Interazioni
Il flusso dei dati all'interno del sistema segue le seguenti fasi principali:

1. **Emissione del Certificato:**
   - L'ente certificatore accede alla piattaforma tramite wallet Ethereum.
   - Inserisce i dettagli del certificato tramite l'interfaccia web.
   - I dati vengono caricati su IPFS, e l'hash IPFS viene memorizzato nella blockchain come NFT.
   - Il certificato viene assegnato al wallet Ethereum del beneficiario.
2. **Verifica del Certificato:**
   - Un verificatore inserisce l'ID del certificato sulla piattaforma web.
   - La piattaforma richiama lo smart contract per verificare la validità e recuperare l'hash IPFS.
   - Il certificato viene recuperato e mostrato all'utente.
3. **Revoca del Certificato:**
   - L'ente certificatore può revocare un certificato aggiornando il suo stato sulla blockchain.
   - Il certificato viene contrassegnato come non valido e non potrà più essere utilizzato.
4. **Condivisione del Certificato:**
   - Il beneficiario può condividere il proprio certificato tramite un link pubblico IPFS o un QR code generato automaticamente.

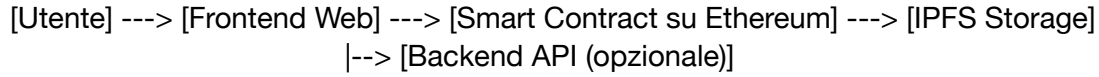
Diagrammi Architetturali
Diagramma a Blocchi dell'Architettura Generale


Diagramma di Emissione del Certificato


Diagramma di Verifica del Certificato


Modellazione del Sistema

Scenari di Utilizzo

Scenario 1: Emissione di un Certificato Digitale

Un'università, in qualità di ente certificatore, desidera emettere un certificato digitale per un corso completato da uno studente. L'amministratore accede alla piattaforma tramite il proprio wallet Ethereum, compila i dettagli del certificato (nome dello studente, nome del corso, data di completamento), e conferma l'emissione. I dati vengono archiviati in modo decentralizzato su IPFS e l'hash generato viene registrato nella blockchain sotto forma di NFT. Lo studente riceve una notifica e può visualizzare il certificato sulla piattaforma.

- **Attori coinvolti**: Ente certificatore, Beneficiario (Studente), Smart Contract, IPFS.
- **Pre-condizioni**: L'ente certificatore è autenticato sulla piattaforma.
- **Post-condizioni**: Il certificato è registrato su blockchain e disponibile per la verifica.

Scenario 2: Verifica di un Certificato

Un’azienda riceve un certificato digitale da un candidato durante un processo di selezione. L’azienda accede alla piattaforma e inserisce l’ID del certificato per verificarne la validità. Il sistema recupera i dati dallo smart contract e mostra le informazioni essenziali, inclusa la conferma dell’autenticità tramite hash IPFS. L’azienda verifica il certificato.

- **Attori coinvolti**: Verificatore (Azienda), Smart Contract, IPFS.
- **Pre-condizioni**: Il certificato deve essere stato precedentemente emesso.
- **Post-condizioni**: Il verificatore ha conferma dell’autenticità del certificato.

Scenario 3: Revoca di un Certificato

Un ente certificatore individua un errore nel certificato di uno studente e decide di revocarlo. L'amministratore accede alla piattaforma, ricerca il certificato, e seleziona l'opzione di revoca. Lo smart contract aggiorna lo stato del certificato su blockchain, segnalandolo come non valido. Qualsiasi verifica futura restituirà lo stato di "Revocato".

- **Attori coinvolti**: Ente certificatore, Beneficiario, Smart Contract.
- **Pre-condizioni**: Il certificato deve essere stato emesso con successo.
- **Post-condizioni**: Il certificato è marcato come revocato e non più valido.

Scenario 4: Condivisione di un Certificato Digitale

Un beneficiario, dopo aver ricevuto un certificato digitale sotto forma di NFT, desidera condividerlo con un datore di lavoro o un’istituzione per dimostrare le proprie credenziali. Accedendo alla piattaforma, visualizza l'elenco dei certificati di sua proprietà e seleziona quello da condividere. Il sistema fornisce un link univoco alla certificazione registrata su blockchain e un QR code che rimanda alla verifica del certificato. Il beneficiario condivide il link o il QR code con la parte interessata, che potrà verificare l’autenticità in tempo reale.

- **Attori coinvolti**: Beneficiario, Verificatore (azienda o ente), Smart Contract, IPFS.
- **Pre-condizioni**: Il certificato deve essere stato precedentemente emesso e disponibile nel wallet del beneficiario.
- **Post-condizioni**: Il certificato viene visualizzato correttamente dal verificatore senza possibilità di alterazione.

Use Cases

UC1 - Emissione di un Certificato

Caso d'uso	Emissione di un Certificato
Attori principali	Ente Certificatore
Descrizione	L'ente certificatore emette un certificato NFT registrandolo sulla blockchain.
Pre-condizioni	L'ente certificatore deve essere autenticato sulla piattaforma.
Post-condizioni	Il certificato viene emesso e associato al beneficiario.
Flusso principale	1. L'ente accede alla piattaforma. 2. Inserisce i dettagli del certificato. 3. Conferma l'emissione. 4. Il certificato viene registrato su blockchain e collegato all'indirizzo del beneficiario.
Flussi alternativi	1a. Se l'autenticazione fallisce, l'emissione viene bloccata. 2a. Se i dati sono incompleti, viene richiesto il completamento.

UC2 - Verifica di un Certificato

Caso d'uso	Verifica di un Certificato
Attori principali	Verificatore (Azienda, Istituzione)
Descrizione	Il verificatore controlla la validità di un certificato tramite l'ID univoco.
Pre-condizioni	Il certificato deve essere stato precedentemente emesso.
Post-condizioni	Il certificato viene verificato e visualizzato con tutte le informazioni associate.
Flusso principale	1. Il verificatore accede alla piattaforma. 2. Inserisce l'ID del certificato. 3. Il sistema recupera le informazioni dal blockchain/IPFS. 4. Mostra i dettagli del certificato.
Flussi alternativi	1a. Se l'ID non esiste, viene mostrato un messaggio di errore. 2a. Se il certificato è revocato, viene mostrato come non valido.

UC3 - Revoca di un Certificato

Caso d'uso	Revoca di un Certificato
Attori principali	Ente Certificatore
Descrizione	L'ente certificatore revoca un certificato esistente, rendendolo non più valido.
Pre-condizioni	Il certificato deve essere stato precedentemente emesso.
Post-condizioni	Il certificato viene marcato come revocato e non può essere utilizzato.

Caso d'uso	Revoca di un Certificato
Flusso principale	1. L'ente certificatore accede alla piattaforma. 2. Seleziona il certificato da revocare. 3. Conferma la revoca. 4. Il sistema aggiorna lo stato del certificato.
Flussi alternativi	1a. Se il certificato non esiste, viene visualizzato un errore. 2a. Se l'utente non ha i permessi, l'operazione viene bloccata.

UC4 - Visualizzazione di un Certificato

Caso d'uso	Visualizzazione di un Certificato
Attori principali	Beneficiario
Descrizione	Il beneficiario visualizza i propri certificati digitali registrati sulla blockchain.
Pre-condizioni	Il beneficiario deve essere autenticato sulla piattaforma.
Post-condizioni	Il certificato viene visualizzato e può essere scaricato o condiviso.
Flusso principale	1. Il beneficiario accede alla piattaforma. 2. Visualizza l'elenco dei certificati. 3. Seleziona un certificato per visualizzarne i dettagli. 4. Può scaricare o condividere il certificato.
Flussi alternativi	1a. Se il beneficiario non possiede certificati, viene mostrato un messaggio di avviso.

UC5 - Condivisione di un Certificato

Caso d'uso	Condivisione di un Certificato
Attori principali	Beneficiario, Verificatore
Descrizione	Il beneficiario condivide il certificato con terze parti attraverso un link blockchain o un QR code.
Pre-condizioni	Il certificato deve essere stato emesso correttamente e disponibile nel wallet del beneficiario.
Post-condizioni	Il verificatore riceve il certificato e può verificarne la validità.
Flusso principale	1. Il beneficiario accede alla piattaforma. 2. Seleziona il certificato da condividere. 3. Genera un link o QR code. 4. Condivide il certificato con il verificatore. 5. Il verificatore accede al certificato e ne verifica la validità.
Flussi alternativi	1a. Se il certificato è revocato, il verificatore viene avvisato della non validità. 2a. Se il certificato non è trovato, viene restituito un errore.

Piano di Sviluppo

Roadmap del Progetto

La roadmap del progetto prevede una pianificazione strutturata in più fasi per garantire lo sviluppo efficiente e graduale della piattaforma. Ogni fase include attività specifiche, tempi stimati e obiettivi da raggiungere.

Fase	Attività	Obiettivo
Fase 1 – Analisi e Pianificazione	Raccolta requisiti, analisi del sistema corrente e definizione degli obiettivi.	Definizione chiara degli obiettivi e vincoli.
Fase 2 – Progettazione Architettura	Definizione dell'architettura tecnica, smart contract e infrastruttura decentralizzata.	Architettura scalabile e documentata.
Fase 3 – Sviluppo Smart Contract	Implementazione degli smart contract per emissione e verifica dei certificati.	Contratti solidi e testati su rete di test.
Fase 4 – Sviluppo Frontend	Realizzazione dell'interfaccia web per interazione con smart contract.	Interfaccia intuitiva e user-friendly.
Fase 5 – Testing e Validazione	Test di sicurezza, performance e usabilità del sistema.	Identificazione e correzione di bug.
Fase 6 – Deploy su Testnet	Rilascio su rete test (Goerli, Sepolia) per valutazione pre-produzione.	Validazione e feedback utenti.
Fase 7 – Deploy su Mainnet	Rilascio finale della piattaforma e monitoraggio.	Disponibilità della piattaforma su Ethereum.
Fase 8 – Manutenzione e Scalabilità	Ottimizzazione continua e aggiunta di nuove funzionalità.	Espansione della piattaforma.

Strumenti di Sviluppo e di Test

Sviluppo

Strumento	Scopo	Motivazione
Solidity	Sviluppo degli smart contract su Ethereum.	Linguaggio standard per smart contract su EVM.
Hardhat	Compilazione, testing e deploy degli smart contract.	Strumento avanzato per il ciclo di vita degli SC.
HTML/CSS/ JavaScript	Sviluppo dell'interfaccia utente web nativa.	Soluzione leggera, veloce e facilmente integrabile.
MetaMask	Autenticazione e firma transazioni blockchain.	Wallet più diffuso per Ethereum.

Strumento	Scopo	Motivazione
IPFS	Archiviazione decentralizzata dei certificati.	Memorizzazione sicura e distribuita.
Node.js / Express.js	Backend opzionale per operazioni non on-chain.	Gestione API e operazioni off-chain.